Maurizio Cailotto

Algebra e Geometria Lineari e Quadratiche

Avvertenza. Questo testo è stato distribuito nel corso dell'anno accademico 2023/24 per il corso di Geometria 1 del Corso di Laurea in Matematica dell'Università di Padova. Tuttavia il suo contenuto è notevolmente maggiore del programma effettivamente svolto, e alcuni paragrafi sono di difficile lettura per studenti del primo anno: essi sono stati indicati con ♠ e ♠♠ nel testo, a seconda del grado di difficoltà.

Questo e alcuni testi associati si possono trovare nella parte didattica della mia home page `http://www.math.unipd.it/~maurizio/`.

Da dove viene e dove va questo testo. Essenzialmente non vi è nulla di originale, se non un lavoro di riordino di conoscenze classiche che deve molto a libri e appunti di I.Barsotti, F. Baldassarri, M. Candilera, G.Gerotto e a discussioni con V. Cristante, M. Candilera, L.Fiorot. Si tratta di un manuale di difficile lettura fuori del contesto di un corso universitario, e anche dentro, mi dicono.

Copyright. Tutti i diritti di questo testo sono riservati all'autore (incluse le eventuali edizioni parziali precedenti). Non ne è consentito alcun uso a scopi commerciali. Sono consentite la riproduzione e la circolazione in formato cartaceo o su supporto elettronico portatile ad esclusivo uso scientifico, didattico o documentario, purché il documento non venga alterato in alcun modo, ed in particolare mantenga le corrette indicazioni di data e fonte originale e la presente nota di copyright.

Note TEXniche. Il testo è stato scritto in PlainTEX, e i disegni presenti sono stati sviluppati in `METAPOST`. Siano ringraziati DEK e JDH. Le figure in copertina e controcopertina sono cespuglio e albero di Pitagora, frattali che si ottengono iterando semplici trasformazioni affini.

settembre 2024

Indice

Introduzione **v**

Capitolo O. Strutture insiemistiche ed algebriche di base **1**
1. Insiemi e funzioni. 1
2. Relazioni, equivalenze ed ordini. 7
3. Cardinalità e combinatorica. 10
4. Numeri Naturali e Induzione. 15
5. Permutazioni. 19
6. Numeri Interi. 22
7. Corpi numerici. 29
   9. Numeri complessi (e geometria del piano). 31
   10. Quaternioni di Hamilton. 46
8. Polinomi. 48
9. Esercizi. 55
   1. Esercizi su Insiemi, Funzioni e Relazioni. 55
   2. Esercizi su Cardinali, Naturali, Combinatorica. 57
   3. Esercizi su Interi, Divisione, MCD. 59
   4. Esercizi su Complessi e Polinomi. 61

Capitolo I. Spazi Vettoriali **65**
1. Definizione ed esempi fondamentali. 65
2. Sottospazi e quozienti. 68
3. Dipendenza e indipendenza lineari. Generatori. 70
4. Basi e dimensione. 71
5. Relazione di Grassmann. 75
6. Coordinate (di vettori) ed equazioni (di sottospazi). 76
7. Esercizi. 79

Capitolo II. Applicazioni Lineari e Matrici **83**
1. Applicazioni lineari. 83
2. Matrici. 89
3. Matrici associate ad applicazioni lineari. 93
4. Dualità. 96
5. Esercizi. 99
   1. Esercizi su Applicazioni Lineari. 100
   2. Esercizi su Matrici. 103
   3. Esercizi sulla Dualità. 106

Capitolo III. Sistemi Lineari **107**
1. Sistemi Lineari. 107
2. Riduzione di Gauss. 110
3. Esercizi. 114

Capitolo IV. Determinanti **117**
0. Motivazioni. 117
1. Determinanti e proprietà fondamentali. 118
2. Sviluppi di Laplace e matrici inverse. 121

3. Sviluppi pivotali. 122
4. Determinanti notevoli. 125
5. Rango e determinanti (minori). 133
6. Esercizi. 136

Capitolo V. Forme canoniche 143
1. Equivalenza di matrici. 143
2. Similitudine di matrici. 144
3. Autoteoria. 145
4. Teoria di Hamilton-Cayley e sottospazi stabili. 149
5. Teoria di Jordan. 154
6. Applicazioni. 161
7. Teoria di Frobenius: Forme Canoniche Razionali. 164
8. Esercizi. 170
   1. Esercizi su Autoteoria. 170
   2. Esercizi su Jordan. 175

Capitolo VI. Geometria Affine 179
1. Spazi affini. 179
2. Calcolo baricentrico. 186
3. Trasformazioni affini e affinità. 194
4. Piano affine. 199
5. Spazio affine. 200
6. Spazi affini di dimensione quattro. 205
7. Esercizi. 205

Capitolo VII. Spazi Vettoriali Euclidei ed Hermitiani 211
1. Spazi Vettoriali Euclidei Reali: dot-product, norma e angoli. 211
2. Spazi Vettoriali Euclidei Reali: cross-product e volumi. 216
3. Trasformazioni ortogonali. 221
4. Teorema spettrale reale e sue applicazioni (valori singolari, pseudoinverse). 228
5. Spazi Vettoriali Euclidei Complessi o Spazi Vettoriali Hermitiani. 231
6. Esercizi. 239

Capitolo VIII. Geometria Euclidea ed Hermitiana 243
1. Spazi Euclidei. 243
2. Trasformazioni Euclidee. 247
3. Piano euclideo. 249
4. Spazio euclideo. 252
5. Spazio euclideo di dimensione quattro. 254
6. Spazi Hermitiani. 255
7. Esercizi. 255

Capitolo IX. Geometria Proiettiva 261
0. Motivazioni. 261
1. Spazi Proiettivi. 263
2. Alcuni modelli per gli spazi proiettivi. 270
3. Applicazioni proiettive e proiettività. 275
   1. Definizioni ed esempi 275
   2. ♠♠ Teoremi Fondamentali (della Geometria Proiettiva): proiezioni. 278
   3. ♠♠ Teoremi Fondamentali (della Geometria Proiettiva): collineazioni. 279
   4. Teoria di Jordan delle proiettività (omologie, involuzioni....) 279
4. Spazi Proiettivi, Spazi Affini e Spazi Euclidei. 286

5. Retta proiettiva e birapporti. 290
6. Piano proiettivo e costruzioni classiche. 296
7. Problemi. 304
1. Problemi di geometria proiettiva. 304
2. Problemi sulle proiettività. 307
3. Problemi dagli esami. 309

Appendice A. Esercizi per sviluppare l'Immaginazione. 315

Introduzione

Questo testo viene usato in un corso dal nome *Geometria 1*, ma sembra in gran parte dedicato ad argomenti di algebra. Quindi conviene spiegare come mai la Geometria all'Università si studia in questo modo, con un salto apparentemente molto grande ripetto alla "Geometria" assiomatica antica che molti hanno studiato nelle scuole superiori, e che ormai ha solo un interesse storico-filosofico-didattico.

La prima sistematizzazione completa della Geometria viene attribuita agli "Elementi" di Euclide, opera che diventa anche un modello di ragionamento chiaro e preciso: da pochi postulati iniziali chiaramente espressi si deducono proprietà via via più complicate con dimostrazioni chiare e precise. Si pensi anche alle imitazioni filosofiche tipo l'"Etica" di Spinoza, o il "Trattato" di Wittenstein.

Il punto principale è che, nonostante Euclide sia considerato per millenni un modello, molte sue "dimostrazioni" non discendono affatto dai suoi postulati (e probabilmente lo sapeva). Per esempio, consideriamo la prima dimostrazione degli "Elementi", ovvero l'esistenza di triangoli equilateri: dati due punti (quindi un lato), si prendono le due circonferenze centrate in un punto e passanti per l'altro (uno dei postulati permette la costruzione delle circonferenze), si prende un punto di intersezione di queste due circonferenze (fa un disegno), e poi si dilunga a mostrare che questo terzo punto con gli altri due forma un triangolo equilatero, ovvero che i tre lati sono uguali tra loro. Il problema è il seguente: come fare per dimostrare che quelle due circonferenze si intersecano? Nessun postulato di Euclide può parlare di intersezione di circonferenze, e in effetti vi sono insiemi di punti e rette che soddisfano a tutti i postulati e in cui quelle due circonferenze non hanno punti in comune (dovreste riuscire a trovarne uno). Quindi è definitivo che la prima dimostrazione degli "Elementi" è incompleta, non può discendere dai postulati (e si fa il disegno esattamente per questo). Essenzialmente tutte le dimostrazioni di Euclide che usano intersezioni di circonferenze (con rette o altre circonferenze) hanno lo stesso problema.

Nel ventesimo secolo Hilbert con i suoi "Fondamenti" costruisce una assiomatica in modo tale che tutte le dimostrazioni di Euclide diventino corrette, ma lo fa aggiungendo molti assiomi, e in particolare l'assioma di continuità, che è, sia come enunciato, sia come uso, decisamente complicato e poco intuitivo, e che serve essenzialmente per "aggiustare" le dimostrazioni che usano intersezioni con circonferenze.

Quindi con la geometria assiomatica, che oggi viene detta "sintetica" (contrapposto ad "analitica"), si arriva all'alternativa: "postulati semplici e dimostrazioni sbagliate" (ma che hanno convinto tutti per secoli!), oppure "dimostrazioni corrette e assiomi complicati". È chiaro che nessuna delle due possibilità è ottimale o soddisfacente. D'altra parte Hilbert mostra anche, sulla base dei suoi assiomi, che i punti del piano possono essere messi in corrispondenza con le coppie ordinate di elementi di una struttura algebrica (un campo) contenente i numeri razionali e chiusa per opportune operazioni algebriche.

In questo modo Hilbert indica di fare la geometria partendo dalla struttura algebrica di base (con una assiomatica molto semplice), e di considerare il piano semplicemente come l'insieme delle coppie ordinate di elementi di quella struttura. Vi sono due vantaggi notevoli nel seguire questa strategia.

In primo luogo le dimostrazioni diventano "conti" che chiunque può controllare, e non vi sono più inganni legati ai disegni.

In secondo luogo si possono studiare allo stesso modo gli spazi in dimensione n (usando n-uple invece di coppie), o anche spazi di dimensione infinita (anche se in questo caso devono intervenire altri strumenti, oltre a quelli algebrici), cosa che sarebbe impraticabile in modo assiomatico-sintetico.

In terzo luogo, questo punto di vista permette di trattare anche spazi geometrici in cui la struttura di base non contiene necessariamente i numeri razionali; per esempio si possono studiare geometrie con un numero finito di punti esattamente con le stesse tecniche con cui di studia la geometria reale (cioè sui numeri reali).

Questo è essenzialmente il motivo per cui in questo corso studieremo la geometria partendo dalle strutture algebriche di campo e di spazio vettoriale. L'approccio algebrico ci permetterà anche

di distinguere meglio quali proprietà geometriche dipendono da una scelta del modo di misurare la distanza tra punti, e quali invece sono indipendenti da questo: per esempio la nozione di punto medio di un segmento, o di baricentro di un triangolo, non dipendono dalla misura di distanza tra i punti. Chiameremo "Geometria Affine" quella che non fa uso di nozioni metriche, "Geometria Conforme" la geometria affine in cui si introduce una nozione di angoli, e "Geometria Euclidea" la geometria affine in cui si introduce la nozione di distanza tra punti (e di conseguenza anche di angoli, vedremo). La geometria classica di Euclide sarà allora semplicemente il caso particolare di Geometria Euclidea in dimensione due (e tre).

Resta ancora da far notare che questi strumenti algebrici di base permetteranno di capire anche Geometrie più generali quali la Geometria Proiettiva (estensione della Geometria Affine), e variando il modo di misurare le distanze tramite strumenti proiettivi, ad uno studio sistematico delle Geometrie non-Euclidee (di cui quella Euclidea è una specie di limite).

A questo punto può sembrare che l'evoluzione del pensiero matematico abbia portato ad una "algebrizzazione" della Geometria, cioè ad uno studio della Geometria tramite strumenti algebrici. In un certo senso è vero anche il contrario: il pensiero matematico moderno tende ormai ad una "geometrizzazione" dell'Algebra, cioè a pensare che ogni struttura algebrica abbia un qualche significato geometrico, e corrisponda a qualche spazio geometrico da scoprire. Questo si sa ormai fare per tutta l'Algebra Commutativa: ogni "anello commutativo con unità", e anche ogni "monoide commutativo con unità", ha uno spazio geometrico associato e ben compreso.

Infine, vogliamo insistere su questo fatto: la presentazione che faremo della geometria moderna è allo stato dell'arte la sistemazione più chiara e che storicamente ha dato i migliori risultati sia teorici sia applicativi. È chiaramente il frutto di secoli se non millenni di pensiero di menti geniali, che hanno segnato un percorso tuttora in divenire, che se si può dire stabile in molti aspetti evolverà ancora certamente in futuro.

È importante nell'affrontare questa materia sia lo studio nozionistico (definizioni, risultati) per cui si deve dare un certo credito allo sviluppo storico di aver distillato le nozioni fondamentali in modo corretto ed efficace, sia capire i metodi proposti ed essere in grado di variarli o di applicarli in altri contesti per ottenere risultati nuovi, non esplicitamente enunciati nel corso. Non è da trascurare il fatto che da uno studio preciso e ragionato della Geometria dovrebbe nascere anche una intuizione nuova e una nuova capacità di immaginazione che a sua volta aiuta nella comprensione degli argomenti trattati.

Capitolo O

Strutture insiemistiche ed algebriche di base

In questo capitolo introduttivo presenteremo alcune nozioni di base già note alla maggior parte degli studenti, ma lo faremo in una forma rigorosa che d'ora in poi deve diventare lo standard nello studio della Matematica. In effetti, la proprietà di linguaggio, la precisione delle definizioni e la chiarezza delle argomentazioni sono strumenti indispensabili per evitare errori ed ambiguità.

Vi sarà anche nel contesto l'occasione di approfondimenti o di sviluppare qualche nuovo concetto.

Nei primi due paragrafi daremo per note le nozioni di numeri interi e di operazioni tra essi; giustificheremo, almeno parzialmente, queste nozioni nei paragrafi successivi.

1. Insiemi e funzioni.

1.1. Diamo per note le nozioni di insieme e di elementi di un insieme, avendo solo cura di specificare che intenderemo fissato una volta per tutte un ambiente (detto Universo) in cui insiemi ed elementi vivono, sufficientemente grande da contenere tutte le costruzioni di cui avremo bisogno per ogni fissata teoria. Questo permette di evitare che nel linguaggio compaiano antinomie antipatiche, seppure poco significative, la più nota delle quali è la nozione dell'"insieme degli insiemi che non appartengono a se stessi" (il quale non può né appartenere, né non appartenere a se stesso). In effetti è la stessa nozione di "insieme di tutti gli insiemi" a generare tali antinomie, ed essa viene esclusa dal fatto di limitare a priori l'Universo di riferimento.

In generale indicheremo con lettere maiuscole quali A, B, C, X, Y, Z gli insiemi e con lettere minuscole quali a, b, c, x, y, z gli elementi. Talvolta le lettere saranno scritte con font diversi (e indicheranno diversi insiemi), talvolta addirittura useremo lettere greche o di altri sistemi di scrittura. Per esempio indicheremo con il simbolo $\varnothing$ e chiameremo insieme vuoto quell'insieme che non contiene alcun elemento.

Per comodità inseriamo una referenza per le lettere greche:

alpha: α, A	beta: β, B	gamma: γ, Γ	delta: δ, Δ	epsilon: ε, ϵ, E	zeta: ζ, Z
eta: η, H	theta: $\vartheta, \theta, \Theta$	iota: ι, I	kappa: $\kappa, \varkappa, K$	lamba: λ, Λ	mu(mi): μ, M
nu(ni): ν, N	xi: ξ, Ξ	omicron: o, O	pi: π, ϖ, Π	rho: ϱ, ρ, P	sigma: $\sigma, \varsigma, \Sigma$
tau: τ, T	upsilon: υ, Υ	phi: φ, ϕ, Φ	psi: ψ, Ψ	chi: χ, X	omega: ω, Ω

e ricordiamo anche alcune lettere ebraiche, di qualche uso in matematica: $\aleph$ (aleph), $\beth$ (beth), $\daleth$ (daleth), $\gimel$ (gimel).

Per dire che un elemento a appartiene ad un insieme A scriveremo $a \in A$. Dunque $a \notin \varnothing$ per qualsiasi elemento a: una barra sul simbolo significa in generale la negazione del simbolo stesso; nel caso specifico: qualsiasi sia a, allora a non appartiene all'insieme vuoto.

Di solito usiamo le parentesi grafe per definire un insieme tramite la lista dei suoi elementi; per esempio scriveremo $\mathbf{3} = \{0, 1, 2\}$, e allora $1 \in \mathbf{3}$, ma $3 \notin \mathbf{3}$; si osservi che $\{\varnothing\}$ è un insieme non vuoto, contenente un unico elemento che è l'insieme vuoto: $\varnothing \in \{\varnothing\}$ (oltre che $\varnothing \subseteq \{\varnothing\}$, come vedremo subito, ma significa un'altra cosa).

1.2. Definizione (Sottinsiemi). *Un insieme B si dice sottinsieme di un altro insieme A e si scrive $B \subseteq A$ se vale la seguente implicazione: per ogni elemento b, se b è elemento di B, allora b è elemento di A. Di solito si usa il simbolo $\forall$ come quantificatore universale ("per ogni"), e il simbolo $\Longrightarrow$ per intendere l'implicazione ("allora"); quindi la frase precedente si potrà scrivere così: $\forall b,\ b \in B \Longrightarrow b \in A$.*

1.2.1. Per esempio $\varnothing \subseteq A$ per ogni insieme A; A stesso è sottinsieme di A per ogni A; questi due sottinsieme si dicono i sottinsiemi impropri o banali di A. Se $B \subseteq A$ e $B \neq A$ (significa che esiste qualche elemento di A che non appartiene a B: usando il simbolo $\exists$ di quantificazione esistenziale si scrive $\exists a \in A,\ a \notin B$), allora si scrive $B \subset A$, e si dice un sottinsieme proprio se non è vuoto.

1.2.2. Se $C \subseteq B$ e $B \subseteq A$, allora $C \subseteq A$, come si verifica subito.

1.2.3. Due insiemi si considerano uguali se e solo se sono formati dagli stessi elementi; dunque possiamo dire che $A = B$ se e solo se valgono contemporaneamente $A \subseteq B$ e $B \subseteq A$. Per dimostrare un'uguaglianza tra due insiemi converrà spesso dimostrare separatamente le due inclusioni.

1.2.4. Per ogni numero intero n, definiamo l'insieme $\mathbf{n} = \{0, 1, 2, \dots, n-1\}$ formato dai numeri naturali minori di n. Allora $\mathbf{n} \subseteq \mathbf{m}$ se e solo se $n \leqslant m$. Useremo spesso il simbolo $\Longleftrightarrow$ per intendere "se e solo se" (qualche volta abbreviato anche "sse"); quindi possiamo scrivere: $\mathbf{n} \subseteq \mathbf{m} \Longleftrightarrow n \leqslant m$.

1.3. Definizione (Unione). *Dati due insiemi A e B, l'insieme unione, indicato con $A \cup B$, è l'insieme formato dagli elementi che appartengono ad A oppure appartengono a B (o anche ad entrambi). In simboli:*

$$A \cup B := \{x \mid x \in A \text{ oppure } x \in B\}$$

ove il simbolo $\mid$ si legge "tale che" (e $:=$ significa che il termine a sinistra è definito essere uguale all'espressione a destra).

1.3.1. Si osservi che $A \subseteq A \cup B$, $B \subseteq A \cup B$ e che ogni altro insieme C contenente sia A che B contiene anche $A \cup B$; in altri termini, $A \cup B$ è il più piccolo insieme contenente sia A che B.

1.3.2. Per ogni tre insiemi A, B, C abbiamo che $(A \cup B) \cup C = A \cup (B \cup C)$, e dunque scriveremo unioni multiple senza specificare le parentesi (associatività). Inoltre abbiamo $A \cup B = B \cup A$ (commutatività), $A \cup A = A$ (idempotenza), $A \cup \varnothing = A$. Si osservi che $A \cup B = A$ se e solo se $B \subseteq A$.

1.3.3. Unioni arbitrarie. Possiamo anche definire unioni di famiglie non necessariamente finite di insiemi nel modo seguente: se I è un insieme (detto spesso "di indici") e per ogni $i \in I$ è dato un insieme A_i, allora definiamo l'unione della famiglia come

$$\bigcup_{i \in I} A_i := \{x \mid \exists i \in I \text{ con } x \in A_i\}\ .$$

1.4. Definizione (Intersezione). *Dati due insiemi A e B, l'insieme intersezione, indicato con $A \cap B$, è l'insieme formato dagli elementi che appartengono sia ad A sia a B. In simboli:*

$$A \cap B := \{x \mid x \in A \text{ e } x \in B\}\ .$$

1.4.1. Si osservi che $A \supseteq A \cap B$, $B \supseteq A \cap B$ e che ogni altro insieme C contenuto sia in A che in B è contenuto anche in $A \cap B$; in altri termini, $A \cap B$ è il più grande insieme contenuto sia in A che in B.

1.4.2. Per ogni tre insiemi A, B, C abbiamo che $(A \cap B) \cap C = A \cap (B \cap C)$, e dunque scriveremo unioni multiple senza specificare le parentesi (associatività). Inoltre abbiamo $A \cap B = B \cap A$ (commutatività), $A \cap A = A$ (idempotenza), $A \cap \varnothing = \varnothing$. Si osservi che $A \cap B = A$ se e solo se $A \subseteq B$.

1.4.3. Intersezioni vuote. Due insiemi si dicono disgiunti se la loro intersezione è vuota; cioè se non hanno alcun elemento in comune.

1.4.4. Intersezioni arbitrarie. Possiamo anche definire intersezioni di famiglie non necessariamente finite di insiemi nel modo seguente: se I è un insieme (detto spesso "di indici") e per ogni $i \in I$ è dato un insieme A_i, allora definiamo l'intersezione della famiglia come

$$\bigcap_{i \in I} A_i := \{x \mid \forall i \in I,\ x \in A_i\}\ .$$

Si osservi che tale intersezione risulta vuota se e solo se per ogni elemento x, esiste un indice i tale che $x \notin A_i$.

1.5. Teorema (leggi distributive). *Unioni finite ed intersezioni finite sono operazioni mutuamente distributive, cioè (espresse per il caso binario)*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad e \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)\ .$$

Più generalmente abbiamo

$$A \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (A \cup A_i) \quad e \quad A \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (A \cap A_i)\ .$$

Dimostrazione. Dimostriamo per esempio la prima delle formule generalizzate, dimostrando separatamente le due inclusioni. Se $x \in A \cup (\bigcap_{i\in I} A_i)$ allora o $x \in A$ oppure $x \in \bigcap_{i\in I} A_i$ (cioè $x \in A_i$ per ogni i). In entrambi i casi abbiamo che $x \in A \cup A_i$ per ogni i, e dunque x appartiene all'intersezione di tutti. Viceversa, se $x \in \bigcap_{i\in I}(A \cup A_i)$, allora $x \in A \cup A_i$ per ogni i; se $x \in A_i$ per ogni i allora $x \in \bigcap_{i\in I} A_i$, altrimenti vi è un j per cui $x \notin A_j$, ma poiché $x \in A \cup A_j$ si deve avere $x \in A$. Allora in entrambi i casi x deve appartenere all'unione di A con $\bigcap_{i\in I} A_i$ □

1.6. Definizione (Complemento). *Dato un insieme A, il suo complemento (nel fissato Universo) è l'insieme degli elementi che non appartengono ad A. Si indica con $\complement A$, oppure A^c (qualche volta $\overline{A}$, ma solo se si evitano confusioni con altre operazioni come la chiusura topologica). Dunque $x \in \complement A$ se e solo se $x \notin A$.*

1.7. Teorema (leggi di De Morgan). *Le relazioni tra complementazione e le operazioni di unione ed intersezione sono date da*

$$\complement(A \cap B) = (\complement A) \cup (\complement B) \quad e \quad \complement(A \cup B) = (\complement A) \cap (\complement B) \ .$$

Più generalmente abbiamo

$$\complement\Big(\bigcap_{i\in I} A_i\Big) = \bigcup_{i\in I} \complement A_i \quad e \quad \complement\Big(\bigcup_{i\in I} A_i\Big) = \bigcap_{i\in I} \complement A_i \ .$$

Dimostrazione. Mostriamo per esempio la prima delle formule generalizzate: $x \in \complement(\bigcap_{i\in I} A_i)$ vale se e solo se $x \notin \bigcap_{i\in I} A_i$, che vale se e solo se $x \notin A_j$ per qualche $j \in I$, dunque se solo se $x \in \complement A_j$ per qualche $j \in I$, e questo vale se e solo se $x \in \bigcup_{i\in I} \complement A_i$. Abbiamo così verificato che i due insiemi contengono esattamente gli stessi elementi. □

1.8. Definizione (Prodotto cartesiano). *Dati due elementi x, y, diciamo coppia ordinata e scriviamo (x, y) la coppia formata dai due elementi dati nell'ordine scritto (x si dice il primo elemento della coppia, e y il secondo; potremmo formalizzare il concetto di coppia ordinata senza ricorrere a nuovi simboli dicendo che una coppia ordinata è un insieme della forma $\{x, \{x, y\}\}$); dunque $(x, y) = (a, b)$ se e solo se $x = a$ e $y = b$; in particolare $(x, y) \neq (y, x)$ (a meno che non sia $x = y$). Dati due insiemi A e B definiamo il loro prodotto cartesiano, indicato con $A \times B$ come l'insieme delle coppie ordinate il cui primo elemento sta in A, e il secondo in B. Dunque:*

$$A \times B := \{(a, b) \mid a \in A,\ b \in B\} \ .$$

1.8.1. A rigor di termini, se abbiamo tre insiemi A, B e C, i prodotti $(A \times B) \times C$ e $A \times (B \times C)$ non sono proprio uguali, ma vedremo parlando di funzioni che essi sono canonicamente in biiezione, e quindi ci permetteremo di identificarli. Di conseguenza parleremo del prodotto cartesiano di più insiemi senza specificare (tramite parentesi) l'ordine in cui le operazioni sono svolte.

Scriveremo spesso A^2 invece di $A \times A$, e in generale A^n invece di $\underbrace{A \times \cdots \times A}_{n \text{ volte}}$.

Allo stesso modo esiste una biiezione canonica tra $A \times B$ e $B \times A$.

1.8.2. Si osservi che $A \times \varnothing = \varnothing$, e viceversa, se $A \times B = \varnothing$, allora uno dei due insiemi tra A e B deve essere vuoto.

1.8.3. Vi sono facili relazioni tra le operazioni prima introdotte e il prodotto cartesiano: per esempio $A \times (B \cup C) = (A \times B) \cup (A \times C)$, e anche $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

D'altra parte in generale vale solo che $(\complement A) \times (\complement B) \subseteq \complement(A \times B)$, l'inclusione nell'altro senso essendo in generale falsa. Farsi un disegno per capire la situazione, e scrivere una formula per $\complement(A \times B)$ (come unione di tre insiemi disgiunti).

1.9. Definizione (Unione disgiunta). *Dati due insiemi A e B, definiamo l'unione disgiunta $A \sqcup B$ come l'insieme $(\{A\} \times A) \cup (\{B\} \times B)$. In generale data una famiglia A_i di insiemi indiciata da un insieme I, definiamo l'unione disgiunta $\coprod_{i\in I} A_i$ come l'insieme $\bigcup_{i\in I} \{i\} \times A_i$.*

1.9.1. In generale $A \sqcup B$ e $B \sqcup A$ non sono proprio uguali, ma si possono identificare in un modo canonico. La differenza rispetto alla unione usuale di insiemi sta nel fatto che gli elementi in comune tra A e B "compaiono due volte" in $A \sqcup B$, mentre "compaiono una sola volta" in $A \cup B$. Vedremo che nel caso che A e B siano disgiunti c'è un modo canonico di identificare $A \sqcup B$ con $A \cup B$.

1.10. Definizione (Differenza). *Dati due insiemi A e B definiamo la differenza $A \smallsetminus B$ tra A e B come l'insieme degli elementi di A che non appartengono a B. Dunque*

$$A \smallsetminus B := \{x \in A \mid x \notin B\}$$

o equivalentemente $A \smallsetminus B = A \cap \complement B$.

1.10.1. Evidentemente abbiamo che $A \smallsetminus B$ è un sottinsieme di A disgiunto da B, ed è in effetti il più grande sottinsieme di A avente la proprietà di essere disgiunto da B.

Si osservi anche che $A \cup B$ è unione dei tre insiemi $A \smallsetminus B$, $A \cap B$ e $B \smallsetminus A$ che sono a due a due disgiunti.

1.10.2. La differenza possiede proprietà simili alla complementazione (che può essere vista come differenza tra l'Universo e un insieme); in particolare

$A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C) = (A \smallsetminus B) \smallsetminus C$;
$(A \cup B) \smallsetminus C = (A \smallsetminus C) \cup (B \smallsetminus C)$;
$A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C)$;
$(A \cap B) \smallsetminus C = (A \smallsetminus C) \cap (B \smallsetminus C)$;
$A \cup (B \smallsetminus C) \supseteq (A \cup B) \smallsetminus C$ (e vale l'uguaglianza sse $A \cap C = \varnothing$);
$A \cap (B \smallsetminus C) = (A \cap B) \smallsetminus C$;
abbiamo l'inclusione $(A \smallsetminus B) \times (A \smallsetminus C) \subseteq (A \times A) \smallsetminus (B \times C)$ (stretta in generale).

1.10.3. Vale anche che $\complement A \smallsetminus \complement B = B \smallsetminus A$ e $A \smallsetminus \complement B = A \cap B$.

1.10.4. Si osservi inoltre che $A \smallsetminus B = \varnothing$ sse $A \subseteq B$; $A \smallsetminus B = A$ sse $A \cap B = \varnothing$; $A \smallsetminus B = A \smallsetminus C$ sse $A \cap B = A \cap C$; $A \smallsetminus A = \varnothing$ e $A \smallsetminus \varnothing = A$.

1.11. Definizione (Differenza simmetrica). *La differenza simmetrica $A \vartriangle B$ di A e B è definita come l'unione di $A \smallsetminus B$ e $B \smallsetminus A$; dalle osservazioni precedenti si vede subito che $A \vartriangle B = (A \cup B) \smallsetminus (A \cap B)$*

1.11.1. Naturalmente $A \vartriangle B = B \vartriangle A$ (da cui l'aggettivo simmetrica), e $A \vartriangle B = \varnothing$ se e solo se $A = B$. Risultano inoltre le seguenti facili relazioni:

$A \cap (B \vartriangle C) = (A \cap B) \vartriangle (A \cap C)$,
$A \vartriangle (B \vartriangle C) = (A \vartriangle B) \vartriangle C$,
$A \vartriangle \complement B = \complement(A \vartriangle B) = \complement A \vartriangle B$;
$\complement A \vartriangle \complement B = A \vartriangle B$.

1.12. Definizione (Potenza o Parti). *Dato un insieme A, l'insieme formato da tutti i sottinsiemi di A si dice parti di A o potenza di A e si indica con $\mathscr{P}(A)$ o $\mathbf{2}^A$; dunque*

$$\mathscr{P}(A) := \{B \mid B \subseteq A\} .$$

1.12.1. Singoletti. Si osservi che $\mathscr{P}(A)$ contiene sempre $\varnothing$ e A stesso, e dunque contiene sempre almeno due elementi se $A \neq \varnothing$; inoltre $\mathscr{P}(\varnothing) = \{\varnothing\}$.

Per ogni $a \in A$, abbiamo che $\{a\}$ (l'insieme contenente come unico elemento a) appartiene a $\mathscr{P}(A)$, $\{a\} \in \mathscr{P}(A)$, e gli insiemi di questo tipo si dicono i singoletti di A.

1.13. Definizione (Funzioni). *Una funzione f di A in B, scritta $f : A \to B$ o $A \xrightarrow{f} B$, è una regola che ad ogni elemento a di A associa un unico elemento $f(a)$ di B. Si dice che A è il dominio e B il codominio di f. Vedremo in seguito che le funzioni di A in B si identificano ad opportuni sottinsiemi di $A \times B$ (il loro grafico). Se abbiamo due funzioni $f : A \to B$ e $g : B \to C$ in cui il dominio della seconda è il codominio della prima, allora possiamo definire una funzione detta composta $g \circ f : A \to C$ che manda $a \in A$ in $g(f(a)) \in C$ (spesso si indica $g \circ f$ semplicemente come gf).*

1.13.1. Talvolta l'insieme delle funzioni di A in B viene indicato con B^A.

1.13.2. (non) Commutatività. Si osservi che se abbiamo due funzioni componibili in entrambi i sensi, allora le due composizioni non sono necessariamente uguali: in generale $g \circ f \neq f \circ g$ per funzioni $f : A \to B$ e $g : B \to A$ anche se $A = B$ (farsi qualche esempio).

1.13.3. Associatività. Se abbiamo una terza funzione $h : C \to D$ allora possiamo formare le composizioni di tre funzioni in due modi possibili, e i risultati coincidono: $h \circ (g \circ f) = (h \circ g) \circ f$ come funzione $A \to D$.

1.13.4. Funzioni identità. Per ogni insieme A esiste una funzione $A \to A$ detta identica che ad ogni elemento associa l'elemento stesso. Si scrive spesso id_A o 1_A. Per ogni funzione $f : A \to B$ abbiamo che $f \circ \mathrm{id}_A = f$ e $\mathrm{id}_B \circ f = f$.

1.13.5. Per ogni insieme A esiste una unica funzione $\varnothing \to A$ (infatti per definire una tale funzione non serve nulla), e per ogni singoletto $\{x\}$ esiste una unica funzione $A \to \{x\}$ (necessariamente tutti gli elementi di A sono mandati nell'unico elemento di $\{x\}$).

1.13.6. Immagini dirette e inverse tramite funzioni. Una funzione $f : A \to B$ determina due altre funzioni, dette immagine diretta ed inversa tramite f.

L'immagine diretta è la funzione $f_* : \mathscr{P}(A) \to \mathscr{P}(B)$ (ma denotata di solito f per abuso di linguaggio) definita per ogni $X \in \mathscr{P}(A)$ (cioè $X \subseteq A$) da $f_*(X) = \{f(a) \mid a \in X\} \in \mathscr{P}(B)$ (si tratta del sottinsieme di B formato dalle immagini tramite f degli elementi di X). Si osservi che valgono le seguenti regole:

$(D1)$ $f_*(X \cup X') = f_*(X) \cup f_*(X')$ per ogni $X, X' \subseteq A$;
$(D2)$ $f_*(X \cap X') \subseteq f_*(X) \cap f_*(X')$ per ogni $X, X' \subseteq A$ (ma in generale questa inclusione è stretta);
$(D3)$ $f_*(\complement X)$ in generale non ha relazioni con $\complement f_*(X)$.

Di solito $f_*(A) \neq B$, e si dice l'immagine di f. Si costruiscano degli esempi per realizzare tutti i casi possibili.

L'immagine inversa tramite f è la funzione $f^* : \mathscr{P}(B) \to \mathscr{P}(A)$ definita per ogni $Y \in \mathscr{P}(B)$ (cioè $Y \subseteq B$) da $f^*(Y) = \{a \in A \mid f(a) \in Y\} \in \mathscr{P}(A)$ (si tratta del sottinsieme di A formato dagli elementi le cui immagini tramite f stanno in Y; di solito si chiama antimmagine di Y tramite f). Si osservi che valgono le seguenti regole:

$(I1)$ $f^*(Y \cup Y') = f^*(Y) \cup f^*(Y')$ per ogni $Y, Y' \subseteq B$;
$(I2)$ $f^*(Y \cap Y') = f^*(Y) \cap f^*(Y')$ per ogni $Y, Y' \subseteq B$;
$(I3)$ $f^*(\complement Y) = \complement f^*(Y)$ per ogni $Y \subseteq B$.

Si osservi anche che $f^*(B) = A$. Si estendano le regole precedenti ai casi di unioni ed intersezioni arbitrarie.

Le composizioni di f_* e f^* danno luogo alle seguenti osservazioni:

(C1) $f^* \circ f_*(X) \supseteq X$ (e l'inclusione in generale è stretta);
(C2) $f_* \circ f^*(Y) \subseteq Y$ (e l'inclusione in generale è stretta, ma per un motivo ovvio: vale in generale che $f_* \circ f^*(Y) = Y \cap f(A)$).

Si consiglia ancora di costruirsi degli esempi per realizzare tutti i casi possibili.

1.13.7. Osserviamo infine le relazioni tra immagine diretta ed inversa e composizione di funzioni:

(IC) $(\mathrm{id}_A)^* = \mathrm{id}_{\mathscr{P}(A)}$ e $(g \circ f)^* = f^* \circ g^*$ se $f : A \to B$ e $g : B \to C$ (si noti l'inversione nella composizione);
(DC) $(\mathrm{id}_A)_* = \mathrm{id}_{\mathscr{P}(A)}$ e $(g \circ f)_* = g_* \circ f_*$ se $f : A \to B$ e $g : B \to C$.

1.13.8. Definizione (Funzioni Iniettive, Suriettive, Biiettive). *Una funzione $f : A \to B$ si dice:*

(I) iniettiva se vale la seguente implicazione: $f(a) = f(a') \Longrightarrow a = a'$ per ogni $a, a' \in A$ (se due elementi di A hanno la stessa immagine in B, allora si tratta dello stesso elemento di A).
(S) suriettiva se vale la seguente condizione: per ogni $b \in B$ esiste $a \in A$ tale che $b = f(a)$ (ogni elemento di B è immagine di qualche elemento di A).
(B) biiettiva se è iniettiva e suriettiva, cioè se per ogni elemento $b \in B$ esiste un unico elemento $a \in A$ tale che $f(a) = b$.

1.13.9. In termini della funzione immagine inversa possiamo dire che una mappa è iniettiva se e solo se l'antimmagine di ogni singoletto di B contiene al più un elemento di A; è suriettiva se e solo se l'antimmagine di ogni singoletto di B non è vuota; e dunque è biiettiva se e solo se l'antimmagine di ogni singoletto di B è un singoletto di A.

In termini della funzione immagine diretta possiamo dire che una mappa è suriettiva se e solo se la sua immagine è tutto il codominio.

1.13.10. Che relazioni vi sono tra iniettività, suriettività e biiettività per f e le analoghe condizioni per le funzioni f_* e f^*?

1.13.11. Anticipando per il momento la nozione di insieme finito, una facile ma importante osservazione è la seguente: se A è un insieme finito, allora per le funzioni di A in sè le nozioni di essere iniettiva, suriettiva e biiettiva sono tutte tra loro equivalenti.

1.13.12. Teorema (Invertibilità delle funzioni). *Valgono le seguenti equivalenze per una funzione $f : A \to B$:*

(I) la funzione è iniettiva se e solo se esiste una funzione $g : B \to A$ tale che $g \circ f = \mathrm{id}_A$ (una tale f si dice invertibile a sinistra, e g si dice una inversa sinistra per f; dunque f è iniettiva se e solo se è invertibile a sinistra);

(S) la funzione è suriettiva se e solo se esiste una funzione $h : B \to A$ tale che $f \circ h = \mathrm{id}_B$ (una tale f si dice invertibile a destra, e h si dice una inversa destra per f; dunque f è suriettiva se e solo se è invertibile a destra);

(B) la funzione è biiettiva se e solo se esiste una funzione $g : B \to A$ tale che $g \circ f = \mathrm{id}_A$ e $f \circ g = \mathrm{id}_B$ (una tale f si dice invertibile, e g si dice una inversa per f, e si scrive di solito f^{-1}; dunque f è biiettiva se e solo se è invertibile).

Dimostrazione. La prima e la terza affermazione sono facilmente dimostrabili; la seconda affermazione invece non è ovvia, e una dimostrazione rigorosa richiede (e anzi è equivalente) all'assioma della scelta, che vedremo tra qualche pagina. □

1.13.13. Si osservi che le eventuali inverse destre e sinistre per una funzione non sono uniche, a meno che la funzione stessa non sia invertibile sia a destra che a sinistra: in tal caso esiste un'unica inversa destra, un'unica inversa sinistra ed esse coincidono, come mostra la serie di uguaglianze

$$g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h$$

se $\mathrm{id}_B = f \circ h$ e $g \circ f = \mathrm{id}_A$.

1.13.14. Una funzione $f : A \to B$ è iniettiva se e solo se gode della seguente proprietà "di cancellazione a sinistra": per ogni coppia $g_1, g_2 : C \to A$ di funzioni tali che $f \circ g_1 = f \circ g_2$ allora $g_1 = g_2$.

Una funzione $f : A \to B$ è suriettiva se e solo se gode della seguente proprietà "di cancellazione a destra": per ogni coppia $g_1, g_2 : B \to C$ di funzioni tali che $g_1 \circ f = g_2 \circ f$ allora $g_1 = g_2$.

1.13.15. Inclusioni come funzioni. Per ogni insieme A ed ogni suo sottinsieme B, la regola che ad ogni $b \in B$ associa $b \in A$ è una funzione iniettiva $i_B^A : B \to A$ che si dice l'inclusione di B in A; essa è suriettiva (e allora una biiezione) se e solo se $A = B$. Se abbiamo $C \subseteq B \subseteq A$ allora risulta $i_B^A \circ i_C^B = i_C^A$.

1.13.16. Composizioni e proprietà delle funzioni. Si verifica facilmente che la composizione di funzioni iniettive (risp. suriettive, risp. biiettive) mantiene la stessa proprietà.

Valgono i seguenti risultati (converse parziali): se una composizione è iniettiva (risp. suriettiva) allora la prima funzione è iniettiva (risp. la seconda funzione è suriettiva); in particolare se una composizione è biiettiva, allora la prima funzione è iniettiva e la seconda funzione è suriettiva, ma nessuna delle due è in generale biiettiva.

1.13.17. Grafico. Una funzione $f : A \to B$ definisce un sottinsieme di $A \times B$, detto il suo grafico, dato da

$$\Gamma(f) := \{(a, f(a)) \mid a \in A\}$$

dotato della seguente proprietà: per ogni $a \in A$ esiste una ed una sola coppia in $\Gamma(f)$ il cui primo elemento sia a (tali sottinsiemi di $A \times B$ sono detti grafici). Viceversa ogni sottinsieme Γ di $A \times B$ che gode della proprietà detta è il grafico di una unica ben determinata funzione $f(\Gamma) : A \to B$.

Si verifichi che le funzioni che mandano f in $\Gamma(f)$ (dall'insieme delle funzioni di A in B nell'insieme dei grafici di $A \times B$) e Γ in $f(\Gamma)$ sopra definite sono biiezioni una inversa dell'altra.

Le proprietà di essere iniettiva, suriettiva, biiettiva per una funzione si riconoscono dal suo grafico nel modo seguente: f è iniettiva se e solo se per ogni b esiste al più un a tale che $(a, b) \in \Gamma(f)$; f è suriettiva se e solo se per ogni b esiste almeno un a tale che $(a, b) \in \Gamma(f)$; f è biiettiva se e solo se per ogni b esiste uno ed un solo a tale che $(a, b) \in \Gamma(f)$.

1.13.18. Alcune funzioni canoniche notevoli. Spesso succede che tra due insiemi vi siano delle funzioni naturali, definite in modo intrinseco: tali funzioni si dicono canoniche; se si tratta di biiezioni, si dice che i due insiemi sono canonicamente in biiezione.

Per esempio abbiamo già accennato al caso del prodotto cartesiano: vi è una funzione naturale $A \times B \to B \times A$ che manda (a, b) in (b, a) (talvolta detta la simmetria), e che si verifica subito essere una biiezione.

Un altro esempio è dato dalla funzione $A\times(B\times C)\to(A\times B)\times C$ che manda $(a,(b,c))$ in $((a,b),c)$; anche in questo caso si vede subito che si tratta di una biiezione, che permette allora di identificare canonicamente i prodotti tripli (e perciò multipli).

Dato un insieme A, vi è una biiezione naturale tra l'insieme potenza $\mathscr{P}(A)$ di A e l'insieme $\mathbf{2}^A$ delle funzioni di A in $\mathbf{2}$ che associa ad ogni sottinsieme B la cosiddetta funzione caratteristica di B che vale 1 su B e 0 su $A\smallsetminus B$.

1.13.19. Prodotti infiniti. Dato un insieme I e una famiglia di insiemi A_i indiciata da $i\in I$, possiamo definire il prodotto della famiglia stessa, indicato come $\prod_{i\in I}A_i$, come l'insieme delle funzioni di I in $\bigcup_{i\in I}A_i$ tali che per ogni $i\in I$ la sua immagine appartenga ad A_i. Se $I=\{1,2,\dots,n\}$ allora si scrive anche $\prod_{i\in I}A_i=\prod_{i=1}^n A_i=A_1\times A_2\times\cdots\times A_n$. Nel caso che $I=\{1,2\}$, questa definizione non è esattamente quella data parlando di prodotto cartesiano, ma si può facilmente vedere che si tratta di due definizioni equivalenti in modo canonico.

2. Relazioni, equivalenze ed ordini.

2.1. Definizione (Relazioni). *Una relazione è una terna (A,B,R) in cui A e B sono insiemi, e R è un sottinsieme del prodotto cartesiano $A\times B$; spesso si parla di relazione tra un insieme A ed un insieme B e si specifica semplicemente il terzo termine R. Se $(a,b)\in R$ si dice che a è in relazione con b secondo R, e si scrive anche aRb. Elenchiamo qualche importante definizione per relazioni tra un insieme e se stesso, insieme a delle caratterizzazioni su cui il lettore dovrebbe riflettere:*

(R) una relazione si dice riflessiva se per ogni $a\in A$ abbiamo aRa (ovvero $(a,a)\in R$, ovvero se R contiene la diagonale di $A\times A$);

(S) una relazione si dice simmetrica se per ogni $a,b\in A$ abbiamo che aRb implica bRa (ovvero se $(a,b)\in R$, allora anche $(b,a)\in R$, ovvero se R è "simmetrico rispetto alla diagonale" come sottinsieme di $A\times A$);

(A) una relazione si dice antisimmetrica se per ogni $a,b\in A$ abbiamo che aRb e bRa implicano $a=b$ (ovvero se $(a,b)\in R$ e $(b,a)\in R$, allora a e b sono lo stesso elemento, ovvero se R è "antisimmetrico rispetto alla diagonale" come sottinsieme di $A\times A$);

(t) una relazione si dice transitiva se per ogni $a,b,c\in A$ abbiamo che aRb e bRc implicano aRc (ovvero se $(a,b)\in R$ e $(b,c)\in R$, allora anche $(a,c)\in R$; cosa significa questo in $A\times A$?);

(T) una relazione si dice totale se per ogni $a,b\in A$ abbiamo che aRb oppure bRa sono veri (ovvero $(a,b)\in R$ oppure $(b,a)\in R$; cosa significa questo in $A\times A$?); si osservi che una relazione totale è certo riflessiva. Una relazione non totale si dice parziale.

2.1.1. Abbiamo già visto una importante classe di relazioni tra A e B costituita dai grafici di funzioni di A in B. Per abuso di linguaggio, una relazione soddisfacente alla condizione per essere un grafico (per ogni $a\in A$ esiste una ed una sola coppia nella relazione il cui primo elemento sia a) si dirà una funzione.

2.1.2. Operazioni tra relazioni. Trattandosi di sottinsiemi di $A\times B$, le relazioni tra A e B sono soggette alle nozioni insiemistiche usuali; dunque possiamo parlare di inclusione tra relazioni, di unione, intersezione, differenza tra relazioni e così via.

Poiché alcune proprietà delle relazioni come la simmetria e la transitività sono stabili per intersezioni arbitrarie, ciò ci permette di parlare per ogni relazione R data della sua chiusura simmetrica o transitiva (la più piccola relazione simmetrica o transitiva contenente R, ovvero l'intersezione di tutte le relazioni simmetriche o transitive contenenti R).

2.1.3. Composizioni tra relazioni. Analogamente alle funzioni, possiamo anche parlare di composizioni di relazioni nel modo seguente: se R è relazione di A con B e S è relazione di B con C, allora definiamo RS relazione di A con C tramite $a(RS)c$ se e solo se esiste $b\in B$ tale che aRb e bSc. La composizione tra relazioni, similmente a quella tra funzioni, è associativa ma non commutativa.

2.2. Definizione (Equivalenze). *Una relazione R su un insieme A si dice di equivalenza se soddisfa alle proprietà riflessiva, simmetrica e transitiva. Di solito le relazioni di equivalenza si indicano con simboli quali $\sim$, $\simeq$, $\cong$, $\approx$. Se $a\in A$, indichiamo con $[a]_R$ oppure $[a]$ oppure $\overline{a}$ (se R può essere sottintesa) e chiamiamo la classe di equivalenza di a modulo R il sottinsieme di A formato dagli elementi equivalenti ad a: $[a]_R=\{b\in A\mid aRb\}$.*

Per ogni insieme A vi è una più piccola relazione di equivalenza (nel senso delle inclusioni in $A \times A$), ed è la relazione di identità (aRb se e solo se $a = b$; si tratta della diagonale $\{(a, a) \mid a \in A\}$ in $A \times A$). Vi è anche una massima relazione di equivalenza, quella per cui ogni elemento è in relazione con ogni altro; corrisponde a tutto l'insieme $A \times A$.

2.2.1. Teorema (Partizione associate). *Data una relazione di equivalenza su un insieme A, l'insieme delle classi di equivalenza degli elementi di A formano una partizione di A (cioè le classi di equivalenza sono non vuote, a due a due disgiunte e la loro unione dà A), detta partizione associata alla relazione. Viceversa data una partizione di A esiste una unica relazione di equivalenza in A tale che la partizione associata sia quella data.*

Perciò esiste una biiezione tra relazioni di equivalenza su un insieme e partizioni di quello stesso insieme.

Dimostrazione. Che le classi di equivalenza per una relazione di equivalenza costituiscano una partizione di A si vede facilmente: ogni classe è non vuota (per la riflessività), le classi sono a due a due disgiunte (se due classi hanno un elemento in comune, allora, per la transitività e la simmetria, esse coincidono), l'unione dà tutto A (di nuovo per la riflessività). Ad ogni partizione di A associamo la relazione definita da $a \sim b$ se e solo se essi appartengono allo stesso insieme della partizione. Allora si verifica subito che si tratta di una relazione di equivalenza (la riflessività viene dal fatto che la riunione dei sottinsiemi della partizione dà tutto A, la simmetria viene dalla corrispondente proprietà dell'inclusione, e la transitività segue dalla condizione che i sottinsiemi della partizione sono a due a due disgiunti). Le due assegnazioni fatte (ad ogni equivalenza su A una partizione di A, e ad ogni partizione di A una relazione di equivalenza su A) danno luogo a due funzioni una inversa dell'altra (verificare). □

2.2.2. Definizione (Insiemi quoziente). *L'insieme delle classi di equivalenza in A per una fissata relazione di equivalenza R su A si indica con A/R e si chiama l'insieme quoziente di A modulo R. Abbiamo che $[a]_R = [b]_R$ (in A/R) se e solo se aRb in A. Ogni $b \in [a]_R$ si dice un rappresentante della classe $[a]_R$. Quando si definiscono delle nozioni su un insieme quoziente facendo uso dei rappresentanti per ciascuna classe è necessario controllare che la definizione non dipende dal particolare rappresentante scelto: parleremo di "problema di buona definizione" in questi casi.*

2.2.3. Proiezioni. Esiste una funzione detta proiezione $p_R^A : A \to A/R$ che ad ogni $a \in A$ associa la sua classe di equivalenza $[a]_R \in A/R$; si tratta di una funzione suriettiva, ed è iniettiva se e solo se R è la relazione di identità. La proiezione gode della seguente proprietà di fattorizzazione: una qualsiasi funzione $f : A \to C$ si fattorizza come $f = g \circ p_R^A$ con $g : A/R \to C$ se e solo se vale l'implicazione: $aRa' \Longrightarrow f(a) = f(a')$ (cioè se e solo se f è costante sulle classi di equivalenza modulo R).

2.2.4. Teorema (di omomorfismo per insiemi). *Data una funzione $f : A \to B$, sia $\sim$ la relazione su A definita da $a \sim a'$ se e solo se $f(a) = f(a')$. Allora $\sim$ è una relazione di equivalenza ed esiste una unica funzione $\overline{f} : A/\sim \to B$ tale che $f = \overline{f} \circ p_\sim^A$. La funzione $\overline{f}$ risulta iniettiva; inoltre risulta che f ed $\overline{f}$ hanno la stessa immagine B' in B, e la funzione $\overline{f} : A/\sim \to B'$ è una biiezione.*

Dimostrazione. Che $\sim$ sia una relazione di equivalenza è facile. Per definizione la funzione f è costante sulle classi di equivalenza di $\sim$, dunque la fattorizzazione richiesta esiste (definita da $\overline{f}(\overline{a}) = f(a)$), ed è unica poiché la proiezione è suriettiva. La funzione $\overline{f}$ è iniettiva poiché da $\overline{f}(\overline{a}) = \overline{f}(\overline{a'})$ segue $f(a) = f(a')$, e dunque $\overline{a} = \overline{a'}$ per definizione di $\sim$. Che le immagini di f ed $\overline{f}$ coincidano è facile, e l'ultima affermazione è allora una conseguenza ovvia della iniettività di $\overline{f}$. □

2.2.5. Equivalenze generate. L'intersezione (in $A \times A$) di una famiglia di relazioni di equivalenza è ancora una relazione di equivalenza; quindi dato un qualunque sottinsieme di $A \times A$ possiamo parlare della relazione di equivalenza su A da esso generata: si tratta della più piccola relazione di equivalenza che lo contiene, ovvero della intersezione di tutte le relazioni di equivalenza che lo contengono.

2.3. Definizione (Preordini e Ordini). *Una relazione R su un insieme A si dice un preordine se essa è transitiva; si dice un ordine se soddisfa alle proprietà riflessiva, antisimmetrica e*

transitiva. Di solito le relazioni di (pre)ordine si indicano con simboli quali $<$, $\leqslant$, $\prec$, $\preccurlyeq$. *Un ordine si dice totale se lo è in quanto relazione, parziale altrimenti.*

2.3.1. Dati due insiemi ordinati A e B, una funzione $A \to B$ si dice ordinata o crescente se vale la seguente implicazione: per ogni $a, a' \in A$ da $a \leqslant a'$ (in A) segue che $f(a) \leqslant f(a')$ (in B). Viceversa la funzione si dice antiordinata o decrescente se per ogni $a, a' \in A$ da $a \leqslant a'$ (in A) segue che $f(a) \geqslant f(a')$ (in B). Una funzione si dice disordinata altrimenti, cioè se non è né crescente né decrescente.

Per ogni insieme ordinato A con relazione $\leqslant$ possiamo costruire la relazione d'ordine trasposta $\leqslant$ data da $a \leqslant a'$ se e solo se $a' \leqslant a$ (l'ordine viene "rovesciato"); allora una funzione antiordinata diventa una funzione ordinata dal dominio al codominio con l'ordine trasposto.

2.3.2. Ad ogni relazione R su A che sia riflessiva e transitiva (un preordine riflessivo) è associata una relazione d'equivalenza E definita da aEb se e solo se valgono aRb e bRa. Sull'insieme quoziente A/E la relazione R induce una relazione d'ordine parziale.

2.3.3. Minimali, massimali, minimo, massimo. Se B è un sottiniseme di un insieme ordinato A, diciamo che $b \in B$ è elemento massimale (risp. minimale) di B se dalla relazione $b' \in B$ e $b \leqslant b'$ (risp. $b' \in B$ e $b' \leqslant b$) segue $b = b'$; si osservi che un insieme può avere più massimali (risp. minimali) distinti (necessariamente non confrontabili tra loro). Diciamo che $b \in B$ è elemento massimo (risp. minimo) di B se $b' \leqslant b$ (risp. $b \leqslant b'$) per ogni altro $b' \in B$; se b è massimo (risp. minimo) in B, allora è l'unico massimale (risp. minimale) di B; il viceversa è falso? Se esiste il massimo (risp. il minimo) di A si dice l'ultimo (risp. il primo) elemento.

2.3.4. Buoni ordinamenti. Un insieme si dice bene ordinato se ogni suo sottinsieme non vuoto ammette elemento minimo (di conseguenza l'ordine è totale).

2.3.5. Minoranti e maggioranti. Se B è un sottinsieme di un insieme ordinato A, diciamo che $a \in A$ è maggiorante (risp. minorante) di B se vale la relazione $b \leqslant a$ (risp. $a \leqslant b$) per ogni $b \in B$.

2.3.6. Estremi inferiore e superiore. Se B è un sottiniseme di un insieme ordinato A, si dice estremo superiore (risp. inferiore) di B, se esiste, il minimo dei maggioranti (risp. il massimo dei minoranti).

♠ **2.3.7.** Vi sono altre fondamentali nozioni che riguardano gli ordinamenti: sottinsiemi limitati inferiormente e superiormente, segmenti iniziali, intervalli, catene, salti e lacune, densità, completezza e continuità ordinali, ecc. Queste nozioni sono alla base della definizione e di una possibile costruzione dei numeri reali, e saranno viste nel corso di Analisi. Il lettore interessato può riferirsi per approfondimenti al testo "Appunti di Algebra" (lezioni 11-14, 26-31) di I. Barsotti.

♠ **2.3.8.** Insiemi ordinati induttivi. Un insieme ordinato si dice induttivo se ogni sua catena (sottinsieme non vuoto in cui l'ordine indotto sia totale) ammette maggiorante. Si dice strettamente induttivo se ogni sua catena ammette estremo superiore. Vi è un importante e classico risultato riguardo a questo tipo di insiemi, che lega tra loro nozioni apparentemente indipendenti:

♠♠ **2.3.9.** Teorema. *Le seguenti asserzioni:*

(Z) lemma di Zorn: *ogni insieme ordinato induttivo ammette massimali;*

(Z') *ogni insieme ordinato strettamente induttivo ammette massimali;*

(S) assioma della scelta: *per ogni famiglia A_i, per $i \in I$, non vuota di insiemi non vuoti a due a due disgiunti, esiste un insieme S tale che $S \cap A_i$ è formato da un solo elemento per ogni i (in altri termini, possiamo scegliere un elemento in ogni insieme di una qualunque famiglia data; se la famiglia fosse finita non ci sarebbero problemi: ma se la famiglia è infinita il problema è "evidentemente" non banale);*

(P) assioma del prodotto: *per ogni famiglia A_i, per $i \in I$, non vuota di insiemi non vuoti, il prodotto cartesiano $\prod_{i \in I} A_i$ è non vuoto, cioè esistono funzioni $f : I \to \bigcup_{i \in I} A_i$ tali che $f(i) \in A_i$ per ogni $i \in I$ (anche qui il problema è non banale per insiemi infiniti di indici);*

(ID) *la proprietà di esistenza di una inversa destra per ogni funzione suriettiva: se $f : A \to B$ è una funzione suriettiva, allora esiste una funzione $g : B \to A$ che ne è inversa a destra, cioè tale che $f \circ g = \mathrm{id}_B$;*

(BO) principio del buon ordinamento: *ogni insieme è bene ordinabile (cioè su ogni insieme si può definire una relazione d'ordine che sia un buon ordinamento);*

sono tutte tra loro equivalenti.

Dimostrazione. Per vedere che (Z) e (Z') sono equivalenti, basta mostrare che (Z') implica (Z) (l'altra implicazione essendo ovvia). Sia allora A un insieme ordinato induttivo; consideriamo l'insieme A' di tutte le catene di A. Allora A' è ordinato dall'inclusione e risulta strettamente induttivo (l'estremo superiore di una catena di catene essendo l'unione delle catene stesse). Dunque in A' esistono elementi massimali, e un qualunque maggiorante in A di un massimale di A' è un massimale in A, dunque esistono massimali in A.

Che l'assioma (S) della scelta e quello (P) del prodotto siano equivalenti è facile, e lasciato al lettore. Essi implicano (ID) poiché per ogni funzione suriettiva $f : A \to B$, trovare una inversa destra si riduce a scegliere un elemento in ognuno dei sottinsiemi di A dati dalle antimmagini degli elementi di b. Viceversa, l'assioma del prodotto è dimostrato se è possibile scegliere una inversa destra della funzione $\bigcup_{i\in I} A_i \to I$ che ad ogni $a_i \in A_i$ associa i, che è ben definita perché gli insiemi sono disgiunti, ed evidentemente suriettiva poiché gli insiemi sono non vuoti. Quindi (ID) implica (P).

È anche facile dimostrare che il principio del buon ordinamento implica (S), (P) o (ID). Per dimostrare (ID) per esempio, basta infatti ben ordinare l'insieme A e per ogni $b \in B$ scegliere come $g(b)$ il minimo dell'antimmagine di b tramite f.

Vediamo che il lemma di Zorn implica (BO). Sia A un insieme qualsiasi e consideriamo l'insieme X formato dai sottinsiemi di X dotati di un buon ordine. Quest'insieme è non vuoto, poiché ogni singoletto di A gli appartiene (anzi ogni insieme finito di A dotato di un ordine totale gli appartiene). Ordiniamo X tramite l'ordine delle inclusioni crescenti: dunque un elemento di X è minore di un altro se il primo è incluso nel secondo e possiede l'ordine indotto dall'inclusione. Così ordinato, X è insieme induttivo (ogni catena in X ha come massimale l'unione dei suoi elementi), e quindi esiste elemento massimale in X, sia A', dotato di un buon ordinamento, e supponiamo che sia $A' \neq A$. Allora esiste $a \in A$, ma $a \notin A'$, e il sottinsieme $A' \cup \{a\}$ ordinato usando a come minimo elemento contraddice la massimalità di A' in X. Dunque $A' = A$, e allora abbiamo un buon ordinamento su A.

Per esercizio far vedere che il lemma di Zorn implica (S), (P) e (ID) (direttamente, senza passare per (BO)).

La parte più impegnativa della dimostrazione è invece data dal fatto che il lemma di Zorn è implicato da una delle altre asserzioni (S), (P) o (ID); classicamente si dimostra che l'assioma della scelta implica (Z'), e per questo rimandiamo il lettore interessato al libro "Appunti di Algebra" (lezioni 15-16) di I. Barsotti. □

3. Cardinalità e combinatorica.

In questo paragrafo daremo una definizione precisa della nozione intuitiva di "numerosità" di un insieme, vale a dire del "numero di elementi che lo compongono".

3.1. Definizione (Cardinalità, Equipotenza). *Due insiemi A e B si dicono equipotenti (o aventi la stessa cardinalità) se esiste una biiezione di A in B. La collezione di tutti gli insiemi (dell'Universo fissato) equipotenti ad un fissato insieme A si dice una cardinalità, e si indica con $|A|$, $c(A)$, $\mathrm{card}(A)$ o $\#A$ a seconda dei contesti.*

3.2. Operazioni tra le cardinalità. Possiamo definire tra le cardinalità alcune relazioni e operazioni analoghe a quelle ben note per i numeri naturali (che tra poco vedremo essere particolari cardinalità, quelle finite). Siano A e B due insiemi disgiunti;

(S) la somma delle due cardinalità $|A|$ e $|B|$ è la cardinalità dell'unione: $|A|+|B| = |A\cup B|$ (si presenta qui un problema generale: nella definizione abbiamo usato due specifici insiemi appartenenti a fissate cardinalità, e dobbiamo controllare che il risultato non dipenda dagli insiemi, ma solo dalla loro cardinalità; ovvero che scegliendo altri insiemi della stessa cardinalità il risultato della definizione non cambi);

(P) il prodotto delle due cardinalità $|A|$ e $|B|$ è la cardinalità del prodotto cartesiano: $|A|\cdot|B| = |A\times B|$

(E) l'elevamento a potenza della cardinalità $|A|$ alla cardinalità $|B|$ è la cardinalità dell'insieme delle funzioni di B in A: $|A|^{|B|} = |A^B|$.

Una cardinalità $|A|$ si dice minore o uguale ad una cardinalità $|B|$ e si scrive $|A| \leqslant |B|$ se esiste una funzione iniettiva di A in B (oppure una funzione suriettiva di B su A). Si scrive $|A| < |B|$ se $|A| \leqslant |B|$ e $|A| \neq |B|$.

Se $|C| = |A| + |B|$ allora scriveremo anche $|A| = |C| - |B|$ oppure $|B| = |C| - |A|$, ma si tratta di espressioni un po' pericolose, come vedremo.

3.2.1. Proprietà delle operazioni tra cardinali. Avendo usato delle operazioni insiemistiche per definire le operazioni tra cardinali, queste ultime ereditano le proprietà delle prime; per esempio commutatività (e associatività) per somma e prodotto seguono dalla stessa proprietà per unione e prodotto cartesiano; la distrubutività del prodotto rispetto alla somma segue dalla analoga proprietà del prodotto cartesiano rispetto alla unione (da notare che l'altra distributività è falsa).

Useremo liberamente in futuro queste facili proprietà. Segnaliamo per esempio che da $A^{B\cup C} = A^B \times A^C$ se $B \cap C = \varnothing$ segue una ben nota formula per gli esponenti: $|A|^{|B|+|C|} = |A|^{|B|}|A|^{|C|}$.

3.2.2. Formula di inclusione-esclusione. Per ogni coppia di insiemi A e B abbiamo la relazione

$$|A \cup B| = |A| + |B| - |A \cap B| \ .$$

Infatti poiché A è unione disgiunta di $A \smallsetminus B$ e $A \cap B$, B è unione disgiunta di $B \smallsetminus A$ e $A \cap B$, e $A \cup B$ è unione disgiunta di $A \smallsetminus B$, $A \cap B$ e $B \smallsetminus A$, abbiamo

$$|A \cup B| + |A \cap B| = |A \smallsetminus B| + |A \cap B| + |B \smallsetminus A| + |A \cap B| = |A| + |B|$$

(abbiamo fatto uso implicitamente della proprietà associativa della somma).

Nel caso di tre insiemi A, B, C abbiamo una formula analoga:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

che si giustifica in modo analogo.

Più in generale, abbiamo la seguente formula detta di inclusione-esclusione: data una famiglia finita $A_1, A_2, \dots, A_n$ di insiemi, vale che

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{i_1<i_2=1}^{n} |A_{i_1} \cap A_{i_2}| + \cdots + (-1)^{j+1} \sum_{i_1<\cdots<i_j=1}^{n} |\bigcap_{\ell=1}^{j} A_{i_\ell}| + \cdots + (-1)^{n+1} |\bigcap_{i=1}^{n} A_i|$$

la cui dimostrazione diretta è laboriosa, ma che si potrà dimostrare facilmente una volta noto il principio di induzione, tra poche pagine.

3.3. Teorema (Cardinalità potenza). *Per ogni insieme A, abbiamo che $|\mathscr{P}(A)| > |A|$.*

La cardinalità $|\mathscr{P}(A)|$ si indica spesso con $2^{|A|}$ poiché esiste una biiezione tra l'insieme delle parti di A e l'insieme $\mathbf{2}^A$ delle funzioni di A in $\{0, 1\}$. Dunque il teorema dice che per ogni insieme A vale che $2^{|A|} > |A|$.

Dimostrazione. Certamente $|A| \leqslant |\mathscr{P}(A)|$ poiché la funzione di A in $\mathscr{P}(A)$ che porta ogni elemento a nel singoletto $\{a\}$ è iniettiva. Basta quindi mostrare che non esistono funzioni suriettive di A in $\mathscr{P}(A)$. Sia $\varphi : A \to \mathscr{P}(A)$ una qualsiasi funzione e consideriamo il sottinsieme di A dato da $A' = \{a \in A \mid a \notin \varphi(a)\}$. Allora è chiaro che A' non appartiene all'immagine di φ, poiché altrimenti sarebbe $A' = \varphi(a')$ con $a' \in A$ e risulterebbe $a' \in A'$ se e solo se $a' \notin \varphi(a') = A'$, assurdo. Quindi alcuna tale funzione può essere suriettiva; di conseguenza non esistono biiezioni tra A e la sua potenza, e quindi la cardinalità di quest'ultima è strettamente superiore. □

♠ **3.4.** Teorema (Cantor-Schröder-Bernstein). *Se $|A| \leqslant |B|$ e $|B| \leqslant |A|$ allora $|A| = |B|$. In altri termini, se esistono una funzione iniettiva di A in B e una funzione iniettiva di B in A, allora esiste una biiezione tra A e B.*

Dimostrazione. La dimostrazione è particolarmente interessante, anche se non immediata, e ne presentiamo solo le linee guida. Date due funzioni iniettive $f : A \to B$ e $g : B \to A$ garantite dalle ipotesi, per ogni elemento a di A e ogni elemento b di B diciamo che a è figlio di b se $a = g(b)$ e che b è figlio di a se $b = f(a)$. Possiamo dunque parlare di "antenati" per ogni fissato elemento nel senso genealogico. Studiando la linea genealogica di ogni elemento possiamo dividere A in tre sottinsiemi disgiunti: sia A' l'insieme degli elementi che non hanno capostipite; sia A_A l'insieme degli elementi che hanno capostipite in A; sia A_B l'insieme degli elementi che hanno capostipite in B. Stessa cosa si può fare per B.

Ora possiamo definire una funzione biiettiva di A verso B nel modo seguente: f su A' (biiezione tra A' e B'), f su A_A (biiezione tra A_A e B_A), l'inversa di g su A_B (biiezione tra A_B e B_B). □

♠ **3.5.** Teorema (totalità dell'ordine). *Dati due insiemi qualsiasi A e B, o esiste una funzione iniettiva di A in B oppure esiste una funzione iniettiva di B in A; dunque due cardinali sono sempre confrontabili: o $|A| \leqslant |B|$ oppure $|B| \leqslant |A|$.*

Dimostrazione. Ci si riduce al caso di insiemi ben ordinati, e in questo caso si dimostra che uno dei due è incluso ordinatamente nell'altro. Non banale: vedi Esercizi 1-10, pg. 22-23 di I. Barsotti. □

3.6. Cardinalità finite. Gli insiemi $\mathbf{n} = \{0, 1, \dots, n-1\}$ introdotti all'inizio si dicono insiemi finiti, e le loro cardinalità si dicono finite; potremmo definire i numeri naturali allora nel modo seguente: essi sono le cardinalità di insiemi del tipo $N_0 = \varnothing$ (e poniamo $|N_0| = 0$), $N_1 = \{\varnothing\}$ (e poniamo $|N_1| = 1$), $N_2 = \{\varnothing, \{\varnothing\}\}$ (e poniamo $|N_2| = 2$), $N_3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$ (e poniamo $|N_3| = 3$), e così via, definito N_n (e posto $|N_n| = n$) definiamo $N_{n+1} = N_n \cup \{N_n\}$ (che ha un elemento in più, dunque porremo $|N_{n+1}| = n + 1$).

È chiaro che in questo modo costruiamo infiniti insiemi (nel senso che non c'è un limite alla costruzione), e che le operazioni di somma e prodotto tra cardinali corrispondono esattamente alle usuali operazioni tra numeri naturali. Ci occuperemo poi di problemi di combinatorica tra insiemi finiti.

Un altro modo possibile per costruire (a partire dal vuoto $\varnothing$) le cardinalità finite è il seguente: $M_0 = \varnothing$, $M_1 = \{\varnothing\}$, $M_2 = \{\varnothing, \{\varnothing\}\}$, $M_3 = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\}$ e così via, definito M_n definiamo $M_{n+1} = \{\varnothing\} \cup \mathscr{S}(M_n)$ ove $\mathscr{S}(M_n)$ indica l'insieme dei singoletti di M_n.

3.7. Cardinalità infinite. Si dicono infiniti invece gli insiemi la cui cardinalità non sono finite. Per esempio la collezione di tutti gli insiemi N_n, prima usati per definire le cardinalità finite, non è finita. A rigor di termini dovremmo postulare la sua esistenza come insieme, visto che non lo possiamo esplicitamente presentare per intero. La sua cardinalità si chiama "infinito numerabile" e si indica con $\aleph_0$ (alef zero). Dunque abbiamo $n < \aleph_0$ per ogni cardinale finito n.

3.7.1. Proprietà di $\aleph_0$. L'infinito numerabile è particolarmente importante, e quindi ne elenchiamo alcune proprietà:

(CI1) $\aleph_0 + n = \aleph_0$ per ogni cardinale finito n; infatti l'applicazione $(\mathbb{N} \times \{0\}) \cup (\mathbf{n} \times \{1\}) \to \mathbb{N}$ che manda $(i, 0)$ in $i + n$ e $(j, 1)$ in j è una applicazione biiettiva;

(CI2) $\aleph_0 + \aleph_0 = \aleph_0$; infatti l'applicazione $(\mathbb{N} \times \{0\}) \cup (\mathbb{N} \times \{1\}) \to \mathbb{N}$ che manda (i, α) in $2i + \alpha$ è una applicazione biiettiva;

(CI3) $\aleph_0 \aleph_0 = \aleph_0$; infatti (primo argomento diagonale di Cantor) possiamo trovare una biiezione di $\mathbb{N}$ su $\mathbb{N} \times \mathbb{N}$ ben ordinando quest'ultimo insieme con la regola $(a, b) \leqslant (a', b')$ se e solo se $a + b \leqslant a' + b'$ oppure $a + b = a' + b'$ e $a \leqslant a'$. Possiamo allora mandare $\ell \in \mathbb{N}$ nell'ℓ-esimo elemento di $\mathbb{N}^2$ per quest'ordine, e si tratta di una mappa suriettiva (e iniettiva: farsi un disegno).

(CI4) $\aleph_0^{\aleph_0} = 2^{\aleph_0}$; infatti l'insieme delle funzioni di $\mathbb{N}$ in sè è in biiezione con il sottinsieme delle funzioni (strettamente) crescenti di $\mathbb{N}$ in sè, e queste a loro volta sono definite dall'insieme dei valori assunti, e quindi dalla funzione caratteristica dell'insieme immagine (che è una funzione di $\mathbb{N}$ in $\mathbf{2}$). Si osservi che allora per ogni n finito si ha $\aleph_0^{\aleph_0} = n^{\aleph_0} = 2^{\aleph_0}$ per confronto.

Le stesse proprietà sono vere per ogni cardinale infinito, ma dimostrarlo è più difficile. Ricordiamo inoltre che $\mathfrak{c} = 2^{\aleph_0} > \aleph_0$ si dice la cardinalità del continuo (si vedrà essere la cardinalità dell'insieme dei numeri reali).

3.7.2. Il secondo argomento diagonale di Cantor si usa per mostrare che la cardinalità di $\mathbb{N}^{\mathbb{N}}$ è strettamente maggiore della cardinalità di $\mathbb{N}$ (il risultato l'abbiamo già visto, ma l'argomento di Cantor si usa anche in altri contesti, per esempio per dimostrare che l'insieme dei numeri reali ha cardinalità maggiore dell'insieme dei numeri naturali). Si ragiona per assurdo nel modo seguente: supponiamo che $\mathbb{N}^{\mathbb{N}}$ sia numerabile, e sia $f : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ una biiezione (per ogni n chiamiamo f_n la funzione corrispondente); costruiamo allora una funzione $g : \mathbb{N} \to \mathbb{N}$ che non è nessuna delle f_n, dunque contraddicendo la suriettività di f. Basta per questo definire $g(m) = f_m(m) + 1$, perché allora per ogni n abbiamo $f_n \neq g$ in quanto $f_n(n) \neq g(n)$.

♠ **3.7.3.** Proprietà degli insiemi infiniti. Ogni insieme infinito contiene un sottinsieme numerabile, dunque ha cardinalità maggiore o uguale ad $\aleph_0$, e quindi $\aleph_0$ è la più piccola cardinalità infinita. Si tratta di un risultato la cui dimostrazione richiede l'uso del lemma di Zorn, o di uno degli enunciati equivalenti.

3.7.4. Teorema. *Un insieme è infinito se e solo se esiste una biiezione con un suo sottinsieme proprio.*

Dimostrazione. Ogni funzione di un insieme finito in sè che sia iniettiva è anche suriettiva, quindi il "se" della proposizione è chiaro. Per il viceversa consideriamo prima il caso di un insieme numerabile, per esempio i numeri naturali: è chiaro allora che la funzione che manda ogni numero nel suo successore dà una biiezione di tutto l'insieme con l'insieme costituito dai numeri non nulli (sottinsieme proprio). Poiché ogni insieme infinito X contiene un insieme numerabile N, possiamo scrivere $X = N \cup (X \smallsetminus N)$ (unione disgiunta) e definire una funzione di X in sè che sia l'identità su $X \smallsetminus N$ e che identifichi N a un suo sottinsieme stretto N'; allora la funzione costruita è una biiezione di X con $X' = N' \cup (X \smallsetminus N) \subset X$, come si voleva. □

♠ **3.7.5.** Ogni insieme infinito è unione disgiunta di insiemi numerabili (si deve usare il lemma di Zorn).

♠ **3.7.6.** Conseguenze: $c + n = c$, $nc = c$, $c + \aleph_0 = c$, $c\aleph_0 = c$, $c + c = c$, $cc = c$, le somme finite tra cardinali di cui almeno uno sia infinito coincidono con il massimo dei sommandi, i prodotti finiti tra cardinali di cui almeno uno sia infinito coincidono con il massimo dei fattori, $2^c = c^c > c$.

♠ **3.7.7.** Se A è infinito, e $\mathscr{P}'(A)$ indica l'insieme delle parti finite di A, allora abbiamo $|\mathscr{P}'(A)| = |A|$.

3.8. Combinatorica delle funzioni. Se A e B sono insiemi finiti di cardinalità m ed n rispettivamente, possiamo chiederci qual è la cardinalità dell'insieme delle funzioni di A in B, e di certi tipi particolari di funzioni. Calcolare il numero di funzioni di A in B è facile: al fine di costruire una funzione, per ogni elemento di A dobbiamo decidere quale elemento di B è la sua immagine, ed ogni volta possiamo scegliere tra n elementi; le scelte da fare sono tutte indipendenti tra loro, e dunque in totale abbiamo n^m possibili funzioni. Quindi risulta

$$|B^A| = |B|^{|A|}$$

che giustifica la simbologia B^A per l'insieme delle applicazioni di A in B.

3.8.1. Anche l'insieme delle funzioni biiettive di A in B è facilmente controllabile: è vuoto, ovvero di cardinalità zero se $|A| \neq |B|$; altrimenti è $(|A|)!$, il fattoriale della cardinalità di A (prodotto di tutti i numeri interi da 1 a $|A|$; si pone per definizione $0! = 1$). Infatti in questo caso costruendo la funzione dobbiamo fare attenzione a non ripetere le scelte già fatte per le immagini: quindi vi sono n scelte per l'immagine del primo elemento, $n-1$ per il secondo, $n-2$ per il terzo e così via.

3.8.2. L'insieme delle funzioni iniettive di A in B è nullo se $|A| > |B|$ (principio dei cassetti: se vi sono più oggetti che cassetti, in qualche cassetto deve stare più di un oggetto; talvolta detto anche principio della piccionaia: se ci sono più piccioni che casette, in qualche casetta ci deve stare più di un piccione); altrimenti, ragionando analogamente a prima, si vede che si tratta del prodotto degli m numeri naturali in discesa partendo da n; dunque la cardinalità è $(|B|)!/(|B| - |A|)!$.

3.8.3. Nettamente più difficile è studiare il numero di funzioni suriettive di A in B; certamente è zero se $|A| < |B|$. Una strategia costruttiva diretta, cioè cercare tutti i modi possibili di costruire funzioni suriettive, in questo caso non è ovvia (provare per credere); conviene invece ricorrere al principio di inclusione-esclusione per conteggiare le funzioni non suriettive di A in B. In effetti se definiamo F_b l'insieme delle funzioni la cui immagine non contiene $b \in B$, abbiamo che la cardinalità dell'insieme $\bigcup_{b\in B} F_b$ delle funzioni non suriettive è dato da

$$\sum_{b\in B} |F_b| - \sum_{b,b'\in B} |F_b \cap F_{b'}| + \cdots + (-1)^{i+1} \sum_{b_1,\ldots,b_i\in B} |F_{b_1} \cap \cdots \cap F_{b_i}| + \cdots + (-1)^{|B|+1} |\bigcap_{b\in B} F_b|$$

e di conseguenza la cardinalità delle funzioni suriettive è

$$|B|^{|A|} - |B|(|B|-1)^{|A|} + \binom{|B|}{2}(|B|-2)^{|A|} + \cdots + (-1)^i \binom{|B|}{i}(|B|-i)^{|A|} + \cdots + (-1)^{|B|}\binom{|B|}{|B|}(|B|-|B|)^{|A|}$$

poiché il numero di addendi nella i-esima sommatoria è $\binom{|B|}{i}$ (coefficiente binomiale) e $(|B| - i)^{|A|}$ è il numero di elementi che ogni intersezione di quella sommatoria comporta (sì, è vero che l'ultimo addendo scritto è sempre zero, ma lo si è lasciato ugualmente per rispettare la simmetria della formula).

3.8.4. Nel prossimo paragrafo la formula precedente, sia

$$S_{n,k} = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$$

se $S_{n,k}$ indica il numero di funzioni suriettive da un insieme con n elementi a uno con k elementi, potrà essere dimostrata per induzione a partire dalla seguente osservazione: se fissiamo un elemento del dominio, allora possiamo distinguere le funzioni suriettive in due tipi (quali?) e di conseguenza

$$S_{n+1,k} = k(S_{n,k} + S_{n,k-1})$$

(si osserverà anche la parentela con la formula ricorsiva dei coefficienti binomiali). Problema per il (paragrafo) futuro: che tipo di formula ricorsiva si può scrivere fissando un elemento del codominio?

3.9. Disposizioni e Combinazioni. Una disposizione di classe k di un insieme A è una k-upla ordinata di elementi di A; si chiamano disposizioni con ripetizione se si permette che possano comparire più volte gli stessi elementi, senza ripetizione altrimenti. Se $|A| = n$, il numero di disposizioni di classe k con ripetizione è dato da n^k. Infatti l'insieme di tali disposizioni è in biiezione con l'insieme delle funzioni da un insieme con k elementi ad A. Il numero di disposizioni (semplici, ovvero senza ripetizioni) di classe k di un insieme con n elementi si indica con $D_{n,k}$. Poiché l'insieme di tali disposizioni è in biiezione con l'insieme delle funzioni iniettive da un insieme con k elementi ad A, abbiamo che

$$D_{n,k} = n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!} \ .$$

Una combinazione di classe k di un insieme A è invece una scelta non ordinata di k elementi di A; di nuovo si distinguono le combinazioni con ripetizione se si permette che possano comparire più volte gli stessi elementi, senza ripetizione altrimenti. Per il caso delle combinazioni senza ripetizioni, la differenza rispetto alle disposizioni di classe k consiste solo nel considerare irrilevante "l'ordine di scelta" degli elementi di A; dunque vi sono sempre $k!$ disposizioni che identificano la stessa combinazione. Da questa osservazione si deduce che le combinazioni di classe k (semplici, ovvero senza ripetizioni) di un insieme con n elementi sono in numero

$$C_{n,k} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

(coefficiente binomiale: la tavola di questi numeri è il ben noto triangolo di Tartaglia, che ricorderemo tra poche pagine).

Poiché l'insieme delle parti di A si può vedere come unione disgiunta degli insiemi formati dai sottinsiemi di fissate cardinalità, deduciamo dalle formule precedenti che $\sum_{i=0}^{n}\binom{n}{k} = 2^n$ (cardinalità dell'insieme potenza, essendo in biiezione con l'insieme delle funzioni di A in $\mathbf{2}$), la ben nota formula del binomio di Newton che studieremo in generale per anelli commutativi.

Si osservi infine che l'uguaglianza evidente $\binom{n}{k} = \binom{n}{n-k}$ per ogni n e k ha una ovvia interpretazione combinatorica (passando agli insiemi complementari).

Il caso delle combinazioni con ripetizione è nettamente diverso, e può essere visto nel modo seguente. Dare una combinazione con ripetizione di classe k a partire da un insieme di n elementi è come dare una distribuzione di k palline (tutte uguali) in n scatole diverse (ogni scatola rappresenta un elemento dell'insieme, e il numero di palline nella scatola rappresenta quante volte quell'elemento viene scelto). Si tratta allora di contare in quanti modi l'insieme delle k palline (pensate allineate) può essere diviso usando $n-1$ sbarrette. Si vede facilmente che questo numero è $\binom{n+k-1}{k}$.

3.10. Partizioni di insiemi. Una partizione di un insieme A è un sottinsieme di $\mathscr{P}(A)$ formato da sottinsiemi non vuoti di A a due a due disgiunti e la cui unione dà tutto A; una partizione si dice di classe k se è formata da k sottinsiemi di A. Se $n = |A|$, allora certamente $k \leqslant n$. Ogni funzione suriettiva di A verso un insieme formato di k elementi dà luogo ad una partizione di A, ed evidentemente vi sono $k!$ di tali funzioni che identificano la stessa partizione (si possono scambiare comunque gli elementi dell'immagine, ovvero si può comporre la funzione data con una qualunque biiezione del codominio).

Detto $P_{n,k}$ il numero di partizioni di classe k di un insieme con n elementi, abbiamo allora che

$$P_{n,k} = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n \ .$$

Si osservi per esempio che per $k = n$ vi è esattamente una partizione (quella in singoletti), che dunque ci restituisce la formula

$$n! = \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^n$$

che non è facilmente verificabile in modo diretto. È istruttivo per il lettore farsi la tavola dei numeri $P_{n,k}$ per valori piccoli di n e di k, diciamo minori o uguali a 10.

3.11. Partizioni di numeri. Una partizione di un numero naturale n è una collezione formato da numeri naturali non nulli (eventualmente ripetuti) la cui somma dà n; una partizione di n si dice di classe k se è formata da k numeri interi. Il lettore è invitato a farsi la tavola del numero di partizioni di classe k di n per valori piccoli di n e di k, diciamo minori o uguali a 10.

♠ **3.12.** Combinatorica delle relazioni. Dato un insieme A di cardinalità finita n, possiamo considerare l'insieme delle possibili relazioni su A: si tratta dell'insieme delle parti di $A \times A$, e dunque di cardinalità 2^{n^2}.

3.12.1. Relazioni riflessive. Le relazioni soddisfacenti alla proprietà riflessiva sono invece in numero $2^{n(n-1)}$; infatti in questo caso i termini diagonali (che sono esattamente $|A|$) di $A \times A$ devono comparire necessariamente, gli altri essendo liberi: si tratta quindi delle funzioni da un insieme con $|A \times A| - |A| = n^2 - n$ elementi in $\mathbf{2}$.

3.12.2. Relazioni simmetriche. Le relazioni soddisfacenti alla proprietà simmetrica sono invece in numero $2^{\frac{n(n+1)}{2}}$; infatti in questo caso i termini diagonali (che sono esattamente $|A|$) di $A \times A$ sono liberi, mentre i termini non diagonali devono essere simmetrici: si tratta quindi delle funzioni da un insieme con $\frac{|A\times A|-|A|}{2} + |A| = \frac{n^2+n}{2}$ elementi in $\mathbf{2}$.

3.12.3. Relazioni simmetriche e riflessive. Un analogo ragionamento mostra che le relazioni riflessive e simmetriche sono $2^{\frac{n(n-1)}{2}}$

3.12.4. Relazioni di equivalenze. Poiché le relazioni di equivalenza sono in biiezione con le partizioni dell'insieme A, esse sono in numero di $\sum_{k=1}^{n} P_{n,k}$.

3.12.5. Relazioni antisimmetriche. Il numero di relazioni antisimmetriche può essere valutato tenendo conto che per ogni coppia di posizioni simmetriche non diagonali, solo tre possibilità sono compatibili con la condizione; quindi si tratta di $2^n 3^{\frac{n(n-1)}{2}}$ relazioni.

3.12.6. Relazioni riflessive e antisimmetriche. Analogamente, le relazioni che sono riflessive e antisimmetriche sono in numero di $3^{\frac{n(n-1)}{2}}$.

3.12.7. Relazioni d'ordine. Le relazioni d'ordine totale sono $n!$, come le permutazioni possibili; invece risulta difficile conteggiare le relazioni d'ordine parziale, come pure contare le relazioni soddisfacenti alla proprietà transitiva.

4. Numeri Naturali e Induzione.

La più semplice struttura algebrica è quella data da una regola per combinare due elementi di un insieme per produrne un altro.

4.1. Definizione (Magma). *Diciamo magma un insieme M dotato di una operazione binaria, cioè di una funzione $M \times M \to M$ che manda (m, m') in $m * m'$. Un magma si dice associativo se per ogni terna di elementi $m, m', m'' \in M$ si ha che $(m * m') * m'' = m * (m' * m'')$ (nel qual caso le operazioni si possono scrivere senza parentesi). Si dice unitario se esiste un elemento $\imath \in M$ (chiamato elemento neutro per l'operazione) tale che $\imath * m = m = m * \imath$ per ogni $m \in M$. Si dice commutativo se per ogni coppia $m, m' \in M$ si ha che $m * m' = m' * m$.*

Talvolta un magma associativo ed unitario si chiama un semigruppo, e un magma commutativo, associativo ed unitario si chiama un monoide.

Una funzione tra due magma $f : M \to N$ si dice un omomorfismo di magma, oppure funzione di magma, se rispetta l'operazione e gli eventuali elementi neutri, cioè se $f(m * m') = f(m) * f(m')$ per ogni $m, m' \in M$ (si noti che il primo $*$ denota l'operazione su M, e il secondo quella su N), ed eventualmente $f(\imath_M) = \imath_N$.

Data una definizione di una struttura algebrica, si può sempre trarne una piccola messe di facili conseguenze; ne esplicitiamo alcune:

4.1.1. In un magma associativo, l'elemento neutro se esiste è unico. Siano infatti $\imath$ e $\imath'$ due elementi neutri; allora si ha $\imath = \imath * \imath' = \imath'$.

4.1.2. Se esiste l'elemento neutro $\imath$, un simmetrico destro (risp. sinistro) di $m \in M$ è un elemento $m^* \in M$ (resp. ${}^*m \in M$) tale che $m * m^* = \imath$ (risp. ${}^*m * m = \imath$); un elemento simmetrico di

$m \in M$ è un elemento m^* tale che $m * m^* = \imath = m^* * m$. Allora in un magma associativo, l'elemento simmetrico di un dato elemento se esiste è unico, e se un elemento ha simmetrico destro e sinistro, questi coincidono e sono un simmetrico per quell'elemento. Infine se m ammette simmetrico m^*, anche m^* ammette un simmetrico che è $m^{**} = m$.

4.1.3. In un magma associativo il risultato dell'applicazione ripetuta dell'operazione non dipende dalla sequenza in cui viene effettuata (fermo restando l'ordine degli elementi).

4.1.4. In un magma associativo e commutativo il risultato dell'applicazione ripetuta dell'operazione non dipende dall'ordine con cui vengono presi gli elementi.

4.1.5. Magma integro. Un magma M si dice integro se per ogni $a \in M$ dalla relazione $a * b = a * c$ segue che $b = c$. Data una funzione tra magma unitari, se essa rispetta la somma, allora rispetta anche l'elemento neutro sotto ipotesi che il codominio sia magma integro. Infatti in tal caso da $f(\imath_M) * f(\imath_M) = f(\imath_M * \imath_M) = f(\imath_M) = f(\imath_M)\imath_N$ deduciamo che $f(\imath_M) = \imath_N$.

4.1.6. Congruenze. Una relazione di equivalenza $\sim$ in un magma M si dice una congruenza se $a \sim b$ implica $a * c \sim b * c$ per ogni $c \in M$. Si osservi che questo è equivalente a che se $a \sim b$ e $a' \sim b'$ allora $a * a' \sim b * b'$.

In tal caso l'insieme quoziente $M/\sim$ è dotato di una struttura di magma (ben) definita da $[a] * [b] = [a * b]$ (ben definita significa che la definizione dipende solo dalle classi $[m]$ e non dai singoli elementi di una classe).

4.1.7. Notazioni additive e moltiplicative. Nel caso di magmi commutativi, si usa spesso indicare con $+$ (somma) l'operazione, con 0 (zero) l'elemento neutro, e con $-m$ (opposto) il simmetrico di m. Nel caso di magmi non commutativi si preferisce usare la notazione moltiplicativa cioè indicare con $\cdot$ (prodotto, spesso muto) l'operazione, con 1 (uno o unità) l'elemento neutro, e con m^{-1} (inverso) il simmetrico di m.

4.2. Dato un qualsiasi insieme A, l'insieme A^A di tutte le funzioni di A in sè, dotato della operazione di composizione di funzioni, è un magma associativo, unitario (elemento neutro è la mappa identica) e non commutativo. Gli elementi invertibili sono le biiezioni.

Lo stesso si può dire dell'insieme $\mathscr{P}(A \times A)$ delle relazioni di A in sè, dotato della composizione di relazioni; in questo caso vi è anche un elemento ω (la relazione vuota) tale che $m * \omega = \omega = \omega * m$ per ogni $m \in M$, che si dice elemento killer.

Abbiamo già usato l'insieme dei numeri naturali nell'eccezione ingenua, e parlando di cardinalità (finite) ne abbiamo anche definito precisamente gli elementi. Diamo ora una descrizione rigorosa di questo insieme e di alcune sue importanti proprietà.

4.3. Definizione (Numeri Naturali). *L'insieme $\mathbb{N}$ dei numeri naturali ha come elementi le cardinalità finite. Esiste in $\mathbb{N}$ una operazione somma che è commutativa ed associativa, con elemento neutro lo zero (che è anche l'unico elemento simmetrizzabile). Inoltre l'ordinamento tra i cardinali finiti dà un ordinamento totale su $\mathbb{N}$ che è un buon ordinamento (cioè ogni sottinsieme non vuoto di $\mathbb{N}$ ha minimo).*

4.3.1. Prodotto nei naturali. Abbiamo anche dato una nozione di prodotto tra cardinali, e quindi tra numeri naturali; in effetti per i numeri naturali l'operazione di prodotto può essere ridotta a quella della somma nel modo seguente: il prodotto nm corrisponde a "sommare m volte il numero n con se stesso":

$$mn = \underbrace{n + \cdots + n}_{m \text{ volte}}$$

poiché $\mathbf{n} \times \mathbf{m} = (\mathbf{n} \times \{0\}) \cup \cdots \cup (\mathbf{n} \times \{m-1\})$ (si tratta di una unione di insiemi a due a due disgiunti).

Si osservi che l'insieme dei cardinali finiti con l'operazione di prodotto è anch'esso un magma associativo, commutativo e unitario (con elemento neutro 1), ma la sua struttura come ben noto, è molto più complicata; per esempio non è integro a causa della presenza di un elemento killer (lo zero).

4.4. Tecniche di Induzione. Introduciamo ora un principio fondamentale della matematica: il principio di induzione per i numeri naturali. Si tratta di una tecnica di dimostrazione di famiglie infinite di enunciati indiciate sui numeri naturali, e che riduce a dimostrare il primo degli enunciati (base dell'induzione) e poi a dimostrare che dalla validità di un enunciato segue la validità del successivo (passo detto induttivo). Vi sono alcune variazioni possibili che esamineremo.

4.5. Teorema (Principio di Induzione (prima forma)). *Sia M un sottinsieme di $\mathbb{N}$ soddisfacente alle due proprietà seguenti:*
(0) $0 \in M$;
(i) *per ogni $n \in \mathbb{N}$, se $n \in M$ allora $n+1 \in M$;*
allora $M = \mathbb{N}$.

Sia ora A_n una famiglia di asserzioni indiciate da $n \in \mathbb{N}$; supponiamo soddisfatte le due proprietà seguenti:
(0) *A_0 è vera*
(i) *per ogni $n \in \mathbb{N}$, se A_n è vera allora A_{n+1} è vera;*
allora le affermazioni A_n sono vere per ogni $n \in \mathbb{N}$.

Dimostrazione. La seconda asserzione del teorema segue dalla prima usando l'insieme $M = \{i \in \mathbb{N} \mid A_i \text{ è vera}\}$. La prima asserzione segue dal buon ordinamento di $\mathbb{N}$: supponiamo che $M \neq \mathbb{N}$; allora esiste un minimo elemento in $\mathbb{N} \smallsetminus M \neq \varnothing$, sia i_0; per minimalità abbiamo che $i_0 - 1 \in M$, da cui segue che $i_0 \in M$ (per la prima condizione se $i_0 = 1$, per la seconda se $i_0 > 1$), assurdo. □

4.5.1. Ad esempio mostriamo per induzione la formula $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Verifichiamo il caso $n = 1$, che dà in effetti $1 = \frac{1(1+1)}{2}$. Ora supponiamo vera la formula per il valore n, e vediamo cosa succede per $n + 1$:

$$1 + 2 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

(nel primo passaggio abbiamo usato l'ipotesi induttiva) che è esattamente la stessa formula con $n+1$ invece di n; quindi le formule sono dimostrate per ogni n.

Questa formula può anche essere dimostrata "alla Gauss" osservando che ogni coppia di numeri "equidistanti dagli estremi" dà come somma $n + 1$, e che di tali coppie ve ne sono $n/2$ (anche se in questo c'è una imprecisione: quale?).

Un metodo ulteriore per dimostrare la formula senza induzione è la seguente osservazione:

$$\sum_{i=1}^{n} i^2 + (n+1)^2 - 1 = \sum_{i=1}^{n} (i+1)^2 = \sum_{i=1}^{n} i^2 + 2\sum_{i=1}^{n} i + n$$

(sviluppando in due modi diversi il termine centrale), da cui, uguagliando i termini estremi, sparisce la sommatoria dei quadrati e si può ricavare la sommatoria voluta.

4.5.2. Trovare e dimostrare per induzione una formula per la sommatoria dei quadrati dei primi n numeri naturali.

4.5.3. Dimostrare per induzione che la somma dei cubi dei primi n numeri naturali è pari al quadrato della somma dei primi n numeri naturali; in formule $\sum_{i=1}^{n} i^3 = (\sum_{i=1}^{n} i)^2$, e dunque $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.

4.5.4. Trovare e dimostrare per induzione una formula per la sommatoria delle quarte potenze dei primi n numeri naturali.

4.5.5. Mostrare per induzione (su j) che la somma delle j-esime potenze dei primi n naturali è data da un polinomio in n di grado $j + 1$?

4.5.6. Dimostrare per induzione la formula di inclusione-esclusione.

4.6. Teorema (Principio di Induzione (seconda forma)). *Sia M un sottinsieme di $\mathbb{N}$ soddisfacente alle due proprietà seguenti:*
(0) $0 \in M$;
(i) *per ogni $n \in \mathbb{N}$, se $i \in M$ per ogni $i \leqslant n$ allora $n+1 \in M$;*
allora $M = \mathbb{N}$.

Sia ora A_n una famiglia di asserzioni indiciate da $n \in \mathbb{N}$; supponiamo soddisfatte le due proprietà seguenti:
(0) *A_0 è vera*
(i) *per ogni $n \in \mathbb{N}$, se A_i è vera per ogni $i \leqslant n$ allora A_{n+1} è vera;*
allora le affermazioni A_n sono vere per ogni $n \in \mathbb{N}$.

Dimostrazione. Analoga a quella della prima forma. □

4.6.1. (PROPRIETÀ ARCHIMEDEA DELL'ORDINE DI $\mathbb{N}$). Sia $n \geqslant 1$ un numero naturale; allora per ogni naturale m esiste un naturale p tale che $pn \geqslant m$. Ragioniamo per induzione su m. Se $m = 1$ allora basta usare $p = 1$ e $pn = n \geqslant 1 = m$. Osserviamo anche che lo stesso vale per ogni $m \leqslant n$. Supponiamo ora che $m > 1$, e possiamo supporlo $> n$; consideriamo $m' = m - n < m$ e per ipotesi induttiva troviamo p' tale che $p'n \geqslant m'$. Allora posto $p = p' + 1$ abbiamo $pn = p'n + n \geqslant m' + n = m$, come si voleva.

4.6.2. Altri importanti esempi di questo tipo di induzione si vedranno discutendo la "divisione con resto" tra numeri interi e tra polinomi.

4.7. ULTERIORI VARIAZIONI. Talvolta vi sono enunciati indiciati da numeri naturali che hanno significato solo da un certo valore dell'indice in poi (per esempio: l'unione di n insiemi non dipende dall'ordine in cui viene effettuata; a rigori avrebbe senso solo per $n \geqslant 2$); quindi può essere utile usare delle induzioni che partano da questo indice "minimo" per gli enunciati che si studiano.

Si osservi anche che, se il passo induttivo delle dimostrazioni utilizza diciamo gli m casi precedenti, indipendentemente dal livello n del passo induttivo, allora i "primi m casi" devono essere dimostrati tutti indipendentemente.

4.8. DEFINIZIONI PER INDUZIONE. Un procedimento per induzione si usa anche per definire certi oggetti matematici; noi abbiamo definito "per induzione" degli insiemi N_i che rappresentano le cardinalità finite (infatti abbiamo definito il primo, e poi abbiamo specificato come costruire "il successivo" dato uno qualunque degli elementi). Dare una definizione per induzione di oggetti F_i per $i \in \mathbb{N}$, $i \geqslant k$, significa:

(0) definire il primo F_k;

(i) definire F_{n+1} potendo usare nella definizione gli oggetti F_i con $i \geqslant k$ e $i \leqslant n$.

Spesso risulta facile, o spontaneo dare definizioni per induzione, ma per costruirli veramente bisogna procedere "uno dopo l'altro"; è un problema non facile caratterizzare questi oggetti tramite una "definizione chiusa" che permetta di costruire ciascuno di questi senza essere passati per tutti i precedenti.

4.8.1. FATTORIALI, SEMIFATTORIALI. Un esempio facile è la definizione induttiva del fattoriale: si tratta della funzione $! : \mathbb{N} \to \mathbb{N}$ definita dalla condizione di base $0! = 1$ e dalla condizione induttiva $(n+1)! = (n+1)(n!)$. È immediato in questo caso riconoscere che si tratta della usuale definizione per cui $n!$ è il prodotto dei numeri interi da 1 a n.

Il semifattoriale $!! : \mathbb{N} \to \mathbb{N}$ è la funzione induttivamente definita da $0!! = 1$, $1!! = 1$ e dalla condizione induttiva $(n+2)!! = (n+2)(n!!)$. Anche in questo caso è facile trovare una "formula chiusa", poiché

$$n!! = n(n-2)!! = n(n-2)(n-4)!! = \cdots = n(n-2)(n-4)\cdots(n-2i)\cdots \begin{cases} 0!! & \text{se } n \text{ pari} \\ 1!! & \text{se } n \text{ dispari} \end{cases}$$

e dunque si tratta del prodotto dei numeri pari o dei numeri dispari minori o uguali ad n a seconda che n sia pari o dispari. Come mai abbiamo usato due "condizioni di base"?

4.8.2. NUMERI DI FIBONACCI. I numeri di Fibonacci sono definiti dalle condizioni seguenti: $F(0) = 0$, $F(1) = 1$ e ricorsivamente $F(n+2) = F(n+1) + F(n)$. Si tratta di una funzione $F : \mathbb{N} \to \mathbb{N}$ che ha la caratteristica di crescere molto velocemente (in modo immaginifico, si tratta della crescita di una popolazione di organismi immortali che ad ogni generazione aumenta di numero in modo pari alla somma delle due popolazioni precedenti). I primi numeri di Fibonacci sono i seguenti:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$F(n)$	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946

Esiste una formula chiusa per trovare l'n-esimo numero di Fibonacci, data da

$$F(n) = \frac{\lambda_+^n - \lambda_-^n}{\lambda_+ - \lambda_-} = \frac{1}{2^{n-1}} \sum_{\substack{i=1 \\ i \text{ dispari}}}^{n} \binom{n}{i} 5^{\frac{i-1}{2}}$$

ove $\lambda_\pm = \frac{1 \pm \sqrt{5}}{2}$ ma trovarla con metodi elementari non è facile.

4.8.3. Qual'è la funzione definita da $M(0) = 0$ ed $M(n) = n - M(n-1)$?

4.9. INDUZIONE DOPPIA. L'induzione si basa essenzialmente sulle proprietà d'ordine dell'insieme $\mathbb{N}$; analogamente si possono sfruttare proprietà d'ordine sull'insieme $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ per ottenere tecniche di dimostrazione di enunciati o di definizione di oggetti indiciati da coppie di numeri naturali.

4.9.1. Coefficienti binomiali. I coefficienti binomiali $\binom{n}{k}$ possono essere definiti ricorsivamente per $n \geqslant 0$ e $0 \leqslant k \leqslant n$ nel seguente modo: $\binom{n}{0} = \binom{n}{n} = 1$ per ogni n, e $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. Questa è la formula che permette di costruire il ben noto triangolo di Tartaglia

$k \diagdown n$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	1	1	1	1	1	1	1	1	1	1	1
1		1	2	3	4	5	6	7	8	9	10
2			1	3	6	10	15	21	28	36	45
3				1	4	10	20	35	56	84	110
4					1	5	15	35	70	126	210
5						1	6	21	56	126	252
6							1	7	28	84	210
7								1	8	36	120
8									1	9	45
9										1	10
10											1

ovvero, mettendo le potenze in riga:

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1
1 10 45 120 210 252 210 120 54 10 1

e si può dimostrare per induzione che questa definizione restituisce quella combinatorica già incontrata: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Qual'è l'interpretazione combinatorica della uguaglianza induttiva del triangolo di Tartaglia?

4.9.2. Coefficienti multinomiali. I coefficienti binomiali e il triangolo di Tartaglia di ottengono dallo sviluppo del binomio $(X+Y)^n$. Analizzando gli sviluppi del multinomio $(X_1 + \cdots + X_r)^n$ per induzione su n (con numero di variabili r) si ottengono i coefficienti multinomiali, definendo $\binom{n}{k_1 \cdots k_r}$ (qualche volta non si scrive l'ultimo perché deve essere il complementare ad n della somma dei precedenti) il coefficiente del monomio $X_1^{k_1} \cdots X_r^{k_r}$ (dove la somma dei k_i dà n). Trovare formule ricorsive e chiuse per i coefficienti multinomiali. Nel caso $r = 2$ abbiamo $\binom{n}{k_1\, k_2} = \binom{n}{k_1}$ (coefficienti binomiali usuali).

5. Permutazioni.

5.1. Definizione (Gruppo). *Un gruppo G è un magma associativo con elemento neutro in cui ogni elemento è simmetrizzabile. Un gruppo di dice commutativo o abeliano se è commutativo in quanto magma. Esplicitamente dunque un gruppo è un insieme munito di una operazione $* : G \times G \to G$ soddisfacente alle proprietà seguenti:*

(G1) associatività: $a * (b * c) = (a * b) * c$ per ogni $a, b, c \in G$;

(G2) elemento neutro: esiste $\imath \in G$ tale che $a * \imath = a = \imath * a$ per ogni $a \in G$;

(G3) esistenza dei simmetrici: per ogni $a \in G$ esiste $a^* \in G$ tale che $a * a^* = \imath = a^* * a$;

si tratta di un gruppo abeliano se inoltre vale la

(G4) commutatività: $a * b = b * a$ per ogni $a, b \in G$.

Una funzione $f : G \to H$ tra due gruppi si dice un omomorfismo di gruppi o funzione di gruppi se rispetta le operazioni, ovvero se $f(g * g') = f(g) * f(g')$ per ogni $g, g' \in G$ (si osservi che allora l'elemento neutro di G viene mandato nell'elemento neutro di G').

Piccole conseguenze algebriche:

5.1.1. Simmetrici dei prodotti. Per ogni $a, b \in G$ vale che $(a * b)^* = b^* * a^*$ (il simmetrico di un prodotto è il prodotto dei simmetrici nell'ordine inverso). Infatti $(b^* * a^*) * (a * b) = b^* * (a^* * a) * b = b^* * b = \imath$, e anche in ordine inverso.

5.1.2. Simmetrici dei simmetrici. Per ogni $a \in G$ vale che $(a^*)^* = a$ (il simmetrico del simmetrico è l'elemento stesso). Infatti $a^{**} * a^* = (a * a^*)^* = \imath^* = \imath$, e anche in ordine inverso.

5.1.3. Commutatività. Un gruppo è commutativo se e solo se la funzione simmetria $G \to G$ (che manda ogni elemento nel suo simmetrico) è omomorfismo di gruppi.

5.1.4. Gruppo associato ad un monoide integro. Ad ogni monoide integro M (magma associativo, unitario, commutativo ed integro) si può associare un gruppo (necessariamente abeliano) "aggiungendo i simmetrici di tutti gli elementi che non ce l'abbiano già". Per fare questo si considera l'insieme $M \times M$ e la relazione di equivalenza in esso definita da $(m, n) \sim (x, y)$ se e solo se $m * y = n * x$. Le classi di equivalenza formano allora un gruppo con l'operazione (ben) definita da $(m, n) * (x, y) = (m * x, n * y)$; elemento neutro è la classe di $(\imath, \imath)$, simmetrica della classe (m, n) è la classe (n, m).

La funzione che ad ogni $m \in M$ associa la classe di $(m, \imath)$ dà un morfismo iniettivo di monoidi da M al gruppo associato ad M.

5.1.5. Congruenze e sottogruppi normali. Una relazione di equivalenza R in un gruppo G si dice una congruenza se lo è nel senso dei magmi, cioè se aRb implica $(a * c)R(b * c)$ per ogni $c \in G$, o equivalentemente se aRb e $a'Rb'$ implicano che $(a * a')R(b * b')$.

Contrariamente al caso dei magmi (o anche dei monoidi), una congruenza R su un gruppo G è completamente determinata dalla classe dell'elemento neutro. Detta infatti H la classe $[\imath]_R$, si tratta di un sottinsieme di G dotato delle seguenti proprietà: esso è non vuoto, se $a, b \in H$ allora $a * b^* \in H$ (in particolare $\imath \in H$), se $a \in H$ e $b \in G$ allora $b^* * a * b \in H$. Un tale sottiniseme di G si chiama di solito un sottogruppo normale di G. Ad ogni sottogruppo normale H di G è associata una relazione di equivalenza per cui la classe di congruenza è esattamente H: essa è definita dalla condizione aRb se e solo se $a * b^* \in H$.

Le funzioni che ad ogni relazione di congruenza associa la classe dell'elemento neutro, e che ad ogni sottogruppo normale associa la corrispondente relazione di congruenza sono una l'inversa dell'altra. Anche nel caso dei magmi o dei monoidi queste funzioni potevano essere definite, ma non sarebbero state delle biiezioni una inversa dell'altra.

L'esempio fondamentale di gruppi è dato dai gruppi di permutazioni su n oggetti:

5.2. Definizione (Permutazioni). *Una permutazione su n oggetti è una applicazione biiettiva di $\mathbf{n}$ in sè. L'insieme delle permutazioni su n oggetti si indica con $\mathfrak{S}_n$ (e chiamato anche gruppo simmetrico) ed è un gruppo sotto l'operazione di composizione; elemento neutro è l'applicazione identica, simmetrico di un elemento dato è la funzione inversa. Si tratta di un gruppo, non commutativo se $n > 2$, di cardinalità $n!$ (fattoriale di n).*

5.2.1. Rappresentazione delle permutazioni. Studiando le permutazioni è tradizione usare l'insieme $\{1, 2, \ldots, n\}$ (piuttosto che $\mathbf{n}$). Una permutazione è in effetti una funzione biiettiva, e per facilitare i calcoli algebrici viene utile usare la seguente rappresentazione: se σ è la permutazione, la descriveremo completamente tramite la tabella

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} .$$

Quindi per esempio $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{smallmatrix}\right)$ indica la permutazione identica di $\mathfrak{S}_4$, $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right)$ indica la permutazione che manda 1 in 2, 2 in 3, 3 in 4, 4 in 1. Calcolare la composizione di due permutazioni in questa forma diventa facile, ma per tradizione si calcola prima la permutazione "a sinistra" nella scrittura; così se $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right)$ e $\sigma' = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right)$ abbiamo allora

$$\sigma \circ \sigma' = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{smallmatrix}\right) \text{ e } \sigma' \circ \sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{smallmatrix}\right) .$$

5.2.2. Cicli. Un ciclo è una permutazione in $\mathfrak{S}_n$ che lascia fissi $n - m$ elementi e i restanti m si possono ordinare in modo tale che ognuno sia mandato nel successivo (e l'ultimo nel primo, di conseguenza). L'intero m si dice lunghezza del ciclo (un ciclo di lunghezza 1 è dunque l'identità, e non si dice). Se un ciclo σ ha lunghezza m, allora σ^m è l'identità, e nessun σ^l con $l < m$ è l'identità (per questo m si dice anche periodo del ciclo).

Si osservi che la composizione di due cicli di solito non è un ciclo.

Usualmente per rappresentare un ciclo si scrive semplicemente la sequenza nell'ordine del ciclo degli elementi che non sono fissi; per esempio $(2,4,1)$ rappresenta in $\mathfrak{S}_n$ il 3-ciclo che manda 2 in 4, 4 in 1 e 1 in 2, lasciando fermi tutti gli altri elementi. Si noti che la scrittura non è unica: $(2,4,1) = (4,1,2) = (1,2,4)$.

Si osservi che cicli disgiunti (cioè tali che gli elementi mossi da uno siano fissi per l'altro) commutano tra di loro.

5.2.3. Scambi. I cicli di ordine due si dicono scambi. Gli scambi sono permutazioni idempotenti, e dunque autoinverse.

5.3. Teorema (decomposizione in cicli). *Ogni permutazione si scrive unicamente come composizione dei suoi cicli, che sono a due a due disgiunti.*

Dimostrazione. Data la permutazione $\sigma \in \mathfrak{S}_n$ consideriamo la relazione di equivalenza su $\{1,2,\dots,n\}$ data da $a \sim_\sigma b$ se esiste $i \in \mathbb{Z}$ tale che $a = \sigma^i b$. Trattandosi di una relazione di equivalenza possiamo considerare la partizione associata: ogni elemento della partizione rappresenta un ciclo, trattandosi degli elementi della forma $a, \sigma a, \sigma^2 a, \dots, \sigma^i a$. È chiaro anche che si tratta di cicli disgiunti (sono classi diverse di una partizione), e dunque commutanti tra loro. □

5.4. Teorema (decomposizione in scambi). *Ogni permutazione si scrive (non unicamente) come combinazione di scambi.*

Dimostrazione. Poiché ogni permutazione si decompone in cicli, basta mostrare che ogni ciclo di decompone in scambi, e a meno di cambiare i nomi agli elementi è sufficiente controllare che

$$(1,2,3,\dots,i{-}1,i) = (1,i)\circ(1,i{-}1)\circ\cdots\circ(1,3)\circ(1,2) = (1,2)(1,3)\cdots(1,i{-}1)(1,i)\ .$$

□

5.5. Teorema (segno). *La funzione, detta segno,* $\mathrm{sgn} : \mathfrak{S}_n \to \{\pm 1\}$ *che manda una permutazione in* 1 *se essa si decompone in un numero pari di scambi,* -1 *altrimenti, è un morfismo di gruppi (usando l'operazione di prodotto in* $\{\pm 1\}$*). In particolare, il numero di cicli in due decomposizioni diverse di una data permutazione è determinato modulo* 2 *dalla permutazione (cioè ogni decomposizione in cicli di una fissata permutazione ha un numero pari oppure dispari di cicli).*

Dimostrazione. Consideriamo per ogni permutazione $\sigma \in \mathfrak{S}_n$ il prodotto

$$s(\sigma) = \prod_{1\leqslant i<j\leqslant n} (\sigma(j) - \sigma(i))\ .$$

Ora è chiaro che $s(\sigma) = \pm s(\mathrm{id})$ per ogni σ, poiché si tratta del prodotto di interi dello stesso modulo (cambiano eventualmente l'ordine e il segno); poniamo allora $\mathrm{sgn}(\sigma) = s(\sigma)/s(\mathrm{id}) \in \{\pm 1\}$ D'altra parte, se σ e σ' sono due permutazioni, abbiamo $\mathrm{sgn}(\sigma\sigma') = \mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma')$; infatti

$$\begin{aligned}\mathrm{sgn}(\sigma\sigma') &= \frac{\prod_{i<j}(\sigma'\sigma(j) - \sigma'\sigma(i))}{\prod_{i<j}(j-i)} = \frac{\prod_{i<j}(\sigma(j)-\sigma(i))}{\prod_{i<j}(j-i)}\frac{\prod_{i<j}(\sigma'\sigma(j)-\sigma'\sigma(i))}{\prod_{i<j}(\sigma(j)-\sigma(i))} = \\ &= \mathrm{sgn}(\sigma)\frac{\prod_{\sigma(i)<\sigma(j)}(\sigma'\sigma(j)-\sigma'\sigma(i))}{\prod_{\sigma(i)<\sigma(j)}(\sigma(j)-\sigma(i))} = \mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma')\ .\end{aligned}$$

È facile vedere che per ogni scambio τ abbiamo $\mathrm{sgn}(\tau) = -1$, e quindi per ogni decomposizione in scambi $\sigma = \tau_1\cdots\tau_r$ vale $\mathrm{sgn}(\sigma) = (-1)^r$; quindi due decomposizioni in scambi di σ devono avere la stessa parità. Questo assicura che la funzione così definita è proprio quella cercata, e anche che si tratti di un morfismo di gruppi. □

5.5.1. Gli scambi hanno segno -1; in generale i cicli hanno segno opposto alla parità della loro lunghezza: i cicli dispari hanno segno 1, quelli pari hanno segno -1.

5.5.2. Il segno di una permutazione può anche essere caratterizzato come la parità del numero di scambi che bisogna fare per "riordinare gli oggetti".

5.6. Definizione (gruppo alterno). *Il gruppo alterno su n elementi $\mathfrak{A}_n$ è il sottinsieme di $\mathfrak{S}_n$ formato dalle permutazioni di segno 1; esso è in effetti un gruppo con l'operazione indotta (e anzi un sottogruppo normale di $\mathfrak{S}_n$, e il quoziente $\mathfrak{S}_n/\mathfrak{A}_n$ è proprio $\{\pm 1\}$: perché?).*

5.6.1. Si osservi invece che le permutazioni di segno -1 non formano un gruppo, ma sono in biiezione (non canonica) con le permutazioni di segno 1 (basta fare la composizione con una qualsiasi permutazione di segno -1 per ottenere una tale biiezione). In effetti formano l'altra classe laterale del gruppo quoziente $\mathfrak{S}_n/\mathfrak{A}_n$.

6. Numeri Interi.

6.1. Definizione (Anelli). *Un anello A è un insieme dotato di due operazioni binarie, indicate come somma $(+)$ e prodotto ($\cdot$ o più spesso nulla), verificanti le seguenti proprietà:*

(S) A con la somma è un gruppo commutativo, cioè:
- *(S1) $(a+b)+c = a+(b+c)$ per ogni $a,b,c \in A$;*
- *(S2) esiste un elemento nullo 0 tale che $a+0 = a = 0+a$ per ogni $a \in A$;*
- *(S3) per ogni $a \in A$ esiste un elemento $a' \in A$ tale che $a+a' = 0 = a'+a$ (di solito a' si dice opposto di a e si indica con $-a$);*
- *(S4) $a+b = b+a$ per ogni coppia $a,b \in A$;*

(P) $A \smallsetminus \{0\}$ con il prodotto è un semigruppo, cioè:
- *(P1) $(ab)c = a(bc)$ per ogni $a,b,c \in A$;*
- *(P2) esiste un elemento unità 1 tale che $a1 = a = 1a$ per ogni $a \in A$;*

(D) il prodotto è distributivo rispetto alla somma: $a(b+c) = ab+ac$ e $(b+c)a = ba+ca$ per ogni $a,b,c \in A$.

L'anello si dice commutativo se il prodotto è commutativo.

Una funzione $A \to B$ tra due anelli si dice un morfismo di anelli se rispetta somma e prodotto e manda l'unità di A nell'unità di B (questo non è garantito dalle precedenti condizioni, in generale).

Messe di piccoli risultati algebrici:

6.1.1. Prodotto per zero. Risulta dalle definizioni che $a0 = 0 = 0a$ per ogni $a \in A$; infatti $a = 1a = (1+0)a = 1a+0a = a+0a$ (e anche nell'altro ordine).

6.1.2. Opposto. Per ogni a abbiamo che l'opposto è $-a = (-1)a = a(-1)$; infatti $a+(-1)a = 1a+(-1)a = (1+(-1))a = 0a = 0$ (e anche nell'altro ordine).

Di conseguenza il passaggio all'opposto è un omomorfismo di gruppo per la somma, e quindi la proprietà $(S4)$ è ridondante (segue dalle altre).

6.1.3. Regole dei segni. $a(-b) = -(ab) = (-a)b$, $(-a)(-b) = ab$ (segue dal punto precedente).

6.1.4. Un elemento a di un anello A si dice unipotente se una sua potenza non nulla dà l'unità, cioè se esiste un intero n non nullo per cui $a^n = 1$; in tal caso a è invertibile e $a^{-1} = a^{n-1}$.

Un elemento non nullo a di un anello A si dice nilpotente se una sua potenza dà lo zero, cioè se esiste un intero n per cui $a^n = 0$; in tal caso $1+a$ è invertibile e $(1+a)^{-1} = 1-a+a^2-\cdots+(-1)^{n-1}a^{n-1}$.

Un elemento non nullo a di un anello A si dice divisore di zero se esiste un elemento non nullo b tale che $ab = 0$. I nilpotenti sono divisori di zero.

6.1.5. Anelli integri. Un anello si dice integro se $A \smallsetminus \{0\}$ è integro in quanto semigruppo moltiplicativo, cioè se per ogni $a,b, \in A$ e $c \in A$ non nullo, da $ac = bc$ (oppure $ca = cb$) segue $a = b$. Un anello integro non ha divisori di zero, né nilpotenti.

Un anello integro e commutativo si chiama un dominio.

6.1.6. Anelli ordinati. Un anello si dice ordinato se in esso è definita una relazione d'ordine $\leqslant$ soddisfacente alle seguenti proprietà:

(AO1) se $a \geqslant b$ allora $a+c \geqslant b+c$ per ogni $c \in A$;

(AO2) se $a \geqslant b$ e $c \geqslant 0$ allora $ac \geqslant bc$.

Dato un anello ordinato possiamo definire l'insieme degli elementi positivi $P \subseteq A$ come $P = \{a \in A \mid a > 0\}$; allora P gode delle seguenti proprietà:

(P1) per ogni $c \in A$ non nullo si ha che o $c \in P$ oppure $-c \in P$ (e non entrambe);

(P2) P è chiuso rispetto alla somma dei suoi elementi;

(P3) P è chiuso rispetto al prodotto dei suoi elementi.

Viceversa, dato un insieme P con le proprietà elencate, esiste un unico ordine su A per cui quello sia l'insieme dei positivi: basta definire $a \geqslant b$ se e solo se $a - b \in P$.

Si osservi che in ogni anello ordinato si ha che tutti i quadrati sono positivi e in particolare $1 > 0$. Di conseguenza un corpo ordinato ha infiniti elementi, poiché le somme iterate di 1 sono sempre tra loro diverse.

6.1.7. Congruenze e ideali. Una relazione di equivalenza R su un anello A di dice di congruenza se essa rispetta entrambe le operazioni, cioè se aRb implica $(a+c)R(b+c)$, $acRbc$ e $caRcb$ per ogni $c \in R$ (o equivalentemente se aRb e $a'Rb'$ implicano $(a+a')R(b+b')$ e $aa'Rbb'$). Come nel caso dei gruppi, tali relazioni di equivalenza sono completamente individuate dalla classe $I = [0]_R$ dell'elemento nullo; tale classe è un sottinsieme di A dotato delle seguenti proprietà: non è vuoto, se $a, b \in I$ allora $a - b \in I$ (in particolare $0 \in I$), se $a \in I$ e $b \in A$ allora $ab, ba \in I$. Un tale sottinsieme di A si dice un ideale bilatero di A. Ad ogni ideale bilatero I resta associata una congruenza definita da aRb se e solo se $a - b \in I$ la cui classe di 0 risulta esattamente I.

6.1.8. Ideali massimali. Un ideale bilatero si dice massimale se è diverso dall'anello e non è contenuto in nessun altro ideale bilatero proprio. Usando il lemma di Zorn possiamo dimostrare che ogni anello ammette ideali massimali (anche contenenti un fissato ideale bilatero proprio, o un fissato elemento non invertibile dell'anello).

6.1.9. Divisibilità, relazione di divisibilità. Dati due elementi a, b di un anello A si dice che a divide b e si scrive $a|b$ se esiste $c \in A$ tale che $ac = b$. La relazione di divisibilità è una relazione riflessiva e transitiva. In generale non è una relazione antisimmetrica, e quindi non è una relazione d'ordine; anche quando lo fosse, non sarebbe una relazione d'ordine per l'anello (perché?).

Se abbiamo due elementi $a, b \in A$ tali che $a|b$ e $b|a$ allora a e b si dicono associati e scriviamo $a \sim b$; si tratta di una relazione di equivalenza che non è in generale una congruenza. In un anello integro, due elementi a e b sono associati se e solo se "differiscono per un invertibile", cioè $a = ub$ con $u \in A$ elemento invertibile.

6.1.10. Formula del binomio di Newton. In ogni anello commutativo vale la seguente identità:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

per ogni $a, b \in A$ e ogni $n \in \mathbb{N}$. Questa formula si può dimostrare in almeno due modi. Il primo puramente combinatorico: ogni termine della forma $a^i b^{n-i}$ compare un certo numero di volte nello sviluppo del binomio, esattamente tante quante le combinazioni di i oggetti da un insieme contenente n oggetti. L'altra dimostrazione possibile è per induzione: la formula essendo vera per $n = 0, 1$, basta controllare il passo induttivo:

$$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} = \sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i} =$$
$$= \sum_{i=0}^{n+1} \left(\binom{n}{i} + \binom{n}{i-1} \right) a^i b^{n+1-i} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}$$

ove abbiamo usato l'ipotesi induttiva nel secondo passaggio, e la relazione ricorsiva del triangolo di Tartaglia nell'ultimo passaggio.

6.2. Per ogni insieme X, l'insieme potenza $\mathscr{P}(X)$ dotato delle operazioni di differenza simmetrica (come somma) e di intersezione (come prodotto) ha struttura di anello commutativo.

Il più semplice anello è quello dei numeri interi, che si può vedere come il gruppo associato al monoide $\mathbb{N}$ con l'operazione $+$, e a cui viene estesa l'operazione di prodotto.

6.3. Definizione (Numeri interi). *L'insieme $\mathbb{Z}$ dei numeri interi è definito come l'insieme quoziente di $\mathbb{N}^2$ modulo la relazione di equivalenza definita da $(a, b) \sim (a', b')$ se e solo se $a + b' = a' + b$ (in $\mathbb{N}$); spesso la classe della coppia (a, b) si indica con $a - b$. Quest'insieme è dotato di due operazioni:*
(S) somma $(a - b) + (a' - b') = (a + a') - (b + b')$;
(P) prodotto $(a - b)(a' - b') = (aa' + bb') - (ab' + a'b)$;
queste due operazioni rendono $\mathbb{Z}$ un anello commutativo con elemento nullo $0 - 0$ ($= a - a$ per ogni $a \in \mathbb{N}$), elemento identico $1 - 0$ ($= (a + 1) - a$ per ogni $a \in \mathbb{N}$), opposto di $a - b$ essendo $b - a$.

6.3.1. Rappresentazione usuale. In effetti di solito si dice che i numeri interi sono l'insieme formato dai numeri naturali e "dai loro opposti"; si può riconoscere questa descrizione osservando che ogni intero nel senso della definizione può essere rappresentato da una coppia del tipo $(a, 0)$ e allora è un numero naturale, oppure da una coppia del tipo $(0, a)$ e allora è l'opposto di un numero naturale.

Identifichiamo $\mathbb{N}$ con le coppie del tipo $(a, 0)$, cioè con le classi $a - 0$, tramite la funzione iniettiva $\mathbb{N} \to \mathbb{Z}$ che manda a in $a - 0$ $(= (a+b) - b$ per ogni $b \in \mathbb{N}$, e possiamo indicare con a anche l'immagine). D'altra parte possiamo chiamare $-\mathbb{N}$ l'immagine della funzione iniettiva $\mathbb{N} \to \mathbb{Z}$ che manda a in $0 - a$ $(= b - (a + b)$ per ogni $b \in \mathbb{N}$, e possiamo indicare con $-a$ l'immagine). Allora risulta che $\mathbb{Z}$ è unione di $\mathbb{N}$ (detti i numeri interi positivi) e di $-\mathbb{N}$ (detti i numeri interi negativi). Risulta $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ e $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$.

6.3.2. Prodotto e regole dei segni. In questa rappresentazione, si ricavano subito le usuali regole di calcolo del prodotto: $(-a)b = -(ab) = a(-b)$ e $(-a)(-b) = ab$. In effetti tutto segue dal fatto che $-a = (-1)a$, come s'è visto in generale per gli anelli.

6.3.3. L'unità e il suo opposto sono gli unici elementi invertibili di $\mathbb{Z}$.

6.3.4. Integrità. Si verifica anche facilmente che $\mathbb{Z}$ è anello integro, poiché ci si riduce al prodotto in $\mathbb{N}$.

6.3.5. Ordine. Vi è un unico modo di estendere l'ordine di $\mathbb{N}$ ad un ordine totale su $\mathbb{Z}$, dato dalla seguente definizione: $(a - b) \leqslant (a' - b')$ se e solo se $a + b' \leqslant a' + b$ (in $\mathbb{N}$). Si verifica allora immediatamente che i numeri negativi sono minori di zero, e che $a \leqslant b$ se e solo se $-b \leqslant -a$.

6.4. Definizione (Norma o Valore assoluto di numeri interi). *La funzione $\mathbb{Z} \to \mathbb{N}$ definita da $|z| = \begin{cases} z & \text{se } z \geqslant 0 \\ -z & \text{se } z < 0 \end{cases}$ si dice norma o valore assoluto e soddisfa alle seguenti proprietà:*

(N1) $|z| = 0$ *se e solo se* $z = 0$*;*

(N2) moltiplicatività: $|zz'| = |z||z'|$*;*

(N3) subadditività: $|z + z'| \leqslant |z| + |z'|$ *(e vale l'uguaglianza se sono entrambi positivi o entambi negativi);*

6.5. Teorema (Divisione con resto). *Dati due numeri interi a e b con $b \neq 0$ esiste una unica coppia di numeri interi q, r tali che $a = qb + r$ con $0 \leqslant r < |b|$. Si dice che q è il quoziente e r il resto della divisione di a (dividendo) per b (divisore).*

Dimostrazione (algoritmo di divisione). Basta mostrare il risultato quando a e b sono interi positivi (perché?). Possiamo procedere per induzione su a nel modo seguente: se $a = 0$, evidentemente $q = r = 0$ qualsiasi sia b. Se ora $a > 0$; se $a < b$ abbiamo ancora $q = 0$ e $r = a$; se invece $a \geqslant b$ abbiamo $a > a - b \geqslant 0$. Possiamo allora usare la seconda forma dell'induzione e supporre che esistano unici q_1 ed r_1 interi positivi tali che $a - b = q_1 b + r_1$ con $r_1 < b$; ma allora basta scegliere $q = q_1 + 1$ e $r = r_1$ per ottenere $a = qb + r$ come voluto.

L'unicità di quoziente e resto può essere dimostrata direttamente: se $a = qb + r$ con $0 \leqslant r < b$ e $a = q'b + r'$ con $0 \leqslant r' < b$, supponendo $r > r'$ la differenza dà $(q' - q)b = r - r'$ che è assurdo, poiché $b \leqslant (q' - q)b = r - r' < b$. Dunque dev'essere $r = r'$ e di conseguenza $q = q'$. □

Dimostrazione alternativa (usando il buon ordinamento di $\mathbb{N}$). Consideriamo l'insieme $R = \{a - qb : b \in \mathbb{Z}\}$; allora $R \cap \mathbb{N}$ (in quanto sottinsieme di $\mathbb{N}$) ha elemento minimo, che è il resto cercato. □

6.5.1. Ideali principali. Dall'esistenza della divisione con resto, si deduce che tutti gli ideali di $\mathbb{Z}$ sono principali, cioè formati dai multipli di un unico elemento. Infatti ciò è ovvio per gli ideali banali (nullo e tutto, generati rispettivamente da 0 e 1); sia ora I un ideale non banale, e sia b il minimo positivo in I: allora $I = b\mathbb{Z}$. Infatti se $a \in I$, operando la divisione di a per b otteniamo $a = qb + r$ da cui si vede che $r \in I$; ora siccome b è il minimo elemento positivo di I, deve risultare $r = 0$ (nella divisione $r < b$), e allora a è multiplo di b.

6.6. Definizione (MCD, mcm). *Dati due numeri interi a e b definiamo un massimo comun divisore* $\mathrm{MCD}(a, b)$*, spesso denotato semplicemente (a, b), come un massimo (per il preordine di divisibilità) dei divisori comuni di a e b; si tratta cioè di un intero d che divide sia a che b e tale che ogni divisore comune di a e b divida anche d. Due massimo comun divisori di a e b sono dunque tra loro associati.*

Analogamente si definisce un minimo comune multiplo, denotato $\mathrm{mcm}(a,b)$*, come un minimo (per la divisibilità) dei multipli comuni di* a *e* b*.*

6.6.1. È chiaro che MCD e mcm sono unici a meno del segno (se d e d' lo sono, allora ciascuno divide l'altro). Se chiediamo che siano interi positivi, allora sono unicamente definiti. Lo sottintenderemo sempre nel seguito.

6.6.2. Relazione tra MCD e mcm. Dati due numeri interi positivi risulta che

$$\mathrm{mcm}(a,b)\mathrm{MCD}(a,b) = ab\ ;$$

infatti posto $d = \mathrm{MCD}(a,b)$ abbiamo $a = a'd$, $b = b'd$ (con $\mathrm{MCD}(a',b') = 1$), da cui segue che $a'b'd = ab/d$ è un multiplo comune di a e di b; se ora m è multiplo comune di a e di b (dunque $m = a''a$ e $m = b''b$), e fosse un divisore di $a'b'd = ab/d$ (dunque $mc = ab/d$ ovvero $mcd = ab$) avremmo che $mcd = a''acd = ab$ e $mcd = b''bcd = ab$, da cui si vede che cd sarebbe divisore comune di a e b, assurdo a meno che non sia $c = 1$.

6.6.3. $\mathrm{MCD}(ac,bc) = c\,\mathrm{MCD}(a,b)$, $\mathrm{mcm}(ac,bc) = c\,\mathrm{mcm}(a,b)$?

6.6.4. Estensione a n numeri interi. Definizioni analoghe di massimo comun divisore e minimo comune multiplo si possono dare per ogni insieme finito $a_1, a_2, \dots, a_n$ di numeri interi. La facile relazione $\mathrm{MCD}(a,b,c) = \mathrm{MCD}(\mathrm{MCD}(a,b),c)$ e più generalmente

$$\mathrm{MCD}(a_1, a_2, \dots, a_n) = \mathrm{MCD}(\mathrm{MCD}(a_1, a_2, \dots, a_{n-1}), a_n)$$

riduce induttivamente il calcolo al caso di una coppia di numeri.

6.6.5. mcm. È facile vedere che un minimo comune multiplo tra due interi positivi a e b è il generatore (positivo) dell'ideale intersezione $a\mathbb{Z} \cap b\mathbb{Z}$; più generalmente abbiamo che $\mathrm{mcm}(a_1, \dots, a_n)$ è il generatore (positivo) dell'ideale $\bigcap_{i=1}^n a_i\mathbb{Z}$.

6.7. Teorema (MCD). *Il massimo comun divisore* d *tra tra due interi positivi* a *e* b *è il generatore (positivo) dell'ideale generato da* $a\mathbb{Z} \cup b\mathbb{Z}$ *(il più piccolo ideale contenente sia* a *che* b*); esistono due interi* h, k *tali che* $d = ha + kb$*, e* d *è il minimo intero positivo che si può scrivere in questa forma.*

Dimostrazione. Consideriamo l'insieme I dei numeri interi della forma $ma + nb$ al variare di $m, n \in \mathbb{Z}$. Si tratta chiaramente di un ideale di $\mathbb{Z}$, quindi si tratta dei multipli di un intero positivo d che è il minimo intero positivo di I. Poiché $a, b \in I$, abbiamo che d divide sia a che b, e dunque è un divisore comune. Inoltre per definizione esistono due interi h, k tali che $d = ha + kb$. Sia ora d' un divisore comune di a e b, diciamo $a = a'd'$ e $b = b'd'$; allora abbiamo $d = ha + kb = ha'd' + kb'd' = (ha' + kb')d'$, da cui si vede che d' divide d. □

6.7.1. Nell'enunciato e nella sua dimostrazione si può evitare la nozione di ideale esprimendosi così: *Il massimo comun divisore* d *tra tra due interi positivi* a *e* b *il minimo intero positivo che si può scrivere nella forma* $d = ha + kb$ *con* $h, k \in \mathbb{Z}$. Infatti supponiamo che $d = ha + kb$ sia minimo e mostriamo che divide sia a che b; se non dividesse a potremmo usare la divisione eulcidea $d = aq + r$ con $r > 0$ e $r = d - aq = ((h-q)a + kb$, assurdo perché sarebbe $r < d$.

6.7.2. Dal teorema segue che due numeri interi a e b sono primi tra loro se e solo se esistono interi h, k tali che $ha + kb = 1$.

6.7.3. Il teorema e l'osservazione precedente possono estendersi al caso di un numero finito di interi; il massimo comun divisore tra gli interi $a_1, a_2, \dots, a_n$ è il minimo intero positivo che si scrive nella forma $h_1a_1 + h_2a_2 + \cdots + h_na_n$ con gli h_i interi. Inoltre essi sono coprimi (cioè il loro massimo comun divisore è 1) se e solo se esistono degli interi h_i tali che $h_1a_1 + h_2a_2 + \cdots + h_na_n = 1$.

6.7.4. Relazione di Bézout. I combinatori interi h e k che esprimono d come $ha + kb$ non sono unici, ma se si impone loro di soddisfare certe condizioni di minimalità, allora sono ben determinati e la relazione $d = ha + kb$ si dice di Bézout. La condizione è questa: se $a \geqslant b$, $a = da'$, $b = db'$ allora possiamo chiedere che $|h| < |b'|$ e $|k| < |a'|$. Combinatori con questa proprietà sono forniti dall'algoritmo di Euclide.

6.8. Algoritmo di Euclide. Dalla dimostrazione non è chiaro in effetti come procedere per calcolare il massimo comun divisore tra due numeri, né come calcolare i coefficienti h e k. Un metodo per fare ciò è l'algoritmo di Euclide che ora presentiamo. L'idea fondamentale è semplice, e può dare un'altra dimostrazione del Teorema precedente: se $a = bq + r$ è la divisione euclidea di a per b, allora

$\mathrm{MCD}(a,b) = \mathrm{MCD}(b,r)$, con il vantaggio che nel secondo termine dell'uguaglianza abbiamo numeri più piccoli; ripetendo questo procedimento un numero finito (perché?) di volte si ottiene il risultato voluto (perché?).

Siano a e b due numeri interi positivi di cui vogliamo calcolare il massimo comun divisore (si tratta evidentemente di trovare il generatore positivo dell'ideale generato dai due). Poniamo le seguenti definizioni ricorsive: $a_1 = a$, $a_2 = b$, $a_i = a_{i+1}q_i + a_{i+2}$ (divisione con resto di a_i per a_{i+1}, che dunque definisce il quoziente q_i e il resto a_{i+2} avente la proprietà d'essere minore di a_{i+1}). Dunque abbiamo la sequenza:

$$a_1 = a, \quad a_2 = b, \quad a_3 = a_1 - q_1 a_2, \quad \cdots, \quad a_{i+2} = a_i - q_i a_{i+1}, \quad \cdots$$

Ora è chiaro che ad ogni passo la sequenza a_i al variare di i diminuisce (strettamente), e dunque esiste un n tale che $a_n \neq 0$ ma $a_{n+1} = 0$; allora $d = a_n$. Infatti svolgendo a ritroso le uguaglianze $a_{i+2} = a_i - a_{i+1}q_i$ si vede che a_n si scrive come richiesto nella dimostrazione, dunque appartiene all'ideale cercato I; e d'altra parte dal fatto che a_n divide a_{n-1}, sempre andando a ritroso si vede che a_n divide a_i per ogni $i \leqslant n$, ed in particolare divide sia a che b.

Per tener conto dei coefficienti senza fare i conti a ritroso, conviene ricorrere alla usuale tabellina, ricorsivamente definita in modo che ad ogni passo si abbia $a_i = h_i a_1 + k_i a_2$:

$a_1 = a$	$h_1 = 1$	$k_1 = 0$	
$a_2 = b$	$h_2 = 0$	$k_2 = 1$	
a_3	$h_3 = 1$	$k_3 = -q_1$	$[a_1 = q_1 a_2 + a_3]$
a_4	$h_4 = -q_2 h_3 = -q_2$	$k_4 = 1 - q_2 k_3 = 1 + q_1 q_2$	$[a_2 = q_2 a_3 + a_4]$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{i+2}	$h_{i+2} = h_i - q_i h_{i+1}$	$k_{i+2} = k_i - q_i k_{i+1}$	$[a_i = q_i a_{i+1} + a_{i+2}]$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_n	$h_n = h_{n-2} - q_{n-2} h_{n-1}$	$k_n = k_{n-2} - q_{n-2} k_{n-1}$	$[a_{n-2} = q_{n-2} a_{n-1} + a_n]$
0			$[a_{n-1} = q_{n-1} a_n]$

infatti possiamo osservare che

$$\begin{aligned} a_{i+2} &= a_i - a_{i+1} q_i \\ &= (h_i a_1 + k_i a_2) - (h_{i+1} a_1 + k_{i+1} a_2) q_i \\ &= (h_i - q_i h_{i+1}) a_1 + (k_i - q_i k_{i+1}) a_2 \end{aligned}$$

per il passo induttivo.

6.8.1. Il lettore è invitato a farsi qualche esempio di divisione tra interi e di calcolo di MCD tra interi.

6.8.2. Nota sull'algoritmo. Probabilmente il lettore ha studiato come calcolare MCD e mcm tra numeri interi passando attraverso la fattorizzazione in primi; il punto è che fattorizzare un numero intero in primi non è facile, se non nei casi di numeri piccoli, mentre l'algoritmo di Euclide per il calcolo del MCD è un procedimento molto veloce anche in presenza di numeri grandi.

6.9. Teorema (fondamentale dell'aritmetica: primi e fattorizzazione). *Un numero intero positivo diverso dall'unità si dice primo se è divisibile solo per* 1 *e per se stesso. Ogni numero intero positivo si scrive in modo essenzialmente unico come prodotto di primi (essenzialmente significa a meno dell'ordine).*

Dimostrazione. Si può fare usando la seconda forma dell'induzione; infatti la proprietà è ovvia per 1 e per tutti i numeri primi. Se ora n è un numero maggiore di 1 e non primo, esso si esprime come prodotto $m'm''$ di due interi positivi, ciascuno minore di m; dunque per ipotesi induttiva essi ammettono una fattorizzazione come nell'enunciato, e di conseguenza anche m (facendo il prodotto delle fattorizzazioni).

Per dimostrare l'unicità della fattorizzazione basta applicare a due distinte fattorizzazioni di uno stesso intero positivo il seguente risultato: *se p è un primo, e p divide un prodotto ab, allora p divide almeno uno dei due fattori; quindi per induzione: se p divide un prodotto di interi, allora p divide almeno uno dei fattori.* Supponiamo infatti che p divida ab, ma non divida a, e proviamo che divide b; siccome a e p sono coprimi abbiamo $1 = ah + pk$ per opportuni interi h, k. Moltiplicando per b

otteniamo $b = abh + pbk$, e poiché $ab = pl$ (per ipotesi p divide ab) risulta $b = plh + pbk = p(lh + bk)$, e dunque p divide b, come si voleva. □

Parlando di polinomi, e di particolari tipi di anelli (principali e fattoriali) vedremo che la stessa proprietà si poteva dimostrare usando solo il fatto che gli ideali di $\mathbb{Z}$ sono principali.

6.9.1. Probema. Si generalizzi la proprietà usata nella dimostrazione di unicità della fattorizzazione nel seguente modo: se a divide un prodotto bc e a è primo con b, allora a divide c.

6.9.2. Infinità dei numeri primi. È ben noto dall'antichità che i numeri primi sono infiniti. Ricordiamo una delle prime e più semplici verifiche di questo fatto: se per assurdo vi fosse solo un numero finito di primi, allora il numero intero ottenuto sommando 1 al prodotto di tutti questi primi sarebbe maggiore di ciascuno dei primi dati, e non divisibile per alcuno di essi.

6.9.3. Calcoli di MCD e mcm tramite fattorizzazione. Dati due numeri interi a e b e la loro fattorizzazione in primi $a = \pm p_1^{r_1} \cdots p_i^{r_i} p_{i+1}^{r_{i+1}} \cdots p_m^{r_m}$ e $b = \pm p_1^{s_1} \cdots p_i^{s_i} q_{i+1}^{s_{i+1}} \cdots q_n^{s_n}$ (ove si intende che lettere diverse indicano primi distinti) allora possiamo determinare massimo comun divisore e minimo comune multiplo nel modo seguente: $\mathrm{MCD}(a,b) = p_1^{\min(r_1,s_1)} \cdots p_i^{\min(r_i,s_i)}$ (prodotto dei fattori comuni con il minimo esponente) e $\mathrm{mcm}(a,b) = p_1^{\max(r_1,s_1)} \cdots p_i^{\max(r_i,s_i)} p_{i+1}^{r_{i+1}} \cdots p_m^{r_m} q_{i+1}^{s_{i+1}} \cdots q_n^{s_n}$ (prodotto di tutti i fattori con il massimo esponente).

6.10. Congruenze, anelli modulo. Fissato un intero m, due numeri interi a e b si dicono congrui modulo m e si scrive $a \equiv b \pmod{m}$ se $a - b$ è divisibile per m. Si tratta di una relazione di equivalenza, e anzi di congruenza poiché è definita in termini dell'ideale $m\mathbb{Z}$.

L'anello quoziente $\mathbb{Z}/m\mathbb{Z}$ delle classi resto per la relazione di congruenza modulo m ha un numero finito di elementi (esattamente m) e può essere descritto in termini delle classi degli interi da 0 a $m-1$. La classe dell'intero a è descritta come $[a]_m = \{a + im \mid i \in \mathbb{Z}\}$.

Si osservi che se m non è primo allora $\mathbb{Z}/m\mathbb{Z}$ contiene divisori di zero: infatti se $m = ab$ in $\mathbb{Z}$, allora $[a]_m \neq 0 \neq [b]_m$, ma $[a]_m[b]_m = [ab]_m = [m]_m = [0]_m$. Vedremo che se m è primo, allora le classi modulo m formano un anello integro, ed anzi un corpo (ogni elemento non nullo è invertibile).

6.10.1. In questo tipo di anelli bisogna fare particolare attenzione trattando di equazioni, anche lineari; per esempio può succedere che "una equazione di primo grado $aX = b$ nella incognita X" abbia due soluzioni. Per esempio $aX = 0$ in $\mathbb{Z}/(ab)\mathbb{Z}$ ha come soluzioni sia la classe di 0, sia la classe di b (che sono diverse tra loro). Una interpretazione geometrica di questo fatto può essere la seguente: nel "piano" $(\mathbb{Z}/(ab)\mathbb{Z})^2$ (formato da a^2b^2 "punti") le due "rette" di equazioni $Y = aX$ e $Y = 0$ pur essendo distinte si incontrano in due punti distinti, l'origine $(0,0)$ e il punto $(b,0)$. Queste osservazioni sconsigliano dunque di fare geometria "ingenua" sugli anelli.

6.10.2. Si osservi anche che ogni anello resto, come pure ogni anello con un numero finito di elementi, non può essere ordinato.

6.10.3. Relazioni tra congruenze diverse. Si osservi che:

(*a*) se $a \equiv b \pmod{m}$ e m' divide m allora $a \equiv b \pmod{m'}$;

(*b*) se $a \equiv b \pmod{m}$ allora $ac \equiv bc \pmod{(m,c)}$ (ovvio);

(*c*) se $ac \equiv bc \pmod{m}$ allora $a \equiv b \pmod{m/(m,c)}$ (questo è meno ovvio: conviene vederlo nella forma $ac \equiv 0 \pmod{m}$, e allora abbiamo $c = c'(m,c)$, $m = m'(m,c)$ con $(m',c') = 1$. Allora risulta che m divide ac, dunque m' divide ac', e quindi m' divide a).

6.10.4. Teorema (soluzioni di congruenze). *Consideriamo una congruenza $aX \equiv b \pmod{m}$ con $a, b \in \mathbb{Z}$ e X una incognita; allora esistono soluzioni (cioè valori $x \in \mathbb{Z}$ che soddisfano alla congruenza) se e solo se (a,m) divide b, e in tal caso tutte e sole le soluzioni sono date da $x_0 + \frac{m}{(m,a)}k$ ove $k \in \mathbb{Z}$ e x_0 è una soluzione qualsiasi (si tratta della classe laterale modulo $\frac{m}{(m,a)}$ di una qualsiasi soluzione).*

Dimostrazione. Supponiamo che esista una soluzione x_0; allora abbiamo $ax_0 = b + km$ per qualche $k \in \mathbb{Z}$, da cui $b = ax_0 - km$ e quindi b deve essere un multiplo del MCD tra a e m. Viceversa, supponiamo $b = c(m,a)$; poiché $(m,a) = hm + ka$, troviamo $b = c(hm + ka) = chm + cka$, e dunque $x_0 = ck$ è una soluzione cercata.

Se ora x_0 è una soluzione ($ax_0 \equiv b \pmod{m}$), e x è un'altra soluzione ($ax \equiv b \pmod{m}$), abbiamo $ax \equiv ax_0 \pmod{m}$, e quindi $a(x - x_0) \equiv 0 \pmod{m}$, da cui si deduce che $x - x_0$ è un multiplo di $\frac{m}{(m,a)}$, come si voleva. □

♠ **6.10.5.** Teorema (cinese del resto). *Siano $m_1, m_2, \dots, m_r$ numeri interi a due a due coprimi; allora il sistema di congruenze $X \equiv a_i \pmod{m_i}$ per $i = 1, 2, \dots, r$ ammette soluzioni nell'incognita X, e l'insieme delle soluzioni è dato dagli interi appartenenti ad una classe di $\mathbb{Z}$ modulo $\Pi_i m_i$.*

Dimostrazione. Osserviamo che il minimo comune multiplo tra gli m_i è esattamente il loro prodotto (per l'ipotesi di coprimalità). Consideriamo allora la funzione di anelli

$$\mathbb{Z}/(\Pi_i m_i)\mathbb{Z} \longrightarrow (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})$$

che manda $[x]_m$, se $m = \Pi_i m_i$, in $([x]_{m_1}, \dots, [x]_{m_r})$. Si tratta di una funzione iniettiva tra insiemi finiti della stessa cardinalità. Essa è dunque anche suriettiva, ed è quanto afferma il teorema. □

6.10.6. Invertibili negli anelli di interi modulo n. Un elemento non nullo $\overline{x}$ dell'anello $\mathbb{Z}/m\mathbb{Z}$ è invertibile se e solo se esiste $y \in \mathbb{Z}$ tale che $\overline{xy} = \overline{1}$, ovvero $xy \equiv 1 (\bmod\ m)$, dunque se e solo se esistono $y, z \in \mathbb{Z}$ tali che $xy + zm = 1$. Questo significa esattamente che x e m sono primi tra loro: dunque la classe di $x \in \mathbb{Z}$ è invertibile modulo m (cioè in $\mathbb{Z}/m\mathbb{Z}$) se e solo se x è primo con m.

♠ **6.10.7.** Funzione di Eulero. La funzione $\Phi : \mathbb{N} \to \mathbb{N}$ di Eulero è definita associando ad ogni numero naturale n il numero di elementi invertibili in $\mathbb{Z}/n\mathbb{Z}$, ovvero per $n > 1$ la cardinalità dell'insieme dei numeri minori di n ad esso coprimi. È facile calcolare i primi valori:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\Phi(n)$	2	1	1	2	2	4	2	6	4	6	4	10	4	12	6	10	8	16	6	18	8

ed in effetti si possono determinare con le seguenti osservazioni:

(1) caso di numeri primi p: se p è un primo, allora $\Phi(p) = p - 1$; infatti tutti i numeri naturali non nulli minori di p sono primi con p;

(2) proprietà moltiplicativa per numeri coprimi: se $n, n' \in \mathbb{N}$ e $(n, n') = 1$, cioè n ed n' sono primi tra loro, allora $\Phi(nn') = \Phi(n)\Phi(n')$; questo si può vedere direttamente, ma segue anche dalla dimostrazione vista del teorema cinese del resto, che dice che $\mathbb{Z}/(nn')\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n'\mathbb{Z})$, studiando gli invertibili dell'anello prodotto (sono le coppie formate da elementi invertibili di ciascun anello);

(3) potenze di numeri primi: consideriamo ora p^r con p primo; i numeri naturali minori di p^r e primi con esso sono esattamente quelli non divisibili per p, dunque vale

$$\Phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1) = p^r\left(1 - \frac{1}{p}\right) .$$

Ora per un qualsiasi numero naturale n, possiamo ricorrere alla sua fattorizzazione in numeri primi $n = \Pi_i p_i^{r_i}$ e di conseguenza calcolare

$$\Phi(n) = \prod_i p_i^{r_i - 1}(p_i - 1) = n \prod_i \left(1 - \frac{1}{p_i}\right) .$$

♠ **6.10.8.** Si può provare, per esempio per induzione sul numero di primi nella fattorizzazione di n, l'uguaglianza

$$\sum_{d|n} \Phi(d) = n$$

ove la sommatoria è estesa a tutti i divisori di n (compresi 1 ed n). Si osservi che questa formula può anche essere usata come definizione induttiva (nella seconda forma) della funzione di Eulero.

♠ **6.10.9.** Funzione di Moebius. La funzione di Moebius $\mu : \mathbb{N} \to \{0, \pm 1\}$ è definita per ogni numero naturale nel modo seguente:

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \text{ oppure } n \text{ si fattorizza in un numero pari di primi distinti} \\ 0 & \text{se nella fattorizzazione di } n \text{ vi sono dei primi ripetuti} \\ -1 & \text{se } n \text{ si fattorizza in un numero dispari di primi distinti} \end{cases}$$

ed è ovvio constatare che se n ed m sono coprimi allora $\mu(nm) = \mu(n)\mu(m)$ (se non sono coprimi abbiamo banalmente $\mu(nm) = 0$).

Si può esprimere la funzione di Eulero in termini della funzione di Moebius:

$$\Phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

per qualsiasi $n \in \mathbb{N}$.

7. Corpi numerici.

7.1. Definizione (Corpo). *Un corpo $\Bbbk$ è un anello in cui ogni elemento non nullo ammette un inverso; in dettaglio si tratta di un insieme dotato di due operazioni binarie, indicate come somma (+) e prodotto ($\cdot$ o più spesso nulla), verificanti le seguenti proprietà:*

(S) $\Bbbk$ con la somma è un gruppo commutativo, cioè:
- *(S1) $(a+b)+c = a+(b+c)$ per ogni $a,b,c \in \Bbbk$;*
- *(S2) esiste un elemento nullo 0 tale che $a+0 = a = 0+a$ per ogni $a \in \Bbbk$;*
- *(S3) per ogni $a \in \Bbbk$ esiste un elemento $a' \in \Bbbk$ (detto opposto di a e indicato con $-a$) tale che $a+a' = 0 = a'+a$;*
- *(S4) $a+b = b+a$ per ogni coppia $a,b \in \Bbbk$;*

(P) $\Bbbk^\times = \Bbbk \smallsetminus \{0\}$ con il prodotto è un gruppo, cioè:
- *(P1) $(ab)c = a(bc)$ per ogni $a,b,c \in \Bbbk$;*
- *(P2) esiste un elemento unità 1 tale che $a1 = a = 1a$ per ogni $a \in \Bbbk$;*
- *(P3) per ogni $a \in \Bbbk$ diverso da 0 esiste un elemento $a'' \in \Bbbk$ (detto inverso di a e indicato con a^{-1}) tale che $aa'' = 1 = a''a$;*

(D) il prodotto è distributivo rispetto alla somma: $a(b+c) = ab+ac$ per ogni $a,b,c \in \Bbbk$.

Il corpo si dice commutativo se il prodotto è commutativo; spesso un corpo commutativo di dice un campo.

Una funzione tra due corpi si dice un morfismo di corpi se rispetta le operazioni di somma e prodotto dei due corpi.

Messe di piccoli risultati algebrici:

7.1.1. Leggi di cancellazione. In ogni corpo vale che $ac = bc$ con $c \neq 0$ implica $a = b$; infatti basta moltiplicare per l'inverso di c.

7.1.2. Principio di annullamento del prodotto. In ogni corpo vale che $ab = 0$ implica $a = 0$ oppure $b = 0$; infatti, se $a \neq 0$ basta moltiplicare per l'inverso di a per ottenere $b = 0$.

7.1.3. Un corpo non ha divisori di zero né nilpotenti: segue dall'osservazione precedente.

7.1.4. Corpi ordinati. Un corpo si dice ordinato se lo è in quanto anello. Se $\Bbbk$ è un corpo ordinato e $x \in \Bbbk$, da $x > 0$ segue che $x^{-1} > 0$.

7.1.5. Talvolta si accetta che anche $\{0\}$ (insieme con un solo elemento e con l'unica struttura possibile di gruppo) sia un corpo con identità uguale a zero.

7.2. Numeri razionali. L'insieme dei numeri razionali $\mathbb{Q}$ è il più piccolo corpo contenente l'anello $\mathbb{Z}$ dei numeri interi (in modo che le operazioni in $\mathbb{Q}$ estendano quelle di $\mathbb{Z}$). Si può costruire nel modo seguente: si consideri in $\mathbb{Z} \times (\mathbb{Z} \smallsetminus 0)$ la relazione $\sim$ di equivalenza definita da $(a,b) \sim (x,y)$ se e solo se $ay = bx$ (in $\mathbb{Z}$). Verificato per bene che si tratta di una relazione di equivalenza, costruiamo l'insieme quoziente $\mathbb{Z} \times (\mathbb{Z} \smallsetminus 0)/\sim$, ed indichiamo con la notazione familiare $\frac{a}{b}$ la classe dell'elemento (a,b); allora abbiamo $\frac{a}{b} = \frac{x}{y}$ se e solo se $ay = bx$.

Definiamo ora le operazioni sull'insieme quoziente nel modo usuale: il prodotto di due classi $\frac{a}{b}$ e $\frac{a'}{b'}$ sia $\frac{aa'}{bb'}$ (verificare che il risultato non dipende dai rappresentanti usati per definirlo), e la somma sia $\frac{ab'+a'b}{bb'}$ $(= \frac{ab'}{bb'} + \frac{a'b}{bb'})$ (di nuovo il risultato dipende solo dalla classe di equivalenza, e non dai rappresentanti). Con queste operazioni l'insieme quoziente risulta un corpo ove l'elemento nullo è la classe $\frac{0}{1}$ $(= \frac{0}{a}$ per ogni $a \neq 0)$, l'elemento unità è la classe di $\frac{1}{1}$ $(= \frac{a}{a}$ per ogni $a \neq 0)$ e l'inverso per $\frac{a}{b}$ se $a \neq 0$ è la classe $\frac{b}{a}$.

7.2.1. Ordine in $\mathbb{Q}$. Possiamo anche rendere $\mathbb{Q}$ un corpo ordinato definendo l'insieme degli elementi positivi come le classi $\frac{b}{a}$ con $a,b \in \mathbb{N}$ (i positivi di $\mathbb{Z}$).

7.2.2. Proprietà archimedea di $\mathbb{Q}$. Il corpo ordinato dei razionali gode della seguente proprietà: per ogni coppia a,b di razionali maggiori di 0, esiste un intero positivo n tale che $na > b$.

7.3. Corpo dei quozienti per domini. La strategia utilizzata per costruire $\mathbb{Q}$ a partire da $\mathbb{Z}$ può essere generalizzata nel modo seguente: se A è un qualsiasi dominio (anello commutativo ed integro), allora l'insieme quoziente di $A \times (A \smallsetminus \{0\})$ modulo la relazione di equivalenza definita da $(a,b) \sim (x,y)$ se e solo se $ay = bx$ (in A) ha una struttura di corpo (detto corpo dei quozienti di A) quando sia dotato delle operazioni definite da $\frac{a}{b}\frac{a'}{b'} = \frac{aa'}{bb'}$ (prodotto) e $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+a'b}{bb'}$ (somma) ove $\frac{a}{b}$ indica la classe di (a,b).

L'ipotesi che l'anello sia integro è importante affinché la relazione definita per fare il quoziente sia in effetti una relazione di equivalenza.

7.4. Numeri reali. L'insieme $\mathbb{R}$ dei numeri reali può essere definito come il completamento ordinale del corpo dei numeri razionali $\mathbb{Q}$; esso verrà studiato dettagliatamente in un corso di Analisi. Ricordiamo solo che $\mathbb{R}$ può essere definito come l'unico gruppo (per la somma) archimedeo completo (a meno di isomorfismi ordinati: vedi Barsotti).

7.4.1. Automorfismi di $\mathbb{R}$. Per comodità ricordiamo anche che l'unico automorfismo di corpo di $\mathbb{R}$ è l'identità; ciò si dimostra nel modo seguente: prima di tutto è facile vedere che un'automorfismo di $\mathbb{R}$ dev'essere l'identità su $\mathbb{Z}$ e quindi su $\mathbb{Q}$; poi si verifica che manda l'insieme dei positivi nell'insieme dei positivi, e di conseguenza è crescente. Infine per un elemento $x \in \mathbb{R} \smallsetminus \mathbb{Q}$ si consideri la sua immagine x', e si supponga $x' \neq x$, per esempio $x' > x$; si scelga $q \in \mathbb{Q}$ tale che $x' > q > x$ (densità di $\mathbb{Q}$ in $\mathbb{R}$). Allora calcolando le immagini abbiamo $q = q' > x' > q$, assurdo.

7.5. Corpi finiti. Consideriamo ora in $\mathbb{Z}$ la relazione di congruenza modulo p; allora l'insieme quoziente $\mathbb{Z}/p\mathbb{Z}$, con le due operazioni ereditate da $\mathbb{Z}$, è un corpo se e solo se p è un numero primo. Infatti, se p è primo, per ogni $n \in \mathbb{Z}$ non nultiplo di p abbiamo che $(n, p) = 1$ (sono coprimi) e dunque esistono interi x, y tali che $xn + yp = 1$; ma allora la classe di x è l'inverso della classe di n. Se invece p non è primo, nell'anello quoziente si trovano dei divisori di zero, come abbiamo già visto.

7.5.1. Indichiamo con $\mathbb{F}_p$ il corpo $\mathbb{Z}/p\mathbb{Z}$ se p è primo; si tratta di un insieme con p elementi dotato della struttura di corpo. Invitiamo il lettore a scrivere le tabelle di somma e moltiplicazione per $p = 2, 3, 5, 7$.

I corpi finiti non sono ordinati.

7.5.2. Si osservi che per ogni $x \in \mathbb{F}_p$ si ha $x^p = x$.

7.6. Caratteristica dei corpi. Dato un corpo $\Bbbk$ qualsiasi, possiamo considerare l'unica mappa di anelli $\mathbb{Z} \to \Bbbk$ (definita dal fatto di mandare 1 di $\mathbb{Z}$ nell'1 di $\Bbbk$). Se si osserva l'antimmagine in $\mathbb{Z}$ dello zero (di $\Bbbk$), vi sono due possibilità:

(0) tale insieme contiene solo lo zero; in tal caso la funzione è iniettiva, il corpo $\Bbbk$ contiene una copia di $\mathbb{Z}$ e dunque di $\mathbb{Q}$. In questo caso il corpo $\Bbbk$ si dice di caratteristica zero.

(p) tale insieme contiene tutti i multipli di un fissato primo p; in tal caso la funzione si fattorizza attraverso una mappa iniettiva $\mathbb{Z}/p\mathbb{Z} \to \Bbbk$, e il corpo $\Bbbk$ contiene una copia di $\mathbb{Z}/p\mathbb{Z}$. In questo caso il corpo $\Bbbk$ si dice di caratteristica (positiva) p.

Noi abbiamo visto che esistono corpi di caratteristica p che sono finiti ed hanno esattamente p elementi; in effetti per ogni intero n esiste (ed unico a meno di isomorfismi) un corpo di caratteristica p con esattamente p^n elementi (ma non è $\mathbb{Z}/p^n\mathbb{Z}$: perché?), che si indica non $\mathbb{F}_q$ se $q = p^n$ e si vedrà essere il campo di spezzamento del polinomio $X^q - X$ come polinomio a coefficienti in $\mathbb{F}_p$. Inoltre esistono corpi di caratteristica $p \neq 0$ aventi infiniti elementi (farsi qualche esempio). Non possiamo per il momento giustificare queste affermazioni, che diamo solo per conoscenza, e per le quali rimandiamo ad un corso di Algebra.

Abbiamo visto che ogni corpo contiene una copia del corpo dei numeri razionali (se è di caratteristica nulla) oppure una copia del corpo con p elementi (se è di caratteristica p); perciò questi corpi ($\mathbb{Q}$ ed $\mathbb{F}_p$ al variare di p nei numeri primi) sono detti corpi fondamentali.

7.6.1. In un corpo di caratteristica p abbiamo che $(a \pm b)^p = a^p \pm b^p$, poiché per ogni $0 < i < p$ il fattoriale $\binom{p}{i}$ è divisibile per p. Dunque l'elevamento alla potenza p è un morfismo di corpo per ogni corpo di caratteristica p, ed è l'identità sul suo sottocorpo fondamentale; si chiama endomorfismo di Frobenius.

♠ **7.7.** I numeri di Gauss. Un esempio particolarmente significativo di anello e del suo corpo dei quozienti è dato dai numeri di Gauss che ora definiamo.

7.7.1. Gli interi di Gauss. L'anello degli interi di Gauss è l'insieme $\mathbb{Z}[i]$ delle espressioni del tipo $a + ib$ con $a, b \in \mathbb{Z}$ ove i è il "numero immaginario complesso", con le operazioni definite come nel caso del corpo complesso. Si osservi che gli unici elementi invertibili in $\mathbb{Z}[i]$ sono quelli per cui $a^2 + b^2$ è un intero invertibile, e dunque ± 1: quindi sono ± 1 e $\pm i$.
Si noti che il numero intero primo 2 si fattorizza in $\mathbb{Z}[i]$ nel modo seguente $2 = (1 + i)(1 - i)$; come pure $5 = (2 + i)(2 - i)$.

7.7.2. Il corpo di Gauss. Il corpo delle frazioni di $\mathbb{Z}[i]$ si indica con $\mathbb{Q}[i]$ ed è formato dalle espressioni del tipo $a+ib$ con $a,b\in\mathbb{Q}$ (e si tratta di un sottocorpo del corpo $\mathbb{C}$ dei numeri complessi).

7.7.3. L'anello $\mathbb{Z}[i]$ e il corpo $\mathbb{Q}[i]$ non sono ordinabili: perché?

♠ **7.8.** Estensioni reali quadratiche dei razionali. Consideriamo le espressioni del tipo $a+b\sqrt{2}$ con $a,b\in\mathbb{Q}$; esse formano un insieme indicato con $\mathbb{Q}[\sqrt{2}]$ che si può identificare con un sottinsieme di $\mathbb{R}$ (ma è pericoloso: si può fare in due modi). Con le usuali posizioni possiamo dare a $\mathbb{Q}[\sqrt{2}]$ la struttura di corpo (in effetti sottocorpo del corpo reale); analogamente al caso di Gauss e del corpo complesso possiamo definire per ogni $a+b\sqrt{2}$ il suo coniugato $a-b\sqrt{2}$; allora il prodotto $(a+b\sqrt{2})(a-b\sqrt{2})=a^2-2b^2$ è un numero razionale nullo se e solo se $a=b=0$ (cioè solo per l'elemento nullo); questo equivale al fatto che $\sqrt{2}$ non è un numero razionale, che si dimostra per assurdo usando la proprietà di fattorizzazione unica in $\mathbb{Z}$: se $\sqrt{2}=a/b$ con $a,b\in\mathbb{Z}$ allora $2b^2=a^2$ (uguaglianza di numeri interi in cui il primo 2 comparirebbe nella fattorizzazione un numero dispari di volte a sinistra, e un numero pari a destra).

7.8.1. Il corpo $\mathbb{Q}[\sqrt{2}]$ non ha un ordine canonico. Vi sono due automorfismi che sono l'identità su $\mathbb{Q}$ (quali?).

7.8.2. Il corpo $\mathbb{Q}[\sqrt{2}]$ è corpo dei quozienti di un opportuno anello $\mathbb{Z}[\sqrt{2}]$.

7.8.3. Lo stesso tipo di costruzione si può fare "aggiungendo a $\mathbb{Q}$" la radice quadrata di un elemento (che non sia quadrato in $\mathbb{Q}$).

7.9. Numeri complessi (e geometria del piano).

7.9.1. Numeri complessi. La costruzione dei numeri complessi parte dall'osservazione che il corpo dei numeri reali non è "algebricamente chiuso": ossia esistono delle equazioni polinomiali a coefficienti in $\mathbb{R}$ che non ammettono soluzioni in $\mathbb{R}$; l'esempio più famoso è $X^2=-1$ (infatti se un numero è un quadrato, non può essere negativo nell'ordine di $\mathbb{R}$). D'altra parte si può cercare di costruire un corpo contenente $\mathbb{R}$ e in cui quell'equazione abbia soluzione; per esempio chiamando i un numero (immaginario!) tale che $i^2=-1$, possiamo considerare l'insieme di tutte le espressioni del tipo $a+ib$ ove a e b sono elementi di $\mathbb{R}$. Allora se vogliamo definire una somma ed un prodotto tra scritture di questo tipo, che rispettino le regole distributiva ed associativa, siamo costretti a porre $(a+ib)+(a'+ib')=(a+a')+i(b+b')$ e anche $(a+ib)(a'+ib')=(aa'-bb')+i(ab'+a'b)$ ("infatti" $(a+ib)(a'+ib')=aa'+aib'+iba'+i^2bb'=aa'+iab'+ia'b-bb'$). Risulta allora in effetti che l'insieme così definito è un corpo con zero dato da $0+i0$, unità data da $1+i0$, in cui opposto di $a+ib$ è $-a-ib=(-a)+i(-b)$. Per ogni elemento non nullo $a+ib$, un calcolo diretto mostra che l'elemento $\frac{a}{a^2+b^2}-i\frac{b}{a^2+b^2}$ è il suo inverso. La verifica delle altre proprietà è essenzialmente ovvia.

Di solito si procede in modo più formale, e meno comprensibile, dando la definizione seguente:

7.9.1.1. Definizione (Numeri Complessi). *Il corpo $\mathbb{C}$ dei numeri complessi è l'insieme $\mathbb{R}^2$ dotato delle seguenti operazioni:*
(S) $(a,b)+(a',b')=(a+a',b+b')$;
(P) $(a,b)(a',b')=(aa'-bb',ab'+a'b)$.
Queste operazioni soddisfano agli assiomi affinché $\mathbb{C}$ sia un corpo; in particolare lo zero è $(0,0)$, l'identità è $(1,0)$, opposto di (a,b) è $(-a,-b)$, inverso di (a,b) è $\left(\frac{a}{a^2+b^2},-\frac{b}{a^2+b^2}\right)$. Si osserva poi che l'elemento $(0,1)$ ha come quadrato l'opposto dell'identità (e quindi $\mathbb{C}$ non può essere un corpo ordinato: se 1 è positivo, -1 è negativo e non può essere un quadrato).

Si osserva infine che la funzione $\mathbb{R}\to\mathbb{C}$ che manda a in $(a,0)$ è una funzione iniettiva che identifica $\mathbb{R}$ a un sottinsieme di $\mathbb{C}$ (anche per le operazioni), detto parte reale di $\mathbb{C}$. Invece la funzione $\mathbb{R}\to\mathbb{C}$ che manda b in $(0,b)$ è una funzione iniettiva, ma rispetta solo la somma, e non il prodotto; l'immagine si chiama parte puramente immaginaria di $\mathbb{C}$.

7.9.1.2. Scrivendo $i=(0,1)$ e per ogni numero reale $a=(a,0)$, vediamo che $(a,b)=(a,0)+(0,b)=(a,0)+(0,1)(b,0)=a+ib$, e quindi riconosciamo la costruzione più intuitiva prima introdotta. Di solito i numeri complessi si indicano con lettere tipo z,u,v,w, e se $z=a+ib$, il numero reale a si dice la parte reale di z e si indica con $\Re(z)$, mentre il numero reale b si indica con $\Im(z)$ e si chiama la parte immaginaria di z. Quindi $z=\Re(z)+i\Im(z)$ per ogni $z\in\mathbb{C}$.

7.9.1.3. Coniugazione. Se z è un numero complesso, definiamo il suo coniugato $\overline{z}$ come $\Re(z) - i\Im(z)$ (cambiamo di segno la parte immaginaria). Abbiamo allora una funzione $\mathbb{C} \to \mathbb{C}$ che è un automorfismo di corpo; cioè è una biiezione dotata delle seguenti proprietà:

($C1$) rispetta le operazioni di somma ($\overline{z+z'} = \overline{z} + \overline{z'}$)

($C2$) e di prodotto ($\overline{zz'} = \overline{z}\overline{z'}$).

Notiamo inoltre che:

($C3$) gli elementi fissi della coniugazione (cioè gli elementi mandati in sè stessi) sono tutti e soli i numeri reali: $z = \overline{z}$ se e solo se $z \in \mathbb{R}$;

($C4$) la coniugazione è una involuzione ($\overline{\overline{z}} = z$ per ogni z), e quindi è la sua propria inversa.

7.9.1.4. Le relazioni tra parti reali e immaginarie, e coniugio per un numero complesso z sono riassunte nelle seguenti formule:

$$z = \Re(z) + i\Im(z) \qquad \Re(z) = \frac{z+\overline{z}}{2}$$

$$\overline{z} = \Re(z) - i\Im(z) \qquad \Im(z) = \frac{z-\overline{z}}{2i}$$

(le coordinate $x = \Re(z)$ e $y = \Im(z)$ sono dette cartesiane, mentre le coordinate z e $\overline{z}$ sono dette hermitiane).

7.9.1.5. Norma (o modulo) di numeri complessi. Per ogni numero complesso z definiamo la sua norma (talvolta detta anche modulo) $|z|$ come la radice quadrata positiva del prodotto $z\overline{z} = \Re(z)^2 + \Im(z)^2$, che risulta un numero reale. Abbiamo allora una funzione $\mathbb{C} \to \mathbb{R}$ soddisfacente alle seguenti proprietà:

($N1$) positività: $|z| \geqslant 0$ per ogni $z \in \mathbb{C}$ e $|z| = 0$ se e solo se $z = 0$;

($N2$) moltiplicatività: $|zz'| = |z|\,|z'|$;

($N3$) subaddittività: $|z+z'| \leqslant |z| + |z'|$ (e vale l'uguaglianza se e solo se $z/z' \in \mathbb{R}_{>0}$).

Si osservi anche dalla formula $|z|^2 = z\overline{z}$ segue che

$$z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{\Re(z) - i\Im(z)}{\Re(z)^2 + \Im(z)^2}$$

come già prima osservato per ogni $z \neq 0$. Inoltre abbiamo anche (disuguaglianze sul quadrilatero)

($N4$) $||z| - |z'|| \leqslant |z - z'|$;

($N5$) $|z+z'|^2 + |z-z'|^2 = 2(|z|^2 + |z'|^2)$.

Naturalmente, se $x \in \mathbb{R}$ abbiamo ($x \in \mathbb{C}$ e) $|x| = |x|$ (valore assoluto in senso reale, e norma in senso complesso coincidono, motivo per cui si può ragionevolmente usare lo stesso simbolo).

La proprietà di subaddittività non è banale, e per verificarla possiamo confrontare i termini al quadrato (essendo reali positivi):

a sinistra abbiamo $|z+z'|^2 = (z+z')(\overline{z} + \overline{z'}) = |z|^2 + 2\Re(\overline{z}z') + |z'|^2$,

mentre a destra abbiamo $(|z| + |z'|)^2 = |z|^2 + 2|z||z'| + |z'|^2 = |z|^2 + 2|zz'| + |z'|^2$,

e quindi basta confrontare $\Re(\overline{z}z')$ con $|zz'| = |\overline{z}z'| = \sqrt{\Re(\overline{z}z')^2 + \Im(\overline{z}z')^2}$, che dà immediatamente la disuguaglianza, e anche il criterio per l'uguaglianza (ovvero $\Im(\overline{z}z') = 0$).

Le formule sul quadrilatero si ricavano similmente.

7.9.1.6. Argomento e Versore. I numeri complessi z di norma 1 si dicono unitari, e soddisfano alla condizione $\Re(z)^2 + \Im(z)^2 = 1$; quindi esiste un unico reale $\vartheta \in [0, 2\pi)$ tale che $\Re(z) = \cos\vartheta$ e $\Im(z) = \sin\vartheta$. In generale per ogni numero complesso z non nullo, il numero $\mathrm{ver}(z) = z/|z|$ è unitario, si dice il versore di z, e il valore ϑ associato si dice argomento di z e si indica con $\arg(z)$. Dunque abbiamo definito una funzione

$$\arg : \mathbb{C} \smallsetminus \{0\} \to [0, 2\pi) \qquad (\text{e anche } \ \mathrm{ver} : \mathbb{C} \smallsetminus \{0\} \to \mathbb{S}^1)$$

soddisfacente alle seguenti proprietà: $z \in \mathbb{R}$ se e solo se $\arg(z) \in \{0, \pi\}$ (se e solo se $\mathrm{ver}(z) = \pm 1$); $\arg(zz') = \arg(z) + \arg(z')$ a meno di multipli di 2π (equivalentemente $\mathrm{ver}(zz') = \mathrm{ver}(z)\mathrm{ver}(z')$).

7.9.1.7. Forma trigonometrica. Per ogni numero complesso z, se $\arg(z) = \vartheta$ e $|z| = \varrho$, abbiamo la rappresentazione parametrica di z data da

$$z = \varrho(\cos\vartheta + i\sin\vartheta)$$

che fa vedere come il numero complesso z sia identificato nel piano reale dalle sue "coordinate polari" ϱ (distanza dall'origine) e ϑ (angolo di rotazione rispetto all'asse reale positivo).

In questa rappresentazione è particolarmente facile dare una interpretazione geometrica del prodotto di due numeri complessi; dati infatti $z = \varrho(\cos\vartheta + i\sin\vartheta)$ e $z' = \varrho'(\cos\vartheta' + i\sin\vartheta')$, abbiamo che

$$\begin{aligned} zz' &= \varrho(\cos\vartheta + i\sin\vartheta)\varrho'(\cos\vartheta' + i\sin\vartheta') \\ &= \varrho\varrho'((\cos\vartheta\cos\vartheta' - \sin\vartheta\sin\vartheta') + i(\cos\vartheta\sin\vartheta' + \sin\vartheta\cos\vartheta')) \\ &= \varrho\varrho'(\cos(\vartheta+\vartheta') + i\sin(\vartheta+\vartheta')) \end{aligned}$$

e dunque il prodotto è il numero complesso che ha come norma il prodotto delle norme, e come argomento la somma dei due argomenti (modulo 2π); in altri termini z viene moltiplicato per la norma di z' e ruotato dell'argomento di z'. In particolare diventa facile capire come elevare alla potenza n-esima un numero complesso: z^n è il numero complesso la cui norma è la potenza n-esima della norma di z, e il cui argomento è n volte l'argomento di z:

$$\text{se} \quad z = \varrho(\cos\vartheta + i\sin\vartheta) \quad \text{allora} \quad z^n = \varrho^n(\cos(n\vartheta) + i\sin(n\vartheta)) \ .$$

7.9.1.8. Problema. Dall'espressione $(\cos\vartheta + i\sin\vartheta)^n = \cos(n\vartheta) + i\sin(n\vartheta)$ ricavare le formule di n-plicazione dell'angolo, cioè espressioni di $\cos(n\vartheta)$ e $\sin(n\vartheta)$ in termini di $\cos\vartheta$ e/o $\sin\vartheta$.

7.9.1.9. Formule di De Moivre. Dall'osservazione precedente, si ottiene subito un metodo per il calcolo delle radici n-esime di un numero complesso z. Si tratta delle soluzioni dell'equazione $X^n = z$ in $\mathbb{C}$, che sono sempre n se $z \neq 0$, e si ottengono come i numeri complessi di norma la radice n-esima (reale positiva) della norma di z, e di argomento tale che moltiplicato per n dia (a meno di multipli di 2π) l'argomento di z. In formule (dette di De Moivre): le radici n-esime di $z = \varrho(\cos\vartheta + i\sin\vartheta)$ sono date da

$$\sqrt[n]{\varrho}\Big(\cos\Big(\frac{\vartheta}{n} + \frac{2\pi k}{n}\Big) + i\sin\Big(\frac{\vartheta}{n} + \frac{2\pi k}{n}\Big)\Big)$$

per i valori interi di k compresi tra 0 ed $n-1$.

7.9.1.10. Rappresentazione geometrica: Piano di Gauss. Rappresentando i numeri complessi come coppie di numeri reali è possibile dare un significato geometrico a tutte le nozioni sopra introdotte. Inseriamo qui solamente i disegni, su cui invitiamo il lettore a riflettere.

7.9.1.11. Radici complesse dell'unità. In particolare l'espressione precedente si applica per il calcolo delle radici n-esime dell'unità, ovvero per le soluzioni dell'equazione $X^n = 1$ in $\mathbb{C}$. Dall'interpretazione geometrica prima data dell'elevamento a potenza si capisce subito che si tratta di numeri complessi unitari che sono i vertici del poligono regolare con n lati inscritto nel cerchio unitario e un cui vertice sia 1. Esempi:

(1) l'unica radice 1-aria di 1 è 1;
(2) le due radici quadrate di 1 sono 1 e -1;

(3) le tre radici terze di 1 sono 1 e $\cos\frac{2\pi}{3} \pm \sin\frac{2\pi}{3}$ (vertici del triangolo equilatero);
(4) le quattro radici quarte di 1 sono ± 1 e $\pm i$ (vertici del quadrato);
(5) le cinque radici quinte dell'unità sono 1, $\cos\frac{2\pi}{5} \pm \sin\frac{2\pi}{5}$, $\cos\frac{4\pi}{5} \pm \sin\frac{4\pi}{5}$ (vertici del pentagono regolare);
(6) le sei radici seste dell'unità sono ± 1, $\cos\frac{\pi}{3} \pm \sin\frac{\pi}{3}$, $\cos\frac{2\pi}{3} \pm \sin\frac{2\pi}{3}$ (vertici dell'esagono regolare).

7.9.1.12. Problema. Considerando che $X^n - 1 = \Pi_{i=1}^n (X - \omega_i)$, ove ω_i sono le radici n-esime dell'unità, mostrare che $\Sigma_{i=1}^n \omega_i = 0$, ovvero che la somma di tutte le radici n-esime dell'unità è nulla. Quali altre formule è possibile ricavare da quell'espressione?

7.9.1.13. Radici primitive n-esime dell'unità. Una radice n-esima z dell'unità si dice primitiva se $z^i \neq 1$ per $i < n$ (n è la minima potenza di z che dia 1). Se z è una radice primitiva n-esima dell'unità, allora una sua potenza z^i è ancora una radice primitiva n-esima dell'unità se e solo se i è primo con n (verificare). Di conseguenza per ogni n il numero di radici primitive n-esime dell'unità è uguale a $\Phi(n)$ (funzione di Eulero).

7.9.1.14. Radici n-esime di -1.

7.9.1.15. Radici n-esime di i.

7.9.1.16. Forma esponenziale. La proprietà della funzione argomento rispetto al prodotto di numeri complessi (che diventa la somma degli argomenti) suggerisce di usare una notazione esponenziale per i numeri complessi di norma uno ponendo

$$e^{i\vartheta} = \cos\vartheta + i\sin\vartheta \ .$$

Questa espressione sarà giustificata in un corso di Analisi (studiando gli sviluppi di Taylor delle funzioni esponenziali e circolari trigonometriche), ma possiamo già notare come essa renda sensibilmente semplici alcune formule viste.

Ad esempio ogni numero complesso z si scrive come $\varrho e^{i\vartheta}$, e la sua potenza n-esima si scrive $z^n = (\varrho e^{i\vartheta})^n = \varrho^n e^{in\vartheta}$. Analogamente le radici n-esime sono $\varrho^{\frac{1}{n}} e^{i\frac{\vartheta+2\pi k}{n}}$ per $k = 0, 1, \ldots, n-1$.

Le radici n-esime dell'unità nel corpo complesso si scrivono in notazione esponenziale come $e^{i\frac{k\pi}{n}}$ per $k = 0, 1, \ldots, n-1$.

7.9.1.17. Formula di Eulero. Particolarmente importante, anche se segue subito dalle definizioni, è la seguente uguaglianza:

$$e^{i\pi} + 1 = 0$$

(detta formula di Eulero) che lega le cinque costanti fondamentali $0, 1, i, e, \pi$, considerata tra le più belle formule della Matematica.

7.9.1.18. Funzione esponenziale complessa e logaritmi complessi. La definizione generale di una funzione esponenziale complessa, essenzialmente decisa dalla notazione introdotta, è la seguente: se $z = a + ib$ allora $e^z = e^{a+ib} = e^a e^{ib} = e^a(\cos b + i \sin b)$. Da ciò possiamo anche dedurre la nozione di logaritmo complesso: i numeri complessi w tali che $e^w = z$ (tali w si dicono i logaritmi complessi di z) sono quelli della forma $\log \varrho + i(\vartheta + 2k\pi)$ per $k \in \mathbb{Z}$ se $z = \varrho e^{i\vartheta} \neq 0$. In particolare ogni numero complesso non nullo ha una famiglia numerabile di logaritmi: ciò deriva dal fatto che la funzione esponenziale complessa ha un comportamento periodico riguardo alla componente immaginaria dell'esponente: $e^z = e^{z+i2k\pi}$ per ogni k intero.

7.9.1.19. Teorema (fondamentale dell'algebra). *Ogni polinomio non costante a coefficienti complessi ammette almeno uno zero in $\mathbb{C}$; e dunque ogni tale polinomio ha esattamente tante radici in $\mathbb{C}$ quant'è il suo grado.*

Una dimostrazione di questo risultato basata su metodi analitici reali si può trovare nel testo "Algebraic Structures" di S. Lang, ch. VII, §5. Esistono anche dimostrazioni di carattere algebrico, ma richiedono buone conoscenze: vedi I. Barsotti, "Appunti di Algebra", lezione 70.

7.9.1.20. Teorema (fondamentale dell'algebra, versione reale). *Ogni polinomio non costante a coefficienti reali si fattorizza come prodotto di polinomi reali irriducibili che possono essere di primo grado oppure di secondo grado (e privi di radici reali, dunque con due radici complesse coniugate). In particolare ogni polinomio reale di grado dispari ha almeno una radice reale.*

Dimostrazione. In effetti, se z è una radice complessa del polinomio $P(X)$ a coefficienti reali, allora anche il coniugato $\overline{z}$ è radice dello stesso polinomio (se $P(z) = 0$, allora $0 = \overline{P(z)} = P(\overline{z})$, poiché $P(X)$ ha coefficienti reali). Dunque le radici complesse non reali si presentano sempre a coppie coniugate, e danno luogo a un fattore reale $(X - z)(X - \overline{z}) = X^2 - 2\Re(z)X + |z|^2$ di secondo grado del polinomio $P(X)$. L'ultima affermazione è una ovvia conseguenza. □

7.9.1.21. Identità dei due quadrati. Dalla proprietà moltiplicativa della norma complessa si deriva la seguente regola, detta identità dei due quadrati: *il prodotto di due somme di due quadrati è ancora una somma di due quadrati.* Infatti:

$$(a^2 + b^2)(a'^2 + b'^2) = (aa' - bb')^2 + (ab' + a'b)^2$$

si ottiene esplicitando $|z|^2|z'|^2 = |zz'|^2$.

7.9.2. Geometria del piano usando i numeri complessi. Identificando i numeri complessi con le coppie di numeri reali abbiamo una biiezione canonica tra $\mathbb{C}$ e $\mathbb{R}^2$ (piano cartesiano usuale), ma nei numeri complessi abbiamo anche la nozione di prodotto che si rivela molto utile per impostare e risolvere problemi di geometria del piano.

7.9.2.1. Rette e cerchi nel piano complesso. Insiemisticamente, il corpo $\mathbb{C}$ coincide con $\mathbb{R}^2$, e il lettore conosce già le espressioni cartesiane di rette e cerchi nel piano reale; è interessante vedere le analoghe espressioni usando la variabile complessa.

Cominciamo dalle rette: usando le variabili reali X e Y si tratta delle espressioni del tipo $aX + bY + c = 0$ $(a, b, c \in \mathbb{R})$ in cui almeno uno tra a e b non è nullo (cioè la coppia (a, b) non è nulla). Ricordando che $2X = Z + \overline{Z}$ e $2iY = Z - \overline{Z}$, otteniamo la forma $\overline{\alpha}Z + \alpha\overline{Z} + 2c = 0$, ove $\alpha = a + ib$. Viceversa ogni tale espressione con $\alpha \in \mathbb{C}$ non nullo e $c \in \mathbb{R}$ rappresenta una retta del piano. Si osservi il significato geometrico dei due coefficienti: α come numero complesso indica una direzione ortogonale alla retta (infatti $i\alpha$ risolve l'equazione con $c = 0$); se $|\alpha| = 1$ allora $|c|$ è il doppio della distanza della retta dall'origine (si può verificare per esempio calcolando le intercette della retta con i due assi cartesiani: $x_0 = -c/2\Re(\alpha)$ e $y_0 = -c/2\Im(\alpha)$).

Per le circonferenze, è più facile impostare direttamente la condizione usando la variabile complessa: i punti Z che distano r da z_0 sono tutti e soli quelli per cui $|Z - z_0| = r$, cioè $|Z - z_0|^2 = r^2$, ovvero $(Z - z_0)(\overline{Z} - \overline{z}_0) = r^2$. Si ottiene una espressione del tipo $Z\overline{Z} - \alpha Z - \overline{\alpha}\overline{Z} + c = 0$ ove $\overline{\alpha} = z_0$ è il centro, e $\alpha\overline{\alpha} - c = r^2$ è il quadrato del raggio. Viceversa ogni tale espressione con $\alpha \in \mathbb{C}$ e $c \in \mathbb{R}$ rappresenta una circonferenza del piano (eventualmente con raggio immaginario...). L'espressione reale per le circonferenze si può ottenere ricordando che $Z = X + iY$, $\overline{Z} = X - iY$ e $Z\overline{Z} = X^2 + Y^2$, da cui si ottiene $X^2 + Y^2 - 2\Re(\alpha)X - 2\Im(\alpha)Y + c = 0$, formula usuale.

Si osservi la stretta parentela tra rette e cerchi, che è ben evidente nelle espressioni in variabile complessa: cosa descrive l'equazione $sZ\overline{Z} - \alpha Z - \overline{\alpha}\overline{Z} + c = 0$ con $s, c \in \mathbb{R}$ e $\alpha \in \mathbb{C}$?

7.9.2.2. Distanza, angoli. La distanza tra due punti del piano visti come numeri complessi $z_1 = x_1 + iy_1$ e $z_2 = x_2 + iy_2$ si calcola tramite

$$d(z_1, z_2) = |z_1 - z_2| = \sqrt{(z_1 - z_2)(\overline{z_1} - \overline{z_2})} = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

La distanza è una funzione $d : \mathbb{C} \times \mathbb{C} \to \mathbb{R}_{\geqslant 0}$ che soddisfa alle seguenti proprietà:

$(D1)$ annullamento: $d(z, z') = 0$ se e solo se $z = z'$;

$(D2)$ simmetria: $d(z, z') = d(z', z)$ per ogni coppia di punti z, z';

$(D3)$ disuguaglianza triangolare: $d(z, z') \leqslant d(z, w) + d(w, z')$ per ogni terna di punti z, w, z'.

Si osservi che le proprietà della distanza non usano la struttura algebrica, ed in effetti una funzione distanza può essere definita in un insieme qualsiasi. Se un campo ha una norma, allora possiamo definire una distanza usando la norma della differenza; invece una funzione distanza in generale non viene da una norma (per esempio si può vedere che le distanze definite da norme sono "invarianti per traslazione", cioè $d(z + w, z' + w) = d(z, z')$ per ogni terna z, z', w, proprietà che non viene chiesta alla funzione distanza).

Dati tre numeri complessi z_0, z_1, z_2, possiamo determinare l'angolo in z_0. Conviene supporre inizialmente $z_0 = 0$, e che $z_1 = \alpha$, $z_2 = \beta$ siano di modulo unitario. Allora l'angolo ϑ (tra α e β rispetto a 0) è tale che $\beta = \alpha e^{i\vartheta}$ (β si ottiene da α per una rotazione di angolo ϑ, che è la moltiplicazione per $e^{i\vartheta} = \cos\vartheta + i \sin\vartheta$). Quindi abbiamo $e^{i\vartheta} = \beta/\alpha = \overline{\alpha}\beta$, ovvero

$$\cos\vartheta = \Re(\overline{\alpha}\beta) = \Re(\alpha)\Re(\beta) + \Im(\alpha)\Im(\beta).$$

In generale, usando $\alpha = \frac{z_1 - z_0}{|z_1 - z_0|}$ e $\beta = \frac{z_2 - z_0}{|z_2 - z_0|}$ ne viene:

$$e^{i\vartheta} = \frac{\overline{z_1} - \overline{z_0}}{|z_1 - z_0|} \cdot \frac{z_2 - z_0}{|z_2 - z_0|} = \sqrt{\frac{\overline{z_1} - \overline{z_0}}{z_1 - z_0} \cdot \frac{z_2 - z_0}{\overline{z_2} - \overline{z_0}}}$$

ovvero

$$e^{2i\vartheta} = \frac{\overline{z_1} - \overline{z_0}}{z_1 - z_0} \cdot \frac{z_2 - z_0}{\overline{z_2} - \overline{z_0}}$$

oppure

$$\cos\vartheta = \frac{(x_1 - x_0)(x_2 - x_0) + (y_1 - y_0)(y_2 - y_0)}{\sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2}\sqrt{(x_2 - x_0)^2 + (y_2 - y_0)^2}}$$

Da notare che il calcolo delle funzioni trigonometriche viene fatto con operazioni algebriche a partire dai numeri complessi.

Facciamo anche notare che possiamo esprimere l'angolo come l'argomento del rapporto $\frac{z_2 - z_0}{z_1 - z_0}$ (verrà utile se parliamo di birapporti):

$$\vartheta = \arg\left(\frac{z_2 - z_0}{z_1 - z_0}\right)$$

(attenzione al segno?).

7.9.2.3. Teoremi di Carnot e Pitagora. Vediamo come alcuni teoremi classici si possono dimostrare usando i numeri complessi: dati tre punti (non allineati, ovvero un triangolo) che relazioni vi sono tra le lunghezze dei tre lati? Se i vertici sono z_1, z_2, z_3 , abbiamo la relazione $z_3 - z_2 = (z_3 - z_1) - (z_2 - z_1)$ e calcolando la norma al quadrato otteniamo

$$\begin{aligned} |z_3 - z_2|^2 &= |z_3 - z_1|^2 - 2\Re((\overline{z_3} - \overline{z_1})(z_2 - z_1)) + |z_2 - z_1|^2 \\ &= |z_3 - z_1|^2 + |z_2 - z_1|^2 - 2|z_3 - z_1||z_2 - z_1| \cos\vartheta_1 \end{aligned}$$

dove ϑ_1 è l'angolo nel vertice z_1 (formula di Carnot). In particolare, nel caso di un triangolo rettangolo in z_1, l'ultimo termine si annulla e abbiamo la formula di Pitagora (*in un triangolo rettangolo, il quadrato dell'ipotenusa è pari alla somma dei quadrati dei cateti*).

7.9.2.4. Condizione di allineamento per tre punti, retta per due punti. Tre punti z_0, z_1, z_2 sono allineati se l'angolo formato risulta 0 o π, ovvero sse il rapporto $\frac{z_1 - z_0}{z_2 - z_0}$ risulta reale, ovvero uguale al proprio coniugato:

$$(z_1 - z_0)(\overline{z_2} - \overline{z_0}) = (\overline{z_1} - \overline{z_0})(z_2 - z_0) \quad \text{ovvero} \quad \det\begin{pmatrix} z_1 - z_0 & \overline{z_1} - \overline{z_0} \\ z_2 - z_0 & \overline{z_2} - \overline{z_0} \end{pmatrix} = 0$$

che si può scrivere anche

$$\det\begin{pmatrix} z_0 & \overline{z_0} & 1 \\ z_1 & \overline{z_1} & 1 \\ z_2 & \overline{z_2} & 1 \end{pmatrix} = 0.$$

Quindi la retta per due punti z, w ha equazione data da

$$\det\begin{pmatrix} Z & \overline{Z} & 1 \\ z & \overline{z} & 1 \\ w & \overline{w} & 1 \end{pmatrix} = 0. \quad \text{ovvero} \quad (\overline{z}-\overline{w})Z - (z-w)\overline{Z} + (z\overline{w} - \overline{z}w) = 0$$

(notare che il termine noto è puramente immaginario).

In particolare, se i punti z, w sono sulla circonferenza unitaria abbiamo equazione $Z+zw\overline{Z} = z+w$.

Conviene, nel caso di due rette, calcolare anche il punto di intersezione, se esiste, e in particolare calcolare il punto di intersezione a partire da (in funzione di) due coppie di punti che definiscono le rette.

7.9.2.5. Condizione di ortogonalità, asse di un segmento. Tre punti z_0, z_1, z_2 sono tali da formare un angolo retto in z_0 sse il rapporto $\frac{z_1-z_0}{z_2-z_0}$ risulta puramente immaginario (la moltiplicazione per i dà una rotazione di un angolo retto) ovvero con somma nulla col proprio coniugato:

$$(z_1-z_0)(\overline{z_2}-\overline{z_0}) + (\overline{z_1}-\overline{z_0})(z_2-z_0) = 0.$$

Per calcolare l'asse di un segmento di vertici z, w, cioè la retta per il punto medio e ortogonale al segmento, possiamo impostare la condizione di uguale distanza da z e da w, $|Z-z| = |Z-w|$ e otteniamo

$$(\overline{w}-\overline{z})Z + (w-z)\overline{Z} + (z\overline{z} - w\overline{w}) = 0$$

oppure

$$\det\begin{pmatrix} Z-z & \overline{Z}-\overline{w} \\ Z-w & \overline{Z}-\overline{z} \end{pmatrix} = 0 \quad \text{ovvero} \quad \det\begin{pmatrix} Z & \overline{Z} & 1 \\ z & \overline{w} & 1 \\ w & \overline{z} & 1 \end{pmatrix} = 0.$$

Se poi z, w sono sulla circonferenza unitaria, equazione dell'asse diventa $Z = zw\overline{Z}$.

7.9.2.6. Problema: angoli costanti. Dati due punti z, w qual è il luogo dei punti Z tali che l'angolo visto da Z (a z, w)) sia costante?

7.9.2.7. Angoli al centro e alla circonferenza. Vogliamo mostrare, usando i numeri complessi, il classico risultato secondo cui dati due punti su una circonferenza l'angolo al centro è doppio dell'angolo alla circonferenza (che quindi non dipende dal terzo punto scelto sulla circonferenza).

Possiamo supporre che la circonferenza sia quella unitaria, che un punto sia z e l'altro $w = ze^{2i\vartheta}$ (angolo al centro 2ϑ) e calcolare l'angolo incognito ? dal vertice 1:

$$e^{2i?} = \frac{\overline{z}-1}{z-1}\,\frac{w-1}{\overline{w}-1} = \frac{w}{z} = e^{2i\vartheta}$$

dove abbiamo usato $\overline{z} = 1/z$. Concludiamo che $? = \vartheta$.

7.9.2.8. Teorema di Tolomeo-Eulero. Birapporti. Dati quattro punti $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ possiamo verificare con conti diretti l'uguaglianza

$$(\alpha-\beta)(\gamma-\delta) + (\alpha-\delta)(\beta-\gamma) = (\alpha-\gamma)(\beta-\delta)$$

e applicando la disuguaglianza triangolare otteniamo

$$|\alpha-\beta||\gamma-\delta| + |\alpha-\delta||\beta-\gamma| \geqslant |\alpha-\gamma||\beta-\delta|$$

dove vale l'uguaglianza sse

$$\frac{(\alpha-\beta)(\gamma-\delta)}{(\alpha-\delta)(\beta-\gamma)} \in \mathbb{R}_{>0}$$

ovvero sse

$$\frac{(\alpha-\beta)}{(\alpha-\delta)}\,\frac{(\gamma-\delta)}{(\gamma-\beta)} \in \mathbb{R}_{<0}$$

e questa condizione vale se e solo se

$$\arg\left(\frac{\alpha-\beta}{\alpha-\delta}\right) + \arg\left(\frac{\gamma-\delta}{\gamma-\beta}\right)$$

(ovvero gli angoli con vertici α e γ) vale π (a meno di multipli di 2π), e questo si verifica se e solo se i quattro punti stanno su una stessa retta o su una stessa circonferenza e α, γ separano β, δ.

Espresso in termini di quadrangoli: *le somme dei prodotti dei lati opposti è maggiore o uguale al prodotto delle diagonali, ed è uguale se e solo se i quattro vertici stanno su (una retta o) una circonferenza.*

Il termine (attenzione, non è quello di prima!)

$$(\alpha\,\beta\,\gamma\,\delta) = \frac{(\alpha-\gamma)}{(\alpha-\delta)} \Big/ \frac{(\beta-\gamma)}{(\beta-\delta)} = \frac{(\gamma-\alpha)}{(\gamma-\beta)} \Big/ \frac{(\delta-\alpha)}{(\delta-\beta)}$$

viene detto birapporto (dei quattro numeri nell'ordine dato) ed è reale sse i quattro punti stanno su una stessa retta o su una stessa circonferenza (si dice che sono cociclici), negativo se i primi due separano gli altri due.

7.9.2.9. Cerchio per tre punti. L'equazione della circonferenza passante per tre punti z_1, z_2, z_3 è quindi data dalla condizione $(z_1\, z_2\, z_3\, Z) \in \mathbb{R}$, ovvero dalla uguaglianza con il suo coniugato:

$$(z_3 - z_1)(\overline{z_3} - \overline{z_2})(\overline{Z} - \overline{z_1})(Z - z_2) = (\overline{z_3} - \overline{z_1})(z_3 - z_2)(Z - z_1)(\overline{Z} - \overline{z_2})$$

(sviluppare i conti?).

7.9.2.10. Problema dei quattro cerchi. Siano dati quattro circonferenze C_1, C_2, C_3, C_4 tali che le intersezioni nell'orine ciclico siano formate da due punti: $C_1 \cap C_2 = \{z_1, w_1\}$, $C_2 \cap C_3 = \{z_2, w_2\}$, $C_3 \cap C_4 = \{z_3, w_3\}$, $C_4 \cap C_1 = \{z_4, w_4\}$. Allora i quattro punti z_1, z_2, z_3, z_4 sono cocicici se e solo se lo sono i quattro punti w_1, w_2, w_3, w_4. Basta controllare la realtà dei birapporti.

7.9.2.11. Similitudine di triangoli. Due triangoli di vertici z_1, z_2, z_3 e w_1, w_2, w_3 sono simili se e solo se $w_i = z_0 + \varrho z_i e^{i\vartheta}$ per $i = 1, 2, 3$ (con ϱ, ϑ reali), ovvero

$$\frac{z_2 - z_1}{z_3 - z_1} = \frac{w_2 - w_1}{w_3 - w_1}$$

(questo garantisce la propozionalità di due lati e l'uguaglianza dell'angolo compreso) oppure

$$\det\begin{pmatrix} z_2 - z_1 & w_2 - w_1 \\ z_3 - z_1 & w_3 - w_1 \end{pmatrix} = 0, \quad \text{ovvero} \quad \det\begin{pmatrix} z_1 & w_1 & 1 \\ z_2 & w_2 & 1 \\ z_3 & w_3 & 1 \end{pmatrix} = 0.$$

7.9.2.12. Triangoli equilateri. In particolare un triangolo è equilatero sse è simile al triangolo di vertici $1, \omega, \overline{\omega} = \omega^2$ (dove $\omega = e^{2\pi i/3}$), quindi sse

$$\det\begin{pmatrix} z_1 & 1 & 1 \\ z_2 & \omega & 1 \\ z_3 & \omega^2 & 1 \end{pmatrix} = 0, \quad \text{ovvero} \quad z_1 + \omega z_2 + \omega^2 z_3 = 0.$$

7.9.2.13. Teorema di Napoleone. L'asserzione è la seguente: *dato un triangolo qualsiasi, su ciascuno dei lati si costruisce un triangolo equilatero (sempre esterno o sempre interno al triangolo dato); allora i baricentri di questi tre triangoli formano un triangolo equilatero. Vi sono quindi due triangoli equilateri detti di Napoleone, e i loro baricentri coincidono con quello del triangolo di partenza.*

Il problema essendo solo conforme, possiamo tramite traslazione e omotetia supporre che il triangolo abbia i vertici sul cerchio unitario, e chiamiamo A, B, C i tre vertici (pensati come numeri complessi unitari). Per costruire il triangolo equilatero esterno sul lato A, B cerchiamo il punto C'' tale che $C'' + \omega B + \omega^2 A = 0$ che dà $C'' = -\omega^2 A - \omega B$ e quindi baricentro

$$C' = \frac{A + B + C''}{3} = \frac{(1-\omega^2)A + (1-\omega)B}{3}.$$

Analogamente per il lato A, C cerchiamo B'' tale che $B'' + \omega A + \omega^2 C = 0$ e troviamo il baricentro

$$B' = \frac{A + B'' + C}{3} = \frac{(1-\omega)A + (1-\omega^2)C}{3}$$

e per il lato C, B cerchiamo A'' tale che $A'' + \omega C + \omega^2 B = 0$ e troviamo il baricentro

$$A' = \frac{A'' + B + C}{3} = \frac{(1-\omega^2)B + (1-\omega)C}{3}.$$

Calcolando $A' + \omega B' + \omega^2 C'$ esplicitamente vediamo che viene nullo, e si conclude che A', B', C' formano un triangolo equilatero.

Che cosa bisogna modificare per l'altro triangolo di Napoleone?

7.9.2.14. Teorema di Morley. L'asserzione è la seguente: *dato un triangolo qualsiasi, le trisettrici degli angoli interni si intersecano in coppie adiacenti in tre punti che formano un triangolo equilatero. Lo stesso capita per gli angoli esterni e per gli angoli complementari; questi tre triangoli equilateri sono detti i triangoli principali di Morley.*

Per la dimostrazione, conviene ridursi al caso di un triangolo sul cerchio unitario, con un vertice in $A = 1$, e $B = c^3$, $C = b^3$ come in figura:

Si vedono allora facilmente le trisettrici in B e C. Per trovare le trisettrici in A, detti $3\alpha, 3\beta, 3\gamma$ gli angoli al centro sottesi ai tre lati BC, AC, AB, abbiamo $3\alpha + 3\beta + 3\gamma = 2\pi$, e le trisettrici cercate hanno angoli al centro $3\gamma + \alpha = 2\gamma - \beta - 2\pi/3$ e $3\gamma + 2\alpha = \gamma - 2\beta - 4\pi/3$, e quindi corrispondono ai punti $bc^2\omega$ e $b^2c\omega^2$.

Per intersecare le trisettrici adiacenti conviene avere un metodo veloce per intersecare due rette ciascuna definita da punti sulla circonferenza unitaria: la retta per α, β è $Z + \alpha\beta\overline{Z} = \alpha + \beta$, quella per α', β' è $Z + \alpha'\beta'\overline{Z} = \alpha' + \beta'$, e facendo la differenza troviamo $(\alpha\beta - \alpha'\beta')\overline{Z} = \alpha + \beta - \alpha' - \beta'$, da cui si ricava *il coniugato del punto di intersezione*.

Con qualche conto troviamo allora i tre punti di intersezione C', B', A' e poi verifichiamo che $A' + \omega B' + \omega^2 C' = 0$ o meglio $\overline{A'} + \omega^2\overline{B'} + \omega\overline{C'} = 0$ (visto che calcoliamo più facilmente i coniugati).

Variazioni sul teorema di Morley: in effetti vi sono molti altri triangoli equilateri che si possono ottenere intersecando trisettrici interne, esterne e complementari, in totale 18 e che si ottengono applicando alcune trasformazioni (mandare b in ωb, oppure c in ωc e combinazioni dà 9 variazioni, e scambiando b e c se ne ottengono altre 9). Qui abbiamo cercato di disegnare tutti e 18 i triangoli, ma

vi sono molti vertici in comune: vi sono 18 trisettrici, e ciascuna passa per tre dei vertici dei triangoli equilateri, in totale vi sono 27 vertici, ciascuno usato da due delle trisettrici.

7.9.2.15. Punti notevoli dei triangoli. Fissato un triangolo A, B, C vi sono alcuni punti notevoli classici:

(1) il baricentro, intersezione delle mediane del triangolo (rette per un vertice e il punto medio del lato opposto), di solito viene indicato con G;

(2) l'ortocentro, intersezione delle altezze del triangolo (rette per un vertice e ortogonali al lato opposto), di solito indicato con H;

(3) il circocentro, intersezione degli assi dei lati del triangolo, di solito indicato con K;

(4) l'incentro, intersezione delle bisettrici degli angoli interni del triangolo, di solito indicato con L;

(5) tre exentri, intersezione delle bisettrici di angoli interni con le due bisettrici degli angoli esterni compresi, di solito indicati con A', B', C';

Per vederne le relazioni reciproche, possiamo supporre che i tre vertici siano sulla circonferenza unitaria, cioè il triangolo sia inscritto nella circonferenza unitaria. Allora:

(1) il baricentro è

$$G = \frac{A + B + C}{3}$$

(questo è vero sempre, senza nessuna supposizione);

(2) l'ortocentro è

$$H = A + B + C$$

(qui si usa la supposizione fatta);

(3) il circocentro è 0 (ovvio dalla supposizione!);

(4) in- ed excentri sono più complicati da determinare.

Vediamo il calcolo di H: l'asse del lato A, B ha equazione $Z = AB\overline{Z}$, e quindi l'altezza relativa a C ha equazione $Z - AB\overline{Z} = c$ dove c è tale che C soddisfa l'equazione, $c = C - AB\overline{C}$; quindi l'equazione diventa $CZ - ABC\overline{Z} + (AB - C^2) = 0$. Analogamente si trovano le altre altezze, e si vede che l'intersezione è $H = A + B + C$.

7.9.2.16. Retta di Eulero. Dai calcoli precedenti si vede subito che G, H, K (baricentro, ortocentro e circocentro) sono allineati, e la retta su cui stanno si dice retta di Eulero.

Mostriamo ora che l'incentro di solito non appartiene alla retta di Eulero, e più precisamente che L appartiene a tale retta se e solo se il triangolo è isoscele. Per fare questo conviene supporre (basta una rotazione) $A = 1$, $B = c^2$, $C = b^2$, cosicché le bisettrici sono le rette per $1, -bc$ (in A, per un ragionamento simile a quello fatto per Morley), per c^2, b (in B) e per c, b^2 (in C). Mettendo a sistema si trova $L = b + c - bc$. Ora l'appartenenza alla retta di Eulero, ovvero l'allineamento dei punti, si misura con

$$\det \begin{pmatrix} 0 & 0 & 1 \\ 1 + b^2 + c^2 & 1 + \overline{b}^2 + \overline{c}^2 & 1 \\ b + c - bc & \overline{b} + \overline{c} - \overline{bc} & 1 \end{pmatrix} = \frac{1}{b^2c^2}(bc - 1)(b + c^2)(b^2 + c)$$

(serve qualche conto), e si vede subito che l'annullamento del determinante corrisponde alla condizione di essere isoscele (se $bc = 1$ è isoscele in A).

7.9.2.17. È un problema più facile mostrare che: se due punti tra G, H, K, L coincidono, allora tutti e quattro coincidono e il triangolo è equilatero. Vale anche il viceversa?

7.9.2.18. Cerchio dei nove punti. Il punto medio tra circocentro ed ortocentro, cioè $(A + B + C)/2$ nelle nostre supposizioni, appartiene alla retta di Eulero ed è centro di una circonferenza di raggio $1/2$ (cioè, metà del raggio del circocentro), e che passa per i seguenti nove punti:

(1) i tre punti medi dei lati;

(2) i tre piedi delle altezze (quello rispetto ad A è $(A + B + C - BC/A)/2$);

(3) i tre punti medi tra vertici e ortocentro.

La verifica è immediata, basta calcolare le distanze.

7.9.2.19. È un risultato attribuito a Feuerbach il seguente: il cerchio dei nove punti è tangente all'incerchio e ai tre excerchi.

7.9.2.20. È attribuito a Coolidge invece la seguente sequenza infinita di osservazioni:

(1) dati tre punti z_1, z_2, z_3 unitari, diciamo cerchio del triangolo quello dei 9 punti (raggio $1/2$ e centro $(z_1 + z_2 + z_3)/2$);

(2) dati quattro punti z_1, z_2, z_3, z_4 unitari, abbiamo quattro cerchi per i triangoli che possono formare, e i loro centri stanno su una circonferenza di raggio $1/2$ e centro $(z_1 + z_2 + z_3 + z_4)/2$ (che diciamo cerchio del quadrangolo);

(3) dati cinque punti z_1, z_2, z_3, z_4, z_5 unitari, abbiamo cinque cerchi per i quadrangoli che possono formare, e i loro centri stanno su una circonferenza di raggio $1/2$ e centro $(z_1 + z_2 + z_3 + z_4 + z_5)/2$ (che diciamo cerchio del pentagono);

(4) dati sei punti $z_1, z_2, z_3, z_4, z_5, z_6$ unitari, abbiamo sei cerchi per i pentagoni che possono formare, e i loro centri stanno su una circonferenza di raggio $1/2$ e centro $(z_1 + z_2 + z_3 + z_4 + z_5 + z_6)/2$ (che diciamo cerchio dell'esagono);

e così via...

(disegnare degli excerchi è sempre ingombrante).

7.9.3. Trasformazioni di Mœbius del piano complesso. È di particolare interesse, e riemergerà varie volte durante il corso, la nozione di "trasformazione lineare fratta", o trasformazione di Mœbius, di $\mathbb{C}$. Si tratta funzioni di variabile complessa definite da

$$\varphi(Z) = \frac{c + dZ}{a + bZ}$$

con $a, b, c, d \in \mathbb{C}$ e $ad - bc \neq 0$. Si tratta di una funzione definita su $\mathbb{C}$ tranne che per $Z = -a/b$ (se $b \neq 0$), e a valori in tutto $\mathbb{C}$ tranne il punto d/b (sempre se $b \neq 0$). Tra tali sottinsiemi è invertibile, con inversa data da

$$\psi(Z) = \frac{c - aZ}{-d + bZ},$$

che è una funzione dello stesso tipo (a questo serve la condizione iniziale).
I più semplici esempi di trasformazioni di Mœbius sono:

le traslazioni ($\varphi(Z) = c + Z$),

le omotetie o dilatazioni ($\varphi(Z) = dZ$ con $d \neq 0$), che si possono vedere come composizione di moltiplicazione per un numero reale positivo (dilatazione) e per un numero complesso di norma 1 (rotazione),

le inversioni ($\varphi(Z) = 1/Z$).

Commutano tra loro?

7.9.3.1. Le trasformazioni di Mœbius formano un gruppo?

7.9.3.2. Trasformazioni affini del piano complesso. Si dicono trasformazioni affini le composizioni di traslazioni e dilatazioni, cioè le trasformazioni non fratte, del tipo $\varphi(Z) = c + dZ$. In effetti ogni trasformazioni di Mœbius si può scrivere come composizione di una inversione seguita e preceduta da trasformazioni affini: la generica $\varphi(Z) = \frac{c+dZ}{a+bZ}$ si ottiene applicando prima $\varphi_1(Z) = a + bZ$, poi $\varphi_2(Z) = 1/Z$, e infine $\varphi_3(Z) = \alpha + \beta Z$ per opportuni α, β, per calcolare i quali basta fare la composizione

$$\varphi_3(\varphi_2(\varphi_1(Z))) = \varphi_3(\varphi_2(a + bZ)) = \varphi_3(1/(a + bZ)) = \alpha + \frac{\beta}{a + bZ} = \frac{\alpha a + \beta + \alpha bZ}{a + bZ}$$

e imporre che sia uguale a $\varphi(Z)$, cioè $\alpha a + \beta = c$ e $\alpha b = d$, da cui si ricavano $\alpha = d/b$ e $\beta = (bd - ad)/b$ (naturalmente, se $b = 0$ non c'era bisogno di fare alcun conto, e di nuovo si vede la rilevanza del termine $ad - bc$).

7.9.3.3. Inversione. Siccome le trasformazioni affini sono piuttosto facili da capire (traslazioni, dilatazioni, rotazioni), per capire l'effetto delle trasformazioni di Mœbius si è ricondotti a studiare l'inversione $\iota(Z) = 1/Z$. Si tratta chiaramente di una biiezione di $\mathbb{C} \smallsetminus \{0\}$ in sè, autoinversa (cioè coincide con la sua propria inversa), che fissa il circolo unitario (ma non punto per punto: manda un numero di modulo 1 nel suo inverso, cioè nel suo coniugato), e scambia l'interno del circolo con l'esterno (e anzi scambia le circonferenze centrate in 0 di raggio r con quelle centrate in 0 e di raggio $1/r$).

La cosa più interessante è il comportamento sulle rette (e di conseguenza sui cerchi): *le rette passanti per l'origine vengono trasformate in rette passanti per l'origine, mentre le altre rette vengono trasformate in cerchi passanti per l'origine; viceversa le circonferenze passanti per l'origine vengono trasformate in rette, mentre le altre circonferenze vengono trasformate in circonferenze.*

Verificare queste affermazioni usando le espressioni prima evidenziate per rette e circonferenze: sostituendo ι nella espressione

$$sZ\overline{Z} - \alpha Z - \overline{\alpha}\overline{Z} + c = 0$$

(con $s, c \in \mathbb{R}$ e $\alpha \in \mathbb{C}$) troviamo

$$s - \alpha\overline{Z} - \overline{\alpha}Z + cZ\overline{Z} = 0,$$

che è dello stesso tipo (se $s = 0 \neq c$ si tratta di rette mandate in circonferenze passanti per l'origine, se $c = 0 \neq a$ viceversa; se invece $s = 0 = c$ si tratta delle rette per l'origine, se $s \neq 0 \neq c$ si tratta delle circonferenze non passanti per l'origine). Farsi qualche disegno può aiutare l'intuizione.

7.9.3.4. Proiezione stereografica (e uso del simbolo ∞ in $\mathbb{C}$). Siccome è estremamente antipatico che una trasformazione di Mœbius possa non essere definita su un punto (che vorremmo dire "va all'infinito" perché annulla un denominatore), e possa perdere un punto nell'immagine (che vorremmo dire "è l'immagine dell'infinito"), conviene "completare l'insieme $\mathbb{C}$" aggiungendo un nuovo punto indicato con il simbolo ∞, e vogliamo vedere:

(1) il significato geometrico di questo nuovo insieme $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$

(2) cosa resta della struttura algebrica di $\mathbb{C}$ passando a $\widehat{\mathbb{C}}$.

Per dare un significato geometrico alla costruzione, identifichiamo $\mathbb{C}$ con il piano $\mathbb{R}^2$ (coordinate ξ, η) immerso nello spazio $\mathbb{R}^3$ come insieme di punti con terza coordinata nulla: $\zeta = 0$, e consideriamo la sfera unitaria $\mathbb{S}^2$ centrata nell'origine di equazione $\xi^2 + \eta^2 + \zeta^2 = 1$. Chiamiamo polo nord il punto della sfera di coordinate $\xi = 0 = \eta$ e $\zeta = 1$.

Allora la proiezione stereografica dal polo nord è la funzione $\mathbb{S}^2 \smallsetminus \{N\} \longrightarrow \mathbb{C}$ che manda ogni punto della sfera nella intersezione con $\mathbb{C}$ della retta per N e il punto stesso; si tratta chiaramente di una biiezione con inversa costruita allo stesso modo, mandando ogni punto di $\mathbb{C}$ nella intersezione con la sfera della retta per N e il punto stesso. Questa biiezione di estende ad una biiezione tra tutta la sfera $\mathbb{S}^2$ e $\widehat{\mathbb{C}}$ mandando N in ∞, e da questo si vede il significato geometrico di ∞: i punti "vicini a N" sono quelli "lontani dall'origine in $\mathbb{C}$".

Formule e geometria della proiezione stereografica:

scrivendo $Z = X + iY$ per un punto di $\mathbb{C}$ e ξ, η, ζ per il punto corrispondente sulla sfera, con facili considerazioni su triangoli simili si vede subito che

$$\frac{X}{\xi} = \frac{Y}{\eta} = \frac{1}{1-\zeta}$$

da cui si ricavano subito le formule:

$$\left[\begin{array}{l} X = \dfrac{\xi}{1-\zeta} \\ Y = \dfrac{\eta}{1-\zeta} \\ |Z|^2 = \dfrac{1+\zeta}{1-\zeta} \end{array}\right. \quad \text{e} \quad \left[\begin{array}{l} \xi = \dfrac{2X}{1+|Z|^2} \\ \eta = \dfrac{2Y}{1+|Z|^2} \\ \zeta = \dfrac{|Z|^2-1}{1+|Z|^2} \end{array}\right.$$

Vediamo allora cosa succede ad una retta/circonferenza di $\mathbb{C}$: l'espressione $a(X^2+Y^2)+bX+cY+d = 0$ diventa $a(1+\zeta)+b\xi+c\eta+d(1-\zeta) = 0$, cioè l'equazione di un piano (essendo lineare nelle tre variabili) che interseca la sfera quindi in un cerchio. Inoltre si partiva da una retta ($a = 0$) se e solo se il cerchio immagine sulla sfera passa per il polo nord: questo ci dice che tutte le rette del piano "passano per il punto ∞" (vanno arbitrariamente lontane da 0).

Da un punto di vista algebrico potremmo dire che ∞ sia l'inverso di 0, cioè imporre una uguaglianza del tipo $0 \cdot \infty = 1$, oltre alle ovvie $z + \infty = \infty$ per ogni z. Tuttavia questo crea problemi alla struttura algebrica nel senso che il prodotto non risulta più nemmeno associativo: avremmo $z \cdot (0 \cdot \infty) = z \cdot 1 = z$ ma $(z \cdot 0) \cdot \infty = 0 \cdot \infty = 1$... Si parla di una "algebrizzazione parziale" del simbolo ∞, che useremo solo in certi contesti per "semplificare le espressioni" quando quel simbolo compare sia al numeratore che al denominatore: per esempio $\frac{\infty}{\infty} = 1$, ma $\frac{c+d\infty}{a+b\infty} = \frac{d}{b}$.

Tuttavia, il vantaggio di vedere le trasformazioni di Mœbius definite su tutto $\widehat{\mathbb{C}}$ (o, se si preferisce, vederle come trasformazioni della sfera in sè) è notevole: per esempio si può dire che si tratta di un gruppo. Naturalmente una trasformazione affine φ si estende con $\varphi(\infty) = \infty$, mentre una trasformazione generale si estende con $\varphi(\infty) = d/b$ e $\varphi(-a/b) = \infty$.

La principale proprietà della proiezione stereografica è di essere conforme, cioè di rispettare gli angoli tra rette nel piano e le loro proiezioni sulla sfera.

7.9.3.5. Definizione e transitività delle trasformazioni di Mœbius. Per capire le trasformazioni di Mœbius viene spontaneo chiedersi quante condizioni servono per identificare una unica trasformazione. Il risultato fondamentale è che una trasformazione è determinata dalla immagine di tre punti distinti (si può intuire dal fatto che ci sono quattro coefficienti, ma sono definiti a meno di moltiplicazione per una costante...): se cerchiamo una trasformazione di Mœbius che manda ordinatamente i punti distinti z_1, z_2, z_3 in w_1, w_2, w_3 (distinti, altrimenti non potrebbe essere una biiezione), serve certamente la condizione

$$\frac{Z - z_2}{Z - z_3} = k\frac{\varphi(Z) - w_2}{\varphi(Z) - w_3}$$

dove $k \in \mathbb{C}$ è da determinare in modo tale che $\varphi(z_1) = w_1$, cioè

$$\frac{z_1 - z_2}{z_1 - z_3} = k\frac{w_1 - w_2}{w_1 - w_3}.$$

Risolvendo per k e sostituendo, oppure facendo il rapporto per eliminare k, troviamo

$$\frac{Z-z_2}{Z-z_3}\Big/\frac{z_1-z_2}{z_1-z_3}=\frac{\varphi(Z)-w_2}{\varphi(Z)-w_3}\Big/\frac{w_1-w_2}{w_1-w_3}$$

da cui si può ricavare $\varphi(Z)$ in funzione di Z (e dei sei punti coinvolti). In ogni caso vediamo che per un ulteriore punto z_0 si ha $\varphi(z_0)=w_0$ se e solo se

$$\frac{z_0-z_2}{z_0-z_3}\Big/\frac{z_1-z_2}{z_1-z_3}=\frac{w_0-w_2}{w_0-w_3}\Big/\frac{w_1-w_2}{w_1-w_3}$$

e questa espressione si dice il birapporto dei quattro numeri z_0, z_1, z_2, z_3 nell'ordine dato e si scrive

$$(z_0\, z_1\, z_2\, z_3)=\frac{z_0-z_2}{z_0-z_3}\Big/\frac{z_1-z_2}{z_1-z_3}=\frac{z_2-z_0}{z_2-z_1}\Big/\frac{z_3-z_0}{z_3-z_1}=\frac{z_2-z_0}{z_2-z_1}\cdot\frac{z_3-z_1}{z_3-z_0}.$$

In conclusione abbiamo visto che: *una trasformazione di Mœbius è determinata dalla immagine di tre punti distinti, e conserva i birapporti di ogni quaterna di punti. Dalle formule si può anche dedurre il contrario: una biiezione di $\widehat{\mathbb{C}}$ in sè che conserva i birapporti è necessariamente una trasformazione di Mœbius (quindi i birapporti sono gli unici invarianti).*

Per esempio, l'unica trasformazione di Mœbius che manda a, b, c in $\infty, 0, 1$ è data da

$$\varphi(Z)=\frac{c-a}{c-b}\cdot\frac{Z-b}{Z-a}$$

e $(a\,b\,c\,Z)=\varphi(Z)$, cioè il birapporto è l'immagine del quarto punto per l'unica trasformazione che manda i primi tre ordinatamente in $\infty, 0, 1$.

7.9.3.6. Punti fissi delle trasformazioni di Mœbius. Un modo per capire come si comporta una mappa φ è di studiare i "punti fissi", cioè i punti Z tali che $\varphi(Z)=Z$. Nel caso delle trasformazioni di Mœbius si e' portati a risolvere una equazione di secondo grado:

$$Z=\frac{c+dZ}{a+bZ}\qquad\text{sse}\qquad bZ^2+(a-d)Z-c=0$$

da cui vediamo che:

(1) se $b=0$ possiamo avere una soluzione se $a-d=0$ (allora l'unico punto unito è ∞), oppure due soluzioni altrimenti (che sono ∞ e $c/(a-d)$;

(2) se $b\neq 0$ abbiamo una o due soluzioni a seconda che il discriminante $\Delta=(a-d)^2+4bc$ sia nullo o meno.

Quando ci sono due punti uniti, possiamo supporre che siano 0 e ∞, e allora si tratta di una dilatazione ($Z\mapsto dZ$), se c'è un solo punto unito possiamo supporre che sia ∞ e allora si tratta di una traslazione ($Z\mapsto Z+c$).

7.9.3.7. Invarianti: birapporti, angoli. Vogliamo vedere che le trasformazioni di Mœbius sono conformi, cioè rispettano gli angoli; ciò è ovvio per le trasformazioni affini, quindi basta mostrarlo per l'inversione. Possiamo sia fare un calcolo diretto, sia vedere che l'inversione nel piano complesso corrisponde tramite la proiezione stereografica ad una simmetria sulla sfera, che quindi conserva gli angoli.

Abbiamo visto che i birapporti sono invarianti per trasformazioni di Mœbius. Quindi per vedere che queste sono conformi, cioè rispettano gli angoli, basta vedere che gli angoli si esprimono in termini di birapporti. Questo può essere fatto in vari modi, il più semplice dei quali coinvolge il punto ∞: l'angolo in z_0 tra z_1 e z_2 è

$$\arg\left(\frac{z_2-z_0}{z_1-z_0}\right)=\arg\left(\frac{z_2-z_0}{z_1-z_0}\Big/\frac{z_2-\infty}{z_1-\infty}\right)=\arg(\infty\, z_0\, z_1\, z_2).$$

Questo però dimostra l'ivarianza degli angoli solo per trasformazioni che fissano ∞, cioè per trasformazioni affini. Come fare per la altre? Siccome a noi interessa principalmente calcolare l'angolo tra rette o circonferenze in un loro punto di intersezione, possiamo ragionare così: sia z_0 il punto di intersezione, z_1, z_2 punti sulle rette o circonferenze che consideriamo, z qualsiasi punto diverso dai precedenti tre; allora l'angolo viene calcolato dal limite del seguente birapporto:

$$(z\, z_0\, z_1\, z_2)=\frac{z_1-z}{z_1-z_0}\cdot\frac{z_2-z_0}{z_2-z}=\frac{z_1-z}{z_2-z}\cdot\frac{z_2-z_0}{z_1-z_0}$$

quando z_1 e z_2 tendono a z_0 lungo la retta o la circonferenza su cui stanno (l'angolo in z tende a 0, l'angolo in z_0 tende a quello cercato).

7.9.3.8. Transitività su rette e cerchi. Siccome sappiamo che una trasformazione di Mœbius è determinata unicamente dall'azione su tre punti (distinti), e che tale azione può essere decisa arbitrariamente (dando tre punti distinti come immagini), ne segue che ogni circonferenza (o retta) assegnata può essere trasformata (mediante una trasformazione di Mœbius) in una preassegnata circonferenza o retta.

Ma cosa si può dire di coppie di rette o di circonferenze? Per esempio, se due rette si intersecano con un certo angolo, essendo le trasformazioni conformi, possono essere mandate solo in coppie di rette (o circonferenze) che si intersecano con lo stesso angolo; basta questa condizione? Cosa si può dire di rette parallele?

Cosa si può dire di coppie di circonferenze?

7.9.3.9. Esempio: sequenze di circonferenze tangenti.

7.9.3.10. Inversioni rispetto a rette e cerchi. Vi sono alcune trasformazioni del piano a cui siamo abituati e che non rientrano "per poco" tra le trasformazioni di Mœbius.

Per esempio le simmetrie ortogonali rispetto ad una retta, diciamo per semplicità l'asse delle X (equazione complessa $Z - \overline{Z} = 0$), che semplicemente cambia di segno l'ordinata Y. Questa trasformazione è chiaramente il coniugio di $\mathbb{C}$. Per ottenere una formula che dia la simmetria rispetto ad una retta passante per il punto z_0 e con direzione il numero complesso unitario α possiamo ragionare così: spostiamo la retta sull'asse delle ascisse traslando di z_0 e dividendo per α, poi applichiamo il coniugio, poi usiamo la trasformazione inversa della prima. Siccome inversa di $\varphi(Z) = (Z - z_0)/\alpha$ è $\psi(Z) = z_0 + \alpha Z$, troviamo

$$\iota(Z) = \psi\big(\overline{\varphi(Z)}\big) = \psi\big(\overline{(Z - z_0)/\alpha}\big) = \psi\big(\alpha(\overline{Z} - \overline{z_0})\big) = z_0 + \alpha^2(\overline{Z} - \overline{z_0}),$$

e queste funzioni si dicono le inversioni rispetto a rette.

Invece si dicono inversioni rispetto a circonferenze le funzioni così definite: fissata una circonferenza di centro O e raggio r, per ogni punto P del piano l'immagine è il punto Q appartenente alla retta per O e P e tale che il prodotto delle distanze OP e OQ sia il quadrato del raggio. In termini più geometrici, se Q è esterno alla circonferenza, il punto P appartiene alla retta OQ e alla retta che congiunge i due punti di tangenza alla circonferenza di rette passanti per P; una facile considerazione su triangoli simili permette di riconoscere la condizione precedente, e anche di trovare la relazione nel caso della circonferenza centrata in 0 e di raggio r: $\varphi(Z) = r^2/\overline{Z}$, e quindi, con un ragionamento analogo a prima, per una circonferenza di centro z_0 e raggio r:

$$\iota(Z) = z_0 + \frac{r^2}{\overline{Z} - \overline{z_0}}$$

(basta infatti traslare z_0 in 0 tramite $Z \mapsto Z - z_0$, la cui inversa è $Z \mapsto Z + z_0$).

In entrambi i casi è stato sufficiente usare il coniugio, oltre a trasformazioni lineari fratte. In conclusione possiamo quindi ottenere un gruppo di trasformazioni più grande di quello delle trasformazioni di Mœbius, e che comprenda inversioni rispetto a rette e circonferenze, semplicemente aggiungendo il coniugio. Talvolta viene detto gruppo inversivo.

7.10. Quaternioni di Hamilton.

7.10.1. Quaternioni di Hamilton. I corpi finora visti erano tutti commutativi. Il primo esempio di corpo non commutativo è dato dai quaternioni di Hamilton, che andiamo ora ad illustrare. Vedremo in futuro che essi hanno un importante significato geometrico, poiché interpretano, tra l'altro, l'insieme delle rotazioni (attorno a rette) di uno spazio reale di dimensione tre.

7.10.2. Definizione (Quaternioni). *Consideriamo l'insieme $\mathbb{H}$ formato da tutte le espressioni del tipo $a + ib + jc + kd$ ove a, b, c, d sono numeri reali, e i, j, k sono tre simboli (in particolare non appartengono ad $\mathbb{R}$). Definiamo le seguenti operazioni:*

(S) somma: $(a + ib + jc + kd) + (a' + ib' + jc' + kd') = (a+a') + i(b+b') + j(c+c') + k(d+d')$;

(P) prodotto: pretendendo che il prodotto sia distributivo rispetto alla somma, associativo, e che tra numeri reali sia quello di $\mathbb{R}$, ci basta definire i prodotti tra i simboli i, j, k, cosa che facciamo nella seguente tabella:

$$\begin{array}{ccc} ii = -1 & ij = k & ik = -j \\ ji = -k & jj = -1 & jk = i \\ ki = j & kj = -i & kk = -1 \end{array} \qquad \begin{array}{ccc} i & \longrightarrow & j \\ & \nwarrow \quad \swarrow & \\ & k & \end{array}$$

(per memoria: i quadrati sono tutti -1, i prodotti di due elementi consecutivi nell'ordine ciclico i, j, k dà l'elemento successivo, i prodotti di due elementi consecutivi nell'ordine inverso dà l'opposto dell'elemento mancante).

Gli elementi di $\mathbb{H}$ si chiamano i quaternioni, e il corpo $\mathbb{H}$ si dice il corpo dei quaternioni di Hamilton. Invitiamo il lettore a controllare scrupolosamente che dotato delle operazioni sopra definite l'insieme $\mathbb{H}$ ha struttura di corpo (non commutativo) di elemento nullo $0 + 0i + 0j + 0k$, di elemento unità $1 + 0i + 0j + 0k$. L'associatività del prodotto, l'esistenza degli inversi per elementi non nulli, la distributività sono le proprietà fondamentali non banali da controllare.

7.10.3. Filosofia: Hamilton inventò, o scoperse, i quaternioni cercando operazioni di "moltiplicazione" e "divisione" tra vettori dello spazio tridimensionale (ma non esiste un'algebra reale di dimensione 3...); gli elementi i, j, k saranno interpretati come i generatori di tre direzioni ortogonali. La formulazione originale di Hamilton per definire il prodotto era la seguente:

$$i^2 = j^2 = k^2 = ijk = -1$$

ed è un interessante esercizio far vedere che da queste relazioni segue tutta la tabellina di moltiplicazione scritta sopra.

Si osservi anche che nei quaternioni vi sono almeno 3 soluzioni all'equazione polinomiale $X^2 + 1 = 0$, il che esclude che si tratti di un campo (al massimo ci sarebbero due soluzioni; in effetti nei quaternioni ve ne sono infinite: tutti i quaternioni unitari immaginari), e comunque contiene dei sottinsiemi con le stesse proprietà dei numeri complessi. Per ulteriori generalizzazioni (ad esempio gli ottonioni di Cayley) può essere interessante leggere (verso la fine del corso) il libro "Hypercomplex numbers" di Kantor-Solodovnikov.

7.10.4. Quaternioni reali ed immaginari. Diciamo quaternioni reali quelli dell'immagine della funzione $\mathbb{R} \to \mathbb{H}$ che manda x in $x + 0i + 0j + 0k$; si osservi che questa funzione rispetta le operazioni dei due corpi.

Diciamo invece immaginari i quaternioni che sono mandati a zero dalla funzione $\mathbb{H} \to \mathbb{R}$ che manda $a + ib + jc + kd$ in a (detta parte reale del quaternione); si osservi che questa funzione rispetta la somma, ma non il prodotto dei due corpi.

Ogni quaternione è dunque somma delle sue parti reale ed immaginaria.

7.10.5. Coniugato. Dato un quaternione $z = a + ib + jc + kd$, definiamo il suo coniugato $\overline{z} = a - ib - jc - kd = a + i(-b) + j(-c) + k(-d)$. Otteniamo così una applicazione di $\mathbb{H}$ in sè che soddisfa alle seguenti proprietà:

(C1) rispetta la somma: $\overline{z + z'} = \overline{z} + \overline{z'}$

(C2) $\overline{z} = z$ se e solo se z è (puramente) reale; $\overline{z} = -z$ se e solo se z è (puramente) immaginario;

(C3) (anti)rispetta il prodotto: $\overline{zz'} = \overline{z'}\,\overline{z}$

(C4) $z\overline{z} = \overline{z}z = a^2 + b^2 + c^2 + d^2$ è puramente reale per ogni $z = a + ib + jc + kd$, e si tratta di un numero positivo (se $z \neq 0$).

(C5) $\overline{\overline{z}} = z$ per ogni z (dunque di tratta di un isomorfismo involutorio).

7.10.6. Norma (o modulo) di quaternioni. Definiamo la norma di un quaternione come la radice quadrata (reale positiva) del prodotto $z\overline{z}$. Si tratta allora di una funzione di $\mathbb{H}$ in $\mathbb{R}$ dotata delle seguenti proprietà:

(N1) positività: $|z| \geqslant 0$ per ogni $z \in \mathbb{C}$ e $|z| = 0$ se e solo se $z = 0$;

(N2) moltiplicatività: $|zz'| = |z|\,|z'|$;

(N3) subadditività: $|z + z'| \leqslant |z| + |z'|$.

7.10.7. Inversi. Con le nozioni sopra introdotte, possiamo ora affermare che se z è quaternione non nullo, allora l'inverso di z è $z^{-1} = \frac{\overline{z}}{|z|^2}$.

7.10.8. Applicando l'identità $z\overline{z} = \overline{z}z$ a $z = u + v$, mostrare che per ogni coppia di quaternioni abbiamo $u\overline{v} + \overline{u}v = v\overline{u} + \overline{v}u$.

7.10.9. Identità dei quattro quadrati. Analogamente a quanto visto nel caso complesso, la proprietà moltiplicativa della norma per i quaternioni dà luogo ad una formula che riguarda le somme di quattro quadrati: *il prodotto di due somme di quattro quadrati è ancora una somma di quattro quadrati.* Precisamente:

$$(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) =$$
$$= (aa' - bb' - cc' - dd')^2 + (ab' + ba' + cd' - dc')^2 + (ac' + ca' - db' + bd')^2 + (ad' + da' + bc' - cb')^2 \ .$$

A titolo di informazione diciamo che identità simili valgono solamente per le somme di uno, due, quattro e otto quadrati.

7.10.10. Problema: fattorizzazione di quaternioni. Ogni quaternione (risp. quaternione unitario) q può essere scritto come prodotto di quaternioni (risp. quaternioni unitari) più semplici nei modi seguenti:

(1) $q = (a + ia')(b + jb')(c + kc')$ (sugg.: cercare $c + kc'$ tale che $q(c + kc')^{-1}$ sia un prodotto del tipo...);

(2) $q = (a + ia')(b + kb')(c + ic')$ (sugg.: simile a prima).

8. Polinomi.

I polinomi (almeno in una variabile) sono un oggetto di studio ben noto; daremo qui una definizione rigorosa, e metteremo in evidenza le tecniche più importanti legate a questa nozione.

8.1. Definizione (Polinomi). *Dato un anello A (di solito useremo un corpo), l'anello $A[X]$ dei polinomi in una variabile a coefficienti in A è il sottinsieme di $A^{\mathbb{N}}$ dato dalle funzioni quasi ovunque nulle (cioè che hanno valore 0 tranne che per un numero finito di indici) dotato delle seguenti operazioni:*

(S) $(a_i) + (b_i) = (c_i)$ *ove* $c_i = a_i + b_i$ *(somma coordinata per coordinata),*

(P) $(a_i) \cdot (b_i) = (p_i)$ *ove* $p_i = \sum_{j+k=i} a_j b_k$ *(prodotto alla kronecker),*

ove abbiamo indicato con $(a_i) = (a_0, a_1, \ldots, a_n, \ldots)$ *un polinomio generico (gli* a_i *sono quasi tutti nulli, e si dicono i coefficienti del polinomio). Si verifica allora che si tratta di un anello (commutativo se A è commutativo), con elemento nullo la funzione nulla, elemento unità la funzione che vale* 1 *(di A) in* 0 *e nulla altrove.*

8.1.1. Rappresentazione usuale. Detto e_i l'elemento di $A[X]$ che vale 1 in i e zero altrove, e scrivendo semplicemente a per l'elemento che vale $a \in A$ in posto 0 e zero altrove, allora ogni elemento di $A[X]$ si scrive come somma finita $(a_i) = \sum_{i\in\mathbb{N}} a_i e_i$ con $a_i \in A$ (finita significa che solo un numero finito degli a_i non è nullo). Ora, scrivendo X^i invece di e_i si ottiene la usuale rappresentazione dei polinomi in una indeterminata $\sum_{i\in\mathbb{N}} a_i X^i$, che giustifica la definizione del prodotto, poiché è obbligata dalle proprietà distributiva ed associativa.

8.1.2. Funzioni polinomiali. Poiché ogni polinomio può essere "valutato" in un qualsiasi elemento dell'anello dei coefficienti, esso determina una funzione $A \to A$, che viene detta funzione polinomiale. L'insieme $P(A)$ delle funzioni polinomiali di A in sè è definito come il sottinsieme di A^A dato dalle funzioni $f : A \to A$ per le quali esiste un polinomio P con $f(a) = P(a)$ per ogni $a \in A$. Si verifica subito che $P(A)$ è sottoanello di A^A (che si considera qui come anello con le operazioni di somma e prodotto "coordinata per coordinata", come per A^Z per ogni insieme Z; in particolare non usiamo, non ancora, la composizione di funzioni), e che abbiamo una funzione di anelli $A[X] \to P(A)$, che abbiamo sopra descritto; questa funzione in generale non è iniettiva.

Consideriamo infatti il caso $A = \mathbb{F}_p$ (corpo con p elementi). Allora $\mathbb{F}_p[X]$ è un insieme infinito, mentre le funzioni polinomiali (che sono un sottinsieme delle funzioni di $\mathbb{F}_p$ in sè) sono finite. Quali sono i polinomi che sono nulli come funzioni polinomiali? Quando due polinomi danno luogo alla stessa funzione polinomiale?

8.1.3. Principio di identità dei polinomi. Dalla definizione che abbiamo dato è chiaro che due polinomi sono uguali se e solo se per ogni indice i i coefficienti i-esimi coincidono (questo si dice di solito principio di identità dei polinomi, e spesso si enuncia anche dicendo che un polinomio è nullo se e solo se tutti i suoi coefficienti sono nulli).

Invece che due polinomi assumano gli stessi valori su ogni elemento dell'anello dei coefficienti garantisce solo che essi determinano la stessa funzione polinomiale, non che siano lo stesso polinimio; tuttavia nel caso di domini di cardinalità infinita vale anche che due polinomi che siano uguali come funzioni polinomiali coincidono in quanto polinomi.

8.1.4. Funzioni canoniche. Vi è un morfismo canonico di anelli $A \to A[X]$ che ad $a \in A$ associa il polinomio a di grado zero. Si tratta di un morfismo iniettivo, poiché ha un inverso sinistro dato dalla "valutazione in zero" $A[X] \to A$ che associa ad ogni polinomio $P(X)$ l'elemento $P(0) \in A$ (in effetti il termine noto).

8.1.5. Integrità. Si verifica facilmente che $A[X]$ è integro se A è integro. Infatti basta mostrare che $PQ \neq 0$ se $P \neq 0 \neq Q$; siano a_i il coefficiente direttore di P (coefficiente non nullo con massimo indice i di P), e b_j il coefficiente direttore di Q (coefficiente non nullo con massimo indice j di Q): allora il coefficiente di indice $i+j$ di PQ è $a_i b_j \neq 0$ e dunque $PQ \neq 0$.

D'ora in poi supporremo sempre A anello integro. In questo caso è chiaro che gli unici invertibili di $A[X]$ sono gli elementi invertibili di A.

8.2. Definizione (Grado). *Si definisce grado di un polinomio non nullo $P = (a_i)$, e si indica con $\deg(P)$, il massimo indice n tale che $a_n \neq 0$ (e tale a_n si dice coefficiente direttore di P; il polinomio si dice monico se il coefficiente direttore è 1). Per definizione poniamo $\deg(0) = -\infty$ La funzione $\deg : A[X] \to \mathbb{N} \cup \{-\infty\}$ gode delle seguenti proprietà:*

(G1) $\deg(P) = -\infty$ *se e solo se* $P = 0$; $\deg(P) = 0$ *se e solo se* $P \in A$;

(G2) $\deg(P+Q) \leqslant \max\{\deg(P), \deg(Q)\}$, *e vale l'uguaglianza se e solo se* $\deg(P) \neq \deg(Q)$ *oppure* $\deg(P) = \deg(Q)$ *e i coefficienti direttori non sono uno l'opposto dell'altro; dunque vale la disuguaglianza stretta se e solo se* $\deg(P) = \deg(Q)$ *e i coefficienti direttori sono uno l'opposto dell'altro;*

(G3) $\deg(PQ) \leqslant \deg(P) + \deg(Q)$ *(e vale l'uguaglianza se A è integro).*

8.3. Teorema (Divisione con resto). *Sia $\Bbbk$ un corpo e $\Bbbk[X]$ l'anello dei polinomi su $\Bbbk$. Per ogni coppia di polinomi $M(X)$ e $N(X) \neq 0$ esiste una unica coppia di polinomi $Q(X)$ e $R(X)$ (detti il quoziente ed il resto della divisione del dividendo $M(X)$ per il divisore $N(X)$) con $\deg R(X) < \deg N(X)$ se $R(X) \neq 0$ tale che $M(X) = Q(X)N(X) + R(X)$.*

Dimostrazione (algoritmo di divisione). Si procede per induzione sul grado di $M(X)$. Se $\deg M(X) < \deg N(X)$ allora $Q(X) = 0$ e $R(X) = N(X)$ danno il risultato. Se invece $\deg M(X) \geqslant \deg N(X)$, siano m, n i coefficienti direttori di $M(X)$ e $N(X)$ rispettivamente; allora il polinomio $M'(X) = M(X) - mn^{-1}X^{\deg M(X) - \deg N(X)}N(X)$ ha grado strettamente minore di quello di $M(X)$, e per ipotesi induttiva esistono $Q'(X)$ ed $R'(X)$ tali che $M'(X) = Q'(X)N(X) + R'(X)$ con $\deg R'(X) < \deg N(X)$ se $R'(X) \neq 0$. Allora basta porre $Q(X) = mn^{-1}X^{\deg M(X) - \deg N(X)}N(X) + Q'(X)$ ed $R(X) = R'(X)$ per ottenere il risultato voluto. □

Si osservi che il procedimento induttivo descritto è il ben noto algoritmo per il calcolo della divisione con resto tra polinomi.

8.3.1. Potremmo togliere l'ipotesi che i polinomi abbiano coefficienti in un corpo, imponendo che il secondo polinomio sia monico (o che il coefficiente dominante sia invertibile, che è l'unica richiesta per la dimostrazione).

8.3.2. Ideali principali. Dall'esistenza della divisione possiamo dedurre che gli ideali di un anello di polinomi su un corpo sono tutti principali; infatti basta considerare di un ideale I non nullo gli elementi di grado minimo: uno qualsiasi di essi genera l'ideale. Sia infatti $P(X)$ un tale elemento di grado minimo e $F(X)$ un polinomio dell'ideale; dalla divisione $F(X) = Q(X)P(X) + R(X)$ deduciamo che $R(X)$ appartiene all'ideale, e non potendo avere grado minore di quello di $P(X)$, dev'essere $R(X) = 0$, e dunque $F(X)$ un multiplo di $P(X)$.

8.3.3. Ruffini. Dal procedimento di divisione con resto di un polinomio $P(X)$ per un polinomio del tipo $X - c$ ci dice che $P(X)$ è divisibile per $X - c$ se e solo se il polinomio stesso si annulla in c, cioè $P(c) = 0$. Infatti $P(c)$ è il resto della divisione di $P(X)$ per $X - c$.

8.3.4. Di conseguenza il numero di zeri di un polinomio a coefficienti in un dominio non può superare il grado del polinomio stesso.

8.4. Definizione (MCD, mcm). *Dati due polinomi P e Q in $\Bbbk[X]$ definiamo massimo comun divisore* $\mathrm{MCD}(P,Q)$*, spesso denotato (P,Q) semplicemente, qualsiasi polinomio D che divide sia P che Q e tale che ogni divisore comune di P e Q divida anche D. Un massimo comun divisore è definito a meno di moltiplicazione per un elemento invertibile, dunque per un elemento non nullo di $\Bbbk$.*

Analogamente si definisce minimo comune multiplo, denotato $\mathrm{mcm}(P,Q)$*, come un minimo (per la divisibilità) dei multipli comuni di P e Q. Anche un minimo comune multiplo è definito a meno di moltiplicazione per un elemento invertibile.*

8.4.1. Generalizzazione a n polinomi. Definizioni analoghe di massimo comun divisore e minimo comune multiplo si possono dare per ogni insieme finito $P_1, P_2, \dots, P_n$ di polinomi.

8.5. Teorema (MCD). *Un massimo comun divisore D tra tra due polinomi P e Q è ogni generatore dell'ideale generato da P e Q (il più piccolo ideale contenente sia P che Q); esistono due polinomi H, K tali che $D = HP + KQ$, e D è un polinomio di grado minimo che si può scrivere in questa forma.*

Dimostrazione. Consideriamo l'insieme I dei polinomi della forma $MP + NQ$ al variare di $M, N \in \Bbbk[X]$. Si tratta chiaramente di un ideale di $\Bbbk[X]$, quindi si tratta dei multipli di un polinomio D che è di grado minimo in I. Poiché $P, Q \in I$, abbiamo che D divide sia P che Q, e dunque è un divisore comune. Inoltre per definizione esistono due polinomi H, K tali che $D = HP + KQ$. Sia ora D' un divisore comune di P e Q, diciamo $P = P'D'$ e $Q = Q'D'$; allora abbiamo $D = HP + KQ = D = HP'D' + KQ'D' = (HP' + KQ')D'$, da cui si vede che D' divide D. □

8.5.1. Dal teorema segue che due polinomi P e Q sono primi tra loro se e solo se esistono polinomi H, K tali che $HP + KQ = 1$.

8.5.2. Il teorema e l'osservazione precedente possono estendersi al caso di un numero finito di polinomi; un massimo comun divisore tra i polinomi $P_1, P_2, \dots, P_n$ è ogni polinomio di grado minimo che si scriva nella forma $H_1P_1 + H_2P_2 + \cdots + H_nP_n$ con gli H_i polinomi. Inoltre essi sono coprimi (cioè il loro massimo comun divisore è 1) se e solo se esistono dei polinomi H_i tali che $H_1P_1 + H_2P_2 + \cdots + H_nP_n = 1$.

8.6. Algoritmo di Euclide. Anche per i polinomi possiamo dare un procedimento di calcolo del MCD analogamente a quanto fatto per gli interi, basandoci su un procedimento di divisioni iterate. Si riscriva per bene l'algoritmo, verificando che tutto funzioni.

8.7. Teorema (Irriducibili, fattorizzazione). *Un polinomio di grado positivo (non nullo) si dice irriducibile se non si può scrivere come prodotto di due polinomi di gradi strettamente positivi. Ogni polinomio di grado positivo si scrive in modo essenzialmente unico come prodotto di irriducibili (essenzialmente significa a meno dell'ordine dei fattori e di moltiplicazione dei fattori per invertibili).*

Dimostrazione. Si può fare usando la seconda forma dell'induzione; infatti la proprietà è ovvia per i polinomi di grado 1, che sono tutti irridicibili. Se ora F è un polinomio di grado maggiore di 1 e non irriducibile, esso si esprime come prodotto GH di due polinomi di gradi positivi, ciascuno minore a quello di F; dunque per ipotesi induttiva essi ammettono una fattorizzazione come nell'enunciato, e di conseguenza anche F (facendo il prodotto delle fattorizzazioni).

Per dimostrare l'unicità della fattorizzazione basta applicare a due distinte fattorizzazioni di uno stesso polinomio il seguente risultato: *se P è un polinomio irriducibile, e P divide un prodotto FG, allora P divide almeno uno dei due fattori; quindi per induzione: se P divide un prodotto di polinomi, allora P divide almeno uno dei fattori.*

Supponiamo infatti che P non divida F, e proviamo che divide G; siccome F e P sono comprimi abbiamo $1 = FH + PK$ per opportuni polinomi H, K. Moltiplicando per G otteniamo $G = FGH + PGK$, e poiché $FG = PL$ (per ipotesi P divide FG) risulta $G = PLH + PGK = P(LH + GK)$, e dunque P divide G, come si voleva. □

♠ **8.8.** Corpo delle funzioni razionali. Per ogni corpo $\Bbbk$, indichiamo con $\Bbbk(X)$ e chiamiamo corpo delle funzioni razionali (in X a coefficienti in $\Bbbk$) il corpo delle frazioni dell'anello integro $\Bbbk[X]$.

Gli elementi di $\Bbbk(X)$ sono allora quozienti $\frac{P(X)}{Q(X)}$ con $Q(X) \neq 0$, soggetti alle usuali operazioni di somma e prodotto.

♠♠ **8.9.** Analogia polinomi (su un corpo)-interi: domini euclidei, principali, fattoriali. Il lettore avrà notato una certa aria di ripetizione studiando interi e polinomi. Questo è dovuto (oltre al copia-incolla-modifica fatto in TEX dall'estensore di queste note) ad una analogia assai profonda tra i due casi, che cerchiamo di illustrare qui di seguito.

8.9.1. Definizione (domini euclidei). *Un dominio integro A si dice euclideo se esiste una funzione $\delta : A \smallsetminus \{0\} \to \mathbb{N}$ detta grado dotata delle seguenti proprietà:*

($E1$) *$\delta(a) \leqslant \delta(ab)$ per ogni $a, b \in A$;*

($E2$) *per ogni $a, b \in A$ esistono q e r tali che $a = bq + r$ e $\delta(r) < \delta(b)$ se $r \neq 0$ (algoritmo di divisione euclidea: q si dice quoziente e r resto).*

8.9.2. Osserviamo subito che per ogni $a \in A$ abbiamo $\delta(1) \leqslant \delta(a)$ (segue da ($E1$)); dunque $\delta(1) \in \mathbb{N}$ è il minimo valore assunto da δ, e (eventualmente sottraendolo alla funzione stessa) possiamo supporre che sia $\delta(1) = 0$.

8.9.3. È quasi immediato osservare che un elemento $a \in A$ è invertibile se e solo se $\delta(a) = \delta(1)$. Infatti se a è invertibile abbiamo $\delta(a) \leqslant \delta(aa^{-1}) = \delta(1)$ (l'altra disuguaglianza vale per ogni a, come s'è già detto); viceversa, nella divisione $1 = aq + r$ non può essere $\delta(r) < \delta(a)$ se $\delta(a) = \delta(1)$, e dunque $r = 0$, e allora a è invertibile con inverso q.

8.9.4. Possiamo fare una osservazione più sottile: un elemento $a \in A$ è invertibile se e solo se esiste $b \in A$ tale che $\delta(b) = \delta(ab)$ (e allora ciò vale per ogni $b \in A$, non nullo). Infatti se a è invertibile abbiamo $\delta(b) \leqslant \delta(ab) \leqslant \delta(a^{-1}ab) = \delta(b)$; viceversa, nella divisione $b = (ab)q + r$ non può essere $\delta(r) < \delta(ab) = \delta(b)$ poiché avremmo anche $\delta(b) \leqslant \delta(b(1 - aq) = \delta(r)$, e dunque $r = 0$, e allora da $b = abq$ deduciamo che a è invertibile con inverso q.

8.9.5. L'osservazione precedente si può anche scrivere nella forma: un elemento $a \in A$ non è invertibile se e solo se per ogni $b \in A$ si ha $\delta(b) < \delta(ab)$.

8.9.6. Definizione (domini principali). *Un dominio integro A si dice principale se ogni suo ideale è principale, cioè generato da un elemento.*

8.9.7. Teorema. *I domini euclidei sono principali.*

Dimostrazione. Sia I un ideale non banale, e sia a un suo elemento tale che $\delta(a)$ sia minimo tra i valori della funzione grado sugli elementi di I (essendo $\mathbb{N}$ ben ordinato, $\delta(I)$ ha minimo). Mostriamo che I è l'ideale generato da a. Siccome $a \in I$, basta mostrare che ogni elemento $b \in I$ è multiplo di a. Consideriamo la divisione con resto $b = qa + r$; poiché $a, b \in I$ (e dunque $qa \in I$) abbiamo $r \in I$, e poiché $\delta(r) < \delta(a)$ dev'essere $r = 0$. Dunque $b = qa$ è multiplo di a. □

8.9.8. I domini principali hanno la proprietà che ogni catena crescente di ideali propri diventa stazionaria, cioè ad un certo punto diventa costante: basta infatti considerare un generatore dell'ideale dato dalla unione degli ideali della catena; poiché esso appartiene all'unione, deve appartenere ad uno degli ideali, e a quel punto la catena diventa stazionaria.

8.9.9. Definizione (domini fattoriali). *Un dominio integro A si dice fattoriale se ogni suo elemento non nullo si può scrivere in modo essenzialmente unico come prodotto di elementi irriducibili; cioè se ogni elemento a si scrive come prodotto $\prod_{i=1}^{m} p_i$ di elementi irriducibili, e se $\prod_{j=1}^{n} q_j$ è un'altra tale scrittura, allora $n = m$ e a meno di riordinare gli indici abbiamo che $p_i = u_i q_i$ con $u_i \in A$ invertibili (cioè p_i e q_i sono associati).*

8.9.10. Teorema. *I domini principali sono fattoriali.*

Dimostrazione. Osserviamo che dati due elementi a e b di un dominio A, risulta che a divide b se e solo se l'ideale generato da a contiene l'ideale generato da b. Inoltre l'ideale generato da un elemento è massimale se e solo se l'elemento stesso è irriducibile.

Consideriamo allora un elemento a e l'ideale da esso generato; esiste un ideale massimale che lo contiene, e dunque un elemento irriducibile p_1 tale che $a = p_1 a_1$; ripetiamo il procedimento per a_1 ottenendo $a_1 = p_2 a_2$ con p_2 irriducibile, e così via. Gli elementi $a, a_1, a_2, \ldots$ generano degli ideali che sono via via più grandi. Poiché abbiamo visto che per i domini principali le catene di ideali propri

sono stazionarie, ad un certo punto troviamo un ideale massimale, e quindi una decomposizione di a in un prodotto di irriducibili. □

8.9.11. Nessuna delle implicazioni opposte è vera: esistono domini fattoriali ma non principali (ad esempio i domini di polinomi in più variabili su un dominio fattoriale), ed esistono domini principali ma non euclidei (un esempio è l'anello $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, ma non è facile discuterlo, vedi ???).

8.9.12. I numeri interi (con la funzione del valore assoluto), i polinomi in una variabile a coefficienti in un corpo (con la funzione del grado), gli interi di Gauss (con la funzione data dalla norma come numeri complessi) sono domini euclidei, e dunque principali e fattoriali.

♠♠ **8.10.** Vi sono importanti risultati che riguardano i polinomi a coefficienti in un dominio fattoriale.

8.10.1. Consideriamo il corpo dei quozienti $\Bbbk$ di A e vogliamo confrontare la fattorizzazione di polinomi in $A[X]$ e in $\Bbbk[X]$. Ricordiamo che un polinomio in $A[X]$ si dice primitivo se l'insieme dei suoi coefficienti ha 1 come massimo comun divisore.

8.10.2. Lemma (di Gauss). *Sia A un dominio fattoriale.*

(*a*) *il prodotto di due polinomi primitivi è primitivo;*

(*b*) *siano $P(X)$ e $F(X)$ polinomi in $A[X]$, e supponiamo $F(X)$ primitivo; se $P(X) = F(X)G(X)$ in $\Bbbk[X]$ allora anche $G(X) \in A[X]$;*

(*c*) *se $P(X)$ è polinomio irriducibile in $A[X]$ allora è irriducibile anche in $\Bbbk[X]$; equivalentemente se un polinomio in $A[X]$ si fattorizza come prodotto di polinomi di grado positivo in $\Bbbk[X]$, allora si fattorizza anche in $A[X]$.*

Dimostrazione. Vedi I. Barsotti, "Appunti di Algebra", lez. 60. □

8.10.3. Polinomi a coefficienti interi. In particolare per polinomi in $\mathbb{Z}[X]$, abbiamo che se $a \in \mathbb{Z}$ è uno zero del polinomio (cioè $X - a$ divide il polinomio) allora a divide il temine noto del polinomio. Se $q \in \mathbb{Q}$ è uno zero del polinomio (cioè $X - q$ divide il polinomio) allora espresso $q = a/b$ con $a, b \in \mathbb{Z}$ coprimi, abbiamo che $bX - a$ divide il polinomio stesso, e inoltre a divide il temine noto del polinomio e b divide il termine dominante

8.10.4. Criterio di Eisenstein. Sia $F(X) = \sum_{i=1}^{n} a_i X^i$ un polinomio a coefficienti interi; se un numero primo p divide tutti i coefficienti tranne a_n, ma p^2 non divide a_0 allora $F(X)$ è irriducibile.

8.10.5. Fattorizzazione di $X^p \pm 1$ con p primo. È ben noto che

$$X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1) \qquad \text{e} \qquad X^p + 1 = (X+1)(X^{p-1} - X^{p-2} + \cdots - X + 1)$$

e tramite il criterio di Eisenstein possiamo concludere che i fattori nelle parentesi a destra sono irriducibili: per il primo conviene osservare che un polinomio $P(X)$ è irriducibile se e solo se per qualche (e allora per ogni) elemento a dell'anello si ha che $P(X - a)$ è irriducibile (nel caso specifico conviene sostituire X con $X + 1$). Il secondo caso si può trattare similmente, oppure osservando che un polinomio $P(X)$ è irriducibile se e solo se il polinomio $P(-X)$ lo è.

8.10.6. Teorema. *Se A è un dominio fattoriale, anche $A[X]$ è dominio fattoriale.*

Dimostrazione. Vedi I. Barsotti, "Appunti di Algebra", lez. 61. □

8.10.7. Per induzione sul numero di variabili, potremmo allora dimostrare che ogni anello di polinomi con un numero finito di variabili su un anello fattoriale è esso stesso un anello fattoriale. Con un facile argomento di riduzione al caso finito potremmo allora vedere che qualunque anello di polinomi con un insieme arbitrario di variabili su un dominio fattoriale è fattoriale (uso il condizionale perché non abbiamo veramente definito questi anelli, se non nel caso di una variabile, ma il lettore può pensarci da solo).

8.11. Ricerca delle radici dei polinomi. È un ben noto problema quello di "cercare le radici di un polinomio". Si tratta per un polinomio $F(X) \in A[X]$ di trovare i valori $a \in A$ tali che $F(a) = 0$, ovvero tali che $X - a$ divide $F(X)$. Nel caso di polinomi a coefficienti reali o complessi questo problema è stato risolto per i polinomi di grado minore o uguale a quattro da alcuni matematici italiani (Del Ferro, Tartaglia, Cardano, Ferrari) del sedicesimo secolo, mostrando l'esistenza di formule o procedimenti che tramite operazioni algebriche ed estrazioni di radici producono i valori cercati. Nel diciannovesimo secolo, il matematico francese Galois mostrò che non possono esistere formule risolutive per radicali per le equazioni generali di grado superiore al quarto; questo fondamentale risultato e i

metodi per dimostrarlo sono oggetto di un corso avanzato (Teoria di Galois). Questi risultati erano già in parte noti a Ruffini e Abel.

Ricorderemo qui le soluzioni classiche, e penseremo a polinomi a coefficienti nei corpi reale o complesso; si può generalizzare quello che diremo a corpi la cui caratteristica sia maggiore del grado del polinomio di cui si cercano le radici.

8.11.1. Polinomi di primo grado. Un generico polinomio di primo grado è $aX+b$ con $a \neq 0$. In tal caso l'unica radice del polinomio è $x = -\frac{b}{a}$.

8.11.2. Polinomi di secondo grado. Un generico polinomio di secondo grado è aX^2+bX+c con $a \neq 0$. Un ben noto procedimento di "completamento del quadrato" porta alle formule risolutive già studiate; l'idea è di riscrivere il polinomio in una forma tale che la parte contente l'incognita X sia un quadrato perfetto:

$$4a(aX^2+bX+c) = 4a^2X^2+4abX+4ac = 4a^2X^2+4abX+b^2-b^2+4ac = (2aX+b)^2-b^2+4ac$$

da cui si deduce che le radici del polinomio si ottengono quando $2aX+b = \pm\sqrt{b^2-4ac}$, e sono

$$x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a} \ ,$$

come ben noto. La quantità $\Delta = b^2-4ac$ si dice discriminante del polinomio di secondo grado; nel caso in cui questi abbia coefficienti reali, il discriminante permette di capire la configurazione delle radici: vi sono due radici reali, una sola radice (necessariamente reale, detta "radice doppia") o due radici complesse (necessariamente una coniugata dell'altra) a seconda che il suo discriminante sia positivo, nullo o negativo.

Un metodo alternativo di procedere consiste nella "sostituzione di variabile" $X = Y - \frac{b}{2a}$ che permette di eliminare il termine di primo grado:

$$a\Big(Y-\frac{b}{2a}\Big)^2 + b\Big(Y-\frac{b}{2a}\Big) + c = a\Big(Y^2 - \frac{b^2}{4a^2} + \frac{c}{a}\Big)$$

che evidenzia le radici $y_{1,2} = \pm\sqrt{\frac{b^2}{4a^2}-\frac{c}{a}} = \pm\frac{\sqrt{b^2-4ac}}{2a}$ e da cui si arriva subito alle formule usuali.

Ricordiamo infine le ben note relazioni tra radici x_1, x_2 e coefficienti a, b, c, che si ricavano subito dalla fattorizzazione $aX^2+bX+c = a(X-x_1)(X-x_2)$:

$$x_1+x_2 = -\frac{b}{a} \qquad \text{e} \qquad x_1x_2 = \frac{c}{a} \ .$$

8.11.3. Polinomi di terzo grado. Un generico polinomio di terzo grado è aX^3+bX^2+cX+d con $a \neq 0$. Usando la "sostituzione di variabile" $X = Y - \frac{b}{3a}$ che permette di eliminare il termine di secondo grado abbiamo:

$$a\Big(Y-\frac{b}{3a}\Big)^3 + b\Big(Y-\frac{b}{3a}\Big)^2 + c\Big(Y-\frac{b}{3a}\Big) + d = a\Big(Y^3 + \frac{3ac-b^2}{3a^2}Y + \frac{27a^2d-9abc+2b^3}{27a^3}\Big)$$

e siamo ridotti a cercare le radici di un polinomio del tipo Y^3+pY+q. Il modo più veloce di procedere ora consiste nella misteriosa sostituzione di Vièta $Y = W - \dfrac{p}{3W}$ che dà

$$\Big(W-\frac{p}{3W}\Big)^3 + p\Big(W-\frac{p}{3W}\Big) + q = W^3 - \frac{p^3}{27W^3} + q$$

che ponendo $T = W^3$ e moltiplicando per T ci riporta ad un polinomio di secondo grado $T^2+qT-\frac{p^3}{27}$. Dalle formule risolutive otteniamo che

$$t_{1,2} = \frac{-q \pm \sqrt{q^2+4\frac{p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4}+\frac{p^3}{27}} \ .$$

Estraendo le radici cubiche di t_1 e t_2, potremo trovare sei valori per Y, ma ciascuno ripetuto due volte; dunque possiamo trovare i tre valori cercati per X.

Per arrivare alle classiche formule di Cardano, osserviamo che se w è una radice cubica di t_1, allora $w' = -\frac{p}{3w}$ è radice cubica di t_2; infatti

$$-\frac{p^3}{27w^3} = -\frac{p^3}{27}\frac{1}{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} = -\frac{p^3}{27}\frac{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}{\frac{q^2}{4}-(\frac{q^2}{4}+\frac{p^3}{27})} = t_2 \ .$$

Allora possiamo scrivere le radici come

$$y_{1,2,3} = w_{1,2,3} + w'_{1,2,3}$$

dove w_i sono le radici cubiche di t_1, e w'_i è la corrispondente radice cubica di t_2 tale che $w_i w'_i = -\frac{p}{3}$ (perché?).

Il termine $\Delta = \frac{q^2}{4} + \frac{p^3}{27} = (\frac{q}{2})^2 + (\frac{p}{3})^3$ è detto discriminante della equazione di terzo grado (qualcuno chiama discriminante il termine $D = -108\Delta = -4p^3 - 27q^2$); nel caso che l'equazione abbia coefficienti reali esso permette di distinguere diverse configurazioni delle radici. Se Δ è negativo, allora vi sono tre radici reali distinte; se Δ è positivo allora vi è una radice reale e due radici complesse coniugate; se Δ è zero vi sono radici multiple (un'unica radice se $p = q = 0$ oppure due altrimenti). Non vi sono errori di stampa nelle righe precedenti: il caso di tre radici reali di trova con $\Delta < 0$, e conviene fare qualche disegno con le radici cubiche complesse per capire le asserzioni fatte; in effetti per calcolare le radici reali bisogna fare calcoli con i numeri complessi.

Terminiamo con le relazioni tra radici x_1, x_2, x_3 e coefficienti a, b, c, d, che si ricavano subito dalla fattorizzazione $aX^3 + bX^2 + cX + d = a(X - x_1)(X - x_2)(X - x_3)$:

$$x_1 + x_2 + x_3 = -\frac{b}{a} \quad , \qquad x_1x_2 + x_1x_3 + x_2x_3 = \frac{c}{a} \qquad \text{e} \qquad x_1x_2x_3 = -\frac{d}{a} \ .$$

Può essere di qualche interesse ricordare come Tartaglia comunicò a Cardano il procedimento per trovare una radice reale di una equazione di terzo grado: non avendo una simbologia algebrica moderna, utilizza dei versi (con intento mnemonico) e una terminologia "geometrica":

Quando che 'l cubo con le cose appresso	Se (vuoi risolvere) $x^3 + px =$
Se agguaglia a qualche numero discreto:	$= q$
Trovami dui altri, differenti in esso;	trova u, v tali che $u - v = q$
Dapoi terrai, questo per consueto,	e
Che 'l loro produtto, sempre sia eguale	$uv =$
Al terzo cubo delle cose netto;	$= (p/3)^3$.
El residuo poi suo generale,	Allora
Delli lor lati cubi, ben sottratti	$\sqrt[3]{u} - \sqrt[3]{v} =$
Varrà la tua cosa principale.	$= x$.

(a fianco abbiamo "tradotto" in termini più moderni; quali soluzioni trova veramente Tartaglia?). I versi di Tartaglia continuavano poi per trattare altri casi (all'epoca pare che i coefficienti potessero essere solo positivi, per evitare eresie):

In el secondo, de cotesti atti;
Quando che 'l cubo, restasse lui solo,
Tu osserverai quest'altri contratti,
Del numer farai due tal part' a volo,
Che l' una, in l' altra, si produca schietto,
El terzo cubo delle cose in stolo;
Delle quali poi, per commun precetto,
Terrai li lati cubi, insieme gionti,
El cotal somma, sarà il tuo concetto;
El terzo, poi de questi nostri conti,
Se solve col secondo, se ben guardi
Che per natura son quasi congionti,
Questi trovai, et non con passi tardi
Nel mille cinquecent' e quattro e trenta;
Con fondamenti ben saldi, e gagliardi;
Nella Città del mar 'intorno centa.

(lasciamo al lettore il compito di tradurre, nel caso fosse interessato).

8.11.4. Polinomi di quarto grado. Un generico polinomio di quarto grado è $aX^4 + bX^3 + cX^2 + dX + e$ con $a \neq 0$. Usando la solita "sostituzione di variabile" $X = Y - \frac{b}{4a}$ che permette di

eliminare il termine di terzo grado abbiamo:

$$a\Big(Y-\frac{b}{4a}\Big)^4+b\Big(Y-\frac{b}{4a}\Big)^3+c\Big(Y-\frac{b}{4a}\Big)^2+d\Big(Y-\frac{b}{4a}\Big)+e=$$
$$=a\Big(Y^4+\frac{4ac-3b^2}{4a^2}Y+\frac{16a^2d-8abc+2b^3}{16a^3}Y+\frac{256a^3e-64a^2bd+16ab^2c-3b^4}{256a^4}\Big)$$

e siamo ridotti a cercare le radici di un polinomio del tipo Y^4+pY^2+qY+r. Il metodo di Ferrari consiste ora nell'introdurre un termine U in modo tale che il polinomio si scriva come differenza di due quadrati, e di conseguenza si fattorizzi in polinomi di grado minore di cui si sanno trovare le radici; abbiamo, completando il quadrato contenente Y^4 e pY^2 che

$$Y^4+pY^2+qY+r=\Big(Y^2+\frac{p}{2}-\frac{U}{2}\Big)^2-\Big(UY^2-qY+\frac{U^2}{4}+\frac{pU}{2}+\frac{p^2}{4}-r\Big)$$

e l'espressione nella seconda parentesi è un quadrato perfetto se il discriminante (come polinomio di secondo grado in Y) si annulla; quindi basta che u sia una radice del polinomio

$$q^2-4U\Big(\frac{U^2}{4}+\frac{pU}{4}+\frac{p^2}{4}-r\Big)=-U^3-pU^2-(p^2-4r)U+q^2$$

che è di terzo grado in U e che perciò sappiamo trattare con il metodo di Cardano. Se ora u è una radice, il polinomio nelle Y si scrive

$$Y^4+pY^2+qY+r=\Big(Y^2+\frac{p}{2}-\frac{u}{2}\Big)^2-u\Big(Y-\frac{q}{2u}\Big)^2=\Big(Y^2+vY+\frac{p}{2}-\frac{u}{2}-\frac{q}{2v}\Big)\Big(Y^2-vY+\frac{p}{2}-\frac{u}{2}+\frac{q}{2v}\Big)$$

se v è una radice quadrata di u. Siamo quindi ridotti a due polinomi di secondo grado nella Y, e le quattro radici che otteniamo sono le radici volute del polinomio di quarto grado.

Terminiamo con le relazioni tra radici x_1, x_2, x_3, x_4 e coefficienti a,b,c,d,e, che si ricavano subito dalla fattorizzazione $aX^4+bX^3+cX^2+dX+e=a(X-x_1)(X-x_2)(X-x_3)(X-x_4)$:

$$x_1+x_2+x_3+x_4=-\frac{b}{a}\qquad x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4=\frac{c}{a}$$
$$x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4=-\frac{d}{a}\qquad x_1x_2x_3x_4=\frac{e}{a}\ .$$

8.12. Polinomi sui quaternioni. Quasi tutti i risultati precedenti sono basati sulla commutatività dell'anello/corpo di base. Anche nel caso dei quaternioni, primo esempio di corpo non commutativo, vi sono risultati completamente diversi. Vediamo solo qualche esempio.

8.12.1. Polinomi di secondo grado con infiniti zeri.

8.12.2. Polinomi di terzo grado annullati da tutti i quaternioni.

9. Esercizi.

9.1. Esercizi su Insiemi, Funzioni e Relazioni.

9.1.1. Quanti insiemi distinti si possono formare usando le operazioni di unione, intersezione e complementare a partire da 2 fissati insiemi A e B? Scriverli tutti. E a partire da 3 insiemi? E da 4?

9.1.2. Sviluppare le espressioni $(A\cup B)\cap(C\cup D)$ e $(A\cap B)\cup(C\cap D)$. Cosa succede se in particolare $B=D$?

9.1.3. Mostrare che l'insieme $\complement(A\times B)$ (si intenda: coppie non appartenenti ad $A\times B$) è unione disgiunta dei tre insiemi $(\complement A)\times B$, $(\complement A)\times(\complement B)$ e $A\times(\complement B)$.

9.1.4. Mostrare che l'insieme $(A\times A)\smallsetminus(B\times C)$ è unione dei due insiemi $(A\smallsetminus B)\times A$, $A\times(A\smallsetminus C)$, ed è unione disgiunta dei tre insiemi $(A\smallsetminus B)\times(A\cap C)$, $(A\cap B)\times(A\smallsetminus C)$ e $(A\smallsetminus B)\times(A\smallsetminus C)$. Trovare una descrizione simile per l'insieme $(A\times B)\smallsetminus(C\times D)$.

9.1.5. Scrivere esplicitamente gli elementi dei seguenti insiemi: $\mathscr{P}(\varnothing)$, $\mathscr{P}(\mathscr{P}(\varnothing))$, $\mathscr{P}(\mathscr{P}(\mathscr{P}(\varnothing)))$, $\mathscr{P}(\mathscr{P}(\mathscr{P}(\mathscr{P}(\varnothing))))$.

9.1.6. Mostrare che $A \subseteq B$ se e solo se $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.

9.1.7. Determinare le relazioni tra gli insiemi seguenti:
(a) $\mathscr{P}(A \cup B)$ e $\mathscr{P}(A) \cup \mathscr{P}(B)$; (b) $\mathscr{P}(A \cap B)$ e $\mathscr{P}(A) \cap \mathscr{P}(B)$; (c) $\mathscr{P}(\complement A)$ e $\complement\mathscr{P}(A)$.

9.1.8. Esplorare le relazioni tra le operazioni di differenza insiemistica e di potenza: esprimere $\mathscr{P}(A \smallsetminus B)$ e $\mathscr{P}(A \vartriangle B)$.

9.1.9. Per un fissato insieme X si considerino le funzioni $\mathscr{P}(X) \to \mathscr{P}(X)$ seguenti:
(a) $u_B : A \mapsto A \cup B$ per un fissato $B \subseteq X$;
(b) $i_C : A \mapsto A \cap C$ per un fissato $C \subseteq X$;
(c) le composizioni $u_B \circ i_C$ e $i_C \circ u_B$;
(d) $A \mapsto X \smallsetminus A$;
per ognuna si dicano le proprietà di iniettività, suriettività ecc., se ne indichino eventualmente le inverse, si studi il loro rapporto con la relazione di inclusione e con le operazioni insiemistiche.

9.1.10. Determinare le relazioni tra i seguenti insiemi (di funzioni):
(a) $(A \cup B)^C$ e $A^C \cup B^C$; (b) $A^{(B \cup C)}$ e $A^B \times A^C$;
(c) $(A \cap B)^C$ e $A^C \cap B^C$; (d) $A^{(B \cap C)}$ e $A^B \cup A^C$;
(e) $(A \times B)^C$ e $A^C \times B^C$; (f) $A^{(B \times C)}$, $(A^C)^B$ e $(A^B)^C$.

9.1.11. Si determini se le funzioni $\mathbb{N} \to \mathbb{N}$ definite da $f_1(n) = n + 3$ e $f_2(n) = n^2 + 1$ sono iniettive o suriettive ed eventualmente se ne trovino delle inverse destre o sinistre. Stesso problema considerandole come funzioni $\mathbb{Z} \to \mathbb{Z}$.

9.1.12. Per le seguenti funzioni $f_i : \mathbb{N} \to \mathbb{N}$, si calcolino le due composizioni possibili e si verifichi se esse commutano tra loro oppure no; si studino inoltre le loro proprietà (iniettività, suriettività, ecc.): $f_1(n) = n + 1$, $f_2(n) = 2n$, $f_3(n) = n + 3$, $f_4(n) = n^2$, $f_5(n) = n^2 + n$.

Stesso problema, ma considerando le funzioni $f_i : \mathbb{Z} \to \mathbb{Z}$. Che cosa cambia?

9.1.13. Per le funzioni dell'esercizio precedente, descrivere le funzioni immagine inversa e diretta.

9.1.14. Determinare proprietà e composizioni della funzione $f : \mathbb{N} \to \mathbb{N}$ che manda n in $n/2$ se n è pari, e in 0 altrimenti, e della funzione $g : \mathbb{N} \to \mathbb{N}$ che manda n in $2n$.

9.1.15. Dare un esempio di funzione $f : A \to B$ tale che esistano due insiemi $X, X' \subseteq A$ con $X \cap X' = \varnothing$ ma $f(X) \cap f(X') \neq \varnothing$.

9.1.16. Per una funzione $f : A \to B$, dimostrare che f è iniettiva (risp. suriettiva, biiettiva) se e solo se f_* lo è. Dimostrare inoltre che se f è iniettiva (risp. suriettiva, biiettiva) allora f^* è suriettiva (risp. iniettiva, biiettiva). Valgono i viceversa?

9.1.17. In generale, per una funzione $f : A \to B$ e per ogni $X \subseteq A$ si è visto che $f^* f_*(X) \supseteq X$; mostrare che f è iniettiva se e solo se vale l'uguaglianza per ogni $X \subseteq A$ (basta per qualche X?).

Analogamente per ogni $Y \subseteq B$ si è visto che $f_* f^*(Y) \subseteq Y$; mostrare che f è suriettiva se e solo se vale l'uguaglianza per ogni $Y \subseteq B$ (basta per qualche Y?).

9.1.18. Dare esempi per illustrare che in generale per una funzione $f : A \to B$ e per $X \subseteq A$ non vi sono rapporti tra $f(A \smallsetminus X)$ e $B \smallsetminus f(X)$.

9.1.19. Sia $f : A \to B$ una funzione; come si comportano le immagini dirette ed inverse in relazione alle operazioni di differenza insiemistica? Descrivere $f(X \smallsetminus X')$ e $f(X \vartriangle X')$ per $X, X' \subseteq A$, e $f^*(Y \smallsetminus Y')$ e $f^*(Y \vartriangle Y')$ per $Y, Y' \subseteq B$.

In particolare mostrare che f è iniettiva se e solo se $f(A \smallsetminus X) = f(A) \smallsetminus f(X)$ per ogni X, o anche se e solo se e $f(A \vartriangle X) = B \vartriangle f(X)$ per ogni X.

9.1.20. Per una funzione qualsiasi $f : A \to B$, caratterizzare gli insiemi $X \subseteq A$ tali che $f^* f_*(X) = X$ e gli insiemi $Y \subseteq B$ tali che $f_* f^*(Y) = Y$. È vero che f^* e f_* sono una inversa dell'altra se ristrette a questi sottinsiemi di $\mathscr{P}(A)$ e $\mathscr{P}(B)$?

9.1.21. Si considerino le tre applicazioni seguenti: $p_1 : A \times A \to A$ che manda (a_1, a_2) in a_1 (prima proiezione), $p_2 : A \times A \to A$ che manda (a_1, a_2) in a_2 (seconda proiezione), $d : A \to A \times A$ che manda a in (a, a) (diagonale). Si verifichino le eventuali proprietà di iniettività e suriettività; si calcolino tutte le possibili combinazioni e si dica quali proprietà è possibile dedurre da esse.

9.1.22. Proprietà delle applicazioni $p_A : A \times B \to A$ e $p_B : A \times B \to B$ che mandano (a, b) in a e b rispettivamente: per ogni insieme C e per ogni coppia di funzioni $\alpha : C \to A$ e $\beta : C \to B$ esiste

una unica funzione $f : C \to A \times B$ tale che $p_A \circ f = \alpha$ e $p_B \circ f = \beta$. Questo stabilisce una biiezione canonica tra $A^C \times B^C$ e $(A \times B)^C$.

9.1.23. Dati due insiemi A e B, definiamo unione disgiunta e indichiamo con $A \sqcup B$ l'insieme $(A \times \{1\}) \cup (B \times \{2\})$. Si verifichi che c'è una biiezione canonica tra $A \sqcup B$ e $B \sqcup A$.

Le due funzioni $i_A : A \to A \sqcup B$ e $i_B : B \to A \sqcup B$ che mandano a in $(a, 1)$ e b in $(b, 2)$ rispettivamente, godono della seguente proprietà: per ogni insieme C e per ogni coppia di funzioni $\alpha : A \to C$ e $\beta : B \to C$ esiste una unica funzione $f : A \sqcup B \to C$ tale che $f \circ i_A = \alpha$ e $f \circ i_B = \beta$. Questo stabilisce una biiezione canonica tra $C^A \times C^B$ e $C^{A \sqcup B}$.

Si mostri che esiste una funzione canonica $A \sqcup B \to A \cup B$, che è sempre suriettiva ed è iniettiva se e solo se $A \cap B = \varnothing$.

9.1.24. Sia $R \subseteq A \times B$ una relazione tra A e B; mostrare che essa è grafico di una funzione di A in B se e solo se la funzione $p_A : R \to A$ che manda (a, b) in a è biiettiva. Quando R è grafico di una funzione di B in A?

9.1.25. Studiare la stabilità delle proprietà di una relazione (essere grafico, essere simmetrica, riflessiva, transitiva, antisimmetrica, ecc.) passando alla relazione trasposta.

9.1.26. Nel piano della geometria euclidea elementare, si consideri sull'insieme delle rette la relazione di parallelismo. Mostrare che si tratta di una relazione di equivalenza (se ogni retta viene considerata parallela a se stessa!) e se ne descrivano le classi di equivalenza.

9.1.27. Nel piano della geometria euclidea elementare, si consideri sull'insieme delle rette la relazione di incidenza (due rette sono in relazione se e solo se si intersecano). Di che proprietà gode questa relazione? Si studi la relazione di equivalenza generata e se ne descrivano le classi di equivalenza.

9.1.28. Nello spazio della geometria euclidea elementare, si consideri sull'insieme delle rette (risp. dei piani) la relazione di parallelismo (essere parallele per due rette significa stare su uno stesso piano e lì essere parallele). Mostrare che si tratta di una relazione di equivalenza (se ogni retta, risp. piano, viene considerata parallela a se stessa) e se ne descrivano le classi di equivalenza.

9.1.29. Nello spazio della geometria euclidea elementare, si consideri sull'insieme delle rette (risp. dei piani) la relazione di incidenza (due rette, risp. piani, sono in relazione se e solo se si intersecano). Di che proprietà gode questa relazione? Si studi la relazione di equivalenza generata e se ne descrivano le classi di equivalenza.

9.1.30. Nell'insieme $\mathbb{Z}$ definiamo che $a \sim b$ se e solo se $a - b$ è un numero pari (divisibile per 2). Si tratta di una relazione di equivalenza? Eventualmente quali sono le classi di equivalenza?

9.1.31. Nell'insieme $\mathbb{Z}$ definiamo che $a \sim b$ se e solo se $a - b$ è un numero dispari (non divisibile per 2). Si tratta di una relazione di equivalenza? Eventualmente qual'è la relazione di equivalenza generata, e quali sono le sue classi di equivalenza?

9.1.32. Nell'insieme $\mathbb{N}$ dei numeri naturali definiamo la relazione $n|m$ (letto "n divide m") se m è un multiplo di n, ovvero se $m = pn$ per qualche $p \in \mathbb{N}$. Si tratta di una relazione d'ordine? È totale? Vi sono elementi primo e ultimo? Come sono fatti i sottinsiemi totalmente ordinati per la divisibilità?

9.1.33. Nell'insieme $\mathbb{Z}$ dei numeri interi definiamo la relazione $n|m$ (letto "n divide m") se m è un multiplo di n, ovvero se $m = pn$ per qualche $p \in \mathbb{Z}$. Mostrare che si tratta di una relazione riflessiva e transitiva. Si tratta di una relazione d'ordine? Considerare l'equivalenza $n \sim m$ se e solo se $n|m$ e $m|n$; descrivere l'insieme $\mathbb{Z}/\sim$ e l'ordine indotto dalla divisibilità.

9.1.34. Dire quali delle seguenti funzioni $f_i : \mathbb{N} \to \mathbb{N}$ sono ordinate, sia per l'ordine $\leqslant$, sia per il preordine di divisibilità $|$: $f_1(n) = n + 1$, $f_2(n) = 2n$, $f_3(n) = n + 3$, $f_4(n) = n^2$, $f_5(n) = n^2 + n$.

9.2. Esercizi su Cardinali, Naturali, Combinatorica.

9.2.1. Dati tre cardinali α, β e γ, mostrare che

(a) $(\alpha\beta)^\gamma = \alpha^\gamma \beta^\gamma$;
(b) $\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma = (\alpha^\gamma)^\beta$;
(c) se $\alpha \leqslant \beta$ allora $\alpha + \gamma \leqslant \beta + \gamma$, $\alpha\gamma \leqslant \beta\gamma$, $\alpha^\gamma \leqslant \beta^\gamma$, $\gamma^\alpha \leqslant \gamma^\beta$.

9.2.2. Per ogni due insiemi finiti A e B, mostrare che $|A \smallsetminus B| + |A \cap B| = |A|$, e che se $B \subseteq A$ allora $|A \smallsetminus B| = |A| - |B|$. E per insiemi infiniti?

9.2.3. Siano A e B due insiemi. È vero o falso che $|A| + |B| = |A|$ implica $|B| = 0$? È vero o falso che $|A| \cdot |B| = |A|$ implica $|B| = 1$? Dare esempi e controesempi.

9.2.4. Mostrare le seguenti relazioni:
(*a*) $|\mathbb{Z}| = |\mathbb{N}|$;
(*b*) $|\mathbb{Q}| = |\mathbb{N}|$;
(*c*) $|\mathbb{R}| = |[0,1]| = |(0,1)|$ (con le notazioni usuali: $[0,1]$ e $(0,1)$ sono gli intervalli dei numeri reali compresi tra 0 e 1, inclusi gli estremi o esclusi gli estremi);
(*d*) $|\mathbb{R}| > |\mathbb{N}|$;

9.2.5. Si confrontino le cardinalità dei seguenti insiemi:
(*a*) $\mathbb{N}^{\mathbb{N}}$, insieme delle funzioni di $\mathbb{N}$ in sè;
(*a'*) l'insieme delle funzioni di $\mathbb{N}$ in $\mathbb{N} \smallsetminus \{0\}$;
(*b*) insieme delle funzioni (strettamente) crescenti di $\mathbb{N}$ in sè
(*c*) insieme delle funzioni decrescenti di $\mathbb{N}$ in sè
(*d*) insieme delle funzioni di $\mathbb{N}$ in sè che siano "quasi sempre nulle", cioè che hanno valori diversi da zero solo per un numero finito di elementi;
(*e*) insieme delle funzioni di $\mathbb{N}$ in sè che siano addittive (cioè le funzioni f tali che $f(n+n') = f(n) + f(n')$ per ogni $n, n' \in \mathbb{N}$);
(*f*) insieme delle funzioni di $\mathbb{N}$ in sè che siano moltiplicative (cioè le funzioni f tali che $f(nn') = f(n)f(n')$ per ogni $n, n' \in \mathbb{N}$).

9.2.6. Verificare la formula di inclusione-esclusione per 3, 4, n insiemi (induzione).

9.2.7. Dimostrare le formule seguenti riguardo ai coefficienti binomiali:
(*a*) $\binom{n}{k} = \sum_{i=1}^{n} \binom{n-i}{k-1}$
(*b*) $\binom{n}{k} = \sum_{i=0}^{n} \binom{n-i}{k-i+1}$
(*c*) $\sum_{i=0}^{n} \binom{n}{i} = 2^n$
(*d*) $\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$
(*e*) $\sum_{i=0}^{p} \binom{n}{i}\binom{n-i}{p-i} = 2^n \binom{n}{p}$
Se possibile, se ne dìa una interpretazione combinatorica.

9.2.8. Studiare la funzione ricorsivamente definita da $s(1) = 1$ e $s(n+1) = s(n) + (-1)^n n$.

9.2.9. Studiare la funzione ricorsivamente definita da $f(n,k) = f(n-1,k)f(n-1,k-1)$ e $f(n,0) = s$, $f(n,n) = s$ per ogni $n \in \mathbb{N}$.

9.2.10. Studiare gli sviluppi del trinomio $(x+y+z)^n$ per ogni $n \in \mathbb{N}$, analogamente a quanto fatto per il binomio; in particolare definire dei coefficienti trinomiali e discutere le loro relazioni ricorsive.

9.2.11. Calcolare la somma dei primi n numeri naturali dispari e la somma dei primi n numeri naturali pari per ogni n. Dare una dimostrazione per induzione del proprio risultato.

9.2.12. Determinare, e dimostrare per induzione la correttezza del proprio risultato, le somme
(*a*) $\sum_{i=1}^{n} (-1)^i i$ per ogni n naturale.
(*b*) $\sum_{i=1}^{n} (-1)^i i^2$ per ogni n naturale.
(*c*) $\sum_{i=1}^{n} 2^i$ per ogni n naturale.
(*d*) $\sum_{i=1}^{n} (-1)^i 2^i$ per ogni n naturale.

9.2.13. Mostrare che $\sum_{i=1}^{n} i\, i! = (n+1)! - 1$ per ogni $n \in \mathbb{N}$.

9.2.14. Mostrare che $\sum_{k=1}^{n} (1 + a^k) = n + a\dfrac{a^n - 1}{a - 1}$ per ogni $n \in \mathbb{N} \smallsetminus \{0\}$ e per ogni $a \in \mathbb{R} \smallsetminus \{1\}$.

9.2.15. Disuguaglianze di Bernoulli.
(*a*) Dimostrare che per ogni $n \in \mathbb{N}$ e ogni $x \in \mathbb{R}$ con $x > -1$ si ha $(1+x)^n \geqslant 1 + nx$ (e vale l'uguaglianza se e solo se $x = 0$ oppure $n \in \{0,1\}$;
(*b*) Dimostrare che per ogni $n \in \mathbb{N}$ e ogni $x \in \mathbb{R}$ con $\frac{1}{n} > x > -1$ si ha $\frac{1}{1-nx} \geqslant (1+x)^n$.

9.2.16. Dimostrare che per ogni $n \in \mathbb{N}$ abbiamo

$$(1 + a_1) \cdots (1 + a_n) \geqslant 1 + a_1 + \cdots + a_n$$

se $a_i \in \mathbb{R}$ hanno tutti lo stesso segno e sono tutti maggiori di -1.

9.2.17. Confronto delle Medie Aritmetica e Geometrica. Per ogni $n \in \mathbb{N}$ positivo e ogni famiglia $a_1, \dots a_n$ di reali positivi, la media aritmetica è $m = \frac{1}{n}\sum_{i=1}^n a_i$, mentre la media geometrica è $g = (\prod_{i=1}^n a_i)^{1/n}$. Mostrare che $m \geqslant g$ (e vale l'uguaglianza se e solo se tutti gli a_i sono uguali). Conviene dimostrare che

$$\prod_{i=1}^n a_i \leqslant \left(\frac{1}{n}\sum_{i=1}^n a_i\right)^n$$

procedendo per induzione, e ragionando nel passo induttivo nel modo seguente: se uno degli a_i, diciamo l'ultimo, coincide con la media aritmetica, allora ci si riconduce subito all'ipotesi induttiva; altrimenti vi saranno un a_i, diciamo l'ultimo, che è superiore alla media aritmetica (sia $a_{n+1} = M + c$ con c positivo), e un altro a_i, diciamo il penultimo, che è inferiore alla media aritmetica (sia $a_n = M - d$ con d positivo): si sostituisca a_{n+1} con M, e a_n con $M + c - d$...

9.2.18. Per un poligono piano, si dicono diagonali i segmenti che uniscono due vertici non adiacenti; quante diagonali ha un poligono con n vertici?

9.2.19. Dati n punti nel piano, a tre a tre non allineati, quanti triangoli distinti è possibile formare? E se fossero punti nello spazio?

9.2.20. Quante parole con meno di 5 caratteri si possono formare con alfabeti di due lettere, di tre lettere, di quattro lettere, di cinque lettere, e in generale di n lettere?

Quante di queste parole non hanno lettere consecutive uguali?

9.2.21. In quanti modi si possono distribuire 18 palline uguali in 5 cassetti diversi? E facendo in modo che nessun cassetto rimanga vuoto? E facendo in modo che due siano vuoti? E facendo in modo che due fissati siano vuoti?

9.2.22. In quanti modi si possono distribuire 5 palline uguali in 18 cassetti diversi? E facendo in modo che ogni cassetto abbia al più una pallina?

9.2.23. Nove persone cenano seduti ad un tavolo circolare; in quanti modi diversi si possono disporre? E se fossero su una panchina? Se ci fossero 3 coppie di gemelli identici, quante disposizioni potrebbe distinguere un osservatore?

9.2.24. Quanti sono i numeri di n cifre (nella notazione decimale) divisibili per cinque?

9.2.25. Quanti sono i numeri di n cifre (nella notazione decimale), ognuna non nulla, tale che ogni cifra sia non minore della seguente?

9.2.26. Quanti sono i numeri di 9 cifre (nella notazione decimale) contenenti tre volte la cifra 1, due volte ciascuna le cifre 3, 5, 7?

9.2.27. Quanti sono i numeri dispari di tre cifre distinte (nella notazione decimale)? E di quattro? E di n?

9.2.28. Scrivere tutti gli elementi di $\mathfrak{S}_2$ e tutti i possibili quozienti di questo gruppo.

9.2.29. Scrivere tutti gli elementi di $\mathfrak{S}_3$ e tutti i possibili quozienti di questo gruppo.

9.2.30. Scrivere tutti gli elementi di $\mathfrak{S}_4$ e tutti i possibili quozienti di questo gruppo.

9.2.31. Studiare decomposizione in cicli, in scambi e segno delle seguenti permutazioni:

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}$;

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 3 & 6 & 5 & 7 & 4 & 2 \end{pmatrix}$;

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 \end{pmatrix}$;

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 9 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix}$.

9.2.32. Mostrare che per ogni $\sigma \in \mathfrak{S}_n$ esiste un intero $m \leqslant n!$ tale che σ^m sia la permutazione identica. È vero o falso che esiste un intero $m \leqslant n!$ tale che σ^m sia uno scambio? È vero o falso che esiste un intero $m \leqslant n!$ tale che σ^m sia una permutazione appartenente ad $\mathfrak{A}_n$?

$*$**9.2.33.** Lemma dei matrimoni. Dati due insiemi M e F, e una funzione $p : M \to \mathscr{P}(F)$, esiste una applicazione iniettiva $f : M \to F$ tale che $f(m) \in p(m)$ per ogni $m \in M$ se e solo se per ogni $H \subseteq M$ si ha $|\bigcup_{m\in H} p(m)| \geqslant |H|$.

9.3. Esercizi su Interi, Divisione, MCD.

9.3.1. Eseguire le divisioni con resto tra le seguenti coppie di interi:
(a) 1965 e 23; (b) 1985 e 29; (c) 2004 e 109.

9.3.2. Calcolare il MCD tra le seguenti coppie di interi, e i coefficienti della loro combinazione che lo calcolano:
(a) 300 e 325; (b) 198 e 288; (c) 576 e 840. (d) 630 e 132; (e) 285 e 126.

9.3.3. Se $a = qb + r$ è la divisione con resto di a per b con a, b positivi, scrivere quoziente e resto delle divisioni di a per $-b$, di $-a$ per b e di $-a$ per $-b$.

9.3.4. Mostrare che $\mathrm{MCD}(ac, bc) = c\mathrm{MCD}(a, b)$.

9.3.5. Mostrare che $\mathrm{MCD}(a, b+za) = \mathrm{MCD}(a, b)$ se $z \in \mathbb{Z}$. Usare questo risultato per giustificare l'algoritmo di Euclide di calcolo del massimo comun divisore.

9.3.6. Mostrare che $\mathrm{MCD}(a, bc)$ divide, e in generale non coincide, con il prodotto $\mathrm{MCD}(a, b)\mathrm{MCD}(a, c)$. Mostrare che $\mathrm{MCD}(a, bc) = \mathrm{MCD}(a, b)\mathrm{MCD}(a, c)$ se $\mathrm{MCD}(b, c) = 1$ (cioè se b e c sono coprimi).

9.3.7. Siano $a = qb + r$ e $a' = q'b + r'$ le divisioni con resto di a e a' per b. Cosa possiamo dire delle divisioni con resto di aa', $a + a'$, $a - a'$ per b?

9.3.8. Siano $a = qb + r$ e $b = q'c + r$ le divisioni con resto di a per b e di b per c. Cosa possiamo dire della divisione con resto di a per c?

9.3.9. Date le due divisioni con resto $a = qb + r$ di a per b e $b = q'a + r'$ di b per a, che relazioni vi sono tra q, q', r, r'?

9.3.10. Scrivere le tavole di somma e moltiplicazione di $\mathbb{Z}/n\mathbb{Z}$ per $n = 2, 3, 4, 5, 6, 7, 8, 9$. Trovare i divisori di zero, i nilpotenti, gli unipotenti, gli invertibili.
È vero che in $\mathbb{Z}/n\mathbb{Z}$ un elemento è o invertibile o divisore di zero?

9.3.11. Studiare iniettività e suriettività della funzione che manda x in x^2 come funzione di $\mathbb{Z}$ in sé e come funzione di $\mathbb{Z}/n\mathbb{Z}$ in sé per $n = 2, 3, 4, 5, 6$.

9.3.12. Idem per la funzione che manda x in x^3.

9.3.13. Dati $a, b \in \mathbb{N}$, si studi la funzione $f_{(a,b)} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definita da $f_{(a,b)}(x, y) = ax + by$.

9.3.14. Rappresentazione posizionale in base qualsiasi. Sia b un qualunque numero intero maggiore di 1. Dato un numero intero, esso si può rappresentare come sequenza di cifre comprese tra 0 e $b-1$ nel modo seguente: la sequenza $a_n a_{n-1} \cdots a_2 a_1 a_0$ rappresenta il numero $a_n b^n + a_{n-1} b^{n-1} + \cdots + a_2 b^2 + a_1 b + a_0$ (se $b = 10$, allora si tratta della rappresentazione posizionale in base 10). Dato un numero naturale, come trovare la sua rappresentazione posizionale in base b? [Scrivere un algoritmo, usando ripetutamente la divisione euclidea con resto, per trovare successivamente le cifre a_0, a_1, ..., a_n].
Di solito per indicare che una sequenza $a_n a_{n-1} \cdots a_1 a_0$ di cifre rappresenta un numero in base b, si scrive la base al pedice del numero: $(a_n a_{n-1} \cdots a_1 a_0)_b$

9.3.15. Come mai noi usiamo la base 10? Che base userebbero le scimmie? E i cartoni animati?

9.3.16. Scrivere nelle basi 2, 3, 4, 8, 16 i seguenti numeri scritti in base 10: 2, 4, 8, 16, 32, 64, 256, 3, 9, 27, 81, 243 (per le basi $b > 10$ si usano come cifre successive a 9 le lettere maiuscole dell'alfabeto nell'ordine alfabetico; per esempio in base 16 le cifre sono $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$).

9.3.17. Esprimere in base 10 i seguenti numeri naturali espressi nella base indicata a pedice: 101010_2, 100_8, 101_8, 115_8, 100_{16}, 101_{16}, $11A_{16}$, $A1A_{16}$, $A2C_{16}$, FAC_{16}.

9.3.18. Dare dei criteri per decidere se un numero intero scritto in base 10 è divisibile per 2, 3, 4, 5, 6, 7, 8, 9, 11, 13.

9.3.19. Ricordare la "regola del 9" per il controllo delle moltiplicazioni (e delle somme), e giustificarla in termini di congruenza modulo 9.

9.3.20. Scrivere una regola stenoaritmetica per moltiplicare tra loro numeri interi scritti in base decimale la cui ultima cifra è 5; in particolare, per fare il quadrato di un tale numero.

9.3.21. Sia p un fissato numero primo. Per ogni numero intero non nullo n, definiamo l'ordine in p nel modo seguente: $ord_p(n) = a$ se p^a divide n, e p^{a+1} non divide n (dunque è il massimo esponente

a tale che p^a divide n). Abbiamo allora una funzione $ord_p : \mathbb{Z} \smallsetminus \{0\} \to \mathbb{N}$; mostrare che soddisfa alle seguenti proprietà:
(a) $ord_p(n) = 0$ se e solo se p non divide n;
(b) $ord_p(nm) = ord_p(n) + ord_p(m)$ (moltiplicatività);
(c) $ord_p(n + m) \geqslant \min(ord_p(n), ord_p(m))$ (quando vale l'uguaglianza? quando la disuguaglianza stretta?);
(d) se m divide n allora $ord_p(m) \leqslant ord_p(n)$ (vale il viceversa?).
ord_p è funzione suriettiva? iniettiva?

9.3.22. Calcolare ord_3 e ord_5 dei seguenti interi: 15, 16, 27, 69, 125, 330.

9.3.23. Sia p un fissato numero primo. Per un intero positivo n, calcolare $ord_p(p^n)$, $ord_p(p!)$,$ord_p(p^n!)$, $ord_p(n!)$ [usare le cifre in base p], $ord_p(\binom{p}{n})$.

9.3.24. Mostrare che per ogni coppia di numeri interi x e y abbiamo che $(x+y)^p \equiv x^p+y^p \pmod p$ (si osservi che i coefficienti binomiali $\binom{p}{i}$ sono divisibili per p se p è primo e $i \neq 0, p$).

Dedurne per induzione il piccolo teorema di Fermat: per ogni intero a, abbiamo che $a^p \equiv a \pmod p$.

9.3.25. In una scatola ci sono scorpioni, ragni e centopiedi; in totale si contano 282 zampe. Dire se è possibile, ed eventualmente determinare quale può essere il contenuto della scatola.

9.3.26. Dire se esistono, ed eventualmente trovarli, interi x, y, z tali che $6x + 28y + 15z = 1$.

9.3.27. Risolvere la congruenza $16x \equiv 1000 \pmod{27}$.

9.3.28. Discutere il seguente sistema di congruenze: $\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod 6 \end{cases}$

9.3.29. Discutere il seguente sistema di congruenze: $\begin{cases} x \equiv 5 \pmod{28} \\ 10x \equiv 35 \pmod{125} \end{cases}$

9.3.30. Disponendo di francobolli da 36 e da 45 centesimi, è possibile affrancare un pacco per 2 euro e 34 centesimi? Eventualmente come approssimarlo con la perdita minore? E per un pacco di 3 euro e 51 centesimi?

9.4. Esercizi su Complessi e Polinomi.

9.4.1. Calcolare z^{-1}, w^{-1}, zw, zw^{-1}, $z^{-1}w$, z^2, z^3, z^4, le radici quadrate di z e le radici cubiche di z per le seguenti coppie:
(a) $z = 1 + i$, $w = 2 - i$;
(b) $z = 1 - i$, $w = 1 + 2i$;
(c) $z = 2e^{i\pi/3}$, $w = 3e^{i\pi/4}$
(d) $z = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$, $w = i$
(e) $z = \cos\vartheta + i\sin\vartheta$, $w = \pm i$

9.4.2. Si studino le proprietà di iniettività, suriettività, eventuali inverse destre e sinistre per le seguenti funzioni $\mathbb{C} \to \mathbb{C}$:
(1) $f_1(z) = z^2 + i$;
(2) $f_2(z) = (z + i)^2$;
(3) $f_3(z) = z - \overline{z}$;
(4) $f_4(z) = z/|z|$ se $z \neq 0$, $f_4(0) = 0$.
(5) $f_5(z) = z/\overline{z}$ se $z \neq 0$, $f_5(0) = 0$.
Per ogni $w \in \mathbb{C}$, si determini la sua controimmagine per ciascuna delle funzioni date.

9.4.3. Si consideri l'insieme $\{z^n \mid n \in \mathbb{N}\}$ per un fissato $z \in \mathbb{C}$; trovare condizioni necessarie e sufficienti affinché:
(a) l'insieme sia finito;
(b) l'insieme ammetta una infinità di elementi tra loro allineati;
(c) l'insieme sia tutto contenuto nel cerchio unitario;
(d) l'insieme sia tutto esterno al cerchio unitario.

9.4.4. Come l'esercizio precedente per l'insieme delle radici n-esime di z al variare di n.

9.4.5. Definiamo $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ (circolo unitario o circonferenza unitaria) e $R(1) = \{z \in \mathbb{C} \mid z^n = 1$ per qualche $n \in \mathbb{N}\}$ (radici dell'unità). Mostrare che $R(1) \subseteq \mathbb{S}^1$ e che l'inclusione è stretta. Come si caratterizzano gli elementi di $R(1)$ in termini dell'argomento? Determinare le cardinalità di $R(1)$ e di $\mathbb{S}^1$.

9.4.6. È vero che tra due punti di $\mathbb{S}^1$ si trova sempre qualche punto di $R(1)$ (nel senso della geometria di $\mathbb{S}^1$ nel piano di Gauss)?

9.4.7. Scrivere (e disegnare sul piano di Gauss) le radici n-esime di $-i$, $1+i$, $1-i$ per $n = 2, 3, 4, 5, 6$.

9.4.8. Determinare $\cos(5t)$, $\cos(8t)$, $\sin(6t)$, $\sin(9t)$ in termini delle funzioni trigonometriche di argomento t (e loro potenze).

9.4.9. Calcolare $\sin^3 t$, $\sin^4 t$, $\cos^5 t$, $\cos^6 t$ in termini delle funzioni trigonometriche di argomento t (e multipli di t).

9.4.10. Dimostrare le formule sul parallelogramma per i numeri complessi, e spiegarne l'interpretazione geometrica.

9.4.11. Dare l'interpretazione geometrica nel piano di Gauss della inversione dei numeri complessi: se $z = \varrho e^{i\vartheta}$ allora $z^{-1} = \varrho^{-1} e^{-i\vartheta}$.

9.4.12. Dare l'interpretazione geometrica nel piano di Gauss del passaggio all'opposto dei numeri complessi: se $z = \varrho e^{i\vartheta}$ allora $-z = \varrho e^{(i\vartheta+\pi)}$.

9.4.13. Dare rappresentazioni grafiche nel piano di Gauss per la differenza e la divisione tra numeri complessi.

9.4.14. Rappresentare nel piano di Gauss tutti i logaritmi complessi di e e di ie. Per un qualsiasi $z = \varrho e^{i\vartheta}$ disegnare nel piano di Gauss la famiglia dei suoi logaritmi.

9.4.15. Se $|z| = 1$, è vero che le radici n esime di z si ottengono ruotando opportunamente (e di quanto?) le radici n-esime dell'unità?

9.4.16. Calcolare le lunghezze l_n (risp. L_n) dei lati dei poligoni regolari di n lati inscritti (risp. circoscritti) nella circonferenza unitaria. Quanto valgono i limiti nl_n e nL_n quando n "va all'infinito"?

9.4.17. Mostrare che la funzione $\mathbb{S}^1 \times \mathbb{R}_{>0} \to \mathbb{C} \smallsetminus \{0\}$ che manda (ξ, ϱ) nel prodotto $\xi\varrho$ è una biiezione. Scrivere la funzione inversa.

9.4.18. Inversione del cerchio: studiare le funzioni di $\mathbb{C} \smallsetminus \{0\}$ in sè ottenute mandando z in $1/z$ e $1/\overline{z}$. È vero che entrambe rispettano il circolo unitario (in che senso?)? È vero che invertono interno ed esterno del circolo unitario? Determinare l'immagine delle "rette verticali".

9.4.19. Il semipiano di Poincaré è definito da $P = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ (numeri complessi la cui parte immaginaria è positiva). Il disco unità è $D = \{z \in \mathbb{C} \mid |z| < 1\}$ (numeri complessi di modulo strettamente inferiore a 1). Mostrare che la funzione $f(z) = \frac{z-i}{z+i}$ è una biiezione $P \to D$.

Determinare l'immagine della semicirconferenza di centro origine e raggio 1; e della semiretta verticale passante per l'origine.

Mostrare che i tratti di circonferenze di centro il punto $-i$ sono mandati in tratti di circonferenze di centro il punto 1.

9.4.20. Siano a, b, c, d numeri reali tali che $ad - bc = 1$. Consideriamo la funzione (detta trasformazione lineare fratta) $s : P \to P$ (P è il semipiano di Poincaré) data da $s(z) = \frac{az+b}{cz+d}$.

Mostrare che $\Im(s(z)) = \frac{\Im(z)}{|cz+d|^2}$, cosicché in effetti s è definita da P a P.

Mostrare che s può essere scritta come composizione di funzione dei seguenti tre tipi: traslazione reale ($z \mapsto z + u$ con $u \in \mathbb{R}$), omotetie reali ($z \mapsto vz$ con $v \in \mathbb{R}$, $v > 0$), controinversioni ($z \mapsto -\frac{1}{z}$).

Descrivere le figure formate da $s(z)$ se z descrive le semicirconferenze con centro sull'asse reale, oppure le semirette ortogonali all'asse reale.

9.4.21. Fattorizzare in $\mathbb{Q}[X]$ i seguenti polinomi:
(*a*) $6X^4 - 11X^3 - X^2 - 4$;
(*b*) $2X^3 + 12X^2 + 13X + 15$;
(*c*) $6X^5 + 11X^4 - X^3 + 5X - 6$;
(*d*) $X^6 + 3X^5 + 4X^4 + 3X^3 - 15X^2 - 16X + 20$;
(*e*) $2X^6 + X^5 - 9X^4 - 6X^3 - 5X^2 - 7X + 6$;

9.4.22. Eseguire la divisione tra i seguenti polinomi:
(*a*) $4X^3 + X^2$ e $X + 1 + i$
(*b*) $2X^4 - 3X^3 + 4X^2 - 5X + 6$ e $X^2 - 3X + 1$
(*c*) $X^4 - 2X^3 + 4X^2 - 6X + 8$ e $X - 1$

9.4.23. Determinare il MCD tra i seguenti polinomi:
(*a*) $X^6 - 7X^4 + 8X^3 - 7X + 7$ e $3X^5 - 7X^3 + 3X^2 - 7$
(*b*) $X^5 + X^4 - X^3 - 3X^2 - 3X - 1$ e $X^4 - 2X^3 - X^2 - 2X - 1$
(*c*) X^4 e $(1 - X)^4$.

9.4.24. Mostrare che il MCD tra $X^m - 1$ e $X^n - 1$ è $X^d - 1$ ove d è il MCD tra m ed n. Cioè $(X^m - 1, X^n - 1) = X^{(m,n)} - 1$.

9.4.25. Determinare un polinomio di grado n che abbia n radici fissate; esplicitare i rapporti tra i coefficienti del polinomio e le radici assegnate (relazioni di Vièta).

9.4.26. Formula di interpolazione di Lagrange. Determinare un polinomio di grado n che in $a_0, a_1, \ldots, a_n \in \Bbbk$ (tutti distinti) valga rispettivamente $b_0, b_1, \ldots, b_n \in \Bbbk$. Si tratta di $F(X) = \sum_{i=0}^{n} b_i \frac{\prod_{j\neq i}(X-a_j)}{\prod_{j\neq i}(a_i-a_j)}$.

9.4.27. Discutere la fattorizzazione in $\Bbbk[X]$, in $\mathbb{R}[X]$ e $\mathbb{Q}[X]$ dei polinomi $X^n + 1$ per ogni $n \in \mathbb{N}$; lo stesso per $X^n - 1$.

9.4.28. Si consideri un triangolo di vertici $A, B, C \in \mathbb{C}$. Mostrare che esso è isoscele in A se e solo se esiste un numero complesso unitario α diverso da ± 1 tale che $A = \frac{1}{1+\alpha}B + \frac{1}{1+\overline{\alpha}}C$. Che relazioni vi sono tra α e gli angoli del triangolo? Per quali valori di α il triangolo è rettangolo?

9.4.29. Si consideri un triangolo di vertici $A, B, C \in \mathbb{C}$. Mostrare che esso è rettangolo in A se e solo se esiste un numero complesso unitario α diverso da ± 1 tale che $2A = (1 - \alpha)B + (1 + \alpha)C$. Che relazioni vi sono tra α e gli angoli del triangolo? Per quali valori di α il triangolo è isoscele?

Capitolo I

Spazi Vettoriali

Questo capitolo presenta lo strumento fondamentale per lo sviluppo dei concetti geometrici in termini moderni, che è quello di Spazio Vettoriale. Uno spazio vettoriale è un insieme dotato di alcune strutture algebriche che modellano la nostra esperienza di "muoversi tra i punti di uno spazio geometrico". In realtà già i primi esempi che ne faremo evidenzieranno che la struttura algebrica di spazio vettoriale ha applicazioni molto più ampie, ed è attualmente usato in ogni ramo della Matematica.

D'ora in poi parleremo solo di corpi commutativi, e useremo il termine corpo per intendere corpo commutativo (nella terminologia italiana si parla di campi), a meno che non sia specificato altrimenti.

1. Definizione ed esempi fondamentali.

1.0.1. Campi di base. Come esempi di campi bisogna sempre tener presente i seguenti: $\mathbb{Q}$ (razionali), $\mathbb{R}$ (reali), $\mathbb{C}$ (complessi), $\mathbb{F}_p = \mathbb{Z}/p$ (campi primi finiti), $\Bbbk(X)$ (frazioni di polinomi) se $\Bbbk$ è un campo.

1.1. Definizione (Spazio Vettoriale su un corpo). *Uno spazio vettoriale su un corpo $\Bbbk$ (i cui elementi sono chiamati scalari, in questo contesto) è il dato di un insieme V (i cui elementi sono detti vettori) dotato di due operazioni:*
(S) *somma di vettori:* $V \times V \longrightarrow V : \ (v, w) \mapsto v + w$;
(P) *prodotto per gli scalari:* $\Bbbk \times V \longrightarrow V : \ (\alpha, v) \mapsto \alpha v$;
soggette ai seguenti assiomi:
(S) *V con l'operazione di somma è un gruppo commutativo (o abeliano); cioè:*
- $(S1)$ *esiste un elemento neutro $0 \in V$ tale che $v + 0 = v = 0 + v$ $(\forall v \in V)$;*
- $(S2)$ *l'operazione è associativa, $u + (v + w) = (u + v) + w$ $(\forall u, v, w \in V)$;*
- $(S3)$ *l'operazione è commutativa, $v + w = w + v$ $(\forall v, w \in V)$;*
- $(S4)$ *ogni elemento ha opposto, $(\forall v)(\exists w) v + w = 0 = w + v$;*

(P) *l'operazione di moltiplicazione per gli scalari soddisfa alle seguenti proprietà:*
- $(P1)$ *unitaria: $1v = v$ $(\forall v \in V)$;*
- $(P2)$ *associativa: $\alpha(\beta v) = (\alpha\beta)v$ $(\forall \alpha, \beta \in \Bbbk, \forall v \in V)$;*
- $(P3)$ *lineare sugli scalari: $(\alpha + \beta)v = \alpha v + \beta v$ $(\forall \alpha, \beta \in \Bbbk, \forall v \in V)$;*
- $(P4)$ *lineare sui vettori: $\alpha(v + w) = \alpha v + \alpha w$ $(\forall \alpha \in \Bbbk, \forall v, w \in V)$.*

Si osservi che nella definizione abbiamo usato gli stessi simboli con significati diversi: per esempio il simbolo $+$ denota sia la somma in V che la somma in $\Bbbk$, il simbolo 0 denota sia lo zero di V (che potremmo chiamare 0_V, se ci fossero possibilità di equivoco), sia lo zero di $\Bbbk$ (che potremmo chiamare $0_\Bbbk$). Capiterà spesso di incorrere in questi abusi di linguaggio allo scopo di rendere meno pedante il testo; il lettore è invitato a riflettere e distinguere in ogni formula gli eventuali abusi.

A partire dalla definizione si può trarre una piccola messe di risultati algebrici, quali per esempio:

1.1.1. Unicità dello zero. L'elemento 0 dello spazio vettoriale V è unico; se infatti ve ne fossero due con la proprietà $(S1)$, diciamo 0 e $0'$, avremmo $0 = 0 + 0' = 0'$.

1.1.2. Unicità dell'opposto. Per ogni $v \in V$, l'elemento w tale che $v + w = 0$ è unico; infatti, se ce ne fossero due, w e w', avremmo $w = w + 0 = w + (v + w') = (w + v) + w' = 0 + w' = w'$.

1.1.3. Prodotti con zero. Per ogni $v \in V$ abbiamo $0v = 0_V$ (per esempio aggiungendo $-0v$ alla uguaglianza $0v = (0 + 0)v = 0v + 0v$). Per ogni $\alpha \in \Bbbk$ abbiamo $\alpha 0_V = 0_V$ (similmente).

1.1.4. Relazione tra opposto e -1. Per ogni $v \in V$, l'opposto è l'elemento $(-1)v$; infatti $v + (-1)v = (1 - 1)v = 0v = 0$. Di solito quindi scriveremo $-v$ per indicare l'opposto di v.

1.1.5. Opposto dell'opposto. Risulta $-(-v) = v$; infatti $(-v) + v = 0$. Oppure $-(-v) = (-1)(-1)v = v$.

1.1.6. Si osservi in particolare che la commutatività della somma è conseguenza degli altri assiomi, poiché la mappa opposto è omomorfismo di gruppo (come ogni moltiplicazione per scalari, essendo la moltiplicazione per -1). In modo più esplicito: il vettore $-(v + w)$ si può determinare in due modi, uno è quello generale $(-w) + (-v)$ (somma degli opposti nell'ordine opposto), l'altro è usando la moltiplicazione per -1, cioè $-(v+w) = (-1)(v+w) = (-1)v+(-1)w = (-v)+(-w)$. Per confronto (usando $-v, -w$ invece di v, w) si conclude.

1.1.7. Leggi di cancellazione. Dalla uguaglianza $v + w = u + w$ si deduce $v = u$; infatti basta sommare ad entrambi i lati dell'uguaglianza l'opposto di w. Da $\alpha v = \alpha u$ con $\alpha \in \Bbbk$, $\alpha \neq 0$ abbiamo $v = u$; infatti basta moltiplicare entrambi i membri per l'inverso di α in $\Bbbk$. Da $\alpha v = \beta v$ con $\alpha, \beta \in \Bbbk$ e $v \neq 0$ si ha $\alpha = \beta$ (perché?).

1.1.8. Legge di annullamento. Vale $\alpha v = 0$ se e solo se $\alpha = 0$ oppure $v = 0$. Come si possono dedurre le leggi di cancellazione da quella di annullamento?

Non insisteremo ulteriormente su questi piccoli risultati ed altri analoghi, che verranno d'ora in poi tacitamente usati.

1.2. Esempi Fondamentali. Diamo di seguito alcuni fondamentali esempi di spazi vettoriali; sono tutti estremamente importanti e verranno costantemente usati, quindi invitiamo il lettore ad uno studio accurato di questi casi.

1.2.1. Spazi vettoriali standard. L'insieme delle n-uple

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in \Bbbk \text{ per } i = 1, \dots, n \right\}$$

si indica con $V_n(\Bbbk)$ o semplicemente $\Bbbk^n$ e si dice lo spazio vettoriale standard (di dimensione n) sul corpo $\Bbbk$. La somma dei suoi elementi si definisce "componente per componente", cioè

$$\text{se } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ e } y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \text{ allora } x + y = \begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix}$$

e il prodotto per gli scalari si definisce analogamente

$$\text{se } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ e } \alpha \in \Bbbk \text{ allora } \alpha x = \begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{pmatrix} .$$

Si verifica subito che le condizioni della definizione sono tutte soddisfatte; in particolare lo zero di $V_n(\Bbbk)$ è la n-upla con tutte le componenti nulle (lo zero di $\Bbbk$).

1.2.2. Polinomi. L'insieme dei polinomi in una variabile X e coefficienti in $\Bbbk$ si indica con $\Bbbk[X]$ ed è dotato dalle usuali operazioni di una struttura di spazio vettoriale su $\Bbbk$: somma e prodotto per gli scalari sono definiti da

$$\text{se } P(X) = \sum_{i=0}^{n} \alpha_i X^i \text{ e } Q(X) = \sum_{i=0}^{m} \beta_i X^i \text{ allora } P(X) + Q(X) = \sum_{i=0}^{\max(n,m)} (\alpha_i + \beta_i) X^i$$

e

$$\text{se } P(X) = \sum_{i=0}^{n} \alpha_i X^i \text{ e } \alpha \in \Bbbk \text{ allora } \alpha P(X) = \sum_{i=0}^{n} \alpha\alpha_i X^i$$

(ove si intende $\alpha_i = 0$ se $i > n$ e $\beta_i = 0$ se $i > m$). Si verificano subito le proprietà richieste. Ricordiamo che nell'insieme dei polinomi è definito anche un prodotto tra polinomi e una operazione di composizione, ma per il momento non ce ne occuperemo.

Ricordiamo anche che si dice grado di un polinomio il massimo esponente della variabile che ha coefficiente non nullo: se $P(X) = \sum_{i=0}^{n} \alpha_i X^i$ allora $\deg P(X) = \max\{i : \alpha_i \neq 0\}$.

Si osservi che $\deg(P(X) + Q(X)) \leqslant \max(\deg P(X), \deg Q(X))$ e vale l'uguale se $\deg P(X) \neq \deg Q(X)$ (oppure se i polinomi hanno lo stesso grado e coefficienti del termine direttore non opposti).

1.2.3. Polinomi troncati. Il sottinsieme di $\Bbbk[X]$ formato dai polinomi di grado minore o uguale ad un fissato numero naturale n, dotato delle usuali operazioni di somma e prodotto per gli scalari, forma uno spazio vettoriale su $\Bbbk$ che verrà indicato con $\Bbbk[X]_{\leqslant n}$.

1.2.4. Serie formali. L'insieme delle serie in una variabile X e coefficienti in $\Bbbk$ si indica con $\Bbbk[[X]]$ ed è dotato dalle usuali operazioni di una struttura di spazio vettoriale su $\Bbbk$: somma e prodotto per gli scalari sono definiti esattamente come nel caso dei polinomi (le serie formali sono espressioni del tipo $P(X) = \sum_{i=0}^{\infty} \alpha_i X^i$ con i coefficienti $\alpha_i \in \Bbbk$, ma le operazioni sono definite sempre usando somma e prodotto del corpo $\Bbbk$). I polinomi sono le serie formali per cui i coefficienti sono "quasi tutti nulli", che significa tutti nulli tranne che per un numero finito di indici.

1.2.5. Funzioni reali. Consideriamo l'insieme delle funzioni reali di variabile reale. Anche in questo caso possiamo definire una struttura di spazio vettoriale nel modo seguente:

$$\text{se } f : \mathbb{R} \to \mathbb{R} \text{ e } g : \mathbb{R} \to \mathbb{R} \text{ allora } f + g : \mathbb{R} \to \mathbb{R} \text{ è data da } (f + g)(x) = f(x) + g(x)$$

e

$$\text{se } f : \mathbb{R} \to \mathbb{R} \text{ e } \alpha \in \mathbb{R} \text{ allora } \alpha f : \mathbb{R} \to \mathbb{R} \text{ è data da } (\alpha f)(x) = \alpha f(x) \ .$$

Di nuovo notiamo che l'insieme in questione è dotato di una struttura algebrica più ricca (ha anche operazioni di prodotto di funzioni e di composizione di funzioni), ma per il momento non ce ne occuperemo.

I sottinsiemi di questo spazio vettoriale dati dalle funzioni continue, derivabili, differenziabili fino ad un fissato ordine, periodiche di un fissato periodo, sono altrettanti esempi di spazi vettoriali reali.

1.2.6. Funzioni a valori in un corpo. Più generalmente, consideriamo l'insieme delle funzioni da un fissato insieme X in $\Bbbk$ (corpo). Anche in questo caso possiamo definire una struttura di spazio vettoriale su $\Bbbk$, sfruttando le operazioni di $\Bbbk$, nel modo seguente:

$$\text{se } f : X \to \Bbbk \text{ e } g : X \to \Bbbk \text{ allora } f + g : X \to \Bbbk \text{ è data da } (f + g)(x) = f(x) + g(x)$$

e

$$\text{se } f : X \to \Bbbk \text{ e } \alpha \in \mathbb{R} \text{ allora } \alpha f : X \to \Bbbk \text{ è data da } (\alpha f)(x) = \alpha f(x) \ .$$

Di nuovo notiamo che l'insieme in questione è dotato di una struttura algebrica più ricca (ha anche l'operazioni di prodotto di funzioni), ma per il momento non ce ne occuperemo.

Quali esempi precedenti sono casi particolari di questo? Se usiamo insiemi finiti del tipo $X = \{1, 2, \cdots, n\}$ si ottengono essenzialmente gli spazi vettoriali standard. Se usiamo come insieme $X = \mathbb{N}$ allora otteniamo un insieme in corrispondenza biunivoca con le serie formali. Per ottenere invece i polinomi bisogna considerare le funzioni di $\mathbb{N}$ in $\Bbbk$ che sono quasi ovunque nulle, cioè che sono nulle tranne che per un numero finito di indici.

Se usiamo insiemi finiti del tipo $X = \{1, 2, \cdots, n\} \times \{1, 2, \cdots, m\}$ si ottengono delle tabelle $n \times m$ di coefficienti in $\Bbbk$, e si chiamano matrici con n righe ed m colonne a coefficienti in $\Bbbk$, oppure matrici $n \times m$ in $\Bbbk$. Il caso $m = 1$ dà gli spazi vettoriali standard, il caso $n = 1$ dà uno spazio di vettori-riga o covettori, il caso $n = m$ dà le matrici quadrate, il caso $n = m = 1$ dà il campo di base.

Si generalizzi, parlando delle funzioni a valori in uno spazio vettoriale.

1.2.7. Numeri complessi come spazio vettoriale reale. Il corpo $\mathbb{C}$ dei numeri complessi può essere visto come spazio vettoriale su $\mathbb{R}$ tramite le usuali operazioni di somma di numeri complessi e prodotto di numeri reali con numeri complessi.

1.2.8. Esempio esoterico. Consideriamo come campo $\mathbb{R}$, come insieme $V = \mathbb{R}_{>0}$ (reali positivi) e come somma l'usuale prodotto in $\mathbb{R}_{>0}$, e come prodotto dello scalare $\alpha \in \mathbb{R}$ con il vettore $v \in \mathbb{R}_{>0}$ l'elevamento a potenza v^α (ben definito perché la base è reale positivo). Si tratta di una struttura di $\mathbb{R}$-spazio vettoriale su $V = \mathbb{R}_{>0}$.

1.2.9. Non-esempio. Consideriamo come campo $\mathbb{R}$, come insieme $V = \mathbb{R}$ (numeri reali) e come somma l'usuale somma in $\mathbb{R}$, e come prodotto dello scalare $\alpha \in \mathbb{R}$ con il vettore $v \in \mathbb{R}$ il valore $\alpha v := 0$ (sempre nullo). Non si tratta di una struttura di $\mathbb{R}$-spazio vettoriale su V, ma si noti che l'unica proprietà non verificata è l'unitarietà (tutte le altre sono banalmente verificate).

1.3. Spazi prodotto. Siano V e W spazi vettoriali sullo stesso corpo $\Bbbk$; il prodotto cartesiano $V \times W$ (l'insieme delle coppie ordinate (v, w) con $v \in V$ e $w \in W$) viene dotato della seguente

struttura di spazio vettoriale su $\Bbbk$, definita "componente per componente": somma $(v,w)+(v',w')=(v+v',w+w')$ e prodotto per scalari $\alpha(v,w)=(\alpha v,\alpha w)$. L'elemento neutro di $V\times W$ risulta subito essere $(0,0)=(0_V,0_W)$.

L'osservazione si generalizza ad un numero finito di spazi. Notare che gli spazi vettoriali standard sono esattamente il prodotto del corpo $\Bbbk$ con sé stesso n volte.

2. Sottospazi e quozienti.

2.1. Definizione (sottospazi). *Un sottinsieme W di uno spazio vettoriale V sul corpo $\Bbbk$ si dice un $\Bbbk$-sottospazio vettoriale (o solo sottospazio, se non ci sono ambiguità) se le operazioni di V inducono una struttura di spazio vettoriale su W.*

2.1.1. Esempio (sottospazio nullo). Il più piccolo sottospazio di V è l'insieme $\{0\}$ contenente solo lo zero. Spesso scriveremo semplicemente 0 per indicare anche il sottospazio nullo $\{0\}$.

2.1.2. Esempio. Il più grande sottospazio di V è l'insieme V stesso.

2.1.3. Esempio. Osservando gli esempi fondamentali, si vede che $\Bbbk[X]_{\leqslant n}$ è sottospazio di $\Bbbk[X]$, che a sua volta è sottospazio di $\Bbbk[[X]]$; lo spazio delle funzioni reali differenziabili è sottospazio di quello delle funzioni continue, che è sottospazio dello spazio di tutte le funzioni reali.

2.1.4. Esempio. L'insieme delle funzioni $X\to\Bbbk$ che valgono 0 in tutto un fissato sottinsieme (non vuoto) $Y\subseteq X$ è un sottospazio dello spazio delle funzioni di X in $\Bbbk$; invece l'insieme delle funzioni che valgono costantemente 1 su Y non è un sottospazio.

2.2. Proposizione (criteri per sottospazi). *Per un sottinsieme W di uno spazio vettoriale V, i fatti seguenti sono equivalenti:*
(1) *W è sottospazio vettoriale di V;*
(2) *valgono le seguenti asserzioni:*
  (*i*) *$0\in W$ (contiene lo zero);*
  (*ii*) *se $u,v\in W$ allora $u+v\in W$ (è chiuso rispetto alla somma);*
  (*iii*) *se $u\in W$ e $\alpha\in\Bbbk$ allora $\alpha u\in W$ (è chiuso rispetto al prodotto per gli scalari);*
(3) *valgono le seguenti asserzioni:*
  (*i*) *$W\neq\varnothing$ (non è vuoto);*
  (*ii*) *se $u,v\in W$ e $\alpha,\beta\in\Bbbk$ allora $\alpha u+\beta v\in W$ (contiene tutte le combinazioni lineari di ogni coppia di elementi).*
(4) *valgono le seguenti asserzioni:*
  (*i*) *$W\neq\varnothing$;*
  (*ii*) *se $u,v\in W$ e $\alpha\in\Bbbk$ allora $\alpha u+v\in W$.*

Dimostrazione. Sembra facile, ma invitiamo il lettore a capire bene "che cosa" bisogna dimostrare, esplicitando le implicazioni (1) implica (2) e (3), e le opposte (2) implica (1) e (3) implica (1), come pure le due implicazioni dirette tra (2) e (3). □

2.3. Definizione-Proposizione (combinazioni lineari). *Data una famiglia di vettori $v_i\in V$ ($i\in I$ insieme qualsiasi), per ogni famiglia di scalari $\alpha_i\in\Bbbk$ quasi tutti nulli (cioè $\alpha_i=0$ tranne che per un numero finito di indici $i\in I$), definiamo combinazione lineare (finita) dei v_i con coefficienti α_i la somma $\sum_I\alpha_i v_i$.*

Possiamo dire allora che un sottinsieme di uno spazio vettoriale è un sottospazio se e solo se è chiuso per combinazioni lineari finite (si osservi che per $I=\varnothing$ è "obbligatorio" definire che il valore della combinazione lineare è $0\in V$).

2.4. Definizione-Proposizione (sottospazio generato). *Se S è un sottinsieme qualsiasi di V, indichiamo con $\langle S\rangle$ il più piccolo sottospazio vettoriale di V contenente S. Esso ammette le due descrizioni seguenti:*
(1) *$\langle S\rangle$ è l'intersezione di tutti i sottospazi vettoriali di V contenenti S;*
(2) *$\langle S\rangle$ è l'insieme di tutte le combinazioni lineari (finite) di elementi di S a coefficienti in $\Bbbk$.*

Dimostrazione. La descrizione (1) è essenzialmente tautologica; l'unica cosa da notare è che l'intersezione di un numero arbitrario, non necessariamente finito, di sottospazi è un sottospazio.

Diciamo poi S' l'insieme descritto in (2); certo S' è un sottospazio (verificarlo), e $S' \supseteq S$, da cui $S' \supseteq \langle S \rangle$. Viceversa se W è qualunque sottospazio contenente S, allora $W \supseteq S'$, e passando alla intersezione di tutti questi sottospazi abbiamo $\langle S \rangle \supseteq S'$. Da cui segue $S' = \langle S \rangle$. □

2.4.1. Esempio (sottospazio nullo). $\langle \varnothing \rangle = \{0\}$, cioè l'insieme vuoto genera il sottospazio nullo di V, come pure $\langle 0 \rangle = \{0\}$.

2.4.2. Esempio (rette). Lo spazio vettoriale generato da un vettore non nullo v è l'insieme di tutti i multipli scalari di v, cioè $\langle v \rangle = \{\lambda v : \lambda \in \Bbbk\}$, e si dice una retta di V.

2.4.3. Esempio (piani). Lo spazio vettoriale generato da due vettori non nulli v e w è l'insieme di tutte le combinazioni lineari di v e w, cioè $\langle v, w \rangle = \{\lambda v + \mu w : \lambda, \mu \in \Bbbk\}$. Se i due vettori non sono proporzionali (cioè uno non è un multiplo dell'altro) si dice un piano di V. Cosa succede invece se w è multiplo di v?

2.4.4. Nota. In generale abbiamo le seguenti proprietà:
(*a*) $S \subseteq \langle S \rangle$, e si ha uguaglianza se e solo se S è un sottospazio;
(*b*) se $S_1 \subseteq S_2$ allora $\langle S_1 \rangle \subseteq \langle S_2 \rangle$;
(*c*) $\langle \langle S \rangle \rangle = \langle S \rangle$;
(*d*) $\langle S_1 \rangle \cap \langle S_2 \rangle \supseteq \langle S_1 \cap S_2 \rangle$ (l'uguaglianza in generale è falsa);
(*e*) $\langle S_1 \rangle \cup \langle S_2 \rangle \subseteq \langle S_1 \cup S_2 \rangle$ (l'uguaglianza in generale è falsa per un motivo ovvio, vedi sotto).

2.5. Intersezione e somma di sottospazi. Sia V uno spazio vettoriale su $\Bbbk$ e siano U_1, U_2 due suoi sottospazi. Allora:
(1) l'intersezione insiemistica $U_1 \cap U_2$ è un sottospazio vettoriale di V; è il più grande sottospazio di V contenuto sia in U_1 che in U_2.
(2) l'unione insiemistica $U_1 \cup U_2$ in generale *non* è un sottospazio vettoriale di V; farsi dei controesempi, e poi caratterizzare in generale i casi "fortunati": l'unione di due sottospazi è un sottospazio se e solo se uno dei due è contenuto nell'altro;
(3) in generale definiamo la somma $U_1 + U_2$ come il sottospazio generato dall'unione insiemistica di U_1 ed U_2, cioè $U_1 + U_2 = \langle U_1 \cup U_2 \rangle$. Si tratta del più piccolo sottospazio di V contenente sia U_1 che U_2.

Le considerazioni e le definizioni precedenti si possono estendere ad un numero finito di sottospazi.

2.5.1. Nota. In generale abbiamo $\langle S_1 \rangle + \langle S_2 \rangle = \langle S_1 \cup S_2 \rangle = \langle \langle S_1 \rangle \cup \langle S_2 \rangle \rangle$.

2.5.2. Mancata distributività. Si osservi che le due operazioni di intersezione e somma non si comportano in modo distributivo (come fanno per esempio intersezione e unione insiemistiche); precisamente, per ogni tre sottospazi U_1, U_2, U_3 abbiamo:
(1) $(U_1 \cap U_2) + U_3 \leqslant (U_1 + U_3) \cap (U_2 + U_3)$ e di solito la disuguaglianza è stretta (esempi?);
(2) $(U_1 + U_2) \cap U_3 \geqslant (U_1 \cap U_3) + (U_2 \cap U_3)$ e di solito la disuguaglianza è stretta (esempi?).

Per gli esempi, conviene considerare tre "rette per l'origine" nel piano $V_2(\Bbbk) = \Bbbk^2$. In che casi valgono invece le uguaglianze?

2.5.3. Il reticolo $\mathbb{P}(V)$. Usiamo il simbolo $\mathbb{P}(V)$ per indicare l'insieme di tutti i sottospazi vettoriali di V, mentre ricordiamo che $\mathscr{P}(V)$ è l'insieme di tutti i sottinsiemi di V, quindi $\mathbb{P}(V) \subseteq \mathscr{P}(V)$. Entrambi sono dotati di una relazione d'ordine (l'inclusione di sottinsiemi), entrambi sono dotati di massimo e minimo (ma i minimi sono diversi), inf e sup (ma i sup sono diversi), quindi di struttura di reticolo (ma uno è distributivo, l'altro no), e la generazione di sottospazi può essere vista come funzione

$$\mathscr{P}(V) \longrightarrow \mathbb{P}(V), \qquad S \mapsto \langle S \rangle$$

che rispetta l'ordine, ma non necessariamente le operazioni dei reticoli (rispetta il sup, ma non l'inf).

2.6. Somme dirette, sottospazi complementari. Se $U_1 + U_2 = V$ e $U_1 \cap U_2 = 0$ si dice che U_1 e U_2 sono complementari e si scrive $V = U_1 \oplus U_2$. Più in generale diremo che due sottospazi di V sono in somma diretta se la loro intersezione è nulla, e scriveremo $U_1 + U_2 = U_1 \oplus U_2$ (anche se la somma non è V).

Si osservi che: se $V = U_1 \oplus U_2$ allora ogni vettore $v \in V$ si scrive in modo unico come somma $v = u_1 + u_2$ con $u_1 \in U_1$ e $u_2 \in U_2$. Infatti, che si scriva come somma è chiaro dalla descrizione di $U_1 + U_2$, mentre l'unicità si controlla così: se abbiamo $v = u_1' + u_2'$ (con $u_1' \in U_1$ e $u_2' \in U_2$), allora da

$u_1 + u_2 = u_1' + u_2'$ troviamo $u_1 - u_1' = u_2' - u_2$ che è un vettore di $U_1 \cap U_2$ (il lato sinistro sta in U_1, quello destro in U_2), e quindi nullo, e si trova $u_1 = u_1'$ e $u_2' = u_2$.

2.6.1. Problema. Due sottospazi vettoriali U e W di V sono complementari, cioè $V = U \oplus W$; sia v un vettore non appartenente a $U \cup W$ (cioè non appartenente né a U né a W). Mostrare che: se $v = u + w$, con $u \in U$ e $w \in W$, allora l'intersezione di $U + \langle v \rangle$ e $W + \langle v \rangle$ contiene sia u che w.

2.7. Somme dirette di più sottospazi. Se $V_1, \dots, V_r$ sono sottospazi di V, diremo che essi sono in somma diretta, e scriveremo $V_1 + \cdots + V_r = V_1 \oplus \ldots + \oplus V_r$, estendendo per induzione la definizione precedente (attenzione: scrivere esplicitamente il caso $r = 3$, serve che il terzo sia in somma diretta con la somma dei primi due). Si faccia attenzione a questo: *$V_1, \dots, V_r$ sono in somma diretta se e solo se per ogni i si ha che V_i ha intersezione nulla con la somma degli altri V_j ($j \neq i$). Non basta che due a due abbiano intersezione nulla!*

Questa proprietà è equivalente al fatto che ogni vettore di V si scriva in modo unico come somma di vettori appartenente ai sottospazi $V_1, \dots, V_r$.

2.8. Spazi quoziente. Sia W un sottospazio vettoriale di V; allora la relazione "$u \sim v$ se e solo se $u - v \in W$" definisce una relazione di equivalenza in V che rispetta la struttura di spazio vettoriale, di modo che l'insieme quoziente $V/W := V/\sim$ ha una struttura canonica di spazio vettoriale indotta da quella di V. Gli elementi di V/W sono indicati di solito come $[v]$ oppure $v+W$. Quindi le operazioni si scrivono $[v]+[v'] = [v+v']$ (somma di classi) e $\alpha[v] = [\alpha v]$ (prodotto di una classe per uno scalare) e sono ben definite, ovvero non dipendono dai rappresentanti v e v' usati per le classi (verificare questa asserzione).

2.8.1. Gli elementi dello spazio quoziente V/W sono descritti come sottinsiemi di V da $[v] = v+W = \{v + w : w \in W\}$ al variare di $v \in V$, e possono essere pensati come "paralleli a W" (nessuno di loro è un sottospazio vettoriale, tranne W stesso che è l'unico contenente l'elemento nullo 0 di V, ma si noti che le classi laterali sono tutte "simili" tra loro).

2.8.2. Per l'immaginazione, si può vedere che gli elementi di V/W possono essere messi in corrispondenza biunivoca con i vettori di un qualsiasi sottospazio complementare di W in V. Cioè, se $V = U \oplus W$ allora vi è una biiezione canonica (che rispetta le operazioni di spazi vettoriali) tra U e V/W.

2.8.3. Problema. Abbiamo quindi visto che la relazione di equivalenza associata ad un sottospazio dà un quoziente che è dotato in modo canonico (e ben definito) di una struttura di spazio vettoriale indotta da V. Mostrare che, viceversa, se una relazione di equivalenza in V è tale che l'insieme quoziente abbia struttura di spazio vettoriale con le operazioni definite da quelle di V, allora si tratta della relazione di equivalenza associata ad un sottospazio (che si trova come l'insieme dei vettori equivalenti al vettore nullo).

3. Dipendenza e indipendenza lineari. Generatori.

Sia V spazio vettoriale sul campo $\Bbbk$.

3.1. Definizione (insiemi generatori). *Un sottinsieme S di V si dice un insieme di generatori per V (o che genera V) se $\langle S \rangle = V$, ovvero se ogni elemento $v \in V$ si può scrivere come combinazione lineare finita $v = \sum_{s \in S} \alpha_s s$ di elementi di S (con gli α_s quasi tutti nulli).*

3.1.1. Esempio. Ovviamente V genera sé stesso, ma noi siamo interessati a trovare sistemi di generatori il più piccoli possibile per uno spazio vettoriale. In particolare ci interessiamo a spazi finitamente generati, cioè che ammettono un insieme finito di generatori.

3.1.2. Esempio. Sovrainsiemi di insiemi generatori sono ancora generatori.

3.1.3. Ovviamente ogni sottinsieme S di V è generatore per $\langle S \rangle$.

3.2. Definizione (insiemi linearmente (in)dipendenti). *Sia $S \subseteq V$ un sottinsieme di uno spazio vettoriale; S si dice linearmente indipendente (o libero) se per ogni combinazione lineare $\sum_{s \in S} \alpha_s s$ (in cui quasi tutti gli α_s siano nulli) si ha che: $\sum_{s \in S} \alpha_s s = 0$ implica $\alpha_s = 0$ per ogni s.*

In caso contrario (esistono combinazioni lineari finite non banali che danno il vettore nullo) S si dice un insieme linearmente dipendente.

3.2.1. In altri termini questo significa che un insieme S è linearmente indipendente se (e solo se) il vettore nullo può essere scritto in un unico modo come combinazione lineare di elementi di S (quella avente tutti i coefficienti nulli). Questo è equivalente alle seguente asserzione: *un insieme S è linearmente indipendente se e solo se per ogni vettore di V che si esprima come combinazione lineare di elementi di S, tale combinazione è unica (cioè i coefficienti sono unicamente determinati dal vettore stesso).*

Infatti, se S è linearmente indipendente, e abbiamo che un vettore $v \in V$ si scrive $v = \sum_{s\in S} \alpha_s s$ e anche $v = \sum_{s\in S} \beta_s s$, allora risulta

$$0 = v - v = \sum_{s\in S} \alpha_s s - \sum_{s\in S} \beta_s s = \sum_{s\in S} (\alpha_s - \beta_s) s$$

da cui deduciamo $\alpha_s - \beta_s = 0$ per ogni $s \in S$, cioè $\alpha_s = \beta_s$ per ogni $s \in S$ (cioè i coefficienti erano gli stessi). Il viceversa è banale.

3.2.2. Esempio. Un insieme costituito da un solo vettore è linearmente dipendente se e solo se quel vettore è il vettore nullo. Un insieme contenente il vettore nullo è sempre linearmente dipendente; ovvero un insieme linearmente indipendente non può contenere il vettore nullo.

3.2.3. Esempio. Un insieme costituito da due vettori è linearmente dipendente se e solo se uno dei due è multiplo dell'altro.

3.2.4. Esempio. Quando un insieme costituito da tre vettori è linearmente dipendente?

3.2.5. Esempio. Un sottinsieme finito $v_1, \dots, v_n$ è linearmente indipendente se e solo se ognumo dei vettori v_i non appartiene al sottospazio $\langle v_1, \dots, v_{i-1} \rangle$ generato dai precedenti

3.2.6. Esempio. Sottoinsiemi di insiemi linearmente indipendenti sono ancora linearmente indipendenti. Sovrainsiemi di insiemi linearmente dipendenti sono ancora linearmente dipendenti.

3.3. Problema (proprietà fondamentale). *Un sottinsieme S è linearmente indipendente se e solo se per ogni $s \in S$ si ha $s \notin \langle S \smallsetminus \{s\} \rangle$.*

Per una verifica quasi immediata conviene vedere l'asserzione conversa: *un sottinsieme S è linearmente dipendente se e solo se esiste $s \in S$ tale che $s \in \langle S \smallsetminus \{s\} \rangle$.* Infatti, usando che nel campo $\Bbbk$ vi sono gli inversi, avere una combinazione lineare non banale che sia nulla è lo stesso che scrivere uno dei vettori come combinazione lineare degli altri.

3.4. Osservazione. Se si cerca di applicare queste definizioni ai sottospazi di V, si trova banalmente che i sottospazi sono sempre insiemi linearmente dipendenti (per esempio perché contengono il vettore nullo), e non sono mai generatori, a meno che non siano già tutto lo spazio.

3.5. Osservazione. Si faccia attenzione al fatto che la nozione di indipendenza lineare è una proprietà dell'insieme in questione, ed è difficile dedurla dai suoi sottinsiemi. Per esempio dati tre sottinsiemi A, B, C di uno spazio vettoriale, dai fatti che $A \cup B$ sia indipendente, e che $A \cup C$ sia indipendente non si può dedurre che $A \cup B \cup C$ sia indipendente (per esempio si usino tre vettori nel piano a due a due indipendenti: l'insieme formato dai tre vettori non può essere indipendente).

4. Basi e dimensione.

4.1. Definizione-Teorema (sistemi di generatori indipendenti). *I fatti seguenti sono equivalenti:*
(1) *S è un sistema di generatori linearmente indipendente;*
(2) *S è un insieme massimale di vettori linearmente indipendenti;*
(3) *S è un insieme minimale di generatori per V;*
(qui massimale e minimale si intende rispetto all'ordine dato dalle inclusioni come sottinsiemi di V). Ogni tale insieme S si dice una base di V.

Dimostrazione. È chiaro che (1) implica sia (2) (se si aggiunge un vettore ad un insieme di generatori, ovviamente si ottiene un insieme linearmente dipendente) che (3) (se si toglie un vettore ad un sistema linearmente indipendente, non può più essere un insieme di generatori).

Mostriamo che (2) implica (1): se S non fosse generatore, si potrebbe trovare $v \in V$ ma non in $\langle S \rangle$ e allora $S \cup \{v\}$ sarebbe linearmente indipendente contenente S, contro la massimalità di S.

Mostriamo che (3) implica (1): se S non fosse libero, si potrebbe trovare $v \in S$ con $v \in \langle S \smallsetminus \{v\}\rangle$ e allora $S \smallsetminus \{v\}$ sarebbe insieme generatore contenuto in S, contro la minimalità di S. □

4.2. Definizione-Teorema (basi e dimensione). *Tutte le basi di V sono di una fissata cardinalità, dipendente solo da V e da $\Bbbk$, che si chiama la dimensione di V su $\Bbbk$ e si indica con* $\dim_{\Bbbk} V$.

4.3. Teorema (esistenza di basi). *Ogni spazio vettoriale ammette (almeno) una base. Più precisamente:*
(1) *ogni insieme linearmente indipendente si può completare ad una base;*
(2) *ogni insieme generatore contiene almeno una base dello spazio.*

4.4. Questi due risultati insieme (esistenza di basi e costanza della loro cardinalità) sono spesso indicati come Teorema di struttura degli spazi vettoriali, perché dicono in sostanza che si può capire tutto di uno spazio vettoriale conoscendo la cardinalità di una qualunque sua base. In altri termini, due spazi vettoriali su uno stesso campo $\Bbbk$ sono isomorfi (cioè sono in biiezione tramite funzioni che rispettano le strutture algebriche) se e solo se hanno la stessa dimensione (vedremo meglio questo parlando di applicazioni lineari). O ancora, l'unico invariante di classificazione a meno di isomorfismi per gli spazi vettoriali su un campo $\Bbbk$ è la dimensione.

Questi due risultati si possono dimostrare in modo elementare per gli spazi finitamente generati, mentre si deve ricorrere al Lemma di Zorn nel caso di spazi vettoriali di dimensione arbitraria (non necessariamente finita).

4.5. Dimostrazione per spazi di dimensione finita. Supponiamo che V sia finitamente generato, ovvero ammetta un sistema di generatori formato da un numero finito di vettori.

4.5.1. Lemma (dello scambio). *Dati un insieme linearmente indipendente $S = \{s_1, \dots, s_k\}$ con k elementi e un insieme generatore $G = \{g_1, \dots, g_h\}$ con h elementi di V, si ha $k \leqslant h$.*

Dimostrazione. La strategia della dimostrazione consiste nel sostituire opportuni elementi di G con elementi di S, ottenendo sempre insiemi di generatori. Alla fine avremo inserito tutti gli elementi di S al posto di (altrettanti) elementi di G, da cui la conclusione che la cardinalità di S doveva essere minore o uguale a quella di G. Vediamo in dettaglio.

Essendo G un insieme generatore, abbiamo che $s_1 = \sum_{j=1}^{h} a_j g_j$ ove i coefficienti a_j non sono tutti nulli; eventualmente cambiando la numerazione possiamo supporre $a_1 \neq 0$. Allora l'insieme $G_1 = \{s_1, g_2, \dots, g_h\}$ è ancora un sistema di generatori (perché? da notare che bisogna usare $a_1 \neq 0$, e dunque a_1 ammette un inverso in $\Bbbk$).

Quindi possiamo procedere e scrivere $s_2 = b_1 s_1 + \sum_{j=2}^{h} b_j g_j$ ove i coefficienti b_j con $j \neq 1$ non sono tutti nulli (altrimenti s_1 e s_2 formerebbero un insieme dipendente) e possiamo supporre $b_2 \neq 0$. Allora l'insieme $G_2 = \{s_1, s_2, g_3, \dots, g_h\}$ è ancora un sistema di generatori (perché?).

Continuando in questo modo troviamo dopo k passi un insieme $G_k = \{s_1, s_2, , \dots, s_k, g_{k+1}, \dots, g_h\}$, da cui segue che $k \leqslant h$. □

4.5.2. Dimostrazione (dei Teoremi). Che tutte le basi abbiano la stessa cardinalità (numero di elementi) segue subito dal lemma (le basi sono sia insiemi linearmente indipendenti, sia sistemi di generatori, quindi due basi possono svolgere sia il ruolo di S che quello di G, dimostrando le due disuguaglianze).

Passiamo al teorema di esistenza:
(1) Dimostriamo un risultato più preciso (lemma di completamento): dato un insieme linearmente indipendente S e un fissato sistema (finito) G di generatori di V, si può completare S a una base di V aggiungendovi opportuni elementi di G.
Se $\langle S\rangle \supseteq G$ abbiamo finito. Altrimenti si comincia scegliendo un elemento g_1 di G che non appartenga al sottospazio $\langle S\rangle$; allora $S_1 = S \cup \{g_1\}$ è ancora linearmente indipendente (perché?). Di nuovo, se $\langle S_1\rangle \supseteq G$ abbiamo finito, altrimenti si sceglie un elemento g_2 di G che non appartenga al sottospazio $\langle S_1\rangle$; allora $S_2 = S_1 \cup \{g_2\}$ è ancora linearmente indipendente (perché?).
Procedendo così, dopo un numero finito p di passi (al più il numero di elementi di G) si ha che $\langle S_p\rangle \supseteq G$, e dunque S_p è un insieme (linearmente indipendente e) generatore.
(2) Dato un insieme generatore G, usiamo il procedimento precedente partendo con $S = \varnothing$, e si termina quando abbiamo trovato un numero di elementi di G (linearmente indipendenti e) pari alla dimensione dello spazio (lemma di estrazione).

Nota che se l'insieme di generatori fosse stato finito, si sarebbe potuto procedere anche al contrario: eliminando via via gli elementi linearmente dipendenti, fino ad ottenere un insieme di generatori indipendenti: descrivere bene il procedimento. □

4.5.3. Problema. Dal teorema fondamentale seguono subito alcune osservazioni utili e facili del tipo: se V è spazio vettoriale di dimensione finita n, allora
(1) ogni insieme di generatori ha almeno n elementi;
(2) ogni insieme linearmente indipendente ha al più n elementi;
(3) ogni insieme generatore formato da n elementi è una base;
(4) ogni insieme indipendente formato da n elementi è una base.
Quali di queste proprietà usano solo l'asserzione sulla cardinalità delle basi?

4.5.4. Problema. Sia V uno spazio vettoriale di dimensione finita, e sia W un suo sottospazio. Mostrare che $\dim_{\Bbbk} V = \dim_{\Bbbk} W$ implica che $V = W$.

Più in generale, siano W_1 e W_2 sottospazi vettoriali di dimensione finita di uno spazio vettoriale V (di dimensione arbitraria). Se $W_1 \subseteq W_2$ e $\dim_{\Bbbk} W_1 = \dim_{\Bbbk} W_2$ allora $W_1 = W_2$.

4.5.5. Problema. Due sottospazi vettoriali U e W di V (di dimensione finita) sono complementari, cioè $V = U \oplus W$; mostrare che la somma delle loro dimensioni dà la dimensione di V. Sia ora v un vettore non appartenente a $U \cup W$ (cioè non appartenente né a U né a W). Calcolare la dimensione dei sottospazi $U + \langle v \rangle$, $W + \langle v \rangle$ e della loro intersezione. *Nota: siccome $v = u + w$ con $u \in U$ e $w \in W$, linearmente indipendenti, si deduce che l'intersezione cercata ha dimensione, almeno, due.*

4.5.6. Spazi prodotto. Se V è spazio vettoriale su $\Bbbk$ di dimensione n con base $\mathscr{V} = \{v_1, \dots, v_n\}$, e W è spazio vettoriale su $\Bbbk$ di dimensione m con base $\mathscr{W} = \{w_1, \dots, w_m\}$, allora lo spazio prodotto $V \times W$ ha come base l'insieme delle coppie

$$\{(v_i, 0) : i = 1, \dots, n\} \cup \{(0, w_j) : j = 1, \dots .m\}$$

e dunque ha dimensione $n + m$ (verificare). In generale $\dim_{\Bbbk}(V \times W) = \dim_{\Bbbk} V + \dim_{\Bbbk} W$, cioè lo spazio prodotto ha dimensione pari alla somma delle dimensioni degli spazi dati.

Generalizzare l'esempio al prodotto di un numero finito di spazi vettoriali sullo stesso corpo $\Bbbk$.

4.5.7. Spazi quoziente. Se V è spazio vettoriale su $\Bbbk$ di dimensione n e W è sottospazio vettoriale di V di dimensione m (necessariamente $m \leqslant n$), verificare che lo spazio quoziente V/W ha dimensione $n - m$ (si cominci scegliendo una base per W e completandola ad una base di V; le classi degli elementi che si sono dovuti aggiungere costituiranno una base dello spazio quoziente). In generale $\dim_{\Bbbk}(V/W) = \dim_{\Bbbk} V - \dim_{\Bbbk} W$, cioè lo spazio quoziente ha dimensione pari alla differenza delle dimensioni dello spazio ambiente e del suo sottospazio.

4.5.8. Problema (operazioni elementari di Gauss sulle basi). Come si possono confrontare due basi diverse di uno stesso spazio vettoriale (di dimensione finita)? Definiamo le operazioni elementari di Gauss su una base (ordinata):
(1) scambiare di posto due elementi della base;
(2) sostituire un elemento della base con un suo multiplo scalare non nullo;
(3) sostituire un elemento della base con la somma di lui stesso e di un multiplo scalare di un altro elemento (della base).
Mostrare che:
(a) le operazioni elementari di Gauss danno un insieme di vettori che rimane base dello spazio vettoriale;
(b) date due basi qualsiasi dello spazio vettoriale, una può essere trasformata nell'altra tramite una sequenza finita di operazioni elementari di Gauss.

4.5.9. Problema. Perché questo tipo di risultati non può essere vero se non usiamo un campo come base? Esempi con $\Bbbk = \mathbb{Z}$, $V = \mathbb{Z}$:

$\{1\}$ è una base,

$\{2, 3\}$ è insieme generatore minimale ma non linearmente indipendente (perché $1 = (-1) \cdot 2 + (1) \cdot 3$ ma $0 = 3 \cdot 2 + (-2) \cdot 3$),

$\{2\}$ è un insieme linearmente indipendente massimale, ma non generatore.

♠♠ **4.6.** Dimostrazione per spazi di dimensione arbitraria. Conviene dare un risultato in un contesto un po' più generale, che si applica, oltre che alla discussione per gli spazi vettoriali, anche ad altri contesti in cui una "relazione di dipendenza" con certe proprietà si presenti (ad esempio la "dipendenza algebrica": un numero reale si dice algebrico se esso è radice di un polinomio a coefficienti razionali o, equivalentemente, interi).

I risultati e i metodi qui sviluppati non saranno usati nel seguito, e sono piuttosto difficili; quindi consigliamo di saltare direttamente alla prossima sezione, almeno in prima lettura.

4.6.1. Definizione (relazioni di dipendenza). *Sia A un insieme; una relazione $a \lessdot X$ tra elementi e sottinsiemi di A si dice di dipendenza se valgono i seguenti assiomi:*

($D1$) *se $x \in X$ allora $x \lessdot X$;*
($D2$) *se $z \lessdot Y$ e $Y \lessdot X$ (i.e. $y \lessdot X$ per ogni $y \in Y$) allora $z \lessdot X$;*
($D3$) *se $u \lessdot X \cup \{v\}$ e $u \not\lessdot X$ allora $v \lessdot X \cup \{u\}$;*
($D4$) *se $u \lessdot X$ allora esiste una parte finita X' di X tale che $u \lessdot X'$.*

4.6.2. Dipendenza lineare e dipendenza algebrica. Verificare che le seguenti due definizioni danno luogo a relazioni di dipendenza:

(a) sia V uno spazio vettoriale; per ogni $v \in V$ e X sottoinsieme di V definiamo "$v \lessdot X$ se e solo se $v \in \langle X \rangle$";
(b) sia K un corpo ed H un corpo contenente K; per ogni $\alpha \in H$ e ogni X sottoinsieme di H definiamo "$\alpha \lessdot X$ se e solo se α è zero di un polinomio a coefficienti in $K[X]$, o equivalentemente $K(X)$ (minimo sottocorpo di H contenente K e X)".

4.6.3. Definizione-Proposizione (insiemi generati, generatori). *Definiamo per ogni sottinsieme X di A l'insieme degli elementi dipendenti $\langle X \rangle = \{u \in A | u \lessdot X\}$. Per ogni X e Y risulta allora che:*

(1) *$X \subseteq \langle X \rangle$;*
(2) *se $X \subseteq Y$ allora $\langle X \rangle \subseteq \langle Y \rangle$;*
(3) *$\langle \langle X \rangle \rangle = \langle X \rangle$;*
(4) *$\langle X \cup Y \rangle = \langle \langle X \rangle \cup Y \rangle$ (ma $\langle X \cap Y \rangle$ in generale è strettamente contenuto in $\langle \langle X \rangle \cap \langle Y \rangle \rangle = \langle X \rangle \cap \langle Y \rangle$).*

Un sottinsieme X si dice insieme di generatori, o insieme generatore, per A se $\langle X \rangle = A$.

4.6.4. Definizione-Proposizione (insiemi chiusi). *Diciamo che un insieme è chiuso per la relazione se $\langle X \rangle = X$ (dunque se e solo se $\langle X \rangle \subseteq X$, cioè se $u \lessdot X$ implica $u \in X$). Allora:*

(1) *ogni $\langle X \rangle$ è chiuso per la relazione;*
(2) *se due insiemi sono chiusi per la relazione, anche la loro intersezione lo è (ma l'unione no, in generale);*
(3) *$\langle \varnothing \rangle$ è il minimo e A il massimo tra i chiusi per la relazione.*
(4) *La classe dei sottinsiemi di A chiusi per la relazione è un reticolo (non distributivo) con minimo e massimo sotto le operazioni di inf data da $X \wedge Y = X \cap Y$ e sup data da $X \vee Y = \langle X \cup Y \rangle$.*

Due insiemi X e Y chiusi per la relazione si dicono sghembi se $X \wedge Y = \langle \varnothing \rangle$.

4.6.5. Dipendenza lineare e dipendenza algebrica. Gli insiemi chiusi per la relazione di dipendenza lineare sono i sottospazi vettoriali di V; gli insiemi chiusi per la relazione di dipendenza algebrica sono i sovracorpi di K contenuti in H e algebricamente chiusi in H.

4.6.6. Definizione-Proposizione (insiemi irriducibili). *Un sottinsieme X si dice irriducibile se per ogni $x \in X$ si ha $x \not\lessdot X \smallsetminus \{x\}$, riducibile altrimenti. In particolare:*

(1) *il sottinsieme vuoto $\varnothing$ è irriducibile; un singoletto $\{x\}$ è riducibile sse $x \lessdot \varnothing$, sse $x \in \langle \varnothing \rangle$.*
(2) *Se X è irriducibile, e $X \cup \{u\}$ è riducibile, allora $u \lessdot X$.*
(3) *un insieme X è irriducibile se e solo se ogni suo sottinsieme finito lo è (equivalentemente, X è riducibile se e solo se contiene un insieme finito riducibile).*
(4) *Se X è irriducibile e $u \lessdot X$ allora la classe $\{Z \subseteq X | u \lessdot Z\}$ ha elemento minimo per l'inclusione che è un sottinsieme finito.*

4.6.7. Dipendenza lineare e dipendenza algebrica. Gli insiemi irriducibili per la relazione di dipendenza lineare sono i sottoinsiemi linearmente indipendenti di V; gli insiemi irriducibili per la relazione di dipendenza algebrica sono i sottoinsiemi (formati da elementi di H) trascendenti su K.

4.6.8. Definizione-Teorema (basi). *Un insieme irriducibile di generatori per A si dice una base di A (per la relazione di dipendenza). Sia Y un insieme di generatori per A; allora*
(1) *Y contiene (almeno) una base di A;*
(2) *se X è un sottinsieme irriducibile contenuto in Y, allora X è contenuto in qualche base di A contenuta in Y.*
(3) *Due qualsiasi basi di A sono equipotenti.*

Dimostrazione. Vedi Barsotti "Appunti di Algebra" lez. 36 (per questi risultati si usa il lemma di Zorn). □

4.6.9. Dipendenza lineare e dipendenza algebrica. Di conseguenza esistono basi per ogni spazio vettoriale V, e la loro cardinalità è costante; ed esistono basi di trascendenza di H su K, vale a dire insiemi X di trascendenti indipendenti su K tali che H è algebrico su $K(X)$, e la loro cardinalità è costante.

5. Relazione di Grassmann.

5.1. Teorema (formula di Grassmann). *Siano U_1 ed U_2 sottospazi vettoriali di V; vale la seguente relazione:*

$$\dim_{\Bbbk} U_1 + \dim_{\Bbbk} U_2 = \dim_{\Bbbk}(U_1 + U_2) + \dim_{\Bbbk}(U_1 \cap U_2) \ .$$

Dimostrazione. Scegliamo una base $\mathscr{U} = \{w_1, \dots, w_r\}$ di $U_1 \cap U_2$, e completiamola ad una base $\mathscr{U}_1 = \{w_1, \dots, w_r, u_1, \dots, u_{s_1}\}$ di U_1 e ad una base $\mathscr{U}_2 = \{w_1, \dots, w_r, v_1, \dots, v_{s_2}\}$ di U_2. Dunque con gli indici introdotti abbiamo che $\dim_{\Bbbk}(U_1 \cap U_2) = r$, $\dim_{\Bbbk} U_1 = r + s_1$ e $\dim_{\Bbbk} U_2 = r + s_2$. Di conseguenza basta dimostrare che $\dim_{\Bbbk}(U_1 + U_2) = r + s_1 + s_2$, e per far questo basta trovare una base di $U_1 + U_2$ con esattamente $r + s_1 + s_2$ elementi.

Verifichiamo che l'insieme

$$\mathscr{U}_1 \cup \mathscr{U}_2 = \{w_1, \dots, w_r, u_1, \dots, u_{s_1}, v_1, \dots, v_{s_2}\}$$

(che ha esattamente quel numero di elementi) è una base di $U_1 + U_2$. Che sia un insieme di generatori è quasi ovvio, vista la relazione $U_1 + U_2 = \langle \mathscr{U}_1 \cup \mathscr{U}_2 \rangle$, poiché $U_1 = \langle \mathscr{U}_1 \rangle$ e $U_2 = \langle \mathscr{U}_2 \rangle$.

Resta da verificare che si tratta di un insieme linearmente indipendente. Supponiamo

$$\alpha_1 w_1 + \cdots + \alpha_r w_r + \beta_1 u_1 + \cdots + \beta_{s_1} u_{s_1} + \gamma_1 v_1 + \cdots + \gamma_{s_2} v_{s_2} = 0$$

e vogliamo mostrare che tutti i coefficienti devono essere nulli. Scrivendo

$$\alpha_1 w_1 + \cdots + \alpha_r w_r + \beta_1 u_1 + \cdots + \beta_{s_1} u_{s_1} = -\gamma_1 v_1 - \cdots - \gamma_{s_2} v_{s_2}$$

vediamo che si tratta di un vettore in $U_1 \cap U_2$ (guardando il lato sinistro dell'uguaglianza vi vede che appartiene a U_1, e guardando il lato destro che appartiene a U_2). Allora deduciamo che esistono coefficienti $\delta_1, \dots, \delta_r$ tali che

$$\delta_1 w_1 + \cdots + \delta_r w_r = -\gamma_1 v_1 - \cdots - \gamma_{s_2} v_{s_2}$$

ovvero

$$\delta_1 w_1 + \cdots + \delta_r w_r + \gamma_1 v_1 + \cdots + \gamma_{s_2} v_{s_2} = 0$$

da cui abbiamo $\gamma_1 = \cdots = \gamma_{s_2} = 0$ trattandosi di una combinazione di elementi della base $\mathscr{U}_2$ (anche $\delta_1 = \cdots = \delta_r = 0$, ma non ci interessa). Tornando allora alla prima relazione abbiamo ora

$$\alpha_1 w_1 + \cdots + \alpha_r w_r + \beta_1 u_1 + \cdots + \beta_{s_1} u_{s_1} = 0$$

da cui infine $\alpha_1 = \cdots = \alpha_r = \beta_1 = \cdots = \beta_{s_1} = 0$ trattandosi di una combinazione di elementi della base $\mathscr{U}_1$. □

5.1.1. Esempio (intersezione di sottospazi). Una applicazione particolarmente interessante della formula di Grassmann è la seguente: se due sottospazi hanno dimensione "abbastanza grande", essi devono avere una intersezione non banale (cioè diversa dal solo vettore nullo). Per esempio:
(a) due sottospazi di dimensione 2 in uno spazio di dimensione 3 devono intersecarsi almeno in una retta;

(b) due sottospazi di dimensione 3 in uno spazio di dimensione 4 devono intersecarsi almeno in un piano;
(c) in generale, due sottospazi di dimensione m_1 ed m_2 in uno spazio di dimensione n devono intersecarsi in un sottospazio non banale se $m_1 + m_2 > n$, ed in tal caso la minima dimensione dello spazio intersezione è $m_1 + m_2 - n$.

5.1.2. Problema (somme dirette). Siano U_1 ed U_2 sottospazi vettoriali di V, e sia $W = U_1 + U_2$; i seguenti fatti sono equivalenti:
(1) $\dim_{\Bbbk}(U_1 + U_2) = \dim_{\Bbbk} U_1 + \dim_{\Bbbk} U_2$
(2) $U_1 \cap U_2 = 0$;
(3) $W = U_1 \oplus U_2$;
(4) ogni elemento $w \in W$ si scrive in modo unico come somma $u_1 + u_2$ con $u_1 \in U_1$ e $u_2 \in U_2$;
(5) se $u_1 + u_2 = 0$ con $u_1 \in U_1$ e $u_2 \in U_2$ allora $u_1 = 0 = u_2$.
Estendere l'enunciato al caso di r spazi in somma diretta (attenzione!).

5.1.3. Problema. Come si può generalizzare la formula di Grassmann avendo tre o più sottospazi? In particolare dare un controesempio alla seguente formula (falsa):

$$\begin{aligned}\dim_{\Bbbk}(U_1 + U_2 + U_3) \overset{!?}{=} {} & \dim_{\Bbbk} U_1 + \dim_{\Bbbk} U_2 + \dim_{\Bbbk} U_3 + \\ & - \dim_{\Bbbk}(U_1 \cap U_2) - \dim_{\Bbbk}(U_1 \cap U_3) - \dim_{\Bbbk}(U_2 \cap U_3) + \\ & + \dim_{\Bbbk}(U_1 \cap U_2 \cap U_3)\end{aligned}$$

(osservare invece che la formula diventa vera sostituendo "sottospazi vettoriali di un fissato spazio, dimensione, somma di sottospazi, intersezione" con "sottinsiemi finiti di un fissato insieme, cardinalità, unione, intersezione" rispettivamente: si tratta allora di una delle formule di inclusione-esclusione).

6. Coordinate (di vettori) ed equazioni (di sottospazi).

6.1. Definizione (coordinate dei vettori in una fissata base). *Sia V uno spazio vettoriale su $\Bbbk$ di dimensione n, e sia $\mathscr{V} = (v_1, \dots, v_n)$ una base ordinata di V. Allora per ogni $v \in V$ restano determinati unicamente gli scalari $\alpha_i \in \Bbbk$ tali che $v = \sum_i \alpha_i v_i$; la n-upla $\alpha_1, \dots, \alpha_n$ si dice n-upla delle coordinate di v nella base $\mathscr{V}$ e si scriverà in colonna:*

$$\alpha_{\mathscr{V}}(v) = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \qquad \text{se} \quad v = \sum_{i=1}^{n} \alpha_i v_i .$$

Di solito abuseremo della terminologia dicendo "base" invece di "base ordinata", se sarà chiaro dal contesto. Notare che il simbolo $\alpha_{\mathscr{V}}$ (coordinate nella base $\mathscr{V}$) può essere visto come una funzione biiettiva di V nello spazio vettoriale standard $V_n(\Bbbk)$.

6.1.1. Esempio. Si osservi che le coordinate di un vettore dipendono dalla base scelta per lo spazio vettoriale. Esistono vettori che hanno sempre le stesse coordinate in qualunque base? Fissato un vettore v, esiste sempre qualche base dello spazio in cui quel vettore ha coordinate $(1, 0, \dots, 0)$?

6.2. Esempi. Ritorniamo agli esempi fondamentali di spazi vettoriali.

6.2.1. Spazi vettoriali standard. Si dice base canonica di $\Bbbk^n$ l'insieme ordinato

$$\mathscr{E} = (e_1, \cdots, e_n) \text{ ove } \; e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \; e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \; \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

ovvero e_i è la n-upla che ha 1 come i-sima componente e 0 altrove. In particolare lo spazio vettoriale standard $\Bbbk^n$ ha dimensione n. In questa base, le coordinate di un vettore v sono esattamente le sue componenti numeriche; infatti

$$\text{se } v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, \text{ allora } \quad v = v_1 e_1 + v_2 e_2 + \cdots + v_n e_n \; .$$

Detto $u = e_1 + \cdots + e_n$ (vettore le cui coordinate in base canonica sono tutte 1), verificare che anche l'insieme

$$\mathscr{F} = (u - e_1, \cdots, u - e_n)$$

è una base ordinata di $\Bbbk^n$; trovare le coordinate di u in questa base, e più generalmente trovare le coordinate nella base $\mathscr{F}$ del vettore di coordinate $x_1, \ldots, x_n$ nella base $\mathscr{E}$.

6.2.2. Polinomi. Il principio di uguaglianza tra polinomi (due polinomi sono uguali se e solo se i coefficienti di potenze omologhe della variabile sono uguali; ovvero un polinomio è nullo se e solo se tutti i suoi coefficienti sono nulli) dice che l'insieme

$$\mathscr{X} = \{1, X, X^2, X^3, \ldots, X^n, \ldots\}$$

è un insieme linearmente indipendente, ed in effetti è una base per lo spazio vetoriale $\Bbbk[X]$ dei polinomi; dunque si tratta di uno spazio vettoriale di dimensione infinita (numerabile). In questa base, le coordinate di un polinomio sono esattamente i suoi coefficienti.

Si consideri l'insieme

$$\mathscr{Y} = \{1, 1+X, 1+X+X^2, 1+X+X^2+X^3, \ldots, \sum_{i=0}^{n} X^n, \ldots\}$$

e si dimostri che si tratta di una base per lo spazio dei polinomi; si esprimano in questa base le coordinate di un polinomio $P(X) = \sum_{i=0}^{n} \alpha_n X^n$ in funzione dei suoi coefficienti α_n.

6.2.3. Polinomi troncati. Una base per lo spazio $\Bbbk[X]_{\leqslant n}$ dei polinomi troncati all'ordine n è l'insieme

$$\mathscr{X}_n = \{1, X, X^2, X^3, \ldots, X^n\}$$

da cui si deduce che questo spazio ha dimensione $n + 1$.

Esistono basi di $\Bbbk[X]_{\leqslant n}$ fatte di polinomi di grado (tutti) esattamente n? Se sì, scriverne almeno due, ed esprimere in termini di quelle basi le coordinate di un generico polinomio troncato.

È vero che in ogni base deve esistere almeno un polinomio di grado n? E di grado i per $i < n$?

•• (metodo di) Interpolazione di Lagrange:
dati $\lambda_0, \lambda_1, \ldots, \lambda_n \in \Bbbk$ distinti, esistono $f_0(X), f_1(X), \ldots, f_n(X) \in \Bbbk[X]$ di grado esattamente n, che costituiscono una base di $\Bbbk[X]_{\leqslant n}$ tali che $f_i(\lambda_j) = \delta_{i,j}$ (delta di Kronecker: vale 1 se $i = j$, 0 altrimenti).

Infatti basta usare $f_i(X) = \prod_{j \neq i} \frac{X - \lambda_j}{\lambda_i - \lambda_j}$. Come verificarne l'indipendenza?

Si osservi inoltre che la somma degli $f_i(X)$ dà 1, mentre la somma dei $\lambda_i f_i(X)$ dà X: $\sum_i f_i(X) = 1$ e $\sum_i \lambda_i f_i(X) = X$. Da questo è immediato dedurre per ogni $f(X) \in \Bbbk[X]_{\leqslant n}$ la scrittura come combinazione lineare $f(X) = \sum_i c_i f_i(X)$; infatti si trova $c_i = f(\lambda_i)$.

6.2.4. Serie formali. Poiché le serie formali contengono un sottospazio di dimensione infinita (quello dei polinomi), si tratta di uno spazio di dimensioni infinita, e in realtà più che numerabile. Per studiare questo tipo di spazi vettoriali bisogna considerarne anche altre strutture (quelle topologiche in particolare). Scriverne esplicitamente una base è al di fuori delle nostre attuali possibilità.

6.2.5. Funzioni reali. Lo spazio delle funzioni continue di $\mathbb{R}$ in sè contiene il sottospazio delle funzioni polinomiali; quindi necessariamente è di dimensione infinita. In effetti la sua dimensione è più che numerabile, e scriverne una base è al di fuori delle nostre attuali possibilità.

6.2.6. Funzioni a valori in un corpo. Lo spazio delle funzioni di un insieme X in $\Bbbk$ è di dimensione finita se e solo se X è un insieme finito, ed in tal caso è pari al numero di elementi di X (scrivere esplicitamente una base). Altrimenti, se X è infinito, questo spazio contiene un sottospazio (dato dalle funzioni che si annullano su "quasi ogni" elemento di X) che è di dimensione infinita, pari alla cardinalità di X.

In generale, l'insieme delle funzioni di X (insieme finito) a valori in V (spazio vettoriale), con la naturale struttura di spazio vettoriale, ha dimensione $|X| \dim_{\Bbbk} V$.

6.2.7. Spazi vettoriali reali e complessi. Il corpo $\mathbb{C}$ dei numeri complessi ha dimensione 2 come spazio vettoriale su $\mathbb{R}$; infatti l'insieme $\{1, i\}$ è una base di $\mathbb{C}$ su $\mathbb{R}$: ogni numero complesso z si scrive unicamente come somma $a + ib$ con $a, b \in \mathbb{R}$.

Anche l'insieme $\{1 + i, 1 - i\}$ è base di $\mathbb{C}$ su $\mathbb{R}$; dimostrarlo e calcolare le coordinate del numero complesso $z = a + ib$ in questa nuova base.

Consideriamo ora uno spazio vettoriale V su $\mathbb{C}$, di dimensione n e base $\mathscr{V} = \{v_1, \dots, v_n\}$. Allora V è uno spazio vettoriale su $\mathbb{R}$ (restringendo il prodotto per gli scalari ai numeri reali), di base $\mathscr{V}' = \{v_1, iv_1 \dots, v_n, iv_n\}$, e dunque di dimensione $2n$ su $\mathbb{R}$ (verificare). Dunque per ogni spazio vettoriale complesso V, si ha $\dim_{\mathbb{R}} V = 2 \dim_{\mathbb{C}} V$.

6.3. Descrizione di sottospazi. Vi sono essenzialmente tre modi per descrivere i sottospazi W di un fissato spazio vettoriale V; l'unico visto finora essenzialmente è tramite generatori, possibilmente linearmente indipendenti:

6.3.1. Descrizione tramite generatori. Sia V uno spazio vettoriale di dimensione n, e W un suo sottospazio di dimensione m. Allora W ammette una base formata da esattamente m vettori, siano $w_1, \dots, w_m$, e si può descivere come $W = \langle w_1, \dots, w_m \rangle$, ovvero come l'insieme di tutti i vettori w di V che si scrivono come combinazione

$$w = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_m w_m$$

con i coefficienti $\alpha_1, \alpha_2, \dots, \alpha_m$ in $\Bbbk$:

$$W = \left\{ \sum\nolimits_{i=1}^{m} \alpha_i w_i \mid \alpha_i \in \Bbbk,\ \forall i \right\} .$$

Nel caso di spazi vettoriali di dimensione finita, fissata una base di V e considerando le relative coordinate, abbiamo altri due possibili descrizioni del sottospazio W:

6.3.2. Descrizione tramite equazioni parametriche. Siano

$$\alpha_{\mathscr{V}}(w_1) = \begin{pmatrix} w_{1,1} \\ w_{2,1} \\ \vdots \\ w_{n,1} \end{pmatrix}, \alpha_{\mathscr{V}}(w_2) = \begin{pmatrix} w_{1,2} \\ w_{2,2} \\ \vdots \\ w_{n,2} \end{pmatrix}, \dots, \alpha_{\mathscr{V}}(w_3) = \begin{pmatrix} w_{1,m} \\ w_{2,m} \\ \vdots \\ w_{n,m} \end{pmatrix}$$

le coordinate dei vettori $w_1, \dots, w_m$ nella base scelta $\mathscr{V}$ di V; allora possiamo descivere il sottospazio W come l'insieme dei vettori w di V le cui coordinate nella base scelta si scrivono

$$\begin{cases} x_1 = \alpha_1 w_{1,1} + \alpha_2 w_{1,2} + \ldots + \alpha_m w_{1,m} \\ x_2 = \alpha_1 w_{2,1} + \alpha_2 w_{2,2} + \ldots + \alpha_m w_{2,m} \\ \quad \vdots \\ x_n = \alpha_1 w_{n,1} + \alpha_2 w_{n,2} + \ldots + \alpha_m w_{n,m} \end{cases}$$

al variare dei coefficienti $\alpha_1, \alpha_2, \dots, \alpha_m \in \Bbbk$. Queste espressioni si dicono equazioni parametriche per W, e gli α_i si dicono i parametri.

Dato un tale sistema di equazioni parametriche, è immediato ritrovare un sistema di generatori per W, che risulta una base se il numero di parametri era pari alla dimensione di W.

6.3.3. Descrizione tramite equazioni cartesiane. Dalle equazioni parametriche si può procedere con il metodo di "eliminazione dei parametri": si ricava un parametro dalla prima equazione (eventualmente cambiando l'ordine delle equazioni) e lo sostituisce nelle altre; gettando via la prima equazione si ottiene un sistema con una equazione in meno e un parametro in meno. Ripetendo il processo per tutti i parametri si ottiene un sistema di $n - m$ equazioni (lineari omogenee) nelle coordinate $x_1, x_2, \dots, x_n$ che descrive la sottovarietà W. Queste si dicono equazioni cartesiane per W.

Dato un tale sistema di equazioni cartesiane (lineari omogenee), si può risalire ad una descrizione parametrica, o tramite generatori, del sottospazio "risolvendo il sistema", ovvero esplicitando quali sono tutte e sole le n-uple di coordinate che soddisfano a quel sistema.

6.3.4. Relazioni tra numero di generatori indipendenti, di parametri e di equazioni cartesiane. Seguendo bene i passaggi appena fatti si vede che la dimensione di W corrisponde al numero minimo di generatori necessario per descrivere il sottospazio, e anche al minimo numero di parametri necessari per le equazioni parametriche. Lo stesso spazio W è invece descritto da equazioni cartesiane in numero minimo di $n - m$; questo numero viene spesso indicato come la codimensione di W in V (dipende da V, W e dal corpo $\Bbbk$).

6.3.5. Esempi. Se V è spazio vettoriale di dimensione n, allora:

(0) per descrivere il sottospazio nullo servono 0 generatori, 0 parametri, ovvero n equazioni (indipendenti); si ricordi che $\langle \varnothing \rangle = \langle 0 \rangle = \{0\}$, e che il vuoto $\varnothing$ è base del sottospazio nullo.

(1) per descrivere una retta serve un generatore (non nullo), un parametro, ovvero $n-1$ equazioni (indipendenti);
(2) per descrivere un piano servono due generatori (linearmente indipendenti), due parametri, ovvero $n-2$ equazioni (indipendenti);
(3) per descrivere uno spazio (tridimensionale) servono tre generatori (linearmente indipendenti), tre parametri, ovvero $n-3$ equazioni (indipendenti).

Si dice iperpiano invece un sottospazio definito da una equazione cartesiana, per descrivere il quale servono dunque $n-1$ generatori (indipendenti), ovvero un sistema parametrico con $n-1$ parametri.

7. Esercizi.

7.0. Consideriamo un primo p in $\mathbb{Z}$ e una sua potenza $q = p^r$ (si può pensare $r = 1$, cioè $q = p$ per semplicità). Sappiamo che esiste un (unico) campo finito $\mathbb{F}_q$ che ha esattamente q elementi ed è un campo di caratteristica p (cioè l'unico morfismo di anelli da $\mathbb{Z}$ ha come nucleo l'ideale generato da p, ovvero $\mathbb{F}_q$ contiene $\mathbb{F}_p$, o meglio una copia isomorfa).

Mostrare che $\mathbb{F}_q$ è spazio vettoriale su $\mathbb{F}_p$ di dimensione r. Se $q' = p^{r'}$, quando $\mathbb{F}_q$ è spazio vettoriale su $\mathbb{F}_{q'}$?

Consideriamo ora lo spazio vettoriale standard $V = V_n(\mathbb{F}_q)$ di dimensione n su $\mathbb{F}_q$. Contare gli elementi rilevanti di V, in particolare:
(a) quanti vettori ci sono in V?
(b) quante basi (ordinate) ci sono in V?
(c) per ogni intero m fino a n: quanti sottospazi di dimensione m vi sono in V?
(d) quante coppie di sottospazi complementari ci sono in V?

Se possibile fare dei disegni che illustrino il conteggio nei casi $p = 2, 3, 5$ con $r = 1, 2$.

7.1. Nel piano $\mathbb{R}^2$ consideriamo i vettori $v = \left(\begin{smallmatrix}1\\2\end{smallmatrix}\right)$ e $w = \left(\begin{smallmatrix}-1\\1\end{smallmatrix}\right)$.
(a) mostrare che ogni vettore $x = \left(\begin{smallmatrix}x_1\\x_2\end{smallmatrix}\right)$ del piano si scrive in modo unico come combinazione lineare $x = \alpha v + \beta w$ (determinare i numeri reali α e β in funzione di x_1 ed x_2);
(b) disegnare e caratterizzare (tramite equazioni o disequazioni) i sottoinsiemi di $\mathbb{R}^2$ formati dagli estremi finali dei vettori del tipo $\alpha v + \beta w$ ove α e β sono numeri reali soggetti alle seguenti condizioni:
(C) $\alpha, \beta \in [0, \infty)$
(R) $\alpha + \beta = 1$
(S) $\alpha + \beta = 1$ con $\alpha, \beta \in [0, 1]$
(P) $\alpha, \beta \in [0, 1]$
(T) $\alpha + \beta \leqslant 1$ con $\alpha, \beta \in [0, 1]$
(X) $\alpha + \beta \leqslant 1$.
(c) specificare le relazioni di inclusione tra gli insiemi precedenti.

7.2. Nello spazio $\mathbb{R}^3$ consideriamo i vettori $v = \left(\begin{smallmatrix}1\\2\\0\end{smallmatrix}\right)$ e $w = \left(\begin{smallmatrix}-1\\-1\\2\end{smallmatrix}\right)$.
(a) mostrare che un vettore $x = \left(\begin{smallmatrix}x_1\\x_2\\x_3\end{smallmatrix}\right)$ appartiene al piano generato da v e w se e solo se vale la relazione $4x_1 - 2x_2 + x_3 = 0$;
(b) descrivere i sottoinsiemi analoghi a quelli dell'esercizio precedente.

7.3. Nello spazio $\mathbb{R}^3$ consideriamo i vettori $u = \left(\begin{smallmatrix}1\\0\\1\end{smallmatrix}\right)$ $v = \left(\begin{smallmatrix}1\\2\\0\end{smallmatrix}\right)$ e $w = \left(\begin{smallmatrix}-1\\1\\2\end{smallmatrix}\right)$.
(a) verificare che sono linearmente indipendenti e risolvere in α, β, γ la relazione $x = \alpha u + \beta v + \gamma w$ per un vettore $x = \left(\begin{smallmatrix}x_1\\x_2\\x_3\end{smallmatrix}\right)$ generico;
(b) disegnare e caratterizzare (tramite equazioni o disequazioni) i sottoinsiemi di $\mathbb{R}^3$ formati dagli estremi finali dei vettori del tipo $\alpha u + \beta v + \gamma w$ ove α, β e γ sono numeri reali soggetti alle seguenti condizioni:
(C) $\alpha, \beta, \gamma \in [0, \infty)$
(Pi) $\alpha + \beta + \gamma = 1$
(Tr) $\alpha + \beta + \gamma = 1$ con $\alpha, \beta, \gamma \in [0, 1]$

(Pa) $\alpha, \beta, \gamma \in [0,1]$
(Te) $\alpha + \beta + \gamma \leqslant 1$ con $\alpha, \beta, \gamma \in [0,1]$
(X) $\alpha + \beta + \gamma \leqslant 1$.
(c) specificare le relazioni di inclusione tra gli insiemi precedenti.

7.4. Verificare che l'insieme dei vettori $u = \binom{1}{2}$, $v = \binom{1}{-1}$, $w = \binom{0}{-1}$ e $z = \binom{-2}{2}$ di $\mathbb{R}^2$ è generatore, ed estrarne tutte le basi possibili di $\mathbb{R}^2$.

7.5. Verificare che l'insieme dei vettori $u = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $v = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$, $w = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$, e $z = \begin{pmatrix} -1 \\ 2 \\ -2 \end{pmatrix}$ di $\mathbb{R}^3$ è generatore, ed estrarne tutte le basi possibili di $\mathbb{R}^3$.

7.6. Descrivere tramite equazioni il sottospazio di $\mathbb{R}^4$ generato dai vettori $u = \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \end{pmatrix}$, $v = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}$, $w = \begin{pmatrix} 0 \\ -1 \\ 1 \\ 1 \end{pmatrix}$ (sono linearmente indipendenti?), e poi completare quest'insieme ad una base di $\mathbb{R}^4$.

7.7. Verificare che i sottinsiemi di $\mathbb{R}^4$ formati dai vettori $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ soddisfacenti alle condizioni $x_1 - x_4 = 0 = x_1 + x_2$ (sia U) e $x_3 - x_4 = 0 = x_2 + x_3$ (sia V) sono sottospazi vettoriali, trovarne la dimensione evidenziando delle basi; calcolare poi l'intersezione trovandone una base. Trovare le equazioni del più piccolo sottospazio vettoriale di $\mathbb{R}^4$ contenente sia U che V.

7.8. Siano v e w due vettori non nulli di uno spazio vettoriale V. Sotto quali condizioni i vettori v e $\alpha v + \beta w$ sono linearmente indipendenti?

7.9. Consideriamo lo spazio vettoriale reale delle applicazioni continue di $\mathbb{R}$ in sè.
(a) vero che l'insieme formato dalle tre funzioni 1 (funzione costante), $\sin^2$ e $\cos^2$ è linearmente dipendente?
(b) si consideri l'insieme $\{\sin(nx) : n \in \mathbb{N},\ n \neq 0\} \cup \{\cos(nx) : n \in \mathbb{N}\}$ e si dimostri che è un insieme linearmente indipendente;
(c) cosa dire dell'insieme $\{\sin(\alpha + nx) : n \in \mathbb{N},\ n \neq 0,\ \alpha \in \mathbb{R}\}$?

7.10. Sia $V = \Bbbk[X]_{\leqslant 4}$ lo spazio vettoriale su $\Bbbk$ dei polinomi di grado minore o uguale a 4.
(a) qual è la dimensione di V su $\Bbbk$?
(b) esistono basi di V i cui elementi siano polinomi di grado 4?
(c) esistono basi di V i cui elementi siano polinomi di grado minore o uguale a 3?
(d) esistono basi di V i cui elementi siano polinomi privi di termine noto?

7.11. Si determini se i sottoinsiemi di $\mathbb{R}^3$ formati dai vettori $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ soddisfacenti alle condizioni seguenti siano o meno sottospazi di $\mathbb{R}^3$:
(a) $x_1^2 + x_2^2 = x_3$
(b) $|x_1| = |x_2|$
(c) $x_1 + x_2 = x_3$
(d) $x_1 x_2 + x_2 x_3 = 0$
(e) $x_1 + x_2 - x_3 + 1 = 0$
(f) $x_1 - x_2^2 = 0$ e $x_1 = 0$
(g) $x_1 - x_2 x_3 = 0$ e $x_1 = 0$
In ciascuno dei casi, cercare di disegnare l'insieme in questione.

7.12. Calcolare somma, intersezione (evidenziando basi e dimensioni) per i seguenti sottospazi di $\mathbb{R}^4$:
(a) $V = \langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \rangle$ e $W = \langle \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rangle$.
(b) $V = \langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rangle$ e $W = \langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \rangle$.

7.13. Sia $V = \Bbbk[X]_{\leqslant 4}$ lo spazio vettoriale su $\Bbbk$ dei polinomi di grado minore o uguale a 4. Consideriamo i seguenti sottinsiemi:

$$V_s = \{f \in V : f(X) = f(-X)\} \qquad \text{e} \qquad V_a = \{f \in V : f(X) = -f(-X)\}\ .$$

(a) mostrare che V_s e V_a sono sottospazi, trovarne delle basi e le dimensioni;

(b) è vero che $V = V_s \oplus V_a$?
(c) generalizzare sostituendo 4 con n generico.

7.14. Come l'esercizio precedente usando i sottoinsiemi $U = \{f \in V : f(X) = f(1-X)\}$ e $W = \{f \in V : f(X) = -f(1-X)\}$.

7.15. Qual è la minima dimensione di uno spazio vettoriale V tale che due suoi sottospazi di dimensione m_1 ed m_2 si intersecano solo nel vettore nullo? Dare degli esempi per $m_1, m_2 = 1, 2, 3, 4$.

7.16. Qual è la massima dimensione di uno spazio vettoriale V tale che due suoi sottospazi di dimensione m_1 ed m_2 hanno intersezione sempre non banale? Dare degli esempi per $m_1, m_2 = 1, 2, 3, 4$.

7.17. Sia $Q(X) = c(X-\alpha_1)^{m_1} \cdots (X-\alpha_r)^{m_r}$ un polinomio di grado $n = \sum_{i=1}^{r} m_i$ in $V = \Bbbk[X]$ e consideriamo l'insieme

$$V_Q = \left\{ \frac{P(X)}{Q(X)} : P(X) \in V \text{ con } \deg P(X) < n \right\}$$

(a) mostrare che V_Q è spazio vettoriale su $\Bbbk$ di dimensione n;
(b) mostrare che l'insieme $\left\{ \frac{1}{(X-\alpha_i)^{j_i}} : j_i = 1, \dots, m_i \text{ e } i = 1, \dots, r \right\}$ è una base di V_Q su $\Bbbk$.

7.18. Siano u, v, w e z quattro vettori in $\mathbb{R}^n$ tali che i loro estremi siano i quattro punti consecutivi di un parallelogramma.
(a) interpretare la condizione data in termini dei vettori;
(b) mostrare che $(v-u) - (w-u) + (z-u) = 0$;
(c) verificare che $u + \frac{1}{2}(w-u) = v + \frac{1}{2}(z-v)$ e dare l'interpretazione geometrica dell'uguaglianza.

7.19. Si consideri l'insieme $\mathbb{R}_{>0}$ dei numeri reali strettamente positivi, dotato delle seguenti operazioni: la "somma" di due numeri sia il loro prodotto, il prodotto scalare del reale $\alpha \in \mathbb{R}$ per l'elemento $r \in \mathbb{R}_{>0}$ sia r^α. Dimostrare che $\mathbb{R}_{>0}$ con queste operazioni è uno spazio vettoriale reale il cui vettore nullo è 1. Qual'è la sua dimensione?

7.20. Trasporto di struttura via biiezioni. Se V è spazio vettoriale su $\Bbbk$, e $\varphi : V \longrightarrow S$ è una biiezione insiemistica tra V e un insieme S, con inversa $\psi : S \longrightarrow V$, allora le due posizioni $\alpha \cdot s := \varphi(\alpha\psi(s))$ e $s + s' := \varphi(\psi(s) + \psi(s'))$ (per ogni $\alpha \in \Bbbk$, $s, s' \in S$) danno ad S una struttura di spazio vettoriale su $\Bbbk$. Chi è l'elemento neutro? Qual'è la dimensione di S su $\Bbbk$?

Esplicitare la costruzione nei casi di $\exp : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ (funzione esponenziale), $\operatorname{arctg} : \mathbb{R} \longrightarrow]-\pi, \pi[$ (funzione arcotangente), $\pi : \mathbb{R} \longrightarrow \mathbb{R}$ (funzione "moltiplicazione per π").

Capitolo II

Applicazioni Lineari e Matrici

Uno dei punti fondamentali della Matematica è il fatto di considerare ogni qual volta si definisca un qualche tipo di oggetto anche le funzioni che in qualche senso rispettano la struttura di quel tipo di oggetti. Se tra due insiemi consideriamo funzioni di qualsiasi tipo, tra insiemi dotati di qualche struttura algebrica considereremo solo funzioni che rispettano in qualche senso più o meno forte quelle strutture. Così, tra gruppi consideriamo solo omomorfismi di gruppo, tra anelli solo omomorfismi di anello, tra corpi solo omomorfismi di corpo, tra spazi vettoriali (su uno stesso corpo) solo applicazioni lineari - almeno per il momento.

Il punto fondamentale è che il dato di una applicazione lineare tra spazi vettoriali di dimensione finita è completamente determinato da un insieme finito di dati (le immagini dei vettori di una base), che si possono organizzare in una "matrice" che descrive completamente l'applicazione. Il calcolo matriciale che ne risulta viene definito in modo che le operazioni tra matrici corrispondano alle operazioni tra le applicazioni lineari corrispondenti.

L'esigenza di scegliere basi degli spazi vettoriali per poter usare il cacolo matriciale comporta di dover capire come questo calcolo cambia variando la scelta delle basi; le matrici di cambiamento di base rispondono a questi problemi. Si tenga presente che la scelta di una base in uno spazio vettoriale è spesso del tutto arbitraria, mentre i problemi di tipo geometrico e le loro soluzioni devono essere intrinseci e non devono dipendere da scelte arbitrarie; d'altra parte è chiaro che ogni problema potrà avere una espressione matriciale più semplice in una base opportunamente scelta. È quindi fondamentale sapere come cambia l'espressione matriciale di un dato o di un problema variando la scelta delle basi coinvolte.

1. Applicazioni lineari.

1.1. Definizione (Applicazioni lineari). *Siano V e W spazi vettoriali su un corpo $\Bbbk$. Una applicazione $\varphi : V \longrightarrow W$ si dice lineare se soddisfa alle seguenti condizioni:*

$(L1)$ $\varphi(u+v)=\varphi(u)+\varphi(v)$ $(\forall u, v \in V)$;

$(L2)$ $\varphi(\alpha v)=\alpha\varphi(v)$ $(\forall v \in V, \forall \alpha \in \Bbbk)$.

Queste due condizioni sono equivalenti all'unica condizione

$$(L) \qquad \varphi(\alpha u+\beta v)=\alpha\varphi(u)+\beta\varphi(v) \quad (\forall u, v \in V,\ \forall \alpha, \beta \in \Bbbk),$$

o anche alla condizione

$$(L') \qquad \varphi(\alpha u+v)=\alpha\varphi(u)+\varphi(v) \quad (\forall u, v \in V,\ \forall \alpha \in \Bbbk).$$

1.1.1. Dalla definizione segue subito che si ha $\varphi(0)=0$ e $\varphi(-v)=-\varphi(v)$.

1.1.2. Sempre dalla definizione troviamo che $\varphi(\sum_i \alpha_i v_i)=\sum_i \alpha_i \varphi(v_i)$, cioè

$$\varphi(\alpha_1 v_1+\alpha_2 v_2+\cdots+\alpha_m v_m)=\alpha_1\varphi(v_1)+\alpha_2\varphi(v_2)+\cdots+\alpha_m\varphi(v_m),$$

per ogni insieme finito di vettori v_i e ogni corrispondente insieme di scalari α_i. Da questo si deduce subito che *una applicazione lineare è determinata dai valori assunti su una base del dominio:* infatti noti i valori di φ su una base di V, si può trovare il valore dell'applicazione su ogni vettore di V. Viceversa, una volta assegnati i valori su una base di V, esiste una (unica) applicazione lineare soddisfacente a quelle condizioni (che si ottiene con la formula sopra scritta), che si dice ottenuta "estendendo per linearità" le condizioni date.

1.1.3. Composizione di morfismi lineari. Date due applicazioni lineari $\varphi : V \to W$ e $\psi : W \to U$, segue dalla definizione che la composizione $\psi \circ \varphi : V \to U$ è ancora una applicazione lineare.

1.2. Definizione-Proposizione (nucleo e immagine). *Sia $\varphi : V \to W$ una applicazione lineare. Il nucleo (kernel) di φ è l'antimmagine del vettore nullo*

$$\ker\varphi := \{v \in V \mid \varphi(v)=0\}$$

e l'immagine di φ è l'immagine in senso insiemistico

$$\operatorname{im}\varphi := \{w \in W \mid \text{esiste } v \in V \text{ tale che } w=\varphi(v)\}$$

Nucleo e immagine si φ sono sottospazi vettoriali di V e W rispettivamente.

Dimostrazione. Verifica immediata. □

1.3. Teorema (formula delle dimensioni per applicazioni lineari). *Sia $\varphi : V \to W$ una applicazione lineare, e supponiamo V di dimensione finita. Allora vale la relazione*

$$\dim_{\Bbbk} V = \dim_{\Bbbk} \ker\varphi + \dim_{\Bbbk} \operatorname{im}\varphi \ .$$

Dimostrazione. Osserviamo prima di tutto che le tre dimensioni coinvolte nella formula sono finite (quella di V per ipotesi, quella di $\ker\varphi$ perché si tratta di un sottospazio di V, quella di $\operatorname{im}\varphi$ perché si tratta di un sottospazio vettoriale di W che è generato dall'immagine dei vettori di una qualsiasi base di V). Ora scegliamo una base di $\ker\varphi$, sia $v_1, \dots, v_r$, e completiamola ad una base di V, sia $v_1, \dots, v_r, v_{r+1}, \dots, v_n$. Per dimostrare la formula del teorema basta mostrare che $\varphi(v_{r+1}), \dots, \varphi(v_n)$ costituiscono una base di $\operatorname{im}\varphi$. Mostriamo che sono un sistema di generatori: se $w = \varphi v \in \operatorname{im}\varphi$, allora $v = \sum_{i=1}^n \alpha_i v_i$ e abbiamo

$$w = \varphi v = \varphi(\sum_{i=1}^n \alpha_i v_i) = \sum_{i=r+1}^n \alpha_i \varphi(v_i) \ ,$$

da cui la conclusione voluta. Mostriamo che formano un sistema linearmente indipendente: se $\sum_{i=r+1}^n \alpha_i \varphi v_i = 0$ allora abbiamo $\sum_{i=r+1}^n \alpha_i v_i \in \ker\varphi$, e usando che $\ker\varphi$ è generato da $v_1, \dots, v_r$ abbiamo $\sum_{i=r+1}^n \alpha_i v_i = \sum_{i=1}^r \alpha_i v_i$, da cui deduciamo $\alpha_i = 0$ per ogni $i = r+1, \dots, n$. □

1.3.1. Problema. Se $\varphi : V \longrightarrow W$ è lineare, allora:

(1) immagini di sottospazi di V sono sottospazi di W (cioè se $V' \leqslant V$ allora $\varphi(V') \leqslant W$) contenuti in $\operatorname{im}\varphi$,

(2) antimmagini di sottospazi di W sono sottospazi di V (cioè se $W' \leqslant W$ allora $\varphi^*(W') \leqslant V$) contenenti $\ker\varphi$.

Dare delle formule per le dimensioni di immagini e antimmagini di sottospazi; da cosa dipendono essenzialmente? In particolare, per quali $V' \leqslant V$ si ha $\dim\varphi(V') = \dim V'$?

1.3.2. Problema. Se $\varphi : V \to V$ (endomorfismo di V), allora i sottopazi $\ker\varphi$ e $\operatorname{im}\varphi$ hanno dimensioni comlementari (la somma delle dimensioni è $\dim_{\Bbbk} V$), ma non sono necessariamente complementari come sottospazi: per esempio se $\varphi^2 = 0$ abbiamo addirittura $\operatorname{im}\varphi \subseteq \ker\varphi$; farsi altri esempi per mostrare che non vi sono relazioni predefinite tra $\ker\varphi$ e $\operatorname{im}\varphi$ come sottospazi di V.

1.4. Teorema (iniettivtà e suriettività). *I seguenti fatti sono equivalenti alla iniettività di φ:*

(1) $\ker\varphi = 0$ *(ovvero* $\dim\ker\varphi = 0$*);*
(2) *se $S \subseteq V$ è linearmente indipendente allora $\varphi S \subseteq W$ è linearmente indipendente (equivalentemente: se $\varphi S \subseteq W$ è linearmente dipendente allora $S \subseteq V$ è linearmente dipendente);*
(3) *φ manda basi di V in insiemi linearmente indipendenti di W;*
(4) *φ manda basi di V in basi di* $\operatorname{im}\varphi$*;*
(5) *φ ammette una inversa a sinistra (esiste $\psi : W \to V$ tale che $\psi \circ \varphi = \mathrm{id}_V$).*

Da ciò si deduce che, se φ è iniettiva, allora $\dim_{\Bbbk} V \leqslant \dim_{\Bbbk} W$.

I seguenti fatti sono equivalenti alla suriettività di φ:

(1) $\operatorname{im}\varphi = W$ *(ovvero* $\dim\operatorname{im}\varphi = \dim W$ *se V o W hanno dimensione finita);*
(2) *φ manda basi di V in insiemi generatori di W;*
(3) *l'immagine di una base di V contiene una base di W;*
(4) *φ ammette una inversa a destra (esiste $\psi : W \to V$ tale che $\varphi \circ \psi = \mathrm{id}_W$).*

Da ciò si deduce che, se φ è suriettiva, allora $\dim_{\Bbbk} V \geqslant \dim_{\Bbbk} W$.

Dimostrazione. Esercizio. □

1.5. Teorema (isomorfismi). *Una applicazione lineare $\varphi : V \to W$ si dice un isomorfismo se esiste una applicazione lineare inversa $\psi : W \to V$ (cioè tale che $\psi \circ \varphi = \mathrm{id}_V$ e $\varphi \circ \psi = \mathrm{id}_W$). I seguenti fatti sono equivalenti a che φ sia isomorfismo:*
(1) *φ è biiettiva (come mappa di insiemi; cioè diciamo che l'inversa insiemistica è necessariamente una applicazione lineare);*
(2) *φ è iniettiva e suriettiva;*
(3) $\ker \varphi = 0$ *e* $\operatorname{im} \varphi = W$*;*
(4) *φ manda basi di V in basi di W.*
In particolare, se φ è isomorfismo, allora $\dim_{\Bbbk} V = \dim_{\Bbbk} W$.

Dimostrazione. È conseguenza del precedente. □

1.6. Corollario (endomorfismi). *Se $\dim_{\Bbbk} V = \dim_{\Bbbk} W$ è finita (per esempio se $V = W$ è spazio vettoriale di dimensione finita) allora i seguenti fatti sono equivalenti:*
(1) *φ è un isomorfismo;*
(2) *φ è iniettiva;*
(2′) $\ker \varphi = 0$*;*
(3) *φ è suriettiva;*
(3′) $\operatorname{im} \varphi = W$.

Dimostrazione. Basta usare la formula delle dimensioni per una applicazione lineare: $\ker \varphi = 0$ (iniettività) se e solo se $\dim_{\Bbbk} \ker \varphi = 0$, se e solo se $\dim_{\Bbbk} \operatorname{im} \varphi = \dim_{\Bbbk} W$ se e solo se $\operatorname{im} \varphi = W$ (suriettività). □

1.6.1. Osservazioni sulla finitezza. Si osservi che per il risultato precedente è essenziale l'ipotesi di finitezza delle dimensioni; trovare degli esempi di applicazioni lineari iniettive ma non suriettive, e suriettive ma non iniettive tra gli endomorfismi di uno spazio vettoriale di dimensione infinita (lo spazio dei polinomi per esempio: derivazione, integrazione indefinita "senza costante", composizioni?).

La situazione va paragonata con quella che si ha considerando mappe di insiemi di un insieme finito (con un numero finito di elementi) in sè; anche in quel caso abbiamo che biiettività, iniettività, suriettività sono nozioni equivalenti. Fatto evidentemente falso per applicazioni di un insieme infinito in sè (farsi degli esempi). Nel caso di spazi vettoriali finitamente generati, abbiamo che le mappe lineari sono determinate in effetti dai loro valori su un insieme finito, anche se gli spazi stessi possono avere infiniti elementi.

1.7. Ricordiamo che lo spazio vettoriale standard $V_n(\Bbbk)$ su $\Bbbk$ di dimensione n è l'insieme $\Bbbk^n$ dotato delle operazioni "componente per componente"e che la sua base canonica è data dai vettori e_i. Sia V uno spazio vettoriale su $\Bbbk$ di dimensione finita $\dim_{\Bbbk} V = n$ e scegliamo una base $\mathscr{V} = (v_1, \dots, v_n)$ di V. Questo determina un isomorfismo $V_n(\Bbbk) \longrightarrow V$ mandando la base canonica di $V_n(\Bbbk)$ ordinatamente nella base scelta. Dunque la scelta di una base determina un isomorfismo di un qualsiasi spazio vettoriale di dimensione finita n con lo spazio vettoriale standard $V_n(\Bbbk)$ di quella dimensione. Osserviamo però che questo isomorfismo dipende dalla scelta della base di V, cioè non è intrinseco. L'inverso di questo isomorfismo è esattamente la mappa $\alpha_{\mathscr{V}} : V \longrightarrow V_n(\Bbbk)$ che manda ogni vettore di V nelle sue coordinate nella base $\mathscr{V}$.

1.8. Esempi. Diamo alcuni esempi particolarmente importanti di applicazioni lineari.

1.8.1. Inclusioni di sottospazi. Se W è un sottospazio di V, allora l'inclusione insiemistica $\iota_W : W \to V$ è una applicazione lineare, con nucleo nullo e immagine esattamente W.

1.8.2. Proiezioni su quozienti. Se W è un sottospazio di V, allora il morfismo canonico $\pi_W : V \to V/W$ che ad ogni vettore associa la sua classe modulo W è una applicazione lineare, con nucleo W e immagine tutto V/W. Da questo, usando i prossimo teorema si può ritrovare la formula per la dimensione dei quozienti: $\dim_{\Bbbk} V/W = \dim_{\Bbbk} V - \dim_{\Bbbk} W$.

Si osservi anche che per ogni W' complementare di W (cioè $V = W \oplus W'$, ovvero $V = W + W'$ e $W \cap W' = 0$), si ha una mappa canonica, lineare e biiettiva $W' \longrightarrow V/W$; di nuovo si può dedurre $\dim_{\Bbbk} V/W = \dim_{\Bbbk} W' = \dim_{\Bbbk} V - \dim_{\Bbbk} W$.

1.8.3. Proiezioni. Siano U_1 e U_2 sottospazi vettoriali complementari di uno spazio vettoriale V (dunque $V = U_1 \oplus U_2$, ovvero $V = U_1 + U_2$ e $U_1 \cap U_2 = 0$). Allora l'applicazione $\pi_{U_1}^{U_2} : V \longrightarrow V$ che ad ogni vettore $v = u_1 + u_2$ di V (con $u_1 \in U_1$ e $u_2 \in U_2$) associa il vettore u_1 di dice proiezione su U_1 nella direzione di U_2. Si tratta di una applicazione lineare di immagine U_1 e di nucleo U_2 (dunque è un isomorfismo se e solo se $U_2 = 0$ e $U_1 = V$, nel qual caso si tratta dell'identità). Si osservi che la composizione della proiezione con sé stessa dà ancora la proiezione stessa.

1.8.4. Problema. Siano V uno spazio vettoriale di dimensione n sul corpo $\Bbbk$ ed p un endomorfismo di V tale che $p^2 = p$.

(a) Si mostri che $V = \operatorname{im} p \oplus \ker p$.

(b) Si mostri che esistono una base $(v_1, \dots, v_n)$ di V ed un intero i, $1 \leqslant i \leqslant n+1$, tali che $p(v_j) = v_j$, se $j < i$, e $p(v_j) = 0$, se $j \geqslant i$.

(c) Dedurne che si tratta della proiezione di asse $\operatorname{im} p$ e direzione $\ker p$.

Quindi una applicazione lineare di uno spazio vettoriale di dimensione finita in sè è una proiezione se e solo se coincide con il proprio quadrato.

1.8.5. Simmetrie. Nella stessa situazione, l'applicazione $\sigma_{U_1}^{U_2} : V \longrightarrow V$ che ad ogni vettore $v = u_1 + u_2$ di V (con $u_1 \in U_1$ e $u_2 \in U_2$) associa il vettore $u_1 - u_2$ di dice simmetria di asse U_1 e di direzione U_2. Si tratta di una applicazione lineare di immagine V e di nucleo 0, dunque è sempre un isomorfismo; l'applicazione inversa è la stessa simmetria.

1.8.6. Problema. Siano V uno spazio vettoriale di dimensione n sul corpo $\Bbbk$ (di caratteristica diversa da due) e s un endomorfismo di V tale che $s^2 = \mathrm{id}_V$.

(a) Si mostri che $\ker s = 0$, dunque s è un isomorfismo.

(b) Si mostri che esistono due sottospazi complementari V_+ e V_- di V tali che s agisce come l'identità su V_+ e la moltiplicazione per -1 su V_-.

(c) Si mostri che esistono una base $(v_1, \dots, v_n)$ di V ed un intero i, $1 \leqslant i \leqslant n+1$, tali che $s(v_j) = v_j$, se $j < i$, e $s(v_j) = -v_j$, se $j \geqslant i$.

(d) Dedurne che si tratta della simmetria di asse V_+ e direzione V_-.

Quindi una applicazione lineare di uno spazio vettoriale di dimensione finita (su un corpo di caratteristica $\neq 2$) in sè è una simmetria se e solo se è di quadrato identico.

Cosa succede in caratteristica 2? In questo caso $2 = 0$, $1 = -1$, e quindi l'unica simmetria è l'identità. Per contro possono esistere funzioni lineari non identiche di quadrato identico (per esempio quella di matrice $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$).

1.8.7. Problema. Scrivere le relazioni tra $\pi_{U_1}^{U_2}$, $\pi_{U_2}^{U_1}$, $\sigma_{U_1}^{U_2}$, $\sigma_{U_2}^{U_1}$. Per esempio $\pi_{U_1}^{U_2} + \pi_{U_2}^{U_1} = \mathrm{id}_V$, $\pi_{U_1}^{U_2} - \pi_{U_2}^{U_1} = \sigma_{U_1}^{U_2}$, ecc.

1.9. Teorema (primo teorema di isomorfismo). *Sia $\varphi : V \to W$ una applicazione lineare. Allora φ induce un isomorfismo $\overline{\varphi} : V/\ker\varphi \longrightarrow \operatorname{im}\varphi$ che rende commutativo il seguente diagramma di applicazioni lineari:*

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[d, "\pi"'] & W \\ V/\ker\varphi \arrow[r, "\overline{\varphi}"'] & \operatorname{im}\varphi \arrow[u, "\iota"'] \end{tikzcd}$$

ove π e ι sono le applicazioni canoniche (commutativo significa che $\varphi = \iota \circ \overline{\varphi} \circ \pi$).

Dimostrazione. Più in generale, se V' è un sottospazio di V, è facile osservare che φ si fattorizza tramite il quoziente V/V' (significa che esiste una applicazione lineare $V/V' \to W$ tale che la composizione con la proiezione canonica $V \to V/V'$ sia φ) se e solo se $\varphi(V') = 0$, cioè $V' \subseteq \ker\varphi$. Da questo segue subito il teorema.

In modo più dettagliato possiamo procedere così: definiamo la funzione $\overline{\varphi}$ sulla classe $[v] \in V/\ker\varphi$ tramite $\overline{\varphi}[v] = \varphi(v) \in \operatorname{im}\varphi$. Questa definizione, che usa il rappresentante v della classe $[v]$, è ben posta (se $[v] = [v']$ allora $\varphi(v) = \varphi(v')$), e chiaramente dà una funzione lineare e biiettiva; vale inoltre $\iota\overline{\varphi}\pi(v) = \iota\overline{\varphi}[v] = \iota\varphi(v) = \varphi(v)$ (e anzi questo obbliga la definizione data...). □

1.9.1. Si osservi che la formula delle dimensioni per il morfismo φ dice appunto che $\dim_{\Bbbk}(V/\ker\varphi) = \dim\operatorname{im}\varphi$.

♠ **1.10.** Teorema (secondo teorema di isomorfismo). *Il morfismo di inclusione* $\iota_1 : W_1 \longrightarrow W_1 + W_2$ *induce un isomorfismo* $\bar{\iota}_1 : W_1/(W_1 \cap W_2) \longrightarrow (W_1 + W_2)/W_2$ *che rende commutativo il seguente diagramma di applicazioni lineari:*

$$\begin{tikzcd} W_1 \arrow[r, "\iota_1"] \arrow[d, "\pi_1"'] & W_1 + W_2 \arrow[d, "\pi_2"] \\ W_1/(W_1 \cap W_2) \arrow[r, "\bar{\iota}_1"'] & (W_1 + W_2)/W_2 \end{tikzcd}$$

ove π_1 *e* π *sono le applicazioni canoniche (commutativo significa che* $\pi_2 \circ \iota_1 = \bar{\iota}_1 \circ \pi_1$*).*

Dimostrazione. Basta osservare che $\pi_2 \circ \iota_1 : W_1 \to (W_1 + W_2)/W_2$ è suriettivo e $\ker(\pi_2 \circ \iota_1) = W_1 \cap W_2$; si applica allora il primo teorema di isomorfismo. □

1.10.1. Di solito si esprime questo risultato in modo più pittoresco dicendo che i quozienti dei lati opposti del seguente diagramma di inclusioni

$$\begin{tikzcd} & W_1 + W_2 \arrow[dl, dash, "\sim"'] \arrow[dr, dash, "\approx"] & \\ W_1 \arrow[dr, dash, "\approx"'] & & W_2 \arrow[dl, dash, "\sim"] \\ & W_1 \cap W_2 & \end{tikzcd}$$

sono isomorfi tra loro. Qaule formula delle dimensioni dà l'isomorfismo del teorema?

♠ **1.11.** Teorema (terzo teorema di isomorfismo). *Se abbiamo* $W_1 \supseteq W_2$ *sottospazi di* V*, il morfismo canonico* $\pi : V/W_2 \longrightarrow V/W_1$ *induce un isomorfismo* $\overline{\pi} : (V/W_2)/(W_1/W_2) \longrightarrow V/W_1$ *che rende commutativo il seguente diagramma di applicazioni lineari:*

$$\begin{tikzcd} V \arrow[r, "\pi_1"] \arrow[d, "\pi_2"'] & V/W_1 \\ V/W_2 \arrow[r, "\overline{\pi}_1"'] & (V/W_2)/(W_1/W_2) \arrow[u, "\overline{\pi}"'] \end{tikzcd}$$

ove π_1 *e* π_2 *sono le applicazioni canoniche (commutativo significa che* $\overline{\pi} \circ \overline{\pi}_1 \circ \pi_2 = \pi_1$*; si noti anche che* $\pi = \overline{\pi} \circ \overline{\pi}_1$ *e* $\pi \circ \pi_2 = \pi_1$*).*

Dimostrazione. Il morfismo π esiste perché $W_2 \subseteq W_1 = \ker(V \to V/W_1)$; è facile vedere che π è suriettivo, e che $\ker \pi \cong W_1/W_2$ (canonicamente isomorfo); quindi per l'esistenza e le proprietà di $\overline{\pi}$ basta usare il primo teorema di isomorfismo. La commutatività affermata si può verificare direttamente. □

1.11.1. Si osservi l'analogia con il calcolo delle frazioni: $(a/c)/(b/c) = a/b$ (donde in nome in slang di "teorema della matricola"). Naturalmente, si può esprimere il teorema per tre sottospazi in catena ($W_0 \supseteq W_1 \supseteq W_2$). Quale formula per le dimensioni otteniamo dall'isomorfismo del teorema?

1.12. A titolo di divertimento, si provi a dimostrare il teorema della farfalla: nel seguente diagramma di inclusioni, i quozienti sulle tre frecce verticali sono isomorfi tra loro.

$$\begin{tikzcd} A \arrow[dr, dash] & & & & C \arrow[dl, dash] \\ & B+(A\cap C) \arrow[dr, dash] \arrow[dd, dash] & & (A\cap C)+D \arrow[dl, dash] \arrow[dd, dash] & \\ & & A\cap C \arrow[dl, dash] \arrow[dr, dash] \arrow[dd, dash] & & \\ B+(A\cap D) \arrow[dr, dash] & & & & (B\cap C)+D \arrow[dl, dash] \\ & B \arrow[dr, dash] & (B\cap C)+(A\cap D) \arrow[dl, dash] \arrow[dr, dash] & D \arrow[dl, dash] & \\ & B\cap C & & A\cap D & \end{tikzcd}$$

1.13. Definizione-Proposizione (spazi di morfismi). *L'insieme di tutte le applicazioni $\Bbbk$-lineari di V in W si indica con $\mathrm{Hom}_{\Bbbk}(V,W)$. Esso ha stuttura di spazio vettoriale su $\Bbbk$, come sottospazio di tutte la applicazioni (insiemistiche) di V in W. L'applicazione di composizione, come già detto, rispetta la linearità e dunque dà una mappa*

$$\mathrm{Hom}_{\Bbbk}(V,W)\times\mathrm{Hom}_{\Bbbk}(W,U)\longrightarrow\mathrm{Hom}_{\Bbbk}(V,U)$$

che manda la coppia (φ,ψ) in $\psi\circ\varphi$. L'applicazione di composizione non è lineare, bensì bilineare, ovvero lineare in ogni variabile: valgono le formule

$$\psi\circ(\alpha_1\varphi_1+\alpha_2\varphi_2)=\alpha_1\psi\circ\varphi_1+\alpha_2\psi\circ\varphi_2\quad e\quad(\beta_1\psi_1+\beta_2\psi_2)\circ\varphi=\beta_1\psi_1\circ\varphi+\beta_2\psi_2\circ\varphi$$

per ogni $\varphi,\varphi_1,\varphi_2\in\mathrm{Hom}_{\Bbbk}(V,W)$, $\psi,\psi_1,\psi_2\in\mathrm{Hom}_{\Bbbk}(W,U)$, $\alpha_1,\alpha_2,\beta_1,\beta_2\in\Bbbk$.

Dimostrazione. Esercizio. □

1.14. Definizione (Algebra degli endomorfismi.). *In particolare, definiamo $\mathrm{End}_{\Bbbk}(V)=\mathrm{Hom}_{\Bbbk}(V,V)$ che è un insieme dotato della struttura di algebra associativa (non commutativa) su $\Bbbk$ con unità, ovvero di:*

(V) *una struttura di spazio vettoriale su $\Bbbk$;*

(A) *una operazione di prodotto (composizione) $\mathrm{End}_{\Bbbk}(V)\times\mathrm{End}_{\Bbbk}(V)\to\mathrm{End}_{\Bbbk}(V)$ verificante le proprietà seguenti:*

- $(A1)$ *esiste un elemento neutro per il prodotto (l'applicazione identica id_V tale che $\varphi\circ\mathrm{id}_V=\varphi=\mathrm{id}_V\circ\varphi$ per ogni $\varphi\in\mathrm{End}_{\Bbbk}(V)$),*
- $(A2)$ *il prodotto è associativo ($(\varphi\circ\psi)\circ\vartheta=\varphi\circ(\psi\circ\vartheta)$ per ogni $\varphi,\psi,\vartheta\in\mathrm{End}_{\Bbbk}(V)$),*
- $(A3)$ *il prodotto rispetta la struttura di spazio vettoriale, nel senso che risulta bilineare, come già specificato.*

Anche da questa definizione possiamo trarre molti risultati algebrici puramente formali, quali per esempio:

1.14.1. Prodotto con lo zero. Risulta $0\circ\varphi=0=\psi\circ 0$ per ogni φ e ψ.

1.14.2. Annullamento. Se $\psi\circ\varphi=0$ e uno tra φ e ψ è invertibile (ha inverso per la composizione) allora l'altro è zero.

1.14.3. Sviluppo del binomio. Per definizione si pone $\varphi^n=\varphi\circ\cdots\circ\varphi$ (n volte) e $\varphi^0=\mathrm{id}_V$. Allora vale la formula del binomio per elementi che commutano: se $\psi\circ\varphi=\varphi\circ\psi$ allora $(\varphi+\psi)^n=\sum_{i=0}^n\binom{n}{i}\varphi^i\psi^{n-i}$.

1.14.4. In particolare vale $(\mathrm{id}_V+\varphi)^n=\sum_{i=0}^n\binom{n}{i}\varphi^i$.

♠ **1.15.** Somme e Prodotti (arbitrari). Data una famiglia $\mathscr{I}$ di indici, e un insieme di spazi vettoriali V_i al variare di $i\in\mathscr{I}$, definiamo la somma diretta $\bigoplus_{i\in\mathscr{I}}V_i$ e il prodotto diretto $\prod_{i\in\mathscr{I}}V_i$ come gli insiemi formati dalle $\mathscr{I}$-uple $(v_i)_{i\in\mathscr{I}}$ di elementi con $v_i\in V_i$ per ogni i, e quasi tutti nulli (i.e. nulli tranne che per un numero finito di indici) nel caso della somma diretta. Si hanno strutture canoniche di spazio vettoriale su $\Bbbk$ con le operazioni "componente per componente".

In particolare la somma diretta è un sottospazio vettoriale del prodotto diretto, e se l'insieme di indici è finito, allora le due nozioni coincidono. Discutere i casi in cui le dimensioni di questi spazi risultano finite.

Abbiamo dei morfismi canonici di inclusione $\iota_j:V_j\to\bigoplus_{i\in\mathscr{I}}V_i$ (manda v_j nella $\mathscr{I}$-upla che ha tutte le componenti nulle tranne la j-esima che vale v_j) e di proiezione $\pi_j:\prod_{i\in\mathscr{I}}V_i\to V_j$ (manda una $\mathscr{I}$-upla nella sua j-sima componente) per ogni j. Si verifica subito che $\pi_j\circ\iota_j=\mathrm{id}_{V_j}$ (da cui si vede che ι_j è iniettiva e π_j è suriettiva), $\pi_j\circ\iota_{j'}=0$ se $j\neq j'$.

Per ogni spazio vettoriale W su $\Bbbk$, vi sono i seguenti isomorfismi di spazi vettoriali su $\Bbbk$:

$$\mathrm{Hom}_{\Bbbk}\Big(\bigoplus_{i\in\mathscr{I}}V_i,W\Big)\cong\prod_{i\in\mathscr{I}}\mathrm{Hom}_{\Bbbk}(V_i,W)\quad e\quad\mathrm{Hom}_{\Bbbk}\Big(W,\prod_{i\in\mathscr{I}}V_i\Big)\cong\prod_{i\in\mathscr{I}}\mathrm{Hom}_{\Bbbk}(W,V_i)$$

dati dalle composizioni con le inclusioni e le proiezioni, rispettivamente. Questi isomorfismi si indicano spesso con il nome di "proprietà universale" di somma diretta e prodotto rispettivamente: per ogni spazio vettoriale W e per ogni famiglia di applicazioni lineari da V_i in W (risp. da W in V_i) esiste una unica applicazione lineare corrispondente da $\bigoplus_{i\in\mathscr{I}}V_i$ in W (risp. da W in $\prod_{i\in\mathscr{I}}V_i$).

♠ **1.16.** Nucleo e quoziente. Per ogni applicazione lineare $\varphi : V \to W$ abbiamo i seguenti isomorfismi di spazi vettoriali:

$$\mathrm{Hom}_{\Bbbk}(U, \ker\varphi) \cong \{f \in \mathrm{Hom}_{\Bbbk}(U, V) : \varphi \circ f = 0\}$$

per ogni spazio vettoriale U su $\Bbbk$; in altri termini, le applicazioni lineari da U verso $\ker\varphi$ sono in corrispondenza biunivoca con le applicazioni lineari di U verso V la cui immagine è contenuta in $\ker\varphi$.

Analogamente se W è un sottospazio vettoriale di V, allora abbiamo un isomorfismo di spazi vettoriali

$$\mathrm{Hom}_{\Bbbk}(V/W, U) \cong \{f \in \mathrm{Hom}_{\Bbbk}(V, U) : f(W) = 0\}$$

per ogni spazio vettoriale U su $\Bbbk$; in altri termini, le applicazioni lineari da V/W verso U sono in corrispondenza biunivoca con le applicazioni lineari di V verso U il cui nucleo contiene W, cioè le applicazioni lineari di V verso U il cui valore è stabile sulle classi laterali di W.

1.17. Miscellanea. Sia W un sottospazio di V.

(1) L'inclusione $\iota : W \to V$ induce una biiezione (che rispetta inclusioni, intersezioni e somme) tra i sottospazi di W e i sottospazi di V contenuti in W.
(2) La proiezione $\pi : V \to V/W$ induce una biiezione (che rispetta inclusioni, intersezioni e somme?) tra i sottospazi di V/W e i sottospazi di V contenenti W. Se $U \leqslant V$, verificare che $\pi(U) = (U + W)/W$; in particolare, se $U \leqslant W$ allora $\pi(U) = 0$, se $U \geqslant W$ allora $\pi(U) = U/W$, se $U \cap W = 0$ allora $\pi(U) \cong U$, se $U + W = V$ allora $\pi(U) = V/W$.
(3) Se poi W' è un sottospazio di V complementare di W, confrontare V con $W \times W'$, e W' con V/W. Cosa si può dire dei rapporti tra V e $W \times (V/W)$?
(4) Se $V = W + W'$ e $W \cap W' = U$, allora $V/U \cong (W/U) \oplus (W'/U)$.

2. Matrici.

2.0. Prologo. Ogni funzione lineare φ da $V_m(\Bbbk)$ a $V_n(\Bbbk)$ è completamente determinata dalle immagini dei vettori della base canonica di $V_m(\Bbbk)$, diciamo $\varphi(e_j) = A_j$ dove $A_j = \sum_i A_{i,j} e_i$ sono in $V_n(\Bbbk)$ (per $j = 1, \dots, m$), che possiamo usare come colonne per costruire una matrice $A_\varphi = A = (A_1 \cdots A_m)$ con n righe ed m colonne che quindi determina completamente la funzione lineare φ.

Dato un vettore $v \in V_m(\Bbbk)$, detto $v = \sum_j x_j e_j$, abbiamo che

$$\varphi(v) = \sum_{j=1}^{m} x_j \varphi(e_j) = \sum_{j=1}^{m} x_j A_j = \sum_{j=1}^{m} x_j \sum_{i=1}^{n} A_{i,j} e_i = \sum_{i=1}^{n} \Big(\sum_{j=1}^{m} x_j A_{i,j} \Big) e_i$$

e quindi la sua componente i-esima è data da $\sum_j A_{i,j} x_j$ ("prodotto della i-esima riga di A per la colonna del vettore v").

È facile vedere che la funzione

$$\mathrm{Hom}_{\Bbbk}(V_m(\Bbbk), V_n(\Bbbk)) \longrightarrow M_{n,m}(\Bbbk)$$

definita mandando φ in A_φ è una biiezione insiemistica, e quindi possiamo trasportare agli insiemi di matrici tutte le nozioni note per le applicazioni lineari: struttura di spazio vettoriale, composizione (definisce un prodotto tra matrici di taglia opportuna, automaticamente associativo, corrispondente alla composizione di funzioni lineari: il "prodotto riga per colonna"), struttura di algebra nel caso di matrici quadrate, nozioni di invertibilità, ecc.

Solo per motivi di esposizione preferiamo dedicare una sezione allo studio delle matrici prima di vedere esplicitamente la loro relazione con le funzioni lineari, ma il lettore deve tener presente che vi è un dizionario completo tra applicazioni lineari e matrici: per ogni definizione, proprietà o risultato per matrici si deve sempre esplorare quello corrispondente per applicazioni lineari, e viceversa.

2.1. Definizione (spazio vettoriale delle matrici). *Per ogni naturale n, sia $\mathbf{n}$ l'insieme $\{1, 2, \dots, n\}$. Lo spazio vettoriale $M_{n\times m}(\Bbbk)$ (o $M_{n,m}(\Bbbk)$) delle matrici $n \times m$ (n righe ed m colonne) a coefficienti in un corpo $\Bbbk$ è lo spazio vettoriale delle funzioni da $\mathbf{n} \times \mathbf{m}$ in $\Bbbk$. Una matrice $n \times m$ a*

valori in un corpo $\Bbbk$ *si rappresenta con una scrittura:*

$$A = (a_{i,j})_{\substack{i=1,\dots,n\\ j=1,\dots,m}} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} ;$$

e le operazioni di spazio vettoriale si scrivono nel modo seguente:
(P) *prodotto per elementi* $\alpha \in \Bbbk$*: se* $A = (a_{i,j})$*, allora* $\alpha A = (\alpha a_{i,j})$*.*
(S) *somma: se* $A = (a_{i,j})\,, B = (b_{i,j}) \in M_{n,m}(\Bbbk)$*, allora* $A + B = (a_{i,j} + b_{i,j}) \in M_{n,m}(\Bbbk)$*.*
Useremo anche la seguente scrittura "per colonne" e "per righe":

$$A = \left(A_{(1)} \cdots A_{(m)}\right) = \begin{pmatrix} A^{(1)} \\ \vdots \\ A^{(n)} \end{pmatrix}$$

ove $A_{(i)}$ *sono matrici* $n \times 1$ *e si dicono le colonne di* A*, e* $A^{(j)}$ *sono matrici* $1 \times m$ *e si dicono le righe di* A

2.2. Si osservi che lo spazio vettoriale $M_{n,m}(\Bbbk)$ delle matrici $n \times m$ ha dimensione nm. La base canonica è data dalle matrici $e_{i,j}$ le cui entrate sono tutte nulle tranne quella in posizione (i, j) che vale 1.

2.3. Definizione-Teorema (prodotto righe per colonne di matrici). *Definiamo un prodotto di matrici nel modo seguente: se* $A \in M_{n,m}(\Bbbk)$ *e* $B \in M_{m,l}(\Bbbk)$ *(dunque il numero di colonne di* A *eguaglia il numero di righe di* B*) allora*

$$AB = \left(\sum_{j=1}^{m} a_{i,j} b_{j,k}\right)_{\substack{i=1,\dots,n\\ k=1,\dots,l}} = \left(A^{(i)} B_{(k)}\right)_{\substack{i=1,\dots,n\\ k=1,\dots,l}} \in M_{n,l}(\Bbbk) \ .$$

Abbiamo così definito una applicazione bilineare

$$M_{n,m}(\Bbbk) \times M_{m,l}(\Bbbk) \longrightarrow M_{n,l}(\Bbbk)$$

per la quale vale una proprietà di associatività $(A_1A_2)A_3 = A_1(A_2A_3)$ *per ogni matrice* $A_1 \in M_{n,m}(\Bbbk)$*,* $A_2 \in M_{m,l}(\Bbbk)$*,* $A_3 \in M_{l,h}(\Bbbk)$ *(si osservi in particolare che tutti i prodotti scritti hanno senso).*

Inoltre per ogni n *la matrice quadrata "identità"* $\mathbb{I}_n \in M_{n,n}(\Bbbk)$ *definita da* $(\delta_{i,j})$ *(ove i simboli di Kronecker* $\delta_{i,j}$ *sono uguali a* 1 *se* $i = j$ *e a* 0 *altrimenti) ha la proprietà* $\mathbb{I}_n A = A$ *per ogni* $A \in M_{n,m}(\Bbbk)$ *e* $B\mathbb{I}_n = B$ *per ogni* $B \in M_{m,n}(\Bbbk)$*.*

Dimostrazione. La bilinearità del prodotto di matrici ($(\alpha_1 A_1 + \alpha_2 A_2)B = \alpha_1 A_1 B + \alpha_2 A_2 B$ e $A(\beta_1 B_1 + \beta_2 B_2) = \beta_1 AB_1 + \beta_2 AB_2$) si verifica subito in base alla definizione.

Per dimostrare l'associatività del prodotto è sufficiente mostrare che per ogni i e k si ha l'uguaglianza $(A_1^{(i)} A_2)A_{3(k)} = A_1^{(i)}(A_2 A_{3(k)})$, cioè basta mostrarlo per i prodotto del tipo "riga per matrice per colonna", e in quel caso si tratta di un facile conto.

La verifica per le proprietà delle matrici identiche è immediata. □

2.3.1. Righe e colonne. Sotto quali condizioni si può moltiplicare una riga per una colonna, e che tipo di matrice è l'eventuale risultato? Sotto quali condizioni si può moltiplicare una colonna per una riga, e che tipo di matrice è l'eventuale risultato?

Conviene farsi una immagine chiara delle condizioni per il prodotto di matrici, e del tipo di risultato che ne esce:

2.3.2. Invertibilità destra e sinistra. Una matrice $A \in M_{n,m}$ si dice invertibile a destra se esiste una matrice $B \in M_{m,n}$ tale che $AB = \mathbb{I}_n$; si dice invertibile a sinistra se esiste una matrice $B \in M_{m,n}$ tale che $BA = \mathbb{I}_m$.

2.3.3. Cancellazione? Annullamento? Se abbiamo $AB = AC$ in generale non si può dedurre $B = C$, a meno che la matrice A risulti invertibile a sinistra; similmente per $BA = CA$.

Se abbiamo $AB = 0$ (matrice nulla) in generale non si può dedurre che A oppure B siano nulle (a meno che?); farsi qualche controesempio facile.

2.3.4. Non commutatività. Si osservi che il prodotto di matrici non è commutativo: in primo luogo, se un prodotto è definito, non è nemmeno detto che il prodotto con l'ordine scambiato sia definito. Inoltre, se anche i due prodotti fossero entrambi definiti, i risultati potrebbero essere matrici di taglie diverse. Infine, anche se consideriamo matrici quadrate ($n = m$), in cui i prodotti sono definiti e si tratta di matrici nello stesso spazio vettoriale, i due prodotti in generale sono diversi. Farsi degli esempi.

2.4. Definizione-Proposizione (Trasposizione). *Sia $A \in M_{n,m}(\Bbbk)$; definiamo $A^{\mathrm{t}} \in M_{m,n}(\Bbbk)$ tramite: $A^{\mathrm{t}} := (a_{i,j})_{\substack{j=1,\dots,m\\ i=1,\dots,n}}$. Abbiamo allora per ogni n ad m una applicazione*

$$^{\mathrm{t}} : M_{n,m}(\Bbbk) \longrightarrow M_{m,n}(\Bbbk)$$

con le seguenti proprietà:
(1) $(A^{\mathrm{t}})^{\mathrm{t}} = A$ *(involutoria; di conseguenza è una biiezione inversa della omonima in senso inverso),*
(2) $(A + B)^{\mathrm{t}} = A^{\mathrm{t}} + B^{\mathrm{t}}$ *e* $(\alpha A)^{\mathrm{t}} = \alpha A^{\mathrm{t}}$ *(linearità),*
(3) *inoltre, se A e B sono matrici moltiplicabili (cioè il numero di colonne di A coincide con il numero di righe di B), allora anche B^{t} e A^{t} lo sono e vale $(AB)^{\mathrm{t}} = B^{\mathrm{t}}A^{\mathrm{t}}$ (rispetta il prodotto scambiando l'ordine dei fattori). Di solito si dice che il trasposto del prodotto è il prodotto delle trasposte nell'ordine inverso.*

Dimostrazione. Esercizio. □

2.4.1. Si osservi che data una matrice $A \in M_{m,n}(\Bbbk)$, entrambi i prodotti $A^{\mathrm{t}}A$ e AA^{t} sono definiti, e danno luogo a due matrici quadrate, di solito di ordini diversi. Quand'anche A fosse quadrata, naturalmente, di solito i due prodotti sono diversi.

2.5. Definizione (Algebra delle matrici quadrate d'ordine n). *In particolare le matrici quadrate d'ordine n, ovvero le matrici $n \times n$, a coefficienti in $\Bbbk$, formano una algebra associativa (non commutativa in generale) con elemento neutro per il prodotto (la matrice identica $\mathbb{I}_n$ che ha componenti i simboli di Kronecker $\delta_{i,j}$ uguali a 1 se $i = j$ e a 0 altrimenti). Quest'algebra si indica con $M_n(\Bbbk)$.*

2.5.1. Matrici scalari. Consideriamo l'applicazione

$$scal : \Bbbk \longrightarrow M_n(\Bbbk)$$

che manda ogni $\alpha \in \Bbbk$ nella matrice $scal(\alpha) = \alpha\mathbb{I}_n$ che ha componenti uguali ad α nelle posizioni con $i = j$ (diagonale principale) e zero altrove. Si tratta di una applicazione lineare e iniettiva che rispetta identità e prodotti. Le matrici dell'immagine di *scal* si dicono matrici scalari, formano una sotto-$\Bbbk$-algebra (e in effetti un sottocorpo) dell'algebra della matrici, e ne costituiscono il centro: le matrici scalari sono tutte e sole le matrici S che commutano con tutte le altre matrici, cioè tali che $AS = SA$ per ogni $A \in M_n(\Bbbk)$.

2.5.2. Matrici diagonali. Consideriamo l'applicazione

$$diag : \Bbbk^n \longrightarrow M_n(\Bbbk)$$

che manda ogni $(a_1, \dots, a_n) \in \Bbbk^n$ nella matrice $diag(a_1, \dots, a_n)$ che ha componente uguale ad a_i nelle posizioni (i, i) (diagonale principale) e zero altrove. Si tratta di una applicazione lineare e iniettiva. Le

matrici dell'immagine di *diag* si dicono matrici diagonali, e formano una sotto-$\Bbbk$-algebra dell'algebra della matrici. Le matrici scalari sono particolari matrici diagonali (quali?).

2.5.3. Matrici invertibili. Una matrice $A \in M_n(\Bbbk)$ si dice invertibile se esiste una matrice B tale che $AB = \mathbb{I}_n = BA$, cioè se è invertibile a destra e a sinistra (in tal caso necessariamente le inverse destra e sinistra coincidono). La matrice B è allora unica e si indica con A^{-1}

2.5.4. Una matrice A si dice unipotente se esiste un naturale m tale che $A^m = \mathbb{I}_n$. Ogni matrice unipotente è invertibile.

2.5.5. Una matrice A si dice nilpotente se esiste un naturale m tale che $A^m = 0_n$. Se A è nilpotente, allora $\mathbb{I}_n + A$ è invertibile.

2.5.6. Una matrice A si dice divisore a sinistra di zero se esiste una matrice $B \neq 0_n$ tale che $AB = 0_n$ e divisore a destra di zero se esiste una matrice $B \neq 0_n$ tale che $BA = 0_n$. Una matrice è divisore a sinistra di zero se e solo se è divisore a destra di zero (e quindi si parlerà di divisori di zero senza specificare, ma notare che in generale i divisori di zero a destra e a sinistra per una fissata matrice sono diversi). Una matrice non nulla o è invertibile o è divisore di zero (e le due possibilità si escludono).

2.5.7. Una matrice A si dice simmetrica o antisimmetrica a seconda che $A^{\mathrm{t}} = A$ oppure $A^{\mathrm{t}} = -A$.

2.6. Definizione (rango di matrici). *Il rango* $\mathrm{rg}(A)$, *talvolta* $\mathrm{rk}(A)$, *di una matrice* $A \in M_{n,m}(\Bbbk)$ *è per definizione il massimo numero di colonne linearmente indipendenti.*

2.6.1. Si potrebbe definire anche il "rango per righe" di una matrice, come il massimo numero di righe linearmente indipendenti (cioè il rango della matrice trasposta). In realtà coincide con il rango (per colonne), come vedremo sia come conseguenza della dualità di spazi vettoriali, sia come conseguenza del metodo di riduzione di Gauss per matrici.

2.6.2. Una matrice ha rango nullo se e solo se è la matrice nulla.

2.6.3. Una matrice $A \in M_{n,m}(\Bbbk)$ ha rango 1 se e solo se può essere scritta come prodotto $A = VW$ con $V \in M_{n,1}(\Bbbk)$ e $W \in M_{1,m}(\Bbbk)$ (non nulle).

2.6.4. Una matrice $A \in M_{n,m}(\Bbbk)$ ha rango r se e solo se r è il minimo intero per cui si può scrivere $A = VW$ con $V \in M_{n,r}(\Bbbk)$ e $W \in M_{r,m}(\Bbbk)$.

2.6.5. *Il rango di una matrice coincide con il massimo ordine di sottomatrici quadrate invertibili.* Per sottomatrice di una matrice data si intende una matrice ottenuta cancellando alcune righe e alcune colonne dalla matrice data.

2.7. Definizione-Teorema (gruppo generale lineare). *Il sottinsieme di* $M_n(\Bbbk)$ *delle matrici invertibili si indica con* $\mathrm{GL}(n,\Bbbk)$ *o* $\mathrm{GL}_n(\Bbbk)$, *e si tratta di un gruppo (non commutativo) sotto il prodotto di matrici. In particolare abbiamo*

(1) $diag(a_1,\dots,a_n)^{-1} = diag(a_1^{-1},\dots,a_n^{-1})$ *se* $a_i \neq 0$ *per ogni* i; $scal(\alpha)^{-1} = scal(\alpha^{-1})$ *se* $\alpha \neq 0$; $\mathbb{I}_n^{-1} = \mathbb{I}_n$;

(2) $\left(A^{-1}\right)^{-1} = A$;

(3) $(AB)^{-1} = B^{-1}A^{-1}$, *cioè se le matrici* A *e* B *sono invertibili, nel qual caso anche* AB *è invertibile, l'inversa del prodotto è il prodotto delle inverse nell'ordine inverso;*

(4) *se* A *è invertibile, anche* A^{t} *lo è, e* $(A^{\mathrm{t}})^{-1} = (A^{-1})^{\mathrm{t}}$; *di solito si dice che la trasposta dell'inversa è l'inversa della trasposta (o che gli operatori di inversione e trasposizione commutano tra loro).*

Dimostrazione. Esercizio. □

2.8. Applicazioni lineari associate a matrici. Data una matrice $A \in M_{n,m}(\Bbbk)$, possiamo definire una applicazione lineare $\varphi_A : \Bbbk^m \longrightarrow \Bbbk^n$, che diremo funzione lineare associata ad A, tramite $\varphi_A(v) = Av$ per ogni $v \in \Bbbk^m = M_{m,1}(\Bbbk)$ (prodotto di matrici, con risultato in $M_{n,1}(\Bbbk) = \Bbbk^n$). Si vede subito che $\mathrm{rg}(A) = \dim_{\Bbbk} \mathrm{im}\,(\varphi_A)$, e $\dim_{\Bbbk} \ker(\varphi_A) = n - \mathrm{rg}(A)$ (talvolta detto nullità della matrice A).

2.8.1. Abbiamo definito allora una applicazione

$$M_{n,m}(\Bbbk) \longrightarrow \mathrm{Hom}_{\Bbbk}(\Bbbk^m, \Bbbk^n)$$

che si vede facilmente essere lineare, biiettiva, e quindi un isomorfismo di $\Bbbk$-spazi vettoriali. È chiaro inoltre che due matrici sono moltiplicabili se e solo se le applicazioni associate sono componibili, e in tal caso risulta che $\varphi_A \circ \varphi_B = \varphi_{AB}$ (semplicemente per l'associatività del prodotto tra matrici).

Tutte le proprietà delle matrici si possono ottenere dalle proprietà delle funzioni lineari tra spazi standard tramite questa corrispondenza.

In particolare una matrice è invertibile a sinistra (risp. a destra) se e solo se lo è l'applicazione lineare associata.

2.8.2. Nel caso particolare di matrici quadrate ($n = m$) abbiamo allora un isomorfismo di $\Bbbk$-algebre

$$M_n(\Bbbk) \longrightarrow \mathrm{End}_{\Bbbk}(\Bbbk^n)$$

(significa che è un isomorfismo lineare che rispetta la struttura di prodotto di matrici e di funzioni (composizione)), che si restringe ad un isomorfismo di gruppi moltiplicativi

$$\mathrm{GL}_n(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk^n)$$

(in particolare, una matrice quadrata è invertibile o divisore di zero, ed è invertibile se solo se lo è a destra o a sinistra, perché questo è vero per gli endomorfismi).

2.8.3. Discutere per una matrice $A \in M_{n,m}(\Bbbk)$ le possibili relazioni tra nucleo e immagine di A, e nucleo e immagine di A^{t}. In particolare le due immagini hanno la stessa dimensione (ma possono essere spazi diversi anche se la matrice è quadrata); studiare le relazioni possibili tra immagine di A e nucleo di A^{t} (sono sottospazi del dominio: sotto quali condizioni sono in somma diretta?).

2.9. Matrici a blocchi. Risulta spesso utile dividere una matrice in blocchi, che significa scegliere una partizione dell'insieme delle righe, una partizione dell'insieme delle colonne, e considerare la matrice data come formata dalle sottomatrici identificate dalle due partizioni scelte.

Spesso si usa partizionare righe e colonne senza "salti", scegliendo una partizione $n = n_1 + \ldots + n_r$ per le righe e una $m = m_1 + \ldots + m_c$ per le colonne; i blocchi sono allora formati scegliendo le righe da $n_1 + \cdots + n_i + 1$ a $n_1 + \cdots + n_{i+1}$, e le colonne da $m_1 + \cdots + m_j + 1$ a $m_1 + \cdots + m_{j+1}$. Si tratta quindi di scrivere $A \in M_{n,m}(\Bbbk)$ come formata "accatastando" le rc sottomatrici $A_{i,j} \in M_{n_i,m_j}(\Bbbk)$:

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,c} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,c} \\ \vdots & \vdots & \ddots & \vdots \\ A_{r,1} & A_{r,2} & \cdots & A_{r,c} \end{pmatrix} .$$

Corrispondentemente, si tratta di scrivere la funzione associata $\varphi_A : \Bbbk^m \longrightarrow \Bbbk^n$ come costituita da una collezione di rc funzioni $\varphi_{A_{i,j}} : \Bbbk^{m_j} \to \Bbbk^{n_i}$, tenendo conto che $\Bbbk^m = \bigoplus_i \Bbbk^{m_j}$ e $\Bbbk^n = \bigoplus_j \Bbbk^{n_j}$.

2.9.1. Prodotti di matrici a blocchi. Come esempio di uso delle matrici a blocchi, si scrivano condizioni e regole per moltiplicare "a blocchi" due matrici scritte a blocchi (compatibili); se ne spieghi il procedimento anche in termini delle funzioni lineari associate. Queste scritture diventano spesso utili quando uno o più blocchi sono nulli, semplificando molto il calcolo: per esempio $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)\left(\begin{smallmatrix} D & E \\ 0 & F \end{smallmatrix}\right) = \left(\begin{smallmatrix} AD & AE+BF \\ 0 & CF \end{smallmatrix}\right)$, oppure $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)\left(\begin{smallmatrix} D & 0 \\ E & F \end{smallmatrix}\right) = \left(\begin{smallmatrix} AD+BE & BF \\ CE & CF \end{smallmatrix}\right)$, sotto le opportune condizioni sulle dimensioni dei blocchi (affinché abbiano senso i prodotti scritti!).

2.9.2. Inverse di matrici a blocchi. Per esempio si può vedere che una matrice a blocchi del tipo $\left(\begin{smallmatrix} \mathbb{I} & F \\ 0 & \mathbb{I} \end{smallmatrix}\right)$ è invertibile con inversa $\left(\begin{smallmatrix} \mathbb{I} & -F \\ 0 & \mathbb{I} \end{smallmatrix}\right)$; più precisamente, il prodotto di due matrici di questo tipo corrisponde alla somma del blocco F.

Più generalmente, se A, C sono matrici quadrate invertibili, allora la matrice $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$ è invertibile con inversa data da $\left(\begin{smallmatrix} A^{-1} & -A^{-1}BC^{-1} \\ 0 & C^{-1} \end{smallmatrix}\right)$.

Per esercizio, generalizzare trovando le inverse di matrici a blocchi del tipo $\left(\begin{smallmatrix} \mathbb{I} & A & B \\ 0 & \mathbb{I} & C \\ 0 & 0 & \mathbb{I} \end{smallmatrix}\right)$, ecc.

3. Matrici associate ad applicazioni lineari.

3.1. Definizione-Teorema (matrici associate ad applicazioni lineari). *Siano V e W spazi vettoriali su $\Bbbk$ di dimensione finita $n := \dim_{\Bbbk} V$ ed $m := \dim_{\Bbbk} W$, e siano $\mathscr{V} = (v_1, \ldots, v_n)$*

e $\mathscr{W} = (w_1, \dots, w_m)$ basi ordinate di V e W rispettivamente. Allora ad ogni applicazione lineare $\varphi : V \longrightarrow W$ possiamo associare una matrice $\alpha_{\mathscr{V},\mathscr{W}}(\varphi) \in M_{m,n}(\Bbbk)$ tramite la definizione seguente:

$$(\varphi v_1, \dots, \varphi v_n) = (w_1, \dots, w_m)\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$$

(o in modo compatto $\varphi\mathscr{V} = \mathscr{W}\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$ ove compare il prodotto tra una riga di vettori e una matrice di scalari, il cui risultato è una riga di vettori) cioè le colonne di $\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$ sono le coordinate nella base scelta di W delle immagini tramite φ dei vettori della base scelta di V. In questo modo abbiamo definito una applicazione

$$\alpha_{\mathscr{V},\mathscr{W}} : \mathrm{Hom}_{\Bbbk}(V, W) \longrightarrow M_{m,n}(\Bbbk)$$

che è un isomorfismo di spazi vettoriali (dipendente dalla scelta delle basi $\mathscr{V}$ e $\mathscr{W}$).

Per ogni spazio vettoriale V di dimensione n, l'applicazione identica $\mathrm{id}_V \in \mathrm{Hom}_{\Bbbk}(V, V)$ viene mandata da $\alpha_{\mathscr{V},\mathscr{V}}$ nella matrice identica $\mathbb{I}_n \in M_n(\Bbbk)$ (indipendentemente dalla base $\mathscr{V}$ scelta).

Dimostrazione. L'unica cosa da verificare è che $\alpha_{\mathscr{V},\mathscr{W}}$ sia applicazione lineare suriettiva, e che $\ker \alpha_{\mathscr{V},\mathscr{W}} = 0$ (entrambe le cose sono facili). □

3.1.1. Le notazioni precedenti, piuttosto compatte, sono estremamente utili, ma conviene esplicitarle completamente ogni qual volta diano luogo a problemi di comprensione; per esempio, esplicitiamo la definizione: se abbiamo $\varphi v_i = a_{1,i}w_1 + a_{2,i}w_2 + \cdots + a_{m,i}w_m$ per ogni $i = 1, 2, \dots, n$, allora la matrice $\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$ ha come i-esima colonna i termini $a_{1,i}, a_{2,i}, \dots, a_{m,i}$. In effetti risulta:

$$(\varphi v_1, \dots, \varphi v_i, \dots, \varphi v_n) = (w_1, w_2, \dots, w_m) \begin{pmatrix} a_{1,1} & \cdots & a_{1,i} & \cdots & a_{1,n} \\ a_{2,1} & \cdots & a_{2,i} & \cdots & a_{2,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,i} & \cdots & a_{m,n} \end{pmatrix}$$

(prodotto righe per colonne).

3.1.2. Dal risultato precedente discende subito che lo spazio vettoriale $\mathrm{Hom}_{\Bbbk}(V, W)$ ha dimensione data dal prodotto delle dimensioni dei due spazi coinvolti: $\dim_V \mathrm{Hom}_{\Bbbk}(V, W) = \dim_{\Bbbk} V \dim_{\Bbbk} W$. In effetti si sta dicendo che una applicazione lineare tra V e W è unicamente e completamente determinata da nm scalari (una volta scelte delle basi nei due spazi).

3.1.3. Matrici di cambiamenti di base. In particolare possiamo consideare uno spazio vettoriale V, due sue basi $\mathscr{V}$ e $\mathscr{V}'$ e l'applicazione identica di V in sè. Allora la matrice $\alpha_{\mathscr{V},\mathscr{V}'}(\mathrm{id}_V)$ si dice matrice di cambiamento di base da $\mathscr{V}$ a $\mathscr{V}'$; le sue colonne sono le coordinate nella base $\mathscr{V}'$ dei vettori della base $\mathscr{V}$.

3.1.4. Matrici di proiezioni e di simmetrie. Siano U_1 e U_2 sottospazi vettoriali complementari di uno spazio vettoriale V (dunque $V = U_1 \oplus U_2$). Fissata una base $\mathscr{V}$ di V consideriamo la matrice A le cui colonne sono le coordinate di una base di U_1, e la matrice B di un sistema di equazioni per U_2, allora la matrice $\alpha_{\mathscr{V}}(\pi_{U_2}^{U_1})$ è data da $A(BA)^{-1}B$ (si noti che BA è matrice quadrata invertibile). Infatti si annulla sulle coordinate dei vettori di U_2, e vale come l'identità sulle coordinate dei vettori di U_1.

3.1.5. Problema. Generalizzando la costruzione precedente, se $\varphi : V \to W$ è applicazione lineare, $\mathscr{V}$ base di V, $\mathscr{W}$ base di W allora: detta B una matrice di equazioni cartesiane per $\ker \varphi$, C una matrice le cui colonne siano coordinate di una base di un complementare di $\ker \varphi$, A la matrice delle coordinate delle immagini dei vettori precedenti, allora $\alpha_{\mathscr{V},\mathscr{W}}(\varphi) = A(BC)^{-1}B$.

3.2. Azione sulle coordinate. Se v ha coordinate $\alpha_{\mathscr{V}}(v) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ nella base $\mathscr{V}$, allora le coordinate $\alpha_{\mathscr{W}}(\varphi v) \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$ di $\varphi(v)$ nella base di W sono date da

$$\alpha_{\mathscr{W}}(\varphi v) = \alpha_{\mathscr{V},\mathscr{W}}(\varphi)\alpha_{\mathscr{V}}(v) \quad \text{ovvero} \quad \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \alpha_{\mathscr{V},\mathscr{W}}(\varphi) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

infatti abbiamo

$$\varphi(v) = \varphi((v_1, \dots, v_n)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}) = \varphi(v_1, \dots, v_n)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (w_1, \dots, w_m)\alpha_{\mathscr{V},\mathscr{W}}(\varphi)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

da cui la conclusione.

3.3. Teorema (composizione e prodotti). *Se $\psi : W \longrightarrow U$ è un'altra applicazione lineare, e $\mathscr{U} = (u_1, \dots, u_l)$ una base di U, allora vale l'identità*

$$\alpha_{\mathscr{V},\mathscr{U}}(\psi \circ \varphi) = \alpha_{\mathscr{W},\mathscr{U}}(\psi)\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$$

(la composizione di applicazioni lineari corrisponde alla moltiplicazione di matrici).

Dimostrazione. Segue dai seguenti calcoli:

$$\begin{aligned} \psi \circ \varphi(\mathscr{V}) = \psi(\varphi\mathscr{V}) &= \psi(\mathscr{W}\alpha_{\mathscr{V},\mathscr{W}}(\varphi)) \\ &= \psi(\mathscr{W})\alpha_{\mathscr{V},\mathscr{W}}(\varphi) \\ &= \mathscr{U}\alpha_{\mathscr{W},\mathscr{U}}(\psi)\alpha_{\mathscr{V},\mathscr{W}}(\varphi)\ . \end{aligned}$$

Nel secondo passaggio si è usata la linearità di ψ (gli elementi della matrice $\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$ sono scalari). Se il senso delle uguaglianze precedenti non fosse chiaro, si calcoli per ogni $v_i \in \mathscr{V}$ la sua immagine tramite $\psi \circ \varphi$ in termini della base $\mathscr{U}$:

$$\psi(\varphi(v_i)) = \psi(\sum_{j=1}^{m} a_{j,i}w_j) = \sum_{j=1}^{m} a_{j,i}\psi(w_j) = \sum_{j=1}^{m} a_{j,i}(\sum_{k=1}^{l} b_{k,j}u_k) = \sum_{k=1}^{l}(\sum_{j=1}^{m} b_{k,j}a_{j,i})u_k$$

(ove abbiamo scelto $\alpha_{\mathscr{V},\mathscr{W}}(\varphi) = (a_{j,i})$ e $\alpha_{\mathscr{W},\mathscr{U}}(\psi) = (b_{k,j})$) e si riconosca il termine di posto k, i della matrice $\alpha_{\mathscr{V},\mathscr{U}}(\psi\circ\varphi)$ come prodotto della riga k-esima di $\alpha_{\mathscr{W},\mathscr{U}}(\psi)$ per la i-esima colonna di $\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$. □

3.3.1. Effetto dei cambiamenti di base. Se $\mathscr{V}'$ è un'altra base di V e $\mathscr{W}'$ un'altra base di W, allora la matrice $\alpha_{\mathscr{V}',\mathscr{W}'}(\varphi)$ è legata alla precedente tramite le matrici di cambiamento di base $\alpha_{\mathscr{V}',\mathscr{V}}(\mathrm{id}_V)$ e $\alpha_{\mathscr{W},\mathscr{W}'}(\mathrm{id}_W)$ dalla formula

$$\alpha_{\mathscr{V}',\mathscr{W}'}(\varphi) = \alpha_{\mathscr{W},\mathscr{W}'}(\mathrm{id}_W)\alpha_{\mathscr{V},\mathscr{W}}(\varphi)\alpha_{\mathscr{V}',\mathscr{V}}(\mathrm{id}_V)$$

Si osservi che le matrici di cambiamento di base sono invertibili e si ha $\alpha_{\mathscr{V}',\mathscr{V}}(\mathrm{id}_V)=\alpha_{\mathscr{V},\mathscr{V}'}(\mathrm{id}_V)^{-1}$.

Nel caso che $V = W$ intendiamo sempre scegliere la stessa base su dominio e codominio, sicché la formula di cambiamento di base diventa

$$\alpha_{\mathscr{V}',\mathscr{V}'}(\varphi) = \alpha_{\mathscr{V},\mathscr{V}'}(\mathrm{id}_V)\alpha_{\mathscr{V},\mathscr{V}}(\varphi)\alpha_{\mathscr{V}',\mathscr{V}}(\mathrm{id}_V) = \alpha_{\mathscr{V}',\mathscr{V}}(\mathrm{id}_V)^{-1}\alpha_{\mathscr{V},\mathscr{V}}(\varphi)\alpha_{\mathscr{V}',\mathscr{V}}(\mathrm{id}_V).$$

3.3.2. L'applicazione φ è iniettiva (rispettivamente suriettiva) se e solo se per qualunque scelta delle basi si ha che la matrice $\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$ è invertibile a sinistra (rispettivamente a destra).

3.3.3. In particolare nel caso $\dim_{\Bbbk} V = \dim_{\Bbbk} W$ allora φ è un isomorfismo se e solo se per qualunque scelta delle basi si ha che la matrice $\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$ è invertibile. Dal teorema degli endomorfismi spazi vettoriali di dimensione finita, deduciamo allora che una matrice quadrata è invertibile se e solo se è invertibile a destra, ovvero se e solo se è invertibile a sinistra. Scrivere per bene la dimostrazione; riflettere sulla possibilità di dimostrazioni dirette dello stesso fatto.

3.4. Rango di applicazioni lineari e matrici. Talvolta si usa definire il rango $\mathrm{rg}(\varphi)$ di una applicazione lineare φ: è la dimensione della sua immagine $\mathrm{im}\,\varphi$ come spazio vettoriale. Dunque il rango di una applicazione corrisponde al rango di una qualunque matrice che la rappresennti (indifferentemente alle basi scelte).

3.4.1. Si osservi che una matrice è invertibile a sinistra se e solo se il suo rango coincide con il numero di colonne, cioè se e solo se le sue colonne formano un sistema linearmente indipendente. Corrispondentemente, una matrice è invertibile a destra se e solo se il suo rango coincide con il numero di righe, cioè se e solo se le sue righe (trasposte) formano un sistema linearmente indipendente. Infatti si tratta del rango della matrice trasposta.

3.4.2. Una matrice $A \in M_n(\Bbbk)$ ha rango strettamente minore di n se e solo se è divisore di zero nell'algebra $M_n(\Bbbk)$.

3.5. Algebre di endomorfismi e algebre di matrici quadrate. Nel caso di endomorfismi di uno spazio vettoriale V di dimensione n e per ogni scelta di una base $\mathscr{V}$ abbiamo dunque un isomorfismo di $\Bbbk$-algebre

$$\alpha_{\mathscr{V},\mathscr{V}} : \mathrm{End}(V) \longrightarrow M_n(\Bbbk)$$

(significa un isomorfismo lineare che rispetta identità e moltiplicazione, ovvero $\alpha_{\mathscr{V},\mathscr{V}}(\mathrm{id}_V) = \mathbb{I}_n$ e $\alpha_{\mathscr{V},\mathscr{V}}(\varphi \circ \psi) = \alpha_{\mathscr{V},\mathscr{V}}(\varphi)\alpha_{\mathscr{V},\mathscr{V}}(\psi)$).

Se inoltre $\mathscr{V}'$ è un'altra base di V, allora i due isomorfismi $\alpha_{\mathscr{V},\mathscr{V}}$ e $\alpha_{\mathscr{V}',\mathscr{V}'}$ differiscono per l'automorfismo interno di $M_n(\Bbbk)$ legato alla matrice di cambiamento di base $H = \alpha_{\mathscr{V},\mathscr{V}'}(\mathrm{id}_V)$, cioè al morfismo che manda una matrice X nella matrice $H^{-1}XH$. In altri termini abbiamo un diagramma commutativo di isomorfismi di $\Bbbk$-algebre

$$\begin{tikzcd}
\mathrm{End}(V) \arrow[r, "\alpha_{\mathscr{V},\mathscr{V}}"] \arrow[d, equal] & M_n(\Bbbk) \arrow[d, "\iota_H"] \\
\mathrm{End}(V) \arrow[r, "\alpha_{\mathscr{V}',\mathscr{V}'}"'] & M_n(\Bbbk)
\end{tikzcd}$$

dove $\iota_H(X) = H^{-1}XH$.

L'isomorfismo $\alpha_{\mathscr{V},\mathscr{V}}$ si restringe ad un isomorfismo di gruppi (non abeliani)

$$\alpha_{\mathscr{V},\mathscr{V}} : \mathrm{Aut}(V) \longrightarrow \mathrm{GL}_n(\Bbbk)$$

tra il gruppo degli automorfismi di V (mappe lineari invertibili) con l'operazione di composizione, e il gruppo generale lineare delle matrici invertibili con l'operazione di prodotto.

♠ **3.6.** Problema: disuguaglianze di Frobenius. Date due applicazioni lineari $\varphi : U \to V$ e $\psi : V \to W$, mostrare che $\dim \mathrm{im}\,(\psi \circ \varphi) \geqslant \dim \mathrm{im}\,\varphi + \dim \mathrm{im}\,\psi - \dim V$. Più precisamente si dimostra che

$$\begin{aligned}\dim \mathrm{im}\,(\psi \circ \varphi) &= \dim(\mathrm{im}\,\varphi + \ker \psi) - \dim \ker \psi = \dim(\mathrm{im}\,\varphi + \ker \psi) + \dim \mathrm{im}\,\psi - \dim V \\ &= \dim \mathrm{im}\,\varphi - \dim(\mathrm{im}\,\varphi \cap \ker \psi)\end{aligned}$$

o anche che

$$\dim \mathrm{im}\,(\psi \circ \varphi) = \dim(\mathrm{im}\,\varphi) - \dim(\mathrm{im}\,\varphi \cap \ker \psi)$$

e in particolare $\dim \mathrm{im}\,(\psi \circ \varphi) = \dim \mathrm{im}\,\varphi$ se e solo se $\mathrm{im}\,\varphi \cap \ker \psi = 0$ (conviene anche osservare che $\dim \mathrm{im}\,(\psi \circ \varphi) \leqslant \dim \mathrm{im}\,\varphi$).

Dedurne che, date due matrici $A \in M_{m,n}(\Bbbk)$ e $B \in M_{n,l}(\Bbbk)$, si ha $\mathrm{rg}(AB) \geqslant \mathrm{rg}(A) + \mathrm{rg}(B) - n$ (e $\mathrm{rg}(AB) \leqslant \mathrm{rg}(A)$).

3.6.1. Date tre applicazioni lineari $\varphi : U \to V$, $\psi : V \to W$ e $\eta : W \to \mathbb{U}$ ("doppia U", nuova lettera dell'alfabeto da poco introdotta), mostrare che

$$\dim \mathrm{im}\,(\eta \circ \psi \circ \varphi) \geqslant \dim \mathrm{im}\,(\psi \circ \varphi) + \dim \mathrm{im}\,(\eta \circ \psi) - \dim \mathrm{im}\,\psi$$

(e dedurne la disuguaglianza precedente; si osservi però che non è possibile dedurre questa disuguaglianza dalla precedente...).

Di conseguenza abbiamo che $\mathrm{rg}(ABC) \geqslant \mathrm{rg}(AB) + \mathrm{rg}(BC) - \mathrm{rg}(B)$ per ogni tre matrici moltiplicabili...

3.6.2. Entrambe le disuguaglianze precedenti si possono ottenere usando opportunamente questa facile osservazione: se $\varphi : V \to W$ è applicazione lineare e $U \leqslant V$, consideriamo $\varphi_{|U} : U \to \varphi(U)$; siccome $\ker(\varphi_{|U}) \leqslant \ker(\varphi)$, risulta $\dim U - \dim \varphi(U) \leqslant \dim V - \dim \mathrm{im}\,\varphi$.

4. Dualità.

4.1. Definizione (spazio duale). *Sia V uno spazio vettoriale su $\Bbbk$ di dimensione finita n. Definiamo il suo duale come $V^* := \mathrm{Hom}_{\Bbbk}(V, \Bbbk)$ (applicazioni lineari di V in $\Bbbk$), che ha una struttura naturale di $\Bbbk$-spazio vettoriale data da $(v^*+w^*)(v) := v^*(v)+w^*(v)$ e $(\alpha v^*)(v) := \alpha v^*(v)$ per $v^*, w^* \in V^*$ e $\alpha \in \Bbbk$. Gli elementi di V^* si chiamano spesso forme lineari o covettori.*

4.2. Definizione-Proposizione (basi duali). *Data una base $\mathscr{V} = (v_1, \dots, v_n)$ di V, gli elementi v_i^* di V^* definiti da $v_i^*(v_j) := \delta_{i,j}$ formano una base di V^*; $\mathscr{V}^* = (v_1^*, \dots, v_n^*)$ si dice la*

base duale di $\mathscr{V}$. In particolare $\dim_{\Bbbk} V^* = \dim_{\Bbbk} V$ *(dunque V e V^* sono isomorfi, ma non in modo canonico).*

Dimostrazione. Dimostriamo che $\mathscr{V}^*$ è un insieme linearmente indipendente: se $\sum \alpha_1 v_i^* = 0$, allora, calcolando in v_j troviamo $\alpha_j = (\sum \alpha_1 v_i^*)v_j = 0$ per ogni $j = 1, \dots, n$. Dimostriamo che $\mathscr{V}^*$ è un insieme generatore: se $\varphi \in V^*$, consideriamo $f_i = \varphi(v_i) \in \Bbbk$; allora $\varphi = \sum_i f_i v_i^*$. Per verificare l'uguaglianza basta verificarla per gli elementi della base $\mathscr{V}$, ed è evidente. □

4.2.1. Si osservi che per ogni vettore $v \in V$ (e per ogni base $\mathscr{V} = (v_1, \dots, v_n)$ di V) si ha $v = \sum_i v_i^*(v)v_i$, cioè le coordinate di v nella base $\mathscr{V}$ sono esattamente i valori di v sulla base duale: $\alpha_{\mathscr{V}}(v) = (v_i^*(v))$.

4.3. Definizione-Proposizione (duale di applicazioni lineari). *Se $\varphi : V \longrightarrow W$ è una applicazione lineare, allora definiamo $\varphi^* : W^* \longrightarrow V^*$ tramite la composizione (di applicazioni lineari) $\varphi^*(w^*) = w^* \circ \varphi$, cioè $\varphi^*(w^*)(v) := w^*(\varphi(v))$ per ogni $v \in V$ (i.e. $v \circ (\varphi^* w^*) = (\varphi v) \circ w^*$ $(\forall v \in V,\ \forall w^* \in W^*)$). Abbiamo che* $\mathrm{id}_V^* = \mathrm{id}_{V^*}$, $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Dimostrazione. Esercizio. □

4.3.1. Proposizione (matrice dell'applicazione duale). *La matrice di φ^* nelle basi duali delle basi $\mathscr{V}$ di V e $\mathscr{W}$ di W è data dalla trasposta della matrice di φ in quelle basi:* $\alpha_{\mathscr{W}^*,\mathscr{V}^*}(\varphi^*) = \alpha_{\mathscr{V},\mathscr{W}}(\varphi)^{\mathrm{t}}$.

Dimostrazione. Si verifica con il calcolo diretto (indichiamo con $a_{i,j}$ le entrate di $\alpha_{\mathscr{V},\mathscr{W}}(\varphi)$ e con $a_{i,j}^*$ le entrate di $\alpha_{\mathscr{W}^*,\mathscr{V}^*}(\varphi^*)$): da $\varphi^*(w_i^*) = \sum_k a_{k,i}^* v_k^*$, calcolando in v_j otteniamo per il primo termine $\varphi^*(w_i^*)v_j = w_i^*(\varphi v_j) = w_i^*(\sum_k a_{k,j} w_k) = a_{i,j}$, mentre il secondo termine dà $(\sum_k a_{k,i}^* v_k^*)(v_j) = a_{j,i}^*$; si conclude che $a_{j,i}^* = a_{i,j}$. □

4.4. Definizione-Teorema (di (bi)dualità). *Il morfismo canonico: $V \longrightarrow V^{**} :\ v \mapsto \mathrm{ev}(v)$ ove $\mathrm{ev}(v)(v^*) := v^*(v) = v \circ v^*$ è un isomorfismo di spazi vettoriali (Notare che non c'è un isomorfismo canonico tra V e V^*). Sotto questa identificazione, per un morfismo $\varphi : V \to W$, risulta $\varphi^{**} = \varphi$, ovvero abbiamo un diagramma commutativo di isomorfismi*

$$\begin{tikzcd} V \arrow[r, "\mathrm{ev}_V"] \arrow[d, "\varphi"'] & V^{**} \arrow[d, "\varphi^{**}"] \\ W \arrow[r, "\mathrm{ev}_W"'] & W^{**} \end{tikzcd} .$$

Dimostrazione. Trattandosi di spazi di dimensione finita, basta verificare che $\ker(\mathrm{ev}) = 0$, e di tratta della proprietà di non degenerazione $(N2)$ qui sotto. □

Insistiamo sul fatto che non esista un isomorfismo canonico tra V e il suo duale V^*; tuttavia esistono relazioni molto strette tra il reticolo dei sottospazi di V e quello dei sottospazi di V^*, che cerchiamo ora di esplicitare.

4.5. Proposizione (dualità). *Esiste una applicazione canonica:*

$$V \times V^* \longrightarrow \Bbbk :\ (v, v^*) \mapsto v \circ v^* := v^*(v)$$

che gode delle seguenti proprietà:
(B) *bilineare, cioè soddisfa alle condizioni:*
- $(B1)$ $v \circ (v^* + w^*) = v \circ v^* + v \circ w^*$,
- $(B2)$ $(v + w) \circ v^* = v \circ v^* + w \circ v^*$,
- $(B3)$ $(\lambda v) \circ v^* = \lambda(v \circ v^*) = v \circ (\lambda v^*)$;

(N) *non degenere, cioè soddisfa alle condizioni:*
- $(N1)$ *se $v \circ v^* = 0$ per ogni $v \in V$ allora $v^* = 0$,*
- $(N2)$ *se $v \circ v^* = 0$ per ogni $v^* \in V^*$ allora $v = 0$.*

Dimostrazione. Facile esercizio, ma si faccia bene attenzione alla proprietà $(N2)$, che è, almeno apparentemente, molto diversa dalla $(N1)$ (quest'ultima dice semplicemente che una applicazione è nulla se dà risultato zero su ogni vettore; invece l'altra dice che un vettore che viene annullato da ogni forma lineare dev'essere nullo...). □

4.6. Definizione-Proposizione (ortogonalità). *Nozione di ortogonale: per ogni sottinsieme S di V (risp. V^*) definiamo un sottospazio di V^* (risp. V), detto ortogonale di S,*

$$S^\perp := \{v^* \in V^* \ : \ s \circ v^* = 0 \ (\forall s \in S)\} \qquad (\text{risp.} \quad \{v \in V \ : \ v \circ s = 0 \ (\forall s \in S)\}) \ .$$

Proprietà dell'ortogonale:
$(O1)$ *se $S \subseteq T$ allora $T^\perp \subseteq S^\perp$;*
$(O2)$ *$S^{\perp\perp} = \langle S \rangle$; $W^{\perp\perp} = W$ se W è un sottospazio; $S^{\perp\perp\perp} = S^\perp$;*
$(O3)$ *$(W+W')^\perp = W^\perp \cap W'^\perp$ per ogni W e W' sottospazi di V;*
$(O4)$ *$(W \cap W')^\perp = W^\perp + W'^\perp$ per ogni W e W' sottospazi di V;*
in particolare il passaggio all'ortogonale induce un antiisomorfismo involutorio tra i reticoli di sottospazi di V e V^*; inoltre $\dim_{\Bbbk}(W^\perp) = n - \dim_{\Bbbk} W$.

Dimostrazione. Esercizio; si tenga presente che basta considerare sottinsiemi S di V (usando il teorema di (bi)dualità) e si osservi che $(O4)$ segue da $(O3)$ (molto più facile da verificare), passando agli ortogonali. □

4.7. Definizione-Proposizione (nucleo e immagine di applicazioni duali). *Data una applicazione lineare $\varphi : V \longrightarrow W$, allora $\operatorname{im}(\varphi^*) = \ker(\varphi)^\perp$ e $\ker(\varphi^*) = \operatorname{im}(\varphi)^\perp$. In particolare $\operatorname{rg}(\varphi^*) = \operatorname{rg}\varphi$.*

Dimostrazione. Le due asserzioni seguono una dall'altra, e la seconda è facile da verificare: $v^* \in \ker(\varphi^*)$ sse $\varphi^*(v^*) = 0$ sse $\varphi^*(v^*)(v) = 0$ per ogni $v \in V$, e questo significa $v^*(\varphi(v)) = 0$ per ogni $v \in V$, cioè $v^*(v') = 0$ per ogni $v' \in \operatorname{im}(\varphi)$, e quindi se e solo se $v^* \in \operatorname{im}(\varphi)^\perp$. □

4.7.1. Dall'ultima affermazione segue che per ogni matrice, il rango (per colonne) ed il rango per righe coincidono (il primo è il rango della applicazione lineare associata a quella matrice, il secondo coincide con il rango della applicazione duale). Quindi per ogni matrice $A \in M_{n,m}(\Bbbk)$ abbiamo $\operatorname{rg}(A) = \operatorname{rg}(A^{\mathrm{t}})$. In particolare le applicazioni lineari associate hanno stessa dimensione dell'immagine (ma in generale nuclei di dimensione diverse, rispettivamente $m - r$ ed $n - r$).

4.7.2. Problema. Questa osservazione può comportare qualche confusione in quanto riguarda le matrici, e si tende a confondere uno spazio standard con il suo duale; tuttavia ha un certo interesse pratico. Supponiamo che il campo $\Bbbk$ sia tale che per ogni $w \in \Bbbk^n$, $w \neq 0$, si abbia $w^{\mathrm{t}} w \neq 0$ (ovvero $w^{\mathrm{t}} w = 0$ implichi $w = 0$, si dice che lo spazio non ha vettori isotropi non nulli). Per esempio $\Bbbk = \mathbb{Q}, \mathbb{R}$ (somme di quadrati, non tutti nulli, non sono nulle) ma non $\mathbb{C}$. Allora, presa una matrice $A \in M_{n,m}(\Bbbk)$ e dette $\varphi_A : \Bbbk^m \to \Bbbk^n$ e $\varphi_{A^{\mathrm{t}}} : \Bbbk^n \to \Bbbk^m$, si può mostrare che $\operatorname{im}(\varphi_A)$ e $\ker(\varphi_{A^{\mathrm{t}}})$ sono complementari in $\Bbbk^n$ (e che $\operatorname{im}(\varphi_{A^{\mathrm{t}}})$ e $\ker(\varphi_A)$ sono complementari in $\Bbbk^m$). Usando la formula di Grassmann, basta mostrare che l'intersezione è banale.

Sotto le stesse condizioni (non-isotropia) si ha: se $A \in M_{n,m}(\Bbbk)$, allora $A^{\mathrm{t}} A \in M_m(\Bbbk)$ e $AA^{\mathrm{t}} \in M_n(\Bbbk)$ sono matrici simmetriche e hanno entrambe rango pari al rango di A.

4.7.3. Si osservi anche che φ è iniettiva (risp. suriettiva) se e solo se φ^* è suriettiva (risp. iniettiva).

4.7.4. Teorema (duali di sottospazi e quozienti). *Dato un sottospazio W di V, l'inclusione canonica $W \to V$ induce una mappa suriettiva $V^* \to W^*$ di nucleo $W^\perp$, da cui deduciamo che $W^* \cong V^*/W^\perp$. Inoltre risulta $(V/W)^* \cong W^\perp$.*

Dimostrazione. Il primo risultato è chiaro dal primo teorema di isomorfismo. Per il secondo basta applicare il primo sostituendo V con V^* e W con $W^\perp$, e poi passare al duale: da $(W^\perp)^* \cong (V^*)^*/(W^\perp)^\perp \cong V/W$ si ottiene $W^\perp \cong (W^\perp)^{**} \cong (V/W)^*$; oppure osservare che la proiezione $\pi : V \to V/W$ ha come duale una applicazione iniettiva $\pi^* : (V/W)^* \to V^*$ con $\operatorname{im}(\pi^*) = \ker(\pi)^\perp = W^\perp$ (e applicare il primo teorema di isomorfismo). □

4.8. Conclusione. Si osservi che la scelta di una base di V dà una identificazione di V con $M_{n,1}(\Bbbk)$, e anche di V^* con $M_{1,n}(\Bbbk)$ (usando la base 1 di $\Bbbk$). In questa identificazione il morfismo bilineare canonico $V^* \times V \to \Bbbk$ si scrive come il prodotto di matrici

$$M_{1,n}(\Bbbk) \times M_{n,1}(\Bbbk) \longrightarrow M_{1,1}(\Bbbk) = \Bbbk \ .$$

In un certo senso possiamo dire che lo spazio duale di V è lo spazio vettoriale delle "equazioni di iperpiani di V" (ogni elemento di V^*, in quanto funzione lineare, identifica il suo nucleo, che è un sottospazio di V: di dimensione $n-1$ in generale), tenendo conto che il covettore nullo non descrive un iperpiano ma tutto lo spazio V, e che due covettori descrivono lo stesso iperpiano se e solo se sono non nulli e proporzionali (cioè linearmente dipendenti, condizione necessaria e sufficiente affinché abbiano lo stesso nucleo). In conclusione abbiamo una funzione biiettiva tra $V^* \smallsetminus \{0\}/\Bbbk^\times$ (covettori non nulli modulo proporzionalità sul campo) e iperpiani di V (mandando φ in $\ker\varphi$). L'ortogonale di un vettore è allora il sottospazio delle equazioni di iperpiani che contengono quel vettore; l'ortogonale di un sottospazio di V è l'insieme delle equazioni di iperpiani di V che contengono quel sottospazio.

4.9. Problema. Siano dati due sottospazi $U \leqslant W$ di uno spazio vettoriale V. Mostrare che:
(0) $(W/U)^*$ è canonicamente isomorfo a $U^\perp/W^\perp$.

Usando il risultato precedente, ma anche direttamente, dimostrare che per due sottospazi U, W di V si ha:
(1) $((U+W)/W)^*$ è canonicamente isomorfo a $W^\perp/(U^\perp \cap W^\perp)$;
(2) $(W/(U\cap W))^*$ è canonicamente isomorfo a $(U^\perp + W^\perp)/W^\perp$.

4.10. Problema. Siano V e W spazi vettoriali su $\Bbbk$ di dimensione finita; mostrare che:
(3) $(V\times W)^* = V^* \times W^*$ (isomorfismo canonico);

♠♠ **4.11.** Problema. Siano V e W spazi vettoriali su $\Bbbk$ di dimensione finita; mostrare che:
(4) $\mathrm{Hom}_\Bbbk(V,W)^* = \mathrm{Hom}_\Bbbk(V^*,W^*) = \mathrm{Hom}_\Bbbk(W,V)$ (isomorfismi canonici!).

In particolare $\mathrm{End}_\Bbbk(V)$ è (canonicamente!) isomorfo al proprio duale $\mathrm{End}_\Bbbk(V)^*$ (immagine della funzione identica di V è la traccia di endomorfismi, che a sua volta è mappa duale dell'inclusione di $\Bbbk$ in $\mathrm{End}(V)$ a meno delle identificazioni canoniche), cosa falsa in generale per uno spazio vettoriale.

Attenzione: questo problema si risolve facilmente conoscendo la nozione di prodotto tensoriale (usando $\mathrm{Hom}_\Bbbk(V,W) = V^* \otimes_\Bbbk W$ *e* $(V\otimes_\Bbbk W)^* = V^* \otimes_\Bbbk W^*$*), ma è piuttosto difficile altrimenti e richiede la conoscenza (o la scoperta) della funzione traccia (di un endomorfismo). È scritto qui comunque solo per completezza, essendo del tutto naturale chiedersi come la dualità si comporta con gli spazi di omomorfismi...*

♠♠ **4.12.** Problema. In questa sezione abbiamo parlato solo di spazi vettoriali di dimensione finita, ma le definizioni potevano esser date per spazi vettoriali arbitrari. Farsi degli esempi per vedere che quasi tutti i risultati riportati sono falsi per spazi vettoriali di dimensione infinita (si studi in particolare lo spazio vettoriale duale dello spazio dei polinomi, e lo si identifichi con lo spazio vettoriale delle serie formali). Più in generale, si identifichi lo spazio duale della somma diretta $\Bbbk^{(X)}$ con il prodotto diretto $\Bbbk^X$ (se X è un insieme infinito, per esempio $\mathbb{N}$, i due non sono isomorfi).

5. Esercizi.

5.-1. Realizzazione matriciale dei campi finiti. Conosciamo già una situazione in cui un campo estensione finita di un'altro ammette una biiezione con una sottoalgebra delle matrici del sottocampo: usando $\mathbb{R}$ e l'estensione $\mathbb{C}$ (che ha base $1, i$ su $\mathbb{R}$ come spazio vettoriale, e come campo si ottiene aggiungendo a $\mathbb{R}$ una radice di X^2+1). Le moltiplicazioni per 1 (identità) e per i danno due endomorfismi $\mathbb{R}$-lineari di $\mathbb{C}$ che nella base $1, i$ hanno matrici $\mathbb{I} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ e $\mathbb{J} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Identificando $x+iy \in \mathbb{C}$ con la matrice $x\mathbb{I} + y\mathbb{J} = \left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)$ si ha la biiezione voluta che dà un isomorfismo del campo $\mathbb{C}$ con la sottoalgebra delle matrici $M_2(\mathbb{R})$ generata da $\mathbb{I}$ e $\mathbb{J}$.

Una costruzione simile si può fare per tutte le estensioni finite $\mathbb{F}_q$ di $\mathbb{F}_p$ con $q = p^r$.

Per esempio $\mathbb{F}_4$ è l'estensione di $\mathbb{F}_2$ i cui elementi soddisfano a $X^4 - X = X(X-1)(X^2+X+1)$ (polinomio con coefficienti in $\mathbb{F}_2$), e quindi è l'estensione di $\mathbb{F}_2$ che si ottiene aggiungendo un elemento a tale che $a^2+a+1=0$, ovvero $a^2 = a+1$ (non ci sono errori: in $\mathbb{F}_2$ abbiamo $1=-1$). Ora, le moltiplicazioni per 1 e per a danno endomorfismi $\mathbb{F}_2$-lineari di $\mathbb{F}_4$ che usando la base $1, a$ corrispondono alle matrici in $M_2(\mathbb{F}_2)$ date da $\mathbb{I} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ e $\mathbb{A} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Quindi identificando $x+ay \in \mathbb{F}_4$ (dove $x, y \in \mathbb{F}_2$) con la matrice $x\mathbb{I} + y\mathbb{A} = \left(\begin{smallmatrix} x & y \\ y & x+y \end{smallmatrix}\right)$ si ha la biiezione voluta che dà un isomorfismo del campo $\mathbb{F}_4$ con

la sottoalgebra delle matrici $M_2(\mathbb{F}_2)$ data dalle quattro matrici $\mathbb{O} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\mathbb{I} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathbb{A} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, $\mathbb{I}+\mathbb{A} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Vi sono altre sottoalgebre di $M_2(\mathbb{F}_2)$ isomofe a questa?

Similmente, $\mathbb{F}_8$ è l'estensione di $\mathbb{F}_2$ i cui elementi soddisfano a $X^8 - X = X(X-1)(X^3+X^2+1)(X^3+X+1)$ (polinomio con coefficienti in $\mathbb{F}_2$), e quindi è l'estensione di $\mathbb{F}_2$ che si ottiene aggiungendo un elemento b tale che $b^3+b+1=0$, ovvero $b^3 = b+1$ (vedi sopra). Ora, le moltiplicazioni per 1, per b e per b^2 danno endomorfismi $\mathbb{F}_2$-lineari di $\mathbb{F}_8$ che usando la base $1, b, b^2$ corrispondono alle matrici in $M_3(\mathbb{F}_2)$ date da $\mathbb{I} = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $\mathbb{B} = \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$, $\mathbb{B}^2 = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{smallmatrix}\right)$. Dunque possiamo identificare ogni elemento $x + by + b^2z \in \mathbb{F}_8$ (dove $x, y, z \in \mathbb{F}_2$) con la matrice $x\mathbb{I} + y\mathbb{B} + z\mathbb{B}^2 \in M_3(\mathbb{F}_2)$ per avere un isomorfismo di campi tra $\mathbb{F}_8$ e la sottoalgebra delle matrici in $M_3(\mathbb{F}_2)$ data dalle otto matrici $\mathbb{O} = \left(\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$, $\mathbb{I}$, $\mathbb{B}$, $\mathbb{B}^2$, $\mathbb{I}+\mathbb{B}$, $\mathbb{I}+\mathbb{B}+\mathbb{B}^2$, $\mathbb{I}+\mathbb{B}^2$, $\mathbb{B}+\mathbb{B}^2 = \mathbb{B}(\mathbb{I}+\mathbb{B})$. Vi sono altre sottoalgebre di $M_3(\mathbb{F}_2)$ isomofe a questa?

Provare con $\mathbb{F}_9$ estensione di $\mathbb{F}_3$...

5.0. Consideriamo un primo p in $\mathbb{Z}$ e una sua potenza $q = p^r$ (si può pensare $r = 1$, cioè $q = p$ per semplicità). Sappiamo che esiste un (unico) campo finito $\mathbb{F}_q$ che ha esattamente q elementi ed è un campo di caratteristica p.

Consideriamo ora l'algebra della matrici $M_n(\mathbb{F}_q)$:
(a) determinare il numero di matrici e il numero di matrici invertibili;
(b) per ogni intero m fino a n determinare il numero di matrici di rango m;
(c) determinare il numero di matrici di simmetrie.

5.1. Esercizi su Applicazioni Lineari.

5.1.1. Si consideri l'applicazione f di $\mathbb{R}^2$ in $\mathbb{R}^4$ definita da $f\binom{s}{t} = \begin{pmatrix} 2s+t \\ s-t \\ s+t \\ s+2t \end{pmatrix}$.
(a) Si mostri che f è lineare;
(b) si determini $\ker(f)$;
(c) si trovi una base di $\operatorname{im}(f)$.

5.1.2. Si consideri l'omomorfismo f di $\mathbb{R}^3$ in $\mathbb{R}^2$ definito da $f\begin{pmatrix} r \\ s \\ t \end{pmatrix} = \binom{r+s+t}{2r-s}$.
(a) Si mostri che f è suriettivo;
(b) si determini $\ker(f)$;
(c) trovare $v \in \mathbb{R}^3$ tale che $f^{-1}(\binom{1}{2}) = v + \ker(f)$;
(d) mostrare che per ogni $\binom{a}{b} \in \mathbb{R}^2$, esiste $v \in \mathbb{R}^3$, tale che $f^{-1}(\binom{a}{b}) = v + \ker(f)$.

5.1.3. Considerare l'operazione di derivazione $D = \frac{d}{dX}$ come funzione di $\mathbb{R}[X]$ in sé, di $\mathbb{R}[X]_{\leqslant n}$ in sé, di $\mathbb{R}[[X]]$ in sé (per definizione abbiamo $D(\sum_i \alpha_i X^i) = \sum_i i\alpha_i X^{i-1}$). In ciascuno dei tre casi:
(*a*) verificare che si tratta di una applicazione $\mathbb{R}$-lineare;
(*b*) descrivere nucleo e immagine di D, specificando le dimensioni;
(*c*) determinare se D è o meno iniettiva, suriettiva, biiettiva;
(*d*) ripetere l'esercizio sostituendo $\mathbb{R}$ con il corpo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

5.1.4. Per ognuna delle seguenti condizioni, definire se possibile un endomorfismo di $\mathbb{R}^3$ (non nulli e) che la verifichi:
(*a*) nucleo e immagine coincidano;
(*b*) il nucleo contenga l'immagine;
(*c*) il nucleo sia non nullo e contenuto nell'immagine;
(*d*) nucleo e immagine siano complementari;
(*e*) il nucleo sia diverso dall'immagine e la somma dei due non sia diretta.
Stesso problema nel caso di endomorfismi di $\mathbb{R}^4$.

5.1.5. Sia V uno spazio vettoriale sul corpo $\Bbbk$. Verificare che
(a) se $\alpha : V \to V$ è una applicazione lineare, allora $\{v \in V : \alpha(v) = v\}$ è un sottospazio di V;
(b) se $W \leqslant V$, allora esiste una applicazione lineare $\beta : V \to V$ tale che $\{v \in V : \beta(v) = v\} = W$.

5.1.6. Sia V uno spazio vettoriale su $\mathbb{R}$ di dimensione 3 e base v_1, v_2, v_3. Sia φ_λ l'applicazione lineare definita da

$$\varphi(v_1) = (\lambda-1)v_1 + 2v_2 - (\lambda+1)v_3, \qquad \varphi(v_2) = 2v_1 - \lambda v_3, \qquad \varphi(v_3) = -\lambda v_1 - v_2 + (\lambda+2)v_3$$

al variare di $\lambda \in \mathbb{R}$
(a) determinare immagine e nucleo di φ_λ al variare di λ;
(b) per quali valori di λ l'immagine dell'applicazione φ_λ contiene il vettore $v_1 + 2v_2 + 2v_3$?
(c) l'unione dei nuclei di φ_λ al variare di λ genera V?

5.1.7. Scrivere le proiezioni su U nella direzione di W, e di W nella direzione di U per i seguenti due sottospazi di $\mathbb{R}^3$: $U = \langle \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \rangle$ e $W = \langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \rangle$.

5.1.8. Scrivere le proiezioni su U nella direzione di W, e di W nella direzione di U per i seguenti due sottospazi di $\mathbb{R}^4$: $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \rangle$ e W definito da $\begin{cases} x_1 + x_2 = 0 \\ x_3 - x_4 = 0 \end{cases}$

5.1.9. Si considerino gli $\mathbb{R}$-spazi vettoriali $\mathbb{R}^m$ e $\mathbb{R}^n$.
(a) Si mostri che una applicazione di $\mathbb{R}^n$ in $\mathbb{R}$ è lineare se e solo se è del tipo seguente:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto A_1 a_1 + \ldots + A_n a_n,$$

ove $A_1, \ldots, A_n$ sono numeri reali fissati, cioè una funzione polinomiale omogenea di grado 1. Un caso particolare è l'applicazione di $\mathbb{R}^n$ in $\mathbb{R}$ definita da $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto a_i$, ove $1 \leqslant i \leqslant n$; essa si indica con pr_i, e si dice la proiezione i-esima.
(b) Si mostri che un'applicazione $f : \mathbb{R}^m \to \mathbb{R}^n$ è lineare se e solo se sono lineari le applicazioni $\mathrm{pr}_i \circ f$ per ogni i, $1 \leqslant i \leqslant n$.

5.1.10. Siano U, V spazi vettoriali sul campo $\Bbbk$. Siano W, Z sottospazi di U tali che $W \cap Z = 0$. Dimostrare che se $f : W \to V$ e $g : U \to V$ sono applicazioni lineari, esiste una applicazione lineare $h : U \to V$ tale che $h_{|W} = f$ e $h_{|Z} = g$. Quando h è unica?

5.1.11. Sia P_n lo spazio vettoriale dei polinomi reali di grado $\leqslant n$, e sia $D : P_n \to P_n$ l'usuale derivazione, $D(f) = f'$. Si consideri l'applicazione $\varphi : P_n \to P_n$, $f \mapsto f + xf'$.
(a) Verificare che effettivamente $f + xf' \in P_n$ se $f \in P_n$.
(b) Dimostrare che φ è lineare.
(c) Dimostrare che φ è un isomorfismo.

5.1.12. Si consideri l'endomorfismo $f_{a,b}$ di $\mathbb{R}^2$ determinato dalle condizioni $f_{a,b}(e_1) = 2e_1 + ae_2$ e $f_{a,b}(e_2) = be_1 + e_2$, dove $\{e_1, e_2\}$ è la base canonica di $\mathbb{R}^2$, a, $b \in \mathbb{R}$. Dimostrare che il sottospazio $U = \langle e_1 - e_2 \rangle$ è $f_{a,b}$-stabile (cioè che $f_{a,b}(U) \subseteq U$) se e solo se $a - b + 1 = 0$.

5.1.13. Si considerino i sottoinsiemi $B_t = \{\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2t \\ 0 \end{pmatrix}, \begin{pmatrix} t \\ 3 \\ 1 \end{pmatrix}\}$ di $\mathbb{R}^3$, per ogni $t \in \mathbb{R}$.
(a) Per quali valori di t l'insieme B_t è una base di $\mathbb{R}^3$?
(b) Per quali valori di t esiste un endomorfismo φ di $\mathbb{R}^3$ tale che $\varphi \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $\varphi \begin{pmatrix} 1 \\ 2t \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, $\varphi \begin{pmatrix} t \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$?
(c) Per quali valori di t l'endomorfismo di cui in (b) è unico?

5.1.14. Sia M il campo $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, e sia $f : M \to M$ l'applicazione definita mediante $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, $a, b \in \mathbb{Q}$.
(a) Verificare che M è spazio vettoriale su $\mathbb{Q}$ di dimensione 2.
(b) Verificare che M è spazio vettoriale su M di dimensione 1.
(c) Verificare che f è una applicazione $\mathbb{Q}$-lineare.
(d) Verificare che f non è una applicazione M-lineare.

5.1.15. Siano V e W due spazi vettoriali su $\mathbb{R}$.
(a) Siano f un'applicazione lineare di V in W e $G_f \subset V \times W$ il suo grafico. Si mostri che se f è lineare, allora G_f è un sottospazio vettoriale di $V \times W$.
(b) Sia $G \subset V \times W$ un sottospazio; si mostri che $G = G_f$ per un qualche omomorfismo f, se e solo se l'applicazione π_V da G in V, definita da $(v, w) \mapsto v$, è un isomorfismo.
(c) Si supponga che sia $G = G_f$ per un qualche omomorfismo f. Si mostri che esiste una applicazione lineare π_W da G in W tale che $f = \pi_W \circ \pi_V^{-1}$.

5.1.16. Siano V e W spazi vettoriali su $\Bbbk$ con basi v_1, v_2, v_3, v_4 e w_1, w_2, w_3 rispettivamente.

(a) dire se esiste una applicazione lineare φ tale che

$$\varphi(v_1 + v_2 + v_3 + v_4) = w_1 + w_2 + w_3 \qquad \varphi(v_1 + v_2) = w_1 - w_2$$
$$\varphi(v_1 + v_2 + v_3) = 2w_1 + 2w_2 + 2w_3 \qquad \varphi(v_1 - v_2) = w_1 - w_2$$

ed eventualmente se è unica o no; calcolare nucleo e immagine, discutere iniettività e suriettività;

(b) mostrare che il sottinsieme $\{\psi \in \mathrm{End}_{\mathbb{R}}(V) : \varphi \circ \psi = 0\}$ è un sottospazio vettoriale di $\mathrm{End}_{\mathbb{R}}(V)$ e calcolarne la dimensione e una base;

(c) mostrare che il sottinsieme $\{\vartheta \in \mathrm{End}_{\mathbb{R}}(W) : \vartheta \circ \varphi = 0\}$ è un sottospazio vettoriale di $\mathrm{End}_{\mathbb{R}}(W)$ e calcolarne la dimensione e una base.

5.2. Esercizi su Matrici.

5.2.1. Sia $D : \Bbbk[X]_{\leqslant 4} \to \Bbbk[X]_{\leqslant 4}$ l'usuale derivazione tra polinomi;
(a) scrivere la matrice associata a D nella base canonica $1, X, X^2, X^3, X^4$;
(b) trovare una base di $\Bbbk[X]_{\leqslant 4}$ fatta di polinomi di grado 4 e scrivere la matrice associata a D in questa base;
(c) scrivere la matrice di cambiamento di base tra le due basi precedenti, e verificare la relazione di cambiamento di base per le due matrici associate a D;
(d) esistono mappe inverse a destra o a sinistra per D? in caso affermativo, scriverne le matrici nelle due basi date e verificare la relazione con le matrice di D;
(e) ripetere tutto usando $D : \Bbbk[X]_{\leqslant 4} \to \Bbbk[X]_{\leqslant 3}$.

5.2.2. Sia $f : \mathbb{R}^3 \to \mathbb{R}^3$ l'applicazione lineare definita da $f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x+y \\ y+z \\ z+x \end{pmatrix}$.
(a) Scriverne la matrice in base canonica;
(b) scriverne la matrice nella base v_1, v_2, v_3 ove v_j è il vettore di coordinate tutte uguali a 1 tranne la j-esima uguale a 0;
(c) scrivere la matrice di cambiamento di base e verificare la relazione tra le due matrici di f;
(d) discutere iniettività e suriettività di f.

5.2.3. Consideriamo la proiezione p su V nella direzione di W e la proiezione q su W nella direzione di V ove $V = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \rangle$ e $W = \langle \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rangle$sono sottospazi di $\mathbb{R}^4$.
(a) verificare che $\mathbb{R}^4 = V \oplus W$ e scrivere le matrici di p e q nella base di $\mathbb{R}^4$ formata giustapponendo le basi di V e di W;
(b) si scrivano le matrici A e B di p e q nella base canonica di $\mathbb{R}^4$;
(c) esplicitare le matrici di cambiamento di base e verificare le relazioni tra le matrici precedentemente trovate;
(d) vero che $AB = BA = 0$?

Consideriamo ora la simmetria s di centro V e di asse W e la simmetria t di centro W e di asse V .
(a') verificare che $\mathbb{R}^4 = V \oplus W$ e scrivere le matrici di s e t nella base di $\mathbb{R}^4$ formata giustapponendo le basi di V e di W;
(b') si scrivano le matrici A e B di s e t nella base canonica di $\mathbb{R}^4$;
(c') esplicitare le matrici di cambiamento di base e verificare le relazioni tra le matrici precedentemente trovate;
(d') vero che $AB = BA$? vero che $A^2 = B^2 = \mathbb{I}_4$?

5.2.4. Sia $L : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ l'applicazione definita da $L\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
(a) Verificare che si tratta di una applicazione lineare e scriverne la matrice nella base canonica;
(b) trovare una base del nucleo di L;
(c) L è suriettiva? Trovare la dimensione e una base dell'immagine di L.

5.2.5. Sia $\varphi : \Bbbk[X]_{\leqslant 4} \to \Bbbk[X]_{\leqslant 4}$ la funzione definita da $\varphi(P) = P + XD(P)$ ove D è l'usuale derivazione tra polinomi;
(a) scrivere la matrice associata a φ nella base canonica $1, X, X^2, X^3, X^4$;
(b) scrivere la matrice associata a φ nella base $X^4, D(X^4), D^2(X^4), D^3(X^4), D^4(X^4)$;
(c) scrivere la matrice di cambiamento di base tra le due basi precedenti, e verificare la relazione di cambiamento di base per le due matrici associate a φ;
(d) esistono mappe inverse a destra o a sinistra per φ? in caso affermativo, scriverne le matrici nelle due basi date e verificare la relazione con le matrici di φ.

5.2.6. Sia A una matrice quadrata d'ordine n nilpotente, cioè esista un intero positivo m tale che $A^m = 0$. Mostrare che $\mathbb{I}_n + A$ è una matrice invertibile. Cosa significa la nilpotenza in termini di una applicazione lineare rappresentata da quella matrice?

5.2.7. Si diano degli esempi di matrici quadrate dello stesso ordine, non nulle, A e B tali che $AB = 0$. È vero che allora necessariamente si ha $BA = 0$ (giustificare o dare controesempi)? Interpretare gli esempi in termini di applicazioni lineari rappresentate da quelle matrici.

5.2.8. Dire se è possibile che il prodotto di tre matrici A, B, C, quadrate dello stesso ordine e non nulle, si annulli ($ABC = 0$) nei seguenti casi:
(a) A sia invertibile;
(b) B sia invertibile;
(c) C sia invertibile
(giustificare la risposta o dare dei controesempi).

5.2.9. Siano A e B due matrici quadrate dello stesso ordine. Dire che rapporti vi sono tra il fatto che A e B siano invertibili e il fatto che $A + B$ sia invertibile. Spiegare con degli esempi.

5.2.10. È vero che ogni matrice reale quadrata non (necessariamente) invertibile si può scrivere come somma di due matrici invertibili?
(a) Caratterizzare gli endomorfismi di $\mathbb{R}^n$ che vengono rappresentati sempre dalla stessa matrice in ogni base (i morfismi $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ tali che $\alpha_{\mathscr{V},\mathscr{V}}(\varphi) = \alpha_{\mathscr{W},\mathscr{W}}(\varphi)$ per ogni coppia di basi $\mathscr{V}$ e $\mathscr{W}$ di $\mathbb{R}^n$).
(b) Caratterizzare l'insieme di tutte le matrici quadrate d'ordine n che commutano con tutte le altre matrici (le matrici A tali che $AB = BA$ per ogni altra matrice B; quest'insieme si dice il centro dell'algebra delle matrici).
(c) Che relazione c'è tra i due punti precedenti?

5.2.11. Sia $A = \begin{pmatrix} 2 & 1 & 0 \\ -1 & 1 & 2 \end{pmatrix}$:
(a) determinare, se esistono, le matrici $B \in M_{3\times 2}(\mathbb{Q})$ tali che $AB = \mathbb{I}_2$;
(b) determinare, se esistono, le matrici $C \in M_{3\times 2}(\mathbb{Q})$ tali che $CA = \mathbb{I}_3$;
(c) discutere i punti precedenti in termini di applicazioni lineari, se già non si è fatto;
(d) descrivere l'insieme di cui al punto (a) in termini dello spazio vettoriale $M_{3\times 2}(\mathbb{Q})$.

5.2.12. Siano $A = \begin{pmatrix} 1 & 2 & -4 \\ 2 & 4 & -8 \\ 3 & 6 & -12 \end{pmatrix}$ e $C = \begin{pmatrix} 0 & 1 & 1 & -2 \\ 2 & 0 & -2 & 2 \\ 3 & 2 & -1 & -1 \end{pmatrix}$ e sia $U = \{B \in M_3(\mathbb{R}) : ABC = 0\}$;
(a) mostrare che U è un sottospazio di $M_3(\mathbb{R})$;
(b) calcolare la dimensione di U su $\mathbb{R}$;
(c) trovare una base di U.

5.2.13. Sia $A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 1 & 1 \end{pmatrix}$. Consideriamo l'applicazione $f : M_2(\mathbb{R}) \to M_{3,2}(\mathbb{R})$ data da $f(M) = AM$.
(a) Mostrare che f è lineare e calcolare dimensioni e basi di nucleo e immagine.
(b) Scrivere la matrice di f nelle basi canoniche di dominio e codominio.
(c) Dire se esistono inverse destre e/o sinistre per f, e nel caso determinarle tutte.

5.2.14. Consideriamo l'applicazione $\varphi : \mathbb{R}[X]_{\leqslant 4} \to \mathbb{R}[Y]_{\leqslant 5}$ che manda un polinomio $p(X)$ nel polinomio $\varphi(p(X)) = Yp(1 + Y)$.
(a) Mostrare che φ è lineare e calcolare dimensioni e basi di nucleo e immagine.
(b) Scrivere la matrice di φ nelle basi canoniche di dominio e codominio.
(c) Dire se esistono inverse destre e/o sinistre per φ, e nel caso determinarle tutte.

5.2.15. Siano $A \in M_2(\mathbb{Q})$ e $B \in M_3(\mathbb{Q})$; si consideri l'applicazione $\tau : M_{2\times 3}(\mathbb{Q}) \to M_{2\times 3}(\mathbb{Q})$ definita da $\tau(X) = AXB$.
(a) Si mostri che τ è lineare;
(b) si mostri che τ è invertibile se e solo se A e B sono invertibili;
(c) si scriva una base di τ nella base canonica con l'ordine lessicografico;
(d) stimare le dimensioni di nucleo e immagine di τ in funzione dei ranghi di A e B.

5.2.16. Si considerino gli spazi vettoriali V e W su $\mathbb{R}$ con le rispettive basi $\mathscr{V} = (v_1, v_2, v_3, v_4)$ e $\mathscr{W} = (w_1, w_2, w_3)$.
(a) Si dica se esiste un'applicazione lineare $\varphi : V \to W$ che soddisfa alle seguenti condizioni

$$\varphi(v_1 + v_2) = 2w_1 + w_2 + 3w_3, \qquad \varphi(v_2 + v_3) = 2w_1 + 2w_2 + 5w_3,$$
$$\varphi(v_1 + v_2 + v_3) = 4w_1 + 2w_2 + 6w_3, \qquad \varphi(v_2 + v_3 + v_4) = 4w_1 + w_2 + 4w_3;$$

e se ne scriva la matrice rispetto alle basi date.
(b) Si mostri che il sottoinsieme $A = \{\psi \in \mathrm{Hom}_{\mathbb{R}}(V, V) : \varphi \circ \psi = 0\}$ è un sottospazio dello spazio vettoriale $\mathrm{Hom}_{\mathbb{R}}(V, V)$ e se ne calcoli la dimensione. Sia $\alpha_{\mathscr{V},\mathscr{V}} : \mathrm{Hom}_{\mathbb{R}}(V, V) \to M_4(\mathbb{R})$ l'applicazione

che ad ogni endomorfismo di V associa la sua matrice, rispetto alla base $\mathscr{V}$. Si determini una base per il sottospazio immagine di A.

(c) Si mostri che il sottoinsieme $B = \{\vartheta \in \mathrm{Hom}_{\mathbb{R}}(W, W) : \vartheta \circ \varphi = 0\}$ è un sottospazio dello spazio vettoriale $\mathrm{Hom}_{\mathbb{R}}(W, W)$ e se ne calcoli la dimensione. Sia $\alpha_{\mathscr{W},\mathscr{W}} : \mathrm{Hom}_{\mathbb{R}}(W, W) \to M_3(\mathbb{R})$ l'applicazione che ad ogni endomorfismo di W associa la sua matrice, rispetto alla base $\mathscr{W}$. Si determini una base per il sottospazio immagine di B.

(d) Si consideri il sottinsieme $C = \{(\psi, \vartheta) \in \mathrm{Hom}_{\mathbb{R}}(V, V) \times \mathrm{Hom}_{\mathbb{R}}(W, W) : \vartheta \circ \varphi \circ \psi = 0\}$ del prodotto cartesiano $\mathrm{Hom}_{\mathbb{R}}(V, V) \times \mathrm{Hom}_{\mathbb{R}}(W, W)$, e si mostri che $A \times B$ è contenuto in C. È vero o falso che $A \times B = C$? È vero o falso che C sia un sottospazio di $\mathrm{Hom}_{\mathbb{R}}(V, V) \times \mathrm{Hom}_{\mathbb{R}}(W, W)$?

5.2.17. Si considerino gli spazi vettoriali V e W su $\mathbb{R}$ con le rispettive basi $\mathscr{V} = (v_1, v_2, v_3, v_4)$ e $\mathscr{W} = (w_1, w_2, w_3)$.

(a) Si dica se esistono applicazioni lineari $\varphi : V \to W$ che soddisfano alle seguenti condizioni

$$\begin{aligned} &\varphi(v_1 + v_2 + v_3) = 2w_1 + 4w_2 + 2w_3, && \varphi(v_1 + v_3) = 2w_1 + 3w_2 + w_3, \\ &\varphi(v_1 + v_2) = w_1 + 2w_2 + w_3, && \varphi(v_2 + v_3) = w_1 + 3w_2 + 2w_3; \end{aligned}$$

ed eventualmente si decrive questo insieme come sottoinsieme dello spazio vettoriale $\mathrm{Hom}_{\mathbb{R}}(V, W)$.

(a) Sia $\alpha_{\mathscr{V},\mathscr{W}} : \mathrm{Hom}_{\mathbb{R}}(V, W) \to M_{4\times 3}(\mathbb{R})$ l'applicazione che ad ogni morfismo di V in W associa la sua matrice, rispetto alle basi $\mathscr{V}$ e $\mathscr{W}$. Si descriva l'insieme precedente in termini dello spazio vettoriale $M_{4\times 3}(\mathbb{R})$.

5.2.18. Si considerino gli spazi vettoriali V e W su $\mathbb{R}$ con le rispettive basi $\mathscr{V} = (v_1, v_2, v_3, v_4)$ e $\mathscr{W} = (w_1, w_2, w_3)$.

(a) Si dica se esiste un'applicazione lineare $\varphi : V \to W$ che soddisfa alle seguenti condizioni

$$\begin{aligned} &\varphi(v_1 + v_2 + v_3 + v_4) = w_1 + w_2 + w_3, && \varphi(v_1 + v_2) = w_1 - 2w_2, \\ &\varphi(v_1 + v_2 + v_3) = 2w_1 + 2w_2 + 2w_3, && \varphi(v_1 - v_2) = w_1 - 2w_2; \end{aligned}$$

e se ne scriva la matrice rispetto alle basi date.

(b) Si dica se il sottoinsieme $A = \{\psi \in \mathrm{Hom}_{\mathbb{R}}(V, V) : \varphi \circ \psi = \varphi\}$ è un sottospazio dello spazio vettoriale $\mathrm{Hom}_{\mathbb{R}}(V, V)$, e in ogni caso se ne dia una descrizione esplicita.

(c) Sia $\alpha_{\mathscr{V},\mathscr{V}} : \mathrm{Hom}_{\mathbb{R}}(V, V) \to M_4(\mathbb{R})$ l'applicazione che ad ogni endomorfismo di V associa la sua matrice, rispetto alla base $\mathscr{V}$. Si descriva l'immagine di A in termini dello spazio vettoriale $M_4(\mathbb{R})$.

5.2.19. Siano A e B due matrici quadrate di ordine m ed n rispettivamente a coefficienti in $\Bbbk$; consideriamo i seguenti insiemi:

$$\mathscr{A} = \{X \in M_{m\times n}(\Bbbk) : AX = 0\}\,, \qquad \mathscr{B} = \{X \in M_{m\times n}(\Bbbk) : XB = 0\}\,, \qquad \mathscr{C} = \{X \in M_{m\times n}(\Bbbk) : AXB = 0\}\,.$$

(*a*) Verificare che sono tre sottospazi di $M_{m\times n}(\Bbbk)$ e stabilire le ovvie relazioni di inclusione;

(*b*) calcolare le dimensioni dei tre sottospazi in funzione dei ranghi di A e B;

(*c*) studiare $\mathscr{A} \cap \mathscr{B}$;

(*d*) è vero che $\mathscr{A} + \mathscr{B} = \mathscr{C}$?

5.2.20. Sia $V = M_{3\times 3}(\mathbb{R})$ con la solita struttura di spazio vettoriale su $\mathbb{R}$. Si consideri l'applicazione $\mathrm{tr} : V \to \mathbb{R}$ definita da $\mathrm{tr}(A) = a_{11} + a_{22} + a_{33}$, per ogni $A = (a_{ij}) \in V$.

(a) Si mostri che tr è un'applicazione $\mathbb{R}$-lineare, se ne scriva la matrice nelle basi canoniche, e si calcoli la dimensione del suo nucleo;

(b) Si mostri che per ogni $A, B \in V$ risulta $\mathrm{tr}(AB) = \mathrm{tr}(BA)$;

(c) Si indichi con $\mathscr{E} = (e_{ij} : i, j = 1, 2, 3)$ la base canonica di V; si calcoli la dimensione del sottospazio di V generato dalle matrici $e_{ij}e_{rs} - e_{rs}e_{ij}$ al variare di e_{ij} e e_{rs} in $\mathcal{E}$;

(d) Si calcoli la dimensione del sottospazio di V generato da tutte le matrici del tipo $AB - BA$ al variare di A, B in V.

5.3. Esercizi sulla Dualità.

5.3.1. Sia V uno spazio vettoriale di dimensione n sul corpo $\Bbbk$, e si indichi con V^* lo spazio vettoriale $\mathrm{Hom}_{\Bbbk}(V, \Bbbk)$.
(a) Si mostri che $f \in V^*$ è suriettivo se e solo se $f \neq 0$.
(b) Si mostri che se $f, g \in V^*$ hanno lo stesso nucleo, allora essi sono linearmente dipendenti; in quali casi è vera l'implicazione inversa?
(c) Siano $f, g \in V^*$ linearmente indipendenti; si calcoli $\dim_{\Bbbk}(\ker f \cap \ker g)$.

5.3.2. Sia V uno spazio vettoriale di dimensione n sul corpo $\Bbbk$. Sia $f : V \to V$ un endomorfismo di V. Mostrare che:
(0) f è isomorfismo se e solo se f^* lo è;
(1) f è una proiezione (ovvero $f^2 = f$) se e solo se f^* lo è;
(2) f è una simmetria (ovvero $f^2 = \mathrm{id}_V$) se e solo se f^* lo è;

5.3.3. Sia V uno spazio vettoriale di dimensione n sul corpo $\Bbbk$. Siano U e W sottospazi di V. Mostrare che
(1) $U \cap W = 0$ se e solo se $V^* = U^\perp + W^\perp$.
(2) $U + W = V$ se e solo se $U^\perp \cap W^\perp = 0$.
(3) $V = U \oplus W$ se e solo se $V^* = U^\perp \oplus W^\perp$.
Determinare poi le applicazioni duali di proiezioni e simmetrie associate a due sottospazi in somma diretta.

5.3.4. Date due basi di V (si indichi con H la matrice di cambiamento di base dalla prima alla seconda), determinare la relazione tra le basi duali di V^* (per esempio determinando la matrice di cambiamento di base dalla prima alla seconda, e viceversa).

5.3.5. Studiare lo spazio duale dello spazio dei polinomi troncati, e l'applicazione duale della derivazione.

Capitolo III

Sistemi Lineari

In questo capitolo presentiamo le definizioni ed i risultati fondamentali della teoria dei sistemi di equazioni lineari. Pur trattandosi d'un problema puramente "algebrico", è la sua interpretazione in termini geometrici che permette la migliore comprensione dei risultati importanti, ed è in termini della geometria degli spazi vettorali (ed affini) che le dimostrazioni risultano più chiare.

Il primo paragrafo presenta la teoria generale, che può essere riassunta nel teorema di Rouché-Capelli per i sistemi lineari generali, e nella regola di Cramer per sistemi lineari quadrati invertibili.

Il secondo paragrafo presenta il metodo di riduzione di Gauss per la risoluzione di un sistema lineare, ed ancora si enfatizzano i legami tra il calcolo algebrico (matriciale) e la geometria degli spazi vettoriali.

Nota terminologica: in questo capitolo si parlerà di "sottospazi affini" o di "sottovarietà lineari affini" di uno spazio vettoriale standard. Questi termini saranno definiti più in generale per gli spazi affini in un futuro capitolo. Per ora si deve intendere questo: un sottospazio affine (o equivalentemente una sottovarietà lineare affine) è una qualsiasi classe laterale di un sottospazio vettoriale, cioè un sottinsieme $\mathbb{L}$ di $\Bbbk^n$ del tipo $v + W = \{v + w | w \in W\}$ con $v \in \Bbbk^n$ e W un sottospazio vettoriale di $\Bbbk^n$. Si tratta dei "traslati" di sottospazi vettoriali; talvolta il vettore v, o meglio il suo "estremo", si dice "punto di passaggio" di $\mathbb{L}$ e il sottospazio W si dice "direzione" o "giacitura" di $\mathbb{L}$. In questo contesto l'insieme $\Bbbk^n$ viene indicato anche con il simbolo $\mathbb{A}(\Bbbk^n)$ oppure $\mathbb{A}^n(\Bbbk)$ (e si legge "spazio affine associato a $\Bbbk^n$", oppure "spazio affine di dimensione n su $\Bbbk$").

1. Sistemi Lineari.

Sia $\Bbbk$ un corpo fissato.

1.1. Definizione. *Un* sistema lineare di m equazioni ed n incognite *(e a coefficienti in $\Bbbk$) è una lista di m equazioni nelle incognite $X_1, \dots, X_n$,*

$$\begin{cases} a_{1,1}X_1 + a_{1,2}X_2 + \cdots + a_{1,n}X_n = b_1 \\ a_{2,1}X_1 + a_{2,2}X_2 + \cdots + a_{2,n}X_n = b_2 \\ \vdots \\ a_{m,1}X_1 + a_{m,2}X_2 + \cdots + a_{m,n}X_n = b_m \end{cases}$$

ove $a_{i,j}, b_i \in \Bbbk$ (per ogni $i = 1, \dots, m$ e $j = 1, \dots, n$) si dicono i coefficienti del sistema*; in particolare i b_i (per ogni $i = 1, \dots, m$) si dicono i* termini noti del sistema. *Il sistema si dice* omogeneo *se tutti i termini noti sono nulli, e si dice* quadrato *se m=n.*

1.1.1. Scrittura Matriciale. Un sistema come sopra si rappresenta in forma matriciale come

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

e in forma più compatta con

$$AX = b$$

ove $A = (a_{i,j}) \in M_{m,n}(\Bbbk)$ (matrici $m \times n$ a coefficienti in $\Bbbk$), $X = (X_i)$ e $b = (b_i) \in \Bbbk^m$ (vettore dello spazio vettoriale standard $\Bbbk^m$).

La matrice A si dice la matrice incompleta del sistema o matrice dei coefficienti, la matrice $(A\ b) \in M_{m,n+1}(\Bbbk)$, che si ottiene aggiungendo alla matrice incompleta la colonna dei termini noti,

si dice la matrice completa del sistema. Il sistema è quadrato se la matrice incompleta è quadrata. Omogeneo se b è il vettore nullo.

1.2. Definizione. *Dato un sistema lineare $AX = b$ come sopra, si dice* soluzione del sistema *ogni n-pla $(x_1, \dots, x_n)^{\mathrm{t}} \in \Bbbk^n$ per cui valgono tutte le uguaglianze. Risolvere il sistema significa trovare tutte le soluzioni, cioè descrivere esplicitamente l'insieme*

$$S_{A,b} = \{x \in \Bbbk^n \text{ tali che } Ax = b\}$$

delle soluzioni. Nel caso $S_{A,b}$ sia vuoto il sistema si dice impossibile *o* incompatibile. *In caso contrario il sistema si dice* compatibile.

1.2.1. Interpretazione Vettoriale. La matrice incompleta A del sistema lineare può essere interpretata come la matrice di una applicazione lineare

$$\varphi_A : \Bbbk^n \longrightarrow \Bbbk^m$$

espressa dalla matrice A rispetto alle basi canoniche di $\Bbbk^n$ e $\Bbbk^m$. L'insieme $S_{A,b}$ delle soluzioni si può quindi interpretare come l'immagine inversa tramite φ_A del vettore $b \in \Bbbk^m$:

$$S_{A,b} = \varphi_A^*(b) := \{x \in \Bbbk^n \text{ tali che } \varphi_A(x) = b\} \ .$$

Questa interpretazione ci permette di capire qual è la struttura dell'insieme delle soluzioni.

Nel caso più semplice in cui il sistema è omogeneo, dunque $b = 0$, si tratta di calcolare il nucleo dell'applicazione lineare φ_A. Dunque $S_{A,0} = \ker \varphi_A$, e si tratta di un sottospazio vettoriale di $\Bbbk^n$, di dimensione $\dim_{\Bbbk} \ker \varphi_A = n - \dim_{\Bbbk} \operatorname{im} \varphi_A = n - \operatorname{rg}(A)$. Risolvere il sistema equivale dunque a scrivere una base del nucleo di φ_A.

Nel caso in cui il sistema non sia omogeneo, si possono presentare due casi:

(i) il vettore $b \in \Bbbk^m$ non appartiene all'immagine $\operatorname{im}(\varphi_A)$ dell'applicazione lineare φ_A; in tal caso $S_{A,b} = \varnothing$, e il sistema è impossibile.

(ii) il vettore $b \in \Bbbk^m$ appartiene all'immagine $\operatorname{im}(\varphi_A)$ dell'applicazione lineare φ_A; in tal caso, scelta una soluzione particolare $x_0 \in \Bbbk^n$ del sistema (dunque $Ax_0 = b$), ogni altra soluzione si scrive sommando a x_0 una soluzione del sistema lineare omogeneo avente la stessa matrice dei coefficienti (infatti, se $y \in \Bbbk^n$ è un'altra soluzione, allora $y = x_0 + (y - x_0)$, e $y - x_0$ soddisfa a $A(y - x_0) = Ay - Ax_0 = b - b = 0$, dunque è soluzione del sistema lineare omogeneo associato; viceversa se $z \in \Bbbk^n$ soddisfa $Az = 0$, allora $x_0 + z$ soddisfa a $A(x_0 + z) = Ax_0 + Az = b + 0 = b$, dunque è soluzione del sistema originario). Dunque abbiamo mostrato che $S_{A,b} = x_0 + \ker \varphi_A = x_0 + S_{A,0}$, e si conclude che $S_{A,b}$ è una sottovarietà lineare affine dello spazio affine standard $\mathbb{A}(\Bbbk^n)$. Risolvere il sistema equivale quindi a descrive la sottovarietà affine $x_0 + \ker \varphi_A$, e dunque si riduce a trovare una soluzione particolare x_0 e il sottospazio delle soluzioni del sistema lineare omogeneo associato.

1.2.2. Osservazione sul problema inverso. La discussione precedente mostra che il problema di risolvere un sistema lineare si presenta come il problema di descrivere una sottovarietà affine di $\mathbb{A}(\Bbbk^n)$ a partire da un insieme di equazioni che la definiscono; in altri termini si tratta di trovare equazioni parametriche, ovvero una descrizioni in termini di punti e generatori del sottospazio direttore, per una sottovarietà lineare affine descritta da equazioni "cartesiane" (il sistema di partenza).

Sappiamo che anche il problema inverso è importante: trovare equazioni cartesiane di una sottovarietà affine lineare di $\mathbb{A}(\Bbbk^n)$ che sia descritta in termini di punti, oppure di un punto di passaggio e uno spazio direttore. Si tratta in questo caso di trovare un sistema lineare di equazioni il cui insieme di soluzioni sia la sottovarietà affine lineare data.

Ricordiamo brevemente come risolvere questo problema. Sia $\mathbb{L} = P + W$, con $P \in \mathbb{A}(\Bbbk^n)$ un punto dello spazio affine e $W = \langle w_1, \dots, w_r \rangle$ un sottospazio vettoriale di $\Bbbk^n$ di dimensione r, una varietà affine di dimensione r di $\mathbb{A}(\Bbbk^n)$. Essa si descrive tramite equazioni parametriche: un punto X di $P + W$ si scrive come $X = P + \sum_{i=1}^{r} \alpha_i w_i$ ove gli $\alpha_i \in \Bbbk$ sono i parametri e, se P ha coordinate $(p_1, \dots, p_n)$, si può esplicitare:

$$\begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix} = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} + \alpha_1 \begin{pmatrix} w_{1,1} \\ w_{2,1} \\ \vdots \\ w_{n,1} \end{pmatrix} + \cdots + \alpha_r \begin{pmatrix} w_{1,r} \\ w_{2,r} \\ \vdots \\ w_{n,r} \end{pmatrix} \qquad \text{ovvero} \qquad \begin{cases} X_1 = p_1 + \alpha_1 w_{1,1} + \cdots + \alpha_r w_{1,r} \\ X_2 = p_2 + \alpha_1 w_{2,1} + \cdots + \alpha_r w_{2,r} \\ \cdots \\ X_n = p_n + \alpha_1 w_{n,1} + \cdots + \alpha_r w_{n,r} \end{cases}$$

ove $w_j = (w_{i,j})$ sono le coordinate dei vettori w_j.

Un sistema di equazioni per $\mathbb{L}$ si può ottenere tramite il procedimento di "eliminazione dei parametri" a partire dalle equazioni precedenti (si procede ricavando un parametro da una equazione e sostituendolo nelle rimanenti: dopo aver eliminato tutti i paramentri resta un sistema lineare di $n-r$ equazioni).

Ma *conoscendo la nozione di determinante*, si può procedere in modo più sistematico per trovare subito un sistema di equazioni cartesiane: si impone la condizione

$$\operatorname{rg}\begin{pmatrix} X-P & w_1 & \cdots & w_r \end{pmatrix} \leqslant r$$

(matrice $n\times(r+1)$) che equivale ad annullare tutti i minori d'ordine $r+1$. Equivalentemente si può chiedere che

$$\operatorname{rg}\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ X & P & w_1 & \cdots & w_r \end{pmatrix} \leqslant r+1$$

(matrice $(n+1)\times(r+2)$) che di nuovo equivale ad annullare tutti i minori d'ordine $r+2$. Apparentemente si tratterebbe di $\binom{n+1}{r+2}$ equazioni, ma il rango del sistema sarà comunque $n-r$. Per trovare esattamente $n-r$ equazioni indipendenti si ricorre al *principio dei minori orlati*: dalle ultime $r+1$ colonne, possiamo estrarre una sottomatrice quadrata invertibile di ordine $r+1$; le equazioni richieste si ottengono annullando i determinanti di ordine $r+2$ della matrice completa contenenti la sottomatrice scelta (ovvero i minori che si ottengono "orlando" la sottomatrice invertibile scelta).

Un analogo ragionamento porta a descrivere la sottovarietà affine lineare passante per i punti $P_0, P_1, \ldots, P_r$ tramite la condizione

$$\operatorname{rg}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ X & P_0 & P_1 & \cdots & P_r \end{pmatrix} \leqslant r+1$$

(matrice $(n+1)\times(r+2)$) cui di nuovo si può applicare il principio dei minori orlati per ricavare esattamente $n-r$ equazioni, se i punti dati erano in posizione generale.

Anticipiamo infine che l'interpretazione cartesiana (che verrà trattata parlando di spazi euclidei in un futuro capitolo) dei coefficienti dell'equazione di un iperpiano (essi formano un vettore ortogonale allo spazio direttore dell'iperpiano) dà un metodo pratico per trovare equazioni cartesiane. Sia $\mathbb{L} = P + W$ come usuale, con $P \in \mathbb{A}(\Bbbk^n)$ un punto dello spazio affine e $W = \langle w_1, \ldots, w_r\rangle$ un sottospazio vettoriale di $\Bbbk^n$ di dimensione r. Allora possiamo scrivere un sistema di equazioni per $\mathbb{L}$ della forma $AX = AP$, ove $A \in M_{(n-r),n}$ è una matrice le cui righe sono generatori del sottospazio $W^\perp$ ortogonale di W.

1.2.3. Interpretazione geometrica. Insistiamo ancora sulla interpretazione geometrica di questi oggetti; abbiamo visto che le soluzioni di un sistema lineare $AX = b$ sono una sottovarietà affine lineare $\mathbb{L}$, e che risolvere il sistema significa descrivere la sottovarietà affine parametricamente come $\mathbb{L} = P+\langle w_1, \ldots, w_r\rangle$ ($P \in \mathbb{A}(\Bbbk^n)$ una soluzione particolare e $\langle w_1, \ldots, w_r\rangle$ sottospazio di $\Bbbk^n$ delle soluzioni del sistema omogeneo associato). Si tratta quindi di passare dalla descrizione di $\mathbb{L}$ come "insieme degli zeri" della funzione

$$f : \mathbb{A}(\Bbbk^n) \longrightarrow \mathbb{A}(\Bbbk^m) \qquad X = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \longmapsto AX-b$$

ad una descrizione di $\mathbb{L}$ come "immagine" della funzione

$$g : \mathbb{A}(\Bbbk^r) \longrightarrow \mathbb{A}(\Bbbk^n) \qquad Y = \begin{pmatrix} Y_1 \\ \vdots \\ Y_r \end{pmatrix} \longmapsto P+\sum_i Y_i w_i$$

(e viceversa per il problema inverso). Per rappresentare $\mathbb{L}$ si può sempre scegliere f suriettiva (sistema minimale di equazioni) e g iniettiva (sistema minimale di generatori).

Veniamo ora al risultato fondamentale:

1.3. Teorema di Rouché-Capelli. *Il sistema lineare $AX{=}b$ con $A \in M_{m,n}(\Bbbk)$ e $b \in \Bbbk^m$ ammette soluzioni se e solo se il rango della matrice completa è uguale al rango della matrice incompleta, ed in tal caso se x_0 è una soluzione, l'insieme $S_{A,b}$ di tutte le soluzioni si scrive come*

$x_0 + S_{A,0}$ dove $S_{A,0}$ è il sottospazio vettoriale di $\Bbbk^n$ delle soluzioni del sistema lineare omogeneo associato, i.e. $AX = 0$. Infine si ha che $\dim_{\Bbbk} S_{A,0}{=}n - \mathrm{rg}(A)$.

Dimostrazione. Come abbiamo fatto sopra, interpretiamo il problema usando l'applicazione

$$\varphi_A : \Bbbk^n \longrightarrow \Bbbk^m$$

di matrice A nelle basi canoniche. Affinché il sistema abbia soluzione è necessario e sufficiente che il vettore $b \in \Bbbk^m$ appartenga all'immagine di φ_A, ovvero per definizione che sia combinazione lineare delle colonne della matrice A, ovvero ancora che matrice completa e incompleta del sistema abbiano lo stesso rango (aggiungendo la colonna b il rango non deve aumentare). Nel caso vi siano soluzioni, abbiamo visto prima che esse si scrivano come $x_0 + S_{A,0}$ ove x_0 è una soluzione particolare e $S_{A,0} = \ker \varphi_A$. La formula delle dimensioni per l'applicazione lineare φ_A dà allora $n = \dim_{\Bbbk} \ker \varphi_A + \dim_{\Bbbk} \operatorname{im} \varphi_A = \dim_{\Bbbk} S_{A,0} + \mathrm{rg}(A)$, da cui l'ultima affermazione. □

In particolare, nel caso di sistemi quadrati in cui la matrice $n{\times}n$ dei coefficienti sia invertibile (cioè di rango n), abbiamo uno spazio delle soluzioni ridotto ad un punto: infatti qualunque sia il vettore dei termini noti il rango della matrice completa è comunque n (corrisponde al fatto che l'applicazione φ_A è suriettiva), e lo spazio delle soluzioni del sistema omogeneo associato è ridotto al vettore nullo (corrisponde al fatto che l'applicazione φ_A è iniettiva).

Il seguente risultato permette un calcolo esplicito dell'unico punto soluzione: vi si presuppone la conoscenza della nozione di determinante, e va quindi letto dopo che tale nozione sia stata introdotta.

1.4. Regola di Cramer. *Il sistema $AX{=}b$ con $A \in M_n(\Bbbk)$ (sistema quadrato) ha un'unica soluzione se e solo se $\det A \neq 0$, i.e. se la matrice A è invertibile, e in tal caso l'unica soluzione è $x{=}A^{-1}b$. Se A_i è la matrice che si ottiene da A sostituendo la i-esima colonna con la colonna b dei termini noti, si ha che $x_i{=}\det A_i \big/ \det A$.*

Dimostrazione. Dal teorema di Rouché-Capelli sappiamo che la soluzione esiste unica se e solo se A ha rango massimo, e questo equivale a che A sia invertibile, e anche a che $\det A \neq 0$. Chiaramente la soluzione cercata è data da $x{=}A^{-1}b$. Ricordiamo che la matrice inversa si calcola usando i complementi algebrici della matrice A, precisamente

$$A^{-1} = \frac{1}{\det A}\Big(c_{i,j}\Big)$$

ove $c_{i,j} = (-1)^{i+j} \det A_{j,i}$ è il determinante della matrice che si ottiene da A eliminando la j-esima riga e la i-esima colonna. Di conseguenza si ottiene

$$x_i = \frac{1}{\det A}\sum_{j=1}^{n} c_{i,j} b_j = \frac{1}{\det A}\sum_{j=1}^{n} (-1)^{i+j} b_j \det A_{j,i} = \frac{\det A_i}{\det A}$$

poiché la sommatoria scritta rappresenta lo sviluppo di Laplace del determinante di A_i rispetto alla i-esima colonna (costituita dai termini noti). □

2. Riduzione di Gauss.

Rimane ancora da discutere come risolvere effettivamente un sistema lineare, ovvero dare un procedimento effettivo che permetta di scrivere tutte le soluzioni. Per questo definiamo la nozione di sistemi equivalenti.

2.1. Definizione. *Due sistemi $AX{=}b$ e $A'X{=}b'$, con $A \in M_{m,n}(\Bbbk)$ ed $A' \in M_{m',n}(\Bbbk)$, $b \in \Bbbk^m$ e $b \in \Bbbk^{m'}$ (cioè aventi lo stesso numero di incognite!), si dicono equivalenti se hanno lo stesso insieme di soluzioni. Si tratta ovviamente di una relazione di equivalenza nell'insieme dei sistemi lineari in n incognite.*

Se due sistemi sono equivalenti, allora abbiamo $\mathrm{rg}(A) = \mathrm{rg}(A')$ (il viceversa è ovviamente falso).

Osserviamo subito che, se $H \in M_m(\Bbbk)$ è una matrice invertibile, allora $AX = b$ è equivalente a $(HA)X = Hb$.

La morale di questo paragrafo è la seguente: *tramite operazioni elementari sulle righe della matrice completa si può trasformare il sistema in un sistema equivalente in forma a scalini, da cui*

si leggono subito i ranghi delle matrici (per applicare il teorema di Rouché-Capelli), e si scrivono le eventuali soluzioni.

Vogliamo però insistere sul significato delle operazioni elementari sia in termini di matrici (moltiplicazione per certe matrici invertibili dette "matrici elementari"), sia in termini di applicazioni lineari (cambiamenti di base).

2.2. Definizione (Matrici a scalini (per riga)). *Una matrice $A = (a_{i,j}) \in M_{m,n}(\Bbbk)$ si dice* in forma a scalini (per righe) *se gode della seguente proprietà: per ogni riga, se a_{r,j_r} è il primo elemento non nullo della riga, allora $a_{i,j} = 0$ ogni volta che $i \geqslant r$ e $j \leqslant j_r$, a parte $i = r$ e $j = j_r$ (significa che tutti i termini "a sinistra e in basso" rispetto ad a_{r,j_r} sono nulli, o ancora che a_{r,j_r} è l'unico elemento non nullo della sottomatrice di A che si ottiene cancellando le righe soprastanti e le colonne a destra) . I primi termini non nulli di ciascuna riga si dicono allora i* pivot *o i* termini direttori *della matrice. La matrice si dice* in forma speciale a scalini (per righe) *se è in forma a scalini e tutti i pivot sono uguali ad* 1. *Infine si dice* in forma ridotta (per righe) *se è in forma speciale (per righe) e ogni pivot è l'unico elemento non nullo della sua colonna.*

2.2.1. Il tipico aspetto di una matrice in forma a scalini (per righe) è dunque il seguente:

$$A = \begin{pmatrix} 0 & \cdots & 0 & a_{1,j_1} & \cdots & * & * & \cdots & * & * & \cdots & * & * & \cdots & a_{1,n} \\ 0 & \cdots & 0 & 0 & \cdots & 0 & a_{2,j_2} & \cdots & * & * & \cdots & * & * & \cdots & a_{2,n} \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & a_{3,j_3} & \cdots & * & * & \cdots & a_{3,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & a_{r,j_r} & \cdots & a_{r,n} \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

ove le stelline indicano elementi non (necessariamente) nulli. La condizione della definizione si può esprimere nel modo seguente: sia a_{i,j_i} il primo elemento non nullo della i-esima riga (per $i = 1, \dots, m$) ed intendiamo $j_i = n+i+1$ se la riga è nulla; allora la matrice è in forma a scalini se e solo se $j_1 < j_2 < \cdots < j_m$.

(Che aspetto hanno le forme speciali e ridotte?)

Ad esempio, una matrice quadrata triangolare superiore con tutti i termini diagonali non nulli è in forma a scalini; più generalmente è in forma a scalini una matrice rettangolare con tutti gli elementi di posto (i, i) non nulli e i termini di posto (i, j) con $i < j$ nulli.

2.2.2. Rango di una matrice a scalini. Si vede immediatamente che il rango di una matrice in forma a scalini è uguale al numero di righe non nulle, ovvero uguale al numero dei pivot, che evidentemente corrispondono al numero di colonne linearmente indipendenti. Siccome la riduzione di Gauss non cambia il rango della matrice, potremo concludere che ogni matrice ha rango pari alla sua trasposta.

2.2.3. Soluzioni di un sistema a scalini. Se un sistema ha matrice incompleta in forma a scalini, allora il teorema di Rouché-Capelli si applica immediatamente per dire che il sistema è impossibile se e solo se la colonna dei termini noti contiene qualche nuovo pivot (corrisponde ad avere una equazione del tipo $0 = k$ con $k \neq 0$). Se il sistema ammette soluzioni si scrivono tutte e sole nel modo seguente: comunque si assegnino degli elementi $a_j \in \Bbbk$, per ogni $j \neq j_1, \dots j_r, 1 \leqslant j \leqslant n$, esiste un'unica soluzione del sistema, $(x_1, x_2, \dots, x_n) \in \Bbbk^n$, tale che $x_j = a_j$. Dunque quegli $a_j \in \Bbbk$ (in numero di $n-r$) sono i parametri che permettono di scrivere tutte le soluzioni del sistema lineare.

2.2.4. Verificare per bene le due affermazioni precedenti. Fatto questo, è chiaro che per risolvere esplicitamente un sistema, basta trasformarlo in uno equivalente la cui matrice completa sia in forma a scalini. Ciò si fa tramite le "operazioni elementari" sulle righe della matrice completa.

2.2.5. Soluzioni di un sistema in forma ridotta speciate (metodo dei -1). Se un sistema omogeneo è in forma ridotta speciale, possiamo procedere così: inserire le righe prive di pivot in posizione diagonale, inserendo come pivot un -1 (ottenendo una matrice quadrata triangolare superiore con ± 1 in diagonale); allora le colonne che contengono i pivot -1 aggiunti formano una base

delle soluzioni del sistema. Capire perché. Esmpio:

$$\begin{pmatrix} 0 & 1 & a & 0 & b & c & 0 & d \\ 0 & 0 & 0 & 1 & e & f & 0 & g \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & h \end{pmatrix} \quad \text{diventa} \quad \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & a & 0 & b & c & 0 & d \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & e & f & 0 & g \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & h \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

e le 5 colonne che hanno -1 in posizione diagonale generano le soluzioni.

2.3. Definizione (Operazioni elementari sulle righe). *Le seguenti operazioni si dicono "operazioni elementari sulle righe di una matrice" A:*

(*i*) *scambiare di posto tra di loro due righe;*

(*ii*) *sostituire una riga con la somma di se stessa e di un multiplo scalare di un'altra riga;*

(*iii*) *moltiplicare una riga per uno scalare non nullo.*

2.3.1. Interpretazioni in termini di sistemi lineari. È chiaro che se queste operazioni vengono effettuate sulla matrice completa di un sistema lineare, si ottiene la matrice di un sistema equivalente (le operazioni corrispondono, nell'ordine, a: scambiare di posto due equazioni, sommare ad una un multiplo di un'altra, moltiplicare una equazione per uno scalare non nullo).

2.3.2. Interpretazione in termini di prodotto di matrici. Indichiamo con $e_{i,j}$ la base canonica dello spazio delle matrici quadrate d'ordine m, cioè $e_{i,j} = (\delta_{r,i}\delta_{j,s})_{1\leqslant r,s\leqslant m}$ (*delta* di Kronecker). Le operazioni elementari sulle righe corrispondono a moltiplicare *a sinistra* la matrice A per opportune matrici invertibili $H \in M_m(\Bbbk)$, dette *matrici elementari*. Precisamente:

(*i*) scambiare tra di loro la i-esima e la j-esima riga corrisponde a moltiplicare per $S(i,j) := \mathbb{I} + e_{i,j} + e_{j,i} - e_{i,i} - e_{j,j}$;

(*ii*) sostituire la i-esima riga con la somma di se stessa e di $\alpha \in \Bbbk$ volte la j-esima riga corrisponde a moltiplicare per $H(i,j,\alpha) := \mathbb{I} + \alpha e_{i,j}$;

(*iii*) moltiplicare la riga i-esima per $\alpha \in \Bbbk$ corrisponde a moltiplicare per $H(i,\alpha) := \mathbb{I} + (\alpha - 1)e_{i,i}$.

Che le matrici elementari siano invertibili si può vedere direttamente, ma sarà chiaro per l'osseravzione successiva.

2.3.3. Interpretazione in termini di cambiamento di base. Identificando la matrice A con la matrice di una applicazione lineare, le operazioni elementari sulle righe si possono interpretare come cambiamenti di base *nel codominio*. Precisamente

(*i*) scambiare tra di loro la i-esima e la j-esima riga corrisponde a scambiare di posto i vettori e_i ed e_j della base canonica;

(*ii*) sostituire la i-esima riga con la somma di se stessa e di $\alpha \in \Bbbk$ volte la j-esima riga corrisponde a sostituire il vettore e_j della base canonica con il vettore $e_j - \alpha e_i$;

(*iii*) moltiplicare la riga i-esima per $\alpha \in \Bbbk$ corrisponde a sostituire il vettore e_i della base canonica con il vettore $\alpha^{-1}e_i$.

Che si tratti ancora di basi di $\Bbbk^m$ è evidente, e permette subito anche di calcolare le inverse delle matrici elementari, poiché basta identificare le operazioni (elementari) che ristabiliscono la base canonica. Abbiamo $S(i,j)^{-1} = S(i,j)$ (cioè $S(i,j)^2 = \mathbb{I}$), $H(i,j,\alpha)^{-1} = H(i,j,-\alpha)$ ed infine $H(i,\alpha)^{-1} = H(i,\alpha^{-1})$.

2.3.4. Riassunto. Conviene forse riassumere la discussione precedente in una tabella:

operazioni elementari sulle righe di una matrice:	*moltiplicazione a sinistra per:*	*cambiamenti di base nel codominio:*
scambio tra loro le righe i-esima e j-esima	la matrice elementare $S(i,j)$	scambio tra loro i vettori i-esimo e j-esimo
sommo alla riga i-esima la j-esima moltiplicata per α	la matrice elementare $H(i,j,\alpha)$	sottraggo al j-esimo vettore l'i-esimo moltiplicato per α

moltiplico la riga i-esima per $\alpha \neq 0$	la matrice elementare $H(i,\alpha)$	divido l'i-esimo vettore per α

Si osservi in particolare che se la matrice A dopo operazioni elementari $H_1, \dots, H_r$ (nell'ordine in cui sono eseguite) sulle sue righe viene trasformata nella matrice A', allora $A' = HA$ dove $H = H_r \dots H_1$.

2.4. Teorema (Riduzione di Gauss). *Tramite operazioni elementari sulle righe ogni matrice può essere ridotta in forma a scalini (per righe) usando operazioni dei tipi (i) e (ii); usando anche operazioni elementari del terzo tipo ogni matrice può essere ridotta in forma speciale a scalini (per righe).*

Dimostrazione (Metodo di riduzione di Gauss). Si procede per induzione sul numero di righe. A meno di un'operazione elementare del tipo (i) (scambiare la prima riga con un'altra) possiamo supporre che la prima colonna non nulla abbia il primo termine non nullo, sia a_{1,j_1}. Allora tramite operazioni elementari del secondo tipo (sommando ad ogni riga un opportuno multiplo della prima) possiamo far sì che tutti gli altri termini di quella colonna diventino nulli. Ora si procede per induzione, sulla sottomatrice che si ottiene cancellando la prima riga e la prime j_1 colonne.

Per ottenere la forma speciale per righe è ora sufficiente moltiplicare ogni riga non nulla per l'inverso del suo termine direttore. □

2.5. Calcolo dell'inversa d'una matrice quadrata invertibile. Ogni matrice quadrata invertibile A può essere ridotta (tramite il metodo di Gauss) alla matrice identica, e questa riduzione permette il calcolo dell'inversa: la matrice rettangolare $(A\ \mathbb{I})$ viene ridotta (per righe) a $(\mathbb{I}\ A^{-1})$. La riduzione fino alla forma speciale per righe di A porta ad avere a sinistra una matrice triangolare superiore con tutti i termini diagonali uguali ad 1; ora delle operazioni elementari sulle righe procedendo dal basso verso l'alto permettono di ricondursi alla matrice identica. Le operazioni elementari che vengono fatte sono via via accumulate nella parte destra della matrice rettangolare, che perciò alla fine del procedimento restituisce la matrice inversa di A.

Che cosa succederebbe in questo procedimento se la matrice A non fosse invertibile?

2.6. Calcolo delle inverse sinistre d'una matrice rettangolare invertibile a sinistra. Una matrice $A \in M_{m,n}(\Bbbk)$ è invertibile a sinistra se (e solo se) la corrispondente applicazione lineare $\varphi_A : \Bbbk^n \to \Bbbk^m$ è iniettiva, e in particolare $n \leqslant m$ e il rango di A è pari ad n. Facendo la riduzione di Gauss alla matrice $(A\ \mathbb{I}_m)$ e arrivando alla forma ridotta speciale, si ottiene una matrice a blocchi della forma:

$$\begin{pmatrix} \mathbb{I}_n & B' \\ \mathbb{O} & B'' \end{pmatrix}$$

e si ha che $B'A = \mathbb{I}_n$ mentre $B''A = \mathbb{O}$. In particolare B' è una inversa sinistra di A, e per trovare tutte le inverse sinistre di A basta sommare B' con le matrici la cui righe sono combinazioni lineari delle righe di B'' (giustamente si tratta di un traslato di un sottospazio di matrici di dimensione $n(m-n)$, come si può capire dal fatto che vi sono mn incognite e n^2 equazioni da soddisfare per trovare le inverse sinistre).

2.7. Calcolo delle inverse destre d'una matrice rettangolare invertibile a destra. Una matrice $A \in M_{m,n}(\Bbbk)$ è invertibile a destra se (e solo se) la corrispondente applicazione lineare $\varphi_A : \Bbbk^n \to \Bbbk^m$ è suriettiva, e in particolare $n \geqslant m$ e il rango di A è pari ad m. Per trovare le inverse destre, ovvero le matrici $B \in M_{n,m}(\Bbbk)$ tali che $AB = \mathbb{I}_m$, basta risolvere i sistemi lineari $AX = e_i$ visto che i vettori e_i (base canonica di $\Bbbk^m$) sono le colonne della matrice $\mathbb{I}_m$. Riducendo in forma a scala ridotta speciale la matrice $(A\ \mathbb{I}_m)$ si possono risolvere contemporaneamente tutti questi sistemi.

Oppure, con meno calcoli, si calcolano le trasposte delle inverse sinistre della trasposta della matrice di partenza: descrivere il procedimento diretto senza trasporre (cioè usando operazioni elementari sulle colonne).

2.8. Operazioni elementari sulle colonne. Chiudiamo questo paragrafo facendo notare che (quasi) tutto quello che si è detto si potrebbe riscrivere per le colonne di una matrice, piuttosto che per le righe. Cioè *possiamo definire la forma (eventualmente speciale) a scalini per colonne, e tramite*

opportune operazioni elementari sulle colonne possiamo ridurre ogni matrice in quella forma. Le operazioni elementari sulle colonne ammettono ugualmente interpretazioni in termini di moltiplicazione *a destra* per matrici elementari, ed in termini di cambiamenti di base *nel dominio*:

(*i*) scambiare di posto le colonne A_i e A_j corrisponde a moltiplicare per $S(i,j) := \mathbb{I} + e_{i,j} + e_{j,i} - e_{i,i} - e_{j,j}$;

(*ii*) sostituire la i-esima colonna con la somma di quella colonna e il prodotto di $\alpha \in \Bbbk$ per la j-esima colonna corrisponde a moltiplicare per $H(j,i,\alpha) := \mathbb{I} + \alpha e_{j,i}$;

(*iii*) moltiplicare la colonna i-esima per $\alpha \in \Bbbk$; corrisponde a moltiplicare per $H(i,\alpha) := \mathbb{I} + (\alpha - 1)e_{i,i}$.

Va osservato però che queste operazioni applicate alla matrice completa di un sistema lineare *non danno sistemi lineari equivalenti*, e dunque non possono essere usate per la risoluzione.

Conviene organizzare una tabella simile a quella vista per le operazioni elementari sulle righe.

2.9. Problema: decomposizioni di matrici. Operare con (alcune delle) operazioni elementari su una fissata matrice, permette di scrivere quella matrice come prodotto di matrici in qualche modo più semplici: da un lato una matrice ridotta in una forma di Gauss, dall'altro un prodotto di matrici elementari (usando le operazioni sulle righe si arriva ad una decomposizione $A = EU$ dove E è prodotto di matrici elementari (quindi invertibile) e U è matrice con termini nulli sotto la "diagonale principale" e dello stesso rango di A.

Provare ad esplorare le proprietà possibili per queste decomposizioni; per esempio: quando il prodotto di matrici elementari sarà triangolare? quando avrà tutti i termini diagonali uguali ad 1? quando non interverranno matrici di permutazioni?

In particolare se la riduzione di Gauss non richiede scambi di riga, allora le matrici elementari utilizzate sono solo matrici triangolari inferiori, e si ottiene una decomposizione $A = LU$ dove L è matrice triangolare inferiore prodotto di matrici elementari (quindi invertibile) e U è matrice con termini nulli sotto la "diagonale principale" e dello stesso rango di A. Si parla allora di decomposizione LU (lower-upper decomposition). Questa è possibile se tutte le sottomatrici quadrate di A ottenute dalle prime righe e prime colonne sono invertibili.

3. Esercizi.

3.0. Quante soluzioni ha un sistema lineare non omogeneo su un campo finito?

3.1. Risolvere il sistema lineare $Ax = b$ di matrice completa $\begin{pmatrix} 10 & 23 & 17 & 44 & 25 \\ 15 & 35 & 26 & 69 & 40 \\ 25 & 57 & 42 & 108 & 65 \\ 30 & 69 & 51 & 133 & 95 \end{pmatrix}$.

3.2. Al variare di $\ell \in \mathbb{R}$, risolvere i sistemi lineari $A_\ell x = b_\ell$ di matrice completa

$$\begin{pmatrix} 5 & -3 & 2 & 4 & 3 \\ 4 & -2 & 3 & 7 & 1 \\ 8 & -6 & -1 & -5 & 9 \\ 7 & -3 & 7 & 17 & \ell \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 2 & 5 & 1 & 3 & 2 \\ 4 & 6 & 3 & 5 & 4 \\ 4 & 14 & 1 & 7 & 4 \\ 2 & -3 & 3 & \ell & 7 \end{pmatrix}.$$

3.3. Al variare di $\ell \in \mathbb{R}$ risolvere l'equazione $XA_\ell = 0$, dove $A_\ell = \begin{pmatrix} \ell & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}$. In questo problema l'incognita è la matrice $X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$, quindi l'equazione $XA_\ell = 0$ diventa un sistema lineare omogeneo in $x_{11}, x_{12}, x_{21}, x_{22}$.

3.4. Sia $\Sigma : Ax = b$ un sistema lineare con $A \in M_{m\times n}(\Bbbk)$. Sia $H \in M_m(\Bbbk)$ e $\Pi : HAx = b$. Se Σ ha soluzioni, Π ha soluzioni? In generale che relazione c'è tra i due insiemi di soluzioni? La stessa domanda con H invertibile.

3.5. In $\mathbb{R}^4$ si considerino i sottospazi $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \rangle$, e $V = \langle \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \rangle$. Determinare tre sistemi lineari tali che U, V e $U \cap V$ ne siano rispettivamente gli insiemi delle soluzioni. Risolvere lo stesso problema trovando però sistemi minimali di equazioni per ciascuno dei sottospazi U, V e $U \cap V$.

3.6. Sia S l'insieme $\left\{ \begin{pmatrix} 2\lambda-1 \\ \mu+3 \\ 3\lambda+1 \\ -\lambda+\mu \end{pmatrix} \text{ tali che } \lambda, \mu \in \mathbb{R} \right\}$. Determinare un sistema lineare il cui insieme delle soluzioni coincide con S.

3.7. Sia $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$. Dimostrare che l'insieme delle matrici che commutano con A (cioè l'insieme delle matrici $B \in M_2(\mathbb{R})$ tali che $AB = BA$) è un sottospazio di $M_2(\mathbb{R})$ e calcolarne la dimensione. Per ogni intero n calcolare A^n. Determinare, per ogni $n \in \mathbb{Z}$, la dimensione dello spazio delle matrici di $M_2(\mathbb{R})$ che commutano con A^n.

3.8. Per ogni $t \in \mathbb{R}$ si consideri il sistema lineare $\Sigma_t : \begin{cases} -tx + (t-1)y + z = -1 \\ (t-1)y + tz = 1 \\ 2x + z = 5 \ . \end{cases}$ Sia S_t l'insieme delle soluzioni di Σ_t.

(a) Per quali valori di t S_t è costituito da un solo punto?
(b) Per quali valori di t S_t è vuoto?
(c) Per quali valori di t S_t è una sottovarietà lineare affine di dimensione 1?
(d) Per i valori di t di cui al punto (c), esibire equazioni parametriche di S_t.

3.9. Sia dato il sistema lineare reale Σ_k: $A_k x = b_k$ di matrice completa $C_k = \begin{pmatrix} 0 & 2k & k^2-1 & 0 \\ k & -1 & -k & -1 \\ 1 & -k & 1 & k \end{pmatrix}$ al variare di $k \in \mathbb{R}$. Determinare per quali valori di k Σ_k ammette un'unica soluzione e, in questi casi, determinare la soluzione di Σ_k. Risolvere lo stesso problema su $\mathbb{C}$.

3.10. Consideriamo il sistema lineare reale $\begin{cases} x + y = 1 \\ x + z = \lambda \\ (2-\lambda)x + y + z = 1 \end{cases}$ al variare di $\lambda \in \mathbb{R}$.

(a) Discutere i ranghi delle matrici completa e incompleta al variare di $\lambda \in \mathbb{R}$.
(b) Determinare per ogni $\lambda \in \mathbb{R}$ l'insieme delle soluzioni S_λ.
(c) Descrivere l'insieme S unione di tutti gli S_λ.
(d) È vero che S è una sottovarietà affine lineare? Eventualmente qual'è la minima sottovarietà affine lineare contenente S?

3.11. Come l'esercizio precedente, usando il sistema $\begin{cases} x + (1-\lambda)y + z = 1 + \lambda \\ (2-\lambda)x + (\lambda-1)^2 y + \lambda z = 3 - \lambda^2 \\ x + (\lambda-1)z = 2 + \lambda \end{cases}$

3.12. Sia $A = \begin{pmatrix} 1 & 3 & 5 & 3 \\ 1 & 4 & 7 & 3 \\ 0 & 1 & 2 & 0 \\ 1 & 2 & 3 & 2 \end{pmatrix}$. Si discuta il sistema $AX = b$ al variare di b in $\mathbb{R}^4$; in particolare si mostri che i b per i quali il sistema ammette soluzione, sono tutte e sole le soluzioni di un'equazione lineare omogenea.

3.13. Si consideri il seguente sistema lineare $\begin{cases} lx + my - mz = m \\ mx - ly = l \\ x - y - z = 0 \end{cases}$.
Si dica per quali coppie $(l, m) \in \mathbb{R}^2$ il sistema ammette soluzioni, e per quali la soluzione è unica.

3.14. Calcolare il rango della matrice $A = \begin{pmatrix} 1 & 1 & 3 & 1 & 0 \\ 3 & 2 & 3 & 1 & 1 \\ 2 & 1 & t & 0 & 1 \\ t & t & 2t+t^2 & t^2 & 0 \end{pmatrix}$ al variare di t in $\mathbb{R}$.

3.15. Si calcolino le inverse delle seguenti matrici:

$$A = \begin{pmatrix} 6 & -2 & -3 \\ -2 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 2 & 3 \\ 1 & -1 & 0 \\ -1 & 2 & 1 \end{pmatrix} \quad C = \begin{pmatrix} 1 & a & a^2 & a^3 \\ 0 & 1 & a & a^2 \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

3.16. Si indichino con A e B gli spazi delle soluzioni dei seguenti sistemi lineari omogenei:

$$\begin{cases} 2x_1 & -3x_2 & & -x_4 & = 0 \\ & 3x_2 & -2x_3 & +x_4 & = 0 \\ x_1 & & & +x_4 & = 0 \end{cases} \quad \text{e} \quad \begin{cases} x_1 & +2x_2 & -3\lambda x_3 & & = 0 \\ (\lambda+1)x_1 & +2x_2 & -3\lambda x_3 & +x_4 & = 0 \\ & 2\lambda x_2 & -3x_3 & +2\lambda x_4 & = 0 \end{cases}$$

Si determini la funzione d definita su $\mathbb{R}$ da $d(\lambda) = \dim(A \cap B)$.

3.17. Quadrati Magici. Un quadrato magico è una matrice quadrata, con termini interi positivi o nulli, tale che le somme dei termini su ogni riga, su ogni colonna e sulle due diagonali coincidano tutte. Determinare tutti i quadrati magici d'ordine 2 (sono solo quelli banali, con tutte le entrate uguali) e 3 (mostrare in particolare che il termine centrale della matrice è necessariamente un terzo della somma).

3.18. (il rango per righe coincide con il rango per colonne) Siano $\Bbbk$ un campo e $A \in M_{m\times n}(\Bbbk)$; allora indicheremo con $(A_{(1)}, \dots, A_{(n)})$ (risp. con $(A^{(1)}, \dots, A^{(m)})$) le colonne (risp. le righe) di A; quindi $A = (A_{(1)} \dots A_{(n)}) = \begin{pmatrix} A^{(1)} \\ \vdots \\ A^{(m)} \end{pmatrix}$.

Definiamo $\mathrm{rkc}(A) = \dim\langle A_{(1)}, \dots, A_{(n)}\rangle$ e $\mathrm{rkr}(A) = \dim\langle A^{(1)}, \dots, A^{(m)}\rangle$.

(a) Sia $Y \in M_{n\times n}(\Bbbk)$; si mostri che $\mathrm{rkc}(AY) \leqslant \mathrm{rkc}(A)$ e che $\mathrm{rkr}(AY) \leqslant \mathrm{rkr}(A)$;
(b) Sia $Y \in GL_n(\Bbbk)$; si mostri che $\mathrm{rkc}(AY) = \mathrm{rkc}(A)$ e che $\mathrm{rkr}(AY) = \mathrm{rkr}(A)$;
(c) Sia $X \in M_{n\times n}(\Bbbk)$; si mostri che $\mathrm{rkc}(XA) \leqslant \mathrm{rkc}(A)$ e che $\mathrm{rkr}(XA) \leqslant \mathrm{rkr}(A)$;
(d) Sia $X \in GL_n(\Bbbk)$; si mostri che $\mathrm{rkc}(XA) = \mathrm{rkc}(A)$ e che $\mathrm{rkr}(XA) = \mathrm{rkr}(A)$;
(e) Si mostri che $\mathrm{rkc}(A) = \mathrm{rkr}(A)$.

3.19. Con le notazioni dell'esercizio precedente, sia

$$A = \begin{pmatrix} 1 & -1 & 2 \\ 2 & 1 & 1 \\ 3 & 1 & 2 \end{pmatrix} \in M_{3\times 3}(\mathbb{R}).$$

(a) Calcolare il rango di A;
(b) Trovare una matrice $Y \in \mathrm{GL}_3(\mathbb{R})$, tale che $AY = (B_{(1)}B_{(2)}0)$;
(c) Trovare una matrice $X \in \mathrm{GL}_3(\mathbb{R})$, tale che $XA = \begin{pmatrix} C^{(1)} \\ C^{(2)} \\ 0 \end{pmatrix}$;
(d) Trovare X, Y come nei punti precedenti, e tali inoltre che $XAY = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

Capitolo IV

Determinanti

La nozione di determinante per endomorfismi e per matrici quadrate è forse lo strumento più basilare ed importante del corso. È nozione ubiquitaria per i suoi significati geometrici e per le sue applicazioni.

0. Motivazioni.

0.1. Risoluzioni di sistemi lineari quadrati. Nella risoluzione di un sistema lineare di due equazioni in due incognite

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 = b_2 \end{cases}$$

troviamo, tramite metodi elementari e senza preoccuparci dei passaggi, le "soluzioni"

$$\begin{cases} x_1 = \dfrac{b_1a_{2,2} - b_2a_{2,1}}{a_{1,1}a_{2,2} - a_{1,2}a_{2,1}} \\ x_2 = \dfrac{a_{1,1}b_2 - a_{1,2}b_1}{a_{1,1}a_{2,2} - a_{1,2}a_{2,1}} \end{cases}$$

e quindi siamo portati a chiamare il termine $a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$ il "determinante" del sistema: se esso non è nullo, la soluzione scritta è l'unica. Se invece è nullo, nei passaggi fatti si sono commesse delle imprecisioni, e il sistema può essere impossibile o indeterminato.

Analogamente, nel caso di sistemi di tre equazioni in tre incognite, ma con molti più calcoli, si possono scrivere le soluzioni come rapporti in cui al denominatore compare sempre lo stesso termine dipendente solo dai coefficienti delle equazioni e non dai termini noti.

Il concetto di determinante per una matrice quadrata permette di estendere queste osservazioni a tutti i sistemi di n equazioni in n incognite: esiste un termine (il determinante appunto) che dipende dai coefficienti delle equazioni e determina l'unicità o meno delle soluzioni a seconda che sia diverso da zero o no.

0.2. Indipendenza lineare di vettori. Dati n vettori in uno spazio vettoriale di dimensione n, sappiamo che essi formano una base se e solo se sono linearmente indipendenti. Decidere se sono linearmente indipendenti significa esattamente capire se la soluzione nulla è l'unica soluzione di un sistema lineare omogeneo di n equazioni in n incognite (i combinatori lineari). Dunque la discussione precedente ci dice che il concetto di determinante dà un test di indipendenza lineare.

0.3. Calcolo di equazioni cartesiane di sottospazi. La nozione di determinante permetterà anche un modo automatico e spesso utile per la ricerca di equazioni cartesiane di sottospazi, una volta che siano noti dei generatori, senza passare per le equazioni parametriche.

0.4. Studio delle forme canoniche delle matrici. Lo studio delle forme canoniche delle matrici, nel prossimo capitolo, utilizzerà in modo essenziale la nozione di determinante per il calcolo del cosiddetto polinomio caratteristico associato alla matrice.

0.5. Calcolo di volumi in geometria euclidea. Vedremo parlando di Geometria Euclidea che il calcolo del determinante è anche legato al calcolo del volume di certi oggetti geometrici (parallelepipedi e simplessi n-dimensionali). Vedere quali proprietà debba soddisfare la nozione di volume motiva bene la prima definizione che daremo; se vogliamo ottenere una funzione $A(v_1, v_2)$ di due vettori v_1 e v_2 che misuri l'area del parallelogramma descritto, la funzione dovrà rispettare alcune regole ovvie:

(1) se uno dei vettori è moltiplicato per uno scalare, l'area sarà moltiplicata per quello scalare: $A(\alpha v_1, v_2) = \alpha A(v_1, v_2) = A(v_1, \alpha v_2)$;

(2) se nella prima variabile si sommano due vettori, il risultato è la somma delle aree: $A(v_1+v_1', v_2) = A(v_1, v_2) + A(v_1', v_2)$ (idem per la seconda variabile); farsi un disegno per capire: si tratta di decomporre un parallelogramma in due aventi stesse "basi" e "altezze" dei due sommati;
(3) se i due vettori sono dipendenti il risultato è nullo;
(4) il quadrato unitario ha volume 1: $A(e_1, e_2) = 1$.

Di solito le prime due condizioni si riassumono dicendo che la funzione è bilineare (lineare in ogni variabile) e la terza dicendo che è alternante (perché se ne deduce che $A(v_1, v_2) = -A(v_1, v_2)$). Se si trova che esiste una unica tale funzione, essa dà la "giusta definizione" di area. Andiamo a formalizzare e studiare tali condizioni.

1. Determinanti e proprietà fondamentali.

In tutto il capitolo, il corpo $\Bbbk$ ha caratteristica diversa da 2.

1.1. Definizione (Funzioni multilineari alternanti). *Se V è uno spazio vettoriale sul corpo $\Bbbk$, una funzione m-lineare a valori in un altro spazio vettoriale W su $\Bbbk$ è una applicazione*

$$\delta : \underbrace{V \times \cdots \times V}_{m \text{ volte}} \longrightarrow W$$

che è lineare separatamente in ogni variabile, per qualsiasi fissati valori delle altre. Inoltre si dice alternante se si annulla ogni qual volta due argomenti sono uguali.

Se $W = \Bbbk$ si parla di forme m-lineari, eventualmente alternanti. Si osservi che gli insiemi delle funzioni m-lineari e m-lineari alternanti formano in modo naturale spazi vettoriali su $\Bbbk$.

1.1.1. La condizione di m-linearità della definizione si può esprimere dicendo che per ogni i e per ogni scelta di vettori $v_j \in V$ per $j \neq i$, la funzione $v \mapsto \delta(v_1, \dots, v, \dots, v_m)$ (v in posizione i-esima) è lineare. Si osservi che non basta che tutte le composizioni $\delta \circ \iota_j$ siano applicazioni lineari ove $\iota_j : V \to V \times \cdots \times V$ è la j-esima inclusione per ogni $j = 1, \dots, m$ (chi sono queste funzioni se δ è multilineare?). È sufficiente limitare la condizione sopra scritta per i vettori v_j di una fissata base di V (!)?

1.1.2. Proposizione (proprietà fondamentali). *Sia δ una applicazione m-lineare alternante. Allora:*
(1) *δ si annulla non appena si applichi ad un insieme di m vettori linearmente dipendenti;*
(2) *δ cambia di segno se si scambiano di posto due qualsiasi suoi argomenti.*

Dimostrazione. Possiamo supporre $v_m = \sum_{i=1}^{m-1} a_i v_i$; allora risulta

$$\begin{aligned}\delta(v_1, v_2, \dots, v_m) &= \delta(v_1, v_2, \dots, \sum_{i=1}^{m-1} a_i v_i) \\ &= \sum_{i=1}^{m-1} a_i \delta(v_1, v_2, \dots, v_i) = \sum_{i=1}^{m-1} a_i 0 = 0 \ .\end{aligned}$$

Per il secondo punto, possiamo supporre di scambiare di posto v_1 e v_2, e dal calcolo

$$0 = \delta(v_1+v_2, v_1+v_2, v_3, \dots, v_m) = \delta(v_1, v_2, v_3, \dots, v_m) + \delta(v_2, v_1, v_3, \dots, v_m)$$

abbiamo il risultato voluto (tenendo conto che il corpo ha caratteristica diversa da due). □

1.1.3. Problema. Indichiamo con $m\text{-Lin}_{\Bbbk}(V, W)$ e $m\text{-LinAlt}_{\Bbbk}(V, W)$ gli spazi vettoriali delle forme m-lineari (risp. e alternanti), e sottoindentiamo W se $W = \Bbbk$. Che dimensioni hanno questi spazi, in funzione delle dimensioni di V e di W?

1.2. Definizione-Teorema (determinante di applicazioni lineari). *Sia V uno spazio vettoriale di dimensione n. Allora:*
(1) *lo spazio delle forme n-lineari alternanti ha dimensione 1 su $\Bbbk$, e dunque ogni suo elemento non nullo ne costituisce una base; scelta una base ordinata $\mathscr{V}$ di V, l'applicazione $n\text{-LinAlt}_{\Bbbk}(V) \to \Bbbk$ che manda D in $D(\mathscr{V})$ è un isomorfismo di spazi vettoriali.*

(2) *una forma n-lineare alternante non identicamente nulla si annulla se e solo se l'insieme costituito dagli argomenti è un insieme linearmente dipendente.*

Detta D una qualunque forma n-lineare alternante non nulla, definiamo il determinante di un endomorfismo φ di V come il rapporto

$$\det \varphi = \frac{D(\varphi v_1, \dots, \varphi v_n)}{D(v_1, \dots, v_n)}$$

ove $v_1, \dots, v_n$ è una qualsiasi base di V; questa definizione non dipende né da D né dalla base scelta, ma solo dal morfismo φ (il che giustifica la notazione). In particolare si ha che $\det(\mathrm{id}_V) = 1$.

Dimostrazione. Osserviamo innanzitutto che una applicazione n-lineare alternante D è determinata dal valore che assume in una base qualsiasi: se infatti $v_1, \dots, v_n$ è una qualsiasi base di V, allora

$$\begin{aligned} D(\sum_{i_1=1}^{n} \alpha_{i_1,1} v_{i_1}, \dots, \sum_{i_n=1}^{n} \alpha_{i_n,n} v_{i_n}) &= \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} \alpha_{i_1,1} \cdots \alpha_{i_n,n} D(v_{i_1}, \dots, v_{i_n}) \\ &= \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) \alpha_{\sigma(1),1} \cdots \alpha_{\sigma(n),n} D(v_1, \dots, v_n) \end{aligned}$$

ove $\mathfrak{S}_n$ indica l'insieme delle permutazioni sull'insieme $\{1, \dots, n\}$ e $\mathrm{sgn}(\sigma)$ è il segno della permutazione σ (uguale a 1 se σ è composizione di un numero pari di scambi, -1 se σ è composizione di un numero dispari di scambi). Si osservi che nel primo passaggio abbiamo usato la multilinearità, nel secondo abbiamo usato la proprietà di alternanza.

Da questo deduciamo subito che se D e D' sono due applicazioni n-lineari alternanti non nulle, allora $D = kD'$ ove $k = D(v_1, \dots, v_n)/D'(v_1, \dots, v_n) \in \Bbbk$. Rimane da vedere che in effetti non tutte le applicazioni n-lineari alternanti sono nulle, ma questo è immediato osservando che definendo $D(v_1, \dots, v_n) = 1$ e usando la formula precedente per definire l'applicazione D, otteniamo una applicazione n-lineare alternante non nulla.

D'altra parte è chiaro che ogni forma di questo tipo si annulla su un insieme di n vettori linearmente dipendenti; viceversa, se si annulla su una base, allora per la formula precedente dev'essere l'applicazione nulla.

Dimostriamo ora che la definizione di determinante non dipende dalla base scelta: se $v'_1, \dots, v'_n$ è un'altra base di V, abbiamo $(v'_1, \dots, v'_n) = (v_1, \dots, v_n)H$ ove H è una matrice invertibile, di conseguenza abbiamo

$$\frac{D(\varphi v'_1, \dots, \varphi v'_n)}{D(v'_1, \dots, v'_n)} = \frac{D((\varphi v_1, \dots, \varphi v_n)H)}{D((v_1, \dots, v_n)H)} = \frac{hD(\varphi v_1, \dots, \varphi v_n)}{hD(v_1, \dots, v_n)}$$

ove $h = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) h_{\sigma(1),1} \cdots h_{\sigma(n),n}$ è una costante non nulla. In effetti questa verifica è inutile, se si ricorda che il rapporto che definisce det è il rapporto tra due funzioni n-lineari alternanti non nulle (D e una sua modificata tramite una trasformazione H invertibile). □

1.2.1. Segue subito dal risultato precedente che il determinante di una applicazione φ è non nullo se e solo se φ è un isomorfismo.

1.3. Definizione-Teorema (determinante di matrici). *Detta D una qualunque forma n-lineare alternante non nulla di $V_n(\Bbbk)$, definiamo il determinante di una matrice $A \in M_n(\Bbbk)$ come il determinante della applicazione lineare di $V_n(\Bbbk)$ in sè che è rappresentata dalla matrice A nella base canonica. Il determinante di A è dunque l'elemento di $\Bbbk$ dato da*

$$\det A = |A| := \sum\nolimits_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

ove $\mathfrak{S}_n$ indica l'insieme delle permutazioni sull'insieme $\{1, \dots, n\}$. In particolare si ha che $\det \mathbb{I}_n = 1$.

Da quanto detto possiamo allora dire che $\det : M_n(\Bbbk) \to \Bbbk$ *è l'unica funzione n-lineare alternante sulle colonne delle matrici e che vale 1 sulla matrice identica.*

Dimostrazione. È nascosta nella dimostrazione del precedente teorema. □

1.3.1. Segue subito dal risultato precedente che il determinante di una matrice A è non nullo se e solo se A è invertibile. In particolare n vettori formano una base di V (ovvero sono linearmente indipendenti) se e solo se il determinante della matrice che ha come colonne le loro coordinate (in una base qualsiasi) è non nullo.

1.3.2. Si osservi che il determinante di una matrice può essere visto come un polinomio omogeneo di grado (totale) n nelle entrate della matrice, ed esso è di primo grado rispetto a ciascuna entrata.

In quanto polinomio nelle n^2 variabili $a_{i,j}$, il determinante è irriducibile, cioè non può essere scritto come prodotto di due polinomi di grado strettamente minore.

1.4. Teorema (di Binet). *Le applicazioni* $\det : \mathrm{End}_{\Bbbk}(V) \to \Bbbk$ *e* $\det : M_n(\Bbbk) \to \Bbbk$ *rispettano identità e prodotto, cioè:*

(1) $\det(\mathrm{id}_V) = 1$ *e* $\det \mathbb{I}_n = 1$*;*

(2) $\det(\psi \circ \varphi) = \det(\psi)\det(\varphi)$ *per ogni* $\varphi, \psi \in \mathrm{End}_{\Bbbk}(V)$ *e* $\det(AB) = \det(A)\det(B)$ *per ogni* $A, B \in M_n(\Bbbk)$.

Dimostrazione. Il primo punto si è già visto, ed è ovvio dalla definizione. Per il secondo punto, se uno dei due determinanti è nullo, il risultato è chiaro. Altrimenti φ e ψ sono isomorfismi e possiamo calcolare, usando qualsiasi forma multilineare alternante D e qualsiasi base di V,

$$\begin{aligned}\det(\psi \circ \varphi) &= \frac{D(\psi \circ \varphi v_1, \dots, \psi \circ \varphi v_n)}{D(v_1, \dots, v_n)} \\ &= \frac{D(\psi \circ \varphi v_1, \dots, \psi \circ \varphi v_n)}{D(\varphi v_1, \dots, \varphi v_n)} \frac{D(\varphi v_1, \dots, \varphi v_n)}{D(v_1, \dots, v_n)} \\ &= \det(\psi)\det(\varphi)\end{aligned}$$

poiché il calcolo del determinante non dipende dalla base scelta dello spazio. □

1.4.1. Problema. Si osservi invece che la somma di matrici non è rispettata dal determinante, cioè in generale $\det(A + B) \neq \det(A) + \det(B)$ (farsi degli esempi).

Mostrare che $\det(-A) = (-1)^n \det(A)$ se $A \in M_n(\Bbbk)$.

Più in generale, abbiamo $\det(\alpha A) = \alpha^n \det(A)$ se $A \in M_n(\Bbbk)$ e $\alpha \in \Bbbk$.

1.5. Teorema (determinante della trasposta). *Se* $\varphi \in \mathrm{End}_{\Bbbk}(V)$ *allora abbiamo* $\varphi^* \in \mathrm{End}_{\Bbbk}(V^*)$ *e risulta* $\det(\varphi^*) = \det \varphi$*. Per ogni matrice* $A \in M_n(\Bbbk)$ *si ha* $\det(A^{\mathrm{t}}) = \det A$*.*

Dimostrazione. La prima asserzione segue dalla seconda, che è evidente:

$$\det A^{\mathrm{t}} = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i} = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) \prod_{j=1}^{n} a_{j,\sigma^{-1}(j)} = \sum_{\pi \in \mathfrak{S}_n} \mathrm{sgn}(\pi) \prod_{j=1}^{n} a_{j,\pi(j)} = \det A\ .$$

□

1.6. Esempi. Riepiloghiamo alcuni esempi facili di determinanti:

1.6.1. Matrici 2×2. Risulta $\det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = ad - bc$ (diagonale meno antidiagonale);

1.6.2. Matrici 3×3. Risulta $\det \left(\begin{smallmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{smallmatrix}\right) = a_1b_2c_3 + a_2b_3c_1 + a_3b_1c_2 - a_3b_2c_1 - a_2b_1c_3 - a_1b_3c_2$ (diagonali meno antidiagonali: regola di Sarrus);

1.6.3. Matrici 4×4. Esercizio: si tratta di una somma con 24 addendi, metà con "segno meno"; di conseguenza non possono essere solo le diagonali e le antidiagonali (che comunque compaiono: ma con che segni?) poiché si tratterebbe solo di 8 elementi...

1.6.4. Matrici diagonali. Il determinante è il prodotto degli elementi diagonali.

1.6.5. Matrici antidiagonali. Il determinante è il prodotto degli elementi nella antidiagonale, a meno di un segno: quale?

1.6.6. Matrici triangolari. Il determinante è il prodotto degli elementi diagonali.

1.7. Proposizione (gruppo generale lineare). *Il gruppo generale lineare* $\mathrm{GL}(n,\Bbbk)$ *si caratterizza come il sottinsieme di* $M_n(\Bbbk)$ *delle matrici di determinante non nullo. Il determinante si restringe ad un morfismo di gruppi*

$$\det : \mathrm{GL}_n(\Bbbk) \longrightarrow \Bbbk^\times$$

tra il gruppo delle matrici invertibili con l'operazione di prodotto e il gruppo degli elementi non nulli di $\Bbbk$ *con l'operazione di prodotto.*

Dimostrazione. Ovvio dalle definizioni e dai risultati precedenti. □

1.7.1. In particolare abbiamo $\det(A^{-1}) = \det(A)^{-1}$, e che $\det(H^{-1}AH) = \det(A)$.

1.7.2. L'applicazione $\det : \mathrm{GL}_n(\Bbbk) \longrightarrow \Bbbk^\times$ è suriettiva; è vero che esistono delle inverse a destra? Trovarne qualcuna la cui immagine sia contenuta nel sottogruppo delle matrici diagonali. È possibile trovare una inversa a destra la cui immagine sia contenuta nel sottogruppo delle matrici scalari?

1.7.3. Le matrici di determinante uguale ad 1 formano un sottogruppo normale di $\mathrm{GL}_n(\Bbbk)$ indicato con $\mathrm{SL}_n(\Bbbk)$ (gruppo Speciale Lineare). È vero che ogni matrice invertibile si può scrivere come prodotto di una matrice scalare (risp. diagonale) e di una matrice di determinante 1? Chi è il gruppo quoziente $\mathrm{GL}_n(\Bbbk)/\mathrm{SL}_n(\Bbbk)$?

2. Sviluppi di Laplace e matrici inverse.

2.1. Teorema (sviluppi di Laplace). *Il determinante di una matrice* $A \in M_n(\Bbbk)$ *si calcola mediante gli sviluppi di Laplace per riga o colonna, riconducendosi a determinanti di matrici in* $M_{n-1}(\Bbbk)$*:*

$$\begin{aligned} |A| &= \sum\nolimits_{j=1}^{n} (-1)^{i+j} a_{i,j} |A_{i,j}| \qquad \textit{(sviluppo secondo la } i\textit{-esima riga)} \\ &= \sum\nolimits_{i=1}^{n} (-1)^{i+j} a_{i,j} |A_{i,j}| \qquad \textit{(sviluppo secondo la } j\textit{-esima colonna)} \end{aligned}$$

ove $A_{i,j} \in M_{n-1}$ *è la matrice che si ottiene da* A *eliminando la* i*-esima riga e la* j*-esima colonna. I termini* $(-1)^{i+j}|A_{i,j}|$ *si chiamano i complementi algebrici di posto* (j,i) *della matrice* A*.*

Dimostrazione. Si tratta di vedere che le funzioni definite dalle formule di Laplace valgono 1 sulla matrice identica, e sono n-lineari alternanti sulle colonne della matrice. Il gioco dei segni $(-1)^{i+j}$ (scacchiera) serve solo per dimostrare l'alternanza. Una volta dimostrata l'alternanza, basta mostrare la formula di sviluppo per la prima colonna (per le altre colonne si deduce per alternanza, per le righe si deduce per trasposizione). Questa strategia è "elementare" ma piuttosto lunga.

In alternativa si può dimostrare la formula di sviluppo a partire dal calcolo del determinante con le permutazioni, partizionando le permutazioni a seconda della immagine di 1: se $\sigma(1) = i$, diciamo σ_i la permutazione σ ristretta a $\{2,\dots,n\}$ (leggero abuso di linguaggio, avendo valori in $\{1,\dots,\hat{i}\dots,n\}$):

$$\sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j} = \sum_{i=1}^{n} \sum_{\substack{\sigma\in\mathfrak{S}_n \\ \sigma(1)=i}} \mathrm{sgn}(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j} = \sum_{i=1}^{n} (-1)^{i-1} a_{i,1} \Big[\sum_{\sigma_i} \mathrm{sgn}(\sigma_i) \prod_{j=2}^{n} a_{\sigma_i(j),j} \Big]$$

e tra le parentesi quadre si riconosce $\det(A_{i,1})$. L'osservazione fondamentale è $\mathrm{sgn}(\sigma) = (-1)^{i-1}\mathrm{sgn}(\sigma_i) = (-1)^{i+1}\mathrm{sgn}(\sigma_i)$. □

2.1.1. Annullamenti o sviluppi (con cofattori) alieni. Dal risultato precedente segue subito che

$$\sum\nolimits_{j=1}^{n} (-1)^{i+j} a_{k,j} |A_{i,j}| = 0 \qquad (\text{risp.} \quad \sum\nolimits_{i=1}^{n} (-1)^{i+j} a_{i,k} |A_{i,j}| = 0 \quad)$$

per ogni $k \neq i$ (risp. $k \neq j$), poiché si tratta di sviluppi di Laplace di matrici con due righe (risp. colonne) uguali.

2.1.2. Definizione-Teorema (matrice dei complementi algebrici). *Data una matrice quadrata* A*, si dice complemento algebrico o minore segnato di posto* i,j *e si indica con* $a^{\mathrm{c}}_{i,j}$

il determinante $(-1)^{i+j}|A_{j,i}|$. *La matrice dei complementi algebrici* A^{c} *è la matrice* $(a^{\mathrm{c}}_{i,j})$. *Vale la relazione*

$$AA^{\mathrm{c}} = A^{\mathrm{c}}A = |A|\mathbb{I}_n \ .$$

Inoltre abbiamo $\mathbb{I}_n^{\mathrm{c}} = \mathbb{I}_n$ *e* $(AB)^{\mathrm{c}} = B^{\mathrm{c}}A^{\mathrm{c}}$.

Dimostrazione. Segue subito dagli sviluppi di Laplace (e alieni). L'ultima asserzione segue essenzialmente dal confronto tra $(AB)(AB)^{\mathrm{c}} = |AB|\mathbb{I}_n$ e $ABB^{\mathrm{c}}A^{\mathrm{c}} = |B|AA^{\mathrm{c}} = |A||B|\mathbb{I}_n$. □

2.2. Teorema (inversa). *Una matrice è invertibile se e solo se il suo determinante è diverso da zero. Se* $A \in M_n(\Bbbk)$ *è invertibile la sua matrice inversa si indica con* A^{-1} *e si calcola tramite:*

$$A^{-1} = \frac{1}{|A|}A^{\mathrm{c}} = \frac{1}{|A|}\left((-1)^{i+j}|A_{j,i}|\right)_{\substack{i=1,\dots,n\\ j=1,\dots,n}} \ .$$

Dimostrazione. Facile conseguenza del risultato precedente. □

2.3. Teorema (Cauchy). *Il determinante della matrice dei complementi algebrici di* A *è dato dalla potenza* $n-1$*-esima del determinante di* A*, cioè* $|A^{\mathrm{c}}| = |A|^{n-1}$.

Dimostrazione. Se $|A| = 0$ il risultato è ovvio, poiché anche $|A^{\mathrm{c}}| = 0$, altrimenti basta calcolare il determinante della uguaglianza $AA^{\mathrm{c}} = |A|\mathbb{I}_n$, da cui $|A||A^{\mathrm{c}}| = |A|^n$. □

2.3.1. Osservazione (rango della matrice dei complementi algebrici). Si noti per inciso che il rango di A^{c} è n, 1, 0 a seconda che il rango di A sia n, $n-1$, minore di $n-1$: perché? Il primo e l'ultimo caso sono ovvii, invece va giustificata bene la seguente asserzione: se una matrice ha rango $n-1$ allora la matrice dei suoi complementi algebrici è non nulla e di rango esattamente 1.

Si trovi almeno una giustificazione geometrica dell'asserzione precedente (pensare all'immagine degli iperpiani).

2.3.2. Osservazione. Vale che $A^{\mathrm{cc}} = |A|^{n-2}A$. Si ottiene per esempio confrontando $AA^{\mathrm{c}} = |A|\mathbb{I}_n$ con $A^{\mathrm{c}}A^{\mathrm{cc}} = |A^{\mathrm{c}}|\mathbb{I}_n$, se A è invertibile (altrimenti?).

♠♠ **2.4.** Sviluppi di Laplace generalizzati. Il calcolo del determinante tramite sviluppo di Laplace può essere generalizzato nel modo seguente: fissate r righe (risp. r colonne), invece di una sola, si può calcolare il determinante come somma di prodotti dei determinanti delle sottomatrici quadrate di quelle righe (risp. colonne) per il determinante della sottomatrice "complementare" (che si ottiene sopprimendo quelle righe e quelle colonne). La parte sofisticata della formula è nel tener conto dei segni con cui tali prodotti devono essere conteggiati.

2.4.1. Teorema (sviluppi di Laplace generalizzati). *Sia* K *sottinsieme (ordinato) di* $\{1, 2, \dots, n\}$ *e indichiamo con* $K' = \{1, 2, \dots, n\} \smallsetminus K$ *il complementare (ordinato). Sia* $\varepsilon(K, K')$ *il segno della permutazione che manda* i *nell'*i*-esimo elemento della lista* (K, K'). *Allora*

$$\det A = \varepsilon(K, K') \sum_H \varepsilon(H, H') \det A_{H,K} \det A_{H',K'}$$

dove la sommatoria è estesa a tutti i sottinsiemi H *di* $\{1, 2, \dots, n\}$ *aventi la stessa cardinalità di* K, H' *è l'insieme complementare,* $A_{H,K}$ *indica la sottomatrice quadrata che si ottiene selezionando le righe (risp. le colonne) i cui indici sono in* H *(risp. in* K*), e* $A_{H',K'}$ *indica la sottomatrice quadrata che si ottiene eliminando le righe (risp. le colonne) i cui indici sono in* H *(risp. in* K*).*

Dimostrazione. Si tratta di vedere che le funzioni definite dalle formule di Laplace valgono 1 sulla matrice identica, e sono n-lineari alternanti sulle colonne della matrice. □

Esempi. **2.4.2.** Se $K = \{i\}$ è di cardinalità uno, oppure $K = \{1, 2, \dots, n\} \smallsetminus \{i\}$ è di cardinalità $n-1$, si tratta dello sviluppo di Laplace secondo la i-esima colonna.

2.4.3. Una generalizzazione analoga può essere fatta per lo sviluppo di Laplace per righe (invece che per colonne), e si può dedurre dal teorema scritto passando alla matrice trasposta.

2.4.4. Se $K = \{1, 2\}$ e $n = 4$?

2.4.5. Se $K = \{1, 2\}$ e $n = 5$?

2.4.6. Annullamenti o sviluppi (con cofattori) alieni. Si osservi anche che, analogamente al caso di "sviluppi di Laplace su una riga (o una colonna) sbagliata" si ha che

$$\sum_H \varepsilon(H, H') \det A_{H,K} \det A_{H',L} = 0$$

per ogni $L \subseteq \{1, 2, \dots, n\}$ della stessa cardinalità di K' ma diverso da K'.

3. Sviluppi pivotali.

Poiché il determinante di una matrice è funzione multilineare in ogni riga o colonna, è possibile sfruttare il metodo di riduzione di Gauss per semplificare la forma della matrice di cui calcolare il determinante, per esempio portando la matrice alla forma triangolare. Questo tipo di procedimento dà luogo a formule interessanti, dette sviluppi pivotali.

3.1. Determinante delle operazioni elementari. Le matrici elementari che si usano nella riduzione hanno determinanti facilmente calcolabili: abbiamo $\det S(i,j) = -1$, $\det H(i,j,\alpha) = 1$ e $\det H(i,\alpha) = \alpha$.

In particolare, sommare ad una riga un qualsiasi multiplo di un'altra riga non altera il determinante, mentre lo scambio di due righe cambia di segno il determinante.

♠ **3.2.** Le operazioni elementari sulle righe possono essere usate per esprimere un determinante $n \times n$ in termini di un determinante $(n-2) \times (n-2)$ e di un determinante 2×2 le cui entrate sono determinanti $(n-1) \times (n-1)$. Prima di dare un enunciato generale, proponiamo i casi di determinanti di ordine 3, 4 e 5 quali esempi.

3.2.1. Determinanti d'ordine 3. Dopo aver moltiplicato la seconda e la terza riga per l'elemento a_1 di posto $1,1$, supposto diverso da zero, procediamo con la riduzione per righe:

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_1a_2 & a_1b_2 & a_1c_2 \\ a_1a_3 & a_1b_3 & a_1c_3 \end{pmatrix} \xRightarrow[III-a_3I]{II-a_2I} \begin{pmatrix} a_1 & b_1 & c_1 \\ 0 & a_1b_2 - a_2b_1 & a_1c_2 - a_2c_1 \\ 0 & a_1b_3 - a_3b_1 & a_1c_3 - a_3c_1 \end{pmatrix}$$

da cui si ricava subito che

$$a_1 \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{Vmatrix} \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} & \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix} \\ \begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} & \begin{vmatrix} a_1 & c_1 \\ a_3 & c_3 \end{vmatrix} \end{Vmatrix}$$

(sviluppo rispetto al pivot a_1).

3.2.2. Determinanti d'ordine 4. Dopo aver moltiplicato la seconda, la terza e la quarta riga per l'elemento a_1 di posto $1,1$, supposto diverso da zero, procediamo con la riduzione per righe:

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_1a_2 & a_1b_2 & a_1c_2 & a_1d_2 \\ a_1a_3 & a_1b_3 & a_1c_3 & a_1d_3 \\ a_1a_4 & a_1b_4 & a_1c_4 & a_1d_4 \end{pmatrix} \xRightarrow[\substack{III-a_3I \\ IV-a_4I}]{II-a_2I} \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ 0 & a_1b_2 - a_2b_1 & a_1c_2 - a_2c_1 & a_1d_2 - a_2d_1 \\ 0 & a_1b_3 - a_3b_1 & a_1c_3 - a_3c_1 & a_1d_3 - a_3d_1 \\ 0 & a_1b_4 - a_4b_1 & a_1c_4 - a_4c_1 & a_1d_4 - a_4d_1 \end{pmatrix}$$

da cui si ricava subito che

$$a_1^2 \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{vmatrix} = \begin{Vmatrix} \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} & \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix} & \begin{vmatrix} a_1 & d_1 \\ a_2 & d_2 \end{vmatrix} \\ \begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} & \begin{vmatrix} a_1 & c_1 \\ a_3 & c_3 \end{vmatrix} & \begin{vmatrix} a_1 & d_1 \\ a_3 & d_3 \end{vmatrix} \\ \begin{vmatrix} a_1 & b_1 \\ a_4 & b_4 \end{vmatrix} & \begin{vmatrix} a_1 & c_1 \\ a_4 & c_4 \end{vmatrix} & \begin{vmatrix} a_1 & d_1 \\ a_4 & d_4 \end{vmatrix} \end{Vmatrix}$$

(sviluppo rispetto al pivot a_1); usando poi lo sviluppo pivotale del determinante a destra rispetto al primo termine, ed interpretando il risultato in termini di uno sviluppo pivotale rispetto ad a_1 risulta che

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{vmatrix} = \begin{Vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} & \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix} \\ \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_4 & b_4 & c_4 \end{vmatrix} & \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_4 & b_4 & d_4 \end{vmatrix} \end{Vmatrix}$$

sotto ipotesi che il primo determinante scritto sia non nullo.

3.2.3. Determinanti d'ordine 5. Un analogo procedimento (riduzione di Gauss per quattro righe, poi uso degli sviluppi pivotali nei casi d'ordine 4 e 3), porta alla formula

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 & d_1 & e_1 \\ a_2 & b_2 & c_2 & d_2 & e_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 \\ a_4 & b_4 & c_4 & d_4 & e_4 \\ a_5 & b_5 & c_5 & d_5 & e_5 \end{vmatrix} = \begin{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{vmatrix} & \begin{vmatrix} a_1 & b_1 & c_1 & e_1 \\ a_2 & b_2 & c_2 & e_2 \\ a_3 & b_3 & c_3 & e_3 \\ a_4 & b_4 & c_4 & e_4 \end{vmatrix} \\ \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_5 & b_5 & c_5 & d_5 \end{vmatrix} & \begin{vmatrix} a_1 & b_1 & c_1 & e_1 \\ a_2 & b_2 & c_2 & e_2 \\ a_3 & b_3 & c_3 & e_3 \\ a_5 & b_5 & c_5 & e_5 \end{vmatrix} \end{vmatrix}$$

sotto ipotesi che il primo determinante scritto sia non nullo.

♠♠ **3.3.** Teorema (sviluppi pivotali). *Data una matrice quadrata A d'ordine $n \geqslant 3$, e indici $1 \leqslant i_1 < \cdots < i_r \leqslant n$ e $1 \leqslant j_1 < \cdots < j_r \leqslant n$, indichiamo con $A^{(i_1,\dots,i_r)}_{(j_1,\dots,j_r)}$ la sottomatrice quadrata d'ordine r che si ottiene scegliendo gli elementi di A il cui indice di riga appartiene a $\{i_1,\dots,i_r\}$ e il cui indice di colonna appartiene a $\{j_1,\dots,j_r\}$; indichiamo con $A^{(\hat{i_1},\dots,\hat{i_r})}_{(\hat{j_1},\dots,\hat{j_r})}$ la sottomatrice quadrata d'ordine $n-r$ che si ottiene sopprimendo le righe il cui indice appartiene a $\{i_1,\dots,i_r\}$ e le colonne il cui indice appartiene a $\{j_1,\dots,j_r\}$. Allora risulta che*

$$\left|A^{(\hat{i_1},\hat{i_2})}_{(\hat{j_1},\hat{j_2})}\right| |A| = \begin{vmatrix} \left|A^{(\hat{i_1})}_{(\hat{j_1})}\right| & \left|A^{(\hat{i_1})}_{(\hat{j_2})}\right| \\ \left|A^{(\hat{i_2})}_{(\hat{j_1})}\right| & \left|A^{(\hat{i_2})}_{(\hat{j_2})}\right| \end{vmatrix}$$

sotto ipotesi che il primo determinante sia non nullo.

Dimostrazione. Induzione sull'ordine del determinante. Si può supporre, scambiando righe e colonne, che $i_1 = j_1 = n-1$ e $i_2 = j_2 = n$. Si usa il procedimento di Gauss per eliminare i termini della prima colonna, ottenendo una espressione del tipo

$$\frac{1}{a_1^{n-1}} |A| = \begin{vmatrix} \left|A^{(1,2)}_{(1,2)}\right| & \left|A^{(1,2)}_{(1,3)}\right| & \cdots & \left|A^{(1,2)}_{(1,n)}\right| \\ \left|A^{(1,3)}_{(1,2)}\right| & \left|A^{(1,3)}_{(1,3)}\right| & \cdots & \left|A^{(1,3)}_{(1,n)}\right| \\ \vdots & \vdots & \ddots & \vdots \\ \left|A^{(1,n)}_{(1,2)}\right| & \left|A^{(1,n)}_{(1,3)}\right| & \cdots & \left|A^{(1,n)}_{(1,n)}\right| \end{vmatrix}$$

Detta B la matrice d'ordine $n-1$ il cui determinante sta sul lato destro, abbiamo (usando lo sviluppo pivotale dell'ordine precedente) che

$$\left|B^{(\widehat{n-2},\widehat{n-1})}_{(\widehat{n-2},\widehat{n-1})}\right| |B| = \begin{vmatrix} \left|B^{(\widehat{n-2})}_{(\widehat{n-2})}\right| & \left|B^{(\widehat{n-2})}_{(\widehat{n-1})}\right| \\ \left|B^{(\widehat{n-1})}_{(\widehat{n-2})}\right| & \left|B^{(\widehat{n-1})}_{(\widehat{n-1})}\right| \end{vmatrix}$$

e d'altra parte, usando le formule intermedie date dagli sviluppi pivotali rispetto al primo termine degli ordini precedenti, abbiamo che

$$\frac{1}{a_1^{n-3}} \left|A^{(\widehat{n-1},\widehat{n})}_{(\widehat{n-1},\widehat{n})}\right| = \left|B^{(\widehat{n-2},\widehat{n-1})}_{(\widehat{n-2},\widehat{n-1})}\right|$$

e

$$\frac{1}{a_1^{n-2}} \left|A^{(\widehat{i})}_{(\widehat{j})}\right| = \left|B^{(\widehat{i-1})}_{(\widehat{j-1})}\right| \qquad \text{(da usare per } i,j = n-1, n).$$

Sostituendo nella prima espressione trovata otteniamo il risultato voluto. □

4. Determinanti notevoli.

4.1. Matrici di permutazioni. Se σ è una permutazione di $1, \dots, n$, sia M_σ la matrice di permutazione (la cui i-esima colonna è $e_{\sigma i}$). Allora $\det M_\sigma = \operatorname{sgn}\sigma$.

4.2. Matrici triangolari. Se la matrice A è triangolare (inferiore se $a_{i,j}$=0 per $i > j$; superiore se $a_{i,j}$=0 per $i < j$) allora il determinante è il prodotto degli elementi in diagonale: $\det A = \prod_{i=1}^n a_{i,i}$. È una conseguenza immediata del calcolo secondo Laplace, ma anche della definizione stessa. In particolare, una matrice triangolare è invertibile se e solo se i suoi elementi diagonali sono tutti non nulli. Verificare che, allora, anche la matrice inversa è triangolare.

4.3. Matrici a blocchi. Se la matrice è "a blocchi":

$$\det \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \det(A)\det(D) = \det \begin{pmatrix} A & 0 \\ C & D \end{pmatrix} ,$$

con A e D matrici quadrate. Anche questo segue subito dalla definizione (ogni addendo del determinante che coinvolge un elemento di B o di C coinvolge anche un fattore nullo), come pure da un facile argomento usando la riduzione di Gauss. Si generalizzi per più blocchi. Si può dare una interpretazione geometrica (in termini di volumi)?

4.4. Se $A, B \in M_{n,m}(\Bbbk)$ (non necessariamente quadrate), allora $A^{\mathrm{t}}B \in M_m(\Bbbk)$, $AB^{\mathrm{t}} \in M_n(\Bbbk)$ (se $n \neq m$ quella di ordine maggiore ha necessariamente determinante nullo). Abbiamo che

$$\det(\,\mathbb{I}_m + A^{\mathrm{t}}B\,) = \det(\,\mathbb{I}_n + AB^{\mathrm{t}}\,)$$

(esplicitare in particolare se A, B sono righe o colonne). Il risultato si può dedurre facilmente dai seguenti prodotti di matrici quadrate:

$$\begin{pmatrix} \mathbb{I}_n & A \\ -B^{\mathrm{t}} & \mathbb{I}_m \end{pmatrix} \begin{pmatrix} \mathbb{I}_n & 0 \\ B^{\mathrm{t}} & \mathbb{I}_m \end{pmatrix} = \begin{pmatrix} \mathbb{I}_n + AB^{\mathrm{t}} & A \\ 0 & \mathbb{I}_m \end{pmatrix} \qquad \text{e} \qquad \begin{pmatrix} \mathbb{I}_n & 0 \\ B^{\mathrm{t}} & \mathbb{I}_m \end{pmatrix} \begin{pmatrix} \mathbb{I}_n & A \\ -B^{\mathrm{t}} & \mathbb{I}_m \end{pmatrix} = \begin{pmatrix} \mathbb{I}_n & A \\ 0 & \mathbb{I}_m + B^{\mathrm{t}}A \end{pmatrix}$$

(uguagliando i determinanti) e si può generalizzare usando una matrice scalare invece che la matrice identica:

$$c^n \det(\,c\mathbb{I}_m + A^{\mathrm{t}}B\,) = c^m \det(\,c\mathbb{I}_n + AB^{\mathrm{t}}\,)$$

(anche se $c = 0$?).

4.5. Complemento di Schur. In generale, se A e D sono matrici quadrate possiamo cercare una fattorizzazione di una matrice a blocchi nel seguente modo:

$$P = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & 0 \\ C & \mathbb{I} \end{pmatrix} \begin{pmatrix} \mathbb{I} & Y \\ 0 & X \end{pmatrix} = \begin{pmatrix} A & AY \\ C & CY + X \end{pmatrix}$$

da cui segue che $AY = B$ e $CY + X = D$, e se A è invertibile deve essere $Y = A^{-1}B$ e $X = D - CA^{-1}B$ (quest'ultimo termine si chiama complemento di Schur della matrice a blocchi P rispetto al blocco A, e si indica con $(P|A)$). Si conclude che, se A è invertibile, allora

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(A)\det(X) = \det(A)\det(D - CA^{-1}B) = \det(AD - ACA^{-1}B).$$

4.5.1. In particolare: se A è invertibile e $AC = CA$ (A e C commutano, in particolare sono quadrate dello stesso ordine...), allora la formula si riduce a

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - CB).$$

Calcoli analoghi si possono impostare se D è invertibile.

4.5.2. Nel caso $D = d \in \Bbbk = M_1(\Bbbk)$, $u, v \in \Bbbk^n = M_{n,1}(\Bbbk)$ abbiamo:

$$\det \begin{pmatrix} A & u \\ v^{\mathrm{t}} & d \end{pmatrix} = \det(A)(d - v^{\mathrm{t}}A^{-1}u) = d\det(A) - v^{\mathrm{t}}A^{\mathrm{c}}u$$

e nel caso $d = 1$ abbiamo anche

$$\det(A - v^{\mathrm{t}}u) = \det \begin{pmatrix} A & u \\ v^{\mathrm{t}} & 1 \end{pmatrix} = \det(A) - v^{\mathrm{t}}A^{\mathrm{c}}u$$

(la prima uguaglianza è quella nuova, si ottiene per esempio con operazioni elementari sul secondo membro per cancellare u; cosa succede se $d = 0$ oppure $d \neq 0, 1$?).

4.5.3. Come applicazione si può vedere che

$$\det \begin{pmatrix} \mathbb{I} & A \\ A^{\mathrm{t}} & \mathbb{I} \end{pmatrix} = \det(\mathbb{I} - A^{\mathrm{t}}A) = 1 - \Sigma M_1^2 + \Sigma M_2^2 - \Sigma M_3^2 + \cdots$$

dove ΣM_i^2 sono le somme dei quadrati dei minori di ordine i di A, ovvero la somma dei minori principali di ordine i di $A^{\mathrm{t}}A$ (si capisce meglio dai coefficienti del polinomio caratteristico di una matrice...).

4.6. Alternanti. In generale si dicono alternanti i polinomi di più variabili che cambiano di segno quando "si scambino tra loro" due qualsiasi delle variabili. È chiaro che, dati n polinomi $f_1(x), \dots, f_n(x)$ in una variabile e n termini $x_1, \dots, x_n$, i determinanti di matrici del tipo $(f_i(x_j))$ sono polinomi alternanti delle variabili x_j, e per questo vengono anch'essi detti alternanti.

I più semplici alternanti, ed in effetti quelli importanti, sono quelli di Vandermonde e le loro generalizzazioni.

4.6.1. Matrici e determinanti di Vandermonde. Si dice matrice di Vandermonde di termini $x_0, x_1, \dots, x_n$ e si indica con $VdM(x_0, x_1, \dots, x_n)$ la matrice d'ordine $n+1$ la cui i-esima colonna è formata dalle potenze (da 0 a n) del termine x_i. Per il determinante, abbiamo

$$vdm(x_0, x_1, \dots, x_n) := \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ x_0^2 & x_1^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_0^n & x_1^n & \cdots & x_n^n \end{pmatrix} = \prod_{0 \leqslant i < j \leqslant n} (x_j - x_i) \ ;$$

il calcolo può essere fatto per induzione su n (conviene effettuare operazioni elementari sulle righe, sottraendo ad ogni riga la precedente moltiplicata per x_0; si ottengono dei fattori $(x_i - x_0)$ da raccogliere e rimane una matrice dello stesso tipo e di ordine diminuito).

In particolare si vede che una matrice di Vandermonde è invertibile se e solo se $x_i \neq x_j$ per ogni $i \neq j$; in questo caso, possiamo calcolarne la matrice inversa usando la seguente osservazione: il polinomio nelle X dato da

$$(X - a_1)(X - a_2) \cdots (X - a_n) = X^n - p_1 X^{n-1} + p_2 X^{n-2} + \cdots + (-1)^i p_i X^{n-i} + \cdots + (-1)^{n-1} p_{n-1} X + (-1)^n p_n$$

si annulla per $X = a_1, a_2, \dots, a_n$ (i termini p_ℓ sono i polinomi simmetrici elementari nei valori $a_1, a_2, \dots, a_n$: p_ℓ è la somma di tutti i possibili prodotti di ℓ valori distinti tra gli a_i). Usando questo fatto si vede che la matrice inversa della matrice di Vandermonde ha come i-esima riga i polinomi simmetrici p_ℓ calcolati nelle variabili x_j con $j \neq i$, moltiplicata per un opportuno coefficiente (quale?).

4.6.2. Nel caso speciale in cui $x_i = x^i$ $(i = 1, \dots, n)$ si ottiene che il determinante è

$$VdM(1, x, x^2, \dots, x^n) = x^{\frac{n(n^2-1)}{6}} (x-1)^n (x^2-1)^{n-1} (x^3-1)^{n-2} \cdots (x^{n-1}-1)^2 (x^n - 1).$$

4.6.3. Un caso particolarmente interessante sono le matrici di Vandermonde del tipo $\Omega_n = \frac{1}{\sqrt{n}} VdM(1, \omega, \omega^2, \dots, \omega^{n-1})$ nel caso che $\omega \in \mathbb{C}$ sia una radice primitiva n-esima dell'unità. In tal caso si tratta di matrici simmetriche, e la matrice inversa è la (trasposta) coniugata. I primi esempi sono:

$$\Omega_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \Omega_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \overline{\omega} \\ 1 & \overline{\omega} & \omega \end{pmatrix},$$

ove $\omega = e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}$,

$$\Omega_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & -1 & \overline{\omega} \\ 1 & -1 & 1 & -1 \\ 1 & \overline{\omega} & -1 & \omega \end{pmatrix},$$

ove $\omega = \pm i$,

$$\Omega_5 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \overline{\omega}^2 & \overline{\omega} \\ 1 & \omega^2 & \overline{\omega} & \omega & \overline{\omega}^2 \\ 1 & \overline{\omega}^2 & \omega & \overline{\omega} & \omega^2 \\ 1 & \overline{\omega} & \overline{\omega}^2 & \omega^2 & \omega \end{pmatrix}$$

ove $\omega = e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}} e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}$. Quali sono i determinanti di queste matrici?

♠ **4.6.4.** Applicazione alle formule di Cardano. Consideriamo l'equazione standard di terzo grado $x^3 + px + q = 0$, e sia $X = diag(x_1, x_2, x_3)$ la matrice diagonale avente in diagonale le soluzioni (si noti che $\operatorname{tr} X = x_1 + x_2 + x_3 = 0$). Allora risulta $X^3 + pX + q\mathbb{I}_3 = \mathbb{O}_3$. Se consideriamo la matrice $\overline{\Omega_3} X \Omega_3 = \alpha\Sigma + \beta\Sigma^2$ ove $\Sigma = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, abbiamo che $\sqrt{3}(0, \beta, \alpha) = (x_1, x_2, x_3)\overline{\Omega_3}$ da cui $(x_1, x_2, x_3) = (0, \beta, \alpha)\Omega_3 = (\beta, \alpha) \left(\begin{smallmatrix} 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{smallmatrix}\right)$ (principio di sovrapposizione). I valori di α e β possono essere ricavati dal sistema (di grado sei, ma bicubico) che si ottiene sostituendo $\overline{\Omega_3} X \Omega_3 = \alpha\Sigma + \beta\Sigma^2$ nell'equazione $(\overline{\Omega_3} X \Omega_3)^3 + p(\overline{\Omega_3} X \Omega_3) + q\mathbb{I}_3 = \mathbb{O}_3$.

♠ **4.6.5.** Applicazione alle formule di Ferrari. Consideriamo l'equazione standard di quarto grado $x^4 + px^2 + qx + r = 0$, e sia $X = diag(x_1, x_2, x_3, x_4)$ la matrice diagonale avente in diagonale le soluzioni (si noti che $\operatorname{tr} X = x_1 + x_2 + x_3 + x_4 = 0$). Allora risulta $X^4 + pX^2 + qX + r\mathbb{I}_4 = \mathbb{O}_4$. Se consideriamo la matrice $\overline{\Omega_4} X \Omega_4 = \alpha\Sigma + \beta\Sigma^2 + \gamma\Sigma^3$ ove $\Sigma = \left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right)$, abbiamo che $2(0, \gamma, \beta, \alpha) = (x_1, x_2, x_3, x_4)\overline{\Omega_4}$ da cui $(x_1, x_2, x_3, x_4) = (0, \gamma, \beta, \alpha)\Omega_4 = (\gamma, \beta, \alpha) \left(\begin{smallmatrix} 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & 1 & \omega^2 \\ 1 & \omega^3 & \omega^2 & \omega \end{smallmatrix}\right)$ (principio di sovrapposizione). I valori di α, β e γ possono essere ricavati dal sistema (di grado alto, e di soluzione difficile, ma possibile) che si ottiene sostituendo $\overline{\Omega_4} X \Omega_4 = \alpha\Sigma + \beta\Sigma^2 + \gamma\Sigma^3$ nell'equazione $(\overline{\Omega_4} X \Omega_4)^4 + p(\overline{\Omega_4} X \Omega_4)^2 + q(\overline{\Omega_4} X \Omega_4) + r\mathbb{I}_4 = \mathbb{O}_4$.

♠♠ **4.6.6.** Matrici e determinanti di Vandermonde generalizzati. Le matrici di Vandermonde generalizzate $VdM(x, \alpha) = VdM(x_0, \dots, x_n; \alpha_0, \dots, \alpha_n)$ di variabili $x_0, \dots, x_n$ ed esponenti $\alpha_0 \leqslant \dots \leqslant \alpha_n$ sono le matrici definite da $VdM(x, \alpha) = (x_i^{\alpha_j})$. È chiaro che il loro determinante si annulla se due valori o due esponenti coincidono. Osserviamo che $VdM(x_0, \dots, x_n) = VdM(x_0, \dots, x_n; 0, 1, \dots, n)$. Inoltre l'ovvia relazione

$$vdm(x_0, \dots, x_n; \alpha_0, \alpha_1, \dots, \alpha_n) = (\Pi_i x_i^{\alpha_0}) vdm(x_0, \dots, x_n; 0, \alpha_1 - \alpha_0, \dots, \alpha_n - \alpha_0)$$

permette di ricondursi al caso $\alpha_0 = 0$. Un'altra relazione ovvia è data da

$$vdm(x_0, \dots, x_n; \alpha\alpha_0, \alpha\alpha_1, \dots, \alpha\alpha_n) = vdm(x_0^\alpha, \dots, x_n^\alpha; \alpha_0, \alpha_1, \dots, \alpha_n) \ .$$

Per il calcolo del determinante $vdm(x, \alpha)$ conviene osservare che, poiché esso si annulla se due valori delle variabili coincidono, esso sarà divisibile per il determinante $vdm(x)$ prima calcolato, e il rapporto $vdm(x, \alpha)/vdm(x)$ è un polinomio simmetrico nelle variabili $x_0, \dots, x_n$. Dobbiamo perciò introdurre qualche nozione sui polinomi simmetrici delle variabili $x_1, x_2, \dots, x_n$. Conviene introdurre il prodotto

$$p(x_1, x_2, \dots, x_n, T) = \prod_{i=1}^{n} (1 - x_i T) = \sum_{j=0}^{n} (-)^j p_j(x_1, x_2, \dots, x_n) T^j$$

(dunque $p_0 = 1$, $p_1 = \Sigma_i x_i$, $p_2 = \Sigma_{i<j} x_i x_j$, ed in generale p_j è la somma degli $\binom{n}{j}$ prodotti degli x_i presi a j a j senza ripetizioni: si dicono i polinomi simmetrici elementari) e il prodotto inverso

$$h(x_1, x_2, \dots, x_n, T) = \prod_{i=1}^{n} \frac{1}{1 - x_i T} = \prod_{i=1}^{n} (1 + x_i T + x_i^2 T^2 + x_i^3 T^3 + \cdots) = \sum_{j=0}^{\infty} h_j(x_1, x_2, \dots, x_n) T^j$$

(dunque $h_0 = 1$, $h_1 = \Sigma_i x_i$, $h_2 = \Sigma_i x_i^2 + \Sigma_{i<j} x_i x_j$, ed in generale h_j è la somma degli $\binom{n+j-1}{j}$ monomi di grado j negli x_i: si dicono i polinomi simmetrici elementari completi). Dalla ovvia relazione

$p(x,T)h(x,T) = h(x,T)p(x,T) = 1$ otteniamo che, dette

$$P = \begin{pmatrix} p_0 & 0 & 0 & \cdots & 0 \\ -p_1 & p_0 & 0 & \cdots & 0 \\ p_2 & -p_1 & p_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (-)^n p_n & (-)^{n-1}p_{n-1} & (-)^{n-2}p_{n-2} & \cdots & p_0 \end{pmatrix} \quad \text{e} \quad H = \begin{pmatrix} h_0 & 0 & 0 & \cdots & 0 \\ h_1 & h_0 & 0 & \cdots & 0 \\ h_2 & h_1 & h_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_n & h_{n-1} & h_{n-2} & \cdots & h_0 \end{pmatrix}$$

si ha $PH = HP = \mathbb{I}_n$, ovvero $PH_{(1)} = e_1$ che riassume le cosiddette relazioni di Wronski:

$$\begin{aligned} 1 &= p_0 h_0 \\ 0 &= -p_1 h_0 + p_0 h_1 \\ 0 &= p_2 h_0 - p_1 h_1 + p_0 h_2 \\ &\vdots \\ 0 &= (-)^n p_n h_0 + (-)^{n-1} p_{n-1} h_1 + \cdots + p_0 h_n \ . \end{aligned}$$

I polinomi simmetrici elementari completi ci saranno particolarmente utili poiché soddisfano a importanti relazioni ricorsive: infatti dalle ovvie relazioni

$$h_r(x_1, \ldots, x_i, \ldots, x_n) = h_r(x_1, \ldots, \widehat{x_i}, \ldots, x_n) + x_i h_{r-1}(x_1, \ldots, x_i, \ldots, x_n)$$

(che abbreviamo con

$$h_r = h_r(\widehat{x_i}) + x_i h_{r-1} \ ;$$

ricordiamo che l'accento circonflesso indica che il termine accentato viene tolto dall'espressione) valide per ogni r e ogni i, possiamo ottenere (per sottrazione) che

$$(x_j - x_i) h_{r-1} = h_r(\widehat{x_i}) - h_r(\widehat{x_j}) \ .$$

♠♠ **4.6.7.** Valutazione dei determinanti di Vandermonde generalizzati in termini dei polinomi simmetrici elementari completi. Consideriamo ora la matrice

$$VdM(x_0, \ldots, x_n; \alpha_0, \ldots, \alpha_n) = (h_{\alpha_j}(x_i))$$

(ogni riga ha sempre la stessa variabile, elevata alle diverse potenze α_j). Considerando la seguente sequenza di operazioni elementari:

(1) togliere ad ogni riga (dalla seconda in poi) la prima, e raccogliere i fattori $x_i - x_0$, lasciando i termini $h_{\alpha_j - 1}(x_0, x_i)$;

(2) togliere ad ogni riga (dalla terza in poi) la seconda, e raccogliere i fattori $x_i - x_1$, lasciando i termini $h_{\alpha_j - 2}(x_0, x_1, x_i)$; ...

(ℓ) togliere ad ogni riga (dalla ℓ+1-esima in poi) la ℓ-esima, e raccogliere i fattori $x_i - x_\ell$, lasciando i termini $h_{\alpha_j - \ell}(x_0, \ldots, x_\ell, x_i)$; ...

(n) togliere all'ultima riga la penultima riga , e raccogliere il fattore $x_n - x_{n-1}$, lasciando i termini $h_{\alpha_j - n}(x_0, x_1, \ldots, x_n)$;

in cui ogni volta si usa la formula induttiva dei polinomi simmetrici elementari completi, si ottiene l'uguaglianza di determinanti

$$vdm(x_0, \ldots, x_n; \alpha_0, \ldots, \alpha_n) = vdm(x_0, \ldots, x_n) \det \big(h_{\alpha_j - i}(x_0, \ldots, x_i)\big) \ .$$

Per ottenere una espressione più omogenea nelle variabili, si possono continuare le operazioni elementari, sommando ripetutamente ad ogni riga i-esima la successiva moltiplicata per x_{i+1}, per ottenere l'espressione di Cauchy

$$\begin{aligned} vdm(x_0, \ldots, x_n; \alpha_0, \ldots, \alpha_n) &= vdm(x_0, \ldots, x_n) \det \big(h_{\alpha_j - i}(x_0, \ldots, x_n)\big) \\ &= vdm(x_0, \ldots, x_n) \det \begin{pmatrix} h_{\alpha_0} & h_{\alpha_1} & \cdots & h_{\alpha_n} \\ h_{\alpha_0 - 1} & h_{\alpha_1 - 1} & \cdots & h_{\alpha_n - 1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{\alpha_0 - n} & h_{\alpha_1 - n} & \cdots & h_{\alpha_n - n} \end{pmatrix} \ . \end{aligned}$$

♠ **4.6.8.** Casi particolari. Se $\alpha_i = i$ per ogni i, allora ritroviamo il determinante di Vandermonde, poiché abbiamo a destra una matrice triangolare con 1 su tutta la diagonale. Si osservino poi i casi interessanti

$$vdm(x_0,\dots,x_n;0,1,\dots,n{-}1,n{+}1) = (\Sigma_i x_i) vdm(x_0,\dots,x_n)$$

e in generale per $N > n$

$$vdm(x_0,\dots,x_n;0,1,\dots,n{-}1,N) = h_{N-n}(x_0,\dots,x_n) vdm(x_0,\dots,x_n)\ .$$

Inoltre per $M, N > n-1$ abbiamo

$$\begin{aligned} vdm(x_0,\dots,x_n;0,1,\dots,n{-}2,M,N) &= \det\begin{pmatrix} h_{M-n+1} & h_{N-n+1} \\ h_{M-n} & h_{N-n} \end{pmatrix} vdm(x_0,\dots,x_n) \\ &= (h_{M-n+1}h_{N-n} - h_{N-n+1}h_{M-n}) vdm(x_0,\dots,x_n)\ . \end{aligned}$$

♠♠ **4.6.9.** Valutazione dei determinanti di Vandermonde generalizzati in termini dei polinomi simmetrici elementari. Il determinante che descrive il rapporto $vdm(x;\alpha)/vdm(x)$ può anche essere espresso in termini di polinomi simmetrici elementari. Detti $\beta_1,\dots,\beta_m$ l'insieme complementare agli indici $\alpha_0,\dots,\alpha_n$ in $\{0,1,\dots,\alpha_n\}$, il (futuro) teorema di Jacobi sui minori della matrice dei complementi algebrici dà la formula

$$\begin{aligned} vdm(x_0,\dots,x_n;\alpha_0,\dots,\alpha_n) &= vdm(x_0,\dots,x_n)\det\big(p_{n-\beta_j+i}(x_0,\dots,x_n)\big) \\ &= vdm(x_0,\dots,x_n)\det\begin{pmatrix} p_{n-\beta_0+1} & p_{n-\beta_1+1} & \cdots & p_{n-\beta_m+1} \\ p_{n-\beta_0+2} & p_{n-\beta_1+2} & \cdots & p_{n-\beta_m+2} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n-\beta_0+m} & p_{n-\beta_1+m} & \cdots & p_{n-\beta_m+m} \end{pmatrix} \end{aligned}$$

(a meno di un segno?) che risulta particolarmente utile quando $m = \alpha_n - n \leqslant n$.

♠♠ **4.6.10.** Matrici e determinanti differenziati confluenti. Per ogni $m \leqslant n$ consideriamo le matrici "differenziate"

$$D_{m,n}(x) := \begin{pmatrix} 1 \\ \frac{d}{dx} \\ \frac{1}{2}\frac{d^2}{dx^2} \\ \vdots \\ \frac{1}{m!}\frac{d^m}{dx^m} \end{pmatrix} \begin{pmatrix} 1 & x & x^2 & \cdots & x^n \end{pmatrix} = \begin{pmatrix} 1 & x & x^2 & x^3 & \cdots & \cdots & x^n \\ 0 & 1 & 2x & 3x^2 & \cdots & \cdots & nx^{n-1} \\ 0 & 0 & 1 & 3x & \cdots & \cdots & \binom{n}{2}x^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \cdots & \binom{n}{m}x^{n-m} \end{pmatrix}$$

ove il termine in posto (i,j) è $\binom{j}{i-1}x^{j-i}$.

Considerata ora una partizione $n_1, n_2, \dots, n_s$ di n (dunque n_i sono interi positivi con somma n), consideriamo la matrice quadrata

$$D_{(n_1,\dots,n_s)}(x_1,\dots,x_s) = \begin{pmatrix} D_{n_1,n}(x_1) \\ D_{n_2,n}(x_2) \\ \cdots \\ D_{n_s,n}(x_s) \end{pmatrix}$$

di cui vogliamo calcolare il determinante. Si tratta in effetti di una forma confluente (cioè in cui si identificano più variabili) di una matrice di Vandermonde opportunamente trasformata: se infatti ad ogni blocco di n_i righe della matrice $VdM(y_1,\dots,y_n) = (y_i^j)$ si applicano le trasformazioni elementari usate per studiare la forma generalizzata, e poi si identificano con x_t tutte le variabili y_i ove $n_{t-1} \leqslant i < n_t$, otteniamo esattamente la matrice $D_{(n_1,\dots,n_s)}(x_1,\dots,x_s)$. Quindi abbiamo che

$$d_{(n_1,\dots,n_s)}(x_1,\dots,x_s) = \lim_{\substack{y_i = x_t \\ (n_{t-1} \leqslant i < n_t)}} \frac{vdm(y_1,\dots,y_n)}{vdm(y_1,\dots,y_{n_1})\cdots vdm(y_{n_{s-1}+1},\dots,y_{n_s})} = \prod_{i<j}(x_j - x_i)^{n_i n_j}\ .$$

4.6.11. Alternanti doppi di Cauchy. Gli alternanti doppi di Cauchy sono i determinanti di matrici della forma

$$C(x_1,\dots,x_n;y_1,\dots,y_n) = \left(\frac{1}{y_i - x_j}\right)\ .$$

La valutazione del determinante si può fare in modo ricorsivo mediante le seguenti operazioni elementari:
(1) ad ogni colonna togliere l'ultima colonna, raccogliendo i fattori $\frac{y_n-y_i}{y_n-x_j}$;
(2) ad ogni riga togliere l'ultima riga, raccogliendo i fattori $\frac{x_j-x_n}{y_i-x_n}$;
ci si è ricondotti allora alla relazione ricorsiva

$$c(x_1,\dots,x_n;y_1,\dots,y_n)=\frac{\prod_i(y_n-y_i)\prod_j(x_j-x_n)}{\prod_j(y_n-x_j)\prod_i(y_i-x_n)}c(x_1,\dots,x_{n-1};y_1,\dots,y_{n-1})$$

che reiterato fornisce il risultato voluto:

$$c(x_1,\dots,x_n;y_1,\dots,y_n)=\frac{vdm(x_n,\dots,x_1)vdm(y_1,\dots,y_n)}{\prod_{i,j}(y_i-x_j)}\ .$$

Espandendo in serie nelle y_i i due membri dell'equazione, e poi equiparando i termini con potenze uguali, si riottengono le formule per i determinanti delle matrici generalizzate di Vandermonde.

4.7. Matrici antisimmetriche. Ricordiamo che una matrice quadrata A si dice antisimmetrica se $A^{\mathrm{t}}=-A$. Supponiamo che il corpo $\Bbbk$ abbia caratteristica diversa da 2 (altrimenti le matrici sono antisimmetriche se e solo se sono simmetriche); se A è antisimmetrica di ordine dispari, allora $|A|=0$. Infatti abbiamo $\det(A)=\det(A^{\mathrm{t}})=\det(-A)=-\det(A)$, da cui la conclusione. Inoltre abbiamo

$$\begin{vmatrix}0&a\\-a&0\end{vmatrix}=a^2\qquad\text{e}\qquad\begin{vmatrix}0&a&b&c\\-a&0&d&e\\-b&-d&0&f\\-c&-e&-f&0\end{vmatrix}=(af-be+cd)^2\ .$$

♠ **4.7.1.** Pfaffiani. Più in generale, il determinante di una matrice antisimmetrica d'ordine pari è il quadrato di un polinomio (a coefficienti interi) nelle entrate della matrice stessa; questa affermazione (tranne la parentesi) può essere dimostrata per induzione usando le formule degli sviluppi pivotali viste nel paragrafo precedente.

Il polinomio (determinato a meno del segno) il cui quadrato dà il determinante di una matrice antisimmetrica d'ordine $2n$ si dice Pfaffiano d'ordine n e si indica con $\mathrm{Pf}^n(x_{i,j})$ (le variabili hanno indici $1\leqslant i<j\leqslant 2n$ e sono in numero di $n(n-1)/2$). Di nuovo per induzione sull'ordine si può dimostrare che

$$\mathrm{Pf}^n(x_{i,j})=\sum_{\substack{1\leqslant i_s<j_s\leqslant n\\(1\leqslant s\leqslant n)}}\operatorname{sgn}\begin{pmatrix}1&2&3&4&\cdots&2n-1&2n\\i_1&j_1&i_2&j_2&\cdots&i_n&j_n\end{pmatrix}x_{i_1,j_1}x_{i_2,j_2}\cdots x_{i_n,j_n}$$

ove la sommatoria comprende $(2n-1)!!$ termini (e sono tutti i prodotti di n termini $x_{i,j}$ ove $i<j$ e gli indici sono tutti diversi).

4.8. Circolanti. Si chiamano circolanti le matrici le cui righe si ottengono ognuna dalla precedente "circolando" i termini di un posto a destra; si tratta quindi di matrici della forma

$$C(a_1,a_2,a_3,\dots,a_{n-1},a_n)=\begin{pmatrix}a_1&a_2&a_3&\cdots&a_{n-1}&a_n\\a_n&a_1&a_2&\cdots&a_{n-2}&a_{n-1}\\a_{n-1}&a_n&a_1&\cdots&a_{n-3}&a_{n-2}\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\a_3&a_4&a_5&\cdots&a_1&a_2\\a_2&a_3&a_4&\cdots&a_n&a_1\end{pmatrix}\ .$$

Per calcolare il determinante $c(a_1,a_2,a_3,\dots,a_{n-1},a_n)=|C(a_1,a_2,a_3,\dots,a_{n-1},a_n)|$ di una matrice circolante (detto esso stesso circolante) a coefficienti complessi possiamo ricorrere al metodo di Brioschi: moltiplicando a destra la matrice circolante $C=C(a_1,a_2,\dots,a_n)$ per la matrice di Vandermonde $V=VdM(1,\omega,\omega^2,\dots,w^{n-1})$, ove ω è una radice primitiva n-esima dell'unità, otteniamo $CV=V\mathrm{diag}(\vartheta_0,\dots,\vartheta_{n-1})$ ove $\vartheta_i=\sum_{j=0}^{n-1}a_{i+1}\omega^{ij}$ per $i=0,1,\dots,n-1$. Passando ai determinanti, otteniamo che

$$c(a_1,a_2,a_3,\dots,a_{n-1},a_n)=\prod_{i=0}^{n-1}\vartheta_i=\prod_{i=0}^{n-1}\sum_{j=0}^{n-1}a_{i+1}\omega^{ij}\ .$$

Si osservi che se la matrice circolante ha coefficienti reali, anche il determinante è reale, sebbene la formula comporti calcoli con radici complesse dell'unità.

4.8.1. Matrici e determinanti anticircolanti si ottengono da una riga circolando a sinistra i termini. Che relazioni vi sono con le matrici e i determinanti circolanti?

4.8.2. Un caso particolare in cui è possibile semplificare il calcolo è la matrice circolante

$$C(a, a+d, a+2d, \dots, a+(n-1)d)\ .$$

In tal caso sottraendo ad ogni colonna la precedente si trova una matrice della forma

$$\begin{pmatrix} a & d & d & \cdots & d \\ a+(n-1)d & -(n-1)d & d & \cdots & d \\ a+(n-2)d & d & -(n-1)d & \cdots & d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a+d & d & d & \cdots & -(n-1)d \end{pmatrix}$$

e sostituendo la prima riga con la somma di tutte le righe si può valutare il determinante come

$$c(a, a+d, a+2d, \dots, a+(n-1)d) = n(a+\frac{n-1}{2}d)(-1)^{n-1}d^{n-1}n^{n-2} = (-nd)^{n-1}\left(a+\frac{n-1}{2}d\right)$$

(si osservi che la matrice d'ordine n avente entrate non diagonali tutte uguali ad 1 ed entrate non diagonali uguali ad $1-x$ vale $(n-x)(-x)^{n-1} = (-1)^n x^{n-1}(x-n)$; si può vedere con le riduzioni elementari consistenti nel sottrarre alla prima riga tutte le altre, poi raccogliere il termine comune, e infine sottrarre la prima riga a tutte le altre; ma sarà più facile quando si conosceranno le nozioni di polinomio caratteristico e autovalori di una matrice).

4.8.3. In particolare abbiamo che $c(1, 2, \cdots, n) = \dfrac{n+1}{2}(-n)^{n-1}$.

4.9. Ricorrenti. Si indicano con il nome di ricorrenti i determinanti di matrici le cui entrate sono nulle per indici (i, j) con $i > j+1$, quindi del tipo

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n-1} & a_{2,n} \\ 0 & a_{3,2} & \cdots & a_{3,n-1} & a_{3,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{n,n-1} & a_{n,n} \end{pmatrix}\ .$$

Il nome è dovuto al fatto che questi determinanti soddisfano a delle uguaglianze ricorsive al variare dell'ordine n. Detto infatti R_n il determinante della matrice d'ordine n, sviluppando rispetto all'ultima riga abbiamo due termini, uno contenente R_{n-1}, e l'altro contenente il determinante di una matrice con soli due termini nell'ultima riga; sviluppando ripetutamente rispetto all'ultima riga otteniamo che

$$R_n = a_{n,n}R_{n-1} - a_{n,n-1}a_{n-1,n}R_{n-2} + a_{n,n-1}a_{n-1,n-2}a_{n-2,n}R_{n-3} - \cdots + (-1)^n \Pi_j a_{j,j-1}$$

(il termine che moltiplica R_{n-i} è $a_{n,n-1}a_{n-1,n-2}\cdots a_{n-i+2,n-i+1}a_{n-i+1,n}$ con il segno $(-1)^{i+1}$).

4.9.1. Casi in cui in ogni diagonale i termini sono tutti uguali?

4.9.2. Casi in cui la diagonale sotto la principale ha termini tutti 1?

4.10. Tridiagonanti. Un caso interessante è quello di ricorrenti in cui solo la diagonale principale e i termini immediatamente adiacenti sono non nulli; si parla allora di tridiagonanti. Indicato con T_n il determinante della matrice

$$\begin{pmatrix} a_0 & b_1 & 0 & \cdots & 0 & 0 \\ c_1 & a_1 & b_2 & \cdots & 0 & 0 \\ 0 & c_2 & a_2 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & a_{n-2} & b_{n-1} \\ 0 & 0 & 0 & \cdots & c_{n-1} & a_{n-1} \end{pmatrix}\ .$$

la relazione ricorsiva diventa semplicemente

$$T_n = a_{n-1}T_{n-1} - c_{n-1}b_{n-1}T_{n-2} \ .$$

Nel caso in cui $a_i = a$, $b_i = b$ e $c_i = c$ sono costanti per $i \geqslant 2$ da queste relazioni ricorsive si possono determinare formule chiuse per tali determinanti (come vedremo in un futuro capitolo studiando le forme canoniche delle matrici).

4.10.1. Nel caso in cui $a_i = 0$ per ogni i?

4.10.2. Nel caso in cui $b_i = i$ e $c_i = n - i + 1$ per ogni i?

4.10.3. Nel caso in cui $b_i = 1$ e $c_i = 1$ per ogni i?

♠ **4.11.** Continuanti. Si dicono continuanti i tridiagonanti con $c_i = -1$ per ogni i. In questo caso essi soddisfano alle formule ricorsive

$$T_n = a_{n-1}T_{n-1} + b_{n-1}T_{n-2} \ .$$

Il nome è dovuto al seguente fatto: una frazione continua è una espressione del tipo

$$F_n = \cfrac{1}{a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \ddots + \cfrac{b_{n-2}}{a_{n-2} + \cfrac{b_{n-1}}{a_{n-1}}}}}}$$

ove $a_i, b_i \in \mathbb{N}$ per ogni i (queste frazioni continue sono importanti, poiché ogni numero reale compreso tra 0 e 1 si può scrivere in tali termini con frazioni continue infinite, e le approssimazioni successive che si ottengono troncando la frazione continua sono particolarmente buone). Si dimostra per induzione su n che, detto $F_n = p_n/q_n$ (numeratore e denominatore sono funzioni di a_i e b_i), valgono le relazioni ricorsive $p_n = a_{n-1}p_{n-1} + b_{n-1}p_{n-2}$ ($p_0 = 0$ e $p_1 = 1$) e $q_n = a_{n-1}q_{n-1} + b_{n-1}q_{n-2}$ ($q_{-1} = 0$ e $q_0 = 1$). Infatti possiamo calcolare facilmente i primi casi:

$$\begin{array}{lll}
F_1 = \dfrac{1}{a_0} & p_1 = 1 & q_1 = a_0 \\
F_2 = \dfrac{a_1}{a_0a_1 + b_1} & p_2 = a_1 & q_2 = a_0a_1 + b_1 \\
F_3 = \dfrac{a_1a_2 + b_2}{a_0a_1a_2 + a_0b_2 + a_2b_1} & p_3 = a_1a_2 + b_2 & q_3 = a_0a_1a_2 + a_0b_2 + a_2b_1
\end{array}$$

e per il caso induttivo, possiamo calcolare F_n tenendo conto che $\frac{b_{n-2}}{a_{n-2} + \frac{b_{n-1}}{a_{n-1}}} = \frac{a_{n-1}b_{n-2}}{a_{n-1}a_{n-1} + b_{n-1}}$ otteniamo

$$\begin{aligned}
\frac{p_n}{q_n} &= \frac{p_{n-1}(b_{n-2} = a_{n-1}b_{n-2}; a_{n-2} = a_{n-1}a_{n-2} + b_{n-1})}{q_{n-1}(b_{n-2} = a_{n-1}b_{n-2}; a_{n-2} = a_{n-1}a_{n-2} + b_{n-1})} \\
&= \frac{(a_{n-1}a_{n-2} + b_{n-1})p_{n-2} + (a_{n-1}b_{n-2})p_{n-3}}{(a_{n-1}a_{n-2} + b_{n-1})q_{n-2} + (a_{n-1}b_{n-2})q_{n-3}} \\
&= \frac{a_{n-1}(a_{n-2}p_{n-2} + b_{n-2}p_{n-3}) + b_{n-1}p_{n-2}}{a_{n-1}(a_{n-2}q_{n-2} + b_{n-2}q_{n-3}) + b_{n-1}q_{n-2}} \\
&= \frac{a_{n-1}p_{n-1} + b_{n-1}p_{n-2}}{a_{n-1}q_{n-1} + b_{n-1}q_{n-2}}
\end{aligned}$$

(abbiamo usato l'ipotesi induttiva nel secondo e nel quarto passaggio).

Siccome le relazioni ricorsive che danno i continuanti t_n sono le stesse che regolano numeratore p_n e denominatore q_n della frazione continua, e tenendo conto dei valori iniziali, possiamo concludere che

$$F_n(a_0, a_1, b_1, \ldots, a_{n-1}, b_{n-1}) = \frac{T_{n-1}(a_1, a_2, b_2, \ldots, a_{n-1}, b_{n-1})}{T_n(a_0, a_1, b_1, \ldots, a_{n-1}, b_{n-1})}$$

per ogni $n \geqslant 1$ (ponendo $T_0 = 1$, determinante della matrice quadrata vuota).

4.12. Determinante di Cayley-Menger (Erone). Si osservi che

$$\begin{vmatrix} 0 & a & b & c \\ a & 0 & c & b \\ b & c & 0 & a \\ c & b & a & 0 \end{vmatrix} = \begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & c^2 & b^2 \\ 1 & c^2 & 0 & a^2 \\ 1 & b^2 & a^2 & 0 \end{vmatrix} = -16\Delta^2$$

ove $\Delta = \sqrt{s(s-a)(s-b)(s-c)}$ è il termine di Erone per il calcolo dell'area del triangolo i cui lati hanno lunghezze a, b, c.

Inoltre

$$16\Delta^2 = \begin{pmatrix} a^2 & b^2 & c^2 \end{pmatrix} \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} a^2 \\ b^2 \\ c^2 \end{pmatrix}$$

(generalizzazioni?).

4.13. Matrici Elementari (ed una assiomatica alternativa per il determinante). Abbiamo già calcolato i determinanti delle matrici elementari; è interessante osservare che la funzione determinante è completamente definita dalle seguenti due condizioni:

$(D1)$ è moltiplicativa: $\det(AB) = \det A \det B$;

$(D2)$ vale α sulle matrici $H(i,\alpha) = \mathbb{I}_n + (\alpha - 1)e_{i,i}$.

Queste due proprietà possono essere prese come definizione per la funzione determinante, ed è facile allora dimostrarne l'unicità, meno facile dimostrarne l'esistenza.

Per mostrare l'unicità si procede per gradi (usiamo le lettere minuscole per indicare i determinanti):

(1) certamente le matrici $H(i,j,\alpha)$ hanno determinante non nullo, poiché $H(i,j,\alpha)H(i,j,-\alpha) = \mathbb{I}$; poiché inoltre $H(i,j,\alpha) = H(i,\alpha)H(i,j,1)H(i,1/\alpha)$ (se $\alpha \neq 0$) abbiamo che il determinante non dipende da α; ma allora da $h(i,j,\alpha) = h(i,j,2\alpha) = h(i,j,\alpha)h(i,j,\alpha)$ concludiamo che tale determinante è 1.

(2) dalla relazione $S(i,j) = H(i,-1)H(i,j,-1)H(j,i,1)H(i,j,-1)$ si deduce allora che $s(i,j) = -1$.

(3) usando la riduzione di Gauss per righe e per colonne, ogni matrice può essere scritta come prodotto di matrici elementari e di una matrice diagonale (eventualmente con zeri in diagonale se è degenere), e quindi il suo determinante può essere calcolato tramite questa decomposizione.

Si osservi anche che la proprietà richiesta $(D2)$ può essere indebolita, chiedendo solo che $\det H(1,\alpha) = \alpha$ (per ogni α). Infatti $H(i,\alpha) = S(1,i)H(1,\alpha)S(1,i)$.

4.13.1. Mostrare direttamente che le proprietà precedenti definiscono una funzione multilineare alternante sulle colonne (che vale 1 sulla matrice identica).

5. Rango e determinanti (minori).

5.1. Definizione-Teorema (minori e rango). *Sia $A \in M_{n,m}(\Bbbk)$ una matrice. I minori di ordine k della matrice A sono i determinanti delle sottomatrici quadrate di ordine k di A che si ottengono cancellando $n-k$ righe ed $m-k$ colonne di A. Il rango di una matrice coincide con il massimo ordine di un minore non nullo: la matrice A ha rango k se e solo se esiste un minore non nullo d'ordine k e tutti i minori d'ordine maggiore di k sono nulli.*

Dimostrazione. Se il rango di A è k, allora vi sono k colonne indipendenti, e dunque possiamo scegliere in quella sottomatrice k righe tali che il minore d'ordine k così trovato sia non nullo. Viceversa, se vi è un minore d'ordine k non nullo, le colonne coinvolte sono k colonne linearmente indipendenti, e dunque la matrice ha rango almeno k. □

5.1.1. Sia $A \in M_{n,m}(\Bbbk)$ una matrice. I minori d'ordine k sono in numero di $\binom{n}{k}\binom{m}{k}$. Supponiamo di avere un minore non nullo d'ordine $k-1$; qual è il numero minimo di minori d'ordine k che devono essere nulli affinché la matrice abbia rango $k-1$?

5.1.2. Si noti che se tutti i minori di ordine k sono nulli, allora anche tutti i minori d'ordine maggiore di k sono nulli. Come dimostrare direttamente questo risultato?

5.2. Principio dei minori orlati. Sia $A \in M_{n,m}(\Bbbk)$, e sia A' una sottomatrice quadrata d'ordine r il cui determinante sia non nullo. Allora il rango di A è r se e solo se tutti i minori di

A di ordine $r+1$ ottenuti da sottomatrici di A contenenti A' (sono i minori orlati di A') sono nulli (osservare che la condizione è ovviamente necessaria; che sia sufficiente invece non è ovvio: sono solo $(m-r)(n-r)$ i minori d'ordine $r+1$ nulli per ipotesi...). Dimostrazione?

5.2.1. Equazioni di sottospazi. Dati i vettori linearmente indipendenti $v_1, \dots, v_r$ nello spazio vettoriale standard $\Bbbk^n$, il sottospazio da essi generato è formato dai vettori X tali che la matrice $\begin{pmatrix} X & v_1 & \cdots & v_r \end{pmatrix}$ abbia rango r (e non $r+1$); quindi esso è descritto dall'annullamento di tutti i minori d'ordine $r+1$ della matrice detta: si tratta delle equazioni cartesiane del sottospazio. Sappiamo già che possiamo sceglierne $n-r$ per descrivere il sottospazio, e il principio dei minori orlati permette di farlo senza esplicitare tutti i minori: basta trovare un minore d'ordine r non nullo della matrice $\begin{pmatrix} v_1 & \cdots & v_r \end{pmatrix}$ (esiste per ipotesi, poiché $v_1, \dots, v_r$ sono linearmente indipendenti) e annullare tutti i minori d'ordine $r+1$ della matrice $\begin{pmatrix} X & v_1 & \cdots & v_r \end{pmatrix}$ che contengono il minore scelto, ovvero che si ottengono "orlando" la sottomatrice quadrata invertibile prima scelta. Si tratta esattamente di $n-r$ equazioni cartesiane indipendenti (perché? Osservare che la matrice del sistema si presenta quasi in forma a scalini).

♠ **5.3.** Teorema (di Jacobi sui minori della matrice dei complementi algebrici). *Siano I e J due sottinsiemi di $\{1, \dots, n\}$ di cardinalità k e indichiamo con $A^{(I)}_{(J)}$ la sottomatrice di A che si ottiene selezionando gli elementi $a_{i,j}$ con $i \in I$ e $j \in J$. Siano I' e J' gli insiemi complementari. Allora abbiamo*

$$|A^{\mathrm{c}(I)}_{(J)}| = \varepsilon(I, I')\varepsilon(J, J')|A|^{k-1}|A^{\mathrm{t}(I')}_{(J')}| \ ,$$

ovvero i minori d'ordine k di A^{c} coincidono con i minori segnati di A^{t} di indici complementari, moltiplicati per la potenza $k-1$-esima del determinante di A.

Dimostrazione. Vedremo dopo una generalizzazione con una dimostrazione più elegante. La dimostrazione classica procede invece così: supponiamo $I = J = \{1, \dots, k\}$ e consideriamo il prodotto di matrici

$$\begin{pmatrix} A^{(1)} \\ \vdots \\ A^{(k)} \\ A^{(k+1)} \\ \vdots \\ A^{(n)} \end{pmatrix} \begin{pmatrix} A^{\mathrm{c}}_{(1)} \cdots A^{\mathrm{c}}_{(k)} & e_{k+1} \cdots e_n \end{pmatrix} = \begin{pmatrix} |A|e_1 \cdots |A|e_k & A_{(k+1)} \cdots A_{(n)} \end{pmatrix}$$

dove la prima matrice è A (scritta a righe), la seconda è la matrice A^{c} in cui le colonne con indici in J' sono state sostituite con i vettori della base canonica di indici in I'. Calcolando i determinanti si ottiene il risultato voluto. In modo analogo si può tener conto della trasposizione e dei segni dei minori, come il lettore può scoprire calcolando i determinanti di $AB = C$ ove B è la matrice tale che $B_{(j_\ell)} = A^{\mathrm{c}}_{(j_\ell)}$ se $j_\ell \in J$ e $B_{(j'_\ell)} = e_{i_\ell}$ se $j'_\ell \notin J$; e quindi le colonne di C sono $C_{(j_\ell)} = |A|e_{(j_\ell)}$ se $j_\ell \in J$ e $C_{(j'_\ell)} = A_{(i'_\ell)}$ se $j'_\ell \notin J$. □

♠♠ **5.4.** Per capire meglio la rilevanza della nozione dei minori di una matrice quadrata, conviene dare delle definizioni più generali, e costruire, per ogni matrice $A \in M_n(\Bbbk)$ e per ogni $k \leqslant n$ la matrice formata da tutti i suoi minori d'ordine k (considerati nell'ordine lessicografico degli indici che lo formano) e una ulteriore matrice formata dai relativi cofattori (o minori complementari segnati) che entrano nelle formula generalizzate di Laplace. Si tratta di matrici quadrate d'ordine $\binom{n}{k}$.

5.4.1. Definizione (Ordine lessicografico). *Dati due sottinsiemi $I = \{i_1, i_2, \dots, i_k\}$ e $J = \{j_1, j_2, \dots, j_k\}$ di $\{1, 2, \dots, n\}$, diciamo che $I \preccurlyeq J$ (I precede J) se per il primo indice ℓ tale che $i_\ell \neq j_\ell$ si ha $i_\ell \leqslant j_\ell$. Si tratta dell'ordine che si usa nei vocabolari, ed è un ordine totale.*

5.4.2. Definizione (Matrici composte e matrici composte complementari). *Data $A \in M_n(\Bbbk)$, per ogni $k \leqslant n$ definiamo $M^{(k)}(A)$ la k-esima matrice composta o matrice dei minori d'ordine k come*

$$M^{(k)}(A) := \left(\left| A^{(I)}_{(J)} \right| \right)_{\substack{|I|=k \\ |J|=k}}$$

con l'ordine lessicografico degli indici I e J; e $C^{(k)}(A)$ la k-esima matrice complementare composta o matrice dei minori complementari segnati d'ordine $n-k$ come

$$C^{(k)}(A) := \left(\varepsilon(I,I')\varepsilon(J,J')\left|A^{(I')}_{(J')}\right|\right)^{\mathrm{t}}_{\substack{|I|=k\\|J|=k}}$$

con l'ordine lessicografico degli indici I e J (si tratta della matrice trasposta della matrice $M^{(k)}(A)$ in cui ogni minore è stato sostituito con il suo complemento segnato).

Si ha subito che $M^{(1)}(A) = A$ e $C^{(1)}(A) = A^{\mathrm{c}}$.

5.4.3. Teorema (rango). *Il rango di A è uguale ad r se e solo se $M^{(r)}(A) \neq \mathbb{O}$ e $M^{(r-1)}(A) = \mathbb{O}$; più in generale, il rango di $M^{(k)}(A)$ è uguale a $\binom{r}{k}$.*

Dagli sviluppi generalizzati di Laplace segue subito che:

5.4.4. Teorema (prodotto di composte e loro complementari). *Per ogni $k \leqslant n$ risulta*

$$M^{(k)}(A)C^{(k)}(A) = C^{(k)}(A)M^{(k)}(A) = |A|\mathbb{I}_{\binom{n}{k}} .$$

5.4.5. Teorema (Binet-Cauchy). *Per ogni $k \leqslant n$ risulta:*

(i) $M^{(k)}(\mathbb{I}_n) = \mathbb{I}_{\binom{n}{k}}$;

(ii) $M^{(k)}(AB) = M^{(k)}(A)M^{(k)}(B)$ *per ogni* $A, B \in M_n(\Bbbk)$;

(iii) $M^{(k)}(\alpha A) = \alpha^k M^{(k)}(A)$ *per ogni* $\alpha \in \Bbbk$;

(i′) $C^{(k)}(\mathbb{I}_n) = \mathbb{I}_{\binom{n}{k}}$;

(ii′) $C^{(k)}(AB) = C^{(k)}(B)C^{(k)}(A)$ *per ogni* $A, B \in M_n(\Bbbk)$;

(iii′) $C^{(k)}(\alpha A) = \alpha^{n-k}C^{(k)}(A)$ *per ogni* $\alpha \in \Bbbk$.

Dimostrazione. Non sono ovvii i punti (ii) e (ii'), che seguono dal calcolo di Binet-Cauchy per il determinante del prodotto $A'B'$ di matrici rettangolari $A' \in M_{k\times n}(\Bbbk)$ e $B' \in M_{n\times k}(\Bbbk)$. Si consideri infatti la seguente astuzia (di Binet):

$$\begin{pmatrix} \mathbb{O}_k & A' \\ B' & \mathbb{I}_n \end{pmatrix}\begin{pmatrix} -\mathbb{I}_k & \mathbb{O} \\ B' & \mathbb{I}_n \end{pmatrix} = \begin{pmatrix} A'B' & A' \\ \mathbb{O} & \mathbb{I}_n \end{pmatrix}$$

e sfruttando gli sviluppi di Laplace secondo le prime k righe otteniamo che $|A'B'|$ è nullo ogni volta che $k > n$, mentre è la somma $\Sigma_H |A'_{(H)}||B'^{(H)}|$ dei prodotti dei minori di indici corrispondenti di A' e B' se $k \leqslant n$.

Ora basta applicare questo principio al minore di righe I e colonne J della matrice AB, tenendo conto che

$$\begin{pmatrix} A^{(I)} \\ A^{(I')} \end{pmatrix}\begin{pmatrix} B_{(J)} & B_{(J')} \end{pmatrix} = \begin{pmatrix} A^{(I)}B_{(J)} & A^{(I)}B_{(J')} \\ A^{(I')}B_{(J)} & A^{(I')}B_{(J')} \end{pmatrix}$$

e il minore di interesse è proprio $A^{(I)}B_{(J)}$. □

5.4.6. Teorema (Cauchy-Sylvester). *Per ogni $k \leqslant n$ risulta $|M^{(k)}(A)C^{(k)}(A)| = |A|^{\binom{n}{k}}$; inoltre*

(i) $|M^{(k)}(A)| = |A|^{\binom{n-1}{k-1}}$;

(i′) $|C^{(k)}(A)| = |A|^{\binom{n-1}{k}}$.

Dimostrazione. La prima formula è ovvia dal prodotto delle matrici, quindi basta dimostrare (i). Poiché $|A|$ è polinomio irriducibile nelle entrate della matrice, il determinante cercato non può che esserne una potenza, e basta allora sapere qual è il grado omogeneo dei suoi termini. Ora $|M^{(k)}(A)|$ è polinomio di grado $k\binom{n}{k}$ nelle entrate di A, mentre $|A|$ è polinomio di grado n nelle stesse variabili. Poiché $\frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}$, abbiamo il risultato voluto. □

5.4.7. Teorema (inverse di composte e loro complementari). *Per ogni $k \leqslant n$ e per ogni matrice invertibile A, risulta*

(i) $M^{(k)}(A)^{-1} = M^{(k)}(A^{-1}) = |A|^{-1}C^{(k)}(A)$;

(i') $C^{(k)}(A)^{-1} = C^{(k)}(A^{-1}) = |A|^{-1}M^{(k)}(A)$.

Dimostrazione. Per dimostrare (i) basta applicare $M^{(k)}$ al prodotto $AA^{-1} = \mathbb{I}_n$, da cui $M^{(k)}(A)M^{(k)}(A^{-1}) = \mathbb{I}_{\binom{n}{k}}$, da cui la prima uguaglianza. La seconda uguaglianza segue dal confronto con la formula del prodotto $M^{(k)}(A)C^{(k)}(A) = |A|\mathbb{I}_{\binom{n}{k}}$. □

Si osservi anche che $M^{(k)}(A)^{\mathrm{t}} = M^{(k)}(A^{\mathrm{t}})$ e analogamente $C^{(k)}(A)^{\mathrm{t}} = C^{(k)}(A^{\mathrm{t}})$ (infatti $|A^{(I)}_{(J)}| = |(A^{\mathrm{t}})^{(J)}_{(I)}|$).

5.4.8. Teorema (Franke). *Per ogni $h, k \leqslant n$ risulta*
(i) $C^{(h)}(M^{(k)}(A)) = |A|^{\binom{n-1}{k-1}-h}M^{(h)}(C^{(k)}(A))$;
(i') $C^{(h)}(C^{(k)}(A)) = |A|^{\binom{n-1}{k}-h}M^{(h)}(M^{(k)}(A))$.

Dimostrazione. Basta confrontare l'espressione

$$M^{(h)}(M^{(k)}(A))M^{(h)}(C^{(k)}(A)) = |A|^h\mathbb{I}_{\binom{\binom{n}{k}}{h}}$$

ottenuta applicando $M^{(h)}$ al prodotto $M^{(k)}(A)C^{(k)}(A) = |A|\mathbb{I}_{\binom{n}{k}}$, con l'espressione

$$M^{(h)}(M^{(k)}(A))C^{(h)}(M^{(k)}(A)) = |M^{(k)}(A)|\mathbb{I}_{\binom{\binom{n}{k}}{h}} = |A|^{\binom{n-1}{k-1}}\mathbb{I}_{\binom{\binom{n}{k}}{h}}$$

ottenuta sostituendo A con $M^{(k)}(A)$ in $M^{(h)}(A)C^{(h)}(A) = |A|\mathbb{I}_{\binom{n}{h}}$, per ottenere (i); e con l'espressione

$$C^{(h)}(C^{(k)}(A))M^{(h)}(C^{(k)}(A)) = |C^{(k)}(A)|\mathbb{I}_{\binom{\binom{n}{k}}{h}} = |A|^{\binom{n-1}{k}}\mathbb{I}_{\binom{\binom{n}{k}}{h}}$$

ottenuta sostituendo A con $C^{(k)}(A)$ in $C^{(h)}(A)M^{(h)}(A) = |A|\mathbb{I}_{\binom{n}{h}}$, per ottenere (i'). □

In particolare usando $k = 1$ in (i) possiamo ritrovare il teorema di Jacobi sui minori di A^{c}, nella forma $C^{(h)}(A) = |A|^{1-h}M^{(h)}(A^{\mathrm{c}})$ (cioè $M^{(h)}(A^{\mathrm{c}}) = |A|^{h-1}C^{(h)}(A)$), mentre ponendo $h = 1$ otteniamo una espressione di $C^{(k)}(A)$ come matrice dei complementi algebrici di $M^{(k)}(A)$ moltiplicata per una opportuna costante.

Analoghe osservazioni si possono fare per (i').

6. Esercizi.

6.1. Sia $X = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ una matrice a blocchi, ove $A \in M_{r\times r}(\mathbb{R})$ e $C \in M_{s\times s}(\mathbb{R})$. Si mostri che $\det X = \det A \det C$, usando la tecnica di riduzione di Gauss.

6.2. Sia $X = \begin{pmatrix} B & A \\ C & 0 \end{pmatrix}$ una matrice a blocchi, ove $A \in M_{r\times r}(\mathbb{R})$ e $C \in M_{s\times s}(\mathbb{R})$. Si calcoli il determinante di X.

6.3. Sia $A \in M_{(2n+1)\times(2n+1)}(\mathbb{R})$ tale che $A = -A^{\mathrm{t}}$. Mostrare che $\det A = 0$.

6.4. Determinare due matrici quadrate A, B tali che $\det(A + B) \neq \det A + \det B$.

6.5. Sia $\mathfrak{S}_n$ il gruppo simmetrico su $\{1, \dots, n\}$. Per ogni $\sigma \in \mathfrak{S}_n$ sia φ_σ l'unico automorfismo di $\mathbb{R}^n$ tale che $\varphi_\sigma(e_i) = e_{\sigma(i)}$ per ogni $i = 1, \dots, n$, dove $\{e_1, \dots, e_n\}$ è la base canonica di $\mathbb{R}^n$. Verificare che $\det \varphi_\sigma = \mathrm{sgn}(\sigma)$ per ogni $\sigma \in \mathfrak{S}_n$.

6.6. Calcolare i determinanti delle seguenti matrici $n \times n$

$$\begin{pmatrix} 1-n & 1 & 1 & \cdots & 1 \\ 1 & 1-n & 1 & \cdots & 1 \\ 1 & 1 & 1-n & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 1-n \end{pmatrix}, \quad \begin{pmatrix} 1 & n & n & \cdots & n \\ n & 2 & n & \cdots & n \\ n & n & 3 & \cdots & n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n & n & n & \cdots & n \end{pmatrix}$$

al variare di n.

6.7. Si scriva il triangolo di Tartaglia fino all'ordine n come matrice quadrata triangolare inferiore. È vero che per ogni n essa ha determinante 1? Calcolarne la matrice inversa.

6.8. Mostrare che $\det \begin{pmatrix} 1 & a & b+c \\ 1 & b & a+c \\ 1 & c & a+b \end{pmatrix} = 0$.

6.9. Mostrare che $\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1+x & 1 \\ 1 & 1 & 1+y \end{pmatrix} = xy$, e generalizzare.

6.10. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} x & a_1 & a_2 & \cdots & a_{n-1} & 1 \\ a_1 & x & a_2 & \cdots & a_{n-1} & 1 \\ a_1 & a_2 & x & \cdots & a_{n-1} & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 & a_2 & a_3 & \cdots & x & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n & 1 \end{pmatrix}, \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n \\ -x & x & 0 & \cdots & 0 & 0 \\ 0 & -x & x & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & x & 0 \\ 0 & 0 & 0 & \cdots & -x & x \end{pmatrix}, \begin{pmatrix} -x & 0 & 0 & \cdots & 0 & a_0 \\ 1 & -x & 0 & \cdots & 0 & a_1 \\ 0 & 1 & -x & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & -x & a_{n-1} \\ 0 & 0 & 0 & \cdots & 1 & -x+a_n \end{pmatrix}$$

al variare di n.

6.11. Calcolare i determinanti delle matrici $n \times n$ $\begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ddots & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}$ al variare di n.

6.12. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & 0 & b \\ 0 & c & 0 \\ d & 0 & f \end{pmatrix}, \begin{pmatrix} a & 0 & 0 & b \\ 0 & c & d & 0 \\ 0 & e & f & 0 \\ g & 0 & 0 & h \end{pmatrix}, \begin{pmatrix} a & 0 & 0 & 0 & b \\ 0 & c & 0 & d & 0 \\ 0 & 0 & e & 0 & 0 \\ 0 & f & 0 & g & 0 \\ h & 0 & 0 & 0 & i \end{pmatrix}.$$

6.13. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & 1 & 0 \\ 1 & b & 1 \\ 0 & 1 & c \end{pmatrix}, \begin{pmatrix} a & 1 & 0 & 0 \\ 1 & b & 1 & 0 \\ 0 & 1 & c & 1 \\ 0 & 0 & 1 & d \end{pmatrix}, \begin{pmatrix} a & 1 & 0 & 0 & 0 \\ 1 & b & 1 & 0 & 0 \\ 0 & 1 & c & 1 & 0 \\ 0 & 0 & 1 & d & 1 \\ 0 & 0 & 0 & 1 & e \end{pmatrix}.$$

6.14. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} 1 & a & 0 \\ b & 1 & b \\ 0 & a & 1 \end{pmatrix}, \begin{pmatrix} 1 & a & 0 & 0 \\ c & 1 & b & 0 \\ 0 & b & 1 & c \\ 0 & 0 & a & 1 \end{pmatrix}, \begin{pmatrix} 1 & a & 0 & 0 & 0 \\ d & 1 & b & 0 & 0 \\ 0 & c & 1 & c & 0 \\ 0 & 0 & b & 1 & d \\ 0 & 0 & 0 & a & 1 \end{pmatrix}.$$

6.15. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^n & b^n & c^n \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ a^m & b^m & c^m \\ a^n & b^n & c^n \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^m & b^m & c^m & d^m \\ a^n & b^n & c^n & d^n \end{pmatrix}.$$

6.16. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 0 & a \\ 0 & 0 & b & 0 \\ 0 & c & 0 & 0 \\ d & 0 & 0 & 0 \end{pmatrix}.$$

e in generale calcolare il determinante di matrici che hanno entrate non nulle solo sulla antidiagonale principale (cioè nelle posizioni $(i, n+1-i)$ se n è l'ordine della matrice).

6.17. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & a & b \\ c & 0 & d \\ e & f & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & a & b & c \\ d & 0 & e & f \\ g & h & 0 & i \\ l & m & n & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & a & b & c \\ 1 & 0 & d & e \\ 1 & 1 & 0 & f \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

6.18. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & b \\ c & a \end{pmatrix}, \qquad \begin{pmatrix} a & b & c \\ d & e & b \\ f & d & a \end{pmatrix}, \qquad \begin{pmatrix} a & b & c & d \\ e & f & g & c \\ h & i & f & b \\ l & h & e & a \end{pmatrix}.$$

6.19. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \qquad \begin{pmatrix} a & b & 0 \\ c & 0 & -b \\ 0 & -c & -a \end{pmatrix}, \qquad \begin{pmatrix} a & b & c & 0 \\ d & e & 0 & -c \\ f & 0 & -e & -b \\ 0 & -f & -d & -a \end{pmatrix}.$$

e in generale discutere il determinante di matrici che sono "antisimmetriche" rispetto alla antidiagonale (cioè tali che $a_{i,j} = -a_{n+1-j,n+1-i}$ se n è l'ordine della matrice).

6.20. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}.$$

6.21. Sia $A \in M_n(\Bbbk)$ una matrice tale che $A^{\mathrm{t}}A = \mathbb{I}_n$; dimostrare che $\det A = \pm 1$. È vero il viceversa?

Sia $A \in M_n(\Bbbk)$ una matrice tale che $A^{\mathrm{t}}PA = P$ con $P \in \mathrm{GL}_n(\Bbbk)$; dimostrare che $\det A = \pm 1$.

6.22. Siano $A, B \in M_n(\Bbbk)$; mostrare che AB è invertibile se e solo se A e B sono invertibili. Generalizzare ad un numero finito di matrici.

Interpretare e ridimostrare il risultato in termini di applicazioni lineari.

6.23. Supponiamo $A \in M_n(\Bbbk)$ matrice invertibile. Mostrare che $A + A^{-1}$ è invertibile se e solo se $\mathbb{I}_n + A^2$ è invertibile. È sempre vero che $A + A^{-1}$ è invertibile?

6.24. Usando la formula di Vandermonde, calcolare il determinante

$$\det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & x & x^2 & \cdots & x^k \\ 1 & x^2 & x^4 & \cdots & x^{2k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x^k & x^{2k} & \cdots & x^{k^2} \end{pmatrix}$$

e dire quando la matrice è degenere. Provare a calcolare l'inversa di questa matrice, se essa è invertibile.

6.25. Calcolare il determinante

$$\det \begin{pmatrix} 1 & \binom{x_1}{1} & \binom{x_1}{2} & \cdots & \binom{x_1}{n-1} \\ 1 & \binom{x_2}{1} & \binom{x_2}{2} & \cdots & \binom{x_2}{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \binom{x_n}{1} & \binom{x_n}{2} & \cdots & \binom{x_n}{n-1} \end{pmatrix}$$

(le entrate della matrice sono i "coefficienti binomiali" $\binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!}$, che sono polinomi in x).

6.26. Calcolare il determinante

$$\det\begin{pmatrix} 1 & f_1(x_1) & f_2(x_1) & \cdots & f_{n-1}(x_1) \\ 1 & f_1(x_2) & f_2(x_2) & \cdots & f_{n-1}(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & f_1(x_n) & f_2(x_n) & \cdots & f_{n-1}(x_n) \end{pmatrix}$$

ove $f_i(x)$ sono polinomi nella variabile x.

6.27. Dimostrare che ogni matrice di rango r si può scrivere come somma di r matrici di rango 1; viceversa, è vero che la somma di r matrici di rango 1 dà una matrice di rango r?

6.28. Principio dei minori orlati. Sia $A \in M_n(\Bbbk)$ una matrice avente un minore non nullo di ordine k, e sia $B \in M_k(\Bbbk)$ la sottomatrice di A che dà quel minore. Dimostrare che se tutti i minori di ordine $k+1$ ottenuti da sottomatrici di A contenenti B sono nulli, allora la matrice A ha rango esattamente k (principio dei minori orlati).

6.29. Principio dei minori orlati ed equazioni di sottospazi. Mostrare che il sottospazio W di $V_n(\Bbbk)$ generato dai vettori linearmente indipendenti $v_1, v_2, \ldots, v_m$ ha equazioni cartesiane ottenute annullando i minori d'orine $m+1$ della matrice

$$A = \begin{pmatrix} X_1 & & & \\ \vdots & v_1 & \cdots & v_m \\ X_n & & & \end{pmatrix}$$

in $M_{n,m+1}(\Bbbk[X_1, \ldots, X_n])$. Si mostri inoltre che, detta B la matrice in $M_{n,m}(\Bbbk)$ le cui colonne siano i vettori dati e scelto un minore non nullo d'ordine m di B, per descrivere W è sufficiente (e necessario) annullare i minori d'ordine $m+1$ di A che contengono la sottomatrice di B relativa al minore scelto (principio dei minori orlati).

Usando il principio di cui sopra, si diano equazioni cartesiane per i seguenti sottospazi di $V_3(\Bbbk)$ o $V_4(\Bbbk)$:

$$\langle\begin{pmatrix}1\\2\\1\end{pmatrix}\rangle,\ \langle\begin{pmatrix}1\\2\\1\end{pmatrix},\begin{pmatrix}1\\-1\\1\end{pmatrix}\rangle, \langle\begin{pmatrix}1\\2\\3\end{pmatrix},\begin{pmatrix}3\\2\\1\end{pmatrix}\rangle, \langle\begin{pmatrix}1\\0\\1\\2\end{pmatrix}\rangle,\ \langle\begin{pmatrix}1\\0\\1\\2\end{pmatrix},\begin{pmatrix}1\\-1\\1\\2\end{pmatrix}\rangle, \langle\begin{pmatrix}1\\0\\1\\2\end{pmatrix},\begin{pmatrix}1\\-1\\1\\2\end{pmatrix},\begin{pmatrix}1\\-1\\0\\0\end{pmatrix}\rangle\ .$$

6.30. Sviluppando il prodotto di determinanti

$$\det\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \det\begin{pmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix}$$

discutere dell'identità dei quattro quadrati di Eulero (il prodotto di due somme di quattro quadrati è una somma di quattro quadrati; per la somma di uno o di due quadrati è facile).

6.31. Discutere il rango delle matrici in funzioni dei parametri:

$$\begin{pmatrix} 1 & 1 & x-y & 1+x \\ 1 & 2+x & 1+x & 1+x \\ 1 & x+1 & y & 1 \\ -1 & -1 & x-y & x-1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 3 & 1 & xy-y \\ 2 & 2 & xy-x & x+2 \\ 2 & 4 & 1 & xy-y+1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & x^2-x \\ 1 & 1 & 1 & 1 \\ 1 & xy-x & xy-x+1 & x \\ -1+x-x^2 & x-x^2 & -1+x-x^2 & 0 \end{pmatrix}.$$

6.32. Calcolare i determinanti delle seguenti matrici:

$$\begin{pmatrix} 1 & 1 & 3 & 4 \\ 2 & 0 & 0 & 8 \\ 3 & 0 & 0 & 2 \\ 4 & 4 & 7 & 5 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & a & b & c & d \\ 0 & a^2 & b^2 & c^2 & d^2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 3 \\ 6 & 5 & 7 & 8 & 4 & 2 \\ 9 & 8 & 6 & 7 & 0 & 0 \\ 3 & 2 & 4 & 5 & 0 & 0 \\ 3 & 4 & 0 & 0 & 0 & 0 \\ 5 & 6 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

6.33. Calcolare i determinanti delle matrici:

$$\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{pmatrix},$$

e generalizzare.

6.34. Calcolare i determinanti delle matrici:

$$\begin{pmatrix} 1 & 4 \\ 4 & 9 \end{pmatrix}, \quad \begin{pmatrix} 1 & 4 & 9 \\ 4 & 9 & 16 \\ 9 & 16 & 25 \end{pmatrix}, \quad \begin{pmatrix} 1 & 4 & 9 & 16 \\ 4 & 9 & 16 & 25 \\ 9 & 16 & 25 & 36 \\ 16 & 25 & 36 & 49 \end{pmatrix}.$$

6.35. Si considerino le matrici di ordine n date da:

$$A_n = \begin{pmatrix} 1 & x & 0 & 0 & \cdots & 0 \\ y & 1 & x & 0 & \cdots & 0 \\ 0 & y & 1 & x & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 & x \\ 0 & 0 & 0 & \cdots & y & 1 \end{pmatrix}$$

(1 sulla diagonale principale, x subito sopra, y subito sotto, altrove zero), e sia $a_n = \det(A_n)$.
(a) Calcolare i determinanti a_2 e a_3.
(b) Calcolare i determinanti a_4 e a_5.
(c) Determinare una formula ricorsiva che esprima a_n in termini di a_{n-1} e a_{n-2}.
(d) Determinare l'espressione di a_n in quanto polinomio nelle variabili x, y specificando (con formule chiuse, cioè non ricorsive) i coefficienti di tale polinomio.

6.36. Sia A_n matrice diagonale con termini $a_{i,i} = a_i$ in diagonale, e sia B_n matrice antidiagonale con termini $b_{i,n-i+1} = b_i$. Poniamo $C_n = A_n + B_n$ (matrice santandrea).
(a) Calcolare i determinanti di C_n per $n = 2, 3, 4$.
(b) Dare e dimostrare una formula per il determinante di C_n per ogni n.
(c) Esistono basi di $\Bbbk^n$ in cui la matrice dell'applicazione lineare rappresentata da C_n in base canonica risulti a blocchi diagonali (e di che tipo)?

6.37. Sia A_n la matrice quadrata di ordine $2n$ costituita dai seguenti blocchi: $A_n = \begin{pmatrix} a\mathbb{I}_n & b\mathbb{I}_n \\ c\mathbb{I}_n & d\mathbb{I}_n \end{pmatrix}$ con $a, b, c, d \in \Bbbk$.
(a) Calcolare i determinanti di A_n per $n = 1, 2, 3$.
(b) Dare e dimostrare una formula per il determinante di A_n per ogni n.
(c) Esistono basi di $\Bbbk^{2n}$ in cui la matrice dell'applicazione lineare rappresentata da A_n in base canonica risulti a blocchi diagonali (e di che tipo)?

6.38. Consideriamo le seguenti matrici quadrate di ordine n: A_n la matrice avente i termini $a_1, \dots, a_n$ nella prima colonna e zero altrove; B_n la matrice avente i termini $b_1, \dots, b_n$ nella diagonale e zero altrove; C_n la matrice avente i termini $c_1, \dots, c_n$ nell'ultima colonna e zero altrove; infine $N_n = A_n + B_n + C_n$ ("matrice a N", o napoleonica)
(a) Calcolare i determinanti di N_n per $n = 2, 3, 4$.
(b) Dare e dimostrare una formula per il determinante di N_n per ogni n.
(c) Nei casi in cui N_n sia invertibile, determinare la matrice inversa.

6.39. Siano $V = \Bbbk^n$ e $v_1, \dots, v_{n-1} \in V$; consideriamo l'applicazione $h : V \to \Bbbk$ definita da $h(v) = \det(v_1 \cdots v_{n-1}\ v)$. È lineare?
(1) determinare matrice nelle basi canoniche, nucleo e immagine di h.
(2) determinare nucleo e immagine di $h^* : \Bbbk^* \to V^*$.

6.40. Discutere i sistemi lineari di matrici complete:

$$\begin{pmatrix} 1 & b & 1 & 1 \\ 1 & ab & 1 & b \\ 1 & b & a & 1 \end{pmatrix}, \quad \begin{pmatrix} a & b & 2 & 1 \\ a & 2b-1 & 3 & 1 \\ a & b & b+3 & 2b-1 \end{pmatrix}, \quad \begin{pmatrix} 2a+2 & 3 & a & a+4 \\ 4a-1 & a+1 & 2a-1 & 2a+2 \\ 5a-4 & a+1 & 3a-4 & a-1 \end{pmatrix}.$$

6.41. Quante somme e prodotti è necessario fare in linea di principio per calcolare un determinante d'ordine n (tramite la formula delle permutazioni)? E tramite le formule di Laplace? E tramite riduzione di Gauss?

6.42. Scrivere il determinante della matrice $A + B$, ove A e B sono matrici d'ordine n e B ha rango 1, come la somma di $n + 1$ determinanti di matrici d'ordine n.

6.43. Si consideri l'applicazione φ di $M_3(\mathbb{R})$ in sè che manda la generica matrice $\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$ nella matrice $\begin{pmatrix} a_1b_2 - a_2b_1 & a_1c_2 - a_2c_1 & b_1c_2 - b_2c_1 \\ a_1b_3 - a_3b_1 & a_1c_3 - a_3c_1 & b_1c_3 - b_3c_1 \\ a_2b_3 - a_3b_2 & a_2c_3 - a_3c_2 & b_2c_3 - b_3c_2 \end{pmatrix}$.

Verificare che $\varphi(\mathbb{I}_3) = \mathbb{I}_3$, $\varphi(\alpha A) = \alpha^2\varphi(A)$ e che $\varphi(AB) = \varphi(A)\varphi(B)$.

Dimostrare che:

(a) $\mathrm{rk}\varphi(A) = 0$ se e solo se $\mathrm{rk}(A) \leqslant 1$;

(b) $\mathrm{rk}\varphi(A) = 1$ se e solo se $\mathrm{rk}(A) = 2$;

(c) $\mathrm{rk}\varphi(A) = 3$ se e solo se $\mathrm{rk}(A) = 3$.

Capitolo V

Forme canoniche

Come ormai dovrebbe essere chiaro al lettore, noi intendiamo occuparci di proprietà intrinseche degli spazi vettoriali e delle applicazioni lineari, mentre per svolgere dei calcoli espliciti abbiamo bisogno di fare alcune scelte arbitrarie (generalmente scelte di basi per gli spazi vettoriali e tradurre i problemi in forma matriciale). D'altra parte, siccome queste scelte sono arbitrarie, conviene farle in modo che il problema in questione ottenga una forma matriciale semplice. Per esempio se si vuole studiare una applicazione lineare, converrebbe scegliere una base in cui la matrice associata sia il più semplice possibile, per esempio triangolare o diagonale. In questo capitolo ci occuperemo in modo sistematico di questo tipo di problemi.

In tutto questo capitolo $\Bbbk$ sarà un corpo commutativo arbitrario, a meno che non sia specificato altrimenti.

1. Equivalenza di matrici.

1.1. Definizione (equivalenza di matrici.). *Due matrici $A, B \in M_{m,n}(\Bbbk)$ si dicono equivalenti (in $\Bbbk$) se esistono due matrici invertibili $P \in \mathrm{GL}(n, \Bbbk)$ e $Q \in \mathrm{GL}(m, \Bbbk)$ tali che $B = QAP$. Due matrici sono equivalenti se e solo se rappresentano la stessa applicazione lineare di $V_n(\Bbbk)$ in $V_m(\Bbbk)$ con la scelta di diverse basi nei due spazi (legate dai cambiamenti di base dati da P su $V_n(\Bbbk)$ e Q su $V_m(\Bbbk)$).*

La relazione di equivalenza è una relazione di equivalenza tra matrici, come si verifica subito (sic).

1.1.1. Una matrice nulla è equivalente solo a se stessa. Una matrice di rango r può essere equivalente solo a matrici dello stesso rango. Una matrice identica di ordine n è equivalente a qualsiasi matrice invertibile dello stesso ordine (cioè: se una matrice quadrata è invertibile, allora è equivalente alla matrice identica del suo ordine).

1.2. Problema. Fare una classificazione per equivalenza delle matrici significa identificare le classi di equivalenza delle matrici secondo la relazione di equivalenza, e possibilmente per ogni classe identificare un rappresentante (il più semplice possibile).

Dal punto di vista delle applicazioni lineari di $V_n(\Bbbk)$ in $V_m(\Bbbk)$, si tratta di rappresentare un morfismo tramite una matrice semplice, scegliendo opportunamente le basi dei due spazi.

1.3. Teorema (il rango classifica le matrici per equivalenza). *Due matrici a coefficienti in un corpo sono equivalenti se e solo se hanno lo stesso rango r, e in tal caso sono equivalenti alla matrice le cui entrate sono tutte nulle, tranne le entrate nelle posizioni $(1,1), (2,2), \dots, (r,r)$ tutte uguali ad 1, ovvero la matrice a blocchi*

$$\begin{pmatrix} \mathbb{I}_r & \mathbb{O}_{r,n-r} \\ \mathbb{O}_{m-r,r} & \mathbb{O}_{m-r,n-r} \end{pmatrix}$$

(detta rappresentante canonico di quella classe di equivalenza).

Dimostrazione. Si possono pensare due dimostrazioni del risultato.

La prima consiste nell'usare la tecnica di riduzione di Gauss, operando prima sulle righe e successivamente sulle colonne della matrice (oppure in ordine inverso), ed è chiaro che la matrice può essere ridotta come affermato; inoltre un opportuno prodotto di matrici elementari dà le matrici P e Q invertibili che rendono la matrice equivalente alla forma canonica.

La seconda consiste nella scelta opportuna di basi in $V_n(\Bbbk)$ e $V_m(\Bbbk)$ adattate al morfismo $\varphi : V_n(\Bbbk) \to V_m(\Bbbk)$ rappresentato, nelle basi canoniche, dalla matrice data. Dapprima si sceglie una base di $\ker \varphi$ e la si estende ad una base di $V_n(\Bbbk)$; poi come base su $V_m(\Bbbk)$ si sceglie quella formata dalle

immagini dei vettori scelti come base in $V_n(\Bbbk)$ che non appartenevano a $\ker\varphi$, eventualmente completandola arbitrariamente. Allora è chiaro che la matrice di φ in queste nuove basi (opportunamente ordinate) diventa quella canonica detta. □

1.3.1. Si possono definire anche le relazioni di equivalenza destra (moltiplicando a destra per matrici invertibili) e di equivalenza sinistra (moltiplicando a sinistra per matrici invertibili), e sono relazioni diverse tra loro e diverse dalla equivalenza di matrici.

Mostrare che matrici dello stesso rango possono essere equivalenti senza essere equivalenti destre o equivalenti sinistre. Cercare dei teoremi di classificazione per le equivalenze destre e sinistre.

1.3.2. Problema di equivalenza simultanea. Sotto quali condizioni due matrici possono essere portate simultaneamente (cioè con le stesse trasformazioni) in forma pseudoidentica?

2. Similitudine di matrici.

Nel caso di matrici quadrate, interpretate in termini di applicazioni lineari da $V_n(\Bbbk)$ in sé stesso, siamo interessati ad usare la stessa base nel dominio e nel codominio; quindi diamo la seguente definizione.

2.1. Definizione (similitudine di matrici.). *Due matrici quadrate $A, B \in M_n(\Bbbk)$ si dicono simili (in $\Bbbk$) se esiste una matrice invertibile $P \in \mathrm{GL}(n, \Bbbk)$ tale che $B = P^{-1}AP$. Due matrici sono simili se e solo se rappresentano la stessa applicazione lineare di $V_n(\Bbbk)$ in sè in due basi diverse (legate dal cambiamento di base dato da P).*

La relazione di similitudine è una relazione di equivalenza tra matrici, come si verifica subito.

2.1.1. La matrice identica e la matrice nulla sono simili solamente a sé stesse. Quali sono le matrici che hanno questa proprietà (la loro classe di similitudine è ridotta ad un elemento)?

2.1.2. Due matrici diagonali non sono necessariamente simili tra di loro; caratterizzare i casi in cui lo sono, e farsi degli esempi.

2.1.3. Se due matrici sono simili, allora sono anche equivalenti, mentre il viceversa è falso (basta pensare alla matrice identica); dunque la relazione di similitudine è più fine (o meno grossolana) della relazione di equivalenza tra matrici. In particolare, ogni classe di equivalenza è unione disgiunta di classi di similitudine, e ogni classe di similitudine è contenuta in una classe di equivalenza.

2.1.4. La similitudine dipende dal corpo $\Bbbk$, nel senso che le classi di similitudine dipendono dal corpo $\Bbbk$, ma solo perché estendendo il corpo le classi di similitudine possono avere più elementi (e anche elementi più semplici), ma non capita mai che due matrici in $\Bbbk$ possano diventare simili in $\Bbbk' \supseteq \Bbbk$ senza che lo fossero già in $\Bbbk$. *Questo risultato è però di difficile dimostrazione, e non verrà qui né dimostrato, né utilizzato.*

Nel caso $\Bbbk = \mathbb{R}$ (e $\Bbbk' = \mathbb{C}$) si può per esempio ragionare così: se $A, B \in M_n(\mathbb{R})$ e $H \in \mathrm{GL}(n, \mathbb{C})$ è tale che $AH = HB$, allora scrivendo $H = U + iV$ con $U, V \in M_n(\mathbb{R})$ si ha $AU = UB$ e $AU = UB$ (ma U e V non sono necessariamente invertibili); quindi il sottospazio di $M_n(\mathbb{C})$ formato dalle matrici X tali che $AX = XB$ è non nullo, ammette una base di matrici reali, e la funzione determinante non vi è identicamente nulla, quindi esiste una matrice reale invertibile in tale spazio.

2.2. Problema. Fare una classificazione per similitudine delle matrici significa identificare le classi di equivalenza delle matrici secondo la relazione di similitudine, e possibilmente per ogni classe identificare un rappresentante (il più semplice possibile).

Dal punto di vista delle applicazioni lineari di $V_n(\Bbbk)$ in sè, si tratta di rappresentare un morfismo tramite una matrice semplice, scegliendo opportunamente una base dello spazio.

2.3. Definizione (diagonalizzabilità e triangolarizzabilità). *Una matrice $A \in M_n(\Bbbk)$ si dice diagonalizzabile (risp. triangolarizzabile) in $\Bbbk$ se è simile (in $\Bbbk$) ad una matrice diagonale (risp. triangolare), cioè se esistono $P \in \mathrm{GL}(n, \Bbbk)$ e $\Delta \in M_n(\Bbbk)$ diagonale tale che $A = P^{-1}\Delta P$ (risp. e $T \in M_n(\Bbbk)$ triangolare tale che $A = P^{-1}TP$).*

Una applicazione lineare φ di V in sè si dice diagonalizzabile (risp. triangolarizzabile) in $\Bbbk$ se esiste una base di V tale che la matrice di φ in quella base sia diagonale (risp. triangolare).

2.3.1. Motivazione per il seguito di questo capitolo: affinché una funzione o matrice sia triangolarizzabile o diagonalizzabile è necessario che vi siano vettori mandati in un multiplo di sè stessi. Quindi andremo ad esplorare l'esistenza di vettori di questo tipo (detti autovettori della funzione).

3. Autoteoria.

3.1. Definizione (autovalori e autovettori). *Sia $\varphi : V \to V$ un endomorfismo di uno spazio vettoriale V. Un vettore non nullo $v \in V$ si dice un autovettore di φ di autovalore $\lambda \in \Bbbk$ se $\varphi(v) = \lambda v$, e $\lambda \in \Bbbk$ si dice un autovalore di φ se esiste un vettore $v \in V$ non nullo tale che $\varphi(v) = \lambda v$.*

Sia $A \in M_n(\Bbbk)$ una matrice; autovalori e autovettori di A per definizione sono quelli della applicazione lineare di $V = V_n(\Bbbk)$ in sè a cui è associata la matrice A nella base canonica. Dunque $v \in V_n(\Bbbk)$ non nullo (che confonderemo con le sue coordinate in base canonica) si dice autovettore di A di autovalore $\lambda \in \Bbbk$ se $Av = \lambda v$, e $\lambda \in \Bbbk$ si dice un autovalore di A se esiste un vettore $v \in V_n(\Bbbk)$ non nullo tale che $Av = \lambda v$.

L'insieme degli autovalori di A (o di φ) si chiama spettro di A (o di φ).

Per un fissato autovalore λ, l'insieme di tutti gli autovettori di autovalore λ forma un sottospazio vettoriale di V, detto autospazio di λ e che si indica con $V_\lambda(A)$ (o $V_\lambda(\varphi)$).

3.1.1. Lo spettro di una matrice diagonale è formato dagli elementi che compaiono nella diagonale. I vettori della base canonica di $V_n(\Bbbk)$ sono autovettori per ogni matrice diagonale.

3.1.2. Gli autovettori di autovalore 0 sono gli elementi di $\ker\varphi$. Gli autovettori di autovalore 1 sono gli elementi mandati da φ in sé stessi; dunque l'autospazio di 1 è il più grande sottospazio di V in cui φ si restringe all'identità. Gli autovettori di autovalore -1?

3.1.3. Criterio banale di diagonalizzabilità. È un fatto evidente che una matrice è diagonalizzabile se e solo se $V_n(\Bbbk)$ ammette una base fatta di autovettori per la matrice. Equivalentemente, un endomorfismo di V è diagonalizzabile se e solo se V ammette una base di autovettori per quell'endomorfismo.

In tali casi, una matrice diagonale simile ad A (o associata a φ) ha in diagonale esattamente gli autovalori di A (di φ).

3.2. Proposizione (intersezione di autospazi). *Autospazi relativi ad autovalori distinti hanno intersezione nulla. In particolare autovettori relativi ad autovalori distinti sono linearmente indipendenti.*

Più in generale, autospazi relativi ad autovalori distinti sono in somma diretta (ogni autospazio ha intersezione nulla con la somma degli altri).

Dimostrazione. Sia $v \in V_\lambda(\varphi) \cap V_\mu(\varphi)$ con $\lambda \neq \mu$. Allora abbiamo $\lambda v = \varphi(v) = \mu v$ da cui $(\lambda - \mu)v = 0$, e poiché $\lambda - \mu \neq 0$ abbiamo $v = 0$. La seconda affermazione è allora chiara (per esempio dalla formula di Grassmann).

L'asserzione generale può essere dimostrata in un modo simile (per induzione: provare), ma vi sono alcune strategie più simpatiche. Una è questa: se $v_1, \dots, v_r$ sono autovettori di autovalori $\lambda_1, \dots, \lambda_r$ (diversi tra loro), e abbiamo $v_1 + \dots + v_r = 0$, allora applicando $\varphi, \varphi^2, \dots, \varphi^{r-1}$ alla relazione otteniamo $\lambda_1^i v_1 + \dots + \lambda_r^i v_r = 0$ per ogni $i = 0, 1, \dots, r-1$, cioè

$$\mathrm{VdM}(\lambda_1, \dots, \lambda_r) \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

da cui la conclusione $v_i = 0$ per ogni i (la matrice di Vandermonde è invertibile).

Un'altra è la seguente: se $v_1, \dots, v_r$ sono autovettori di autovalori $\lambda_1, \dots, \lambda_r$ (diversi tra loro), e abbiamo $v_1 + \dots + v_r = 0$, applichiamo (per ogni indice i) la composizione $\underset{j \neq i}{\circ}(\varphi - \lambda_j \mathrm{id})$ alla relazione, e otteniamo $\Pi_{j \neq i}(\lambda_i - \lambda_j)v_i = 0$, da cui $v_i = 0$ (per ogni i). □

3.3. Teorema (criterio per autovalori). *Uno scalare $\lambda \in \Bbbk$ è un autovalore di $A \in M_n(\Bbbk)$ (risp. di $\varphi \in \mathrm{End}(V)$) se e solo se $\det(A - \lambda \mathbb{I}_n) = 0$ (risp. $\ker(\varphi - \lambda \mathrm{id}_V) \neq 0$).*

Dimostrazione. Per definizione $\lambda \in \Bbbk$ è un autovalore di $A \in M_n(\Bbbk)$ se e solo se esiste $v \in V_n(\Bbbk)$ non nullo con $Av = \lambda v$, cioè $(A - \lambda \mathbb{I}_n)v = 0$ e questo significa che il sistema omogeneo di

matrice $A - \lambda \mathbb{I}_n$ ha una soluzione non nulla, e ciò equivale a che la matrice abbia determinante nullo. $\square$

3.4. Definizione-Teorema (polinomio caratteristico). *Il polinomio caratteristico di* $A \in M_n(\Bbbk)$ *è*

$$p_A(X) := \det(X\mathbb{I}_n - A) = (-1)^n \det(A - X\mathbb{I}_n) \ .$$

Si tratta di un polinomio monico di grado n*, è invariante per similitudine, e dunque si può chiamare anche polinomio caratteristico* $p_\varphi(X)$ *di* φ*. Uno scalare* $\lambda \in \Bbbk$ *è un autovalore di* A *(o di* φ*) se e solo se è zero del polinomio* $p_A(X)$*.*

Si dice che A *(o* φ*) ha tutti i suoi autovalori in* $\Bbbk$ *se il polinomio caratteristico* $p_A(X)$ *si fattorizza in fattori lineari in* $\Bbbk[X]$*.*

Dimostrazione. Mostriamo l'invarianza per similitudine: se $B = P^{-1}AP$ allora

$$\begin{aligned} p_B(X) &= \det(X\mathbb{I}_n - B) \\ &= \det(X\mathbb{I}_n - P^{-1}AP) \\ &= \det(P^{-1}(X\mathbb{I}_n - A)P) \\ &= \det(P)^{-1}\det(X\mathbb{I}_n - A)\det(P) \\ &= p_A(X) \ . \end{aligned}$$

L'altra affermazione è chiara in base al criterio precedente. $\square$

3.4.1. In particolare, tutti i coefficienti del polinomio caratteristico di una matrice sono invarianti per similitudine; il primo e l'ultimo sono particolarmente importanti:

$$p_A(X) = X^n - \operatorname{tr}(A)X^{n-1} + \cdots + (-1)^n \det(A)$$

ove $\operatorname{tr}(A)$ per definizione è la somma dei termini nella diagonale principale di A.

3.4.2. Gli altri coefficienti, con segno alternato, sono le somme dei minori diagonali dell'ordine corrispondente al complementare del grado dell'indeterminata; per esempio;

($n = 2$) $p_A(X) = X^2 - \operatorname{tr}(A)X + \det(A)$;

($n = 3$) $p_A(X) = X^3 - \operatorname{tr}(A)X^2 + d_2(A)X - \det(A)$, ove $d_2(A)$ è la somma dei minori diagonali d'ordine 2;

($n = 4$) $p_A(X) = X^4 - \operatorname{tr}(A)X^3 + d_2(A)X^2 - d_3(A)X + \det(A)$, ove $d_2(A)$ è la somma dei minori diagonali d'ordine 2, $d_3(A)$ è la somma dei minori diagonali d'ordine 3.

3.4.3. Conseguenza fondamentale del teorema precedente è che lo spettro di ogni matrice (e di ogni automorfismo) è finito: si tratta degli zeri di un polinomio di grado n a coefficienti in $\Bbbk$, e dunque un insieme con al più n elementi.

3.4.4. Gli autovalori di una matrice triangolare sono tutti e soli i suoi elementi diagonali. Dunque una matrice triangolare ha tutti i suoi autovalori in $\Bbbk$.

3.4.5. Traccia. Dal teorema sappiamo ancora che la traccia $\operatorname{tr}(A)$ di una matrice è un invariante per similitudine (dunque possiamo anche parlare di traccia di una applicazione lineare), e si tratta di una applicazione lineare $\operatorname{tr} : M_n(\Bbbk) \to \Bbbk$, cioè $\operatorname{tr}(A+B) = \operatorname{tr}(A) + \operatorname{tr}(B)$, e $\operatorname{tr}(\alpha A) = \alpha \operatorname{tr}(A)$. Chiaramente $\operatorname{tr}(\mathbb{O}) = 0$ e $\operatorname{tr}(A) = \operatorname{tr}(A^{\mathrm{t}})$.

In generale non è moltiplicativa, ovvero $\operatorname{tr}(AB) \neq \operatorname{tr}(A)\operatorname{tr}(B)$ (farsi degli esempi; traccia dell'inversa? e della matrice identica?).

Tuttavia vale che $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, quindi $\operatorname{tr}(ABC) = \operatorname{tr}(BCA) = \operatorname{tr}(CAB)$, ma in generale $\operatorname{tr}(ABC) \neq \operatorname{tr}(ACB)$. Cioè la traccia è invariante per permutazioni cicliche dei fattori, non per tutte le permutazioni.

Si osservi anche che l'applicazione $\tau : \operatorname{Hom}_\Bbbk(V, W) \times \operatorname{Hom}_\Bbbk(W, V) \longrightarrow \Bbbk$ definita da $\tau(f, g) = \operatorname{tr}(g \circ f) = \operatorname{tr}(f \circ g)$ è bilineare non degenere (dunque?).

3.4.6. Significati geometrici della traccia. Conosciamo già il significato geometrico del determinante come misura di un volume (nel caso reale), e quello algebrico come test di indipendenza; i significati algebrico/geometrici della traccia sono più difficili da vedere, e ne elenchiamo qualcuno:

(0) la traccia $\operatorname{End}_\Bbbk(V) \to \Bbbk$ è il morfismo che corrisponde alla dualità canonica tra V e V^* (per chi conosce già il calcolo tensoriale: $\operatorname{End}_\Bbbk(V) = V^* \otimes_\Bbbk V \to \Bbbk$ dalla mappa $\Bbbk$-bilineare di dualità $V^* \times V \to \Bbbk$);

(1) la traccia $\mathrm{End}_{\Bbbk}(V) \to \Bbbk$ è il morfismo duale del morfismo canonico $\Bbbk \to \mathrm{End}_{\Bbbk}(V)$ (identificando canonicamente $\Bbbk$ e $\mathrm{End}_{\Bbbk}(V)$ con i loro duali) che manda uno scalare nel prodotto per quello scalare;
(2) se φ ha rango 1, allora $\varphi^2 = \lambda\varphi$ e $\mathrm{tr}\,(\varphi) = \lambda$ (la traccia indica la dilatazione di una funzione di rango 1 sui vettori della sua immagine; siccome ogni endomorfismo è somma di endomorfismi di rango 1, e la traccia è lineare, questo basta per caratterizzarla);
(3) se $\varphi^2 = \varphi$ (proiezione) allora $\mathrm{tr}\,(\varphi) = \dim_{\Bbbk} \mathrm{im}\,(\varphi)$ (se $\Bbbk$ è di caratteristica nulla, altrimenti non ha senso l'uguaglianza);
(4) siccome $\det(1+t\varphi) = 1+\mathrm{tr}\,(\varphi)t+o(t^2)$, la traccia dice come cambia il volume di un endomorfismo "vicino all'identità" (quando ha senso parlare di piccoli valori di t), e questo è legato alla formula della traccia come somma degli autovalori di φ.
(5) la traccia è l'unica forma lineare che si annulla sui commutatori?

3.4.7. Problema. Possono esistere due matrici quadrate A, B tali che $AB - BA = \mathbb{I}$? È vero che $AB - BA = A$ implica $\det A = 0$?

3.5. Teorema (criterio di triangolarizzabilità). *Una matrice $A \in M_n(\Bbbk)$ è simile (in $\Bbbk$) a una matrice in forma triangolare se e solo se ha tutti i suoi autovalori in $\Bbbk$.*

Un endomorfismo è triangolarizzabile se e solo se ha tutti i suoi autovalori in $\Bbbk$.

Dimostrazione. Il "solo se" è già stato osservato prima. Resta da dimostrare il "se"; supponiamo dunque che A abbia tutti i suoi autovalori in $\Bbbk$ e procediamo per induzione su n.

Se $n = 1$ tutte le matrici sono triangolari (e anzi diagonali), e non c'è nulla da dimostrare. Supponiamo allora $n > 1$, e il teorema vero per matrici di ordine $n-1$. Sia λ un autovalore, e $v \in V_n(\Bbbk)$ un autovettore relativo a λ. Scelta una base di $V_n(\Bbbk)$ il cui primo vettore è v, abbiamo che, posto P la matrice invertibile di cambiamento di base dalla base canonica alla nuove, risulta

$$P^{-1}AP = \begin{pmatrix} \lambda & b \\ 0 & B \end{pmatrix}$$

ove $B \in M_{n-1}(\Bbbk)$. Per l'invarianza del polinomio caratteristico abbiamo $p_A(X) = (X - \lambda)p_B(X)$, e dunque la matrice B ha tutti i suoi autovalori nel corpo $\Bbbk$ (sono esattamente quelli di A, tranne una occorrenza di λ). Dunque per ipotesi induttiva, esiste $Q \in \mathrm{GL}_{n-1}(\Bbbk)$ tale che $Q^{-1}BQ = T$ è matrice triangolare superiore. Di conseguenza abbiamo:

$$\begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix}^{-1} P^{-1}AP \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & Q^{-1} \end{pmatrix} \begin{pmatrix} \lambda & b \\ 0 & B \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} = \begin{pmatrix} \lambda & b' \\ 0 & T \end{pmatrix}$$

e il risultato è una matrice triangolare superiore. □

3.5.1. Si provi a riscrivere la dimostrazione in termini di applicazioni lineari, invece che di matrici, dimostrando per induzione l'esistenza di una base triangolarizzante. È utile osservare che se $\varphi : V \to V$ è endomorfismo, e $W \leqslant V$ tale che $\varphi(W) \subseteq W$, allora φ definisce la funzione ristretta $\varphi_{|W} : W \to W$ e la funzione quoziente $\varphi_{/W} : V/W \to V/W$, e risulta che il polinomio caratteristico di φ è il prodotto dei polinomi caratteristici di restrizione e quoziente: $p_\varphi(X) = p_{\varphi_{|W}}(X)p_{\varphi_{/W}}(X)$.

3.5.2. In particolare quindi, se $\Bbbk$ è un corpo algebricamente chiuso (ogni polinomio in $\Bbbk[X]$ ha tutte le sue radici nel corpo) allora ogni matrice in $M_n(\Bbbk)$ è triangolarizzabile in $\Bbbk$. D'altra parte, se il corpo non è algebricamente chiuso esistono matrici che non sono triangolarizzabili su quel corpo (ma lo sono in una chiusura algebrica): farsi qualche esempio usando come corpi $\mathbb{Q}$ (suggerimento: studiare la matrice $\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$) e $\mathbb{R}$ (suggerimento: studiare la matrice $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$).

3.6. Definizione-Teorema (molteplicità e nullità). *Ad ogni autovalore λ (di una matrice $A \in M_n(\Bbbk)$ o di una applicazione lineare $\varphi \in \mathrm{End}_{\Bbbk}(V)$) restano associati due numeri interi positivi $\mathrm{M}(\lambda)$ e $\mathrm{N}(\lambda)$ così definiti:*
(1) $\mathrm{M}(\lambda)$ *si dice la molteplicità (o molteplicità algebrica) di λ, ed è la molteplicità di λ in quanto radice del polinomio caratteristico.*
(2) $\mathrm{N}(\lambda)$ *si dice la nullità (o molteplicità geometrica) di λ, ed è la dimensione del sottospazio degli autovettori associati a λ; dunque $\mathrm{N}(\lambda) := \dim_{\Bbbk} \ker(\varphi - \lambda \mathrm{id}_V) = n - \mathrm{rk}(A - \lambda\mathbb{I}_n)$.*

In generale, per ogni autovalore λ si ha $\mathrm{M}(\lambda) \geqslant \mathrm{N}(\lambda) \geqslant 1$.

Dimostrazione. Sia $m = \mathrm{N}(\lambda)$; allora possiamo trovare un sistema di m autovettori per φ di autovalore λ linearmente indipendenti, diciamo $v_1, \dots, v_m$. Completando ad una base $v_1, \dots, v_n$ di V, vediamo che la matrice di φ in questa base si scrive a blocchi:

$$A' = \begin{pmatrix} \lambda \mathbb{I}_m & B \\ 0 & C \end{pmatrix}$$

e calcolando il polinomio caratteristico si ha

$$p_A(X) = \det(X\mathbb{I}_n - A') = \det(X\mathbb{I}_m - \lambda\mathbb{I}_m)\det(X\mathbb{I}_{n-m} - C) = (X-\lambda)^m \det(X\mathbb{I}_{n-m} - C)$$

da cui si vede che $\mathrm{M}(\lambda) \geqslant m$. □

3.7. Teorema (primo criterio di diagonalizzabilità). *Una matrice $A \in M_n(\Bbbk)$ (risp. un endomorfismo $\varphi \in \mathrm{End}_{\Bbbk}(V)$ di uno spazio vettoriale V di dimensione n su $\Bbbk$) è simile (in $\Bbbk$) a una matrice in forma diagonale (risp. è diagonalizzabile in $\Bbbk$) se e solo se ha tutti i suoi autovalori in $\Bbbk$ e ogni autovalore ha molteplicità e nullità uguali.*

Dimostrazione. Il "solo se" è chiaro: se una matrice è diagonalizzabile il polinomio caratteristico è uguale a quello di una matrice diagonale, e gli autovalori sono esattamente i termini nella diagonale. Inoltre, per ogni autovalore, l'autospazio corrispondente è generato dai vettori della base diagonalizzante corrispondenti alle occorrenze dell'autovalore nella diagonale, quindi in numero uguale alla nullità dell'autovalore.

Viceversa, si scelga su $V = V_n(\Bbbk)$ l'insieme costituito giustapponendo le basi degli autospazi relativi agli autovalori dati: per l'ipotesi fatta, si tratta di esattamente n elementi, ed è un insieme linearmente indipendente (si ricordi che autospazi relativi ad autovalori distinti sono in somma diretta), e dunque di una base. Sia P la matrice di cambiamento di base (dalla base di autovettori a quella iniziale); allora è chiaro che $P^{-1}AP$ è una matrice diagonale. □

3.7.1. In particolare quindi, anche se $\Bbbk$ è un corpo algebricamente chiuso non è detto che allora ogni matrice in $M_n(\Bbbk)$ sia diagonalizzabile in $\Bbbk$. Farsi degli esempi usando il corpo complesso $\mathbb{C}$ (si consideri per esempio la matrice $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$).

3.7.2. Si osservi che il prodotto e la somma di matrici diagonalizzabili non sono necessariamente diagonalizzabili: per esempio la matrice $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ è prodotto (e anche somma) di due matrici diagonalizzabili.

3.8. Problema: diagonalizzazione simultanea. Due matrici A e B sono simultaneamente diagonalizzabili (i.e. esiste $P \in \mathrm{GL}(n, \Bbbk)$ tale che $P^{-1}AP$ e $P^{-1}BP$ sono entrambe diagonali) se e solo se sono (separatamente) diagonalizzabili e commutano tra loro (i.e. $AB = BA$, nel qual caso ciascuna delle due matrici è stabile sugli autospazi dell'altra).

Generalizzare ad un numero finito di matrici.

3.9. Problema curioso. Consideriamo $\mathbf{A} \in M_n(M_m(\Bbbk))$; cioè $\mathbf{A}$ è una matrice d'ordine n le cui entrate sono matrici $A_{i,j} \in M_m(\Bbbk)$ d'ordine m, e supponiamo che tutte queste matrici commutino tra loro (a due a due): diciamo che $\mathbf{A}$ è una matrice a blocchi quadrati commutanti. Sia $A \in M_{mn}(\Bbbk)$ la matrice che si ottiene da $\mathbf{A}$ "dimenticando la divisione in blocchi". Allora vale che $\det(\det(\mathbf{A})) = \det(A)$ (a sinistra, si noti che $\det(\mathbf{A}) \in M_m(\Bbbk)$, cioè è una matrice). Dedurne che $\det(p_{\mathbf{A}}(X)) = p_A(X)$. *[per questo problema può essere necessario ridursi a forme canoniche tipo Jordan...]*

3.10. Problema: prodotto di matrici quadrate. Se almeno una tra due matrici A e B (quadrate dello stesso ordine) è invertibile, allora AB è simile a BA (dunque AB hanno BA gli stessi polinomi caratteristico e minimo). In generale (senza alcuna ipotesi) resta vero che AB e BA hanno gli stessi autovalori e stesso polinomio caratteristico: si può vederlo confrontando le due matrici a blocchi $\left(\begin{smallmatrix} AB & A \\ 0 & 0 \end{smallmatrix}\right)$ e $\left(\begin{smallmatrix} 0 & A \\ 0 & BA \end{smallmatrix}\right)$ che risultano simili via $\left(\begin{smallmatrix} \mathbb{I} & 0 \\ B & \mathbb{I} \end{smallmatrix}\right)$.

Gli autovalori di AB e BA hanno le stesse nullità? Si consideri l'esempio $A = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ e $B = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. Ma per gli autovalori non nulli? Per che cosa possono differire i polinomi minimi?

3.10.1. Problema: prodotto di matrici. Se $A, B \in M_{n,m}(\Bbbk)$ (non necessariamente quadrate), allora $A^{\mathrm{t}}B \in M_m(\Bbbk)$, $AB^{\mathrm{t}} \in M_n(\Bbbk)$ e abbiamo già visto che

$$X^n \det(\, X\mathbb{I}_m + A^{\mathrm{t}}B\,) = X^m \det(\, X\mathbb{I}_n + AB^{\mathrm{t}}\,)$$

da cui si deduce che $X^n p_{A^{\mathrm{t}}B}(X) = X^m p_{AB^{\mathrm{t}}}(X)$; lo stesso risultato si può ottenere osservando che le matrici a blocchi $\begin{pmatrix} AB^{\mathrm{t}} & A \\ 0 & 0 \end{pmatrix}$ e $\begin{pmatrix} 0 & A \\ 0 & B^{\mathrm{t}}A \end{pmatrix}$ risultano simili via $\begin{pmatrix} \mathbb{I} & 0 \\ B^{\mathrm{t}} & \mathbb{I} \end{pmatrix}$.

3.11. Problema. Siano A e B matrici quadrate dello stesso ordine n; consideriamo l'applicazione $\psi_{A,B} : M_n(\Bbbk) \to M_n(\Bbbk)$ data da $\psi_{A,B}(X) = AX - XB$. Si verifichi che si tratta di una applicazione lineare, i cui autovalori sono le differenze tra gli autovalori di A e quelli di B. Precisamente, se v è un autovettore di A relativo all'autovalore α e w è un autovettore di B^{t} relativo all'autovalore β, allora vw^{t} è automatrice di $\psi_{A,B}$ di autovalore $\alpha - \beta$. Viceversa, se N è automatrice di $\psi_{A,B}$ di autovalore γ, si consideri un autovettore v di B di autovalore β con $Nv \neq 0$, e si concluda che Nv è autovettore di A di autovalore $\beta + \gamma$. Se invece gli autospazi di B sono contenuti nel nucleo di N, si ripete il ragionamento trovando un vettore v non appartenente al nucleo di N e tale che $Bv = \beta v + w$ con $Nw = 0$ (vedi teoria di Jordan).

4. Teoria di Hamilton-Cayley e sottospazi stabili.

Per avere una comprensione più approfondita della classe di similitudine di una matrice, e di come scegliere un rappresentante semplice per quella classe, bisogna capire meglio la relazione tra polinomi e matrici, ovvero capire la sottoalgebra delle matrici generata da una fissata matrice. La teoria di Hamilton-Cayley fa vedere come alcune fattorizzazioni di polinomi che annullano la matrice diano luogo a una decomposizione dello spazio in sottospazi stabili per la trasformazione lineare, e quindi alla possibilità di scrivere matrici a blocchi simili a quella data.

4.1. Teorema (Hamilton-Cayley). *Consideriamo le applicazioni di $\Bbbk$-algebre*

$$v_A : \Bbbk[X] \longrightarrow M_n(\Bbbk) \quad \text{e} \quad v_\varphi : \Bbbk[X] \longrightarrow \mathrm{End}_{\Bbbk}(V)$$

("valutazione in A" e "valutazione in φ") definita mandando ogni polinomio $P(X)$ nella matrice $P(A)$ ottenuta sostituendo X con A e nell'endomorfismo $P(\varphi)$ ottenuta sostituendo X con φ.

Abbiamo allora $p_A(A) = 0$ e $p_\varphi(\varphi) = 0$, cioè $v_A(p_A(X)) = 0$ e $v_\varphi(p_\varphi(X)) = 0$. In altri termini, il polinomio caratteristico annulla la corrispondente matrice (o il corrispondente endomorfismo), ovvero il polinomio caratteristico appartiene al nucleo della mappa di valutazione della sua matrice (o del corrispondente endomorfismo).

Dimostrazione. Vi sono varie dimostrazioni possibili per questo risultato. Cominciamo da una *dimostrazione sbagliata*:

$$p_A(A) = \det(A\mathbb{I}_n - A) = \det(\mathbb{O}_n) = 0\ ;$$

dov'è lo sbaglio?

Dimostrazione usando la *triangolarizzabilità*. Si osservi che possiamo sostituire il corpo $\Bbbk$ con una sua estensione $\Bbbk'$ senza che siano alterati la matrice ed il polinomio caratteristico. Dunque possiamo supporre che $\Bbbk$ contenga tutte le radici di $p_A(X)$, e di conseguenza che A sia triangolarizzabile. Siano allora $p_A(X) = \prod_i (X - \alpha_i)$ il polinomio caratteristico di A, e P una matrice invertibile tale che $P^{-1}AP = T$ matrice triangolare superiore avente sulla diagonale ordinatamente gli elementi $\alpha_1, \dots, \alpha_n$. Definiamo $V_i = \langle e_1, \dots, e_i \rangle$ i sottospazi di $V = V_n(\Bbbk)$ generati dai primi i vettori della base canonica (dunque $V_0 = 0$ e $V_n = V$). Notiamo allora che si ha $(T - \alpha_i)V_i \subseteq V_{i-1}$ per ogni $i = 1, \dots, n$. Abbiamo allora

$$\begin{aligned} p_T(T)V &= (T - \alpha_1) \cdots (T - \alpha_{n-1})(T - \alpha_n)V_n \\ &\subseteq (T - \alpha_1) \cdots (T - \alpha_{n-1})V_{n-1} \\ &\subseteq \cdots \\ &\subseteq (T - \alpha_1) \cdots (T - \alpha_i)V_i \\ &\subseteq \cdots \\ &\subseteq (T - \alpha_1)V_1 = 0 \end{aligned}$$

da cui concludiamo che $p_T(T) = 0$. Di conseguenza $p_A(A) = p_A(PTP^{-1}) = Pp_T(T)P^{-1} = 0$, come si voleva.

Dimostrazione usando il *calcolo con matrici polinomiali.* Osserviamo prima che se $p_A(X) = \sum_i p_i X^i$ allora

$$\begin{aligned} p_A(X)\mathbb{I}_n - p_A(A) &= \sum_i p_i(X^i\mathbb{I}_n - A^i) \\ &= \sum_i p_i(X\mathbb{I}_n - A)(X^{i-1}\mathbb{I}_n + X^{i-2}A + \cdots + XA^{i-2} + A^{i-1}) \\ &= (X\mathbb{I}_n - A)\sum_i p_i(X^{i-1}\mathbb{I}_n + X^{i-2}A + \cdots + XA^{i-2} + A^{i-1}) \\ &= (X\mathbb{I}_n - A)Q(X) \end{aligned}$$

ove $Q(X)$ è un polinomio a coefficienti in $M_n(\Bbbk)$. Ora usando la matrice dei complementi algebrici di $(X\mathbb{I}_n - A)$ abbiamo

$$\begin{aligned} p_A(A) &= p_A(X)\mathbb{I}_n - (X\mathbb{I}_n - A)Q(X) \\ &= (X\mathbb{I}_n - A)(X\mathbb{I}_n - A)^{\mathrm{c}} - (X\mathbb{I}_n - A)Q(X) \\ &= (X\mathbb{I}_n - A)((X\mathbb{I}_n - A)^{\mathrm{c}} - Q(X)) \\ &= (X\mathbb{I}_n - A)R(X) \end{aligned}$$

ove $R(X)$ è un polinomio a coefficienti in $M_n(\Bbbk)$. Siccome sul lato sinistro abbiamo una matrice a coefficienti in $\Bbbk$, si deduce che $R(X) = 0$ (perché?), e dunque anche $p_A(A) = 0$. □

4.1.1. Una piccola applicazione del teorema di Hamilton-Cayley è la seguente: se la matrice A è invertibile, allora la matrice inversa si scrive polinomialmente in A, ovvero esiste un polinomio $F(X)$ tale che $A^{-1} = F(A)$. Perché?

In particolare, per matrici d'ordine 2 abbiamo $A^{-1} = \det(A)^{-1}(\operatorname{tr}(A) - A)$.

4.2. Consideriamo ora in generale l'applicazione di valutazione in A, cioè la funzione $v_A : \Bbbk[X] \longrightarrow M_n(\Bbbk)$ definita dalle proprietà di rispettare somma e prodotto e di mandare X in A; abbiamo già detto che è una applicazione di $\Bbbk$-algebre (cioè è $\Bbbk$-lineare e rispetta identità e prodotto). Si osservi per inciso che l'immagine dell'algebra dei polinomi tramite v_A dà luogo ad una sottoalgebra commutativa dell'algebra delle matrici, e quindi non può essere una funzione suriettiva. L'immagine si indica con $\Bbbk[A]$ (matrici polinomiali in A): come caratterizzarla?

4.2.1. Inoltre, che l'applicazione lineare v_A debba avere un nucleo non banale discende a priori da una pura considerazione sulle dimensioni: $\dim_{\Bbbk} \Bbbk[X] = \aleph_0 > n^2 = \dim_{\Bbbk} \operatorname{End}_{\Bbbk}(V)$: esplicitare l'argomento.

4.2.2. Anche se il dominio è di dimensione infinita (e il nucleo anche, in effetti, poiché il codominio ha dimensione finita), possiamo applicare il primo teorema di isomorfismo e dire che $\Bbbk[A]$ è isomorfa al quoziente $\Bbbk[X]/\ker(v_A)$, che è più facile da studiare; sapendo che $\Bbbk[X]$ è anello ad ideali principali, il nucleo $\ker(v_A)$ dev'essere generato da un unico polinomio monico.

4.3. Definizione (polinomio minimo). *Il polinomio minimo di A (o di φ) è il generatore monico dell'ideale* $\ker(v_A)$ *di $\Bbbk[X]$ formato dai polinomi che annullano A (o φ). Si indica con $m_A(X)$ (o $m_\varphi(X)$). Il teorema di Hamilton-Cayley dice allora che il polinomio minimo divide il polinomio caratteristico: $m_A(X)|p_A(X)$.*

4.3.1. Il polinomio minimo è quindi l'unico polinomio monico di grado minimo che annulla la matrice.

4.3.2. Si può subito dimostrare in effetti che polinomio caratteristico e polinomio minimo hanno le stesse radici in (una chiusura algebrica di) $\Bbbk$ (quasi subito: per l'implicazione non banale, per ogni autovalore si consideri un suo autovettore, e si mostri che non può essere annullato da alcun polinomio, calcolato nella matrice, che non abbia tra le radici proprio l'autovalore), e il teorema di Hamilton-Cayley dice che le molteplicità algebriche sono minori o uguali per il polinomio minimo rispetto a quello caratteristico.

4.3.3. È anche facile, una volta noto il polinomio minimo di A, discutere la struttura di $\Bbbk$-algebra di $\Bbbk[A]$: essa è infatti isomorfa alla struttura del quoziente $\Bbbk[X]/(m_A(X))$. Per esempio: vi

sono divisori di zero se e solo se il polinomio minimo non è irriducibile in $\Bbbk[X]$, vi sono elementi nilpotenti se e solo se il polinomio minimo contiene fattori ripetuti di $\Bbbk[X]$, $\Bbbk[A]$ è integra se e solo se $m_A(X)$ è irriducibile (e in tal caso è un corpo). Il secondo criterio di diagonalizzabilità permetterà di legare queste proporietà a proprietà della matrice A.

4.3.4. Esempi. Le matrici triangolari $\begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix}$ hanno polinomio caratteristico $(X-1)^3$ e polinomi minimi rispettivamente $X-1$, $(X-1)^2$, $(X-1)^3$.

Le matrici $\begin{pmatrix} 1 & 0 & 0 \\ & 1 & 0 \\ & & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 & 0 \\ & 1 & 1 \\ & & -1 \end{pmatrix}$, hanno polinomio caratteristico $(X-1)^2(X+1)$ e polinomi minimi rispettivamente $(X-1)(X+1)$, $(X-1)^2(X+1)$, $(X-1)^2(X+1)$.

4.4. Problema. Mostrare in almeno tre modi diversi che se $\varphi : V \to V$ è diagonalizzabile, e W è sottospazio stabile per φ (cioè $\varphi(W) \subseteq W$), allora $\psi = \varphi_{|W}$ è diagonalizzabile come endomorfismo di W. Un metodo chiaramente usa il polinomio minimo. Tuttavia conviene anche cercare di risolvere il problema ragionando sugli autospazi di φ, e come questi possono intersecare un sottospazio stabile per φ...

È molto più facile osservare che sotto la stessa ipotesi anche φ/W, endomorfismo di V/W, è diagonalizzabile. È vero o falso che se per un sottospazio stabile W abbiamo che $\varphi_{|W}$ e φ/W sono diagonalizzabili, anche φ è diagonalizzabile?

4.5. Definizione (sottospazi stabili). *Sia φ un endomorfismo di V, e sia W un sottospazio di V; W si dice stabile per φ o φ-stabile se $\varphi(W) \subseteq W$.*

4.6. Teorema (di decomposizione). *Sia φ un endomorfismo di V, e sia $F(X) \in \Bbbk[X]$ un polinomio tale che $F(\varphi) = 0$. Se $F = F_1 \cdots F_r$ con $F_1, \dots, F_r \in \Bbbk[X]$ non costanti a due a due coprimi, allora posto $V_{F_i} = \ker F_i(\varphi)$ per ogni i risulta*

$$V = V_{F_1} \oplus \cdots \oplus V_{F_r}$$

e ogni V_{F_i} è spazio φ-stabile (decomposizione dello spazio in sottospazi φ-stabili).

Dimostrazione. Per induzione su r; il caso importante da trattare è evidentemente $r = 2$, che permette facilmente anche il passo induttivo. Sia allora $F(X) = F_1(X)F_2(X)$, ed essendo $F_1(X)$ ed $F_2(X)$ polinomi in $\Bbbk[X]$ coprimi, troviamo polinomi $G_1(X)$ e $G_2(X)$ in $\Bbbk[X]$ tali che $F_1(X)G_1(X) + F_2(X)G_2(X) = 1$. Calcolando in φ si ottiene

$$F_1(\varphi)G_1(\varphi) + F_2(\varphi)G_2(\varphi) = \mathrm{id}_V = G_1(\varphi)F_1(\varphi) + G_2(\varphi)F_2(\varphi).$$

Dimostriamo allora che V_{F_1} e V_{F_2} hanno intersezione nulla: se $v \in V$ appartiene all'intersezione allora $v = \mathrm{id}_V(v) = G_1(\varphi)F_1(\varphi)(v) + G_2(\varphi)F_2(\varphi)(v) = 0 + 0 = 0$.

Mostriamo che $V = V_{F_1} + V_{F_2}$: ogni $v \in V$ si scrive come somma

$$v = \mathrm{id}_V(v) = F_1(\varphi)G_1(\varphi)(v) + F_2(\varphi)G_2(\varphi)(v)$$

e posto $v_1 = F_2(\varphi)G_2(\varphi)(v)$ e $v_2 = F_1(\varphi)G_1(\varphi)(v)$ vediamo subito (poiché $0 = F(\varphi) = F_1(\varphi)F_2(\varphi) = F_2(\varphi)F_1(\varphi)$) che $v_1 \in V_{F_1}$ e $v_2 \in V_{F_2}$. □

4.6.1. Si osservi che anche un ragionamento diretto, non induttivo, poteva dare lo stesso risultato. Lo si espliciti secondo queste linee: Sia $Q_i = \Pi_{j \neq i} F_j$; allora i Q_i sono un insieme coprimo ed esistono polinomi H_i tali che $\Sigma_i Q_i H_i = 1$. Applicando a φ e ad un vettore v troviamo che $v = \mathrm{id}_V(v) = \Sigma_i Q_i(\varphi)H_i(\varphi)v$ e ponendo $v_i = Q_i(\varphi)H_i(\varphi)v$ abbiamo che $v = \Sigma_i v_i$ e $v_i \in V_{F_i}$ ($F_i(\varphi)v_i = F_i(\varphi)Q_i(\varphi)H_i(\varphi)v = F(\varphi)H_i(\varphi)v = 0$). D'altra parte, come prima sappiamo che $V_{F_i} \cap V_{F_j} = 0$ se $i \neq j$.

4.6.2. Caso del polinomio caratteristico. Applicando in particolare il teorema al polinomio caratteristico otteniamo che se $p_\varphi(X) = \Pi_i p_i(X)$ è una sua fattorizzazione in fattori a due a due coprimi, allora V è la somma diretta dei sottospazi $V_{p_i} = \ker p_i(\varphi)$, ciascuno dei quali ha dimensione $\dim_\Bbbk V_{p_i} = \deg p_i(X)$ pari al grado (come polinomio in X) del fattore $p_i(X)$ (perché? si osservi che il polinomio caratteristico di φ ristretto a V_{p_i} non può contenere altri fattori che quelli di $p_i(X)$, essendone annullata, e d'altra parte il prodotto di tali polinomi caratteristici deve ricostruire il polinomio caratteristico di φ). In particolare, per ogni autovalore λ di molteplicità m si deduce che esso compare nel polinomio minimo con un esponente l che è il minimo intero positivo per cui $\dim_\Bbbk \ker(\varphi - \lambda \mathrm{id}_V)^l = m$ (al massimo è proprio m).

4.7. Teorema (secondo criterio di diagonalizzabilità). *Una matrice A è simile (in $\Bbbk$) a una matrice in forma diagonale se e solo se ha tutti i suoi autovalori in $\Bbbk$ e il polinomio minimo si fattorizza in $\Bbbk[X]$ con fattori lineari distinti (cioè non ha radici multiple). Un endomorfismo φ è diagonalizzabile su $\Bbbk$ se e solo se il suo polinomio minimo si fattorizza in $\Bbbk[X]$ con fattori lineari distinti.*

Dimostrazione. Il "solo se" è facile: se A è diagonalizzabile su $\Bbbk$, allora sappiamo già che ha tutti i suoi autovalori in $\Bbbk$, ed è chiaro (guardando per esempio alla matrice diagonalizzata, che nella diagonale principale ha esattamente gli autovalori distinti $\lambda_1, \dots, \lambda_r$, ripetuti ciascuno con la rispettiva molteplicità) che il prodotto $\prod_i (A - \lambda_i \mathbb{I}_n) = 0$, e dunque il polinomio minimo ha fattori al più lineari.

Viceversa, supponiamo che il polinomio minimo si fattorizzi con fattori lineari $m_A(X) = \prod_i (X - \lambda_i)$ con $\lambda_i \neq \lambda_j$ se $i \neq j$; per il teorema di decomposizione abbiamo che $V_n(\Bbbk) = \bigoplus_i V_{\lambda_i}(A)$, ove ricordiamo che $V_{\lambda_i}(A) = \ker(A - \lambda_i \mathbb{I}_n)$ sono gli autospazi di A, e dunque di dimensioni rispettive $N(\lambda_i)$. Dalla decomposizione abbiamo allora

$$\sum_i M(\lambda_i) = n = \dim_{\Bbbk} V_n(\Bbbk) = \sum_i \dim_{\Bbbk} V_{\lambda_i}(A) = \sum_i N(\lambda_i)$$

e poiché $M(\lambda_i) \geqslant N(\lambda_i)$ per ogni i, trattandosi di quantità positive, concludiamo che $M(\lambda_i) = N(\lambda_i)$ per ogni i, e dunque la matrice è diagonalizzabile per il primo criterio (si poteva usare anche il criterio banale di diagonalizzazione, una volta che lo spazio era decomposto in somma diretta dei vari autospazi). □

4.8. Decomposizione spettrale. Vi è una interessante descrizione-caratterizzazione geometrica dei morfismi diagonalizzabili in termini di proiezioni: *una matrice $A \in M_n(\Bbbk)$ è diagonalizzabile su $\Bbbk$ se e solo se essa si scrive come somma $A = \sum_i \lambda_i A_i$ dove i $\lambda_i \in \Bbbk$ sono gli autovalori (distinti) di A, e le A_i sono matrici di proiettori complementari, cioè $\sum_i A_i = \mathbb{I}$ e $A_i A_j = \delta_{i,j} A_i$.* Tali scritture si dicono decomposizioni spettrali. Usando gli interpolatori di Lagrange (dove si sono visti?) $f_i(X)$ relativi agli autovalori λ_i, si ha $A_i = f_i(A)$.

In termini di endomorfismi: *φ è diagonalizzabile se e solo se è combinazione lineare (secondo i suoi autovalori) delle proiezioni complementari sui propri autospazi nella direzione degli altri.*

♠ **4.9.** *Il seguito del paragrafo è dedicato ad uno studio preciso dei sottospazi stabili, e delle loro relazioni con i polinomi divisori del polinomio minimo; si tratta di argomenti che possono essere saltati in prima lettura, e anche nelle eventuali successive.*

4.9.1. Proposizione (polinomi e sottospazi stabili). *Sia $F = F(X) \in \Bbbk[X]$ un polinomio non costante; allora il sottospazio $V_F = \ker F(\varphi)$ è un sottospazio di V stabile per φ; inoltre se abbiamo due polinomi $F, F' \in \Bbbk[X]$ e $F | F'$ (F divide F') allora $V_F \subseteq V_{F'}$.*

Viceversa, se W è un sottospazio φ-stabile, possiamo associargli il polinomio minimo della restrizione di φ a W, sia m_W (che è un divisore del polinomio minimo di φ); se $W \subseteq W'$ allora $m_W | m_{W'}$ (m_W divide $m_{W'}$ in $\Bbbk[X]$).

Dimostrazione. Formale. □

4.9.2. Teorema (Struttura dei sottospazi stabili?). *Per ogni polinomio $F = F(X) \in \Bbbk[X]$ risulta che $m_{V_F} | F$ (il polinomio minimo di φ ristretto a $\ker F(\varphi)$ divide F) e per ogni sottospazio stabile W risulta che $V_{m_W} \supseteq W$ (W è contenuto nello spazio φ-stabile associato al polinomio minimo di φ ristretto a W).*
Ne segue che abbiamo una biiezione tra i seguenti due insiemi:
(1) *polinomi della forma m_W ove W è un sottospazio φ-stabile;*
(2) *sottospazi di V della forma V_F ove F è un polinomio non costante (che si può supporre un divisore monico del polinomio minimo di φ).*

Dimostrazione. La seconda parte segue formalmente dalle prime due osservazioni e dal seguente risultato generale:

Siano A e B due insiemi ordinati (significa per A che è data una relazione, scritta di solito $\leqslant$, che è riflessiva ($a \leqslant a$ per ogni $a \in A$), transitiva (se $a \leqslant a'$ e $a' \leqslant a''$ allora $a \leqslant a''$ per ogni $a, a', a'' \in A$)

e antisimmetrica (se $a \leqslant a'$ e $a' \leqslant a$ allora $a = a'$ per ogni $a, a' \in A$) e similmente per B). Siano date due funzioni ordinate $f : A \to B$ e $g : B \to A$ (significa che da $a \leqslant a'$ segue $f(a) \leqslant f(a')$, e similmente per g) tali che $gf(a) \leqslant a$ per ogni $a \in A$ e $b \leqslant fg(b)$ per ogni $b \in B$. Allora f e g inducono biiezioni una inversa dell'altra tra gli insiemi $\operatorname{im}(g) \subseteq A$ *e* $\operatorname{im}(f) \subseteq B$.

Si tratta in effetti di una conseguenza delle seguenti due facili osservazioni: $fgf(a) = f(a)$ per ogni $a \in A$ (perché da $gf(a) \leqslant a$ segue che $fgf(a) \leqslant f(a)$, mentre da $b \leqslant fg(b)$ per $b = f(a)$ segue $f(a) \leqslant fgf(a)$, da cui l'uguaglianza per antisimmetria) e $gfg(b) = g(b)$ per ogni $b \in B$ (argomento simile). Dunque f e g sono inverse l'una dell'altra quando applicate ad elementi della forma $g(b)$ e $f(a)$ rispettivamente. □

4.9.3. Nota. Si osservi che gli insiemi identificati dal teorema sono finiti (sono finiti i divisori monici possibili di un polinomio), ma non tutti i sottospazi stabili per φ compaiono necessariamente nella forma V_F per qualche F (infatti i sottospazi stabili potrebbero anche essere in numero infinito: quelli in biiezione con i divisori monici del polinomio minimo di φ sono quelli in qualche modo "saturati" tra i sottospazi stabili). Farsi degli esempi.

4.9.4. Problema. Ad ogni sottospazio φ-stabile W si può associare anche il polinomio caratteristico di φ ristretto a quel sottospazio, sia p_W; è ancora vero che se $W \subseteq W'$ allora $p_W | p_{W'}$. Perché non l'abbiamo usato?

4.9.5. Esempio. Al polinomio minimo di φ corrisponde tutto lo spazio V. In effetti $V_F = V$ se e solo se $F(\varphi) = 0$, dunque se e solo se F è un multiplo del polinomio minimo.

4.9.6. Problema. A cosa corrispondono MCD e mcm dei polinomi quando guardiamo agli spazi stabili associati (pensare a somma e intersezione di sottospazi)?

♠ **4.10.** Problema (polinomio caratteristico inverso). Abbiamo definito il polinomio caratteristico di una matrice quadrata A come $p_A(X) = \det(X - A)$. Ora definiamo il polinomio caratteristico inverso di A come $q_A(X) = \det(\mathbb{I} - AX)$, ove $\mathbb{I}$ è la matrice identica dell'ordine di A. Studiare il polinomio caratteristico inverso; in particolare:

(1) è invariante per similitudine;
(2) vale che $q_A(X) = X^n p_A(\frac{1}{X})$ e $p_A(X) = X^n q_A(\frac{1}{X})$; che relazione c'è tra i coefficienti dei due polinomi?
(3) ha grado (in X) minore o uguale ad n, pari al rango di A (come trovare il rango di A dal polinomio caratteristico?); vale $q_A(0) = 1$ (termine noto uno; e termine dominante?);
(4) la matrice A ha determinante nullo sse $q_A(X)$ ha grado minore dell'ordine di A; la matrice A è invertibile sse $q_A(X)$ ha grado pari dell'ordine di A;
(5) uno scalare non nullo α è autovalore di A se e solo se il suo reciproco è zero del polinomio caratteristico inverso, cioè $q_A(1/\alpha) = 0$;
(6) zero è autovalore di A se e solo se il polinomio caratteristico inverso ha grado minore dell'ordine di A;
(7) se $q_A(X) = \sum_{i=0}^n b_i X^i$, allora $b_i = (-)^i \sum_{\substack{I \subseteq \{1,\dots,n\} \\ |I| = i}} \det(A_I)$ ove A_I indica la sottomatrice di A ottenuta selezionando righe e colonne nel sottinsieme di indici I; cioè il coefficiente di X^i è la somma dei "minori principali d'ordine i di A";
(7) quali coefficienti di $q_A(X)$ danno traccia e determinante di A?
(8) verificare l'uguaglianza $q_A(X) = \exp(-\sum_{i=1}^\infty \operatorname{tr}(A^i)\frac{X^i}{i})$ (nell'anello delle serie formali; sugg.: ricondursi al caso di matrice triangolare).

Sia ora $A \in M_{\mathbb{N}}(\Bbbk)$ una matrice "quadrata" indiciata su $\mathbb{N}$, e consideriamo le sottomatrici A_n definite per ogni $n \in \mathbb{N}$ dalle prime n righe e colonne di A. Che relazioni vi sono tra $q_{A_n}(X)$ e $q_{A_{n+1}}(X)$? E per i polinomi caratteristici?

4.10.1. Problema: matrici di permutazioni. Sia σ una permutazione di $1, \dots, n$ e M_σ la matrice di permutazione corrispondente (i-esima colonna è $e_{\sigma i}$). Determinare polinomi caratteristico e minimo e discutere la diagonalizzabilità su $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ di M_σ. Conviene usare la decomposizione di σ in cicli disgiunti.

5. Teoria di Jordan.

Due righe di motivazione: se una matrice è triangolarizzabile (cioè, ha tutti gli autovalori nel campo base, oppure si passa ad una opportuna estensione del campo base), qual è la più semplice matrice triangolare possibile nella sua classe di similitudine? Quali invarianti (di similitudine) danno una classificazione completa? La teoria di Jordan (Camille, era francese) risponde a queste domande.

5.1. Definizione-Teorema (nilpotenza). *L'applicazione φ è nilpotente se esiste $N \in \mathbb{N}$ tale che $\varphi^N = 0$; l'indice di nilpotenza è il minimo intero per cui ciò succede, si indica con* $\operatorname{nilp}(A)$. *L'applicazione φ è nilpotente se e solo se una (e allora ogni) sua matrice associata è nilpotente (e gli ordini di nilpotenza sono uguali). L'applicazione φ è nilpotente se e solo se il polinomio caratteristico è X^n, dunque se e solo se ha l'unico autovalore 0 con molteplicità n; in tal caso, l'indice di nilpotenza è il grado del polinomio minimo, cioè la molteplicità di 0 (unica radice) nel polinomio minimo.*

Dimostrazione. Facile. □

5.2. Definizione (matrici nilpotenti standard). *La matrice nilpotente standard di ordine m è la matrice $N_m := \sum_{i=1}^{n-1} e_{i,i+1} \in M_m(\Bbbk)$, cioè la matrice triangolare superiore*

$$\begin{pmatrix} 0 & & \\ \vdots & \mathbb{I}_{m-1} & \\ 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

5.2.1. Si calcolino le potenze $i = 1, \dots, m$ della matrice M_m (è particolarmente simpatico ragionando in termini di applicazioni lineari) e in particolare si verifichi che $(N_m)^m = \mathbb{O}_m$, ma $(N_m)^i \neq \mathbb{O}_m$ se $i < m$ e dunque il polinomio minimo di M_m è X^m (uguale al polinomio caratteristico).

♠♠ **5.3.** Teorema (struttura degli endomorfismi nilpotenti). *Una matrice A è nilpotente se e solo se è simile a una matrice a blocchi diagonali formati da matrici nilpotenti standard. Dunque un morfismo è nilpotente se e solo se esiste una base dello spazio tale che la matrice in quella base è una matrice a blocchi diagonali formati da matrici nilpotenti standard.*

Dimostrazione. Il "se" è ovvio, visto che le matrici nilpotenti standard sono nilpotenti. Per dimostrare il "solo se" procederemo alla costruzione di una base dello spazio $V_n(\Bbbk)$ tale che la matrice associata all'endomorfismo φ che ha la matrice data in base canonica, sia del tipo detto. Questa è la costruzione fondamentale per la teoria di Jordan, e va capita bene per proseguire nella lettura. Sia N l'ordine di nilpotenza di φ, dunque $\varphi^N = 0$ (e nessuna potenza minore di φ è nulla). Consideriamo le inclusioni di sottospazi di $V_n(\Bbbk)$ dati dai nuclei delle potenze successive di φ

$$\ker\varphi \subset \ker\varphi^2 \subset \ker\varphi^3 \subset \cdots \subset \ker\varphi^{N-1} \subset \ker\varphi^N = V_n(\Bbbk)$$

dove si può verificare in effetti che tutte le inclusioni sono strette (per esempio osservando che se ad un certo punto vale l'uguaglianza allora vale l'uguaglianza da quel punto in poi; sempre tra parentesi: $N \leqslant n$, nonostante sia maiuscola). Consideriamo una decomposizione $V_n(\Bbbk) = \ker\varphi^{N-1} \oplus V_N$ (ovvero V_N è un complementare in $\ker\varphi^N$ di $\ker\varphi^{N-1}$), e sia

$$\mathscr{V}_N = (v_{N,1}, \dots, v_{N,s_N})$$

una base di V_N. Allora l'insieme $\varphi(\mathscr{V}_N)$ è contenuto in $\ker\varphi^{N-1}$ (ma non in $\ker\varphi^{N-2}$) e l'insieme $\mathscr{V}_N \cup \varphi(\mathscr{V}_N)$ è linearmente indipendente.

Consideriamo ora una decomposizione $\ker\varphi^{N-1} = \ker\varphi^{N-2} \oplus V_{N-1}$ (ovvero V_{N-1} è un complementare in $\ker\varphi^{N-1}$ di $\ker\varphi^{N-2}$), e sia

$$\mathscr{V}_{N-1} = (v_{N-1,1}, \dots, v_{N-1,s_{N-1}})$$

un completamento di $\varphi(\mathscr{V}_N)$ a una base di V_{N-1}. Allora gli insiemi $\varphi^2(\mathscr{V}_N)$ e $\varphi(\mathscr{V}_{N-1})$ sono contenuti in $\ker\varphi^{N-2}$ (ma non in $\ker\varphi^{N-3}$) e l'insieme $\mathscr{V}_N \cup \varphi(\mathscr{V}_N) \cup \varphi^2(\mathscr{V}_N) \cup \mathscr{V}_{N-1} \cup \varphi(\mathscr{V}_{N-1})$ è linearmente indipendente.

Procedendo per induzione (discendente) su N, per ogni $i = 1, \dots, N$ si decompone $\ker \varphi^{N-i+1} = \ker \varphi^{N-i} \oplus V_{N-i+1}$ (ovvero V_{N-i+1} è un complementare in $\ker \varphi^{N-i+1}$ di $\ker \varphi^{N-i}$), e sia

$$\mathscr{V}_{N-i+1} = (v_{N-i+1,1}, \dots, v_{N-i+1,s_{N-i+1}})$$

un completamento di $\bigcup_{0 \leqslant j \leqslant i-2} \varphi^{i-j-1}(\mathscr{V}_{N-j})$ a una base di V_{N-i+1}.

Alla fine del procedimento abbiamo decomposto lo spazio $V_n(\Bbbk)$ nella somma diretta

$$\begin{aligned} V_n(\Bbbk) &= \ker \varphi^{N-1} \oplus V_N \\ &= \ker \varphi^{N-2} \oplus V_{N-1} \oplus V_N \\ &= \cdots \\ &= \ker \varphi^{N-i} \oplus V_{N-i+1} \oplus \cdots \oplus V_{N-1} \oplus V_N \\ &= \cdots \\ &= V_1 \oplus V_2 \oplus V_3 \oplus \cdots \oplus V_{N-1} \oplus V_N \end{aligned}$$

ove $V_1 = \ker \varphi$ e per ognuno dei sottospazi V_{N-i} abbiamo una base del tipo $\bigcup_{j \leqslant i} \varphi^{i-j}(\mathscr{V}_{N-j})$. Possiamo riassumere schematicamente il dato nella seguente tabella, dove accanto ad ogni sottospazio viene evidenziata la base costruita:

$$\begin{array}{rcccccccccl}
V_N: & \mathscr{V}_N & & & & & & & & & \rceil \ker \varphi^N = V \\
V_{N-1}: & \varphi\mathscr{V}_N & \mathscr{V}_{N-1} & & & & & & & & \rceil \ker \varphi^{N-1} \\
V_{N-2}: & \varphi^2\mathscr{V}_N & \varphi\mathscr{V}_{N-1} & \mathscr{V}_{N-2} & & & & & & & \rceil \ker \varphi^{N-2} \\
\vdots & \vdots & \vdots & \vdots & \ddots & & & & & & \vdots \\
V_4: & \varphi^{N-4}\mathscr{V}_N & \varphi^{N-5}\mathscr{V}_{N-1} & \varphi^{N-6}\mathscr{V}_{N-2} & \cdots & \mathscr{V}_4 & & & & & \rceil \ker \varphi^4 \\
V_3: & \varphi^{N-3}\mathscr{V}_N & \varphi^{N-4}\mathscr{V}_{N-1} & \varphi^{N-5}\mathscr{V}_{N-2} & \cdots & \varphi\mathscr{V}_4 & \mathscr{V}_3 & & & & \rceil \ker \varphi^3 \\
V_2: & \varphi^{N-2}\mathscr{V}_N & \varphi^{N-3}\mathscr{V}_{N-1} & \varphi^{N-4}\mathscr{V}_{N-2} & \cdots & \varphi^2\mathscr{V}_4 & \varphi\mathscr{V}_3 & \mathscr{V}_2 & & & \rceil \ker \varphi^2 \\
V_1: & \varphi^{N-1}\mathscr{V}_N & \varphi^{N-2}\mathscr{V}_{N-1} & \varphi^{N-3}\mathscr{V}_{N-2} & \cdots & \varphi^3\mathscr{V}_4 & \varphi^2\mathscr{V}_3 & \varphi\mathscr{V}_2 & \mathscr{V}_1 & & \rceil \ker \varphi
\end{array}$$

Scegliendo ora come base di $V_n(\Bbbk)$ la base ottenuta leggendo la tabella nel modo seguente (a partire dalla destra, dal basso in alto per ogni colonna, leggendo per ogni vettore la sua sequenza al contrario)

$$\begin{aligned} &(v_{1,1}, v_{1,2}, \dots, v_{1,s_1}, \\ &\varphi v_{2,1}, v_{2,1}, \varphi v_{2,2}, v_{2,2}, \dots, \varphi v_{2,s_2}, v_{2,s_2}, \\ &\varphi^2 v_{3,1}, \varphi v_{3,1}, v_{3,1}, \varphi^2 v_{3,2}, \varphi v_{3,2}, v_{3,2}, \dots, \varphi^2 v_{3,s_3}, \varphi v_{3,s_3}, v_{3,s_3}, \\ &\dots, \\ &\varphi^{N-1} v_{N,1}, \varphi^{N-2} v_{N,1}, \dots, \varphi v_{N,1}, v_{N,1}, \varphi^{N-1} v_{N,2}, \varphi^{N-2} v_{N,2}, \dots, \varphi v_{N,2}, v_{N,2}, \dots, \\ &\qquad \varphi^{N-1} v_{N,s_N}, \varphi^{N-2} v_{N,s_N}, \dots, \varphi v_{N,s_N}, v_{N,s_N}) \end{aligned}$$

abbiamo esattamente la matrice cercata, cioè della forma

$$\begin{pmatrix} A_1 & \mathbb{O} & \mathbb{O} & \cdots & \mathbb{O} \\ \mathbb{O} & A_2 & \mathbb{O} & \cdots & \mathbb{O} \\ \mathbb{O} & \mathbb{O} & A_3 & \cdots & \mathbb{O} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbb{O} & \mathbb{O} & \mathbb{O} & \cdots & A_N \end{pmatrix}$$

ove i blocchi diagonali A_i sono formati a loro volta da s_i blocchi diagonali del tipo nilpotente standard N_i; ovvero

$$A_1 = \mathbb{O}_{s_1}, \quad A_2 = \underbrace{\begin{pmatrix} N_2 & & \\ & \ddots & \\ & & N_2 \end{pmatrix}}_{s_2 \text{ blocchi}}, \quad A_3 = \underbrace{\begin{pmatrix} N_3 & & \\ & \ddots & \\ & & N_3 \end{pmatrix}}_{s_3 \text{ blocchi}}, \dots, \quad A_N = \underbrace{\begin{pmatrix} N_N & & \\ & \ddots & \\ & & N_N \end{pmatrix}}_{s_N \text{ blocchi}}$$

□

5.3.1. Se invece scegliessimo la base giustapponendo le basi trovate nell'ordine a partire dalla destra, dal basso in alto per ogni colonna, leggendo i blocchi interi:

$$(v_{1,j}, \varphi v_{2,j}, v_{2,j}, \varphi^2 v_{3,j}, \varphi v_{3,j}, v_{3,j}, \dots, \varphi^{N-1} v_{N,j}, \varphi^{N-2} v_{N,j}, \dots, \varphi v_{N,j}, v_{N,j})$$

(variando per primo l'indice j) e la matrice dell'applicazione risulterebbe della forma

$$\begin{pmatrix} B_1 & \mathbb{O} & \mathbb{O} & \cdots & \mathbb{O} \\ \mathbb{O} & B_2 & \mathbb{O} & \cdots & \mathbb{O} \\ \mathbb{O} & \mathbb{O} & B_3 & \cdots & \mathbb{O} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbb{O} & \mathbb{O} & \mathbb{O} & \cdots & B_N \end{pmatrix}$$

ove i blocchi diagonali sono del tipo

$$B_1 = \mathbb{O}_{s_1}, \quad B_2 = \begin{pmatrix} \mathbb{O} & \mathbb{I}_{s_2} \\ \mathbb{O} & \mathbb{O} \end{pmatrix}, \quad B_3 = \begin{pmatrix} \mathbb{O} & \mathbb{I}_{s_3} & \mathbb{O} \\ \mathbb{O} & \mathbb{O} & \mathbb{I}_{s_3} \\ \mathbb{O} & \mathbb{O} & \mathbb{O} \end{pmatrix}, \ldots, \quad B_N = \begin{pmatrix} \mathbb{O} & \mathbb{I}_{s_N} & & & \\ & \mathbb{O} & \mathbb{I}_{s_N} & & \\ & & \ddots & \ddots & \\ & & & \mathbb{O} & \mathbb{I}_{s_N} \\ & & & & \mathbb{O} \end{pmatrix}$$

(ogni matrice B_i ha $i-1$ blocchi identici).

5.3.2. Osservazioni su una costruzione più intrinseca, usando i quozienti successivi dei nuclei ($W_i = \ker\varphi^i / \ker\varphi^{i-1}$) invece della scelta di complementari reciproci (V_i tali che $\ker\varphi^i = V_i \oplus \ker\varphi^{i-1}$). In particolare φ induce una funzione iniettiva $\varphi_i : W_i \to W_{i-1}$.

♠ **5.4.** Definizione-Teorema (tipo di nilpotenza). *Il tipo di nilpotenza di una matrice nilpotente $A \in M_n(\mathbb{k})$ è la N-upla di naturali $(s_1, \ldots, s_N)$ ove s_l è il numero di blocchi nilpotenti standard di ordine l della forma ridotta di A (dunque $\sum_j js_j = n$). Due matrici nilpotenti sono simili se e solo se hanno lo stesso tipo di nilpotenza.*

Dimostrazione. Il "se" è di nuovo ovvio. Per il "solo se" è sufficiente riguardare la dimostrazione precedente: se le matrici sono simili, gli spazi V_i della decomposizione hanno le stesse dimensioni, e dunque otteniamo lo stesso numero di blocchi nilpotenti standard per ogni fissato ordine di nilpotenza. □

5.5. Esempi. Elenchiamo le matrici nilpotenti canoniche a meno di equivalenza per $n \leqslant 5$; notare che il polinomio caratteristico è in ogni caso X^n, mentre il polinomio minimo è dato da $X^{\mathrm{nilp}(A)}$. Si osservi che per $n \leqslant 3$ la nilpotenza caratterizza le matrici nilpotenti canoniche a meno di similitudine; per $n \leqslant 6$ nilpotenza e rango determinano le matrici nilpotente canoniche a meno di similitudine; per $n \geqslant 7$ vi sono matrici nilpotenti aventi stesso rango e stessa nilpotenza, ma non simili.

5.5.1. Per $n = 1$ l'unica matrice nilpotente è la matrice nulla.

5.5.2. Per $n = 2$ le matrici nilpotenti canoniche sono di due tipi: la matrice nulla di tipo $(2, 0)$ e la nilpotente standard $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ di tipo $(0, 1)$.

5.5.3. Per $n = 3$ abbiamo tre tipi di matrici nilpotenti canoniche:
la matrice nulla di tipo $(3, 0, 0)$;
la matrice $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ di tipo $(1, 1, 0)$ (sse $\mathrm{nilp}(A) = 2$ e $\mathrm{rk}(A) = 1$);
la matrice $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ di tipo $(0, 0, 1)$ (sse $\mathrm{nilp}(A) = 3$ e $\mathrm{rk}(A) = 2$);

5.5.4. Per $n = 4$ abbiamo cinque tipi di matrici nilpotenti canoniche:
la matrice nulla di tipo $(4, 0, 0, 0)$;
la matrice $\left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right)$ di tipo $(2, 1, 0, 0)$ (sse $\mathrm{nilp}(A) = 2$ e $\mathrm{rk}(A) = 1$);
la matrice $\left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right)$ di tipo $(1, 0, 1, 0)$ (sse $\mathrm{nilp}(A) = 3$ e $\mathrm{rk}(A) = 2$);
la matrice $\left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right)$ di tipo $(0, 2, 0, 0)$ (sse $\mathrm{nilp}(A) = 2$ e $\mathrm{rk}(A) = 2$);
la matrice standard $\left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{smallmatrix}\right)$ di tipo $(0, 0, 0, 1)$ (sse $\mathrm{nilp}(A) = 4$ e $\mathrm{rk}(A) = 3$).

5.5.5. Per $n = 5$ abbiamo sette tipi di matrici nilpotenti canoniche:
la matrice nulla di tipo $(5, 0, 0, 0, 0)$;
la matrice $\left(\begin{smallmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{smallmatrix}\right)$ di tipo $(3, 1, 0, 0, 0)$ (sse $\mathrm{nilp}(A) = 2$ e $\mathrm{rk}(A) = 1$);
la matrice $\left(\begin{smallmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{smallmatrix}\right)$ di tipo $(1, 2, 0, 0, 0)$ (sse $\mathrm{nilp}(A) = 2$ e $\mathrm{rk}(A) = 2$);

la matrice $\begin{pmatrix} 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{pmatrix}$ di tipo $(2,0,1,0,0)$ (sse $\mathrm{nilp}(A)=3$ e $\mathrm{rk}(A)=2$);

la matrice $\begin{pmatrix} 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&0\\ 0&0&0&0&0 \end{pmatrix}$ di tipo $(1,0,0,1,0)$ (sse $\mathrm{nilp}(A)=4$ e $\mathrm{rk}(A)=3$);

la matrice $\begin{pmatrix} 0&1&0&0&0\\ 0&0&0&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 0&0&0&0&0 \end{pmatrix}$ di tipo $(0,1,1,0,0)$ (sse $\mathrm{nilp}(A)=3$ e $\mathrm{rk}(A)=3$);

la matrice $\begin{pmatrix} 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1\\ 0&0&0&0&0 \end{pmatrix}$ di tipo $(0,0,0,0,1)$ (sse $\mathrm{nilp}(A)=5$ e $\mathrm{rk}(A)=4$).

5.5.6. Elencare le matrici nilpotenti canoniche per $n=6$ (sono 11).

5.5.7. Elencare le matrici nilpotenti canoniche per $n=7$ (sono 14).

5.5.8. Diagrammi: è classico descrivere le classi di nilpotenza precedenti con dei diagrammi in cui si rappresentano in verticale i vettori di un blocco, prima i blocchi maggiori, in basso gli autovettori e via via in alto quelli generalizzati. È un buon esercizio per ciascun diagramma vedere la matrice canonica associata, le dimensioni degli autospazi (generalizzati), dei loro complementari reciproci, e il tipo di nilpotenza.

per $n=1,2,3$:

per $n=4$:

per $n=5$:

per $n=6$:

per $n=7$:

generalizzazione: esercizio...

Nota terminologica: di solito questi diagrammi si chiamano diagrammi di Young, ma prevalentemente in letteratura appaiono ruotati di $\pi/2$ in senso orario (in modo che il nucleo sia rappresentato dalla prima colonna, il che porta il disegno a sembrare "instabile": alcuni quadratini in alto con il vuoto sotto). Compare nei libri anche la versione ruotata di π o addirittura riflessa.

♠ **5.6.** Insiemi di invarianti. Abbiamo definito il tipo di nilpotenza, e mostrato che esso caratterizza per similitudine le matrici nilpotenti, cioè che c'è una corrispondenza biunivoca tra tipi di nilpotenza e classi di similitudine di matrici nilpotenti. Può essere utile chiedersi quali sequenze di numeri possono essere tipo di nilpotenza per qualche matrice nilpotente, o quali sequenze di numeri possono essere le dimensioni dei nuclei successivi di una applicazione nilpotente. Conviene forse definire questi tre insiemi:

$$N(n)=\big\{(n_1,\dots,n_N)\ :\ 0<n_1<n_2<\dots<n_N=n \text{ e } n_1\geqslant n_2-n_1\geqslant n_3-n_2\geqslant\dots\geqslant n_N-n_{N-1}\big\}$$

(i cui elementi corrispondono alle dimensioni dei nuclei: sequenze strettamente crescenti con differenze successive decrescenti),

$$H(n)=\big\{(h_1,\dots,h_N)\ :\ h_1\geqslant h_2\geqslant\dots\geqslant h_N>0 \text{ e } \Sigma_i h_i=n\big\}$$

(i cui elementi corrispondono alle dimensioni dei complementari reciproci dei nuclei, ovvero dei quozienti successivi dei nuclei: sequenze decrescenti con somma la dimensione dello spazio),

$$S(n)=\big\{(s_1,\dots,s_N)\ :\ \Sigma_i i s_i=n\big\}$$

(tipi di nilpotenza), e osservare che tutti e tre danno invarianti completi per classificare per similitudine le matrici nilpotenti d'ordine n; le relazioni (biiezioni, ovviamente) tra questi insiemi sono espresse dalla seguente tabella:

	$N(n)$	$H(n)$	$S(n)$
$N(n)$		$h_i = n_i - n_{i-1}$	$s_i = 2n_i - n_{i-1} - n_{i+1}$
$H(n)$	$n_i = \Sigma_{j\leqslant i} h_j$		$s_i = h_i - h_{i+1}$
$S(n)$	$n_i = \Sigma_{j\leqslant i}\Sigma_{k\geqslant j} s_k$ $= \Sigma_{j\leqslant i} j s_j + i\Sigma_{j>i} s_j$	$h_i = \Sigma_{j\geqslant i} s_j$	

Si verifichino le affermazioni fatte, seguendo la costruzione del teorema di struttura degli endomorfismi nilpotenti (può essere utile osservare la tabella delle dimensioni della tabella di basi là costruita, oppure ragionare sui diagrammi di Young...).

5.6.1. Problema. Come contare le classi di similitudine di matrici nilpotenti di fissato ordine n, cioè come contare gli elementi di $N(n)$, o equivalentemente $H(n)$ o $S(n)$? Si possono trovare formule ricorsive rispetto a n?

♠ **5.7.** Definizione (matrici di Jordan). *Si dice matrice standard di Jordan di ordine m e autovalore λ la matrice $J_m(\lambda) := \lambda\mathbb{I} + N_m$. Si dice matrice di Jordan una matrice quadrata a blocchi diagonali formati da matrici standard di Jordan.*

♠♠ **5.8.** Teorema (di Jordan). *Una matrice $A \in M_n(\Bbbk)$ ha tutti i suoi autovalori in $\Bbbk$ se e solo se è simile (in $\Bbbk$) a una matrice di Jordan, ovvero una matrice a blocchi diagonali formati da matrici standard di Jordan.*

Dimostrazione. Come al solito il "se" è ovvio (una matrice di Jordan è triangolare). Vediamo il "solo se". La dimostrazione procede decomponendo lo spazio negli autospazi generalizzati, che sono stabili per l'applicazione e tali che la restrizione dell'applicazione a ciascuno di essi sia una applicazione lineare con un solo autovalore. In questo modo ci si riconduce al caso di matrici nilpotenti (studiando le varie applicazioni meno il loro autovalore) e poi è sufficiente giustapporre le matrici di Jordan trovate.

5.8.1. Autospazi generalizzati. Sia $p_\varphi(x) = \prod_i (x - \lambda_i)^{r_i}$ ($r_i = m(\lambda_i)$); gli autospazi generalizzati di φ sono $V_i := \ker((\varphi - \lambda_i \mathrm{id}_V)^{r_i})$. Allora $V = \bigoplus_i V_i$, e ogni V_i è sottospazio stabile per φ.

Ora l'applicazione $\varphi_i = \varphi_{|V_i}$ (uguale a φ ristretta a V_i) è applicazione lineare di V_i in sé con un solo autovalore λ_i; perciò la differenza $\varphi_i - \lambda_i \mathrm{id}_{V_i}$ è una applicazione lineare nilpotente a cui si può applicare il teorema di struttura per applicazioni nilpotenti. Giustapponendo le basi dei sottospazi V_i si trova una base rispetto a cui la matrice di φ è nella forma dichiarata. □

♠ **5.9.** Invarianti. La molteplicità di un autovalore λ_i di A come radice del polinomio minimo è la dimensione del più grande blocco di Jordan relativo a quell'autovalore. La nullità di un autovalore λ_i di A è il numero di blocchi di Jordan relativi a quell'autovalore. La molteplicità di un autovalore λ_i di A come radice del polinomio caratteristico è la dimensione dell'autospazio generalizzato relativo a quell'autovalore. Come contare il numero di blocchi di Jordan di un autovalore e di un fissato ordine?

Questi sono degli invarianti della matrice A per similitudine, quindi invarianti di ogni endomorfismo. Invarianti completi per la classificazione per similitudine?

5.10. Esempi. Scriviamo le forme canoniche di Jordan non equivalenti tra loro, e per ognuna specifichiamo i polinomi caratteristico p e minimo m.

5.10.1. Per $n = 1$ ogni matrice è diagonale.

5.10.2. Per $n = 2$ abbiamo tre forme canoniche non equivalenti di Jordan:
la matrice diagonale $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ con $p = m = (X - \alpha)(X - \beta)$;
la matrice diagonale $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}\right)$ con $p = (X - \alpha)^2$ e $m = (X - \alpha)$;
la matrice non diagonalizzabile $\left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)$ con $p = m = (X - \alpha)^2$.

5.10.3. Per $n = 3$ abbiamo sei forme canoniche non equivalenti di Jordan:

la matrice diagonale $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ con $p = m = (X-\alpha)(X-\beta)(X-\gamma)$;
la matrice diagonale $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$ con $p = (X-\alpha)^2(X-\beta)$ e $m = (X-\alpha)(X-\beta)$;
la matrice non diagonalizzabile $\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$ con $p = m = (X-\alpha)^2(X-\beta)$;
la matrice diagonale $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$ con $p = (X-\alpha)^3$ e $m = (X-\alpha)$;
la matrice non diagonalizzabile $\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$ con $p = (X-\alpha)^3$ e $m = (X-\alpha)^2$;
la matrice non diagonalizzabile $\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}$ con $p = m = (X-\alpha)^3$.

5.10.4. Per $n = 4$ abbiamo 14 forme canoniche non equivalenti di Jordan:
$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & \delta \end{pmatrix}$ con $p = m = (X-\alpha)(X-\beta)(X-\gamma)(X-\delta)$;
$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix}$ con $p = (X-\alpha)^2(X-\beta)(X-\gamma)$ e $m = (X-\alpha)(X-\beta)(X-\gamma)$;
$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix}$ con $p = m = (X-\alpha)^2(X-\beta)(X-\gamma)$;
$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X-\alpha)^2(X-\beta)^2$ e $m = (X-\alpha)(X-\beta)$;
$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X-\alpha)^2(X-\beta)^2$ e $m = (X-\alpha)^2(X-\beta)$;
$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 1 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = m = (X-\alpha)^2(X-\beta)^2$;
$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X-\alpha)^3(X-\beta)$ e $m = (X-\alpha)(X-\beta)$;
$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X-\alpha)^3(X-\beta)$ e $m = (X-\alpha)^2(X-\beta)$;
$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 1 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X-\alpha)^3(X-\beta)$ e $m = (X-\alpha)^3(X-\beta)$;
$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$ con $p = (X-\alpha)^4$ e $m = (X-\alpha)$;
$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$ con $p = (X-\alpha)^4$ e $m = (X-\alpha)^2$;
$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$ con $p = (X-\alpha)^4$ e $m = (X-\alpha)^2$;
$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 1 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$ con $p = (X-\alpha)^4$ e $m = (X-\alpha)^3$;
$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 1 & 0 \\ 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$ con $p = (X-\alpha)^4$ e $m = (X-\alpha)^4$.

5.10.5. Scriversi tutte le forme canoniche non equivalenti di Jordan con $n = 5$ (sono 27).

5.10.6. Si noti che fino ad $n = 3$ la coppia dei polinomi caratteristico e minimo determina la forma canonica di Jordan; per $n > 3$ ciò in generale è falso. Cosa serve per la classificazione?

5.11. Uguaglianza di polinomio minimo e caratteristico. Per ogni endomorfismo (o matrice quadrata) polinomio minimo e caratteristico coincidono se e solo se per ogni autovalore (eventualmente in estensioni del campo) vi è un solo blocco standard di Jordan (necessariamente di ordine pari alla molteplicità algebrica, che coincide la nullità, dell'autovalore).

5.12. Prodotto. Mostrare che le matrici AB e BA hanno gli stessi blocchi di Jordan corrispondenti ad autovalori non nulli.

5.13. Trasposizione. Mostrare che ogni matrice è simile alla propria trasposta (per esempio supponendo la matrice triangolarizzabile). Cosa si può dire di una matrice invertibile e della sua inversa?

5.14. Inversione. Un risultato piuttosto facile è il seguente: una matrice è simile alla propria inversa se e solo se per ogni autovalore diverso da ± 1 compare anche l'inverso come autovalore esattamente con la stessa struttura di (blocchi di) Jordan.

Una matrice è simile alla propria inversa se e solo se è prodotto di due (matrici di) involuzioni (cioè matrici di quadrato identità). Un senso è ovvio: se $A^2 = \mathbb{I} = B^2$, allora AB è simile a $BA = (AB)^{-1}$ (usando A o B per fare il coniugio). Per il viceversa, ci si può ridurre alle forme di Jordan (ma è difficile!), oppure usare le matrici compagne (e allora una simmetria si ottiene invertendo l'ordine delle basi, con matrici di "1" antidiagonali).

5.15. Matrici simmetriche. Mostrare che ogni matrice si può scrivere come prodotto di due matrici simmetriche (e una invertibile, l'altra di rango pari alla data). Basta farlo per le matrici di Jordan: se A è tale che $A = PJP^{-1}$ con J di Jordan, e $J = ST$ con S, T simmetriche, allora $A = PJP^{-1} = PSTP^{-1} = PST^{\mathrm{t}}P^{-\mathrm{t}}TP^{-1} = S'T'$ dove $S' = PST^{\mathrm{t}}$ e $T' = P^{-\mathrm{t}}TP^{-1}$ sono simmetriche.

Per un blocco di Jordan standard basta notare che invertendo le righe (o le colonne) si ottiene una matrice simmetrica, e questo si ottiene moltiplicando a sinistra (o a destra) per la matrice simmetrica avente sempre 1 nell'antidiagonale principale.

♠ **5.16.** Problema di commutazione. Date A e B matrici (di ordini opportuni), descrivere le matrici X tali che $AX = XB$. Perché il problema abbia senso è necessario che il numero di colonne di A sia uguale al numero di righe di X (per il prodotto AX), e che il numero di righe di A sia uguale al numero di righe di X (per l'uguaglianza). Quindi, $A \in M_n(\Bbbk)$ e $B \in M_m(\Bbbk)$ devono essere matrici quadrate, e $X \in M_{n,m}(\Bbbk)$. Il problema consiste allora nel cercare il nucleo dell'endomorfismo di $M_{n,m}(\Bbbk)$ che manda X in $AX - XB$.

5.16.1. Osserviamo prima di tutto che nel caso di matrici nilponenti standard (blocco di Jordan nilpotente) la risposta si trova direttamente: $N_pX = XN_q$ se e solo se X è della forma $\begin{pmatrix} 0 & T \end{pmatrix}$ se $p \leqslant q$ oppure $\begin{pmatrix} T \\ 0 \end{pmatrix}$ se $p \geqslant q$, con T matrice triangolare superiore a diagonali costanti:

$$T = \begin{pmatrix} a_1 & a_2 & \cdots & a_r \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_2 \\ 0 & \cdots & 0 & a_1 \end{pmatrix}$$

5.16.2. In secondo luogo, è facile ridurre il problema, per due matrici quadrate qualsiasi, all'analogo problema per le loro forme di Jordan: infatti se $J_A = H^{-1}AH$ e $J_B = K^{-1}BK$ allora abbiamo: $AX = XB$ se e solo se $J_AY = YJ_B$ dove $Y = H^{-1}XK$; quindi identificare le X o le Y è equivalente.

Chiamiamo λ_i gli autovalori di A, μ_j quelli di B. Ora, se dividiamo la matrice Y in blocchi $Y_{i,j} \in M_{p_i,q_j}(\Bbbk)$ seguendo le divisioni in blocchi di Jordan di J_A (per le righe) e di J_B (per le colonne) otteniamo che

$$Y_{i,j} = \begin{cases} 0 & \text{se } \lambda_i \neq \mu_j \\ \begin{pmatrix} 0 & T \end{pmatrix} & \text{se } \lambda_i = \mu_j \text{ e } p_i \leqslant q_j \\ \begin{pmatrix} T \\ 0 \end{pmatrix} & \text{se } \lambda_i = \mu_j \text{ e } p_i \geqslant q_j \end{cases}$$

da cui è possibile ricavare che la dimensione dello spazio delle matrici che commutano con A e B è dato dalla somma degli interi $d_{i,j} = \delta_{\lambda_i,\mu_j} \min(p_i, q_j)$ (somma estesa a tutti i blocchi di Jordan elementari).

5.16.3. Usiamo ora $A = B \in M_n(\Bbbk)$, e definiamo il centralizzante di A come

$$\mathscr{C}(A) = \{X \in M_n(\Bbbk) \ : \ AX = XA\}$$

(sottospazio delle matrici che commutano con A).

Ricordando che $\Bbbk[A] = \operatorname{im}(v_A) = \{p(A) \ : \ p(X) \in \Bbbk[X]\}$, abbiamo che $\Bbbk[A] \leqslant \mathscr{C}(A)$ (matrici polinomiali in A commutano con A, ovviamente). Siccome $\dim_{\Bbbk} \Bbbk[A]$ è pari al grado del polinomio minimo di A (verifica facile), di solito l'inclusione sarà stretta. Mostrare che $\Bbbk[A] = \mathscr{C}(A)$ se e solo se $m_A(X) = p_A(X)$ (polinomio caratteristico e minimo coincidono), cioè se e solo se ogni autovalore ha un unico blocco di Jordan.

5.16.4. In generale, $\Bbbk[A]$ coincide con il sottospazio

$$\mathscr{C}(\mathscr{C}(A)) = \{Y \in M_n(\Bbbk) \ : \ AX = XA \Rightarrow YX = XY\} \ ,$$

cioè: le matrici polinomiali in A sono tutte e sole le matrici che commutano con tutte le matrici che commutano con A.

5.16.5. Chi è $\mathscr{C}(\mathscr{C}(\mathscr{C}(A)))$? E $\mathscr{C}(\mathscr{C}(\mathscr{C}(\mathscr{C}(A))))$?

5.16.6. Si discuta in particolare, e indipendentemente dai ragionamenti precedenti, il caso di matrici diagonalizzabili: in tal caso lo spazio delle matrici che vi commutano ha dimensione data dalla somma dei quadrati delle molteplicità degli autovalori.

5.17. Forma di Jordan Reale. Se $A \in M_n(\mathbb{R})$ è matrice quadrata reale, essa ammette forma di Jordan (in $\mathbb{R}$) se e solo se ha tutti gli autovalori reali. Invece ammette sempre forma di Jordan pensata come matrice a coefficienti complessi, e si vede facilmente che i blocchi di Jordan per un autovalore e il suo coniugato hanno la stessa forma, nel senso che il tipo di nilpotenza è lo stesso. Si può allora (ragionando opportunamente sulle basi: come?) ottenere un teorema di Jordan reale di questo tipo: *Ogni matrice quadrata reale è simile in $\mathbb{R}$ ad una matrice con blocchi diagonali J e J', dove J è una matrice di Jordan reale (e tiene conto degli autovalori reali) mentre J' è una matrice (reale) d'ordine pari che si ottiene da una matrice di Jordan d'ordine metà sostituendo i termini diagonali con opportune matrici d'ordine 2 (quali? tengono conto degli autovalori complessi) e gli eventuali 1 sovradiagonali con matrici $\mathbb{I}_2$ (identiche d'ordine 2).*

♠♠ 5.18. Definizione (semisemplicità). *Una matrice $A \in M_n(\Bbbk)$ si dice semisemplice se essa è diagonalizzabile in una chiusura algebrica di $\Bbbk$. Un endomorfismo di uno spazio vettoriale V di dimensione finita su $\Bbbk$ si dice semisemplice se una matrice associata lo è (e allora tutte lo sono).*

5.18.1. Esempi. Matrici trigonometriche in $M_2(\mathbb{R})$, matrici in $M_2(\mathbb{Q})$ diagonalizzabili in $\mathbb{Q}[\sqrt{2}]$.

5.18.2. Decomposizione astratta di Jordan. Sia A un endomorfismo di uno spazio vettoriale V di dimensione finita (rispettivamente: sia A una matrice quadrata) con tutti i suoi autovalori nel corpo di base $\Bbbk$. Allora esistono due endomorfismi (risp. matrici) A_s, A_n tali che

(*i*) A_s è semisemplice e A_n è nilpotente;
(*ii*) $A_sA_n = A_nA_s$ e $A = A_s + A_n$;
(*iii*) esistono polinomi $p(X), q(X) \in \Bbbk[X]$ privi di termine noto e tali che $A_s = p(A)$, $A_n = q(A)$; in particolare A_s ed A_n commutano con ogni endomorfismo (risp. ogni matrice) che commuti con A;
(*iv*) sottospazi stabili per A sono stabili sia per A_s che per A_n;
(*v*) se $AB = BA$ con A e B soddisfacenti all'ipotesi detta, allora $(A+B)_s = A_s + B_s$ e $(A+B)_n = A_n + B_n$.

5.18.3. Decomposizione astratta moltiplicativa di Jordan. Sia A un automorfismo di uno spazio vettoriale V di dimensione finita (rispettivamente: sia A una matrice quadrata invertibile) con tutti i suoi autovalori nel corpo di base $\Bbbk$. Allora i suoi autovalori sono tutti non nulli, ed esistono due endomorfismi (risp. matrici) A_s, A_u tali che

(*i*) A_s è semisemplice e A_u è unipotente (significa che ha 1 come unico autovalore);
(*ii*) $A_sA_u = A_uA_s = A$;
(*iii*) sottospazi stabili per A sono stabili sia per A_s che per A_u;
(*iv*) se $AB = BA$ con A e B soddisfacenti all'ipotesi detta, allora $(AB)_s = A_sB_s$ e $(AB)_u = A_uB_u$.

6. Applicazioni.

6.1. Calcolo di potenze delle matrici. Data una matrice A, calcolarne le potenze A^m richiede normalmente molti conti, a meno che A non sia di una forma particolare. Due casi particolarmente semplici sono i seguenti:

(6.1.1) se $D = diag(a_1, \dots, a_n)$ è matrice diagonale, allora $D^m = diag(a_1^m, \dots, a_n^m)$;
(6.1.2) se $J = D + N$ è in forma di Jordan, poiché $DN = ND$, possiamo applicare la formula del binomio di Newton: $J^m = (D+N)^m = \sum_{i=0}^m \binom{m}{i} D^i N^{m-i}$ (si ricordi che D ed N commutano tra loro; le potenze delle matrici nilpotenti standard sono di calcolo immediato).

6.1.3. Se una matrice A ammette forma canonica diagonale o di Jordan, allora esiste una matrice invertibile P tale che $A = P^{-1}JP$. In tal caso abbiamo $A^m = P^{-1}J^mP$, il che semplifica notevolmente il calcolo.

6.2. Soluzione di equazioni ricorsive. Supponiamo che una sequenza di numeri $a_i \in \Bbbk$ per $i \in \mathbb{N}$ sia definita ricorsivamente dalle seguenti posizioni: $a_0 = \alpha_0$, $a_1 = \alpha_1$, ..., $a_{n-1} = \alpha_{n-1}$ e $a_k = \beta_1 a_{k-1} + \beta_2 a_{k-2} + \cdots + \beta_n a_{k-n}$ per ogni $k \geqslant n$, ove $\alpha_i, \beta_i \in \Bbbk$. Come trovare una formula chiusa che calcoli a_k, senza dover calcolare tutti i precedenti?

Se consideriamo i vettori le cui componenti sono $a_k, a_{k-1}, \ldots, a_{k-n+1}$, possiamo riassumere la relazione ricorsiva come

$$\begin{pmatrix} a_k \\ a_{k-1} \\ \cdots \\ a_{k-n+1} \end{pmatrix} = \begin{pmatrix} \beta_1 & \beta_2 & \cdots & \beta_n \\ & & & 0 \\ & \mathbb{I}_{n-1} & & \vdots \\ & & & 0 \end{pmatrix} \begin{pmatrix} a_{k-1} \\ \cdots \\ a_{k-n+1} \\ a_{k-n} \end{pmatrix}$$

(qual è il polinomio caratteristico di questa matrice?) da cui si vede che

$$\begin{pmatrix} a_k \\ a_{k-1} \\ \vdots \\ a_{k-n+1} \end{pmatrix} = \begin{pmatrix} \beta_1 & \beta_2 & \cdots & \beta_n \\ & & & 0 \\ & \mathbb{I}_{n-1} & & \vdots \\ & & & 0 \end{pmatrix}^{k-n+1} \begin{pmatrix} \alpha_{n-1} \\ \vdots \\ \alpha_1 \\ \alpha_0 \end{pmatrix}$$

e quindi il problema è ricondotto a calcolare la (prima riga della) potenza $(k-n+1)$-esima della matrice scritta. Tale calcolo può essere effettuato cercando la forma canonica (diagonale o di Jordan), come prima spiegato.

♠ **6.3.** Soluzione di equazioni alle differenze. Più in generale, possiamo porre il seguente problema: trovare le successioni $v_m \in \Bbbk^n$ (per $m \in \mathbb{N}$) tali che $v_{m+1} = Av_m$ per una fissata matrice $A \in M_n(\Bbbk)$. Chiaramente per ogni scelta del vettore iniziale v_0, vi è una unica tale successione definita da $v_n = A^n v_0$, e una descrizione esplicita può essere ottenuta se la matrice A ammette una forma canonica diagonale o di Jordan.

6.3.1. Supponiamo per esempio che A sia diagonalizzabile, che $A = P^{-1}\Delta P$ con Δ matrice diagonale avente in diagonale gli autovalori di A, e P matrice invertibile la cui inversa ha come colonne una base di autovettori per A. Allora $A^m = P^{-1}\Delta^m P$ e, scelta la "condizione iniziale" $v_0 = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ e posto $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, abbiamo che $v_m = \sum_{i=1}^n y_i \lambda_i^m u_i$ ove λ_i sono gli autovalori di A (diagonale di Δ) e u_i sono i rispettivi autovettori (colonne di P^{-1}).

6.3.2. Se invece A ammette forma canonica di Jordan J non diagonale, compaiono nelle soluzioni ulteriori termini dovuti alla parte nilpotente di J. Studiamo per esempio il caso di un blocco di Jordan d'autovalore α e d'ordine n. Sia $A = P^{-1}JP$ con $J = \alpha\mathbb{I}_n + N_n$ tale blocco. Allora $v_m = A^m v_0 = P^{-1}J^m P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P^{-1}J^m \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ (con le notazioni precedenti). Poiché $J^m = (\alpha\mathbb{I}_n + N_n)^m = \sum_{j=0}^{n-1} \binom{m}{j} \alpha^{m-j} N_n^j$ (esplicitare bene questa formula), abbiamo che

$$v_m = \sum_{i=1}^n \Big(\sum_{j=i}^n \binom{m}{j-i} \alpha^{m-j+i} y_j\Big) u_i = \sum_{j=1}^n y_j \Big(\sum_{i=1}^j \binom{m}{j-i} \alpha^{m-j+i} u_i\Big).$$

6.3.3. Processi discreti di Markov. Un caso interessante di equazioni alle differenze è descritto dalle matrici reali con entrate comprese tra 0 e 1, e tali che in ogni colonna la somma delle entrate sia 1. Vengono così descritti dei fenomeni (demografici, statistici, ecc.) in cui ad ogni "passo" certe quantità, rappresentate dalle componenti dei vettori, sono redistribuite secondo una certa regola fissata dalla matrice (detta di transizione).

È facile in questo caso verificare che la matrice ammette sempre l'autovalore 1, e che tutti gli altri autovalori (eventualmente complessi) hanno valore assoluto minore o uguale ad 1. Supponiamo

che il blocco relativo all'autovalore 1 di A sia diagonalizzabile. Allora, se gli autovalori diversi da 1 hanno tutti valore assoluto strettamente minore di 1, la sequenza A^n tende, per n grande ("limite per n che va all'infinito") alla matrice $P^{-1}\Delta' P$ ove Δ' è la matrice diagonale avente nella diagonale solo l'autovalore 1 (con la sua molteplicità). Che conseguenze vi sono per la successione dei v_n?

♠ **6.4.** Esponenziali di matrici. Nel caso di matrici reali o complesse, possiamo definire una nozione di esponenziale di base e per una matrice qualsiasi A usando quale definizione la formula di Taylor:

$$e^A := \sum_{i=0}^{\infty} \frac{A^i}{i!} = \mathbb{I}_n + A + \frac{A^2}{2} + \frac{A^3}{6} + \cdots + \frac{A^i}{i!} + \cdots .$$

Si pone subito un problema di convergenza: abbiamo usato una sommatoria infinita di matrici, e quindi bisogna controllare che esista il limite delle somme parziali.

6.4.1. Per questo occorre introdurre una nozione di norma nell'insieme delle matrici, e ciò può essere fatto in questo modo: per $A = (a_{i,j})$ definiamo $|A| := \max_{i,j} |a_{i,j}|$ (valore assoluto di numeri reali o complessi). Si verifica allora che la definizione data è corretta per ogni matrice A. Si mostra infatti per induzione che $|A^i| \leqslant n^i |A|^i = (n|A|)^i$, e dunque la serie scritta è maggiorata, termine a termine, dalla serie numerica convergente a $e^{n|A|}$.

6.4.2. Abbiamo dunque una applicazione $M_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$ che soddisfa alle usuali proprietà: $e^{\mathbb{O}_n} = \mathbb{I}_n$, $e^{A+B} = e^A e^B$ sotto ipotesi che A e B commutino tra loro (quindi $e^A e^{-A} = \mathbb{I}_n$, per cui e^{-A} è matrice inversa della matrice e^A, e tutte le esponenziali sono matrici invertibili).

6.4.3. Il calcolo della matrice esponenziale è particolarmente facile per matrici diagonali ($e^{diag(a_1,\dots,a_n)} = diag(e^{a_1},\dots,e^{a_n})$ come si vede subito) e per matrici nilpotenti (si tratta di una somma finita, in questo caso).

Per una matrice A che sia diagonalizzabile si può allora calcolarne l'esponenziale nel modo seguente: se $A = P^{-1}\Delta P$ con Δ diagonale, si ha $e^A = P^{-1}e^{\Delta}P$, che è di calcolo immediato.

Per una matrice che ammetta forma di Jordan $J = \Delta + N$ (quindi per tutte se usiamo il corpo complesso) abbiamo $A = P^{-1}JP$ con $J = \Delta + N$, da cui $e^A = P^{-1}e^J P = P^{-1}e^{\Delta}e^N P$.

6.4.4. Si osservi che se λ è autovalore di A, allora e^λ è autovalore di e^A. Da questo si deduce subito che $\det(e^A) = e^{\operatorname{tr} A}$ (infatti $\Pi e^\lambda = e^{\Sigma\lambda}$). In particolare le matrici di traccia nulla hanno esponenziali di determinante 1.

6.4.5. Che proprietà hanno le matrici esponenziali di matrici antisimmetriche?

6.4.6. Sistemi di equazioni differenziali lineari a coefficienti costanti. Una equazione differenziale lineare a coefficienti costanti (reali o complessi) è una espressione del tipo $\dfrac{dv}{dx} = Av$ ove $v = v(x)$ è un vettore di funzioni (reali o complesse) della variabile x e A è una matrice quadrata con coefficienti nel corpo reale o complesso. Soluzioni di questa equazione sono tutti i vettori di funzioni che soddisfano all'uguaglianza.

Si studierà in Analisi che per ogni "condizione iniziale" $v(0) = v_0$ (vettore reale o complesso) esiste una unica soluzione $v(x)$ all'equazione posta che soddisfi anche alla condizione iniziale. Vediamo qui come determinare tale soluzione usando l'esponenziazione di matrici.

Si consideri la matrice e^{Ax} come funzione della variabile x (e si trascurino per il momento problemi di convergenza in x); si verifica quasi subito che $\dfrac{d(e^{Ax})}{dx} = Ae^{Ax}$ e che abbiamo $e^{Ax}{}_{|x=0} = \mathbb{I}_n$.

Quindi il vettore $v(x) = e^{Ax}v_0$ soddisfa alla equazione differenziale e anche alla condizione iniziale; in altri termini, le soluzioni della equazione differenziale data si ottengono mediante combinazioni lineari delle colonne della matrice e^{Ax} secondo dei combinatori che dipendono dalle condizioni iniziali poste.

6.4.7. Problema. Il lettore incuriosito, può esplorare l'estensione del calcolo differenziale a matrici funzioni di una variabile t. Per esempio mostrando che $\frac{d}{dt}(AB) = \frac{d}{dt}(A)B + A\frac{d}{dt}(B)$, o anche $\frac{d}{dt}(H^{-1}) = -H^{-1}\frac{d}{dt}(H)H^{-1}$ ...

6.4.8. Problema: radici di matrici. Discutere l'esistenza di radici m-esime di matrici quadrate: data $A \in M_n(\Bbbk)$ esistono $X \in M_n(\Bbbk)$ tali che $X^m = A$, eventualmente quante e come trovarle?

6.4.9. Problema: logaritmi di matrici.

6.4.10. Problema: algoritmo di google. Cenno al teorema di Perron-Frobenius?

7. Teoria di Frobenius: Forme Canoniche Razionali.

Se $\Bbbk$ non è algebricamente chiuso, esistono matrici a coefficienti in $\Bbbk$ che non ammettono forma di Jordan. In questa sezione vedremo invece una forma canonica diversa, talvolta detta di Frobenius, e per certi aspetti più generale (nel senso che quella di Jordan ne è un caso particolare), tale che ogni matrice quadrata a coefficienti in $\Bbbk$ possiede una tale forma.

Vi sono almeno due modi elementari di introdurre le "forme canoniche razionali", entrambi interessanti. Uno attraverso lo studio dei sottospazi ciclici per l'endomorfismo in questione, più vicino all'atteggiamento di ricercare una base opportuna dello spazio, come si è fatto finora. L'altro invece usa la nozione di equivalenza di matrici in $\Bbbk[X]$ (che è anello, e non campo!), e la sua relazione con la similitudine di matrici in $\Bbbk$; si tratta di un atteggiamento più astratto, ma che mostra tecniche molto interessanti. Li esploreremo entrambi.

7.1. Metodo dei sottospazi φ-ciclici. Consideriamo un endomorfismo $\varphi : V \to V$. Per ogni vettore $v \in V$ definiamo l'ideale di $\Bbbk[X]$ formato dai polinomi $p(X)$ tali che $p(\varphi)v = 0$ (calcolati in φ annullano v); tale ideale si dice il φ-annullatore di v, e il suo generatore monico si indica con $m_{\varphi,v}(X)$ o con $m_v(X)$ se si può sottintendere φ e si dice il (polinomio) φ-annullatore di v.

È chiaro che ogni vettore ammette un polinomio φ-annullatore, e che questo è un divisore del polinomio minimo di φ.

7.1.1. Proprietà fondamentale. *È facile, ma importante, osservare che per ogni $v \in V$ e detto s il grado di $m_v(X)$, allora l'insieme $v, \varphi(v), \dots, \varphi^{s-1}(v)$ è linearmente indipendente, mentre per ogni $t \geqslant s$ l'insieme $v, \varphi(v), \dots, \varphi^{s-1}(v), \varphi^t(v)$ è linearmente dipendente.*

7.1.2. Sottospazi φ-ciclici. *Un sottospazio W di V si dice φ-ciclico se è del tipo*

$$W = \langle v, \varphi(v), \dots, \varphi^i(v), \dots \rangle$$

per qualche $v \in V$; il vettore v si dice in tal caso un φ-generatore di W o vettore ciclico per φ su W.

È facile anche vedere che la dimensione di un sottospazio φ-ciclico W coincide con il grado del φ-annullatore di un suo qualsiasi φ-generatore.

7.1.3. È chiaro che sottospazi φ-ciclici sono φ-stabili, mentre il viceversa in generale è falso. Vale in effetti la seguente proprietà: un sottospazio φ-stabile è φ-ciclico, cioè ammette un vettore ciclico, se e solo se polinomi caratteristico e minimo di φ coincidono sul sottospazio.

In particolare, l'intero spazio ammette un vettore φ-ciclico se e solo se polinomio minimo e caratteristico di φ coincidono.

Più in generale, esiste sempre un vettore tale che il suo φ-annullatore $m_{\varphi,v}(X)$ sia il polinomio minimo $m_\varphi(X)$ di φ. Infatti i φ-annullatori dei vettori di V sono in numero finito (divisori del polinomio minimo di φ), e quindi V è unione (non solo somma!) finita dei sottospazi formati dai vettori annullati da questi polinomi (e non serve considerarli tutti, bastano i divisori "massimali" propri di $m_\varphi(X)$), quindi V deve coincidere con uno di questi sottospazi.

7.1.4. Struttura di sottospazi φ-ciclici. *Se W è φ-ciclico e $v \in V$ ne è un φ-generatore, allora ogni vettore $w \in W$ si scrive $w = f(\varphi)(v)$ per qualche $f(X) \in \Bbbk[X]$; tale polinomio è unico se si impone che abbia grado minore della dimensione di W, cioè* $\deg f(X) < \deg m_v(X)$. Si tratta di facili verifiche.

7.1.5. Sottospazi φ-ciclici φ-irriducibili e φ-equivalenti. Un sottospazio φ-ciclico si dice φ-irriducibile se non può essere scritto come somma diretta di φ-ciclici strettamente più piccoli; se ciò succede, il polinomio minimo di φ ristretto a quel sottospazio è potenza di un polinomio irriducibile.

Due sottospazi φ-ciclici si dicono φ-equivalenti se esiste un isomorfismo tra loro che commuta con (le restrizioni di) φ; ciò succede se e solo se le restrizioni di φ ai due sottospazi hanno ugual polinomio minimo.

7.1.6. Teorema di decomposizione in φ-ciclici. *Sia φ un endomorfismo di V, e sia $m_\varphi(X) = \prod_i p_i(X)^{s_i}$ con $p_i(X) \in \Bbbk[X]$ polinomi irriducibili (in $\Bbbk[X]$). Allora V è somma diretta di sottospazi φ-ciclici φ-irriducibili, siano L_j, tali che $m_{\varphi_{L_j}}(X) = p_{i(j)}(X)^{s_j}$ (divisore di $m_\varphi(X)$).*

Questo è il vero risultato tecnico di questa sezione, e la sua dimostrazione si basa su una delicata induzione. È facile (usando il teorema generale di decomposizione in sottospazi φ-stabili) ridursi al caso $m_\varphi(X) = p(X)^s$, cioè con un unico fattore irriducibile: dimostriamo allora che *se φ è un endomorfismo di V, e $m_\varphi(X) = p(X)^s$ con $p(X)$ irriducibile, allora V è somma diretta di sottospazi φ-ciclici φ-irriducibili.*

Si procede per induzione su $n = \dim V$, essendo banale il caso $n = 1$. Supponiamo allora $n > 1$, $d = \deg p(X)$, dunque $m = \deg m_\varphi(X) = ds$ (divisore di n). Sia $v_0 \in V$ tale che $p(\varphi)^s v_0 = 0$, ma $p(\varphi)^{s-1} v_0 \neq 0$ (esiste perché $p(X)^s$ è il polinomio minimo), e poniamo $V_0 = \langle \varphi^i v_0 \ : \ i = 0, \dots, ds-1 \rangle$ sottospazio φ-ciclico di V generato da v_0.

Sia $\overline{V} = V/V_0$, e $\overline{\varphi}$ l'endomorfismo indotto da φ su $\overline{V}$. Siccome $\dim_{\Bbbk} \overline{V} < \dim_{\Bbbk} V$ (perché $V_0 \neq 0$), e il polinomio minimo di $\overline{\varphi}$ divide quello di φ, quindi è della forma $p(X)^{\overline{s}}$ con $\overline{s} \leqslant s$, possiamo usare l'ipotesi induttiva e scrivere che $\overline{V}$ è somma diretta $\overline{V} = \overline{V}_1 \oplus \cdots \oplus \overline{V}_r$ con i $\overline{V}_i$ sottospazi $\overline{\varphi}$-ciclici (irriducibili). Il problema consiste ora nel rialzare i sottospazi $\overline{V}_i$ di $\overline{V}$ a dei sottospazi V_i di V che siano φ-ciclici (irriducibili) in somma diretta tra loro e con V_0.

Sia $\overline{v}_1$ un $\overline{\varphi}$-generatore di $\overline{V}_1$, e $p(X)^{\overline{s}_1}$ il suo φ-annullatore ($\overline{s}_1 \leqslant s$). Vogliamo ottenere $v_1 \in \overline{v}_1$ tale che $p(X)^{\overline{s}_1}$ sia il suo φ-annullatore. Procediamo scegliendo $w_1 \in \overline{v}_1$ qualsiasi, per cui $p(\overline{\varphi})^{\overline{s}_1} \overline{w}_1 = 0$, cioè $p(\varphi)^{\overline{s}_1} w_1 \in V_0$, da cui $p(\varphi)^{\overline{s}_1} w_1 = k_1(\varphi) v_0$ per qualche polinomio $k(X)$. Siccome $p(\varphi)^s v = 0$ per ogni $v \in V$ abbiamo che $0 = p(\varphi)^{s-\overline{s}_1} p(\varphi)^{\overline{s}_1} w_1 = p(\varphi)^{s-\overline{s}_1} k_1(\varphi) v_0$, da cui segue che $p(X)^s$ divide $p(X)^{s-\overline{s}_1} k_1(X)$, quindi $p(X)^{\overline{s}_1}$ divide $k_1(X)$, e infine $k_1(X) = p(X)^{\overline{s}_1} h_1(X)$. Otteniamo allora che $p(\varphi)^{\overline{s}_1} w_1 = p(\varphi)^{\overline{s}_1} h_1(\varphi) v_0$. Ora ponendo $v_1 = w_1 - h_1(\varphi) v_0$ risulta facile vedere che $p(\varphi)^{\overline{s}_1} v_1 = 0$, e dunque $p(X)^{\overline{s}_1}$ è il φ-annullatore di v_1.

Consideriamo allora $V_1 = \langle \varphi^i(v_1) \ : \ i \geqslant 0 \rangle$ lo spazio φ-ciclico generato da v_1; è chiaro che la mappa di riduzione $V_1 \to \overline{V}_1$ è isomorfismo (spazi φ-ciclici con lo stesso polinomio minimo).

Ripetendo il procedimento per ogni $i = 1, \dots, r$ otteniamo dei sottospazi V_i φ-ciclici tali che $V = \bigoplus_{i=1}^r V_i$ (facile controllo), come si voleva. □

7.1.7. Dimostrazione alternativa. Sempre per induzione su $n = \dim V$, sia m il grado del polinomio minimo, e sia v vettore con φ-annullatore di grado m; possiamo scrivere

$$W = \langle v, \varphi v, \dots, \varphi^{m-1} v \rangle$$

e completare la base di W ad una di tutto V. Usando la base duale su V^*, sia $w = \varphi^{m-1} v$, consideriamo

$$\mathbb{W} = \langle w^*, \varphi^* w^*, \dots, (\varphi^*)^{m-1} w^* \rangle$$

che è sottospazio di V^* che è stabile per φ^* (perché?). Quindi $\mathbb{W}^\perp$ è sottospazio di V stabile per φ, e risulta $V = W \oplus \mathbb{W}^\perp$ (per l'intersezione, basta applicare $w^*, \varphi^* w^*, \dots$ ad una eventuale relazione $\Sigma_i \alpha_i \varphi^i v = 0$). Quindi l'ipotesi induttiva usata su $\mathbb{W}^\perp$ garantisce il risultato. □

7.1.8. Unicità della decomposizione? È chiaro a priori che una decomposizione in φ-ciclici φ-irriducibili non è unica: basta pensare alla applicazione identica. Vale comunque una proprietà di essenziale unicità in questo senso: due decomposizioni diverse, a meno dell'ordine, sono fatte con sottospazi corrispondenti φ-equivalenti. Dimostrarlo non è banale: si dimostra che per ogni potenza di ogni fattore irriducibile del polinomio minimo, il numero di sottospazi φ-ciclici aventi quella come polinomio minimo non dipende dalla decomposizione, ma solo da φ.

7.1.9. Matrici compagne e ipercompagne. Dato un polinomio monico $f(X) = \sum_{i=0}^n a_i X^i$ ($a_n = 1$), diciamo matrice compagna di $f(X)$ e indichiamo con $\mathrm{C}(f)$ la matrice

$$\mathrm{C}(f) = \begin{pmatrix} 0 & -a_0 \\ \mathbb{I}_{n-1} & -a_i \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

che ha chiaramente polinomio caratteristico e minimo coincidenti con $f(X)$.

Ora, se W è un sottospazio φ-ciclico con φ-generatore w e polinomio caratteristico di φ ristretto a W pari a $f(X)$ di grado r, allora nella base $w, \varphi(w), \dots, \varphi^{r-1}(w)$ la matrice di φ (ristretta a W) è esattamente la matrice compagna $\mathrm{C}(f)$.

Se poi W è un sottospazio φ-ciclico con φ-generatore w e polinomio caratteristico di φ ristretto a W pari a $p(X)^s$ con $p(X)$ irriducibile di grado d, allora nella base $w, \varphi(w), \dots, \varphi^{ds-1}(w)$ la matrice di φ (ristretta a W) è la matrice compagna $\mathrm{C}(p^s)$, e nella base costruita nel seguente modo:

$$\begin{matrix} w & \varphi(w) & \varphi^2(w) & \cdots & \varphi^{d-1}(w) \\ p(\varphi)w & p(\varphi)\varphi(w) & p(\varphi)\varphi^2(w) & \cdots & p(\varphi)\varphi^{d-1}(w) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p(\varphi)^{s-1}w & p(\varphi)^{s-1}\varphi(w) & p(\varphi)^{s-1}\varphi^2(w) & \cdots & p(\varphi)^{s-1}\varphi^{d-1}(w) \end{matrix}$$

si ottiene una matrice a blocchi della forma

$$\mathrm{I}(p^s) = \begin{pmatrix} \mathrm{C}(p) & & & & \\ e_{1,d} & \mathrm{C}(p) & & & \\ & e_{1,d} & \mathrm{C}(p) & & \\ & & \ddots & \ddots & \\ & & & e_{1,d} & \mathrm{C}(p) \end{pmatrix} = \begin{pmatrix} 0 & -a_0 & & & & & & & \\ \mathbb{I} & -a_i & & & & & & & \\ & 1 & 0 & -a_0 & & & & & \\ & & \mathbb{I} & -a_i & & & & & \\ & & & 1 & 0 & -a_0 & & & \\ & & & & \mathbb{I} & -a_i & & & \\ & & & & & \ddots & \ddots & & \\ & & & & & & 1 & 0 & -a_0 \\ & & & & & & & \mathbb{I} & -a_i \end{pmatrix}$$

(blocchi diagonali sono le matrici compagne di $p(X)$, mentre i blocchi sottodiagonali sono matrici con un unico 1 nella posizione in alto a destra: in particolare tutta la sottodiagonale è composta di 1) che si dice la matrice ipercompagna del polinomio $p(X)^s$, e che si indica con $\mathrm{I}(p^s)$. In particolare si osservi che matrici compagna e ipercompagna di $p(X)^s$ sono simili tra loro: $\mathrm{C}(p^s) \sim \mathrm{I}(p^s)$ (con che matrice di cambiamento di base?).

7.1.10. Forma canonica razionale. Dal teorema di decomposizione in sottospazi φ-ciclici segue allora che *ogni endomorfismo ammette una base in cui la sua matrice si scrive a blocchi diagonali che sono matrici ipercompagne (o compagne) associate a polinomi del tipo $p(X)^s$ ove $p(X)$ sono i divisori irriducibili del polinomio caratteristico (o minimo). E naturalmente, ogni matrice è simile in $\Bbbk$ ad una matrice a blocchi diagonali che sono matrici ipercompagne (o compagne) associate a polinomi del tipo $p(X)^s$ ove $p(X)$ sono i divisori irriducibili del polinomio caratteristico (o minimo).*

Si osservi che nel caso in cui vi siano tutti gli autovalori di φ in $\Bbbk$, per esempio sempre per $\Bbbk$ algebricamente chiuso, allora la forma canonica razionale tramite ipercompagne è la forma canonica di Jordan (trasposta, veramente).

Si noti infine che le forme canoniche razionali dipendono dal corpo nel senso che una stessa matrice considerata a coefficienti in $\Bbbk$ o in qualche sotto (o sovra) corpo può avere forme canoniche razionali con blocchi diversi: dipende infatti dalla decomposizione in polinomi irriducibili, che può cambiare con estensioni di corpo.

7.2. Metodo della $\Bbbk[X]$-equivalenza (o equivalenza di Smith). Per le matrici a coefficienti polinomiali, cioè in $M_n(\Bbbk[X])$ possiamo definire l'equivalenza elementare come per le matrici a coefficienti in un corpo, tramite le tre operazioni elementari di Gauss su righe e colonne (ma l'operazione di moltiplicare una riga o una colonna per uno scalare si accetta solo per scalari invertibili, cioè per elementi di $\Bbbk^\times$).

D'altra parte possiamo definire la relazione di equivalenza usuale: $A(X)$ è equivalente a $B(X)$ se esistono $H(X), K(X) \in \mathrm{GL}_n(\Bbbk[X])$ (in particolare i loro determinanti sono in $\Bbbk^\times$) tali che $B(X) = H(X)A(X)K(X)$.

Siccome ogni matrice $H(X) \in \mathrm{GL}_n(\Bbbk[X])$ si scrive come prodotto di matrici elementari, le due nozioni di equivalenza coincidono; scriveremo $A(X) \approx B(X)$.

7.2.1. Relazione fondamentale tra similitudine in $\Bbbk$ e equivalenza in $\Bbbk[X]$. Il fatto fondamentale che motiva per noi lo studio della $\Bbbk[X]$-equivalenza di matrici è il seguente: *date $A, B \in M_n(\Bbbk)$, allora A è simile a B in $\Bbbk$ ($A \sim B$) se e solo se $X\mathbb{I} - A$ è equivalente a $X\mathbb{I} - B$ in $\Bbbk[X]$ ($X\mathbb{I} - A \approx X\mathbb{I} - B$). Cioè: due matrici sono simili in $\Bbbk$ se e solo se le loro matrici caratteristiche sono equivalenti in $\Bbbk[X]$.*

Una implicazione è ovvia: se A e B sono simili (in $\Bbbk$), allora $B = H^{-1}AH$ per $H \in \mathrm{GL}_n(\Bbbk)$, e di conseguenza abbiamo $X\mathbb{I} - B = H^{-1}(X\mathbb{I} - A)H$, per cui $X\mathbb{I} - A$ e $X\mathbb{I} - B$ sono simili in $\Bbbk[X]$ e a fortiori $X\mathbb{I} - A$ e $X\mathbb{I} - B$ sono equivalenti in $\Bbbk[X]$.

Per il viceversa bisogna lavorare con matrici polinomiali: supponiamo che

$$X\mathbb{I} - B = P(X)(X\mathbb{I} - A)Q(X)$$

con $P(X), Q(X) \in \mathrm{GL}_n(\Bbbk[X])$ (matrici polinomiali invertibili). Osserviamo che

$$P(X)^{-1}(X\mathbb{I} - B) = (X\mathbb{I} - A)Q(X) \qquad \text{e} \qquad (X\mathbb{I} - B)Q(X)^{-1} = P(X)(X\mathbb{I} - A)$$

e operiamo le divisioni (per matrici moniche in X , quindi funziona l'algoritmo di divisione euclidea nell'anello $M_n(\Bbbk[X]) = M_n(\Bbbk)[X]$, giustificare l'uguaglianza...)

$$P(X) = (X - B)P_1(X) + P_0 \qquad \text{e} \qquad Q(X) = Q_1(X)(X - B) + Q_0$$

con $P_0, Q_0 \in M_n(\Bbbk)$ (matrici di costanti) da cui possiamo ricavare

$$P_0 = P(X) - (X - B)P_1(X) \qquad \text{e} \qquad Q_0 = Q(X) - Q_1(X)(X - B)$$

e anche

$$\begin{aligned} &P_0(X - A) = \\ &= P(X)(X - A) - (X - B)P_1(X)(X - A) \\ &= (X - B)Q(X)^{-1} - (X - B)P_1(X)(X - A) \\ &= (X - B)(Q(X)^{-1} - P_1(X)(X - A)) \end{aligned} \quad \text{e} \quad \begin{aligned} &(X - A)Q_0 = \\ &= (X - A)Q(X) - (X - A)Q_1(X)(X - B) \\ &= P(X)^{-1}(X - B) - (X - A)Q_1(X)(X - B) \\ &= (P(X)^{-1} - (X - A)Q_1(X))(X - B) \end{aligned}$$

Dopo tutto questo possiamo calcolare:

$$\begin{aligned} &X - B = \\ &= P(X)(X - A)Q(X) = \\ &= ((X - B)P_1(X) + P_0)(X - A)(Q_1(X)(X - B) + Q_0) = \\ &= (X - B)P_1(X)(X - A)Q_1(X)(X - B) + (X - B)P_1(X)(X - A)Q_0 + P_0(X - A)Q_1(X)(X - B) + P_0(X - A)Q_0 = \\ &= (X - B)P_1(X)(X - A)Q_1(X)(X - B) + (X - B)P_1(X)(P(X)^{-1} - (X - A)Q_1(X))(X - B) \\ &\quad + (X - B)(Q(X)^{-1} - P_1(X)(X - A))Q_1(X)(X - B) + P_0(X - A)Q_0 = \\ &= (X - B)\Big(P_1(X)P(X)^{-1} - P_1(X)(X - A)Q_1(X) + Q(X)^{-1}Q_1(X)\Big)(X - B) + P_0(X - A)Q_0 \end{aligned}$$

da cui si deduce che la terribile espressione tra parentesi è nulla (altrimenti darebbe un termine di grado almeno 2 in X, rendendo impossibile l'uguaglianza), e siamo ridotti a

$$X - B = P_0(X - A)Q_0$$

che porta alla conclusione voluta poiché si ha subito $P_0Q_0 = \mathbb{I}$ (da $P_0XQ_0 = X$) e $B = P_0AQ_0$, e dunque A e B sono simili.

7.2.2. Classificazione per $\Bbbk[X]$-equivalenza in $M_n(\Bbbk[X])$ (fattori invarianti). *Ogni matrice $A(X) \in M_n(\Bbbk[X])$ è equivalente su $\Bbbk[X]$ ad una matrice diagonale della forma*

$$\begin{pmatrix} f_1(X) & & & & & \\ & f_2(X) & & & & \\ & & \ddots & & & \\ & & & f_r(X) & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$$

con $r = \mathrm{rk}A(X)$, e dove gli $f_i(X)$ sono polinomi monici tali che $f_i(X)$ divide $f_{i+1}(X)$ per ogni $i = 1, \dots, r-1$. Essi si chiamano i fattori invarianti di $A(X)$, e sono determinati unicamente dalla condizione $f_i(X) = \frac{d_i(X)}{d_{i-1}(X)}$ dove $d_i(X)$ è il massimo comun divisore di tutti i minori d'ordine i di $A(X)$.

In particolare, due matrici $A(X)$ e $B(X)$ in $M_n(\Bbbk[X])$ sono equivalenti se e solo se hanno gli stessi fattori invarianti.

La dimostrazione si ottiene per induzione su n (ordine della matrice) usando che $A(X)$ è equivalente in $\Bbbk[X]$ ad una matrice della forma

$$\begin{pmatrix} f_1(X) & 0 \\ 0 & A_1(X) \end{pmatrix}$$

dove $f_1(X)$ è polinomio monico e divide tutte le entrate di $A_1(X)$. Per fare ciò basta pigliare come $f_1(X)$ il polinomio monico di grado minimo tra tutte le entrate di tutte le matrici equivalenti ad $A(X)$; considerata poi una di queste matrici che abbia $f_1(X)$ in posizione iniziale, con operazioni elementari si cancellano tutti i termini della prima riga e della prima colonna.

Per l'asserzione di unicità, basta considerare che per tutte le matrici equivalenti tra loro, il MCD dei minori d'ordine i è costante (è invariante sulla classe di equivalenza). Perché?

7.2.3. Classificazione per $\Bbbk[X]$-equivalenza in $M_n(\Bbbk[X])$ (divisori elementari). *Se $f_1(X), f_2(X), \dots, f_r(X)$ sono i fattori invarianti di $A(X)$, scriviamone la decomposizione in polinomi irriducibili in $\Bbbk[X]$:*

$$\begin{aligned} f_1(X) &= p_1(X)^{e_{11}} p_2(X)^{e_{12}} \cdots p_s(X)^{e_{1s}} \\ f_2(X) &= p_1(X)^{e_{21}} p_2(X)^{e_{22}} \cdots p_s(X)^{e_{2s}} \\ &\cdots \\ f_r(X) &= p_1(X)^{e_{r1}} p_2(X)^{e_{r2}} \cdots p_s(X)^{e_{rs}} \end{aligned}$$

dove per ogni fissato i abbiamo $e_{j+1,i} \geqslant e_{ji}$ (per la divisibilità dei fattori invarianti. I polinomi $p_i(X)^{e_{ij}}$ sono determinati dai fattori invarianti, e a loro volta li determinano senza ambiguità; si chiamano i divisori elementari di $A(X)$.

Possiamo quindi concludere che due matrici $A(X)$ e $B(X)$ in $M_n(\Bbbk[X])$ sono equivalenti se e solo se hanno gli stessi divisori elementari.

7.2.4. Applicazioni alla similitudine in $\Bbbk$. Possiamo allora ritornare alle matrici $A, B \in M_n(\Bbbk)$. Da quanto visto abbiamo che A e B sono simili (su $\Bbbk$) se e solo se le loro matrici caratteristiche $X - A$ e $X - B$ (sono equivalenti su $\Bbbk[X]$, cioè) hanno gli stessi fattori invarianti, oppure se e solo se hanno gli stessi divisori elementari.

Data $A \in M_n(\Bbbk)$, la matrice caratteristica ha comunque rango n; se i fattori invarianti sono $f_1(X), f_2(X), \dots, f_n(X)$, allora abbiamo $p_A(X) = f_1(X) f_2(X) \cdots f_n(X)$ (il polinomio caratteristico è il prodotto dei fattori invarianti), e $m_A(X) = f_n(X)$ (il polinomio minimo è l'ultimo dei fattori invarianti).

In particolare, se $f(X)$ è polinomio monico, allora la sua matrice compagna $\mathrm{C}(f)$ ha matrice caratteristica $X - \mathrm{C}(f)$ con fattori invarianti $1, \dots, 1, f(X)$, cioè è equivalente alla matrice $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & f(X) \end{pmatrix}$.

Problema: in generale i fattori invarianti della matrice caratteristica sono divisori del polinomio minimo della matrice data: che cosa rappresentano per la matrice stessa?

7.2.5. Forma canonica razionale (fattori invarianti). *Se $A \in M_n(\Bbbk)$ ha matrice caratteristica $X - A$ con fattori invarianti $1, \dots, 1, f_1(X), f_2(X), \dots, f_r(X)$, allora A è simile su $\Bbbk$ ad una matrice con blocchi diagonali $\mathrm{C}(f_i)$ (matrici compagne dei fattori invarianti).*

Infatti basta osservare le seguenti equivalenze:

$$X - \begin{pmatrix} \mathrm{C}(f_1) & & \\ & \ddots & \\ & & \mathrm{C}(f_r) \end{pmatrix} = \begin{pmatrix} X-\mathrm{C}(f_1) & & \\ & \ddots & \\ & & X-\mathrm{C}(f_r) \end{pmatrix} \approx \begin{pmatrix} 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & f_1(X) & & & & & & \\ & & & & \ddots & & & & & \\ & & & & & 1 & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & 1 & & \\ & & & & & & & & f_r(X) & \end{pmatrix} \approx \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & f_1(X) & & \\ & & & & \ddots & \\ & & & & & f_r(X) \end{pmatrix} \approx X - A$$

da cui la conclusione. La seconda equivalenza si ottiene facilmente controllando i MCD dei minori d'odini successivi.

7.2.6. Forma canonica razionale (divisori elementari). *Se $A \in M_n(\Bbbk)$ ha matrice caratteristica $X - A$ con divisori elementari $p_i(X)^{e_{ij}}$, allora A è simile su $\Bbbk$ ad una matrice con blocchi diagonali $\mathrm{C}(p_i^{e_{ij}})$ (matrici compagne dei divisori elementari).*

Infatti, in base al risultato precedente, basta dimostrare che se $f(X) = p_1(X)^{e_1} \cdots p_s(X)^{e_s}$, allora $\mathrm{C}(f)$ è simile su $\Bbbk$ alla matrice con blocchi diagonali $\mathrm{C}(p_1^{e_1}), \dots, \mathrm{C}(p_s^{e_s})$. Questo si verifica in base alle

equivalenze seguenti:

$$X-\begin{pmatrix} \mathrm{C}(p_1^{e_1}) & & \\ & \ddots & \\ & & \mathrm{C}(p_s^{e_s}) \end{pmatrix} = \begin{pmatrix} X-\mathrm{C}(p_1^{e_1}) & & \\ & \ddots & \\ & & X-\mathrm{C}(p_s^{e_s}) \end{pmatrix} \approx \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & p_1(X)^{e_1} & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \\ & & & & & & & & p_s(X)^{e_s} \end{pmatrix} \approx \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & f(X) \end{pmatrix} \approx X-\mathrm{C}(f)$$

(la seconda equivalenza si ottiene facilmente controllando i MCD dei minori d'odini successivi).

È interessante anche trovare il cambiamento di base per la similitudine delle due matrici dette, e si ottiene così: se v è vettore tale che $v, \varphi v, \dots$ è base in cui φ ha matrice $\mathrm{C}(f)$, allora posto $f_i(X) = f(X)/p_i(X)^{e_i}$ definiamo i vettori $v_i = f_i(\varphi)v$ e la base data da

$$v_1, \varphi v_1, \dots, v_2, \varphi v_2, \dots, v_s, \varphi v_s, \dots$$

è tale che φ ottiene la matrice a blocchi diagonali $\mathrm{C}(p_i^{e_i})$.

7.2.7. Forma canonica razionale (divisori elementari). *Se $A \in M_n(\Bbbk)$ ha matrice caratteristica $X - A$ con divisori elementari $p_i(X)^{e_{ij}}$, allora A è simile su $\Bbbk$ ad una matrice con blocchi diagonali $\mathrm{I}(p_i^{e_{ij}})$ (matrici ipercompagne dei fattori invarianti).* Infatti, in base al risultato precedente, basta dimostrare che matrici compagna e ipercompagna di $p(X)^e$ sono simili tra loro, e questo segue subito dalle seguenti equivalenze:

$$X - \mathrm{I}(p^e) = X - \begin{pmatrix} \mathrm{C}(p) & & & \\ e_{1s} & \mathrm{C}(p) & & \\ & \ddots & \ddots & \\ & & e_{1s} & \mathrm{C}(p) \end{pmatrix} \approx \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & p(X)^e \end{pmatrix} \approx X - \mathrm{C}(p^e)$$

(nell'unica non banale, si osservi che cancellando prima riga e prima colonna si ottiene una matrice con diagonale unitaria...).

Da qualche parte abbiamo visto in effetti il cambiamento di base corrispondente a questa similitudine.

7.2.8. Capire le relazioni tra forma canonica razionale su un campo $\Bbbk$ e forma di Jordan sulla chiusura algebrica di $\Bbbk$. In particolare, qual è il significato di fattori invarianti e di divisori elementari per le matrici di Jordan?

8. Esercizi.

8.1. Esercizi su Autoteoria.

8.1.1. Verificare che 0, 1 e -1 sono autovalori della matrice reale $A = \begin{pmatrix} -3 & 5 & 1 & 1 \\ -1 & 0 & -1 & 1 \\ 0 & 3 & 2 & -1 \\ -3 & 6 & 1 & 1 \end{pmatrix}$.
Determinare gli autospazi relativi. La matrice A è simile ad una matrice diagonale?

8.1.2. Sia A una matrice quadrata $n \times n$. Verificare che A è non singolare (cioè invertibile) se e solo se 0 non è un autovalore di A.

A si dice nilpotente se e solo se esiste k tale che $A^k = 0$. Verificare che A è nilpotente se e solo se il polinomio caratteristico di A è X^n (sugg.: come risulta il polinomio minimo?).

8.1.3. Sia A una matrice quadrata in $M_n(\Bbbk)$ e α un autovalore di A. Allora α^k è autovalore di A^k (per ogni $k \in \mathbb{N}$). È vero il "viceversa" (se α^k è autovalore di A^k per qualche k...)?

8.1.4. Sia A una matrice quadrata in $M_n(\Bbbk)$ e α un autovalore di A. Se $f(x)$ è un polinomio in $\Bbbk[x]$, allora $f(\alpha)$ è un autovalore di $f(A)$.

Se A è invertibile, allora α^{-1} è un autovalore di A^{-1}. Mostrare che gli autovalori di A^{-1} sono gli inversi degli autovalori di A, esattamente con la stessa molteplicità.

8.1.5. Sia A una matrice quadrata in $M_n(\Bbbk)$, supponiamo $\lambda_1, \dots, \lambda_n$ i suoi autovalori. Discutere autovalori e autovettori della matrice dei complementi algebrici.

8.1.6. Sia A una matrice quadrata in $M_n(\Bbbk)$. Mostrare che se A è diagonalizzabile (risp. triangolarizzabile) allora A^k è diagonalizzabile (risp. triangolarizzabile) (per ogni $k \in \mathbb{N}$). È vero il "viceversa" (se A^k è diagonalizzabile per qualche k...)?

8.1.7. Sia $\mathfrak{S}_n$ il gruppo simmetrico su $\{1, \dots, n\}$. Per ogni $\sigma \in \mathfrak{S}_n$ sia φ_σ l'unico automorfismo di $\mathbb{R}^n$ tale che $\varphi_\sigma(e_i) = e_{\sigma(i)}$ per ogni $i = 1, \dots, n$, dove $\{e_1, \dots, e_n\}$ è la base canonica di $\mathbb{R}^n$. Si tratta di morfismi diagonalizzabili su $\mathbb{R}$? E su $\mathbb{C}$? (*Sugg.: decomporre σ in cicli*).

Se invece $\Bbbk$ è corpo di caratteristica p, ed usiamo $n = p$, allora un ciclo σ induce un morfismo φ_σ che non è diagonalizzabile.

8.1.8. Sia A una matrice quadrata in $M_n(\Bbbk)$. Determinare la relazione tra il polinomio caratteristico $p_A(X)$ di A e il polinomio caratteristico $p_{\alpha A}(X)$ di αA ove $\alpha \in \Bbbk$ e $\alpha \neq 0$.

8.1.9. Sia A una matrice quadrata in $M_n(\mathbb{C})$. Mostrare che $p_{A^k}(X^k) = \prod_\omega p_{\omega A}(X)$ ove il prodotto è indiciato dalle radici k-esime di 1.

In particolare $p_{A^2}(X^2) = p_A(X)p_{-A}(X)$.

8.1.10. Discutere la diagonalizzabilità su $\mathbb{R}$ e su $\mathbb{C}$ di matrici reali A d'ordine 2. In particolare, distinguere i seguenti casi:

(a) $\operatorname{tr}(A)^2 - 4\det(A) > 0$,
(b) $\operatorname{tr}(A)^2 - 4\det(A) = 0$,
(c) $\operatorname{tr}(A)^2 - 4\det(A) < 0$.

($\operatorname{tr}(A)$ indica la traccia di A, ovvero la somma degli elementi diagonali).

8.1.11. Calcolare autovalori, molteplicità e nullità, autospazi per le seguenti matrici:

$$\begin{pmatrix} 5 & -3 & 2 \\ 6 & -4 & 4 \\ 4 & -4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 7 & -12 & 6 \\ 10 & -19 & 10 \\ 12 & -24 & 13 \end{pmatrix}, \quad \begin{pmatrix} 4 & -5 & 7 \\ 1 & -4 & 9 \\ -4 & 0 & 5 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}.$$

Quali sono diagonalizzabili? Quali triangolarizzabili?

8.1.12. Calcolare autovalori, molteplicità e nullità, autospazi per le seguenti matrici:

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 2 & 0 & 2 \\ -2 & 0 & 0 & -2 \\ 0 & 0 & 2 & 0 \\ -2 & -2 & 0 & -4 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & -3 & 0 \\ 0 & 5 & 0 & 3 \\ 3 & 0 & -4 & 0 \\ 2 & 0 & 2 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 2 & 0 & -1 & 0 \\ 2 & 3 & 1 & 1 \\ 1 & 0 & 4 & 0 \\ -1 & 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 3 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & -2 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ -4 & -4 & 1 & -4 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Quali sono diagonalizzabili? Quali triangolarizzabili?

8.1.13. Studiare per quali valori dei parametri le seguenti matrici sono diagonalizzabili:

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 2 & 0 \\ a & 0 & 1-a \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 1 & a & b \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & a \\ a & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & a^2 & -1 \\ 0 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ ab & b^2 & bc \\ ac & bc & c^2 \end{pmatrix}.$$

8.1.14. Studiare per quali valori del parametro la matrice $\begin{pmatrix} 1 & 2 & a^2-a & a \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$ è diagonalizzabile.

8.1.15. Calcolare il polinomio caratteristico delle seguenti matrici

$$\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & c \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & a \\ 1 & 0 & 0 & b \\ 0 & 1 & 0 & c \\ 0 & 0 & 1 & d \end{pmatrix}, \quad \begin{pmatrix} 0 \cdots 0 & a_0 \\ & a_1 \\ \mathbb{I}_{n-1} & \vdots \\ & a_{n-1} \end{pmatrix}.$$

Dedurne che ogni polinomio monico è polinomio caratteristico di qualche matrice.

8.1.16. Una matrice reale d'ordine 2 ha un solo autovalore (di molteplicità 2). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

8.1.17. Una matrice reale d'ordine 3 ha un solo autovalore (di molteplicità 3). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

8.1.18. Una matrice reale d'ordine 3 ha due autovalori distinti (uno dei quali di molteplicità 2). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

8.1.19. Una matrice reale d'ordine 4 ha un solo autovalore (di molteplicità 4). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

8.1.20. Una matrice reale d'ordine 4 ha due autovalori distinti (uno dei quali di molteplicità 3). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

8.1.21. Una matrice reale d'ordine 4 ha due autovalori distinti (ciascuno dei quali di molteplicità 2). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

8.1.22. Calcolare polinomio caratteristico e discutere la diagonalizzabilità per le matrici

$$\begin{pmatrix} 0 & c & 0 & \cdots & 0 \\ 0 & 0 & c & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & c \\ c & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 2 & 0 & \cdots & 0 \\ 1 & 2 & 3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

d'ordine n.

8.1.23. Si diano se possibile esempi di matrici reali d'ordine 2 tali che:
(a) siano prive di autovalori reali;
(b) abbiano un solo autovalore reale.
Se ne discuta eventualmente la diagonalizzabilità.

8.1.24. Si diano se possibile esempi di matrici reali d'ordine 3 tali che:
(a) siano prive di autovalori reali;
(b) abbiano un solo autovalore reale;
(c) abbiano due soli autovalori reali.
Se ne discuta eventualmente la diagonalizzabilità.

8.1.25. Si diano se possibile esempi di matrici reali d'ordine 4 tali che:
(a) siano prive di autovalori reali;
(b) abbiano un solo autovalore reale;
(c) abbiano due soli autovalori reali.

(d) abbiano tre soli autovalori reali.
Se ne discuta eventualmente la diagonalizzabilità.

8.1.26. Si consideri la matrice reale A_n d'ordine n avente entrate $a_{i,j}$ uguali a 1 se $j = n - i + 1$, e nulle altrimenti.
(a) Determinare polinomi caratteristico e minimo per $n = 2, 3$, e discutere la diagonalizzabilità.
(b) Determinare polinomi caratteristico e minimo per $n = 4, 5$, e discutere la diagonalizzabilità.
(c) Determinare polinomi caratteristico e minimo per $n \geqslant 6$, e discutere la diagonalizzabilità.
(d) È vero che si tratta di matrici in base canonica di simmetrie ortogonali? Quali simmetrie ortogonali ammettono matrici di questo tipo (in qualche base)?

8.1.27. Calcolare i determinanti delle seguenti due matrici: $\begin{pmatrix} 0 & b_1 \\ a_1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & b_1 & 0 \\ a_1 & 0 & b_2 \\ 0 & a_2 & 0 \end{pmatrix}$.
Si considerino ora le matrici di ordine n date da:

$$A_n = \begin{pmatrix} 0 & b_1 & 0 & 0 & \cdots & 0 \\ a_1 & 0 & b_2 & 0 & \cdots & 0 \\ 0 & a_2 & 0 & b_3 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & b_{n-1} \\ 0 & 0 & 0 & \cdots & a_{n-1} & 0 \end{pmatrix}$$

(termini eventualmente non nulli solamente sopra e sotto la diagonale principale).
(b) Calcolare il valore dei determinanti di A_4 e A_5.
(c) Si trovi e si dimostri una espressione generale per il determinante delle matrici A_n per ogni $n \in \mathbb{N}$.
(d) Si trovi e si dimostri una espressione ricorsiva per il polinomio caratteristico $p_{A_n}(X)$ delle matrici A_n per ogni $n \in \mathbb{N}$. È vero o falso che il coefficiente di X^{n-1} in $p_{A_n}(X)$ è sempre nullo?

8.1.28. Sia A una matrice reale d'ordine n, e supponiamo che $\lambda \in \mathbb{R}$ sia autovalore dell'applicazione $\varphi_A : \mathbb{R}^n \to \mathbb{R}^n$ definita da $\varphi_A(v) = Av$. Mostrare che λ è anche autovalore dell'applicazione $\psi_A : \mathbb{C}^n \to \mathbb{C}^n$ definita da $\psi_A(v) = Av$, e che le dimensioni degli autospazi relativi a λ sono uguali, cioè $\dim_{\mathbb{R}} V_\varphi(\lambda) = \dim_{\mathbb{C}} V_\psi(\lambda)$. Qual è la dimensione di $V_\psi(\lambda)$ come spazio vettoriale su $\mathbb{R}$?

8.1.29. Sia A una matrice quadrata tale che $A^2 = \mathbb{I}$. Dimostrare che A è diagonalizzabile e che i suoi autovalori sono solo 1 oppure -1. Se B è una matrice quadrata della stessa dimensione di A e se $B^2 = \mathbb{I}$, allora A e B sono simili se e solo se hanno la stessa molteplicità dell'autovalore 1.

8.1.30. Sia A una matrice quadrata tale che $A^2 = A$. Dimostrare che A è diagonalizzabile e che i suoi autovalori sono solo 0 oppure 1. Se B è una matrice quadrata della stessa dimensione di A e se $B^2 = B$, allora A e B sono simili se e solo se hanno lo stesso rango.

8.1.31. Sia A una matrice quadrata tale che $A^3 = A$.
(a) Dimostrare che A è diagonalizzabile e che i suoi autovalori sono solo 0, 1 oppure -1.
(b) Sia B una matrice quadrata della stessa dimensione di A e $B^3 = B$; scrivere e dimostrare un criterio, basato sul rango e sulle molteplicità degli autovalori, affinché A e B siano simili.
(c) Dire quante matrici diagonali non equivalenti tra loro esistono per le matrici $n \times n$ soddisfacenti all'ipotesi dell'esercizio.
(d) Per i casi $n = 2, 3$ controllare il risultato precedente elencando tutte le possibili matrici in questione.

8.1.32. Sia A una matrice quadrata $n \times n$ a coefficienti reali tale che $A^3 = \mathbb{I}_n$.
(a) Dire se A è necessariamente diagonalizzabile nel corpo $\mathbb{C}$ dei numeri complessi;
(b) Dire se A è necessariamente diagonalizzabile nel corpo $\mathbb{R}$ dei numeri reali; è vero che ha 1 come unico autovalore reale?
(c) Discutere il caso della matrice reale $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}$; è diagonalizzabile su $\mathbb{C}$? Lo è su $\mathbb{R}$?

8.1.33. Sia A una matrice quadrata a coefficienti nel campo $\mathbb{R}$ dei numeri reali e tale che $A^3 = 2A$.
(a) Dire se A è necessariamente diagonalizzabile su $\mathbb{R}$.
(b) Elencare tutti i possibili autovalori di A in $\mathbb{R}$.

(c) Dimostrare che se A è a coefficienti nel campo $\mathbb{Q}$ dei numeri razionali, essa è diagonalizzabile su $\mathbb{Q}$ se e solo se A è la matrice nulla.

8.1.34. Sia A una matrice quadrata a coefficienti nel campo $\mathbb{C}$ dei numeri complessi e tale che $A^3 = -A$.
(a) Dire se A è necessariamente diagonalizzabile su $\mathbb{C}$.
(b) Elencare tutti i possibili autovalori di A in $\mathbb{R}$, il campo dei numeri reali.
(c) Dimostrare che se A è a coefficienti in $\mathbb{R}$, essa è diagonalizzabile su $\mathbb{R}$ se e solo se A è la matrice nulla.

8.1.35. Sia A una matrice quadrata tale che $A^3 = A^2$.
(a) Dire se A è necessariamente diagonalizzabile; se no, dare un esempio di matrice non diagonalizzabile soddisfacente all'ipotesi detta.
(b) In ogni caso dimostrare che gli autovalori di A sono solo 0 oppure 1.
(c) È vero o falso che A è diagonalizzabile se e solo se il suo rango coincide con la molteplicità geometrica dell'autovalore 1? Sia B una matrice quadrata dello stesso ordine di A e $B^3 = B^2$; scrivere e dimostrare un criterio, basato sul rango e sulle molteplicità degli autovalori, affinché A e B siano simili.

8.1.36. Diagonalizzare simultaneamente, se possibile, le due matrici

$$A = \begin{pmatrix} 2 & -1 & -1 \\ 0 & 3 & 1 \\ 0 & 1 & 3 \end{pmatrix} \qquad B = \begin{pmatrix} 3 & 0 & 1 \\ -1 & 2 & -1 \\ 1 & 0 & 3 \end{pmatrix}$$

e trovare la trasformazione lineare che le diagonalizza.

8.1.37. Se due endomorfismi φ e ψ sono diagonalizzabili e commutano tra loro, allora $\psi \circ \varphi$ è diagonalizzabile. È vero in generale che il composto di due morfismi diagonalizzabili è diagonalizzabile? E per la somma di due endomorfismi?

8.1.38. Sia f l'endomorfismo di $\mathbb{R}^4$ di matrice $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -2 & -1 & 2 \\ 1 & 0 & 2 & -1 \\ -3 & -3 & 0 & 2 \end{pmatrix}$ rispetto alla base canonica. Determinare il sottospazio massimo X di $\mathbb{R}^4$ ove f coincide con l'applicazione identica. Il sottospazio X ha un complemento f-invariante?

Sia $W = \ker(f-1)^2$. Verificare che W ha un complemento f-invariante Z, e determinare Z. Il sottospazio Z è unico?

8.1.39. Sia f l'endomorfismo di $\mathbb{R}^4$ di matrice $A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ \sqrt{2} & -\sqrt{2} & 0 & -\sqrt{2} \\ 0 & 0 & 2 & 0 \\ 2+\sqrt{2} & \sqrt{2} & 0 & -\sqrt{2} \end{pmatrix}$ rispetto alla base canonica. Verificare che esistono sottospazi f-invarianti di $\mathbb{R}^4$ di dimensione 2 e determinarli tutti.

8.1.40. Se A e B sono matrici quadrate dello stesso ordine, e $B = H^{-1}AH$ (con H invertibile), allora si ha che $B^n = H^{-1}A^nH$. Questo può essere utile per semplificare il calcolo delle potenze di una matrice: studiare il caso di matrice diagonalizzabile.

8.1.41. La successione di Fibonacci è definita da $x_0 = 1$, $x_1 = 1$ e poi ricorsivamente da $x_{n+1} = x_n + x_{n-1}$ (si tratta della crescita di una popolazione di conigli immortali, che ogni anno cresce di un numero di individui pari al numero di individui della popolazione dell'anno precedente). Scrivere i primi numeri della successione. Determinare una formula chiusa, cioè non ricorsiva, che dia x_n in funzione di n.

Suggerimento: il processo di generazione dei numeri si può rappresentare tramite la trasformazione lineare $\left(\begin{smallmatrix} x_n \\ x_{n-1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} x_{n-1} \\ x_{n-2} \end{smallmatrix}\right)$ e iterando il procedimento: $\left(\begin{smallmatrix} x_n \\ x_{n-1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{n-1}\left(\begin{smallmatrix} x_1 \\ x_0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{n}\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ per cui si tratta di calcolare la potenza n-sima di una matrice, che risulta diagonalizzabile: detti $\alpha_\pm = \frac{1\pm\sqrt{5}}{2}$ le radici del polinomio caratteristico, risulta che $\left(\begin{smallmatrix} \alpha_\pm \\ 1 \end{smallmatrix}\right)$ sono gli autovettori, e $x_n = \frac{\alpha_+^{n+1} - \alpha_-^{n+1}}{\alpha_+ - \alpha_-}$ (ma $\sqrt{5}$ deve sparire dalle formule: gli x_n sono interi).

Più in generale, discutere la diagonalizzabilità su $\mathbb{R}$ della matrice della forma $\left(\begin{smallmatrix} b & a \\ 1 & 0 \end{smallmatrix}\right)$, e la sua relazione con formule esplicite per un problema analogo a quello di Fibonacci.

8.1.42. Idem per le matrici $\begin{pmatrix} c & b & a \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ e $\begin{pmatrix} d & c & b & a \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

8.1.43. Sia d_n il determinante della matrice d'ordine n avente entrate non nulle solo sulla diagonale principale (tutte uguali a b), immediatamente sopra la diagonale principale (tutte uguali ad a) e immediatamente sotto (tutte uguali a c); queste matrici e i loro determinanti si dicono trigonanti. Si proceda scoprendo d_1, d_2 e la relazione ricorsiva $d_n = bd_{n-1} - acd_{n-2}$, ragionando poi come nel caso di Fibonacci. I numeri di Fibonacci sono un caso particolare di d_n? Sperimentare con $a = 1$, $b = 3$, $c = 2$.

8.1.44. Studiare i processi di Markov associati alle seguenti matrici, determinando in particolare il comportamento al limite (cioè il limite per n infinito delle potenze n-sime):

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1/2 & 1/3 \\ 1/2 & 2/3 \end{pmatrix}, \quad \begin{pmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{pmatrix},$$

$$\begin{pmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 \\ 1/2 & 0 & 1/2 \end{pmatrix}, \quad \begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 1/3 & 1/3 & 1/3 \\ 1/4 & 1/4 & 1/2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1/4 & 1/2 \\ 1/2 & 1/2 & 1/2 \\ 1/2 & 1/4 & 0 \end{pmatrix}.$$

8.1.45. Sia $G = \mathrm{SL}(2, \mathbb{R}) := \{X \in M_2(\mathbb{R}) : \det(X) = 1\}$. Mostrare che:

(a) se $|\mathrm{tr}\,(X)| > 2$ allora esiste $U \in G$ tale che $UXU^{-1} = \left(\begin{smallmatrix} t & 0 \\ 0 & 1/t \end{smallmatrix}\right)$ con $t \in \mathbb{R} \smallsetminus \{-1, 0, 1\}$ (caso iperbolico);

(b) se $|\mathrm{tr}\,(X)| < 2$ allora esiste $U \in G$ tale che $UXU^{-1} = \left(\begin{smallmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{smallmatrix}\right)$ con $t \in \mathbb{R}$ (caso ellittico);

(c) se $X \neq \pm\mathbb{I}_2$ e $|\mathrm{tr}\,(X)| = 2$ allora esiste $V \in G$ tale che $VXV^{-1} \in \{\pm\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \pm\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)\}$ (caso parabolico);

(d) per ogni $X \in G$ esistono uniche due matrici $U \in K$ e $V \in T$ tali che $X = UV$ ove

$$K := \{\left(\begin{smallmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{smallmatrix}\right) : t \in \mathbb{R}\} \qquad \text{e} \qquad T := \{\left(\begin{smallmatrix} u & v \\ 0 & 1/u \end{smallmatrix}\right) : u, v \in \mathbb{R},\ u > 0\}$$

sono sottogruppi di G. Dedurre che allora possiamo supporre $U \in K$ in (b), e $V \in T$ in (c).

8.1.46. Sia $G = \mathrm{SL}(2, \mathbb{C}) := \{X \in M_2(\mathbb{C}) : \det(X) = 1\}$. Mostrare che:

(a) se $\mathrm{tr}\,(X) \neq \pm 2$ allora esiste $U \in G$ tale che $UXU^{-1} = \left(\begin{smallmatrix} t & 0 \\ 0 & 1/t \end{smallmatrix}\right)$ con $t \in \mathbb{C} \smallsetminus \{-1, 0, 1\}$;

(b) se $X \neq \pm\mathbb{I}_2$ e $\mathrm{tr}\,(X) = 2$ (risp. $= -2$) allora esiste $V \in G$ tale che $VXV^{-1} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ (risp. $= \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$);

(c) per ogni $X \in G$ esistono uniche due matrici $U \in K$ e $V \in T$ tali che $X = UV$ ove

$$K := \{\left(\begin{smallmatrix} u & -\overline{v} \\ v & \overline{u} \end{smallmatrix}\right) : u, v \in \mathbb{C},\ |u|^2 + |v|^2 = 1\} \qquad \text{e} \qquad T := \{\left(\begin{smallmatrix} a & b \\ 0 & 1/a \end{smallmatrix}\right) : a, b \in \mathbb{R},\ a, b > 0\}$$

sono sottogruppi di G.

8.1.47. Matrici Magiche. Da non confondere con i quadrati magici: qui non si chiede nulla sulle diagonali!

(1) Una matrice $M \in M_n(\Bbbk)$ si dice magica se le somme dei termini di ogni riga e di ogni colonna sono tutte uguali; in tal caso tale somma si indica con $s(M)$ e si chiama costante magica di M.

(2) Verificare che se M è magica, allora $s(M)$ è sempre autovalore di M (autovettori?).

(3) Verificare che M è magica se e solo se il vettore $\Sigma_i e_i \in \Bbbk^n$ avente tutte coordinate 1 è autovettore di M ed M^{t} con lo stesso autovalore.

(4) Sia $\mathrm{Mg}_n(\Bbbk)$ l'insieme delle matrici magiche in $M_n(\Bbbk)$. Mostrare che $\mathrm{Mg}_n(\Bbbk)$ è sotto-$\Bbbk$-algebra di $M_n(\Bbbk)$, cioè è chiuso per somma, opposto, prodotto, inversione, contiene le matrici nulla e identica. Inoltre mostrare che $M \mapsto s(M)$ è morfismo di $\Bbbk$-algebre $\mathrm{Mg}_n(\Bbbk) \to \Bbbk$.

(5) Quanto vale la dimensione su $\Bbbk$ di $\mathrm{Mg}_n(\Bbbk)$? Quali matrici diagonali sono magiche?

(6) Sia $\mathrm{Mg}_n^0(\Bbbk)$ l'insieme delle matrici magiche di costante magica nulla, cioè il nucleo di $s : \mathrm{Mg}_n(\Bbbk) \to \Bbbk$. Mostrare che le matrici in $\mathrm{Mg}_n^0(\Bbbk)$ hanno determinante nullo. È vero il viceversa? Cioè: matrici magiche di determinate nullo hanno costante magica nulla?

(7) Sia $\mathrm{GLMg}_n(\Bbbk) = \mathrm{Mg}_n(\Bbbk) \cap \mathrm{GL}_n(\Bbbk)$ l'insieme delle matrici magiche invertibili. Mostrare che le matrici in $\mathrm{GLMg}_n(\Bbbk)$ hanno costante magica non nulla. È vero il viceversa? Cioè: matrici magiche con costante magica non nulla sono invertibili?
(8) È vero o falso che la magia è stabile per coniugio? Cioè: se M è magica, è vero che $H^{-1}MH$ è magica per ogni H invertibile? Eventualmente, per quali H ciò succede?
(9) Nella classe di coniugio di una fissata matrice $A \in M_n(\Bbbk)$, è vero o falso che si trovano sempre matrici magiche? Eventualmente, sotto quali condizioni è vero?
(10) Dato un endomorfismo φ di uno spazio vettoriale V di dimensione finita su $\Bbbk$, è vero o falso che esistono basi $\mathscr{V}$ di V tali che $\alpha_{\mathscr{V}}(\varphi)$ è magica? Eventualmente, sotto quali condizioni è vero?

8.2. Esercizi su Jordan.

8.2.1. Sia f l'endomorfismo di $\mathbb{R}^4$ che, con riferimento alla base canonica (e_1, e_2, e_3, e_4), ha matrice $A = \begin{pmatrix} 2 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.
(a) Determinare il polinomio caratteristico ed il polinomio minimo di f.
(b) Determinare una matrice di Jordan J per f e trovare una base di $\mathbb{R}^4$ rispetto cui f è rappresentata da J.
(c) È vero che esistono vettori u, v, w di $\mathbb{R}^4$, tali che $(u, v, w, f(v) - v)$ sia una base di $\mathbb{R}^4$? Nel caso affermativo si espliciti una tale base e si scriva la matrice di f rispetto ad essa. Si tratta di una matrice di Jordan?

8.2.2. Per ognuna delle seguenti matrici, sia f l'endomorfismo di $\mathbb{R}^4$ che, con riferimento alla base canonica (e_1, e_2, e_3, e_4), ha quella matrice: $A_1 = \begin{pmatrix} 4 & 0 & 6 & 12 \\ 1 & 0 & 0 & 3 \\ 0 & 0 & -2 & 0 \\ 2 & 0 & 0 & 6 \end{pmatrix}$, $A_2 = \begin{pmatrix} 1 & 0 & 0 & 5 \\ 0 & 4 & 0 & 0 \\ 3 & 8 & 0 & 15 \\ -2 & 0 & 0 & -10 \end{pmatrix}$.
(a) Determinare il polinomio caratteristico ed il polinomio minimo di f.
(b) Determinare una matrice di Jordan J per f.
(c) Trovare una base di $\mathbb{R}^4$ rispetto cui f è rappresentata da J.

8.2.3. Sia φ l'endomorfismo di $\mathbb{C}^4$ di matrice $A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ -4 & 2 & -4 & -3 \\ 4 & 0 & 5 & 3 \\ -3 & 0 & -2 & 0 \end{pmatrix}$ rispetto alla base canonica di $\mathbb{C}^4$.
(a) Determinare il polinomio minimo e la forma di Jordan di φ.
(b) Trovare una base di $\mathbb{C}^4$ rispetto cui la matrice di φ è in forma di Jordan.
(c) Determinare la forma di Jordan dell'endomorfismo $(\varphi - a)^2$, al variare di a in $\mathbb{C}$.

8.2.4. Sia φ l'endomorfismo di $\mathbb{R}^4$ rappresentato dalla matrice $A = \begin{pmatrix} 4 & 0 & -1 & 1 \\ 0 & 4 & -1 & 1 \\ 0 & 1 & 6 & -2 \\ 0 & 1 & 2 & 2 \end{pmatrix}$ rispetto alla base canonica.
(a) Calcolare il polinomio minimo e il polinomio caratteristico di φ.
(b) Determinare la forma di Jordan di φ.
(c) Trovare una base di $\mathbb{R}^4$ rispetto cui la matrice di φ assume la forma di Jordan.
(d) Rispondere ai punti a, b e c relativamente all' endomorfismo $\eta = (\varphi - 4)^2$ di $\mathbb{R}^4$.

8.2.5. Sia φ l'endomorfismo di $\mathbb{C}^4$ di matrice $A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ -1 & 2 & 0 & 0 \\ -1 & 1 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{pmatrix}$ rispetto alla base canonica $(e_1, \dots, e_4)$.
(a) Si scriva il polinomio minimo di φ ed una matrice di Jordan J per φ.
(b) Trovare una base di $\mathbb{C}^4$ rispetto cui la matrice di φ è J.

(c) Mostrare tutte le matrici B di $M_4(\mathbb{C})$ tali che $\mathrm{rk}(B) = 4$, $\mathrm{rk}(B-1) = 2$, $\mathrm{rk}(B-1)^2 = 1$, $\mathrm{rk}(B-1)^3 = 0$, sono simili ad A.

8.2.6. Sia φ l'endomorfismo di $\mathbb{C}^4$ che, con riferimento alla base canonica (e_1, e_2, e_3, e_4) di $\mathbb{C}^4$, ha matrice $A = \begin{pmatrix} -2 & 0 & -1 & 0 \\ 6 & -2 & 2 & -1 \\ 0 & 0 & -2 & 0 \\ -4 & 0 & 3 & -2 \end{pmatrix}$.

(a) Determinare il polinomio caratteristico ed il polinomio minimo di φ.
(b) Determinare una matrice di Jordan J per φ e trovare una base di $\mathbb{C}^4$ rispetto cui φ è rappresentata da J.
(c) Esistono una matrice B in $M_3(\mathbb{C})$ ed uno scalare α in $\mathbb{C}$ tale che B e $(A-\alpha)^2$ hanno lo stesso polinomio minimo?

8.2.7. Sia φ l'endomorfismo di $\mathbb{C}^4$ la cui matrice rispetto alla base canonica è $A = \begin{pmatrix} 5 & -1 & 0 & 0 \\ 0 & 3 & 0 & 1 \\ 8 & -4 & 3 & 1 \\ 2 & -1 & 0 & 3 \end{pmatrix}$.

(a) Determinare il polinomio minimo di φ.
(b) Trovare una base di $\mathbb{C}^4$ rispetto cui φ assume la forma di Jordan.
(c) Trovare tutte le matrici di Jordan che hanno lo stesso polinomio caratteristico di A.
(d) Dire se esistono almeno 5 sottospazi φ-invarianti distinti di dimensione 2 di $\mathbb{C}^4$.

8.2.8. Sia φ l'endomorfismo di $\mathbb{C}^4$ di matrice $A = \begin{pmatrix} 3 & 3 & 0 & -4 \\ 0 & 3 & 0 & 0 \\ -1 & 2 & 3 & 6 \\ 0 & -1 & 0 & 3 \end{pmatrix}$ rispetto alla base canonica.

(a) Determinare il polinomio caratteristico, il polinomio minimo e la forma di Jordan di φ.
(b) Trovare una base di $\mathbb{C}^4$ rispetto cui la matrice di φ è in forma di Jordan.
(c) Dire se nella $\mathbb{C}$-algebra $\mathbb{C}[A]$ generata da A esistono divisori di zero non nilpotenti.

8.2.9. Sia φ l'endomorfismo di $\mathbb{C}^4$ di matrice $A = \begin{pmatrix} -2 & 0 & 8 & 2 \\ -1 & -4 & -4 & -1 \\ 0 & 0 & -4 & 0 \\ 0 & 1 & 1 & -4 \end{pmatrix}$ rispetto alla base canonica.

(a) Determinare il polinomio minimo e la forma di Jordan di φ.
(b) Trovare una base di $\mathbb{C}^4$ rispetto cui φ assume la forma di Jordan.
(c) Trovare tutte le matrici di Jordan che hanno lo stesso polinomio caratteristico di A.
(d) Trovare, se esiste, una matrice B di $M_3(\mathbb{C})$ con lo stesso polinomio minimo di A.

8.2.10. Sia φ l'endomorfismo di $\mathbb{R}^4$ di matrice $A = \begin{pmatrix} 2 & 0 & -2 & 2 \\ 0 & 2 & -2 & 2 \\ 0 & 2 & 5 & -3 \\ 0 & 2 & 3 & -1 \end{pmatrix}$ rispetto alla base canonica.

(a) Calcolare il polinomio minimo e il polinomio caratteristico di φ.
(b) Determinare la forma di Jordan di φ.
(c) Trovare una base di $\mathbb{R}^4$ rispetto cui la matrice di φ assume la forma di Jordan.
(d) La $\mathbb{R}$-algebra $\mathbb{R}[A]$ generata da A contiene divisori di zero non nulli? ed elementi nilpotenti non nulli?

8.2.11. Sia φ l'endomorfismo di $\mathbb{R}^4$ rappresentato dalla matrice $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 6 & -5 & -5 & 5 \end{pmatrix}$ rispetto alla base canonica.

(a) Calcolare il polinomio minimo e il polinomio caratteristico di φ.
(b) Determinare la forma di Jordan di φ.
(c) Trovare una base di $\mathbb{R}^4$ rispetto cui la matrice di φ assume la forma di Jordan.

(d) Sia $(s_n)_{n\in\mathbb{N}}$ la successione definita mediante $s_0 = 0$, $s_1 = 3$, $s_2 = 3$, $s_3 = 9$, $s_{n+4} = 6s_n - 5s_{n+1} - 5s_{n+2} + 5s_{n+3}$ per ogni n in $\mathbb{N}$. Calcolare esplicitamente s_n per ogni n in $\mathbb{N}$.

8.2.12. Sia φ l'endomorfismo di $\mathbb{R}^4$ di matrice $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ rispetto alla base canonica $(e_1, \dots, e_4)$.

(a) Verificare che -1 è un autovalore di φ, calcolare $\dim\ker(\varphi + 1)$ e verificare che $e_1 + e_2 + e_3 + e_4$ è un autovettore di φ.

(b) Determinare il polinomio caratteristico ed il polinomio minimo di φ (suggerimento: usare (a)).

(c) Determinare una matrice di Jordan J per φ e trovare una base di $\mathbb{R}^4$ rispetto cui φ è rappresentata da J.

(d) Esiste una matrice Y tale che $Y^{\mathrm{t}}AY = J$?

8.2.13. Si consideri la sequenza $x_i \in \mathbb{Z}$ definita dalla relazione ricorsiva $X_n = X_{n-1} + X_{n-2} - X_{n-3}$ (per $n \geqslant 3$) e dai valori iniziali $x_0, x_1, x_2 \in \mathbb{Z}$.

(a) Determinare la matrice A tale che $\left(\begin{smallmatrix} x_n \\ x_{n-1} \\ x_{n-2} \end{smallmatrix}\right) = A \left(\begin{smallmatrix} x_{n-1} \\ x_{n-2} \\ x_{n-3} \end{smallmatrix}\right)$ e una forma di Jordan per A.

(b) Determinare una formula chiusa per x_n in funzione di n e dei valori iniziali x_0, x_1, x_2.

(c) Sotto quali condizioni (sui valori iniziali) la sequenza diventa costante (da un certo punto in poi)? E crescente?

8.2.14. Studiare la forma di Jordan della derivazione e delle sue potenze come endomorfismi dello spazio dei polinomi di grado minore o uguale ad n.

8.2.15. Un endomorfismo nilpotente φ d'indice 4 di uno spazio vettoriale V soddisfa alle condizioni $\dim\ker\varphi = 5$, $\dim\ker\varphi^2 = 9$, $\dim\ker\varphi^3 = 12$, $\dim\ker\varphi^4 = 14$. Determinare $\dim V$, il numero e la dimensione dei blocchi di Jordan di φ e scrivere la forma canonica di Jordan per φ.

8.2.16. La forma canonica di Jordan di un endomorfismo nilpotente φ di uno spazio vettoriale V comporta 2 blocchi d'ordine 1, 1 blocchi d'ordine 2, 3 blocchi d'ordine 3. Determinare $\dim V$, l'indice di nilpotenza di φ, e $\dim\ker\varphi^j$ per ogni j.

Capitolo VI

Geometria Affine

La nozione di Spazio Affine vuole modellare la nostra esperienza di "spazio geometrico" (senza ancora le nozioni metriche di distanze ed angoli); in uno spazio geometrico vi sono dei punti, e ci si può spostare da un punto ad un altro tramite "vettori-spostamento". D'altra parte in uno spazio geometrico non vi sono riferimenti privilegiati (non esiste una origine, un punto migliore di altri), né ha senso a priori fare operazioni tra punti.

Perciò definiremo uno Spazio Affine come un insieme su cui uno Spazio Vettoriale agisce spostando da un punto ad un altro (e la struttura di spazio vettoriale conviene, poiché siamo interessati a parlare di "spostamento nullo", "somma di spostamenti", "spostamento contrario", ecc.). Un Fisico direbbe che uno spazio vettoriale dà le "velocità" e uno spazio affine dà le "posizioni" per delle particelle.

Per gli Spazi Affini studieremo il calcolo baricentrico, una sorta di "operazione tra punti", e la nozione di trasformazioni affini, cioè di trasformazioni tra Spazi Affini ("deformazioni lineari dello spazio").

1. Spazi affini.

1.1. Definizione (spazio affine). *Uno spazio affine di dimensione n su un corpo $\mathbb{k}$ con spazio delle traslazioni V (spazio vettoriale di dimensione n su $\mathbb{k}$) è un insieme $\mathbb{A}$ (i cui elementi vengono detti punti) dotato di una azione di V:*

$$\mathbb{A} \times V \longrightarrow \mathbb{A} : \ (P, v) \mapsto P+v$$

soggetti ai seguenti assiomi:

($A1$) *nullitarietà: $P + 0 = P$ (per ogni $P \in \mathbb{A}$);*

($A2$) *associatività: $(P + v) + w = P + (v + w)$ (per ogni $P \in \mathbb{A}$ e per ogni $v, w \in V$);*

($A3$) *differenza di punti: per ogni coppia di punti $P, Q \in \mathbb{A}$ esiste un unico vettore $v \in V$ tale che $P + v = Q$. (l'unico vettore v si scrive $v = Q-P$, sicché possiamo parlare di "differenza tra punti").*

1.1.1. Si osservi che ($A3$) chiede esistenza ed unicità del vettore v; in particolare da ($A3$) e ($A1$) segue che $P + v = P$ (per qualche P) implica $v = 0$. Dunque per ogni P vale che: $P + v = P$ se e solo se $v = 0$.

Più in generale si ha che $P+v = P+w$ implica $v = w$ e similmente $P+v = Q+v$ implica $P = Q$. Questo permette di usare la simbologia algebrica con una certa sportività: per esempio è vero che $(P+v)-(Q+w) = (P-Q)+v-w$ nel senso che entrambe le espressioni hanno senso (sono vettori) e che sono uguali, ma per dimostrare l'uguaglianza non si può scrivere che sono uguali a $P+v-Q-w$ che non ha significato; ma si può vedere che sommate al punto $Q + w$ danno lo stesso punto come risultato...

1.1.2. Di solito si riassume la definizione dicendo che $\mathbb{A}$ è un insieme dotato di una *azione fedele e transitiva* di uno spazio vettoriale V, ove:
azione significa la funzione $+ : \mathbb{A} \times V \to \mathbb{A}$ nullitaria ed associativa;
fedele significa: $P + v = P$ (se e) solo se $v = 0$;
transitiva significa: per ogni coppia di punti $P, Q \in \mathbb{A}$ esiste un vettore $v \in V$ tale che $P + v = Q$ (la fedeltà fa sì che v sia unico).

1.1.3. In modo equivalente si può definire uno spazio affine di dimensione n su un corpo $\mathbb{k}$ con spazio delle traslazioni V come un insieme dotato di una mappa "differenza di punti"

$$\mathbb{A} \times \mathbb{A} \longrightarrow V : \ (P, Q) \mapsto Q-P$$

ove V è uno spazio vettoriale di dimensione n su $\mathbb{k}$, soddisfacente alle seguenti proprietà:

$(A'1)$ $P-P=0$ (per ogni $P\in\mathbb{A}$);
$(A'2)$ $(Q-P)+(P-R)=Q-R$ (per ogni $P,Q,R\in\mathbb{A}$);
$(A'3)$ per ogni punto $P\in\mathbb{A}$ e per ogni vettore $v\in V$ esiste un unico punto $Q\in\mathbb{A}$ tale che $v=Q-P$.

1.1.4. Si noti che fissato arbitrariamente un punto P di $\mathbb{A}$, l'applicazione insiemistica $V\to\mathbb{A}$ che manda v in $P+v$ è una biiezione, la cui inversa $\mathbb{A}\to V$ è l'applicazione che manda Q in $Q-P$.

Quindi uno spazio affine è sempre insiemisticamente in biiezione con il suo spazio vettoriale delle traslazioni, ma la biiezione non è canonica: per ogni scelta arbitraria di un punto si ha una biiezione diversa. In un certo senso lo spazio affine può essere visto come uno spazio vettoriale in cui si sono "dimenticate" alcune strutture (in particolare si dimentica che lo 0 *è un vettore con proprietà particolari: negli spazi affini non vi sono punti privilegiati da usare come origine).*

1.1.5. Ogni spazio vettoriale V è uno spazio affine su sé stesso (cioè con spazio delle traslazioni V) sotto l'operazione di somma. In particolare, quando lo spazio vettoriale standard $V_n(\Bbbk)$ viene visto come spazio affine su sé stesso, si indica con il simbolo $\mathbb{A}^n(\Bbbk)$ (o anche $\mathbb{A}^n_\Bbbk$).

♠ **1.2.** Esempio importante: struttura dell'insieme dei complementari di un sottospazio vettoriale. Inseriamo qui un esempio che giustifica la generalità della definizione data di spazio affine. Dato uno spazio vettoriale V di dimensione n e un suo sottospazio vettoriale W di dimensione $m\leqslant n$, consideriamo l'insieme $\mathbb{A}$ formato da tutti i sottospazi complementari di W, cioè $\mathbb{A}=\{U\leqslant V : U\cap W{=}0 \text{ e } U+W{=}V\}$. Che struttura ha l'insieme $\mathbb{A}$?

Questo insieme è uno spazio affine di dimensione $m(n-m)$, e possiamo descrivere in due modi lo spazio delle traslazioni di $\mathbb{A}$. La prima descrizione è la seguente: lo spazio delle traslazioni è lo spazio vettoriale $\mathrm{Hom}_\Bbbk(V/W,W)$, e l'azione sugli elementi di $\mathbb{A}$ si ottiene così: dato $U\in\mathbb{A}$ abbiamo un isomorfismo canonico $U\cong V/W$, e quindi per ogni $\psi:V/W\to W$ abbiamo un'applicazione lineare $\psi:U\to W$; poniamo allora $U+\psi=\{u{+}\psi(u) : u{\in}U\}$, che si verifica facilmente essere un sottospazio di V complementare di W, e dunque un elemento di $\mathbb{A}$.

La seconda descrizione permette di identificare uno strano sottospazio di $\mathrm{Aut}(V)$. Consideriamo $\mathbb{T}=\{\varphi\in\mathrm{Aut}(V) : \varphi_{|W}{=}\mathrm{id}_W \text{ e } \varphi/W{=}\mathrm{id}_{V/W}\}$ cioè l'insieme degli automorfismi di V che si restringono alla identità su W e che inducono il morfismo identico su V/W. La struttura di spazio vettoriale di $\mathbb{T}$ è data usando la composizione di applicazioni (si noti che essa risulta commutativa) e la moltiplicazione per gli scalari definita da $\alpha{\cdot}\varphi=\mathrm{id}_V+\alpha(\varphi{-}\mathrm{id}_V)$. Può essere più facile vedere la struttura di $\mathbb{T}$ osservando che con una opportuna scelta dalla base di V, gli elementi di $\mathbb{T}$ sono rappresentati da matrici a blocchi del tipo $\begin{pmatrix}\mathbb{I}_m & F\\ \mathbb{O}_{n-m,m} & \mathbb{I}_{n-m}\end{pmatrix}$ ove $F\in M_{m,n-m}(\Bbbk)$ (quest'ultima rappresenta un elemento $\psi\in\mathrm{Hom}_\Bbbk(V/W,W)$) e osservando come si comporta il prodotto tra matrici di questo tipo. Ora l'azione di $\varphi\in\mathbb{T}$ su $U\in\mathbb{A}$ è data da $U+\varphi=\varphi(U)$.

1.3. Definizione (posizione generale di punti). *Siano $P_0,P_1,\dots,P_m$ punti di uno spazio affine $\mathbb{A}$ con spazio delle traslazioni V di dimensione n. Essi si dicono "in posizione generale" o "indipendenti" se i vettori $P_1{-}P_0,\dots,P_m{-}P_0$ di V sono linearmente indipendenti (dunque in particolare $m\leqslant n$).*

1.4. Definizione (riferimenti affini e coordinate). *Sia $\mathbb{A}$ uno spazio affine su $\Bbbk$ con spazio delle traslazioni V di dimensione n. Un sistema di riferimento di $\mathbb{A}$ è equivalentemente:*
(R) un insieme di $n+1$ punti $P_0,P_1,\dots,P_n$ di $\mathbb{A}$ in posizione generale;
(R') un punto O di $\mathbb{A}$ e una base $v_1,\dots,v_n$ di V.
Scelto un sistema di riferimento, ad ogni punto P di $\mathbb{A}$ restano associate le sue coordinate $(x_1,\dots,x_n)^{\mathrm{t}}$ (in quel sistema di riferimento) definite equivalentemente da
(R) $P=P_0+\sum_i x_i(P_i{-}P_0)$;
(R') $P=O+\sum_i x_iv_i$.

Il passaggio da (R) a (R') si ottiene definendo $O=P_0$ e $v_i=P_i{-}P_0$ per $i=1,\dots,n$. Il viceversa si ottiene definendo $P_0=O$ e $P_i=P_0{+}v_i$ per $i=1,\dots,n$.

1.4.1. Utilizzando le coordinate in un fissato riferimento affine, possiamo allora dire che i punti $P_0,P_1,\dots,P_m$ sono in posizione generale se e solo se la matrice $\begin{pmatrix}P_1{-}P_0 & \cdots & P_m{-}P_0\end{pmatrix}\in M_{n,m}(\Bbbk)$ ha rango m, o anche se e solo se la matrice

$$\begin{pmatrix}1 & 1 & \cdots & 1\\ P_0 & P_1 & \cdots & P_m\end{pmatrix}\in M_{n+1,m+1}(\Bbbk)$$

ha rango $m+1$.

1.4.2. In particolare, per tre punti in un piano e usando le coordinate in un qualsiasi riferimento affine di quel piano, si ha che i punti sono allineati sse

$$\det\begin{pmatrix} P_1-P_0 & P_2-P_0 \end{pmatrix} = 0 \qquad \text{ovvero} \quad \det\begin{pmatrix} 1 & 1 & 1 \\ P_0 & P_1 & P_3 \end{pmatrix} = 0$$

(annullamento di determinanti).

Generalizzare ad $n+1$ punti in uno spazio affine di dimensione n: la condizione di appartenere ad (almeno) un iperpiano (cioè, non essere in posizione generale) corrisponde all'annullamento di un determinante.

1.5. Definizione (sottospazi affini). *Un sottinsieme del tipo*

$$P+W = \{P+w : w \in W\}$$

con $P \in \mathbb{A}$ e W un sottospazio vettoriale di V di dimensione m si dice una varietà lineare affine (o sottospazio affine) di dimensione m di $\mathbb{A}$; W si chiama lo spazio direttore.

1.5.1. Si noti che $P+W = Q+W$ se e solo se $Q-P \in W$.

1.5.2. I punti di $\mathbb{A}$ sono sottospazi affini con spazio direttore nullo.

1.5.3. Le rette (risp. i piani) di $\mathbb{A}$ sono i sottospazi affini con spazio direttore di dimensione 1 (risp. 2).

1.5.4. Equazioni parametriche e cartesiane. Una varietà affine si descrive tramite equazioni parametriche: se $w_1, \dots, w_m$ sono una base di W, allora ogni punto X di $P+W$ si scrive come $X = P + \sum_i \alpha_i w_i$ ove gli $\alpha_i \in \Bbbk$ sono i parametri.

Fissato un riferimento affine, se P ha coordinate $(x_1, \dots, x_n)^{\mathrm{t}}$, si può esplicitare:

$$\begin{cases} X_1 = x_1 + \sum_i \alpha_i w_{i,1} \\ \dots \\ X_n = x_n + \sum_i \alpha_i w_{i,n} \end{cases}$$

Il sottospazio affine $P+W$ si può descrivere anche tramite un sistema di $n-m$ equazioni lineari (rappresentazione cartesiana) che si ottengono dalla condizione

$$\operatorname{rk}\begin{pmatrix} X-x & w_1 & \cdots & w_m \end{pmatrix} \leqslant m$$

(esiste una sottomatrice quadrata invertibile di ordine m: e allora basta annullare i determinanti di ordine $m+1$ contenenti quella sottomatrice). Equivalentemente si può chiedere che

$$\operatorname{rk}\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ X & x & w_1 & \cdots & w_m \end{pmatrix} \leqslant m+1.$$

Viceversa un sistema lineare di m equazioni nelle incognite $X = (X_1, \dots, X_n)$ (che abbia soluzioni) determina un sottospazio affine di dimensione $n-r$ ove r è il rango comune delle matrici completa e incompleta. Il sistema di equazioni si dice minimale se è composto esattamente da r equazioni. Risolvere il sistema equivale a trovare una rappresentazione parametrica per la varietà lineare.

1.5.5. Una collezione di $m+1$ punti $P_0, P_1, \dots, P_m$ di $\mathbb{A}$ in posizione generale determina una varietà affine di dimensione m: la più piccola varietà affine contenente quei punti. Ha equazioni parametriche $X = P_0 + \sum_i \alpha_i (P_i - P_0)$ ed equazioni cartesiane date dalla condizione:

$$\operatorname{rk}\begin{pmatrix} X-P_0 & P_1-P_0 & \cdots & P_m-P_0 \end{pmatrix} \leqslant m$$

ovvero che

$$\operatorname{rk}\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ X & P_0 & P_1 & \cdots & P_m \end{pmatrix} \leqslant m+1.$$

Si ricordi il principio dei minori orlati al fine di ricavare un sistema minimo di equazioni lineari, a partire dalle condizioni di rango.

1.5.6. In particolare nel caso di n punti in posizione generale in uno spazio affine di dimensione n, l'equazione dell'iperpiano generato da questi punti si ottiene da un determinante.

1.5.7. Una collezione di $m+1$ punti $P_0, P_1, \dots, P_m$ di $\mathbb{A}$ è in posizione generale se e solo se ogni punto non appartiene al sottospazio affine generato dagli altri. Per esempio due punti distinti sono in posizione generale; tre punti non allineati sono in posizione generale; quattro punti non complanari sono in posizione generale.

1.6. Definizione (posizioni reciproche di sottospazi affini). *Siano $L = P + W$ e $L' = P' + W'$; i due sottospazi si dicono*

(1) *incidenti se $L \cap L' \neq \varnothing$ (e l'intersezione è un sottospazio affine); disgiunti in caso contrario; criterio di incidenza: $P - P' \in W + W'$ (infatti questo è equivalente all'l'esistenza di un punto $P + w = P' + w'$ con $w \in W$, $w' \in W'$)*

(2) *paralleli se $W \subseteq W'$ o $W' \subseteq W$; in tal caso possono appartenersi ($L \subseteq L'$ risp. $L' \subseteq L$) oppure essere disgiunti;*

(3) *sghembi se sono disgiunti e $W \cap W' = 0$.*

1.6.1. Secondo la definizione, due punti sono sempre paralleli, ma non si dice.

1.6.2. Secondo la definizione, un punto è parallelo a qualunque sottospazio affine, ma non si dice nemmeno questo.

1.6.3. Due rette sono parallele se e solo se i vettori generatori degli spazi direttori sono proporzionali. Questo si dice.

1.6.4. Una retta $P + \langle v \rangle$ è parallela ad un piano $Q + \langle w_1, w_2 \rangle$ se e solo se $v \in \langle w_1, w_2 \rangle$. Essa è contenuta nel piano se inoltre $P - Q \in \langle w_1, w_2 \rangle$.

1.6.5. Esistono coppie di sottospazi affini che non sono né incidenti, né parallele, né sghembe: per esempio in $\mathbb{A}^4_{\Bbbk}$ sia L definito da $X_1 = X_2 = 0$ e M definito da $X_1 - 1 = X_3 = 0$.

1.6.6. Tuttavia, nel caso di rette (sottospazi di dimensione 1) ed iperpiani (sottospazi di codimensione 1, cioè dimensione 1 meno dello spazio affine) con qualunque altro sottospazio le uniche posizioni reciproche possibili sono le tre definite (incidenti o paralleli o sghembi). In particolare per spazi di dimensione 3 (sottospazi non banali sono solo, tranne i punti, rette e piani).

1.6.7. Questioni antiche. È quasi ovvio osservare che per ogni sottospazio affine $\mathbb{L} = P + W$ di $\mathbb{A}$, e per ogni punto $Q \notin \mathbb{L}$ esiste un unico sottospazio affine passante per Q, parallelo e delle stessa dimensione con $\mathbb{L}$ (si tratta di $Q + W$). Quindi nei nostri Spazi Affini vale sempre l'enunciato "per ogni punto esterno ad una retta data passa una ed una unica retta parallela alla data", equivalente al celebre "quinto postulato" di Euclide.

Facciamo solo notare che noi, nel prossimo capitolo e seguendo la terminologia moderna, useremo il termine "geometria euclidea" non per indicare la validità del postulato, ma per indicare Spazi Affini reali in cui si introduca una nozione di metrica (distanza tra punti, angoli, ortogonalità, tutte nozioni indotte arricchendo la struttura dello spazio vettoriale delle traslazioni).

1.7. Definizione (inf e sup di sottospazi affini). *Siano $L = P + W$ e $L' = P' + W'$ sottospazi affini di $\mathbb{A}$; poniamo*

(1) *inf (o meet, o intersezione) di L e L': $L \wedge L' := L \cap L'$ (massima sottovarietà contenuta sia in L che in L'),*

(2) *sup (o join, o congiungente) di L e L': $L \vee L' :=$ la minima sottovarietà contenente L e L'.*

Quest'ultima si scrive come $P + \langle P' - P, W, W' \rangle$ (ovvero $P' + \langle P - P', W + W' \rangle$) in generale (in particolare se le varietà sono disgiunte); per varietà con intersezione non vuota, possiamo supporre $P = P'$ e allora il sup è dato da $P' + (W + W')$.

Se vogliamo dire che l'intersezione di due sottovarietà affini sia una sottovarietà affine, dobbiamo accettare come tale anche l'insieme vuoto, e per convenzione si pone $\dim_{\Bbbk} \varnothing := -1$ (poiché zero è la dimensione dei punti, che sono sottovarietà affini con spazio direttore $\langle 0 \rangle$ di dimensione 0).

1.7.1. Con queste definizioni possiamo discutere meglio la situazione delle posizioni reciproche per due sottospazi affini:

(1) due rette distinte possono essere complanari (cioè il sup essere un piano, che capita se e solo se sono incidenti o parallele), oppure sghembe (nel qual caso il sup è spazio affine di dimensione 3);

(2) due piani distinti possono avere sup di dimensione 3 (se e solo se sono incidenti in una retta o paralleli), oppure sup di dimensione 4 (nel qual caso sono incidenti in un punto, oppure non sono né incidenti, né paralleli, ma nemmeno sghembi: gli spazi direttori devono avere intersezione in uno spazio di dimensione 1), oppure sghembi (nel qual caso il sup è spazio affine di dimensione 5);

(3) una retta e un piano che non la contiene? Possono generare uno spazio affine di dimensione 3 (se incidenti o paralleli) oppure 4 se sghembi;

(4) consideriamo due sottospazi distinti di dimensione 3: il sup può avere dimensione 4 (se e solo se sono paralleli oppure incidenti in un piano), oppure dimensione 5 (se e solo se sono incidenti in una

retta oppure disgiunti ma con spazi direttori che si intersecano in un piano), oppure dimensione 6 (se e solo se sono incidenti in un punto oppure disgiunti ma con spazi direttori che si intersecano in una retta), oppure dimensione 7 (se e solo se sono sghembi).
(5) una retta e uno spazio di dimensione 3 che non la contiene?
(6) un piano e uno spazio di dimensione 3 che non lo contiene?

1.8. Teorema (grassmann affine). *Risulta che:*

$$\dim_{\Bbbk}(L \vee L') + \dim_{\Bbbk}(L \wedge L') \leqslant \dim_{\Bbbk} L + \dim_{\Bbbk} L'$$

e vale l'uguaglianza se L e L' sono incidenti (oppure sghembe se poniamo $\dim_{\Bbbk} \varnothing := -1$); se le varietà sono disgiunte (in particolare se sono parallele) è

$$\dim_{\Bbbk}(L \vee L') + \dim_{\Bbbk}(W \cap W') = \dim_{\Bbbk} L + \dim_{\Bbbk} L' + 1.$$

Dimostrazione. Evidente dalla descrizione precedente e dalla formula di Grassmann per spazi vettoriali. Infatti, $\dim_{\Bbbk} L = \dim_{\Bbbk} W$ e $\dim_{\Bbbk} L' = \dim_{\Bbbk} W'$; ora:

• se le due sottovarietà sono incidenti abbiamo $\dim_{\Bbbk}(L \vee L') = \dim_{\Bbbk}(W + W')$ e $\dim_{\Bbbk}(L \wedge L') = \dim_{\Bbbk}(W \cap W')$, da cui la formula con l'uguaglianza;

• se invece l'intersezione è vuota abbiamo $\dim_{\Bbbk}(L \vee L') = \dim_{\Bbbk}(W + W') + 1$ (da cui segue la seconda uguaglianza) e $\dim_{\Bbbk}(L \wedge L') = -1$, dunque $\dim_{\Bbbk}(L \vee L') + \dim_{\Bbbk}(L \wedge L') = \dim_{\Bbbk}(W + W')$, da cui segue la disuguaglianza generale, e anche l'uguaglianza nel caso sghembo in cui $\dim_{\Bbbk}(W \cap W') = 0$. □

1.8.1. È interessante notare che nel caso di intersezione vuota abbiamo sempre $\dim_{\Bbbk}(L \vee L') = \dim_{\Bbbk}(W + W') + 1$ e $\dim_{\Bbbk}(L \wedge L') = -1$, e non si tiene per nulla conto del termine $W \cap W'$ (direzioni comuni degli spazi direttori), la cui dimensione è proprio la massima differenza tra i due termini dell'uguaglianza. Per esempio per due iperpiani paralleli e disgiunti in dimensione n, tale differenza è esattamente $n - 1$, mentre per una retta e un iperpiano paralleli e disgiunti, la differenza vale 1.

1.8.2. Si osservi che la seconda formula è particolarmente sgradevole, poiché abbiamo dovuto ricorrere ad un termine (la dimensione dello spazio vettoriale $W \cap W'$) che non ha apparentemente corrispondente nello spazio affine. Si tratta di un termine che tiene conto delle "direzioni in comune" tra L ed L', ma non corrisponde ad alcun punto dello spazio affine. Studiando la Geometria Proiettiva, questi termini saranno interpretati come "punti all'infinito" in comune alle varietà date, e la formula assumerà un aspetto molto più naturale.

1.8.3. Comunque, sotto l'ipotesi che due sottospazi affini non siano paralleli, le formule di Grassmann possono essere usate per dedurre che se le loro dimensioni sono abbastanza grandi, allora devono essere incidenti. Scrivere un enunciato preciso di questo tipo.

Per garantire (condizione sufficiente, non necessaria) che l'intersezione di L ed L' sia non vuota serve che $W + W' = V$ (nel qual caso certamente $P - P' \in V = W + W'$). Dalla formula di Grassmann vettoriale questo è garantito se $\dim_{\Bbbk}(W + W') = \dim_{\Bbbk} W + \dim_{\Bbbk} W' - \dim_{\Bbbk}(W \cap W') \geqslant n$ $(= \dim_{\Bbbk} V)$. Quindi detto $r = \dim_{\Bbbk}(W \cap W')$, che potremmo chiamare indice di parallelismo tra L ed L' (si tratta della massima dimensione di sottospazi affini contenuti in L ed L' e tra loro paralleli), abbiamo che se $\dim L + \dim L' \geqslant n + r$ allora l'intersezione di L ed L' è non vuota (e anzi è sottospazio affine di dimensione r).

In particolare se $r = 0$ (sottospazi direttori con intersezione nulla), allora basta che $\dim L + \dim L' \geqslant n$ per avere (esattamente) un punto di intersezione.

Se si vuole dare una condizione indipendente dal termine r, l'unico caso ovvio è quello degli iperpiani: ogni iperpiano interseca tutti i sottospazi affini che non gli sono paralleli.

1.9. Sottospazi complementari. Due sottospazi affini L ed L' si dicono complementari se sono sghembi ($L \wedge L' = \varnothing$ e l'intersezione degli spazi direttori è nulla) e generano tutto lo spazio affine ($L \vee L' = \mathbb{A}$). In tal caso $\dim_{\Bbbk} L + \dim_{\Bbbk} L' = n - 1$ se n è la dimensione di $\mathbb{A}$ (si noti che gli spazi direttori non generano tutto lo spazio vettoriale delle traslazioni).

1.9.1. Per esempio una retta ed un punto non appartenente ad essa sono complementari in un piano affine.

1.9.2. In uno spazio affine tridimensionale due rette sono complementari se e solo se sono sghembe. Un piano è complementare ad un punto se e solo se il punto non appartiene al piano.

1.9.3. In uno spazio affine quadridimensionale una retta è complementare ad un piano se e solo se retta e piano sono sghembi tra loro.

1.10. Collezioni di iperpiani affini (sottospazi affini di codimensione uno). Dati r iperpiani $\pi_1, \ldots, \pi_r$ in uno spazio affine $\mathbb{A}$ di dimensione n tali che $\pi_1 \cap \cdots \cap \pi_r$ abbia dimensione $n-r$ (equivalentemente: scelto qualsiasi riferimento, il sistema delle equazioni $L_1\binom{1}{X} = 0, \ldots, L_r\binom{1}{X} = 0$ degli iperpiani risulta compatibile di rango r; si noti che $L_1, \ldots, L_r \in M_{1,n+1}(\Bbbk)$), allora: un iperpiano di $\mathbb{A}$ contiene $\pi_1 \cap \cdots \cap \pi_r$ se e solo se la sua equazione è una combinazione lineare a coefficienti non tutti nulli delle equazioni di $\pi_1, \ldots, \pi_r$ (nel riferimento dato dev'essere quindi del tipo $(\alpha_1 L_1 + \ldots + \alpha_r L_r)\binom{1}{X} = 0$ ove $\alpha_1, \ldots, \alpha_r \in \Bbbk$ non tutti nulli).

Si tratta di una applicazione immediata del teorema di Rouché-Capelli: aggiungendo l'equazione del nuovo iperpiano il sistema ha esattamente le stesse soluzioni...

L'insieme di tutti gli iperpiani contenenti l'intersezione di $\pi_1, \ldots, \pi_r$ si chiama collezione di iperpiani di centro $\pi_1 \cap \cdots \cap \pi_r$.

1.10.1. Nel piano affine si dice *fascio di rette di centro un punto P* l'insieme formato da tutte le rette contenenti quel punto; se P ha coordinate $\binom{x}{y}$, ovvero equazioni $X - x = 0 = Y - y$, allora le rette del fascio hanno equazioni $\alpha(X - x) + \beta(Y - y) = 0$ con α, β non entrambi nulli.

Date due rette distinte nel piano affine, se la loro intersezione è un punto siamo esattamente nel caso descritto e le rette del fascio hanno equazioni date dalle combinazioni non nulle delle equazioni date; se invece le due rette sono parallele, le rette che si descrivono tramite combinazioni non nulle sono tutte e sole le rette parallele alle due date (segue ancora da Rouché-Capelli) e la loro collezione si dice un fascio di rette improprio; si dice ancora che queste rette hanno in comune "un punto all'infinito".

Date tre rette in un piano affine, la condizione di appartenere ad (almeno) un fascio si può esprimere usando le equazioni cartesiane in un qualsiasi riferimento affine su quel piano, tramite l'annullamento del determinante della matrice completa del sistema di equazioni delle tre rette.

1.10.2. Nello spazio affine di dimensione 3 si dice *fascio di piani di asse una retta r* l'insieme formato da tutti i piani contenenti quella retta; se r ha equazioni $L = 0 = M$, allora i piani del fascio hanno equazioni $\alpha L + \beta M = 0$ con α, β non entrambi nulli.

Dati due piani distinti nello spazio affine, se la loro intersezione è una retta siamo esattamente nel caso descritto e i piani del fascio hanno equazioni date dalle combinazioni non nulle delle equazioni date; se invece i due piani sono paralleli, i piani che si descrivono tramite combinazioni non nulle sono tutti e soli i piani paralleli ai due dati e l'insieme si dice un fascio di piani improprio; si dice ancora che questi piani hanno in comune "una retta all'infinito".

Come esprimere in un fissato riferimento la condizione per tre piani di appartenere ad un fascio?

1.10.3. Nello spazio affine di dimensione 3 si dice *stella di piani di centro un punto P* l'insieme formato da tutti i piani contenenti quel punto; se P ha coordinate $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$, ovvero equazioni $X - x = Y - y = Z - z = 0$, allora le rette del fascio hanno equazioni $\alpha(X - x) + \beta(Y - y) + \gamma(Z - z) = 0$ con α, β, γ non tutti nulli.

Dati tre piani distinti nello spazio affine, se la loro intersezione è un punto siamo esattamente nel caso descritto e i piani della stella hanno equazioni date dalle combinazioni non nulle delle equazioni date; se invece i tre piani hanno intersezione vuota (ma non sono in un fascio improprio, ovvero non sono tutti a due a due paralleli), i piani che si descrivono tramite combinazioni non nulle sono tutti e soli i piani paralleli alla direzione comune ai tre dati e l'insieme si dice una stella di piani impropria; si dice ancora che questi piani hanno in comune "un punto all'infinito".

Come esprimere in un fissato riferimento la condizione per quattro piani di appartenere ad una stella?

1.10.4. In uno spazio affine di dimensione 4 si possono definire fasci, stelle, reti (propri) di iperpiani, che sono collezioni di iperpiani di centri rispettivamente un piano, una retta, un punto e sono descritti usando rispettivamente due, tre e quattro parametri non tutti nulli.

Dati due, tre, quattro iperpiani, essi definiscono rispettivamente un fascio, una stella, una rete (propri) di iperpiani se la loro intersezione è rispettivamente un piano, una retta, un punto. Se invece le intersezioni hanno dimensioni minori, si parla di fasci, stelle, reti impropri di iperpiani.

♠ **1.11.** Collezioni di sottospazi affini. Allo stesso modo si potrebbe pensare di descrivere l'insieme dei sottospazi affini di dimensione r che contengono un fissato sottospazio affine di dimensione

$s < r$ descritto da $n-s$ equazioni cartesiane (detto centro, intersezione di $n-s$ iperpiani), oppure più generalmente descrivere l'insieme dei sottospazi di dimensione s le cui equazioni si possono scrivere usando combinazioni lineari di $n-s$ equazioni di iperpiani distinti.

Ciò porta a descrivere l'insieme quoziente delle matrici di rango $n-r$ in $M_{n-r,n-s}(\Bbbk)$ sotto l'equivalenza per righe, cioè l'azione di moltiplicazione a sinistra per matrici in $\mathrm{GL}_{n-r}(\Bbbk)$.

Il caso precedente (iperpiani) si ritrova usando righe non nulle modulo la relazione di proporzionalità.

1.12. Problema. *Siano r ed s due rette sghembe in uno spazio affine; si mostri che per ogni punto P appartenente a $r \vee s$ ma non a $r \cup s$ (attenzione!) esiste una unica retta t passante per P e complanare sia con r che con s (ovviamente, in due piani distinti...). Quando tale retta è incidente o parallela con le due date?* Per affrontare il problema, conviene ragionare identificando le condizioni a cui deve soddisfare t: dovendo passare per P e dovendo essere complanare con r, deve stare sul piano $P \vee r$ (un piano?); per lo stesso motivo deve stare su $P \vee s$; ma allora deve essere l'intersezione di questi due piani, se l'intersezione è una retta... Si noti che il ragionamento fatto dà anche un procedimento facile per calcolare delle equazioni per la retta cercata: basta trovare le equazioni dei due piani, e per questi basta imporre al generico piano del fascio di asse r (risp. s) la condizione di passare per P.

Analogamente si può costruire una unica complanare comune che abbia una fissata direzione.

Generalizzare il problema per sottospazi di dimensioni superiori (retta e piano sghembi in dimensione 4, due piani sghembi in dimensione 5...).

1.12.1. È un simpatico e classico esercizio il seguente: *Date tre rette a due a due sghembe in uno spazio di dimensione tre, descrivere l'insieme formato dai punti dello spazio che appartengono a complanari comuni alle tre rette, cioè l'unione di tutte le complanari comuni alle tre rette date.* Che di tali complanari ve ne siano è chiaro: per ogni punto di una delle rette passa una complanare comune alle altre due, quindi... D'altra parte descrivendo con un parametro λ una retta, e usando la costruzione precedente troviamo che la complanare comune (dipendente da λ) si scrive come $\begin{cases} \ell_1 + \lambda\ell_2 = 0 \\ \ell_3 + \lambda\ell_4 = 0 \end{cases}$ dove ℓ_i sono espressioni lineari delle coordinate dello spazio. Dunque i punti cercati (sono quelli che appartengono a una di queste rette per qualche $\lambda \in \Bbbk$, cioè quelli per cui esiste un $\lambda \in \Bbbk$ che soddisfa al sistema) sono caratterizzati dalla equazione di secondo grado $\det \begin{pmatrix} \ell_1 & \ell_2 \\ \ell_3 & \ell_4 \end{pmatrix} = 0$.

Si osservi che un ragionamento del tipo: per ogni punto X imponiamo che i tre piani formati da X con le tre rette date siano coassiali (cioè appartengano ad un fascio di asse una retta), porterebbe apparentemente ad una condizione di terzo grado...

1.13. Interpretazione geometrica di Rouché-Capelli (costellazioni di sottospazi affini). Il teorema di Rouché-Capelli ci permette di discutere completamente tutte le possibili relazioni reciproche di sottospazi affini. Si osservi però che diverse disposizioni geometriche possono comparire aventi gli stessi ranghi completi e incompleti del sistema che descrive i sottospazi coinvolti. Discutiamo solo una paio di casi, invitando il lettore a svilupparne altri.

1.13.1. La costellazione di tre piani in $\mathbb{A}^3$ è descritta da un sistema lineare di matrice incompleta $A \in M_3(\Bbbk)$ e completa $(A\ b) \in M_{3,4}(\Bbbk)$; distinguiamo i casi delle coppie $(\mathrm{rg}A, \mathrm{rg}(A\ b))$:

$(3,3)$ sono tre piani che si incontrano in un punto: piani generici di una stella;

$(2,3)$ i tre piani hanno intersezione vuota, ma è necessario distinguere due casi:
- il rango di A è 2 perché una riga è multipla di un'altra: allora si hanno due piani paralleli e distinti, e un terzo che li interseca in due rette parallele;
- il rango di A è 2 ma nessuna riga è multipla di un'altra: allora si tratta di tre piani aventi una direzione comune delle giaciture, e a due a due si intersecano in (tre) rette tra loro parallele;

$(2,2)$ si tratta di tre piani di un fascio di centro una retta (l'intersezione comune);

$(1,2)$ si tratta di tre piani paralleli di cui almeno due distinti;

$(1,1)$ si tratta di tre piani coincidenti.

1.13.2. La costellazione di due piani in $\mathbb{A}^3$?

1.13.3. La costellazione di un piano e una retta in $\mathbb{A}^3$?

1.13.4. La costellazione di tre rette in $\mathbb{A}^3$?

1.13.5. La costellazione di due piani in $\mathbb{A}^4$ è descritta da un sistema lineare di matrice incompleta $A \in M_4(\Bbbk)$ e completa $(A\ b) \in M_{4,5}(\Bbbk)$; distinguiamo i casi delle coppie $(\mathrm{rg}A, \mathrm{rg}(A\ b))$:

$(4,4)$ sono due piani che si intersecano in un punto: il sottospazio congiungente è tutto $\mathbb{A}^4$;

$(3,4)$ sono due piani con intersezione vuota, ma le cui giaciture hanno una direzione comune: il sottospazio congiungente è tutto $\mathbb{A}^4$; esistono due iperpiani paralleli contenenti ciascuno uno dei due piani;
$(3,3)$ sono due piani che si intersecano in una retta: il sottospazio congiungente è un iperpiano;
$(2,3)$ sono due piani paralleli e distinti contenuti in uno stesso iperpiano;
$(2,2)$ sono due piani coincidenti.

1.13.6. La costellazione di tre iperpiani in $\mathbb{A}^4$?

1.13.7. La costellazione di tre piani in $\mathbb{A}^4$?

2. Calcolo baricentrico.

2.1. Definizione-Teorema (somme pesate o baricentriche di punti). *Dati m punti $P_1,\dots,P_m\in\mathbb{A}$ e m coefficienti $\alpha_1,\dots,\alpha_m\in\Bbbk$ tali che $\sum_i\alpha_i=1$, il punto definito dalla formula*

$$P := Q+\sum_i \alpha_i(P_i-Q)$$

risulta indipendente dal punto "di base" Q arbitrariamente scelto per la definizione, e si può dunque scrivere come

$$P := \sum_i \alpha_i P_i$$

("somma pesata di punti" o "somma baricentrica di punti": la somma dei punti è definita solo se i coefficienti hanno somma 1). Il punto P si dice il baricentro del sistema dei punti $P_1,\dots,P_m\in\mathbb{A}$ con i pesi rispettivi $\alpha_1,\dots,\alpha_m\in\Bbbk$.

Dimostrazione. Se Q' è qualsiasi altro punto, e $P' := Q'+\sum_i\alpha_i(P_i-Q')$, allora la differenza $P-P'$ è

$$\begin{aligned} P-P' &= \Big(Q+\sum_i\alpha_i(P_i-Q)\Big)-\Big(Q'+\sum_i\alpha_i(P_i-Q')\Big)\\ &= (Q-Q')+\sum_i\alpha_i(P_i-Q)-\sum_i\alpha_i(P_i-Q')\\ &= (Q-Q')+\sum_i\alpha_i(Q'-Q)=0 \end{aligned}$$

(nota bene: abbiamo usato $(P+v)-(Q+w)=(P-Q)+v-w$, e $(P-R)-(Q-R)=P-Q$, uguaglianze tra vettori: perché sono vere?). □

2.1.1. Le combinazioni pesate di m punti descrivono il sottospazio affine generato da quei punti; si tratta di un sottospazio di dimensione $m-1$ se i punti sono in posizione generale. Ciò si vede facilmente osservando che $\sum_i\alpha_iP_i = P_0+\sum_i\alpha_i(P_i-P_0)$ descrive esattamente

$$P_0\vee P_1\vee\cdots\vee P_r = P_0+\langle P_i-P_0\rangle.$$

In particolare: le combinazioni pesate di due punti distinti descrivono la retta congiungente i due punti; le combinazioni pesate di tre punti non allineati descrivono il piano congiungente i tre punti (esplicitare bene).

2.1.2. Proprietà distributiva dei baricentri. Data una famiglia di punti $P_{i,j}$ con $i=0,\dots,m$ e $j=0,\dots,r$, una famiglia di pesi $\alpha_{i,j}$ con $i=0,\dots,m$ e $j=0,\dots,r$ tali che $\sum_j\alpha_{i,j}=1$ per ogni i, ed una ulteriore famiglia di pesi β_k con $k=0,\dots,m$ tali che $\sum_k\beta_k=1$ allora risulta

$$\sum_i\beta_i(\sum_j\alpha_{i,j}P_{i,j}) = \sum_{i,j}(\beta_i\alpha_{i,j})P_{i,j}$$

(nel senso che entrambe le espressioni hanno senso, in particolare $\sum_{i,j}\beta_i\alpha_{i,j}=1$, e i due punti coincidono).

Dimostrazione?

2.1.3. Stenografia. Nel seguito verrà spontaneo fare alcuni passaggi "algebrici" che portano da una formula con significato affine ad un'altra formula con significato affine, ma in cui i passaggi

intermedi "non hanno senso". Per esempio: per quattro punti A, B, C, D in uno spazio affine, le uguaglianze $A - B = D - C$ (tra vettori) e $\frac{1}{2}A + \frac{1}{2}C = \frac{1}{2}B + \frac{1}{2}D$ (tra punti) hanno entrambe significato (se il campo non ha caratteristica 2) e sono equivalenti tra loro, ma passare dall'una all'altra con passaggi algebrici del tipo "$A + C = B + D$" e "dividere per 2" dà espressioni che non hanno senso per gli spazi affini (ma hanno senso pensando A, B, C, D come vettori, e per fare questo bisogna aver scelto un punto "origine" nello spazio affine, e questa scelta è arbitraria).

Morale: le espressioni tra vettori che hanno senso in quanto punti di uno spazio affine sono quelle invarianti per traslazione (come la definizione di baricentro), ma per dimostrare che due espressioni di questo tipo sono uguali, possiamo trattarle come uguaglianze tra vettori!

Per esercizio si dimostrino le seguenti uguaglianze sia usando le definizioni (cioè con passaggi che abbiano tutti senso nello spazio affine) sia sportivamente:

(1) $A - B = (A - C) + (C - B)$ (applicati al punto B danno lo stesso risultato);

(2) $A - B = -(B - A)$ (la somma tra i due vettori dà il vettore nullo);

(3) $(A + v) - (B + w) = (A - B) + v - w$ (applicati al punto $B + w$ danno lo stesso risultato);

(4) se il campo non ha caratteristica 2, allora: $A - B = D - C$ se e solo se $\frac{1}{2}A + \frac{1}{2}C = \frac{1}{2}B + \frac{1}{2}D$ (interpretazione geometrica in termini di parallelogrammi e diagonali?);

(5) se $\alpha + \beta = 1$ allora $(\alpha A + \beta B) - (\alpha C + \beta D) = \alpha(A - C) + \beta(B - D)$;

(6) $A+(B-C) = B+(A-C)$ (la differenza dà il vettore nullo, oppure è una somma baricentrica!).

2.2. Proposizione (caratterizzazione baricentrica dei sottospazi affini). *Un sottinsieme L di $\mathbb{A}$ è un sottospazio affine se e solo se è stabile per somme pesate di punti, ovvero sse quando contiene due punti contiene la retta generata (combinazioni pesate di due punti).*

Dimostrazione. Facile esercizio. □

2.3. Definizione (Coordinate baricentriche). *Dato un riferimento affine $P_0, P_1, \dots, P_n$ nello spazio affine $\mathbb{A}$, ogni altro punto P si scrive unicamente come combinazione baricentrica*

$$P = \sum_i \alpha_i P_i \quad \text{con} \quad \alpha_i \in \Bbbk \quad e \quad \sum_i \alpha_i = 1.$$

La $(n+1)$-upla ordinata $\begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_n \end{pmatrix}$ si dice delle coordinate baricentriche di P nel riferimento dato. È una facile osservazione che allora la n-upla $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ è quella delle coordinate cartesiane affini di P in quel riferimento, e che $\alpha_0 = 1 - \sum_{i>0} \alpha_i$.

2.3.1. Condizioni di allineamento di punti in coordinate baricentriche. Dati tre punti in un piano affine, e fissato un riferimento affine su quel piano, i tre punti dati sono allineati se e solo se il determinante della matrice delle loro coordinate baricentriche si annulla. In generale, la condizione per $m + 1$ punti di essere in posizione generale si esprime in coordinate baricentriche tramite il rango della matrice formata dalle coordinate dei punti (rango massimo).

2.3.2. Sottospazi affini in coordinate baricentriche. Scelto un riferimento affine, le coordinate baricentriche dei punti soddisfano sempre alla condizione che la somma sia 1, cioè alla equazione lineare non omogenea $\sum_{i=0}^{1} X_i = 1$. Si vede quasi subito che ogni sottospazio affine può essere descritto usando questa equazione e un sistema di equazioni omogeneo nelle coordinate baricentriche, che si ottiene dalle equazioni cartesiane (lineari non necessariamente omogenee) sostituendo i termini costanti c con $c \sum_{i=0}^{1} X_i$. Queste si dicono equazioni del sottospazio affine nelle coordinate baricentriche di quel riferimento.

Ad esempio, per rette in un piano affine, le equazioni in coordinate baricentriche sono (a parte quella comune di somma 1) equazioni omogenee nelle tre coordinate, e la condizione per tre rette di essere in un fascio è che si annulli il determinante della matrice del sistema delle tre equazioni.

2.4. Definizione (combinazioni convesse reali di punti: m-edri). *Nel caso $\Bbbk = \mathbb{R}$ (in generale per i campi ordinati, per es. $\mathbb{Q}$), possiamo descrivere il segmento tra P_1 e P_2 come le combinazioni pesate dei due punti con i combinatori $\alpha_1, \alpha_2 \in [0, 1]$; il triangolo di vertici P_1, P_2 e P_3*

tramite le combinazioni pesate con $\alpha_1, \alpha_2, \alpha_3 \in [0,1]$*; in generale l'inviluppo convesso di* m *punti si rappresenta tramite le combinazioni*

$$\sum_i \alpha_i P_i, \quad \text{con} \quad \sum_i \alpha_i = 1 \quad e \quad 0 \leqslant \alpha_i \leqslant 1 \quad \text{per ogni } i.$$

L'inviluppo convesso di m *punti in posizione generale si dice un* m*-edro (segmento per* $m=2$*, triangolo per* $m=3$*, tetraedro per* $m=4$*).*

$\alpha P+\beta Q$ $(\alpha+\beta=1)$ $\alpha P+\beta Q+\gamma R$ $(\alpha+\beta+\gamma=1)$ $\alpha P+\beta Q+\gamma R+\delta S$ $(\alpha+\beta+\gamma+\delta=1)$

2.4.1. Osservazione. Si noti che la scelta di un n-edro ($n+1$ punti in posizione generale) in uno spazio affine reale di dimensione n permette di dividere lo spazio affine stesso in 2^n-1 zone definite dalla sequenza dei segni (positivi o negativi) delle coordinate baricentriche (le zone sono in numero di $3, 7, 15, 31, 63...$ in dimensione rispettivamente $1, 2, 3, 4, 5, ...$).

2.5. Definizione-Teorema (baricentri). *Supponiamo il campo di caratteristica nulla, oppure che i denominatori usati siano non nulli.*

Il punto medio del segmento tra P_1 *e* P_2 *è il punto* $\frac{1}{2}P_1+\frac{1}{2}P_2$*.*

Il baricentro del triangolo di vertici P_1*,* P_2 *e* P_3 *(punti non allineati) è il punto* $B=\frac{1}{3}P_1+\frac{1}{3}P_2+\frac{1}{3}P_3$ *e appartiene alle rette congiungenti ogni vertice* P_i *col punto medio* M_i *del lato opposto; risulta che* $B=\frac{1}{3}P_i+\frac{2}{3}M_i$ *(per ogni* i*).*

Il baricentro del tetraedro di vertici P_1*,* P_2*,* P_3 *e* P_4 *(punti non complanari) è il punto* $B=\frac{1}{4}P_1+\frac{1}{4}P_2+\frac{1}{4}P_3+\frac{1}{4}P_4$ *e appartiene alle rette congiungenti ogni vertice* P_i *col baricentro* B_i *del triangolo opposto, e risulta che* $B=\frac{1}{4}P_i+\frac{3}{4}B_i$ *(per ogni* i*).*

Dati m *punti* $P_1, \dots, P_m$ *in posizione generale, il baricentro dell'*m*-edro costituito da quei punti è il punto* $B=\frac{1}{m}P_1+\dots+\frac{1}{m}P_m$*, e appartiene alle rette congiungenti ogni vertice* P_i *col baricentro* B_i *dell'*$(m-1)$*-edro opposto (quello generato dagli altri vertici), e risulta* $B=\frac{1}{m}P_i+\frac{m-1}{m}B_i$ *(per ogni* i*).*

In generale per le definizioni basta che la caratteristica del campo non divida il numero di punti che si usa.

Dimostrazione. Facile esercizio. □

2.5.1. Osservazione. Si osservi che la nozione di punto medio e in generale di baricentro non ha, a priori, a che fare con le distanze; noi non abbiamo ancora definito cosa siano le distanze tra

punti. La definizione di baricentro dipende solo dalla struttura affine, vale a dire dall'azione dello spazio vettoriale, e dal fatto che i vettori possono essere moltiplicati per gli scalari $\frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots$ (in corpi di caratteristica 0, in cui ogni intero è invertibile; cosa succede di queste nozioni in corpi di caratteristica positiva?).

2.5.2. Problema. Per esempio nel caso di caratteristica 2, dato un triangolo (tre punti non allineati e le tre rette congiungenti), è ben definito il baricentro (perché $3 = 1$ è invertibile), ma non sono definiti i punti medi dei lati (perché $2 = 0$ non è invertibile). Si può vedere che le rette congiungenti un vertice e il baricentro sono parallele al lato opposto.

Altro esempio nel caso di caratteristica 3, dato un triangolo (tre punti non allineati e le tre rette congiungenti), non è definito il baricentro (perché $3 = 0$ non è invertibile), ma sono definiti i punti medi dei lati (perché $2 = -1$ è invertibile). Si può vedere che le mediane, ovvero le rette congiungenti un vertice con il punto medio del lato opposto sono parallele tra loro.

2.5.3. Dato un simplesso formato da $n+1$ punti in posizione generale, i baricentri delle sue facce (gli $n+1$ n-simplessi ottenuti dimenticando uno alla volta ciascuno dei punti) formano un $(n+1)$-simplesso in qualche modo "simile" al precedente, i cui punti si ottengono applicando la matrice $\frac{1}{n}(\Sigma e_i)(\Sigma e_i)^{\mathrm{t}} - \frac{1}{n}\mathbb{I}_{n+1}$ (di ordine $n+1$, con zero nella diagonale principale, $1/n$ nelle altre posizioni).

Viceversa, dato un $(n+1)$-simplesso è sempre possibile determinarne un altro di cui quello dato è il simplesso dei baricentri delle facce: si nota facilmente che esso si ottiene applicando la matrice $(\Sigma e_i)(\Sigma e_i)^{\mathrm{t}} - n\mathbb{I}_{n+1}$ (di ordine $n+1$, con $1-n$ nella diagonale principale, 1 nelle altre posizioni), che è quindi l'inversa della matrice precedente...

Si noti la matrice $(\Sigma e_i)(\Sigma e_i)^{\mathrm{t}}$, che è quella di rango 1 avente tutte le entrate uguali ad 1...

2.5.4. Problema: quadrangoli e parallelogrammi. Un quadrangolo piano è il dato di quattro punti distinti ordinati P_1, P_2, P_3, P_4 su un piano affine, e delle quattro rette che congiungono punti successivi nell'ordine ciclico.

Un quadrangolo piano P_1, P_2, P_3, P_4 si dice un parallelogramma se $P_2 - P_1 = P_3 - P_4$. In questo caso vale anche che $P_3 - P_2 = P_4 - P_1$, cioè anche P_2, P_3, P_4, P_1 è un parallelogramma.

Supponiamo che la caratteristica di $\Bbbk$ si diversa da 2: allora P_1, P_2, P_3, P_4 è un parallelogramma se e solo se $\frac{P_1+P_3}{2} = \frac{P_2+P_4}{2}$ (cioè: se e solo se le diagonali si incontrano nei loro punti medi!).

Come si caratterizzano invece i parallelogrammi in caratteristica 2? Risposta divertente: un quadrangolo è parallelogramma se e solo se ogni vertice è baricentro degli altri tre...

2.5.5. Problema. Dati quattro punti P_1, P_2, P_3, P_4 in $\mathbb{A}^n(\mathbb{R})$, si consideri un quadrilatero (non necessariamente piano) da essi formato (basta scegliere un ordine tra i quattro punti); allora i baricentri dei quattro lati formano un parallelogramma, quindi in particolare sono complanari. Quanti di questi piani si possono ottenere a partire da quattro fissati punti?

2.5.6. Problema: quadrilateri piani completi. Un *quadrilatero piano completo* $\mathscr{Q}$ del piano affine $\mathbb{A}^2(\mathbb{C})$ è la figura costituita da quattro rette $r_i, i = 1,2,3,4$ a due a due non parallele, e a tre a tre non appartenenti ad uno stesso fascio. Le rette $r_i, i = 1,2,3,4$ sono dette i *lati* di $\mathscr{Q}$; i sei punti d'intersezione $P_{ij} = r_i \cap r_j$, ove $1 \leqslant i < j \leqslant 4$ sono detti i *vertici*; due vertici si dicono *opposti* se non appartengono ad uno stesso lato; le rette che congiungono una coppia di vertici opposti si dicono *diagonali*. I punti di intersezione delle diagonali si dicono i *punti diagonali*. Si faccia il disegno della figura seguendo la descrizione, e si mostri che i punti medi delle tre diagonali (cioè dei segmenti delimitati dalle coppie di vertici opposti) sono allineati.

Usando coordinate baricentriche nel riferimento P_{12}, P_{13}, P_{23} abbiamo

$$P_{12} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},\ P_{13} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},\ P_{23} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},\ P_{14} = \begin{pmatrix} \alpha \\ 1-\alpha \\ 0 \end{pmatrix},\ P_{24} = \begin{pmatrix} 1-\beta \\ 0 \\ \beta \end{pmatrix},\ P_{34} = \begin{pmatrix} 0 \\ \gamma \\ 1-\gamma \end{pmatrix},$$

e l'allineamento dei punti P_{14}, P_{24}, P_{34} è dato dalla condizione

$$\det \begin{pmatrix} 0 & 1-\beta & \alpha \\ \gamma & 0 & 1-\alpha \\ 1-\gamma & \beta & 0 \end{pmatrix} = 0\ .$$

D'altra parte abbiamo i punti medi

$$\tfrac{1}{2}P_{12} + \tfrac{1}{2}P_{34} = \tfrac{1}{2}\begin{pmatrix} 1 \\ \gamma \\ 1-\gamma \end{pmatrix},\ \tfrac{1}{2}P_{13} + \tfrac{1}{2}P_{24} = \tfrac{1}{2}\begin{pmatrix} 1-\beta \\ 1 \\ \beta \end{pmatrix},\ \tfrac{1}{2}P_{23} + \tfrac{1}{2}P_{14} = \tfrac{1}{2}\begin{pmatrix} \alpha \\ 1-\alpha \\ 1 \end{pmatrix},$$

e il loro allineamento è dato dalla condizione

$$\det\begin{pmatrix} 1 & 1-\beta & \alpha \\ \gamma & 1 & 1-\alpha \\ 1-\gamma & \beta & 1 \end{pmatrix} = \det\begin{pmatrix} 0 & -\beta & \alpha-1 \\ \gamma-1 & 0 & -\alpha \\ -\gamma & \beta-1 & 0 \end{pmatrix} = 0$$

(che è verificata per l'osservazione precedente).

Si vede facilmente che diversi quadrilateri piani completi hanno lo stesso triangolo diagonale. È vero che il quadrilatero è determinato dal triangolo diagonale e da un suo lato?

2.5.7. Problema: quadrangoli piani completi. La nozione precedente non è da confondere con quella di quadrangolo piano completo, che è formato da quattro punti in posizione generale (vertici), dalle sei rette (lati) che si ottengono congiungendo vertici, dai tre punti diagonali che si ottengono intersecando lati opposti (che supponiamo non paralleli), e dalle tre rette diagonali che congiungono punti diagonali.

Anche qui conviene fare un disegno, e si vede facilmente che diversi quadrangoli piani completi hanno lo stesso triangolo diagonale. È vero che il quadrangolo è determinato dal triangolo diagonale e da un suo vertice?

♠ **2.6.** Definizione (rapporto semplice). *Dati tre punti allineati $X, A, B \in \mathbb{A}$, se $X = \lambda A + \mu B$ con $\lambda + \mu = 1$, definiamo*

$$(A\ B\ X) := -\frac{\mu}{\lambda}\ .$$

Se $\xi, \alpha, \beta \in \Bbbk$ sono le coordinate di A, B, X in un riferimento sulla retta che li contiene, allora

$$(A\ B\ X) = \frac{\xi - \alpha}{\xi - \beta}$$

("rapporto tra le distanze", anche se la terminologia è abusiva, visto che non abbiamo ancora definito una nozione di distanza: è tuttavia interessante notare che in Geometria Affine abbiamo un termine che tiene conto del rapporto tra termini che saranno definiti solo in Geometria Euclidea, a meno del segno).

Verifichiamo la seconda formula: siano P_0 e P_1 il riferimento scelto. Allora $X = P_0 + \xi(P_1 - P_0)$, $A = P_0 + \alpha(P_1 - P_0)$, $B = P_0 + \beta(P_1 - P_0)$. e possiamo ricavare

$$X = \lambda A + \mu B = P_0 + (\lambda\alpha + \mu\beta)(P_1 - P_0).$$

Quindi dall'uguaglianza $\xi = \lambda\alpha + \mu\beta$ insieme alla condizione $\lambda + \mu = 1$, troviamo $\lambda = \frac{\xi-\beta}{\alpha-\beta}$ e $\mu = \frac{\alpha-\xi}{\alpha-\beta}$, da cui la formula voluta.

2.6.1. Osservazione sulla notazione. In molti testi classici vi sono notazioni diverse per il rapporto semplice: quello che qui indichiamo con $(A\ B\ X)$ puè essere indicato con $[X; A, B]$ o $(X; A, B)$ per indicare che si usano i punti A, B come riferimento e le coordinate baricentriche di X in quel riferimento.

2.6.2. Un modo più semplice, forse, per pensare al rapporto semplice è il seguente: se X, A, B sono allineati, allora i vettori $X - B$ e $X - A$ sono dipendenti, e possiamo "definire" il loro "quoziente" $\frac{X-A}{X-B}$ come lo scalare $c \in \Bbbk$ tale che $X - A = c(X - B)$. Questo chiaramente si può fare solo per vettori dipendenti (definire un "quoziente" per vettori qualsiasi in $\mathbb{R}^2$ porta alla struttura di $\mathbb{C}$, per vettori in $\mathbb{R}^3$ porta alla struttura dei quaternioni di Hamilton...)

Ebbene: siccome da $X = \lambda A + \mu B$ segue che $X - B = \lambda(A - B)$ e $X - A = -\mu(A - B)$, abbiamo che il rapporto semplice è proprio il quoziente di vettori

$$(A\ B\ X) = \frac{X - A}{X - B}$$

(com'era prevedibile dalla formula in coordinate).

2.6.3. X è il punto medio tra A e B sse $(A\ B\ X) = -1$.

2.6.4. Azione delle permutazioni. Il gruppo delle permutazioni su tre elementi (gruppo di ordine 6) agisce sull'ordine dei tre punti di un rapporto semplice dando sei possibili valori. Dati tre

punti allineati $A, B, C \in \mathbb{A}$, se $(A\ B\ C) = \varrho$, allora:

$$(A\ B\ C) = \varrho \qquad (B\ A\ C) = \frac{1}{\varrho}$$
$$(B\ C\ A) = \frac{\varrho - 1}{\varrho} \qquad (C\ B\ A) = \frac{\varrho}{\varrho - 1}$$
$$(C\ A\ B) = \frac{1}{1-\varrho} \qquad (A\ C\ B) = 1 - \varrho$$

(si lasciano le verifiche per esercizio). Come piccolo esercizio di teoria dei gruppi si può notare che le sei funzioni razionali di ϱ date da

$$\varrho, \quad \frac{1}{\varrho}, \quad 1-\varrho, \quad \frac{1}{1-\varrho}, \quad \frac{\varrho}{\varrho-1}, \quad \frac{\varrho-1}{\varrho},$$

formano un gruppo sotto l'operazione di composizione, e che tale gruppo è isomorfo al gruppo delle permutazioni su tre oggetti. Lo stesso gruppo può essere visto come sottogruppo delle trasformazioni di Moebius, o come sottogruppo delle matrici $\mathrm{GL}_2(\Bbbk)/\pm 1$ formato dalle matrici

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix},$$

(serve che il campo $\Bbbk$ abbia caratteristica diversa da 2 e 3?).

2.6.5. Qualche combinazione.

Dati quattro punti allineati $A, B, C, D \in \mathbb{A}$, abbiamo che $(A\ B\ C) = (A\ D\ C)(D\ B\ C)$.

Da questo, o direttamente, segue anche la relazione tra $(A\ B\ X)$ e $(A'\ B'\ X)$: si ha

$$(A\ B\ X)(B\ B'\ X) = (A\ A'\ X)(A'\ B'\ X)$$

(che è $(A\ B'\ X)$).

Date due coppie di punti allineati A, B e X, Y risulta $(A\ B\ X)(X\ Y\ B) = (A\ B\ Y)(X\ Y\ A)$, ovvero

$$(A\ B\ X)(B\ A\ Y)(X\ Y\ B)(Y\ X\ A) = 1.$$

Date due terne di punti allineati A, B, C e X, Y, Z risulta

$$(A\ B\ Z)(C\ A\ Y)(B\ C\ X)(X\ Y\ C)(Z\ X\ B)(Z\ Y\ A) = 1.$$

♠ **2.7.** Teorema (Ceva e Menelao). *Sia dato un triangolo di vertici i punti A, B, C (non allineati); siano A', B', C' tre punti rispettivamente sulle rette $B \vee C$, $A \vee C$, $A \vee B$; allora:*

(Menelao) *A', B', C' sono allineati se e solo se $(A\ B\ C')(B\ C\ A')(C\ A\ B')$=1;*

(Ceva) *$A \vee A'$, $B \vee B'$, $C \vee C'$ sono in un fascio sse $(A\ B\ C')(B\ C\ A')(C\ A\ B')$=−1.*

Dimostrazione. Siano $A' = \alpha B + \alpha' C$, $B' = \beta A + \beta' C$, $C' = \gamma A + \gamma' B$ (con $\alpha + \alpha' = \beta + \beta' = \gamma + \gamma' = 1$), da cui $(B\ C\ A') = -\alpha'/\alpha$, $(C\ A\ B') = -\beta/\beta'$, $(A\ B\ C') = -\gamma'/\gamma$.

Le coordinate baricentriche dei punti A', B', C' nel sistema di riferimento dato da A, B, C sono date da $\left(\begin{smallmatrix} 0 \\ \alpha \\ \alpha' \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} \beta \\ 0 \\ \beta' \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} \gamma \\ \gamma' \\ 0 \end{smallmatrix}\right)$, rispettivamente, quindi i tre punti sono allineati se e solo se

$$\det \begin{pmatrix} 0 & \beta & \gamma \\ \alpha & 0 & \gamma' \\ \alpha' & \beta' & 0 \end{pmatrix} = \alpha\beta'\gamma + \alpha'\beta\gamma' = 0$$

che equivale a $\frac{\alpha'}{\alpha}\frac{\beta}{\beta'}\frac{\gamma'}{\gamma} = -1$, come si voleva.

Le equazioni in coordinate baricentriche delle rette $A \vee A'$, $B \vee B'$, $C \vee C'$ sono date dalle righe $\begin{pmatrix} 0 & \alpha' & -\alpha \end{pmatrix}, \begin{pmatrix} \beta' & 0 & -\beta \end{pmatrix}, \begin{pmatrix} \gamma' & -\gamma & 0 \end{pmatrix}$, rispettivamente quindi le tre rette sono in un fascio se e solo se

$$\det \begin{pmatrix} 0 & \alpha' & -\alpha \\ \beta' & 0 & -\beta \\ \gamma' & -\gamma & 0 \end{pmatrix} = \alpha\beta'\gamma - \alpha'\beta\gamma' = 0$$

che equivale a $\frac{\alpha'}{\alpha}\frac{\beta}{\beta'}\frac{\gamma'}{\gamma} = 1$, come si voleva. □

2.7.1. Si osservi che il rapporto semplice nel campo reale è positivo o negativo a seconda che il terzo punto sia esterno o interno ai primi due.

Quindi, come conseguenza del teorema di Menelao, si vede che se una retta taglia due lati di un triangolo in punti interni, deve tagliare il terzo lato in un punto esterno; cioè non è possibile che una retta tagli tre lati di un triangolo in punti interni ai lati, o anche uno solo.

Cosa si può dire invece dal teorema di Ceva?

2.7.2. Nella situazione di Menelao, calcolare il rapporto semplice $(A'\ B'\ C')$ (in termini per esempio dei rapporti semplici usati nel teorema). Ha senso fare la stessa domanda nella situazione di Ceva, cioè esiste un rapporto semplice tra tre rette di un fascio (attenzione: distinguere i casi di fasci propri e paralleli)?

2.7.3. Generalizzazioni. Generalizzare il teorema di Menelao per poligoni piani con n vertici: scegliendo un punto su ogni lato, sotto quale condizione questi punti risultano allineati?

Generalizzare il teorema di Menelao agli spazi affini di dimensione n: dato un riferimento affine $P_0, \dots, P_n$, e un punto R_i in ogni retta $P_i \vee P_{i+1}$ (usando $P_{n+1} = P_0$), sotto quali condizioni i punti R_i stanno su un iperpiano?

2.8. Problema: teorema di (iper)Talete. *Dati tre iperpiani π_0, π_1, π_2 paralleli a due a due distinti in uno spazio affine, e due rette r, s trasverse agli iperpiani, siano P_0, P_1, P_2 e Q_0, Q_1, Q_2 rispettivamente i punti di intersezione delle rette con i tre iperpiani.*

Allora abbiamo che $(P_0\ P_1\ P_2) = (Q_0\ Q_1\ Q_2)$ ovvero che $\frac{P_2-P_0}{P_1-P_0} = \frac{Q_2-Q_0}{Q_1-Q_0}$.

Vale il viceversa, cio'è è vero che tre iperpiani distinti sono paralleli se e solo se per tutte le (per quante?) rette trasverse il rapporto semplice dei punti di intersezione è costante?

Si osservi in particolare che il teorema di Talete è affermazione puramente affine, cioè non richiede nozioni di distanza o metrica.

2.8.1. È utile affrontare il problema sia in termini di calcolo vettoriale, o di calcolo baricentrico, sia in termini di coordinate scegliendo un riferimento in cui iperpiani e rette abbiamo equazioni facili...

Per esempio si può scegliere un riferimento in cui i tre piani paralleli abbiano equazioni cartesiane $X_1 = 0$, $X_1 = 1$, $X_1 = a$ e vedere che per ogni retta trasversa abbiamo punti per cui le coordinate X_1 sono rispettivamente $0, 1, a$, e quindi rapporto semplice sempre $(a-0)/(a-1)$ indipendente dalla retta.

Oppure, supponendo le rette r, s sghembe, possiamo ridurre il problema allo spazio di dimensione 3 generato dalle due rette, e usare i punti P_0, P_1, Q_0, Q_1 come riferimento, e imporre la condizione che il vettore differenza tra $P_2 = \lambda_0 P_0 + \lambda_1 P_1$ (con $\lambda_0 + \lambda_1 = 1$, quindi $(P_0\ P_1\ P_2) = -\lambda_1/\lambda_0$) e $Q_2 = \mu_0 Q_0 + \mu_1 Q_1$ (con $\mu_0 + \mu_1 = 1$) appartenga allo spazio generato da $P_0 - Q_0$ e $P_1 - Q_1$.

2.8.2. È possibile, e come, ridursi al caso classico del piano affine (tre rette parallele tagliate da due trasversali...)?

2.8.3. Discutere in particolare il caso di due iperpiani paralleli tagliati dalle rette di una stella (di centro un punto esterno agli iperpiani). In questo caso vi è anche una proporzionalità che riguarda i segmenti tagliati su ciascuno dei piani (questioni di triangoli simili).

2.9. Problema: teorema di Desargues affine. *Dati due triangoli di vertici A, B, C e A', B', C' in un spazio affine, se i lati omologhi sono paralleli (cioè $X \vee Y$ è parallelo a $X' \vee Y'$ per ogni $X \in \{A, B, C\}$), allora le rette per vertici omologhi $A \vee A'$, $B \vee B'$, $C \vee C'$ sono in un fascio (proprio, cioè sono concorrenti in un punto, oppure improprio, cioè sono parallele).*

Cosa si può dire del viceversa? Per esempio: se le rette per vertici omologhi sono in un fascio, e due coppie di lati omologhi sono paralleli, allora anche la terza coppia lo è...

2.9.1. Si può dimostrare usando Talete?

2.9.2. Usando coordinate cartesiane, possiamo dimostrare che se due coppie di lati omologhi sono paralleli, allora la terza coppia lo è se e solo se i triangoli sono prospettivi: possiamo usare un triangolo come riferimento affine, quindi $A = \binom{0}{0}$, $B = \binom{1}{0}$, $C = \binom{0}{1}$, poi $A' = \binom{x}{y}$, $B' = \binom{x'}{y}$, $C' = \binom{x}{y'}$ (abbiamo imposto il parallelismo dei lati AB, $A'B'$ e AC, $A'C'$). Ora la condizione di parallelismo per la terza coppia di lati è $\det \begin{pmatrix} 1 & x'-x \\ -1 & y-y' \end{pmatrix} = 0$, mentre la condizione di fascio per le tre rette sui vertici omologhi è $\det \begin{pmatrix} 0 & y & -x \\ y & -y & x'-1 \\ x & y'-1 & -x \end{pmatrix} = 0$ (le tre righe sono le equazioni cartesiane delle tre rette), e si vede subito che si riducono entrambe a $x' - x = y' - y$, e quindi sono equivalenti.

2.9.3. In Geometria Proiettiva si vedrà il vero teorema di Desargue, molto più semplice ed elegante.

2.10. Problema: teorema di Pappo affine. *Date due rette incidenti in un piano affine, e tre punti A, B, C e A', B', C' su ciascuna retta, distinti tra loro e dal punto di intersezione, abbiamo che: se $A \vee C'$ è parallela a $C \vee A'$ e $A \vee B'$ è parallela a $B \vee A'$, allora anche $B \vee C'$ è parallela a $C \vee B'$.*

2.10.1. Cosa si può invece dire se le coppie di rette evidenziate si intersecano?

2.10.2. Anche in questo caso, in Geometria Proiettiva si vedrà il vero teorema di Pappo, molto più semplice ed elegante.

♠♠ **2.11.** Problema: assiomatica baricentrica per lo spazio affine. *Trovare una assiomatica per lo spazio affine (su un corpo di caratteristica diversa da 2) in cui l'operazione definita sia il calcolo baricentrico tra coppie di punti.* Per esempio, definire lo spazio affine come un insieme $\mathbb{A}$ dotato di una mappa $\Bbbk \times \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ che ad ogni (α, P, Q) con $\alpha \in \Bbbk$ e $P, Q \in \mathbb{A}$ associa $\alpha P + \alpha' Q$ punto di $\mathbb{A}$ ($\alpha' = 1 - \alpha$), soggetta ad alcune condizioni, quali:
(0) $1P + 0Q = P$ e $0P + 1Q = Q$ (azione di 1 e 0);
(1) $\alpha P + \alpha' Q = \alpha' Q + \alpha P$ (commutatività);
(2) distributività sui punti $\beta(\alpha P + \alpha' Q) + \beta'(\gamma P + \gamma' Q) = (\alpha\beta + \beta'\gamma)P + (\alpha'\beta + \beta'\gamma')Q$;
(3) distributività sui pesi $\beta(\alpha P + \alpha' Q) + \beta'(\alpha R + \alpha' S) = \alpha(\beta P + \beta' R) + \alpha'(\beta Q + \beta' S)$;
(4) omogeneità: per ogni $A, B, C \in \mathbb{A}$ e per ogni $\alpha, \beta \in \Bbbk$ esiste unico $X \in \mathbb{A}$ tale che $\alpha A + \alpha' B = \beta C + \beta' X$ (automaticamente per tale X risulta $X = \frac{1}{\beta'}(\alpha A + \alpha' B) - \frac{\beta}{\beta'} C$);
da cui poi ricavare la struttura di spazio vettoriale V delle traslazioni (come definire i vettori? classi di equivalenza di coppie di punti: $V = (\mathbb{A} \times \mathbb{A})/\sim$ con $(A, B) \sim (B, C)$ se e solo se $\frac{1}{2}A + \frac{1}{2}B = \frac{1}{2}C + \frac{1}{2}D$, questione di parallelogrammi, cioè $D = B + C - A = 2(\frac{1}{2}B + \frac{1}{2}C) - A$... poi le operazioni...) e l'azione piena e fedele di V su $\mathbb{A}$.

3. Trasformazioni affini e affinità.

3.1. Definizione (trasformazioni affini). *Siano $\mathbb{A}$ e $\mathbb{B}$ spazi affini di spazi direttori V e W rispettivamente. Una trasformazione affine è una applicazione insiemistica $F : \mathbb{A} \longrightarrow \mathbb{B}$ tale che "rispetta il calcolo baricentrico", i.e. per ogni insieme finito di punti $P_1, \dots, P_n$ e per ogni insieme di numeri reali $\alpha_1, \dots, \alpha_n$ tali che $\sum_{i=1}^n \alpha_i = 1$ si ha $F(\sum_{i=1}^n \alpha_i P_i) = \sum_{i=1}^n \alpha_i F(P_i)$.*

L'insieme delle trasformazioni affini di $\mathbb{A}$ in $\mathbb{B}$ si indica con $\mathrm{Trasf}(\mathbb{A}, \mathbb{B})$.

3.1.1. Nella definizione bastava chiedere che per ogni coppia di punti fossero rispettate le somme baricentriche, e poi estendere la proprietà per induzione ad ogni insieme finito di punti, tenendo conto della distributività del calcolo baricentrico.

3.1.2. La composizione di trasformazioni affini è ancora una trasformazione affine; se $F \in \mathrm{Trasf}(\mathbb{A}, \mathbb{B})$ e $G \in \mathrm{Trasf}(\mathbb{B}, \mathbb{C})$ allora $G \circ F \in \mathrm{Trasf}(\mathbb{A}, \mathbb{C})$.

3.1.3. Dalla definizione segue subito che una trasformazione affine manda sottospazi affini in sottospazi affini (ricordare che i sottospazi affini si descrivono come "somme pesate di punti").

3.2. Teorema (applicazioni lineari soggiacenti). *Sia $F : \mathbb{A} \longrightarrow \mathbb{B}$ una applicazione insiemistica tra spazi affini di spazi direttori V e W rispettivamente. I seguenti fatti sono equivalenti:*
(1) *F è trasformazione affine;*
(2) *esiste una applicazione lineare $\varphi : V \longrightarrow W$ con la proprietà che $F(P + v) = F(P) + \varphi(v)$ per ogni $P \in \mathbb{A}$ e ogni $v \in V$.*
(3) *esiste una applicazione lineare $\varphi : V \longrightarrow W$ tale che $F(P') - F(P) = \varphi(P' - P)$ per ogni coppia $P, P' \in \mathbb{A}$.*

Dimostrazione. Le condizioni (2) e (3) sono evidentemente equivalenti, basta porre $v = P' - P$.

Supponiamo vero (1), e per ogni vettore v, definiamo $\varphi(v) = F(P') - F(P)$ se $v = P' - P$; questa definizione non dipende dalla rappresentazione di v (se $v = Q' - Q$ allora $Q' = Q + P - P'$, e per ipotesi $F(Q') = F(Q) + F(P) - F(P')$), e definisce una applicazione lineare (verificare: è facile vedere che rispetta la somma, e si usa il calcolo baricentrico per verificare che rispetta il prodotto per gli scalari...) di V in W con le proprietà richieste in (3). Viceversa, è facile verificare che una funzione F come in (3) rispetta il calcolo baricentrico, e dunque è una trasformazione affine. □

3.3. Proposizione (rappresentazione vettoriale). *La scelta di un punto $P \in \mathbb{A}$ e un punto $Q \in \mathbb{B}$ permette di descrivere le trasformazioni affini tramite coppie (w, φ) con $w \in W$ e $\varphi : V \longrightarrow W$ applicazione lineare. Precisamente abbiamo una biiezione*

$$\mathrm{Trasf}(\mathbb{A}, \mathbb{B}) \longrightarrow W \times \mathrm{Hom}_{\Bbbk}(V, W)$$

che manda F nella coppia $(F(P)-Q,\varphi)$ se φ è l'applicazione lineare soggiacente a F.

In questi termini, la composizione di due trasformazioni affini $F:\mathbb{A}\longrightarrow\mathbb{B}$ e $G:\mathbb{B}\longrightarrow\mathbb{C}$ (scelti $P\in\mathbb{A}$, $Q\in\mathbb{B}$, $R\in\mathbb{C}$) corrispondenti a (w,φ) e (z,ψ) è la coppia $(z,\psi)\circ(w,\varphi)=(z+\psi w,\psi\circ\varphi)$.

Dimostrazione. Fissato $P\in\mathbb{A}$, ogni trasformazione affine è determinata dal vettore $w=F(P)-Q$ e dalla applicazione lineare associata φ, tramite:

$$F(X)=F(P+(X-P))=F(P)+\varphi(X-P)=Q+w+\varphi(X-P)\ .$$

Viceversa è chiaro che ogni tale formula determina una trasformazione affine, e che due trasformazioni affini coincidono se e solo se sono rappresentate dalla stessa coppia in $W\times\mathrm{Hom}_{\Bbbk}(V,W)$.

L'affermazione per le composizioni segue dal calcolo

$$G\circ F(X)=G(Q+w+\varphi(X-P))=R+z+\psi(w+\varphi(X-P))=R+(z+\psi w)+\psi\circ\varphi(X-P)$$

da cui segue che $G\circ F$ è rappresentata come detto. □

3.3.1. Poiché la scelta di una base di V e una base di W permette di identificare $\mathrm{Hom}_{\Bbbk}(V,W)$ con lo spazio delle matrici $M_{n,m}(\Bbbk)$ (se $\mathbb{A}$ ha dimensione m e $\mathbb{B}$ dimensione n), e W con $M_{n,1}(\Bbbk)$ la scelta di riferimenti affini su $\mathbb{A}$ e $\mathbb{B}$ permette di avere una identificazione $\mathrm{Trasf}(\mathbb{A},\mathbb{B})\cong M_{n,1}(\Bbbk)\times M_{n,m}(\Bbbk)$. Inoltre la composizione di due trasformazioni affini F e G come sopra rappresentate da (w,A) e (z,B) è rappresentata da $(z,B)\circ(w,A)=(z+Bw,BA)$.

3.4. Proposizione (rappresentazione matriciale). *La scelta di un riferimento affine su $\mathbb{A}$ e di un riferimento affine su $\mathbb{B}$ permette di definire una mappa*

$$\mathrm{Trasf}(\mathbb{A},\mathbb{B})\longrightarrow M_{n+1,m+1}(\Bbbk)$$

che manda F nella matrice $\left(\begin{smallmatrix}1&0\\w&A\end{smallmatrix}\right)$ se la coppia $(w,A)\in M_{n,1}(\Bbbk)\times M_{n,m}(\Bbbk)$ rappresentava la trasformazione affine F come sopra. Si tratta di una mappa iniettiva, e ogni matrice della forma detta (la prima riga è $(1,0,\dots,0)\in M_{1,m+1}(\Bbbk)$) corrisponde ad una trasformazione affine.

In questi termini, la composizione di due trasformazioni affini $F:\mathbb{A}\to\mathbb{B}$ e $G:\mathbb{B}\to\mathbb{C}$ (scelti riferimenti affini in $\mathbb{A}$, $\mathbb{B}$, $\mathbb{C}$) è rappresentata dal prodotto delle due matrici.

Dimostrazione. Si tratta di mostrare che la mappa

$$M_{n,1}(\Bbbk)\times M_{n,m}(\Bbbk)\longrightarrow M_{n+1,m+1}(\Bbbk)$$

che manda (w,A) in $\left(\begin{smallmatrix}1&0\\w&A\end{smallmatrix}\right)$ è iniettiva e che l'immagine è quella descritta. Entrambe le cose sono facili. Per vedere che la composizione a sinistra corrisponde alla moltiplicazione di matrici a destra, basta osservare che

$$\begin{pmatrix}1&0\\z&B\end{pmatrix}\begin{pmatrix}1&0\\w&A\end{pmatrix}=\begin{pmatrix}1&0\\z+Bw&BA\end{pmatrix}$$

(facendo il prodotto a blocchi). □

3.4.1. Studiare l'effetto sulle matrici di cambiamenti di riferimento affine ("punto dello spazio affine e base dello spazio direttore") su dominio e codominio.

3.5. Riassunto. Abbiamo quindi visto le seguenti biiezioni:

$$\begin{array}{ccccccc}
\mathrm{Trasf}(\mathbb{A},\mathbb{B}) & \cong & W\times\mathrm{Hom}_{\Bbbk}(V,W) & \cong & M_{n,1}(\Bbbk)\times M_{n,m}(\Bbbk) & \cong & \left\{\left(\begin{smallmatrix}1&0\\w&A\end{smallmatrix}\right)\in M_{n+1,m+1}(\Bbbk)\right\}\\
\text{(scelti } P\in\mathbb{A},Q\in\mathbb{B}) & & \text{(scelte basi di } V,W) & & & & \\
F & \mapsto & (w=F(P)-Q,\varphi) & \mapsto & (w,A=\alpha_{\mathscr{V},\mathscr{W}}\varphi) & \mapsto & \left(\begin{smallmatrix}1&0\\w&A\end{smallmatrix}\right)
\end{array}$$

che rispettano le composizioni definite da:

$$GF\quad\leftrightarrow\quad(z,\psi)(w,\varphi)=(z+\psi w,\psi\varphi)\quad\leftrightarrow\quad(z,B)(w,A)=(z+Bw,BA)\quad\leftrightarrow\quad\left(\begin{smallmatrix}1&0\\z&B\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\w&A\end{smallmatrix}\right)\quad.$$

3.6. Teorema. *Fissato un riferimento nello spazio affine $\mathbb{A}$ e un insieme ordinato di punti della stessa cardinalità nello spazio affine $\mathbb{B}$, esiste una unica trasformazione affine che manda ordinatamente i punti del riferimento nei punti scelti.*

Dimostrazione. Ovvio, dall'analogo risultato per gli spazi vettoriali. □

3.7. Definizione-Teorema (affinità). *Le affinità di uno spazio affine $\mathbb{A}$ sono le trasformazioni affini biiettive di $\mathbb{A}$ in sè. L'insieme delle affinità di $\mathbb{A}$ è un gruppo sotto la composizione e si indica con* $\mathrm{Aff}(\mathbb{A})$. *Fissati due riferimenti affini su $\mathbb{A}$, esiste una unica affinità che manda ordinatamente i punti del primo riferimento nei punti del secondo.*

3.7.1. Dalla definizione segue subito che le affinità rispettano il rapporto semplice di tre punti allineati. Dunque, anticipando la nozione di "distanza tra punti" possiamo dire che le affinità non rispettano in generale le distanze, ma mantengono costanti opportuni rapporti tra le distanze.

3.7.2. La scelta di $P \in \mathbb{A}$ determina un isomorfismo del gruppo delle affinità di $\mathbb{A}$ in sè con il gruppo $V \times \mathrm{Aut}_{\Bbbk}(V)$ dotato di una opportuna composizione dato dalla regola $(v, \varphi) \circ (w, \psi) = (v+\varphi w, \varphi \circ \psi)$.

L'affinità identica è rappresentata dalla coppia $(0_V, \mathrm{id}_V)$. L'inversa dell'affinità rappresentata da (v, φ) è dunque $(-\varphi^{-1}v, \varphi^{-1})$.

3.7.3. La scelta di un riferimento affine in $\mathbb{A}$ determina un isomorfismo del gruppo delle affinità di $\mathbb{A}$ in sè con il sottogruppo del gruppo $\mathrm{GL}_{n+1}(\Bbbk)$ formato dalle matrici del tipo $\left(\begin{smallmatrix} 1 & 0 \\ v & A \end{smallmatrix}\right)$ con $A \in \mathrm{GL}_n(\Bbbk)$.

L'affinità identica è rappresentata dalla matrice identica. L'inversa dell'affinità rappresentata da $\left(\begin{smallmatrix} 1 & 0 \\ v & A \end{smallmatrix}\right)$ è dunque rappresentata dalla matrice inversa $\left(\begin{smallmatrix} 1 & 0 \\ -A^{-1}v & A^{-1} \end{smallmatrix}\right)$.

3.7.4. Analogamente a quanto detto per le trasformazioni affini, le matrici di affinità si indicano con $\mathrm{AGL}_n(\Bbbk)$ o $\mathrm{AGL}(n, \Bbbk)$ e formano un gruppo isomorfo al prodotto semidiretto $\Bbbk^n \rtimes \mathrm{GL}_n(\Bbbk)$ (ovvero, insiemisticamente il prodotto cartesiano, con l'operazione di composizione che tiene conto anche dell'azione di $\mathrm{GL}_n(\Bbbk)$ su $\Bbbk^n$).

3.7.5. Riassunto. Abbiamo quindi visto le seguenti biiezioni:

$$\begin{array}{ccccccc} \mathrm{Aff}(\mathbb{A}) & \cong & V \times \mathrm{Aut}_{\Bbbk}(V) & \cong & M_{n,1}(\Bbbk) \times \mathrm{GL}_n(\Bbbk) & \cong & \left\{ \left(\begin{smallmatrix} 1 & 0 \\ w & A \end{smallmatrix}\right) : A \in \mathrm{GL}_n(\Bbbk) \right\} \\ & \text{(scelto } P \in \mathbb{A}) & & \text{(scelta base di } V) & & & \\ F & \mapsto & (w = F(P) - P, \varphi) & \mapsto & (w, A = \alpha_{\mathscr{V}}\varphi) & \mapsto & \left(\begin{smallmatrix} 1 & 0 \\ w & A \end{smallmatrix}\right) \end{array} .$$

3.7.6. Definizione-Teorema (traslazioni). *Le traslazioni di $\mathbb{A}$ sono le affinità con applicazione lineare associata l'identità; osservare che* $\mathrm{Trasl}(\mathbb{A})$ *è sottogruppo delle affinità di $\mathbb{A}$ isomorfo a V, dunque in particolare commutativo.*

In un riferimento affine le traslazioni si riconoscono dall'avere matrice associata del tipo $\left(\begin{smallmatrix} 1 & 0 \\ v & \mathbb{I}_n \end{smallmatrix}\right)$ con $v \in M_{n,1}(\Bbbk)$; quindi la composizione di traslazioni corrisponde alla somma di vettori, poiché $\left(\begin{smallmatrix} 1 & 0 \\ v & \mathbb{I}_n \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ w & \mathbb{I}_n \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ v+w & \mathbb{I}_n \end{smallmatrix}\right)$.

3.7.7. Definizione-Teorema (affinità centrali). *Le affinità centrali di centro $P \in \mathbb{A}$ sono le affinità F di $\mathbb{A}$ con $F(P) = P$; osservare che* $\mathrm{Centr}_P(\mathbb{A})$ *è sottogruppo delle affinità di $\mathbb{A}$ isomorfo a* $\mathrm{Aut}_{\Bbbk}(V)$ *(quindi non commutativo).*

In un riferimento affine con origine in P le affinità centrali di centro P si riconoscono dall'avere matrice associata del tipo $\left(\begin{smallmatrix} 1 & 0 \\ 0 & A \end{smallmatrix}\right)$ con $A \in \mathrm{GL}_n(\Bbbk)$; quindi la composizione di traslazioni corrisponde al prodotto di matrici, poiché $\left(\begin{smallmatrix} 1 & 0 \\ 0 & A \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & B \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & AB \end{smallmatrix}\right)$.

3.7.8. Si osservi che le traslazioni non commutano in generale con le affinità centrali di centro assegnato, poiché

$$\begin{pmatrix} 1 & 0 \\ v & \mathbb{I}_n \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v & A \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ Av & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}\begin{pmatrix} 1 & 0 \\ v & \mathbb{I}_n \end{pmatrix} ;$$

capire il significato geometrico (si pensi al piano) e caratterizzare i casi in cui le due affinità commutano.

♠ **3.7.9.** Si osservi quindi che $\mathrm{Aff}(\mathbb{A})$ è insiemisticamente, ma non come gruppo, il prodotto cartesiano di $\mathrm{Trasl}(\mathbb{A})$ e $\mathrm{Centr}_P(\mathbb{A})$. In effetti, come gruppo, è un opportuno prodotto semidiretto: $\mathrm{Trasl}(\mathbb{A}) \rtimes \mathrm{Centr}_P(\mathbb{A})$ usando l'azione di $\mathrm{Centr}_P(\mathbb{A})$ su $\mathrm{Trasl}(\mathbb{A})$ tramite coniugio (t in $\varphi t \varphi^{-1}$). Dei due sottogruppi fattori uno risulta normale, l'altro no: quale?

In termini di matrici le matrici di affinità sono il prodotto semidiretto $\Bbbk^n \rtimes GL_n(\Bbbk)$, usando l'azione di $GL_n(\Bbbk)$ su $\Bbbk^n$ (pensato come gruppo di traslazioni) dove l'azione della matrice A manda

w in Aw (basta scrivere At_wA^{-1} che come traslazione è t_{Aw}), ovvero insiemisticamente il prodotto cartesiano con legge di composizione $(v, A)(w, B) = (v + Aw, AB)$.

3.7.10. Decomposizioni. Ogni affinità si può scrivere come composizione di una affinità centrale di centro assegnato seguita da una traslazione, o anche in ordine inverso, poiché

$$\begin{pmatrix} 1 & 0 \\ v & \mathbb{I}_n \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} 1 & 0 \\ A^{-1}v & \mathbb{I}_n \end{pmatrix} .$$

3.7.11. Definizione-Teorema (Omotetie). *Una affinità F di $\mathbb{A}$ ha la proprietà di mandare ogni retta in una retta parallela (cioè r è parallelo a $F(r)$ per ogni retta r) se e solo se l'applicazione lineare φ associata è (la moltiplicazione per) uno scalare $\alpha = \alpha(F)$ non nullo. Se tale scalare è 1, si tratta di una traslazione; altrimenti l'affinità si dice una omotetia, e lo scalare $\alpha \neq 1$ si dice il rapporto di omotetia. Ogni omotetia (non traslazione) possiede un unico punto unito, detto il centro di omotetia $C = C(F)$; centro e rapporto di omotetia determinano completamente l'omotetia.*

Per l'equivalenza si osserva subito che ogni vettore va trasformato in un suo multiplo, cioè $\varphi(v) = \alpha(v)v$, ma per due vettori indipendenti possiamo confrontare le costanti ragionando sulla somma: $\varphi(v) = \alpha(v)v$, $\varphi(w) = \alpha(w)w$ ma anche $\varphi(v + w) = \alpha(v + w)(v + w)$ e si confronta con $\varphi(v + w) = \varphi(v) + \varphi(w) = \alpha(v)v + \alpha(w)w$ per l'indipendenza, ottenendo $\alpha(v) = \alpha(v + w) = \alpha(w)$. Dunque la costante α dipende solo da F e non dai vettori. Il resto è facile. □

3.7.12. Se l'omotetia ha matrice $\left(\begin{smallmatrix} 1 & 0 \\ v & \alpha\mathbb{I}_n \end{smallmatrix}\right)$ allora il centro ha coordinate C che soddisfano $v + \alpha C = C$, ovvero $C = \frac{1}{1-\alpha}v$.

3.7.13. Composizioni. L'insieme di omotetie e traslazioni è un sottogruppo delle affinità. Se la composizione di due omotetie è una omotetia, allora i tre centri di omotetia sono allineati. Se invece la composizione di due omotetie è una traslazione (quando i rapporti di omotetia sono uno inverso dell'altro), la direzione è quella congiungente i due centri di omotetia.

3.7.14. Descrivere il comportamento di centri e rapporti di omotetia per composizione.

3.7.15. Il teorema di Talete, come anche quello di Desargues affine e altri, si può dimostrare usando la nozione di omotetia. Provare.

3.7.16. Simmetrie. Siano U e V sottospazi complementari di $V_n(\Bbbk)$ (i.e. $V_n(\Bbbk) = U \oplus V$). La simmetria di $\mathbb{A}^n(\Bbbk)$ di asse la varietà affine $P + U$ e direzione il sottospazio V è l'affinità definita dall'avere P come punto unito e applicazione lineare associata la simmetria di $V_n(\Bbbk)$ di asse U e direzione V (i.e. l'applicazione che al vettore $u + v$ con $u \in U$ e $v \in V$ associa $u - v$). Si osservi che i punti uniti della simmetria sono tutti e soli i punti di $P + U$. Inoltre il quadrato di una simmetria è sempre l'identità.

Si osservi che in un opportuno riferimento di $\mathbb{A}^n(\Bbbk)$ la simmetria viene rappresentata da una matrice $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & \mathbb{I}_u & 0 \\ 0 & 0 & -\mathbb{I}_v \end{smallmatrix}\right)$.

Cos'è la composizione di due simmetrie di direzione V comune?

3.7.17. Proiezioni (parallele, o dall'infinito). Siano U e V sottospazi complementari di $V_n(\Bbbk)$ (i.e. $V_n(\Bbbk) = U \oplus V$). La proiezione di $\mathbb{A}^n(\Bbbk)$ sulla varietà affine $P + U$ nella direzione del sottospazio V è la trasformazione affine definita dall'avere P come punto unito e applicazione lineare associata la proiezione di $V_n(\Bbbk)$ su U con direzione V (i.e. l'applicazione che al vettore $u + v$ con $u \in U$ e $v \in V$ associa u). Si osservi che i punti uniti della proiezione sono tutti e soli i punti di $P + U$. Inoltre il quadrato di una proiezione è sempre la proiezione stessa. Una proiezione può essere una affinità?

Si osservi che in un opportuno riferimento di $\mathbb{A}^n(\Bbbk)$ la proiezione viene rappresentata da una matrice $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & \mathbb{I}_u & 0 \\ 0 & 0 & \mathbb{O}_v \end{smallmatrix}\right)$.

Cos'è la composizione di due proiezioni di direzione V comune?

3.7.18. Proiezioni di centro affine. Siano L e L' sottospazi affini complementari di $\mathbb{A}^n(\Bbbk)$ (i.e. sghembi e $\mathbb{A}^n(\Bbbk) = L \vee L'$). La proiezione di $\mathbb{A}^n(\Bbbk)$ su L e di centro L' è la funzione $\pi : \mathbb{A}^n(\Bbbk) \smallsetminus L' \longrightarrow \mathbb{A}^n(\Bbbk)$ definita da $\pi(P) = (P \vee L') \cap L$ (verificare usando le formule di Grassmann affini che il risultato in effetti è un punto).

Si tratta di una funzione suriettiva $\pi : \mathbb{A}^n(\Bbbk) \smallsetminus L' \longrightarrow L$ i cui punti fissi sono esattamente gli elementi di L. Per ogni sottospazio affine M complementare con L' (dunque della stessa dimensione di L), π si restringe a una affinità $\pi : M \to L$ che si dice proiezione da M a L di centro L'.

3.8. Invarianti affini. Si dicono invarianti affini le proprietà dello spazio affine che risultano invarianti per affinità. Per esempio il calcolo baricentrico è per definizione invariante (e anzi per definizione caratterizza le trasformazioni affini); le posizioni reciproche di incidenza e parallelismo sono invarianti per ogni trasformazione affine; tutte le posizioni reciproche e i rapporti semplici sono invarianti per affinità. Vediamo alcuni casi di configurazioni nello spazio affine:

3.8.1. per i punti e per le coppie di punti non vi sono invarianti affini (più in generale, le affinità sono transitive su insiemi di punti in posizione generale);

3.8.2. per terne di punti: se sono allineati vi è un invariante affine (il rapporto semplice), altrimenti non vi è alcun invariante affine (tutti i triangoli non degeneri sono affinemente equivalenti);

3.8.3. per coppie di rette gli unici invarianti affini sono le posizioni reciproche;

3.9. Azione su sottospazi affini. *Siano $F \in \mathrm{Aff}(\mathbb{A})$ e $\mathbb{L}$ un sottinsieme di $\mathbb{A}$; allora $\mathbb{L}$ è sottovarietà affine se e solo se $F(\mathbb{L})$ lo è, e in tal caso hanno la stessa dimensione.*

Se $\mathbb{L}$ è definita dalle equazioni $BX = b$ con $B \in M_{m,n}(\Bbbk)$ e $b \in M_{m,1}(\Bbbk)$ e F è rappresentata dalla matrice $A = \left(\begin{smallmatrix} 1 & 0 \\ v & A' \end{smallmatrix}\right)$ allora $F(\mathbb{L})$ è definita dalle equazioni $BA'^{-1}X = b + BA'^{-1}v$. In forma compatta: se $\mathbb{L}$ è dato da $(-b\,B)\left(\begin{smallmatrix} 1 \\ X \end{smallmatrix}\right) = 0$, allora $F(\mathbb{L})$ è dato da $(-b\,B)A^{-1}\left(\begin{smallmatrix} 1 \\ X \end{smallmatrix}\right) = 0$.

Invece l'antimmagine di $\mathbb{L}$ tramite F ha equazioni date da $(-b\,B)A\left(\begin{smallmatrix} 1 \\ X \end{smallmatrix}\right) = 0$.

La prima asserzione dipende dal fatto che una affinità è una biiezione che rispetta il calcolo baricentrico.

D'altra parte, se $\mathbb{L}$ è definita da $(-b\,B)\left(\begin{smallmatrix} 1 \\ X \end{smallmatrix}\right) = 0$, allora

$$\begin{aligned} F(\mathbb{L}) &= \left\{ F(X) \,|\, (-b\,B)\begin{pmatrix} 1 \\ X \end{pmatrix} = 0 \right\} \\ &= \left\{ Y \,|\, \begin{pmatrix} 1 \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix}\begin{pmatrix} 1 \\ X \end{pmatrix} \text{ con } (-b\,B)\begin{pmatrix} 1 \\ X \end{pmatrix} = 0 \right\} \\ &= \left\{ Y \,|\, (-b\,B)\begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix}^{-1}\begin{pmatrix} 1 \\ Y \end{pmatrix} = 0 \right\} \end{aligned}$$

che giustifica la seconda asserzione; per l'ultima basta considerare che $F^*(\mathbb{L}) = (F^{-1})(\mathbb{L})$ (e che F^{-1} è affinità di matrice la matrice inversa di quella di F).

3.9.1. Punti e iperpiani uniti. Data una affinità F di $\mathbb{A}$ in sè, un sottospazio affine $\mathbb{L}$ si dice unito (o fisso) per F se $F(\mathbb{L}) = \mathbb{L}$ (non necessariamente punto per punto: se $F(P) = P$ per ogni $P \in \mathbb{L}$ si dice "puntualmente unito"). È facile studiare punti e iperpiani uniti: sia $A = \left(\begin{smallmatrix} 1 & 0 \\ v & A' \end{smallmatrix}\right)$ la matrice di F nel riferimento scelto.

(p) i punti uniti (o fissi) per F sono i punti $P \in \mathbb{A}$ tali che $F(P) = P$, e si trovano risolvendo il sistema $(\mathbb{I} - A')P = v$; in particolare, se A' non ha l'autovalore 1, allora F ha un unico punto unito, altrimenti può non averne o averne infiniti.

(i) gli iperpiani uniti (o fissi) per F sono gli iperpiani $\mathbb{H} \subseteq \mathbb{A}$ tali che $F(\mathbb{H}) = \mathbb{H}$; le loro equazioni, pensate come righe, devono essere autorighe della matrice A: quindi si tratta di cercare gli autovettori della matrice trasposta di A (a parte l'autovettore banale per l'autovalore 1, che non dà l'equazione di un piano, essendo $1 = 0$).

♠ **3.10.** Rappresentazione delle trasformazioni affini in coordinate baricentriche. Dato un riferimento affine, possiamo rappresentare i punti in termini di coordinate affini (in $\Bbbk^n$), eventualmente aggiungendo un 1 come prima coordinata (coordinate proiettive standard in $\Bbbk^{n+1}$, ma con $X_0 = 1$), oppure in termini di coordinate baricentriche (in $\Bbbk^{n+1}$, ma con $\Sigma_i X_i = 1$). Scrivere esattamente i passaggi tra i tre tipi di coordinate, e anche tra le equazioni cartesiane di iperpiani e sottospazi affini in generale.

Per rappresentare le trasformazioni affini, e in particolare le affinità, tramite matrici abbiamo usato le coordinate proiettive standard. Come si rappresentano le stesse trasformazioni usando le coordinate baricentriche? Si tratta di matrici di ordine $n + 1$ che devono mandare in sè l'iperpiano

$\Sigma_i X_i = 1$, quindi tali che le colonne hanno somma delle entrate pari a 1 (ovvero la matrice trasposta ha un certo autovettore di autovalore 1: quale?). Le matrici di traslazioni e di affinità centrali sono più difficili da scrivere in coordinate baricentriche: la traslazione di vettore $t \in \Bbbk^n$ e una affinità centrale di centro P_0 hanno matrici rispettivamente

$$\mathbb{I}_{n+1} + \begin{pmatrix} -u_n^{\mathrm{t}} t \\ t \end{pmatrix} u_{n+1}^{\mathrm{t}} \qquad \text{e} \qquad \begin{pmatrix} 1 & u_n^{\mathrm{t}}(\mathbb{I}_n - A) \\ 0 & A \end{pmatrix}$$

(in un riferimento che abbia come primo punto P_0), dove $u_m = \Sigma_i e_i$ è in vettore di $\Bbbk^m$ con tutte le coordinate pari a 1.

♠♠ **3.11.** Funzioni affini. In particolare abbiamo le trasformazioni affini di $\mathbb{A}$ sulla retta affine: $\mathbb{A} \longrightarrow \mathbb{A}^1_{\Bbbk}$. Queste trasformazioni si dicono "funzioni (affini) su $\mathbb{A}$", e il loro insieme si indica con $\mathcal{O}(\mathbb{A})$. Ogni trasformazione affine $F : \mathbb{A} \longrightarrow \mathbb{B}$ determina una applicazione $F^* : \mathcal{O}(\mathbb{B}) \longrightarrow \mathcal{O}(\mathbb{A})$ (per composizione). Per una applicazione insiemistica $F : \mathbb{A} \to \mathbb{B}$, i seguenti fatti sono equivalenti:

(i) $F : \mathbb{A} \to \mathbb{B}$ è una trasformazione affine;

(ii) per ogni $f \in \mathcal{O}(\mathbb{B})$ si ha $f \circ F \in \mathcal{O}(\mathbb{A})$;

(iii) scelti un punto $Q \in \mathbb{B}$ e una base $w_1, \dots, w_n$ di W, si ha $f_i \circ F \in \mathcal{O}(\mathbb{A})$ per $i = 1, \dots, n$ ove $f_i \in \mathcal{O}(\mathbb{B})$ sono definite da $f_i(Q + v) = w_i^*(v)$. [riconoscere che le f_i sono delle "proiezioni" per il riferimento scelto: si tratta delle composizioni $\mathbb{B} \xrightarrow{\simeq} \mathbb{A}^n_{\Bbbk} \longrightarrow \mathbb{A}^1_{\Bbbk}$ ove il primo isomorfismo è dato dalla scelta del riferimento in $\mathbb{B}$.]

Dunque le trasformazioni affini tra $\mathbb{A}$ e $\mathbb{B}$ si possono definire come "le applicazioni insiemistiche F il cui pull-back F^* manda $\mathcal{O}(\mathbb{B})$ in $\mathcal{O}(\mathbb{A})$", ovvero rispetta le funzioni (affini) definite sugli spazi.

Ricordare l'analogo risultato per le applicazioni lineari tra due spazi vettoriali. Riflettere sulla opportunità di definire le "trasformazioni tra spazi geometrici" come le applicazioni insiemistiche che "rispettano un prefissato tipo di funzioni" su quegli spazi.

4. Piano affine.

Siano $P_i = \binom{x_i}{y_i} \in \mathbb{A}^2(\Bbbk)$ punti del piano e $v_i = \binom{l_i}{m_i} \in V_2(\Bbbk)$ vettori dello spazio direttore.

4.1. Condizione di allineamento di tre punti. Tre punti P_0, P_1, P_2 sono allineati se e solo se

$$\begin{vmatrix} x_1 - x_0 & x_2 - x_0 \\ y_1 - y_0 & y_2 - y_0 \end{vmatrix} = 0 \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{vmatrix} = 0 \ .$$

4.2. Rette.

4.2.1. retta per due punti. La retta per i punti distinti P_0 e P_1 si scrive $P_0 + \langle P_1 - P_0 \rangle$; ha equazioni parametriche

$$\begin{cases} X = x_0 + \alpha(x_1 - x_0) \\ Y = y_0 + \alpha(y_1 - y_0) \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X - x_0 & x_1 - x_0 \\ Y - y_0 & y_1 - y_0 \end{vmatrix} = 0 \quad \text{ovvero,} \quad \begin{vmatrix} 1 & 1 & 1 \\ X & x_0 & x_1 \\ Y & y_0 & y_1 \end{vmatrix} = 0.$$

4.2.2. retta per un punto e direzione un vettore. La retta per il puntto P_0 e di direzione il vettore non nullo v si scrive $P_0 + \langle v_0 \rangle$; ha equazioni parametriche

$$\begin{cases} X = x_0 + \alpha l_0 \\ Y = y_0 + \alpha m_0 \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X - x_0 & l_0 \\ Y - y_0 & m_0 \end{vmatrix} = 0 \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 0 \\ X & x_0 & l_0 \\ Y & y_0 & m_0 \end{vmatrix} = 0.$$

4.2.3. Posizione reciproche di due rette. Date due rette $r_0{=}P_0{+}\langle v_0\rangle$ e $r_1{=}P_1{+}\langle v_1\rangle$ di equazioni cartesiane rispettivamente $a_0X{+}b_0Y{+}c_0{=}0$ e $a_1X{+}b_1Y{+}c_1{=}0$, esse risultano:

(1) incidenti se v_0 e v_1 sono linearmente indipendenti; ovvero se e solo se la matrice $\left(\begin{smallmatrix} a_0 & b_0 \\ a_1 & b_1 \end{smallmatrix}\right)$ ha rango due. In tal caso il punto di incidenza ha coordinate date dalla regola di Cramer applicata al sistema delle due equazioni.

(2) parallele e distinte se v_0 e v_1 sono linearmente dipendenti e $P_0{\notin}r_1$; ovvero se e solo se la matrice incompleta $\left(\begin{smallmatrix} a_0 & b_0 \\ a_1 & b_1 \end{smallmatrix}\right)$ ha rango uno e la matrice completa $\left(\begin{smallmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{smallmatrix}\right)$ ha rango due.

(3) coincidenti se v_0 e v_1 sono linearmente dipendenti e $P_0{\in}r_1$; ovvero se e solo se le matrici incompleta e completa hanno rango uno.

4.2.4. fasci di rette. Le rette passanti per un fissato punto P_0 si scrivono come $P_0{+}\langle\left(\begin{smallmatrix} l \\ m \end{smallmatrix}\right)\rangle$, ovvero $m(X{-}x_0){-}l(Y{-}y_0){=}0$ con $(l,m)\neq(0,0)$.

Le rette parallele ad un fissato vettore direzione v_0 si scrivono come $P{+}\langle v_0\rangle$ con P punto qualsiasi, ovvero $m_0X{-}l_0Y{+}c{=}0$ con $c{\in}\Bbbk$.

Due rette distinte r_0 e r_1 determinano un fascio di rette che si descrive tramite

$$\lambda(a_0X{+}b_0Y{+}c_0){+}\mu(a_1X{+}b_1Y{+}c_1){=}0, \quad \text{ovvero} \quad (\lambda a_0{+}\mu a_1)X{+}(\lambda b_0{+}\mu b_1)Y{+}(\lambda c_0{+}\mu c_1){=}0$$

al variare di $(\lambda,\mu)\neq(0,0)$.

Una retta r_2 appartiene al fascio determinato da r_0 e r_1 se e solo se la matrice completa del sistema delle tre rette ha determinante nullo.

4.3. Affinità del piano. La scelta di un riferimento affine sul piano $\mathbb{A}^2(\Bbbk)$ determina un isomorfismo del gruppo $\mathrm{Aff}(\mathbb{A}^2(\Bbbk))$ delle affinità del piano con il sottogruppo

$$\left\{\left(\begin{smallmatrix} 1 & 0 & 0 \\ a & & \\ b & & A \end{smallmatrix}\right) | a,b\in\Bbbk;\ A\in\mathrm{GL}_2(\Bbbk)\right\}$$

di $\mathrm{GL}_3(\Bbbk)$.

4.3.1. Azione sulle rette. L'immagine di una retta $r = P\vee Q$ (risp. $r = P+\langle v\rangle$) tramite una affinità F (di applicazione lineare associata φ) si calcola più facilmente come $F(r) = F(P)\vee F(Q)$ (risp. $F(r) = F(P)+\langle\varphi(v)\rangle$). Se la retta r è data tramite equazione cartesiana, per calcolare $F(r)$ bisogna usare la matrice inversa di F in quel riferimento.

4.3.2. Simmetrie rispetto a punti e rette. La matrice associata alla simmetria del piano rispetto al punto $P = \left(\begin{smallmatrix} x_0 \\ y_0 \end{smallmatrix}\right)$ è tale che $A = -\mathbb{I}_2$, e $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2x_0 \\ 2y_0 \end{smallmatrix}\right)$.

La matrice associata alla simmetria del piano di asse la retta $P+\langle v\rangle$ e di direzione w, ove $P = \left(\begin{smallmatrix} x_0 \\ y_0 \end{smallmatrix}\right)$, è tale che, posto $B = (v\,w)$ (matrice invertibile d'ordine due), $A = B\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)B^{-1}$, e $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = B\left(\begin{smallmatrix} 0 & 0 \\ 0 & 2 \end{smallmatrix}\right)B^{-1}\left(\begin{smallmatrix} x_0 \\ y_0 \end{smallmatrix}\right)$.

5. Spazio affine.

Siano $P_i = \left(\begin{smallmatrix} x_i \\ y_i \\ z_i \end{smallmatrix}\right)\in\mathbb{A}^3$ punti dello spazio e $v_i = \left(\begin{smallmatrix} l_i \\ m_i \\ n_i \end{smallmatrix}\right)\in V$ vettori dello spazio delle traslazioni.

5.1. Relazioni tra punti.

5.1.1. condizione di complanarità di quattro punti. quattro punti P_0,P_1,P_2,P_3 sono complanari se e solo se

$$\begin{vmatrix} x_1{-}x_0 & x_2{-}x_0 & x_3{-}x_0 \\ y_1{-}y_0 & y_2{-}y_0 & y_3{-}y_0 \\ z_1{-}z_0 & z_2{-}z_0 & z_3{-}z_0 \end{vmatrix}{=}0, \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 1 & 1 \\ x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ z_0 & z_1 & z_2 & z_3 \end{vmatrix}{=}0\ .$$

5.1.2. condizione di allineamento di tre punti. Tre punti P_0,P_1,P_2 sono allineati se e solo se

$$\mathrm{rk}\begin{pmatrix} x_1{-}x_0 & x_2{-}x_0 \\ y_1{-}y_0 & y_2{-}y_0 \\ z_1{-}z_0 & z_2{-}z_0 \end{pmatrix}{=}1, \quad \text{ovvero} \quad \mathrm{rk}\begin{pmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{pmatrix}{=}2\ .$$

5.2. Piani.

5.2.1. piano per tre punti non allineati. Il piano per tre punti non allineati P_0, P_1, P_2 si scrive $P_0+\langle P_1-P_0, P_2-P_0\rangle$; ha equazioni parametriche

$$\begin{cases} X=x_0+\alpha_1(x_1-x_0)+\alpha_2(x_2-x_0) \\ Y=y_0+\alpha_1(y_1-y_0)+\alpha_2(y_2-y_0) \\ Z=z_0+\alpha_1(z_1-z_0)+\alpha_2(z_1-z_0) \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X-x_0 & x_1-x_0 & x_2-x_0 \\ Y-y_0 & y_1-y_0 & y_2-y_0 \\ Z-z_0 & z_1-z_0 & z_2-z_0 \end{vmatrix}=0, \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 1 & 1 \\ X & x_0 & x_1 & x_2 \\ Y & y_0 & y_1 & y_2 \\ Z & z_0 & z_1 & z_2 \end{vmatrix}=0.$$

5.2.2. piano per un punto e direzione due vettori linearmente indipendenti. Il piano passante per P_0 e di giacitura lo spazio generato da due vettori linearmente indipendenti v_0, v_1 si scrive $P_0+\langle v_0, v_1\rangle$; ha equazioni parametriche

$$\begin{cases} X=x_0+\alpha l_0+\beta l_1 \\ Y=y_0+\alpha m_0+\beta m_1 \\ Z=z_0+\alpha n_0+\beta n_1 \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X-x_0 & l_0 & l_1 \\ Y-y_0 & m_0 & m_1 \\ Z-z_0 & n_0 & n_1 \end{vmatrix}=0 \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 0 & 0 \\ X & x_0 & l_0 & l_1 \\ Y & y_0 & m_0 & m_1 \\ Z & z_0 & n_0 & n_1 \end{vmatrix}=0.$$

5.2.3. posizioni reciproche di due piani. Dati due piani $\pi_0=P_0+\langle v_0, v_0'\rangle$ e $\pi_1=P_1+\langle v_1, v_1'\rangle$ di equazioni cartesiane rispettivamente $a_0X+b_0Y+c_0Z+d_0=0$ e $a_1X+b_1Y+c_1Z+d_1=0$, essi risultano:

(1) incidenti se $\mathrm{rk}(v_0\ v_0'\ v_1\ v_1')=3$; ovvero sse la matrice $\left(\begin{smallmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{smallmatrix}\right)$ ha rango due. In tal caso la retta di incidenza ha equazioni cartesiane date dal sistema delle due equazioni.

(2) paralleli e distinti se $\mathrm{rk}(v_0\ v_0'\ v_1\ v_1')=2$; (i.e. gli spazi direttori coincidono: $\langle v_0, v_0'\rangle=\langle v_1, v_1'\rangle$) e $P_0\notin\pi_1$ (i.e. $\pi_0\cap\pi_1=\varnothing$); ovvero sse la matrice incompleta $\left(\begin{smallmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{smallmatrix}\right)$ ha rango uno e la matrice completa $\left(\begin{smallmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \end{smallmatrix}\right)$ ha rango due.

(3) coincidenti se gli spazi direttori coincidono e $P_0\in\pi_1$; ovvero sse le matrici incompleta e completa hanno rango uno.

5.2.4. Fasci di piani. I piani contenenti una fissata retta $r_0=P_0+\langle v_0\rangle$ (asse del fascio) di equazioni cartesiane $\begin{cases} a_0X+b_0Y+c_0Z+d_0=0 \\ a_0'X+b_0'Y+c_0'Z+d_0'=0 \end{cases}$ si scrivono come $P_0+\langle v_0, \left(\begin{smallmatrix} l \\ m \\ n \end{smallmatrix}\right)\rangle$ con $\left(\begin{smallmatrix} l \\ m \\ n \end{smallmatrix}\right)$ vettore linearmente indipendente con v_0, ovvero

$$\lambda(a_0X+b_0Y+c_0Z+d_0)+\mu(a_0'X+b_0'Y+c_0'Z+d_0')=0$$

cioè

$$(\lambda a_0+\mu a_0')X+(\lambda b_0+\mu b_0')Y+(\lambda c_0+\mu c_0')Z+(\lambda d_0+\mu d_0')=0$$

al variare di $(\lambda,\mu)\neq(0,0)$.

I piani paralleli ad un fissato spazio direttore $\langle v_0, v_1\rangle$ si scrivono come $P+\langle v_0, v_1\rangle$ con P punto qualsiasi, ovvero

$$(m_0n_1-n_0m_1)X+(-l_0n_1+n_0l_1)Y+(l_0m_1-m_0l_1)Z+c=0$$

con $c\in\Bbbk$ (i coefficienti sono i minori d'ordine due di $(v_0\ v_1)$).

Due piani distinti π_0 e π_1 determinano un fascio di piani descritto da

$$\lambda(a_0X+b_0Y+c_0Z+d_0)+\mu(a_1X+b_1Y+c_1Z+d_1)=0,$$

ovvero

$$(\lambda a_0+\mu a_1)X+(\lambda b_0+\mu b_1)Y+(\lambda c_0+\mu c_1)Z+(\lambda d_0+\mu d_1)=0$$

per $(\lambda,\mu)\neq(0,0)$.

Un piano π_2 appartiene al fascio di piani determinato da π_0 e π_1 se e solo se la matrice completa del sistema dei tre piani ha rango due.

5.2.5. STELLE DI PIANI. I piani passanti per un fissato punto P_0 si scrivono come $P_0+\langle v,w\rangle$ con v e w vettori linearmente indipendenti, ovvero $m(X-x_0)+l(Y-y_0)+n(Z-z_0)=0$ con $(l,m,n)\neq(0,0,0)$.

I piani paralleli ad un fissato vettore direzione v_0 (ovvero a una qualsiasi retta r_0 di direzione v_0) si scrivono come $P+\langle v_0,v\rangle$ con P punto qualsiasi e v vettore linearmente indipendenti con v_0, ovvero $aX+bY+cZ+d=0$ con $d\in\Bbbk$, $(a,b,c)\neq(0,0,0)$ tale che $al_0+bm_0+cn_0=0$.

Tre piani distinti π_0, π_1 e π_2 che non appartengano ad un fascio determinano una stella di piani che si descrive tramite

$$\lambda(a_0X+b_0Y+c_0Z+d_0)+\mu(a_1X+b_1Y+c_1Z+d_1)+\nu(a_2X+b_2Y+c_2Z+d_2)=0$$

ovvero

$$(\lambda a_0+\mu a_1+\nu a_2)X+(\lambda b_0+\mu b_1+\nu b_2)Y+(\lambda c_0+\mu c_1+\nu c_2)Z+(\lambda d_0+\mu d_1+\nu d_2)=0$$

per $(\lambda,\mu,\nu)\neq(0,0,0)$.

5.3. RETTE.

5.3.1. RETTA PER DUE PUNTI DISTINTI. La retta per due punti distinti P_0,P_1 si scrive $P_0+\langle P_1-P_0\rangle$; ha equazioni parametriche

$$\begin{cases} X=x_0+\alpha(x_1-x_0)\\ Y=y_0+\alpha(y_1-y_0)\\ Z=z_0+\alpha(z_1-z_0)\end{cases}$$

ed equazioni cartesiane date dalla condizione:

$$\operatorname{rk}\begin{pmatrix} X-x_0 & x_1-x_0\\ Y-y_0 & y_1-y_0\\ Z-z_0 & z_1-z_0\end{pmatrix}=1,\quad \text{ovvero}\quad \operatorname{rk}\begin{pmatrix} 1 & 1 & 1\\ X & x_0 & x_1\\ Y & y_0 & y_1\\ Z & z_0 & z_1\end{pmatrix}=2.$$

5.3.2. RETTA PER UN PUNTO E DI DIREZIONE UN VETTORE. La retta per un punto P_0 e di direzione un vettore non nullo v_0 si scrive $P_0+\langle v_0\rangle$; ha equazioni parametriche

$$\begin{cases} X=x_0+\alpha l_0\\ Y=y_0+\alpha m_0\\ Z=z_0+\alpha n_0\end{cases}$$

ed equazioni cartesiane date da:

$$\operatorname{rk}\begin{pmatrix} X-x_0 & l_0\\ Y-y_0 & m_0\\ Z-z_0 & n_0\end{pmatrix}=1,\quad \text{ovvero}\quad \operatorname{rk}\begin{pmatrix} 1 & 1 & 0\\ X & x_0 & l_0\\ Y & y_0 & m_0\\ Z & z_0 & n_0\end{pmatrix}=2.$$

5.3.3. POSIZIONE RECIPROCHE DI DUE RETTE. Date due rette $r_0=P_0+\langle v_0\rangle$ e $r_1=P_1+\langle v_1\rangle$ di equazioni cartesiane rispettivamente $\begin{cases} a_0X+b_0Y+c_0Z+d_0=0\\ a_0'X+b_0'Y+c_0'Z+d_0'=0\end{cases}$ e $\begin{cases} a_1X+b_1Y+c_1Z+d_1=0\\ a_1'X+b_1'Y+c_1'Z+d_1'=0\end{cases}$, esse risultano:

(1) sghembe se v_0 e v_1 sono linearmente indipendenti e $r_0\cap r_1=\varnothing$, ovvero sse la matrice incompleta del sistema delle due rette ha rango tre, e la matrice completa rango quattro;
(2) incidenti e distinte se v_0 e v_1 sono linearmente indipendenti e $r_0\cap r_1\neq\varnothing$; ovvero sse le matrici incompleta e completa hanno rango tre. In tal caso il piano di appartenenza è dato da $P_0+\langle v_0,v_1\rangle$ ed è l'unico piano appartenente a entrambi i fasci di asse le due rette. Il punto di incidenza ha coordinate date dalla soluzione del sistema delle quattro equazioni.
(3) parallele e distinte se v_0 e v_1 sono linearmente dipendenti e $r_0\cap r_1=\varnothing$; ovvero sse la matrice incompleta ha rango due e la matrice completa ha rango tre. Il piano di appartenenza è $P_0+\langle P_1-P_0,v_0\rangle$ ed è l'unico piano appartenente a entrambi i fasci di asse le due rette.
(4) coincidenti se v_0 e v_1 sono linearmente dipendenti e $r_0\cap r_1\neq\varnothing$; ovvero sse la matrice incompleta e la matrice completa hanno rango due.

5.3.4. FASCI DI RETTE IN UN PIANO. Usando equazioni cartesiane, si tratta di intersecare il piano dato con la stella dei piani che soddisfano alle condizioni poste (passaggio per un punto o contenente una fissata direzione).

Se $\pi_0{=}P_0{+}\langle v_0, v_0'\rangle$ è il piano di giacenza, e si tratta del fascio per $P_1{\in}\pi_0$, il fascio di rette si scrive come $P_1{+}\langle \alpha v_0{+}\beta v_0'\rangle$ con $(\alpha,\beta)\neq(0,0)$; se si tratta del facio di rette di direzione $v_1{\in}\langle v_0, v_0'\rangle$ allora si scrive come $(P_0{+}\alpha v_0{+}\beta v_0'){+}\langle v_1\rangle$ con (α,β) qualsiasi.

5.3.5. STELLE DI RETTE. Le rette passanti per un fissato punto P_0 si scrivono come $P_0{+}\langle\left(\begin{smallmatrix} l\\ m\\ n\end{smallmatrix}\right)\rangle$ con $\left(\begin{smallmatrix} l\\ m\\ n\end{smallmatrix}\right)\neq\left(\begin{smallmatrix} 0\\ 0\\ 0\end{smallmatrix}\right)$, ovvero scegliendo due equazioni indipendenti tra le seguenti:
$m(X{-}x_0){-}l(Y{-}y_0){=}0$, $n(X{-}x_0){-}l(Z{-}z_0){=}0$ e $n(Y{-}y_0){-}m(Z{-}z_0){=}0$.

Le rette parallele ad un fissato vettore direzione v_0 si scrivono come $P{+}\langle v_0\rangle$ con $P=\left(\begin{smallmatrix} x\\ y\\ z\end{smallmatrix}\right)$ punto qualsiasi, ovvero scegliendo due equazioni indipendenti tra le seguenti:
$m_0(X{-}x){-}l_0(Y{-}y){=}0$, $n_0(X{-}x){-}l_0(Z{-}z){=}0$ e $n_0(Y{-}y){-}m_0(Z{-}z){=}0$.

5.4. POSIZIONI RECIPROCHE DI RETTE E PIANI: dati un piano $\pi_0{=}P_0{+}\langle v_0, v_0'\rangle$ e una retta $r_1{=}P_1{+}\langle v_1\rangle$, di equazioni cartesiane rispettivamente $a_0X{+}b_0Y{+}c_0Z{+}d_0{=}0$ e $\begin{cases} a_1X{+}b_1Y{+}c_1Z{+}d_1{=}0\\ a_1'X{+}b_1'Y{+}c_1'Z{+}d_1'{=}0\end{cases}$, essi risultano:

(1) incidenti se v_0,v_0' e v_1 sono linearmente indipendenti; ciò accade sse le matrici completa e incompleta del sistema piano-retta hanno rango comune tre; le coordinate del punto di intersezione si ottengono applicando la regola di Cramer a tale sistema;
(2) paralleli e disgiunti se $v_1{\in}\langle v_0, v_0'\rangle$ (i.e. se v_0,v_0' e v_1 sono linearmente dipendenti) e $\pi_0\cap r_1=\varnothing$; ovvero sse la matrice incompleta ha rango due e la matrice completa ha rango tre.
(3) appartenersi se $v_1{\in}\langle v_0, v_0'\rangle$ (i.e. se v_0,v_0' e v_1 sono linearmente dipendenti) e $\pi_0\cap r_1\neq\varnothing$; ovvero sse le matrici incompleta e completa hanno rango due. In tal caso $r_1\subseteq\pi_0$.

5.5. AFFINITÀ DELLO SPAZIO. La scelta di un riferimento affine sullo spazio $\mathbb{A}^3(\Bbbk)$ determina un isomorfismo del gruppo $\mathrm{Aff}(\mathbb{A}^3(\Bbbk))$ delle affinità dello spazio con il sottogruppo

$$\left\{\left(\begin{smallmatrix} 1 & 0\ 0\ 0\\ a & \\ b & A\\ c & \end{smallmatrix}\right)\,|a,b,c\in\Bbbk;\ A\in\mathrm{GL}_3(\Bbbk)\right\}$$

di $\mathrm{GL}_4(\Bbbk)$.

5.5.1. AZIONE SULLE RETTE E SUI PIANI. L'immagine di una retta $r=P\vee Q$ (risp. $r=P+\langle v\rangle$) tramite una affinità F (di applicazione lineare associata φ) si calcola più facilmente come $F(r)=F(P)\vee F(Q)$ (risp. $F(r)=F(P)+\langle\varphi(v)\rangle$).

L'immagine di un piano $\pi=P\vee Q\vee R$ (risp. $\pi=P+\langle v,w\rangle$) tramite una affinità F (di applicazione lineare associata φ) si calcola più facilmente come $F(\pi)=F(P)\vee F(Q)\vee F(R)$ (risp. $F(r)=F(P)+\langle\varphi(v),\varphi(w)\rangle$).

Se la retta r o il piano π sono dati tramite equazioni cartesiane, per calcolare $F(r)$ o $F(\pi)$ bisogna usare la matrice inversa di F in quel riferimento.

5.5.2. SIMMETRIE RISPETTO A PUNTI, RETTE E PIANI. La matrice associata alla simmetria dello spazio rispetto al punto $P=\left(\begin{smallmatrix} x_0\\ y_0\\ z_0\end{smallmatrix}\right)$ è tale che $A=-\mathbb{I}_3$, e $\left(\begin{smallmatrix} a\\ b\\ c\end{smallmatrix}\right)=\left(\begin{smallmatrix} 2x_0\\ 2y_0\\ 2z_0\end{smallmatrix}\right)$.

La matrice associata alla simmetria dello spazio di asse la retta $P+\langle u\rangle$ e di direzione $\langle v,w\rangle$, ove $P=\left(\begin{smallmatrix} x_0\\ y_0\\ z_0\end{smallmatrix}\right)$, è tale che, posto $B=(u\,v\,w)$ (matrice invertibile d'ordine tre), $A=B\left(\begin{smallmatrix} 1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{smallmatrix}\right)B^{-1}$, e $\left(\begin{smallmatrix} a\\ b\\ c\end{smallmatrix}\right)=B\left(\begin{smallmatrix} 0 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 2\end{smallmatrix}\right)B^{-1}\left(\begin{smallmatrix} x_0\\ y_0\\ z_0\end{smallmatrix}\right)$.

La matrice associata alla simmetria dello spazio di asse il piano $P+\langle u,v\rangle$ e di direzione $\langle w\rangle$, ove $P=\left(\begin{smallmatrix} x_0\\ y_0\\ z_0\end{smallmatrix}\right)$, è tale che, posto $B=(u\,v\,w)$ (matrice invertibile d'ordine tre), $A=B\left(\begin{smallmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{smallmatrix}\right)B^{-1}$, e $\left(\begin{smallmatrix} a\\ b\\ c\end{smallmatrix}\right)=B\left(\begin{smallmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 2\end{smallmatrix}\right)B^{-1}\left(\begin{smallmatrix} x_0\\ y_0\\ z_0\end{smallmatrix}\right)$.

5.6. ESEMPIO: SPAZIO (DELLE CODIFICHE *rgb*, *cmy*, *cmyk*) DEI COLORI. I problemi tecnici di produzione dei colori portano a privilegiare diversi tipi di rappresentazioni: nel caso di illuminazione e schermi si tende a sommare tre colori fondamentali (maggiore l'intensità più chiaro il colore), nel

caso di stampa su carta bianca si tende a sommare pigmenti colorati (maggiore quantità più scuro il colore), e cercando di minimizzare l'uso inserendo un colore nero nel caso delle stampanti.

La codifica internazionale *rgb* dei colori del 1931 usa come fondamentali $R = \left(\begin{smallmatrix}1\\0\\0\end{smallmatrix}\right)$ (red, rosso), $G = \left(\begin{smallmatrix}0\\1\\0\end{smallmatrix}\right)$ (green, verde), $B = \left(\begin{smallmatrix}0\\0\\1\end{smallmatrix}\right)$ (blue, blu), con valori compresi in un intervallo limitato che possiamo pensare $[0,1]$, e quindi rappresenta tutti i colori in un cubo $[0,1]^3$ dove $K = \left(\begin{smallmatrix}0\\0\\0\end{smallmatrix}\right)$ è il nero (black) e $W = \left(\begin{smallmatrix}1\\1\\1\end{smallmatrix}\right)$ è il bianco (white). Ogni colore X ha tre coordinate r, g, b tali che

$$X = K + r(R - K) + g(G - K) + b(B - K).$$

Qui abbiamo disegnato i lati del cubo dei colori evidenziando anche la diagonale dei grigi (segmento tra K e W).

La seconda immagine mostra la colorazione delle facce esterne del cubo, cioè delle facce sul vertice W.

Tecnicamente ogni coordinata è codificata con 8 bit, quindi ogni coordinata ha valori da 0 a $2^8 - 1 = 255$ (da 0 a FF in esadecimale), e ogni colore si rappresenta tramite una terna con notazione decimale o esadecimale. In totale si codificano quindi $(2^8)^3 = 2^{24} = 16777216$ colori.

Pensando invece ad un foglio di carta bianco, conviene usare un riferimento affine in cui l'origine sia W, e i punti fondamentali siano $C = \left(\begin{smallmatrix}0\\1\\1\end{smallmatrix}\right)$ (cian), $M = \left(\begin{smallmatrix}1\\0\\1\end{smallmatrix}\right)$ (magenta), $Y = \left(\begin{smallmatrix}1\\1\\0\end{smallmatrix}\right)$ (yellow, giallo), e allora ogni colore X viene determinato da tre coordinate c, m, y tali che

$$X = W + r(C - W) + g(M - W) + b(Y - W)$$

da cui si deduce quasi subito che

$$\begin{pmatrix}c\\m\\y\end{pmatrix} = \begin{pmatrix}1-r\\1-g\\1-b\end{pmatrix} \qquad \text{e} \qquad \begin{pmatrix}r\\g\\b\end{pmatrix} = \begin{pmatrix}1-c\\1-m\\1-y\end{pmatrix}$$

(questo si vede facilmente nel cubo).

Nelle stampanti tuttavia è costoso usare pigmenti colorati e quindi si utilizza un pigmento nero (meno costoso) e si realizza ogni colore usando il nero e solo due dei pigmenti *cmy*: infatti per ogni colore $X \neq K$ la retta $K \vee X$ incontra una (almeno) delle facce esterne del cubo diciamo nel punto $X_0 = \frac{1}{h}X$ con $h = \max X = \max\{r, g, b\}$ (una almeno delle coordinate *rgb* di X_0 uguale a 1, quindi una almeno delle coordinate *cmy* uguale a 0), e quindi X si può ottenere come $X = kK + (1-k)X_0 = (1-h)K + hX_0$. Possiamo allora identificare X usando le coordinate *cmy* di X_0 e la componente k di nero, che sono

$$c = \frac{h-r}{h}, \quad m = \frac{h-g}{h}, \quad y = \frac{h-b}{h}, \quad k = 1 - h$$

(come prima $h = \max X = \max\{r, g, b\}$), e una almeno delle prime tre è nulla. Queste sono dette coordinate *cmyk* di X; è standard rappresentare tridimensionalmente queste coordinate usando l'esagono dei colori *cmy* di X_0 e pensando alla piramide con quella base e vertice nel nero (più grande k, più si

scurisce il colore andando verso il vertice della piramide):

Anche il problema di passare da una immagine colorata ad una in toni di grigio ha una sua interpretazione in termini dello spazio affine; la più semplice strategia potrebbe essere di fare la proiezione ortogonale (vedi la geometria euclidea) sulla diagonale dei grigi $K \vee W$, il che porta facilmente alla formula grigio$(X) = \frac{r+g+b}{3}W$ ovvero a fare la media delle rgb. Non si usa mai questa proiezione: per questioni estetiche si preferisce dare alle coordinare rgb dei pesi diversi, tenendo conto che i tre colori fondamentali sono percepiti come non ugualmente scuri, quindi si danno dei pesi p_r, p_g, p_b con $p_r + p_g + p_b = 1$ e $p_g > p_r > p_b$ (il verde è più chiaro del rosso, che è più chiaro del blu).

6. Spazi affini di dimensione quattro.

La stesura di questa sezione, sulla falsariga delle precedenti, è un esercizio per il lettore.

7. Esercizi.

7.0. Consideriamo un primo p in $\mathbb{Z}$ e una sua potenza $q = p^r$ (si può pensare $r = 1$, cioè $q = p$ per semplicità). Sappiamo che esiste un (unico) campo finito $\mathbb{F}_q$ che ha esattamente q elementi ed è un campo di caratteristica p (cioè l'unico morfismo di anelli da $\mathbb{Z}$ ha come nucleo l'ideale generato da p, ovvero $\mathbb{F}_q$ contiene $\mathbb{F}_p$, o meglio una copia isomorfa).

Consideriamo ora lo spazio affine standard $\mathbb{A}^n(\mathbb{F}_q)$ di dimensione n su $\mathbb{F}_q$. Contare gli elementi rilevanti di V, in particolare:
(a) quanti punti ci sono in V?
(b) per ogni intero m fino a n: quanti sottospazi di dimensione m vi sono in V?
(c) quante coppie di sottospazi complementari ci sono in V?
Se possibile fare dei disegni ($n = 2, 3$) che illustrino il conteggio nei casi $p = 2, 3, 5$ con $r = 1, 2$.

Simmetrie? Baricentri? Triangoli? Attenzione alla caratteristica: punti medi in caratteristica 2? Mediane e baricentri di triangoli in caratteristica 3?

7.1. In ciascuno dei seguenti casi determinare un'equazione cartesiana della retta di $\mathbb{A}^2(\mathbb{C})$ contenente i punti:
(a) $(-1, -1)$, $(3, 2i)$, (b) $(-1, i)$, $(-i, -i)$, (c) $(1, 2i)$, $(1, -2i)$.

7.2. Verificare se le seguenti rette di $\mathbb{A}^2(\mathbb{C})$ sono in un fascio: $r : 3i + iX_1 - X_2 = 0$, $s : 5 + X_1 + 3iX_2 = 0$, $t : 1 + X_1 - iX_2 = 0$.

7.3. Verificare se le rette $r : \begin{cases} 1 - X_1 + X_2 = 0 \\ X_1 - 2X_2 + X_3 = 0 \end{cases}$, $s : \begin{cases} 1 + X_2 - 3X_3 = 0 \\ 1 - 2X_1 - 2X_2 = 0 \end{cases}$ di $\mathbb{A}^3(\mathbb{R})$ sono sghembe oppure incidenti.

7.4. Per ogni $t \in \mathbb{R}$ si consideri il sistema lineare $\Sigma_t : \begin{cases} -tx + (t-1)y + z = -1 \\ (t-1)y + tz = 1 \\ 2x + z = 5 \end{cases}$. Sia S_t l'insieme delle soluzioni di Σ_t.

(a) Per quali valori di t S_t è costituito da un solo punto?
(b) Per quali valori di t S_t è vuoto?
(c) Per quali valori di t S_t è una sottovarietà lineare affine di dimensione 1?
(d) Per i valori di t di cui al punto (c), esibire equazioni parametriche di S_t.

7.5. Nello spazio affine tridimensionale, sono date tre famiglie di piani di equazioni

$$a_\lambda : X + \lambda Z = \lambda \qquad b_\lambda : \lambda X + Y + (1+\lambda^2)Z = \lambda^2 \qquad c_\lambda : (1-\lambda)X - Y - Z = 1 - \lambda^2$$

al variare del parametro $\lambda \in \mathbb{R}$.

(a) determinare per quali valori di λ i tre piani si intersecano esattamente in un punto, e per tali valori determinare il punto di intersezione P_λ.
(b) determinare se esistono valori di λ per i quali i tre piani si intersecano in una retta, ed eventualmente dare una espressione parametrica per questa retta.
(c) determinare se esistono valori di λ per i quali i tre piani non hanno punti in comune.
(d) è vero che le soluzioni del sistema formato dai tre piani al variare del parametro $\lambda \in \mathbb{R}$ giacciono tutte su uno stesso piano?

7.6. Discutere (usando il teorema di Rouché-Capelli) tutte le posizioni reciproche possibili delle seguenti costellazioni di sottovarietà affini lineari:
(1) tre piani in $\mathbb{A}^3(\mathbb{R})$; (2) quattro piani in $\mathbb{A}^3(\mathbb{R})$; (3) un piano ed una retta in $\mathbb{A}^3(\mathbb{R})$;
(4) due piani in $\mathbb{A}^4(\mathbb{R})$; (5) tre piani in $\mathbb{A}^4(\mathbb{R})$;
(6) tre iperpiani in $\mathbb{A}^4(\mathbb{R})$; (7) quattro iperpiani in $\mathbb{A}^4(\mathbb{R})$.

7.7. Siano r_1, r_2 ed r_3 tre fissate rette a due a due sghembe nello spazio affine tridimensionale reale. Sia L l'insieme di tutte le rette che si appoggiano a tutte e tre le rette date (cioè che intersecano sia r_1 che r_2 che r_3), e sia C il sottinsieme dello spazio affine dato dall'unione di tutte le rette in L. Descrivere L e C.

In particolare, se r_1, r_2 ed r_3 hanno equazioni rispettivamente $\begin{cases} X = 0 \\ Y = 0 \end{cases}$, $\begin{cases} X = 1 \\ Z = 0 \end{cases}$ e $\begin{cases} Y = 1 \\ Z = 1 \end{cases}$ dare delle equazioni per la generica retta in L, e scrivere una equazione che descriva l'insieme C.

7.8. Si scriva l'equazione del piano di $\mathbb{A}^3(\Bbbk)$ passate per il punto $P = \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$ e parallelo alle rette r, s di equazioni rispettive $X = Y = Z$ e $X + 3Y = 0 = X - Y + Z - 1$.

7.9. Si scriva l'equazione della retta t di $\mathbb{A}^3(\Bbbk)$ passate per il punto $P = \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$ e complanare alle rette r, s di equazioni rispettive $X = Y = Z$ e $X + 3Y = 0 = X - Y + Z - 1$. Si verifichi poi se t è incidente o parallela a r ed s.

7.10. Nel piano affine $\mathbb{A}^2(\Bbbk)$ si considerino due rette r, s distinte, tre punti distinti P_1, P_2, P_3 di r, ed altri tre punti Q_1, Q_2, Q_3 di s distinti tra di loro e dai precedenti. Si indichi con u_{ij} la retta passante per P_i e Q_j, e si mostri che i tre punti $u_{12} \cap u_{21}$, $u_{13} \cap u_{31}$,$u_{23} \cap u_{32}$ sono allineati.

7.11. Si considerino le tre rette r, s, t di $\mathbb{A}^3(\Bbbk)$ di equazioni rispettive

$$X + 3Y = 0 = X - Y + Z - 1, \qquad X = Y = Z, \qquad X = -Y = 1\ ;$$

(i) Si mostri che per ogni punto P di t passa una ed una sola retta u_P complanare con r ed s.
(ii) Si mostri che se $P \neq Q$ sono due punti di t, allora u_P ed u_Q sono sghembe;
(iii) Si trovino le coordinate del punto P di t per cui passa una retta parallela ad r ed incidente s.

7.12. Si considerino le tre rette r, s, t di $\mathbb{A}^3(\Bbbk)$ di equazioni rispettive

$$X = 2Y - 1, Z = 1; \quad X = Y + 1, Z = -1; \quad X = Y = Z - 1.$$

(i) Si trovino un punto P di r ed un punto Q di s tali che il punto medio del segmento PQ appartenga a t.

(ii) Si trovi il luogo dei punti medi dei segmenti con un estremo in r e l'altro in s.

7.13. Nello spazio affine $\mathbb{A}^3(\mathbb{R})$ si considerino i piani $\gamma : 3x - y = 3,\ \pi : x + y - 4z = -1$, e la famiglia di coppie di piani (α_k, β_k) di equazioni $\alpha_k : kx + y + 2z = 1,\ \beta_k : x - 2y - kz = 2$, al variare di k in $\mathbb{R}$.

(a) Dimostrare che i piani α_k, β_k si intersecano in una retta r_k e dare equazioni parametriche di questa retta per ogni valore di k in $\mathbb{R}$.
(b) Studiare la posizione reciproca tra la retta r_k ed il piano γ al variare di k in $\mathbb{R}$.
(c) Esiste k in $\mathbb{R}$ tale che la retta r_k sia parallela alla retta $\gamma \cap \pi$?

7.14. Nello spazio affine $\mathbb{A}^3(\mathbb{R})$ si consideri la famiglia di terne di piani $(\alpha_s, \beta_s, \gamma_s)$ di equazioni

$$-(2s+1)x + 2sy + z = -1, \quad 2x + z = 5, \quad 2sy + (2s+1)z = 1,$$

al variare di s in $\mathbb{R}$.

(a) Per quali valori di s l'intersezione dei piani α_s, β_s, γ_s è costituita da un punto?
(b) Per quali valori di s l'intersezione dei piani α_s, β_s, γ_s è vuota?
(c) Per quali valori di s l'intersezione dei piani α_s, β_s, γ_s è una retta?
(d) Per i valori di s di cui al punto (c), esibire equazioni parametriche della retta $r_s = \alpha_s \cap \beta_s \cap \gamma_s$.

7.15. Si considerino, al variare di λ tra i numeri reali, i piani $\alpha_\lambda, \beta_\lambda, \gamma_\lambda$ di $\mathbb{A}^3(\mathbb{R})$ di equazioni

$$(\lambda+1)x + 2y - (\lambda+1)z = 1 - \lambda, \qquad (-\lambda+1)x - \lambda y + (\lambda+1)z = \lambda, \qquad 2x - z = 0.$$

Senza risolvere il sistema formato dalle tre equazioni si risponda ai seguenti quesiti:

(a) Per quali valori di λ l'insieme $\alpha_\lambda \cap \beta_\lambda \cap \gamma_\lambda$ è un punto?
(b) Per quali valori di λ l'insieme $\alpha_\lambda \cap \beta_\lambda \cap \gamma_\lambda$ è una retta?
(c) Per quali valori di λ l'insieme $\alpha_\lambda \cap \beta_\lambda \cap \gamma_\lambda$ è vuoto?

7.16. Nello spazio affine standard $\mathbb{A}^3(\mathbb{R})$ si considerino le tre rette r, s, t, le cui equazioni sono:

$$r : \begin{cases} x - y + z = 1 \\ 2x + 3y = 0 \end{cases}, \qquad s : \begin{cases} 2x + y - z = 1 \\ x + y + z = 2 \end{cases}, \qquad t : x = y = -z.$$

(i) Si verifichi che le rette r ed s sono sghembe.
(ii) Si scrivano le equazioni cartesiane di tutte le rette incidenti t e complanari con r ed s.
(iii) Si dica se tra le rette di cui in (ii) ve ne sono di parallele ad s.

7.17. Consideriamo i quattro punti $P_0 = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$, $P_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $P_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $P_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, e le quattro rette $r_0 :\ X - Y = 0 = Z - 1$, $r_1 :\ X + Y - Z = 0 = 2Z - 1$, $r_2 :\ X - Y = 0 = Z - 2$, $r_3 :\ X + Y = 0 = Z$. Dire quali rette attraversano il tetraedro formato dai quattro punti, eventualmente specificando le facce o gli spigoli che esse toccano.

7.18. Dati tre punti non allineati di un piano affine reale, le tre rette che essi determinano dividono il piano stesso in sette zone. Descrivere queste zone tramite disequazioni a partire dai punti $P_0 = \binom{1}{2}$, $P_1 = \binom{2}{1}$, $P_3 = \binom{-1}{-1}$.

Analogamente, dati quattro punti non complanari in uno spazio affine reale tridimensionale, i quattro piani che essi determinano dividono lo spazio stesso in 15 zone. Descrivere queste zone tramite disequazioni a partire dai punti $P_0 = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$, $P_0 = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$, $P_0 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$, $P_0 = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$.

Generalizzare le affermazioni precedenti per spazi affini reali n-dimensionali (dati $n+1$ punti non appartenenti allo stesso iperpiano,...).

7.19. Si considerino le due famiglie di piani in $\mathbb{A}^4(\mathbb{R})$ di equazioni cartesiane:

$$\pi_\lambda : \begin{cases} (4+\lambda)X_1 + \lambda X_2 + X_3 - \lambda X_4 = 1 \\ (1+\lambda)X_2 + \lambda X_3 = \lambda \end{cases} \qquad \sigma_\lambda : \begin{cases} (4+\lambda)X_1 + (1-\lambda)X_3 - \lambda X_4 = -\lambda \\ X_2 + \lambda X_4 = 8\lambda \end{cases}$$

al variare di $\lambda \in \mathbb{R}$.

(*a*) Dire per quali valori di λ i due piani si incontrano in un punto e determinare il punto in funzione di λ.
(*b*) Per quali valori di λ i due piani hanno intersezione vuota? In tali casi sono paralleli?
(*c*) Per quali valori di λ i due piani si intersecano in una retta?
(*d*) Dire per quali valori di λ i due piani sono contenuti in una varietà lineare affine di dimensione 3, e determinare equazioni cartesiane per tali spazi.

7.20. Sono dati i piani dello spazio affine $\mathbb{A}^4(\mathbb{R})$:

$$\pi_1 : \begin{cases} -3X_1 - X_2 + 4X_4 = 3 \\ -X_3 + X_4 = 4 \end{cases} \qquad \pi_2 : \begin{cases} 4X_1 - 4X_3 + X_4 = 20 \\ 5X_1 - 4X_3 = 20 \end{cases} .$$

(a) Determinare $\pi_1 \wedge \pi_2$ e $\pi_1 \vee \pi_2$. Esistono sottospazi di dimensione 3 contenenti entrambi i piani?
(b) Si mostri che per ogni punto P non appartenente a $\pi_1 \cup \pi_2$ passa un unico piano σ_P "conspaziale con π_1 e π_2" (cioè tale che le congiungenti $\pi_1 \vee \sigma_P$ e $\pi_2 \vee \sigma_P$ abbiano dimensione 3).
(c) Sia r la retta per l'origine e direzione e_1; descrivere tramite equazione cartesiane l'insieme $\bigcup_{P \in r} \sigma_P$. Si tratta di un sottospazio affine?
($d*$) Generalizzare l'esercizio ad $\mathbb{A}^n(\mathbb{R})$: dati due sottospazi affini $\mathbb{L}_1$ ed $\mathbb{L}_2$ di dimensione $n-2$ tali che ..., per ogni punto P non appartenente alla loro unione, esiste unico ...

7.21. Sono dati la retta ed il piano dello spazio affine $\mathbb{A}^4(\mathbb{R})$:

$$r : \begin{pmatrix} 1 \\ 2 \\ 2 \\ -1 \end{pmatrix} + \langle \begin{pmatrix} 1 \\ 2 \\ 0 \\ 2 \end{pmatrix} \rangle \qquad \pi : \begin{cases} 4X_1 - 2X_2 + X_3 = 1 \\ X_1 + X_2 - X_4 = 1 \end{cases} .$$

(a) Determinare la posizione reciproca di r e π. Esistono sottospazi di dimensione 3 contenenti entrambi?
(b) Si mostri che esiste un unico iperpiano Σ_r contenente r e parallelo a π, ed un unico iperpiano Σ_π contenente π e parallelo ad r, e se ne determinino le equazioni. È vero o falso che i due iperpiani sono paralleli tra loro?
(c) Per ogni iperpiano Γ contenente r e diverso da Σ_r, determinarne la posizione reciproca con π.
($d*$) Generalizzare l'esercizio ad $\mathbb{A}^n(\mathbb{R})$: dati due sottospazi affini complementari $\mathbb{L}$ ed $\mathbb{M}$, esiste un unico iperpiano $\Sigma_\mathbb{L}$ ... , e per ogni altro iperpiano Γ contenente $\mathbb{L}$ e diverso da $\Sigma_\mathbb{L}$ si ha che $\Gamma \wedge \mathbb{M}$ ...

7.22. Sono dati i piani dello spazio affine $\mathbb{A}^4(\mathbb{R})$:

$$\pi_1 : \begin{cases} X_1 - X_3 + X_4 = 1 \\ X_2 - X_4 = 1 \end{cases} \qquad \pi_2 : \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \\ 1 \end{pmatrix} \rangle .$$

(a) Determinare $\pi_1 \wedge \pi_2$ e $\pi_1 \vee \pi_2$. Esistono sottospazi di dimensione 3 contenenti entrambi i piani?
(b) Esistono rette di $\mathbb{A}^4(\mathbb{R})$ che siano parallele ad entrambi i piani? Eventualmente trovarle tutte.
(c) Esistono iperpiani di $\mathbb{A}^4(\mathbb{R})$ che siano paralleli ad entrambi i piani? Eventualmente trovarli tutti.
(d) È vero o falso che la relazione di parallelismo tra sottovarietà affini di uno spazio affine è transitiva? E tra sottospazi della stessa dimensione? Esistono piani di $\mathbb{A}^4(\mathbb{R})$ che siano paralleli ad entrambi i piani dati?

7.23. Nello spazio affine $\mathbb{A}^4(\Bbbk)$ si considerino la retta r passante per i punti $\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 2 \\ 3 \end{pmatrix}$ e il piano π di equazioni $\begin{cases} X_2 - X_3 = 0 \\ X_1 - X_2 + X_4 = 3 \end{cases}$.

(a) Determinare la posizione reciproca di r e π: sono paralleli, incidenti, sghembi, complementari?
(b) Mostrare che per ogni punto P non appartenente a $r \cup \pi$ esiste una unica retta s_P per P, complanare con r e conspaziale con π; determinare tale retta per ciascun punto della retta parallela ad r e passante per l'origine.
(c) Determinare per quali punti P dello spazio affine la retta s_P è parallela a r o a π o ad entrambi.
($d*$) Generalizzare l'enunciato dell'esercizio in dimensione n: *data una retta e un sottospazio complementare in $\mathbb{A}^n(\Bbbk)$, per ogni punto P non appartenente all'unione dei due esiste una unica retta ..., ed essa è parallela a ... se e solo se...* .

7.24. Dare caratterizzazioni geometrica ed algebrica ed espressione esplicita delle simmetrie di $\mathbb{A}^3_\mathbb{R}$:
(1) di asse un punto P e direzione $\mathbb{R}^3$;
(2) di asse una retta $r = P + \langle u \rangle$ e direzione $\langle v, w \rangle$;
(3) di asse un piano $\pi = P + \langle u, v \rangle$ e direzione $\langle w \rangle$;
(4) di asse tutto $\mathbb{A}^3_\mathbb{R}$ e direzione 0.

[Esempio per (2): geometricamente è una applicazione F tale che per ogni punto Q si ha $F(Q) - Q \in \langle v, w \rangle$ e $\frac{1}{2}F(Q) + \frac{1}{2}Q \in r$ (cioè con punto medio tra Q e $F(Q)$ in r); nel riferimento affine

dato da P, u, v, w è l'applicazione $F(x, y, z) = (x, -y, -z)$; algebricamente si tratta di affinità aventi (almeno) un punto unito e applicazione lineare associata diagonalizzabile di polinomio caratteristico $(x-1)(x+1)^2$.]

Generalizzare le descrizioni al caso di simmetrie di $\mathbb{A}^n_{\mathbb{R}}$. Esplicitare il caso $n = 2$.

7.25. Determinare i simmetrici di $s : \begin{cases} z = 5 \\ 4x + y = 8 \end{cases}$ e $\pi :\ z = 5$ rispetto alla retta r di equazioni parametriche $\begin{cases} x = 1 + 2t \\ y = 2 - t \\ z = 3 + t \end{cases}$ secondo la direzione $\langle v, w \rangle$ con $v = \left(\begin{smallmatrix} 1 \\ 0 \\ 0 \end{smallmatrix}\right)$ e $w = \left(\begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix}\right)$. Scrivere esplicitamente l'espressione della simmetria in questione nel riferimento dato.

7.26. Dare caratterizzazioni geometrica ed algebrica ed espressione esplicita delle proiezioni di $\mathbb{A}^3_{\mathbb{R}}$:
(1) su un punto P e direzione $\mathbb{R}^3$;
(2) su una retta $r = P + \langle u \rangle$ e direzione $\langle v, w \rangle$;
(3) su un piano $\pi = P + \langle u, v \rangle$ e direzione $\langle w \rangle$;
(4) su tutto $\mathbb{A}^3_{\mathbb{R}}$ e direzione 0.

[Esempio per (3): geometricamente è una applicazione F tale che per ogni punto Q si ha $F(Q) - Q \in \langle w \rangle$ e $F(Q) \in \pi$; nel riferimento affine dato da P, u, v, w è l'applicazione $F(x, y, z) = (x, y, 0)$; algebricamente si tratta di trasformazioni affini aventi (almeno) un punto unito e applicazione lineare associata diagonalizzabile di polinomio caratteristico $x(x-1)^2$.]

Generalizzare le descrizioni al caso di proiezioni di $\mathbb{A}^n_{\mathbb{R}}$. Esplicitare il caso $n = 2$.

7.27. Scrivere le proiezioni di $r : \begin{cases} y - 1 = 0 \\ x - z = 0 \end{cases}$, $s : \begin{cases} x = 1 + t \\ y = 2 - t \\ z = 3 + 2t \end{cases}$ e $\sigma : x - z = 6$ sul piano π di equazione $x + y = 5$ secondo la direzione $\langle w \rangle$ con $w = \left(\begin{smallmatrix} 1 \\ 0 \\ 1 \end{smallmatrix}\right)$. Spiegare i risultati con un disegno. Scrivere l'espressione della proiezione nel riferimento dato.

7.28. Nello spazio affine $\mathbb{A}^3(\mathbb{R})$ si consideri l'affinità F di matrice

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -2 & -1 & 2 \\ 1 & 0 & 2 & -1 \\ 3 & -3 & 0 & 2 \end{pmatrix}$$

rispetto al sistema di riferimento canonico.
(a) Determinare le equazioni cartesiane di tutti i piani uniti sotto F. I piani uniti sono in un fascio?
(b) Si scrivano le equazioni di tutte le rette r di $\mathbb{A}^3(\mathbb{R})$ tali che $F(r)$ sia parallela ad r.

Capitolo VII

Spazi Vettoriali Euclidei ed Hermitiani

In questo capitolo introdurremo una nuova struttura nello spazio vettoriale standard su $\mathbb{R}$ di dimensione n; si tratta della operazione di "prodotto scalare" tra vettori (il risultato è un numero reale) che vedremo essere la base comune per due nozioni ben note: quella di norma (o lunghezza) di vettori e quella di (misura del coseno dell')angolo tra due vettori (la "trigonometria" lega queste due nozioni). In particolare avremo una nozione di ortogonalità tra vettori, ed una riscrittura di risultati classici (Pitagora, Euclide, Carnot). Studieremo le trasformazioni che rispettano l'operazione di prodotto scalare, dette isometrie o trasformazioni ortogonali. E vedremo le nozioni di base per il calcolo di volumi (di parallelepipedi e tetraedri r-dimensionali), e il loro legame con il calcolo di determinanti. Per questo sarà anche introdotto il cross-product di vettori,

Estenderemo infine questi argomenti al caso di spazi vettoriali ed affini sul corpo complesso, dando le definizioni fondamentali di Spazi Vettoriali Hermitiani.

Le definizioni verranno date solo per spazi vettoriali standard ed useranno in modo esplicito la base canonica; quindi non sono propriamente "intrinseche": dare le stesse definizioni usando una base qualsiasi porta a risultati non confrontabili. Per una teoria intrinseca dei "prodotti scalari" bisognerà studiare più in generale le forme bilineari e quadratiche, cosa che si farà in futuro, e sarà molto facilitata dall'avere una conoscenza, seppure non intrinseca, degli spazi euclidei.

1. Spazi Vettoriali Euclidei Reali: dot-product, norma e angoli.

1.1. Definizione-Teorema (Dot-Product, o Prodotto Scalare). *Sia $V_n(\mathbb{R})$ lo spazio vettoriale standard su $\mathbb{R}$ di dimensione n. Definiamo il prodotto scalare di due vettori $v = (x_i)^{\mathrm{t}}$ e $w = (y_i)^{\mathrm{t}}$ come $v \cdot w := v^{\mathrm{t}} w = \sum_i x_i y_i$, ove si sono usate le coordinate nella base canonica.*

Il prodotto scalare dà una funzione $V_n(\mathbb{R}) \times V_n(\mathbb{R}) \longrightarrow \mathbb{R}$ che gode delle seguenti proprietà:

$(PS1)$ *simmetria: $v \cdot w = w \cdot v$ (per ogni $v, w \in V_n(\mathbb{R})$);*

$(PS2)$ *bilinearità: $v \cdot (\alpha_1 w_1 + \alpha_2 w_2) = \alpha_1 (v \cdot w_1) + \alpha_2 (v \cdot w_2)$ e $(\alpha_1 v_1 + \alpha_2 v_2) \cdot w = \alpha_1 (v_1 \cdot w) + \alpha_2 (v_2 \cdot w)$ (per ogni $v, v_1, v_2, w, w_1, w_2 \in V_n(\mathbb{R})$, ed ogni $\alpha_1, \alpha_2 \in \mathbb{R}$);*

$(PS3)$ *positività: $v \cdot v \geqslant 0$ (per ogni $v \in V_n(\mathbb{R})$); $v \cdot v = 0$ se e solo se $v = 0$.*

Lo spazio vettoriale $V_n(\mathbb{R})$ dotato del prodotto scalare si dice lo spazio euclideo (reale) standard di dimensione n.

Dimostrazione. Facili conti. □

1.1.1. Notazioni. In letteratura il dot-product viene indicato con simboli diversi a seconda dei testi: si può trovare $v \cdot w$ oppure $v \circ w$ oppure $\langle v, w \rangle$ e altri ancora come $\langle v | w \rangle$. Nella versione $\langle v | w \rangle$ (soprattutto in Fisica) l'operazione viene spesso chiamata "bra-ket" e vengono distinte le due operazioni $\langle v |$ (detta Bra) e $| w \rangle$ (detta Ket).

1.1.2. Non degenerazione. Si osservi anche che questo prodotto non gode assolutamente di proprietà di annullamento: può essere $v \cdot w = 0$ con $v \neq 0 \neq w$ (esempi?). Tuttavia valgono le seguenti regole di non degenerazione (una segue dall'altra per simmetria): se $v \cdot w = 0$ per ogni vettore $w \in V_n(\mathbb{R})$, allora $v = 0$, e se $v \cdot w = 0$ per ogni vettore $v \in V_n(\mathbb{R})$, allora $w = 0$. Questo segue dalla proprietà di positività in modo banale: siccome per ipotesi si ha $v \cdot v = 0$, si deduce subito che $v = 0$. Da notare comunque che le proprietà di degenerazione non implica la positività, che è proprietà ben più forte. La non degenerazione si può ottenere direttamente dalla definizione di prodotto scalare applicando l'ipotesi ai vettori della base canonica.

1.2. Definizione (norma). *La norma di un vettore $v \in V_n(\mathbb{R})$ è definita come*

$$\|v\| := \sqrt{v \cdot v}$$

(si usa la positività). Un vettore di norma 1 *si dice un versore.*

1.3. Teorema (disuguaglianza di Cauchy-Schwarz). *Per ogni $v, w \in V_n(\mathbb{R})$ vale che*

$$(v \cdot w)^2 \leqslant (v \cdot v)(w \cdot w)$$

e dunque

$$|v \cdot w| \leqslant \|v\| \, \|w\| \, .$$

Inoltre vale l'uguaglianza se e solo se v e w sono linearmente dipendenti.

Dimostrazione. Supponiamo v e w non nulli (altrimenti è ovvio) e usiamo la disuguaglianza $(v + \lambda w) \cdot (v + \lambda w) \geqslant 0$ per ogni $\lambda \in \mathbb{R}$. Svolgendo il prodotto per bilinearità otteniamo

$$v \cdot v + 2\lambda v \cdot w + \lambda^2 w \cdot w \geqslant 0$$

per ogni $\lambda \in \mathbb{R}$; da questo segue che il discriminante dell'equazione di secondo grado in λ dev'essere negativo o nullo: $(v \cdot w)^2 - (v \cdot v)(w \cdot w) \leqslant 0$, da cui la disuguaglianza. Se poi vale l'uguaglianza allora per $\lambda = -\frac{v \cdot w}{w \cdot w}$ abbiamo $v + \lambda w = 0$; viceversa se v e w sono linearmente dipendenti possiamo supporre $v = \alpha w$ e i due lati della disequazione sono entrambi uguali ad $\alpha^2 (v \cdot v)$.

Una dimostrazione alternativa si può ottenere sostituendo direttamente $\lambda = w \cdot w$ e $\mu = -v \cdot w$ nella disuguaglianza $(\lambda v + \mu w) \cdot (\lambda v + \mu w) \geqslant 0$.

Una ulteriore e più chiara dimostrazione si può ottenere calcolando la norma della proiezione di v ortogonale a w (vedi la formula per la proiezione ortogonale). □

1.3.1. Si osservi che per $x_1, \ldots, x_n$ e $y_1, \ldots, y_n$ n-uple in $\mathbb{R}$ abbiamo

$$\Big(\sum_i x_i y_i\Big)^2 \leqslant \Big(\sum_i x_i^2\Big)\Big(\sum_i y_i^2\Big) \, .$$

Per quali termini differiscono i due membri della disuguaglianza? Si può dimostrare questa disuguaglianza in modo più elementare? Confrontare in seguito con il teorema di Lagrange e sue generalizzazioni.

1.4. Teorema (proprietà della norma).

$(N1)$ $\|v\| = 0$ *se e solo se* $v = 0$*;*

$(N2)$ $\|\alpha v\| = |\alpha| \, \|v\|$*;*

$(N3)$ $\|v + w\| \leqslant \|v\| + \|w\|$ *(disuguaglianza triangolare);*

$(N4)$ $\|v \pm w\|^2 = \|v\|^2 \pm 2(v \cdot w) + \|w\|^2$ *(teorema di Carnot);*

$(N5)$ $\|v + w\|^2 + \|v - w\|^2 = 2\left(\|v\|^2 + \|w\|^2\right)$.

Dimostrazione. I primi due e gli ultimi due punti sono facili a partire dalle definizioni; per esempio l'ultimo si ottiene così:

$$\begin{aligned}\|v + w\|^2 + \|v - w\|^2 &= (v + w) \cdot (v + w) + (v - w) \cdot (v - w) \\ &= (v \cdot v + 2v \cdot w + w \cdot w) + (v \cdot v - 2v \cdot w + w \cdot w) = 2v \cdot v + 2w \cdot w \, .\end{aligned}$$

La disuguaglianza triangolare segue da quella di Cauchy-Schwarz: considerando infatti i quadrati si ha

$$\|v + w\|^2 = (v + w) \cdot (v + w) = v \cdot v + 2v \cdot w + w \cdot w \leqslant \|v\|^2 + 2\|v\| \, \|w\| + \|w\|^2 = (\|v\| + \|w\|)^2 \, .$$

□

1.5. Definizione (misura di angoli). *Nozione di misura (del coseno) dell'angolo $\vartheta(v, w)$ tra due vettori non nulli $v, w \in V_n(\mathbb{R})$:*

$$\cos \vartheta(v, w) := \frac{v \cdot w}{\|v\| \, \|w\|}$$

(ha senso per la disuguaglianza di Cauchy-Schwarz).

1.5.1. Usando la funzione arcocoseno ($\arccos : [-1, 1] \to [0, \pi]$ dell'Analisi, definita come inversa per composizione della funzione ristretta $\cos : [0, \pi] \to [-1, 1]$, strettamente descrescenti) possiamo anche definire la misura dell'angolo propriamente detta. In effetti tale funzione è definita da

$$\arccos(x) = \int_x^1 \frac{1}{\sqrt{1 - t^2}} dt \qquad \text{e} \qquad \arccos(-1) = \pi$$

(in cui si riconoscerà un integrale che dà una "lunghezza d'arco" della circonferenza unitaria), in maniera del tutto indipendente dalla geometria. Tuttavia, è da notare che il calcolo del coseno si fa con operazioni algebriche (comprese radici quadrate) a partire dai vettori coinvolti.

1.5.2. Definizione di seno e teoremi dei coseni e dei seni. La definizione precedente è giustificata dalla geometria elementare: il teorema di Carnot prima enunciato diventa il teorema dei coseni usuale, poiché

$$\|v \pm w\|^2 = \|v\|^2 \pm 2(v \cdot w) + \|w\|^2 = \|v\|^2 \pm 2\,\|v\|\,\|w\| \cos\vartheta(v,w) + \|w\|^2 \ .$$

Inoltre, definendo il seno dell'angolo (a meno del segno) tramite l'usuale relazione

$$\cos^2\vartheta(v,w) + \sin^2\vartheta(v,w) = 1$$

possiamo ritrovare con facili conti il teorema dei seni:

$$\frac{\|v\|}{\sin\vartheta(u,w)} = \frac{\|w\|}{\sin\vartheta(u,v)} = \frac{\|u\|}{\sin\vartheta(v,w)} = \frac{\|u\|\,\|v\|\,\|w\|}{\sqrt{\|v\|^2\,\|w\|^2 - (v\cdot w)^2}}$$

per $u = v - w$ (ovvero i tre vettori formano i "lati" di un triangolo). Infatti il denominatore dell'ultima espressione rimane lo stesso usando i vettori u, v o u, w invece di v, w. Vedremo che tale denominatore si interpreta come il doppio dell'area del triangolo (vedi generalizzazione del teorema di Lagrange).

1.5.3. Proprietà degli angoli:
(0) $\vartheta(v,w) \in \{0,\pi\}$ se e solo se v e w sono linearmente dipendenti;
(1) $\vartheta(v,w) = \vartheta(w,v)$ per ogni v, w (simmetria);
(2) $\vartheta(\alpha v, w) = \vartheta(v, \alpha w) = \vartheta(v,w)$ se $\alpha > 0$ ($\alpha \in \mathbb{R}$);
(3) $\vartheta(-v,w) = \vartheta(v,-w) = \pi - \vartheta(v,w)$;
(4) $\vartheta(v,w) \leqslant \vartheta(v,z) + \vartheta(z,w)$ per ogni z, v, w.
Le prime proprietà sono evidenti. Per l'ultima si può supporre che v e w siano indipendenti (altrimenti è ovvio), e si tratta prima il caso in cui $z \in \langle v,w\rangle$; in questo caso si tratta di un problema sul piano euclideo che si può vedere in vari modi (per esempio considerando le rotazioni del piano). Se poi $z \notin \langle v,w\rangle$, possiamo decomporre (vedi sotto) $z = z' + z''$ con $z' \in \langle v,w\rangle$ e $z'' \in \langle v,w\rangle^\perp$, e osservare che $\vartheta(v,z') \leqslant \vartheta(v,z)$, da cui segue la diguaglianza in generale, a partire da quella sul piano.

1.6. Definizione (ortogonalità). *Due vettori $v, w \in V_n(\mathbb{R})$ si dicono ortogonali e si scrive $v \perp w$ se vale $v \cdot w = 0$ (il loro prodotto scalare è zero).*

1.6.1. Si noti che 0 è l'unico vettore ortogonale a tutti i vettori dello spazio. Per non degenerazione: se $v \cdot w = 0$ per ogni $w \in V_n(\mathbb{R})$, allora $v = 0$ (basta che la condizione valga per i vettori w appartenenti ad una base qualsiasi di $V_n(\mathbb{R})$? e meno?).

1.6.2. Due vettori ortogonali e non nulli sono linearmente indipendenti; più in generale un insieme di vettori non nulli a due a due ortogonali è linearmente indipendente; infatti da $\sum_i \alpha_i v_i = 0$, usando il prodotto scalare con v_j si deduce $\alpha_j v_j \cdot v_j = 0$, da cui $\alpha_j = 0$, per ogni j.

1.7. Teorema (Pitagora). *Abbiamo che $v \perp w$ se e solo se $\|v+w\|^2 = \|v\|^2 + \|w\|^2$. In generale vale il teorema del coseno: $\|v \pm w\|^2 = \|v\|^2 + \|w\|^2 \pm 2\,\|v\|\,\|w\| \cos\vartheta(v,w)$.*

Dimostrazione. Segue immediatamente dalle definizioni poste e dalle proprietà già viste della norma. Si osservi che la definizione di misura del coseno dell'angolo che abbiamo dato è "giustificata" da questi risultati, nel senso che risulta compatibile con le nozioni della geometria elementare. □

1.7.1. Teorema dei seni. Ricavare da queste definizioni il teorema dei seni elementare: in ogni triangolo i rapporti tra lunghezza di un lato e seno dell'angolo opposto sono costanti (ma è più facile usando le nozioni di area).

1.8. Definizione (proiezione ortogonale). *Proiezione ortogonale di un vettore v nella direzione di w:*

$$p_w(v) = \frac{v\cdot w}{\|w\|^2} w = \frac{v \cdot w}{w \cdot w} w \ .$$

Risulta che $p_w(v) \perp (v - p_w(v))$.

Possiamo pensare p_w come una applicazione (lineare) $V_n(\mathbb{R}) \to V_n(\mathbb{R})$ (con immagine $\langle w\rangle$ e nucleo $\langle w\rangle^\perp$): come scriverne la matrice in base canonica?

1.8.1. Interpretazione elementare. La definizione precedente si giustifica in questo modo: la proiezione ortogonale di v nella direzione di w dev'essere un vettore di direzione quella di w (dunque di versore $w/\|w\|$) e di lunghezza la proiezione della lunghezza di v lungo w, dunque $\|v\|\cos\vartheta(v,w)$; in conclusione:

$$\|v\|\cos\vartheta(v,w)\frac{w}{\|w\|} = \|v\|\,\frac{v\cdot w}{\|v\|\,\|w\|}\,\frac{w}{\|w\|} = \frac{v\cdot w}{\|w\|^2}w$$

come si vede dal disegno:

1.8.2. Si ha che $v+w = p_{v+w}(v)+p_{v+w}(w)$, i.e. $v-p_{v+w}(v) = -(w-p_{v+w}(w))$ (farsi un buon disegno può aiutare ad identificare un'altezza del triangolo di lati v, w e $v+w$).

1.9. Teorema (Euclide). *Siano $v,w\in V_n(\mathbb{R})$; allora:*

(1) *$v\perp w$ se e solo se $\|v\|^2 = \|v+w\|\,\|p_{v+w}(v)\|$ (riconoscere il quadrato di un cateto e il rettangolo costruito sull'ipotenusa con la proiezione del cateto);*

(2) *$v\perp w$ se e solo se $\|v-p_{v+w}(v)\|^2 = \|p_{v+w}(v)\|\,\|p_{v+w}(w)\|$ (riconoscere il quadrato dell'altezza relativa all'ipotenusa e il rettangolo costruito dalle proiezioni dei cateti).*

Dimostrazione. Si osservi che $\|p_{v+w}(v)\| = |v\cdot(v+w)|/\|v+w\|$, da cui (1) segue quasi immediatamente confrontando $\|v\|$ con $v\cdot(v+w)$.

Per (2) si osservi che $\|v-p_{v+w}(v)\|^2 = \|v\|^2 - \|p_{v+w}(v)\|^2 = (\|v\|^2\,\|w\|^2 - (v\cdot w)^2)/\|v+w\|^2$, da cui si conclude confrontando $\|v\|^2\,\|w\|^2-(v\cdot w)^2$ con $|v\cdot(v+w)||w\cdot(v+w)|$. □

1.10. Basi ortogonali e ortonormali. Una base di $V_n(\mathbb{R})$ si dice ortogonale se essa è formata di vettori a due a due ortogonali; si dice ortonormale se inoltre i sui vettori hanno tutti norma 1. Se $(v_1,\dots,v_n)$ è una base ortonormale di $V_n(\mathbb{R})$, allora le coordinate di un vettore $v\in V_n(\mathbb{R})$ in quella base sono date da $\begin{pmatrix} v\cdot v_1\\ \vdots\\ v\cdot v_n\end{pmatrix}$. Infatti da $v=\sum_i\alpha_i v_i$, usando il prodotto scalare con v_j si deduce $v\cdot v_j = \alpha_j v_j\cdot v_j = \alpha_j$. In altri termini, per ogni vettore v risulta

$$v = \sum_{i=1}^n (v\cdot v_i)v_i = (v\cdot v_1)v_1 + (v\cdot v_2)v_2 + \cdots + (v\cdot v_n)v_n\ .$$

1.10.1. Calcolando allora il prodotto scalare tra $v=\sum_{i=1}^n(v\cdot v_i)v_i$ e $w=\sum_{i=1}^n(w\cdot v_i)v_i$ per bilinearità otteniamo la cosiddetta formula di Parseval (reale): se $v_1,\dots,v_n$ è base ortonormale di $V_n(\mathbb{R})$ e $v,w\in V_n(\mathbb{R})$ allora $v\cdot w=\sum_{i=1}^n(v\cdot v_i)(w\cdot v_i)$. Dunque: il prodotto scalare tra v e w si può calcolare facendo la somma dei prodotti delle coordinate omonime *in una qualsiasi base ortonormale di $V_n(\mathbb{R})$*.

1.10.2. Ricerca di basi ortogonali e ortonormali. Si possono costruire molte basi ortogonali (e quindi anche ortonormali di $V_n(\mathbb{R})$ in modo molto libero, sfruttando l'indipendenza di vettori a due a due ortogonali: si parte da un vettore qualsiasi non nullo, poi si sceglie un secondo vettore ortogonale al primo (basta che soddisfi alla condizione di ortogonalità, ovvero appartenere ad un iperpiano), poi un terzo vettore ortogonale ad entrambi i precedenti, e si continua così fino ad avere n vettori.

1.10.3. Ricerca di basi ortogonali e ortonormali: procedimento di Gram-Schmidt. Data una base qualsiasi $v_1,\dots,v_n$ di $V_n(\mathbb{R})$ è sempre possibile ricavarne una base ortogonale $u_1,\dots,u_n$ tale che $\langle v_1,\dots,v_i\rangle = \langle u_1,\dots,u_i\rangle$ (per ogni $i=1,\dots,n$, cioè rispetta la bandiera dei sottospazi della base data) nel modo seguente: ad ogni passo si aggiunge il vettore u_i ottenuto togliendo a v_i tutte le

sue proiezioni ortogonali sui precedenti vettori $u_1, \dots, u_{i-1}$. Dunque si ha:

$$\begin{aligned}
u_1 &= v_1 \\
u_2 &= v_2 - \frac{u_1 \cdot v_2}{u_1 \cdot u_1} u_1 \\
u_3 &= v_3 - \frac{u_1 \cdot v_3}{u_1 \cdot u_1} u_1 - \frac{u_2 \cdot v_3}{u_2 \cdot u_2} u_2 \\
&\dots \\
u_n &= v_n - \sum_{i=1}^{n-1} \frac{u_i \cdot v_n}{u_i \cdot u_i} u_i \ .
\end{aligned}$$

Per ottenere una base ortonormale, basta poi dividere ogni vettore u_i per la sua norma.

Si osservi che il procedimento funziona (cioè fornisce una base ortogonale) anche a partire da un qualsiasi insieme di generatori di $V_n(\mathbb{R})$, eliminando naturalmente i vettori nulli generati dal procedimento stesso.

1.10.4. Il procedimento di Gram-Schmidt si può tradurre anche in formule chiuse (non induttive) in termini di determinanti:

$$u_\ell = \frac{1}{\det\Big((v_i \cdot v_j)_{i,j<\ell}\Big)} \det \begin{pmatrix} v_1 \cdot v_1 & v_1 \cdot v_2 & \cdots & v_1 \cdot v_\ell \\ v_2 \cdot v_1 & v_2 \cdot v_2 & \cdots & v_2 \cdot v_\ell \\ \vdots & \vdots & \ddots & \vdots \\ v_{\ell-1} \cdot v_1 & v_{\ell-1} \cdot v_2 & \cdots & v_{\ell-1} \cdot v_\ell \\ v_1 & v_2 & \cdots & v_\ell \end{pmatrix}$$

come si osserva subito dal fatto che ognuno di questi vettori è ortogonale ai precedenti nella base data (calcolare la forma) e che il coefficiente di v_i è 1 nella i-esima formula. Queste formule hanno interesse teorico ma non computazionale: il procedimento induttivo è più veloce.

1.11. Definizione-Teorema (ortogonali di sottospazi). *Per S sottinsieme di $V_n(\mathbb{R})$ definiamo l'ortogonale $S^\perp = \{v \in V_n(\mathbb{R}) | v \perp s \ (\forall s \in S)\}$, che risulta un sottospazio vettoriale. Si ha:*
($O0$) $\{0\}^\perp = V_n(\mathbb{R})$, $V_n(\mathbb{R})^\perp = 0$, $\dim_{\Bbbk} W^\perp = n - \dim_{\Bbbk} W$.
($O1$) *Se $S \subseteq T$ allora $T^\perp \subseteq S^\perp$.*
($O2$) $\langle S \rangle = (S^\perp)^\perp$; *dunque per W sottospazio:* $(W^\perp)^\perp = W$. *Inoltre* $((S^\perp)^\perp)^\perp = S^\perp$.
($O3$) *Se W e W' sono sottospazi vettoriali di $V_n(\mathbb{R})$:* $(W + W')^\perp = W^\perp \cap W'^\perp$.
($O4$) *Se W e W' sono sottospazi vettoriali di $V_n(\mathbb{R})$:* $(W \cap W')^\perp = W^\perp + W'^\perp$.

Dimostrazione. I primi tre punti sono facili. L'ultimo segue dal penultimo applicato agli spazi ortogonali e poi prendendo l'ortogonale. Il penultimo si dimostra così: affinché un vettore sia ortogonale a tutti i vettori di $W + W'$ è necessario che sia ortogonale sia ai vettori di W che a quelli di W'; dalla bilinearità del prodotto scalare segue che queste due condizioni sono anche sufficienti. □

1.11.1. Relazioni con gli ortogonali sul duale. La definizione di prodotto scalare permette di identificare lo spazio duale di $V_n(\mathbb{R})$ con lo spazio $V_n(\mathbb{R})$ stesso nel modo seguente: ad ogni applicazione lineare $\alpha : V_n(\mathbb{R}) \to \mathbb{R}$ resta associato il vettore dato dalla trasposta della sua matrice nella base canonica, sia v_α. Allora abbiamo $\alpha(v) = v_\alpha \cdot v$ per ogni $v \in V_n(\mathbb{R})$. Da questo isomorfismo $V_n(\mathbb{R})^* \cong V_n(\mathbb{R})$ abbiamo che la nozione di ortogonale qui definita corrisponde a quella definita per gli spazi duali.

Otteniamo in particolare *l'interpretazione euclidea delle equazioni cartesiane: i coefficienti della equazione di un iperpiano formano un vettore ortogonale all'iperpiano stesso; quindi l'ortogonale di un sottospazio è formato dai coefficienti delle equazioni degli iperpiani che lo contengono: una base dello spazio ortogonale dà un sistema minimale di equazioni cartesiane.*

1.11.2. Teorema (Decomposizioni ortogonali). *Per ogni sottospazio W di $V_n(\mathbb{R})$ si ha che $W \oplus W^\perp = V_n(\mathbb{R})$, cioè W e $W^\perp$ sono sottospazi complementari (talvolta si scrive $W \boxplus W^\perp$ per indicare la mutua ortogonalità).*

Dimostrazione. Per il teorema precedente, basta dimostrare che l'intersezione tra W e $W^\perp$ è nulla, e questo discende dal fatto che vettori ortogonali tra loro sono linearmente indipendenti. □

1.11.3. Simmetrie e proiezioni ortogonali. Dato un sottospazio W, diciamo simmetria (risp. proiezione) ortogonale di asse W la simmetria (risp. proiezione) di asse W e di direzione $W^\perp$. Similmente per simmetrie (risp. proiezioni) ortogonali di direzione W (significa che l'asse è $W^\perp$).

Usando come colonne i vettori di una base di W otteniamo una matrice $A \in M_{n,m}(\mathbb{R})$ di rango $m = \dim_{\mathbb{R}} W$, e il sistema di equazioni per $W^\perp$ ha matrice A^{t}. Quindi la proiezione ortogonale su W ha matrice (nella base canonica) data da $A(A^{\mathrm{t}}A)^{-1}A^{\mathrm{t}}$. Infatti questa matrice annulla i vettori di $W^\perp$ e agisce come l'indentità sui vettori di W (una cui base è data dalle colonne della matrice A).

1.11.4. In generale diremo che due sottospazi sono ortogonali, scritto $V \perp W$ se $v \cdot w = 0$ per ogni $v \in V$ e $w \in W$. È equivalente alla condizione $V \leqslant W^\perp$, o anche alla condizione $W \leqslant V^\perp$.

1.12. Soluzioni ai minimi quadrati per sistemi incompatibili. Dato un sistema lineare $AX = b$ privo di soluzioni, ci si può chiedere quali siano i vettori x tali che la norma di $Ax - b$ sia minima possibile (quelli dunque che meglio approssimano una soluzione nel senso della distanza euclidea). Ora questa condizione è realizzata se e solo se $Ax - b$ è ortogonale allo spazio generato dalle colonne di A, dunque se e solo se $A^{\mathrm{t}}(Ax - b) = 0$, e dunque se e solo se x risolve il sistema lineare $A^{\mathrm{t}}AX = A^{\mathrm{t}}b$ (la matrice $A^{\mathrm{t}}A$ è simmetrica, e il suo rango è uguale al rango di A: perché?).

Equivalentemente, se decomponiamo $b = a + a'$ con a appartenente al sottospazio generato dalle colonne di A, e a' ortogonale allo stesso sottospazio, si tratta delle soluzioni del sistema lineare $AX = a$ (un lato dell'equivalenza è ovvio: se $Ax = a$ allora $A^{\mathrm{t}}Ax = A^{\mathrm{t}}a = A^{\mathrm{t}}b$, poiché $A^{\mathrm{t}}a' = 0$ per ipotesi; d'altro lato, se $A^{\mathrm{t}}Ax = A^{\mathrm{t}}b = A^{\mathrm{t}}a$ abbiamo che $Ax - a$ appartiene sia allo spazio delle colonne di A, sia al suo ortogonale, e dunque è nullo).

2. Spazi Vettoriali Euclidei Reali: cross-product e volumi.

Avvertenza terminologica. *Nel seguito scriveremo dei determinanti "misti", ovvero determinanti di matrici quadrate in cui alcune entrate della matrice saranno occupate da vettori. Intendiamo queste scritture come una semplice stenografia, e quei determinanti calcolati secondo le usuali regole usando il prodotto tra scalari, il prodotto tra scalari e vettori, e il prodotto scalare tra vettori: trattandosi di operazioni commutative e la terza bilineare, nessuna ambiguità ne dovrebbe risultare. Il lettore è sempre invitato a capire bene qual è il risultato dei calcoli (un vettore o uno scalare?).*

Segnaliamo infine che tutte le formule di questo tipo qui scritte possono essere rigorosamente interpretate in una opportuna algebra tensoriale sullo spazio vettoriale che si usa, o in un opportuno suo quoziente.

2.1. Definizione (Cross-Product o Prodotto Vettore). *Sia $V_n(\mathbb{R})$ lo spazio vettoriale standard su $\mathbb{R}$ di dimensione n e sia $\mathscr{E} = (e_1, \dots, e_n)$ la base canonica. Definiamo una applicazione* $\mathrm{cross} : V_n(\mathbb{R})^{n-1} \longrightarrow V_n(\mathbb{R})$ *tramite la formula:*

$$\mathrm{cross}(v_1, \dots, v_{n-1}) := \det\begin{pmatrix} \mathscr{E}^{\mathrm{t}} & v_1 & \dots & v_{n-1} \end{pmatrix} = \begin{vmatrix} e_1 & v_{1,1} & \cdots & v_{n-1,1} \\ e_2 & v_{1,2} & \cdots & v_{n-1,2} \\ \vdots & \vdots & \ddots & \vdots \\ e_n & v_{1,n} & \cdots & v_{n-1,n} \end{vmatrix}$$

In generale le componenti di $\mathrm{cross}(v_1, \dots, v_{n-1})$ *sono i minori segnati d'ordine $n-1$ della matrice che ha come colonne le componenti dei vettori $v_1, \dots, v_{n-1}$.*
In particolare:

2.1.1. *per $n = 1$ si ha* $\mathrm{cross}(\varnothing) = 1$;

2.1.2. *per $n = 2$ si ha* $\mathrm{cross}(v) = \begin{pmatrix} v_2 \\ -v_1 \end{pmatrix}$ *se* $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$;

2.1.3. *per $n = 3$ scriviamo* $v \times w = \mathrm{cross}(v, w) = \begin{pmatrix} v_2w_3 - v_3w_1 \\ -v_1w_3 + v_3w_1 \\ v_1w_2 - v_2w_1 \end{pmatrix}$ *se* $v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$ *e* $w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}$.

2.1.4. Si osservi quindi che il vettore $\mathrm{cross}(v_1, \dots, v_{n-1})$ può essere caratterizzato (o definito) come l'unico vettore tale che

$$w \cdot \mathrm{cross}(v_1, \dots, v_{n-1}) = \det\begin{pmatrix} w & v_1 & \cdots & v_{n-1} \end{pmatrix} \qquad \text{per ogni } w \in V_n(\mathbb{R})$$

(infatti, per non degenerazione, per definire un vettore basta definire il suo prodotto scalare contro tutti i vettori dello spazio, o tutti i vettori di una base). Applicando questo a $w = v_i$, $w = \mathrm{cross}(v_1, \dots, v_{n-1})$, $w = \mathrm{cross}(u_1, \dots, u_{n-1})$ troveremo proprietà interessanti dell'operazione.

2.2. Teorema (Proprietà del cross-product).

($C1$) $\mathrm{cross}(v_1,\dots,v_{n-1})=0$ *se e solo se* $v_1,\dots,v_{n-1}$ *sono linearmente dipendenti;*

($C2$) $\mathrm{cross}(v_{\sigma(1)},\dots,v_{\sigma(n-1)})=\mathrm{sgn}(\sigma)\mathrm{cross}(v_1,\dots,v_{n-1})$ *(per ogni permutazione* $\sigma\in\mathfrak{S}_{n-1}$*);*

($C3$) $v_i\cdot\mathrm{cross}(v_1,\dots,v_{n-1})=0$ *(cioè parlando in termini di spazi vettoriali euclidei,* $\mathrm{cross}(v_1,\dots,v_{n-1})$ *è ortogonale a* v_i*) per ogni* i*;*

($C4$) *multilinearità:* $\mathrm{cross}(v_1,\dots,\sum_j\alpha_j w_j,\dots,v_{n-1})=\sum_j\alpha_j\mathrm{cross}(v_1,\dots,w_j,\dots,v_{n-1})$ *per ogni posizione delle variabili;*

($C5$) *Se* $v_1,\dots,v_{n-1}$ *sono linearmente indipendenti, allora* $\mathrm{cross}(v_1,\dots,v_{n-1}),v_1,\dots,v_{n-1}$ *formano una base di* $V_n(\mathbb{R})$ *equiorientata con la base canonica.*

Dimostrazione. Tutte le proprietà seguono immediatamente dalla definizione e dalle proprietà del determinante. Per l'ultimo punto basta calcolare il determinante della matrice che ha come colonne i vettori $\mathrm{cross}(v_1,\dots,v_{n-1}),v_1,\dots,v_{n-1}$, sviluppando rispetto alla prima colonna: ne risulta una somma di quadrati non tutti nulli. □

2.3. Teorema (Lagrange). *Consideriamo ora lo spazio euclideo* $V_n(\mathbb{R})$*; allora la norma del cross-product si può calcolare tramite il determinante:*

$$\|\mathrm{cross}(v_1,\dots,v_{n-1})\|^2=\left|(\,v_i\cdot v_j\,)_{i,j}\right|=\begin{vmatrix}\|v_1\|^2 & v_1\cdot v_2 & \cdots & v_1\cdot v_{n-1}\\ v_2\cdot v_1 & \|v_2\|^2 & \cdots & v_2\cdot v_{n-1}\\ \vdots & \vdots & \ddots & \vdots\\ v_{n-1}\cdot v_1 & v_{n-1}\cdot v_2 & \cdots & \|v_{n-1}\|^2\end{vmatrix}.$$

In particolare:

2.3.1. *per* $n=1$ *si ha* $\|\mathrm{cross}(\varnothing)\|=1$*;*

2.3.2. *nel caso* $n=2$ *l'identità di Lagrange si riduce a* $\|\mathrm{cross}(v)\|=\|v\|$*;*

2.3.3. *nel caso* $n=3$, $v\times w=\mathrm{cross}(v,w)$, *l'identità di Lagrange è*

$$\|v\times w\|^2=\begin{vmatrix}\|v\|^2 & v\cdot w\\ w\cdot v & \|w\|^2\end{vmatrix}=\|v\|^2\,\|w\|^2-(v\cdot w)^2=\|v\|^2\,\|w\|^2\sin^2\vartheta(v,w)$$

e si generalizza in

$$\sum_{i<j}(x_iy_j-x_jy_i)^2=\left(\sum_{i=1}^n x_i^2\right)\left(\sum_{i=1}^n y_i^2\right)-\left(\sum_{i=1}^n x_iy_i\right)^2$$

ovvero

$$\|(x\ y)\|^2=\|x\|^2\,\|y\|^2-(x\cdot y)^2$$

ove $x,y\in V_n(\Bbbk)$ *e* $\|(x\ y)\|$ *è la radice quadrata della somma dei quadrati dei minori* 2×2 *della matrice formata dai due vettori.*

Dimostrazione. Si sviluppano i calcoli:

$$\begin{aligned}\|\mathrm{cross}(v_1,\dots,v_{n-1})\|^2&=\mathrm{cross}(v_1,\dots,v_{n-1})\cdot\mathrm{cross}(v_1,\dots,v_{n-1})\\&=\det\begin{pmatrix}\mathscr{E}^{\mathrm{t}} & v_1 & \cdots & v_{n-1}\end{pmatrix}^{\mathrm{t}}\det\begin{pmatrix}\mathscr{E}^{\mathrm{t}} & v_1 & \cdots & v_{n-1}\end{pmatrix}\\&=\det\left(\begin{pmatrix}\mathscr{E}^{\mathrm{t}} & v_1 & \cdots & v_{n-1}\end{pmatrix}^{\mathrm{t}}\begin{pmatrix}\mathscr{E}^{\mathrm{t}} & v_1 & \cdots & v_{n-1}\end{pmatrix}\right)\\&=\det\left(\begin{pmatrix}\mathscr{E}\\ v_1^{\mathrm{t}}\\ \vdots\\ v_{n-1}^{\mathrm{t}}\end{pmatrix}\begin{pmatrix}\mathscr{E}^{\mathrm{t}} & v_1 & \cdots & v_{n-1}\end{pmatrix}\right)\\&=\begin{vmatrix}n & v_1 & v_2 & \cdots & v_{n-1}\\ v_1^{\mathrm{t}} & \|v_1\|^2 & v_1\cdot v_2 & \cdots & v_1\cdot v_{n-1}\\ v_2^{\mathrm{t}} & v_2\cdot v_1 & \|v_2\|^2 & \cdots & v_2\cdot v_{n-1}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ v_{n-1}^{\mathrm{t}} & v_{n-1}\cdot v_1 & v_{n-1}\cdot v_2 & \cdots & \|v_{n-1}\|^2\end{vmatrix}\end{aligned}$$

e poi si sviluppa rispetto alla prima riga.

In alternativa si può usare il seguente prodotto di matrici:

$$\begin{pmatrix} v_0^{\mathrm{t}} \\ v_1^{\mathrm{t}} \\ \vdots \\ v_{n-1}^{\mathrm{t}} \end{pmatrix} \begin{pmatrix} v_0 & v_1 & \cdots & v_{n-1} \end{pmatrix} = \begin{pmatrix} \|v_0\|^2 & 0 & 0 & \cdots & 0 \\ 0 & \|v_1\|^2 & v_1 \cdot v_2 & \cdots & v_1 \cdot v_{n-1} \\ 0 & v_2 \cdot v_1 & \|v_2\|^2 & \cdots & v_2 \cdot v_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & v_{n-1} \cdot v_1 & v_{n-1} \cdot v_2 & \cdots & \|v_{n-1}\|^2 \end{pmatrix}$$

dove $v_0 = \mathrm{cross}(v_1, \dots, v_{n-1})$, e passare ai determinanti (discutendo a parte il caso 0; le matrici a sinistra hanno determinante $\|v_0\|^2$). □

2.3.4. Generalizzazione: formule di Binet-Gram. Dati r vettori $v_1, \dots, v_r$ in $V_n(\mathbb{R})$ con $r \leqslant n$, sia $W \in M_{n,r}(\Bbbk)$ la matrice che ha quei vettori come colonne. Allora, definito $\|W\|$ ("norma della matrice W") come la radice quadrata della somma dei quadrati dei minori di ordine r della matrice stessa (si tratta di $\binom{n}{r}$ termini), la formula di Lagrange si generalizza in

$$\|W\|^2 = \left| \left(v_i \cdot v_j \right)_{i,j} \right| = \det(W^{\mathrm{t}} W)$$

(spesso la matrice dei prodotti scalari, cioè la $W^{\mathrm{t}}W$, si dice matrice di Gram dei vettori dati, e questa formula si dice calcolo di Binet del determinante di Gram).

Una dimostrazione elementare della formula Binet-Gram si può ottenere ricordando l'astuzia di Binet: $\begin{pmatrix} \mathbb{O} & B \\ A & \mathbb{I}_n \end{pmatrix} \begin{pmatrix} -\mathbb{I}_r & \mathbb{O} \\ A & \mathbb{I}_n \end{pmatrix} = \begin{pmatrix} BA & B \\ \mathbb{O} & \mathbb{I}_n \end{pmatrix}$ che dà i determinanti $\det(BA) = \sum_{|I|=r} \det A^{(I)} \det B_{(I)}$ (somma sugli insiemi di indici I con r termini), applicata a $A = W$ e $B = W^{\mathrm{t}}$.

È forse più interessante notare il significato geometrico della formula: essa dice che il quadrato del volume r-dimensionale del parallelepipedo generato da r vettori (vedi sotto) si può ottenere come somma dei quadrati dei volumi r-dimensionali che questi vettori proiettano sugli spazi coordinati di dimensione r. In questo senso si tratta di una generalizzazione del teorema di Pitagora (che è il caso $r = 1$, lunghezza di un vettore), o ancora che si tratta del quadrato della norma euclidea del vettore di $\mathbb{R}^{\binom{n}{r}}$ dato dai minori di rango massimo della matrice dei vettori dati.

Più in generale, che relazione c'è tra il quadrato del volume r-dimensionale del parallelepipedo generato da r vettori (vedi sotto) e la somma dei quadrati dei volumi s-dimensionali che questi vettori proiettano sugli spazi coordinati di dimensione $s \leqslant r$? In qualche senso questo generalizza la formula di Lagrange e di Binet-Gram, che indica la dipendenza del volume dalla lunghezza dei vettori generatori tramite un prodotto con una complicata matrice trigonometrica.

2.3.5. Nota sulla matrice trigonometrica. La formula del teorema di Lagrange si può riscrivere usando la definizione di coseno nel modo seguente:

$$\begin{aligned} \|\mathrm{cross}(v_1, \dots, v_{n-1})\|^2 &= \|v_1\|^2 \|v_2\|^2 \cdots \|v_{n-1}\|^2 \left| \left(\cos \vartheta(v_i, v_j) \right)_{i,j} \right| \\ &= \|v_1\|^2 \|v_2\|^2 \cdots \|v_{n-1}\|^2 \begin{vmatrix} 1 & \cos\vartheta_{1,2} & \cdots & \cos\vartheta_{1,n-1} \\ \cos\vartheta_{1,2} & 1 & \cdots & \cos\vartheta_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \cos\vartheta_{1,n-1} & \cos\vartheta_{2,n-1} & \cdots & 1 \end{vmatrix} \end{aligned}$$

ove $\vartheta_{i,j} = \vartheta(v_i, v_j)$. *Si osservi che il determinante della matrice dei coseni è sempre positivo, e ha una facile interpretazione nel caso $n = 2$ (seno di un angolo, area del parallelogramma); esplicitare il conto e trovare una simile interpretazione nel caso $n = 3$ (calcolo del volume di un parallelepipedo), e generalizzare in dimensione n: la formula di Lagrange generalizza il calcolo dei volumi in termini di "base per altezza", in particolare è il prodotto delle lunghezze dei lati se sono a due a due ortogonali.*

2.3.6. Problema. Usando gli stessi metodi che per il teorema di Lagrange, si dimostri la seguente generalizzazione:

$$\mathrm{cross}(u_1, \dots, u_{n-1}) \cdot \mathrm{cross}(v_1, \dots, v_{n-1}) = \det(u_i \cdot v_j) \ .$$

Conviene usare il prodotto delle matrici $\begin{pmatrix} u_0 & v_1 & \cdots & v_{n-1} \end{pmatrix}^{\mathrm{t}}$ e $\begin{pmatrix} v_0 & u_1 & \cdots & u_{n-1} \end{pmatrix}^{\mathrm{t}}$ dove $v_0 = \mathrm{cross}(v_1, \dots, v_{n-1})$ e $u_0 = \mathrm{cross}(u_1, \dots, u_{n-1})$.

In particolare:

per $n = 2$ si ha che $\mathrm{cross}(u) \cdot \mathrm{cross}(v) = u \cdot v$

per $n = 3$ si ha che $(u_1 \times u_2) \cdot (v_1 \times v_2) = \det(u_i \cdot v_j) = (u_1 \cdot v_1)(u_2 \cdot v_2) - (u_1 \cdot v_2)(u_2 \cdot v_1)$.

2.3.7. Problema. Provare che risulta:

$$\mathrm{cross}(u_2, \dots, u_{n-1}, \mathrm{cross}(v_1, \dots, v_{n-1})) = \sum_{i=1}^{n-1} (-1)^{i+1} \big| u_a \cdot v_b \big|_{\substack{a \neq 1 \\ b \neq i}} v_i \ .$$

Suggerimento: conviene utilizzare il punto precedente osservando che il vettore cercato appartiene allo spazio $\mathrm{cross}(v_1, \dots, v_{n-1})^\perp = \langle v_1, \dots, v_{n-1} \rangle$, cioè è del tipo $\sum_i \alpha_i v_i$ e dunque basta trovare i coefficienti α_i. Tali coefficienti si possono determinare a partire dal sistema lineare delle equazioni che impongono l'ortogonalità di $\sum_i \alpha_i v_i$ ai vettori u_j per $j = 2, \dots, n-1$, aggiungendo una equazione corrispondente al prodotto scalare con un vettore u_1 indipendente dagli altri...

In particolare:

per $n = 2$ si ha che $\mathrm{cross}(\mathrm{cross}(u)) = -u$

per $n = 3$ si ha che $u \times (v \times w) = (u \cdot w)v - (u \cdot v)w$; di conseguenza abbiamo $v \times (v \times w) = (v \cdot w)v - \|v\|^2 w$ e $w \times (v \times w) = \|w\|^2 v - (w \cdot v)w$.

Problema: dimostrare questa formula direttamente, usando che l'ortogonalità con $v \times w$ per dire che $u \times (v \times w) = \alpha v + \beta w$, e poi i prodotti scalari con u e con v per ottenere le equazioni da cui ricavare α e β.

Si osservi in particolare che il prodotto vettore non è associativo!

2.3.8. Problema. Se $v_1, v_2 \in \Bbbk^3$, allora $v_1 \times v_2$ ha come componenti i coefficienti di una equazione del piano generato da v_1, v_2. Poi, se $u_1, u_2 \in \Bbbk^3$ sono altri vettori, l'intersezione tra i piani generati (se ha dimensione 1) ha come generatore $(v_1 \times v_2) \times (u_1 \times u_2)$. Provare che

$$(v_1 \times v_2) \times (u_1 \times u_2) = \det(v_1\, v_2\, u_2)u_1 - \det(v_1\, v_2\, u_1)u_2 = -\det(u_1\, u_2\, v_2)v_1 + \det(u_1\, u_2\, v_1)v_2 \ .$$

Quale altra interpretazione geometrica è possibile per questo prodotto? Pensare ai vettori come equazioni di piani...

2.4. Definizione (Prodotto misto). $|w\ v_1 \cdots v_{n-1}| := w \cdot \mathrm{cross}(v_1, \dots, v_{n-1})$ *è il determinante della matrice che ha come colonne gli n vettori, e si dice il prodotto misto dei vettori w e $v_1, \dots, v_{n-1}$; è un elemento di $\Bbbk$ che si annulla se e solo se gli n vettori coinvolti sono linearmente dipendenti. Si ha $|v_{\sigma 1} \cdots v_{\sigma n}| = \mathrm{sgn}(\sigma)|v_1 \cdots v_n|$ per ogni permutazione σ.*

2.4.1. Nel caso $n = 2$ la formula delle permutazioni si riduce a $|v\ w| = -|w\ v|$.

2.4.2. Nel caso $n = 3$ la formula delle permutazioni dà luogo a sei termini:

$$|u\ v\ w| = |v\ w\ u| = |w\ u\ v| = -|u\ w\ v| = -|w\ v\ u| = -|v\ u\ w|$$

(i 3-cicli mantengono il prodotto misto, gli scambi ne cambiano il segno).

2.5. Definizione (volumi). *Nel caso di spazi vettoriali euclidei, definiamo il volume orientato (risp. volume assoluto o volume) n-dimensionale dell'n-poliparallelepipedo generato da n vettori $v_1, \dots, v_n$ come il valore del prodotto misto (risp. il modulo del prodotto misto) di quegli n vettori. Dunque si tratta del determinante (risp. del valore assoluto del determinante) della matrice che ha quei vettori come colonne. Si scrive* $\mathrm{Vol}_n \Pi(v_1, \dots, v_n)$ *se $v_1, \dots, v_n$ sono i lati del parallelepipedo.*

2.5.1. Ricordiamo che dati m vettori $v_1, \dots, v_m$ di uno spazio vettoriale euclideo, indichiamo con $\Pi(v_1, \dots, v_m)$ (m-parallelepipedo) l'insieme delle combinazioni lineari con coefficienti compresi tra 0 e 1, e $\Delta(v_1, \dots, v_m)$ (m-edro) l'insieme delle combinazioni lineari con coefficienti non negativi e di somma non superiore ad 1. In particolare $\Delta(v_1, \dots, v_m) \subseteq \Pi(v_1, \dots, v_m)$.

2.5.2. Giustificazione della definizione discende dal fatto che le proprietà del determinante (valere 1 sui vettori della base canonica e la multilinearità alternante sulle colonne) fissano quella funzione e sono le proprietà corrette per un calcolo di volumi (orientati): l'ipercubo unitario abbia n-volume 1; se si moltiplica un lato per un certo valore il volume sia moltiplicato per quel valore; se si accostano due parallelepipedi di "basi uguali" allora la somma dei volumi corrisponda al volume del parallelepipedo che ha come ultimo lato la somma dei due ultimi vettori dei solidi dati (riflettere su questo fatto facendo qualche disegno); se i lati non sono indipendenti il volume sia nullo.

2.5.3. Automorfismi e volumi. Dalla definizione segue subito che gli automorfismi moltiplicano i volumi orientati per il loro determinante (e i volumi per il valore assoluto del loro determinante): se Π indica un poliparallelepipedo determinato da $v_1, \dots, v_n$ e $\varphi\Pi$ indica il poliparallelepipedo determinato da $\varphi v_1, \dots, \varphi v_n$, allora $\mathrm{Vol}_n(\varphi\Pi) = \det(\varphi)\mathrm{Vol}_n(\Pi)$.

In particolare le trasformazioni ortogonali conservano i volumi (non orientati), mentre le conformità li moltiplicano per la potenza n-esima del rapporto di conformità.

2.6. Teorema (calcolo di m-volumi di m-parallelepipedi e m-edri). *Siano $v_1, \dots, v_m$ m vettori di $V_n(\mathbb{R})$, con $m \leqslant n$. Il volume m-dimensionale dell'm-parallelepipedo $\Pi(v_1, \dots, v_m)$ generato da quei vettori è dato da*

$$\mathrm{Vol}_m(\Pi(v_1, \dots, v_m)) = \sqrt{\det(W^{\mathrm{t}}W)} = \sqrt{\det\left(\, v_i \cdot v_j \,\right)_{i,j}} = \|W\|$$

mentre quello dell'm-edro $\Delta(v_1, \dots, v_m)$ generato è $\frac{1}{m!}$ volte quello di $\Pi(v_1, \dots, v_m)$, e dunque:

$$\mathrm{Vol}_m(\Delta(v_1, \dots, v_m)) = \frac{1}{m!}\sqrt{\det(W^{\mathrm{t}}W)} = \frac{1}{m!}\sqrt{\det\left(\, v_i \cdot v_j \,\right)_{i,j}} = \frac{1}{m!}\|W\|$$

ove $W \in M_{n,m}$ è la matrice le cui colonne sono gli m vettori dati.

Dimostrazione. Sia $T \in M_{n,n-m}$ una matrice le cui colonne formino una base ortonormale dello spazio ortogonale a $\langle v_1, \dots, v_m \rangle$. Allora il volume cercato è

$$|\det(W|T)| = \sqrt{\det((W|T)^{\mathrm{t}}(W|T))} = \sqrt{\det(\begin{pmatrix} W^{\mathrm{t}} \\ T^{\mathrm{t}} \end{pmatrix}(W|T))} = \sqrt{\det\begin{pmatrix} W^{\mathrm{t}}W & 0 \\ 0 & \mathbb{I}_{n-m} \end{pmatrix}} = \sqrt{\det(W^{\mathrm{t}}W)}.$$

Per quanto riguarda gli m-edri, si tratta di mostrare che un m-parallelepipedo si decompone in $m!$ m-edri tutti di "ugual volume". Questo si può "vedere" per induzione nel modo seguente: è ben noto per $n = 2$ (un parallelogramma si decompone in due triangoli sovrapponibili) e anche per $n = 3$ (un parallelepipedo si decompone in sei tetraedri di ugual volume, avendo a due a due basi uguali e uguali altezze); preso poi un m-parallelepipedo, e scelta una sua $m-1$-faccia come "base", questa può essere decomposta per ipotesi induttiva in $(m-1)!$ $m-1$-edri di ugual volume, in modo da ottenere $(m-1)!$ m-solidi con "facce parallele" e basi gli $m-1$-edri. Ciascuno di questi solidi contiene esattamente m m-edri, ciascuno dei quali ha una base $m-1$-edrale di ugual volume con un'altro e stessa altezza. Provare a rendere rigoroso questo discorso, discutendo il caso dell'n-cubo unitario. □

2.6.1. Si osservi che dalla formula $\mathrm{Vol}_m(\Pi) = \sqrt{\det\left(\, v_i \cdot v_j \,\right)_{i,j}}$ segue che se i vettori sono a due a due ortogonali allora il volume del parallelepipoide m-dimensionale è semplicemente il prodotto delle norme dei vettori che lo generano.

2.6.2. Area di triangoli. Dati due vettori indipendenti $v_1, v_2 \in V_n(\mathbb{R})$ abbiamo che l'area del triangolo $\Delta(v_1, v_2)$ da essi definito è

$$\mathrm{Vol}_2\Delta(v_1, v_2) = \frac{1}{2}\|\left(\, v_1 \;\; v_2 \,\right)\| = \frac{1}{2}\sqrt{\det(v_i \cdot v_j)} = \frac{1}{2}\sqrt{\|v_1\|^2\,\|v_2\|^2 - (v_1 \cdot v_2)^2} = \frac{1}{2}\,\|v_1\|\,\|v_2\|\,|\sin\vartheta(v_1, v_2)|$$

e dall'ultima formula si riconosce l'area in senso elementare.

2.6.3. Volume di tetraedri. Dati tre vettori indipendenti $v_1, v_2, v_3 \in V_n(\mathbb{R})$ abbiamo che il volume del tetraedro $\Delta(v_1, v_2, v_3)$ da essi definito è

$$\mathrm{Vol}_3\Delta(v_1, v_2, v_3) = \frac{1}{6}\|\left(\, v_1 \;\; v_2 \;\; v_3 \,\right)\| = \frac{1}{6}\sqrt{\det(v_i \cdot v_j)} = \frac{1}{6}\,\|v_1\|\,\|v_2\|\,\|v_3\|\,\sqrt{\det(\cos\vartheta(v_i, v_j))}$$

2.6.4. $(n-1)$-volume di $(n-1)$-edri. Dati $n-1$ vettori indipendenti $v_1, \dots, v_{n-1} \in V_n(\mathbb{R})$ abbiamo che il volume dell'$n-1$-edro $\Delta(v_1, \dots, v_{n-1})$ da essi definito è

$$\mathrm{Vol}_{n-1}\Delta(v_1, \dots, v_{n-1}) = \frac{1}{(n-1)!}\|\left(\, v_1 \cdots v_{n-1} \,\right)\| = \frac{1}{(n-1)!}\sqrt{\det(v_i \cdot v_j)}$$

2.6.5. n-Volume di n-edri. Dati n vettori indipendenti $v_1, \dots, v_n \in V_n(\mathbb{R})$ abbiamo che il volume dell'n-edro $\Delta(v_1, \dots, v_n)$ da essi definito è

$$\mathrm{Vol}_n\Delta(v_1, \dots, v_n) = \frac{1}{n!}\,|\, v_1 \quad \cdots \quad v_{n-1} \,|\ .$$

2.6.6. Interpretazione geometrica del cross product. Nel caso di spazi euclidei $V_n(\mathbb{R})$, da un punto di vista geometrico, il cross product di $n-1$ vettori linearmente indipendenti si caratterizza come: il vettore di direzione ortogonale ai vettori dati, di verso tale che l'orientazione di $\mathrm{cross}(v_1,\dots,v_{n-1}), v_1,\dots,v_{n-1}$ concordi con quella della base scelta per esprimere le coordinate (si osservi che il determinante della matrice che ha come colonne i vettori nell'ordine scritto è esattamente il quadrato della norma di $\mathrm{cross}(v_1,\dots,v_{n-1})$), di lunghezza pari al volume $(n-1)$-dimensionale del "poliparallelepipedo" formato dai vettori $v_1,\dots,v_{n-1}$ (per Lagrange).

2.6.7. Orientazioni. Definiamo esattamente cosa intendiamo per orientazione dello spazio: nell'insieme di tutte le basi di $\mathbb{R}^n$ possiamo introdurre la relazione di equivalenza seguente: due basi sono equiorientate se (e solo se) la matrice di cambiamento di base ha determinante positivo (si noti che questo si può fare solo per corpi ordinati: i numeri non nulli si dividono in positivi e negativi a seconda che siano maggiori o minori di zero). Le classi di equivalenza di basi rispetto alla equiorientazione si dicono le orientazioni dello spazio: chiaramente vi sono solo due orientazioni, quella della base canonica, e quella opposta.

2.6.8. Volume e volume laterale per cubi ed edri unitari. Si osservi che il volume dell'n-cubo unitario di $V_n(\mathbb{R})$ è sempre 1, mentre il volume laterale (somma degli $(n-1)$-volumi delle sue facce laterali) cresce al variare di n, e vale esattamente $2n$. Quindi il rapporto tra volume e volume laterale per l'ipercubo unitario è $1/2n$ e diminuisce con n.

Sappiamo che l'n-edro costruito sui vettori della base canonica ha n-volume $1/n!$ e un facile calcolo permette di stabilire che il suo $(n-1)$-volume laterale è $\frac{n+\sqrt{n}}{(n-1)!}$. Quindi il rapporto tra volume e volume laterale per l'n-edro unitario è $1/n(n+\sqrt{n})$ e diminuisce con n più velocemente di quello dell'n-cubo.

3. Trasformazioni ortogonali.

3.1. Definizione-Teorema (trasformazioni ortogonali o isometrie). *Sia φ un automorfismo di $V_n(\mathbb{R})$ in sè; le due proprietà seguenti sono equivalenti:*
(1) *φ rispetta la struttura euclidea, i.e. $\varphi(v)\cdot\varphi(w) = v\cdot w$ per ogni $v,w\in V_n(\mathbb{R})$;*
(2) *φ rispetta la norma dei vettori, i.e. $\|\varphi(v)\| = \|v\|$ per ogni $v\in V_n(\mathbb{R})$;*
(3) *φ manda una (e allora ogni) base ortonormale in una base ortonormale.*
Tali automorfismi si dicono trasformazioni ortogonali o isometrie di $V_n(\mathbb{R})$.

Dimostrazione. È ovvio che (1) implica (2) (basta usare $v=w$). Viceversa per vedere che (2) implica (1) basta notare che applicando l'ipotesi a $v+w$ otteniamo $\|\varphi(v)+\varphi(w)\| = \|v+w\|$, da cui $\|\varphi(v)\|^2 + 2\varphi(v)\cdot\varphi(w) + \|\varphi(w)\|^2 = \|v\|^2 + 2v\cdot w + \|w\|^2$, e si conclude che $\varphi(v)\cdot\varphi(w) = v\cdot w$ (per ogni v e w). □

3.1.1. Una applicazione insiemistica di $V_n(\mathbb{R})$ in sè che soddisfi alla proprietà (1) è necessariamente un morfismo lineare; infatti si tratta di verificare che $\varphi(v+\alpha w) - \varphi(v) - \alpha\varphi(w) = 0$, ovvero che il suo prodotto scalare con sé stesso è nullo.

D'altra parte un morfismo lineare che rispetti la proprietà (2) è necessariamente biiettivo, e dunque un automorfismo. Infatti da $\varphi v = 0$ segue $\|v\| = \|\varphi v\| = 0$, e dunque $v=0$.

Quindi il teorema poteva essere enunciato così: *una applicazione insiemistica di $V_n(\mathbb{R})$ in sè rispetta il prodotto scalare se e solo se è una applicazione lineare che rispetta la norma; e in tal caso si tratta di una applicazione biiettiva, dunque di un automorfismo.*

3.1.2. Si osservi anche che la proprietà (1) è equivalente alla condizione che $\|\varphi(v)-\varphi(w)\| = \|v-w\|$ per ogni $v,w\in V_n(\mathbb{R})$, unito alla condizione $\varphi(0)=0$; per questo tali funzioni vengono chiamate isometrie dello spazio vettoriale euclideo (in cui 0 sia un "punto fisso"): rispettano (lo zero e) le distanze tra i punti dello spazio affine associato allo spazio vettoriale euclideo $V_n(\mathbb{R})$.

3.1.3. Problema. Quali sono le trasformazioni di $V_n(\mathbb{R})$ che rispettano il cross-product, nel senso che $\mathrm{cross}(\varphi v_1,\dots,\varphi v_{n-1}) = \varphi\mathrm{cross}(v_1,\dots,v_{n-1})$ (per ogni scelta dei vettori)? Si osservi che richiedere la proprietà $\mathrm{cross}(\varphi v_1,\dots,\varphi v_{n-1}) = \mathrm{cross}(v_1,\dots,v_{n-1})$ (per ogni scelta dei vettori) è molto restrittivo e porta ad una risposta banale.

3.1.4. Problema. Come le trasformazioni lineari cambiano i volumi? Quali trasformazioni lineari rispettano i volumi?

3.2. Teorema (Gruppo Ortogonale). *Sia φ una trasformazione ortogonale. Ogni matrice A associata a φ usando una base di vettori ortonormali (tali che $v_i \cdot v_j = \delta_{i,j}$) risulta una matrice ortogonale, i.e. tale che $A^{\mathrm{t}}A = \mathbb{I}$, ovvero $A^{-1} = A^{\mathrm{t}}$. Le matrici ortogonali formano un sottogruppo (non normale, se $n > 1$) di $\mathrm{GL}(n, \mathbb{R})$ che si indica con $\mathrm{O}(n, \mathbb{R})$ o $\mathrm{O}_n(\mathbb{R})$ e si dice il Gruppo Ortogonale. Se $A \in \mathrm{O}(n, \mathbb{R})$, allora $\det A = \pm 1$ e gli autovalori complessi di A hanno tutti modulo 1 (dunque se sono reali sono ± 1).*

Dimostrazione. Le colonne $A_{(i)}$ della matrice A sono le immagini dei vettori di una base ortonormale, quindi risulta $A_{(i)} \cdot A_{(j)} = \delta_{i,j}$, da cui segue subito che $A^{\mathrm{t}}A = \mathbb{I}$. Da questo segue che $1 = \det \mathbb{I} = \det(A^{\mathrm{t}}A) = \det(A)^2$, da cui l'asserzione sul determinante.

Se poi α è un autovalore (eventualmente complesso di A) e v autovettore, allora anche il coniugato $\overline{\alpha}$ è autovalore con autovettore $\overline{v}$ (perché la matrice ha coefficienti reali), e allora abbiamo $v^{\mathrm{t}}\overline{v} = (Av)^{\mathrm{t}}\overline{Av} = \alpha\overline{\alpha}v^{\mathrm{t}}\overline{v}$ da cui risulta $|\alpha| = \alpha\overline{\alpha} = 1$ poiché $v^{\mathrm{t}}\overline{v} \neq 0$ (somma di quadrati). □

3.2.1. Alcune osservazioni sugli autospazi e sugli spazi stabili per trasformazioni ortogonale saranno sviluppate in seguito, nel contesto del teorema spettrale.

3.2.2. Il gruppo ortogonale $\mathrm{O}_n(\mathbb{R})$ è un sottogruppo (moltiplicativo) dell'algebra delle matrici $M_n(\mathbb{R})$, ovviamente non è un sottospazio. In effetti usando le coordinate nella base standard delle matrici, esso è definito dalle equazioni di secondo grado $A^{\mathrm{t}}A = \mathbb{I}$. Ci si può comunque chiedere quanti "parametri liberi" servono per definire unicamente (o a meno di una scelta finita) una matrice ortogonale: una matrice qualsiasi è determinata dalle n^2 coordinate (le sue entrate), e per essere ortogonale deve soddisfare un sistema di n^2 equazioni che però non sono indipendenti (per simmetria), e in effetti si vede subito che le condizioni indipendenti sono $n + (n-1) + \cdots + 2 + 1 = n(n+1)/2$, da cui si ricava che rimangono $n^2 - n(n+1)/2 = n(n-1)/2$ parametri indipendenti. Quindi per $n = 1, 2, 3, 4, 5, 6, 7, 8...$ troviamo rispettivamente $0, 1, 3, 6, 10, 15, 21, 28, ...$ gradi di libertà (dimensione come varietà reale del gruppo ortogonale).

3.2.3. Gruppo ortogonale speciale. Il sottinsieme di $\mathrm{O}_n(\mathbb{R})$ formato dalle matrici di determinante 1 si indica con $\mathrm{SO}(n, \mathbb{R})$ o $\mathrm{SO}_n(\mathbb{R})$ e si dice il Gruppo Ortogonale Speciale. Si tratta di un sottogruppo normale di indice 2 di $\mathrm{O}_n(\mathbb{R})$, cioè il quoziente $\mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R})$ è isomorfo a $\{\pm 1\}$ (gruppo moltiplicativo con due elementi: restringendo la funzione determinante al sottogruppo $\mathrm{O}_n(\mathbb{R})$, abbiamo che il nucleo è dato da $\mathrm{SO}_n(\mathbb{R})$, e l'immagine da $\{\pm 1\}$).

Si osservi che scelta $S \in \mathrm{O}_n(\mathbb{R}) \smallsetminus \mathrm{SO}_n(\mathbb{R})$, la moltiplicazione per S induce una biiezione insiemistica $\mathrm{SO}_n(\mathbb{R}) \to \mathrm{O}_n(\mathbb{R}) \smallsetminus \mathrm{SO}_n(\mathbb{R})$ (qual'è l'applicazione inversa? perché non si parla di morfismo di gruppi?).

3.2.4. Formula di Parseval reale. Se $v_1, \ldots, v_n$ è base ortonormale di $V_n(\mathbb{R})$, allora sappiamo che le coordinate di $v \in V_n(\mathbb{R})$ in questa base sono date da Ax ove x è la colonna delle componenti di v (coordinate di v nella base canonica) e A è matrice ortogonale del cambiamento di base dalla base canonica alla base data. Dunque risulta $v \cdot w = x^{\mathrm{t}}y = x^{\mathrm{t}}A^{\mathrm{t}}Ay = (Ax)^{\mathrm{t}}(Ay)$, ovvero il prodotto scalare tra v e w si può calcolare facendo la somma dei prodotti delle coordinate omonime *in una qualsiasi base ortonormale di $V_n(\mathbb{R})$*.

Ricordando poi che la coordinata i-esima di v nella base ortonormale $v_1, \ldots, v_n$ è data da $v \cdot v_i$ (ri)otteniamo la cosiddetta formula di Parseval (reale): se $v_1, \ldots, v_n$ è base ortonormale di $V_n(\mathbb{R})$ e $v, w \in V_n(\mathbb{R})$ allora $v \cdot w = \sum_{i=1}^{n}(v \cdot v_i)(w \cdot v_i)$.

3.2.5. Matrici di simmetrie ortogonali. Consideriamo un vettore non nullo $v \in V_n(\mathbb{R})$ e scriviamo la matrice della simmetria di direzione v e asse l'iperpiano ortogonale $v^{\perp}$. Si tratta dell'applicazione $s_v : V_n(\mathbb{R}) \to V_n(\mathbb{R})$ che manda un generico vettore x in

$$s_v(x) = x - 2p_v(x) = x - 2\frac{x \cdot v}{v \cdot v}v = (\mathrm{id} - 2\frac{vv^{\mathrm{t}}}{v^{\mathrm{t}}v})x$$

da cui si legge direttamente la matrice. Se supponiamo $v \cdot v = v^{\mathrm{t}}v = 1$, allora la matrice di s_v è data da $\mathbb{I}_n - 2vv^{\mathrm{t}}$. Si noti che vv^{t} è la matrice della proiezione su v con direzione $v^{\perp}$ (quindi matrice di rango 1), mentre $\mathbb{I}_n - vv^{\mathrm{t}}$ è matrice della proiezione su $v^{\perp}$ con direzione v (quindi di rango $n-1$).

Più generalmente, se W è un sottospazio di $v \in V_n(\mathbb{R})$ di dimensione m possiamo scrivere la matrice della simmetria ortogonale su W (cioè di direzione $W^\perp$) nel modo seguente. Sia $w_1, \dots, w_r$ una base ortonormale di $W^\perp$; allora la simmetria s_W in questione ha matrice $\mathbb{I}_n - 2\sum_{i=1}^r w_i w_i^{\mathrm{t}}$. Si osservi che $\sum_{i=1}^r w_i w_i^{\mathrm{t}}$ è la matrice della proiezione ortogonale su $W^\perp$ (dunque di rango $r = n-m$), mentre $\mathbb{I}_n - \sum_{i=1}^r w_i w_i^{\mathrm{t}}$ è la matrice della proiezione ortogonale su W (dunque di rango m).

3.2.6. Decomposizione in simmetrie ortogonali (Cartan-Dieudonné). *Ogni isometria di uno spazio euclideo di dimensione n si scrive come composizione di al più n simmetrie ortogonali (rispetto a vettori non nulli). In particolare, le simmetrie ortogonali generano tutto il gruppo delle isometrie.*

Si dimostra per induzione sulla dimensione: se vi è un autovettore non nullo ci si riconduce subito all'ipotesi induttiva usando l'ortogonale dell'autovettore (sottospazio di dimensione minore e stabile per l'isometria), altrimenti si sceglie un vettore v, e si compone l'isometria con la riflessione ortogonale rispetto al vettore $\varphi v - v$, che dà una isometria con vettore unito v, e quindi permette di usare l'ipotesi induttiva.

3.2.7. Supponiamo ora che il sottospazio W sia generato dalle colonne della matrice A (matrice $n \times m$ di rango m); allora:

(1) se $A^{\mathrm{t}}A = \mathbb{I}_m$ allora AA^{t} è la matrice della proiezione ortogonale su W, $\mathbb{I}_n - AA^{\mathrm{t}}$ è la matrice della proiezione ortogonale su $W^\perp$, e $\mathbb{I}_n - 2AA^{\mathrm{t}}$ è la matrice della simmetria ortogonale si asse W;

(2) in generale, la matrice della proiezione ortogonale su W è data da $A(A^{\mathrm{t}}A)^{-1}A^{\mathrm{t}}$ (infatti si vede subito che le colonne di A sono autovettori d'autovalore 1, e che i vettori ortogonali alle colonne di A sono annullati), e dunque la simmetria ortogonale di asse W ha matrice data da $\mathbb{I}_n - 2A(A^{\mathrm{t}}A)^{-1}A^{\mathrm{t}}$. Si osservi la similitudine con il caso di un vettore, e si tenga presente che A non è quadrata (la formula non è stupida).

3.3. Trasformazioni ortogonali del piano. Si consideri lo spazio vettoriale reale $V_2(\mathbb{R})$ munito del prodotto scalare e si indichi con $\mathrm{O}_2(\mathbb{R})$ il gruppo delle matrici delle isometrie di $V_2(\mathbb{R})$. Si osservi che tali matrici possono avere autovalori reali ± 1, oppure due autovalori complessi di modulo uno (uno inverso dell'altro, cioè uno coniugato dell'altro).

3.3.1. $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{O}_2(\mathbb{R})$ se e solo se le due colonne formano una base ortonormale di $V_2(\mathbb{R})$: se la prima si scrive $\left(\begin{smallmatrix} \cos\vartheta \\ \operatorname{sen}\vartheta \end{smallmatrix}\right)$, la seconda dev'essere $\pm\left(\begin{smallmatrix} -\operatorname{sen}\vartheta \\ \cos\vartheta \end{smallmatrix}\right)$; dunque esiste un unico numero reale ϑ, $0 \leqslant \vartheta < 2\pi$, tale che

$$A = \begin{pmatrix} \cos\vartheta & \mp\operatorname{sen}\vartheta \\ \operatorname{sen}\vartheta & \pm\cos\vartheta \end{pmatrix}$$

ove si prendono o entrambi i segni superiori , o entrambi gli inferiori.

3.3.2. Il sottoinsieme $\mathrm{SO}_2(\mathbb{R}) = \left\{\left(\begin{smallmatrix} \cos\vartheta & -\operatorname{sen}\vartheta \\ \operatorname{sen}\vartheta & \cos\vartheta \end{smallmatrix}\right) | 0 \leqslant \vartheta < 2\pi\right\}$ di $\mathrm{O}_2(\mathbb{R})$ è il gruppo speciale ortogonale del piano $\mathrm{SO}_2(\mathbb{R})$ e si dice anche il gruppo delle rotazioni del piano euclideo.

3.3.3. Se $A \in \mathrm{O}_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R})$ allora $A^2 = \mathbb{I}_2$, cioè le matrici ortogonali non speciali sono tutte matrici di riflessioni (ortogonali); è vero il viceversa? Si interpreti tramite un disegno la seguente relazione:

$$\left(\begin{smallmatrix} \cos\vartheta & \operatorname{sen}\vartheta \\ \operatorname{sen}\vartheta & -\cos\vartheta \end{smallmatrix}\right) = \left(\begin{smallmatrix} \cos\frac{\vartheta}{2} & -\operatorname{sen}\frac{\vartheta}{2} \\ \operatorname{sen}\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \cos\frac{\vartheta}{2} & \operatorname{sen}\frac{\vartheta}{2} \\ -\operatorname{sen}\frac{\vartheta}{2} & \cos\frac{\vartheta}{2} \end{smallmatrix}\right).$$

3.3.4. Invece, in $\mathrm{SO}_2(\mathbb{R})$ vi sono elementi di periodo n, per ogni intero $n \geqslant 1$, ed elementi di periodo infinito (i.e. $A^n \neq \mathbb{I}_2$ se $n > 0$).

3.3.5. L'applicazione $x \mapsto \left(\begin{smallmatrix} \cos 2\pi x & -\operatorname{sen} 2\pi x \\ \operatorname{sen} 2\pi x & \cos 2\pi x \end{smallmatrix}\right)$ induce un isomorfismo di gruppi $\varphi : (\mathbb{R}/\mathbb{Z}, +) \longrightarrow \mathrm{SO}_2(\mathbb{R})$ (che trasforma la somma in $\mathbb{R}/\mathbb{Z}$ nel prodotto di matrici. Usando la legge di composizione di $\mathrm{SO}_2(\mathbb{R})$ (prodotto di matrici) possiamo riscrivere le formule di addizione per il seno ed il coseno.

3.3.6. L'applicazione $z = a + ic \mapsto A_z = \left(\begin{smallmatrix} a & -c \\ c & a \end{smallmatrix}\right)$ induce un isomorfismo di gruppi (moltiplicativi) $\mathbb{S}^1 \longrightarrow \mathrm{SO}_2(\mathbb{R})$ dei complessi di modulo 1 sul gruppo ortogonale speciale.

3.3.7. Riassumendo, abbiamo i seguenti isomorfismi di gruppi:

$$\begin{array}{ccccc} \mathrm{SO}_2(\mathbb{R}) & \cong & \mathbb{S}^1 & \cong & \mathbb{R}/2\pi\mathbb{Z} \\ \left(\begin{smallmatrix} \cos\vartheta & -\operatorname{sen}\vartheta \\ \operatorname{sen}\vartheta & \cos\vartheta \end{smallmatrix}\right) & \mapsto & \cos\vartheta + i\operatorname{sen}\vartheta & \mapsto & \vartheta \end{array}$$

(moltiplicativi i primi due, addittivo il terzo).

3.3.8. Siano $A, B \in \mathrm{O}_2(\mathbb{R}) \setminus \mathrm{SO}_2(\mathbb{R})$; si mostri che $AB \in \mathrm{SO}_2(\mathbb{R})$ (che rotazione è?); è vero che ogni elemento di $SO_2(\mathbb{R})$ si può scrivere come prodotto di al più due elementi di $\mathrm{O}_2(\mathbb{R})$ di periodo 2

(due riflessioni fanno una rotazione, e di che angolo?)? *Di solito si dice che piegando un foglio di carta (ogni punto si scambia con quello sovrapposto dalla piegatura) si possono ottenere tutte le rotazioni del piano.*

3.4. Trasformazioni ortogonali dello spazio. Si consideri lo spazio vettoriale reale $V_3(\mathbb{R})$ munito del prodotto scalare; si indichi con $\mathrm{O}_3(\mathbb{R})$ il gruppo delle matrici delle isometrie di $V_3(\mathbb{R})$.

3.4.1. Allora $A \in \mathrm{O}_3(\mathbb{R})$ se e solo se le sue colonne (risp. righe) sono una base ortonormale di $\mathbb{R}^3$; oppure se e solo se $A^{\mathrm{t}}A = \mathbb{I}_3$. Se ne deduca che, se $A \in \mathrm{O}_3(\mathbb{R})$, allora $\det A = \pm 1$, e che $\mathrm{O}_3(\mathbb{R})$ contiene un sottogruppo isomorfo al gruppo $\mathfrak{S}_3$ delle permutazioni su 3 oggetti (permutazioni dei tre vettori della base canonica).

3.4.2. Il sottoinsieme $\mathrm{SO}_3(\mathbb{R})$ di $\mathrm{O}_3(\mathbb{R})$, costituito dalle matrici di determinante 1, è un sottogruppo normale di $\mathrm{O}_3(\mathbb{R})$ di indice 2.

3.4.3. Per ogni $A \in \mathrm{O}_3(\mathbb{R})$ si ha $\det[(A - \mathbb{I}_3)(A^{\mathrm{t}} + \mathbb{I}_3)] = 0$ (ricordare che il determinante di matrici antisimmetriche d'ordine dispari è nullo), e quindi A possiede l'autovalore 1 oppure -1. Si arriva allo stesso risultato ricordando che una matrice reale d'ordine dispari deve avere almeno una autovalore reale, e dovendo essere di norma unitaria (come numero complesso) dev'essere uno tra ± 1.

3.4.4. Per ogni isometria φ esiste una base ortonormale (v_1, v_2, v_3) di $\mathbb{R}^3$ rispetto alla quale la matrice di φ assume la forma seguente: $B = \left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & B' \end{smallmatrix}\right)$, ove $B' \in \mathrm{O}_2(\mathbb{R})$.

In particolare se $\det \varphi = 1$ allora possiamo scegliere la base in modo che $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & B' \end{smallmatrix}\right)$, ove $B' \in \mathrm{SO}_2(\mathbb{R})$. e si tratta di una rotazione attorno ad un asse.

Se invece $\det \varphi = -1$ allora possiamo scegliere la base in modo che $B = \left(\begin{smallmatrix} -1 & 0 \\ 0 & B' \end{smallmatrix}\right)$, con $B' \in \mathrm{SO}_2(\mathbb{R})$ e si tratta una rotazione seguita da una riflessione di direzione l'asse di rotazione. Come si riduce il caso di $B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & B' \end{smallmatrix}\right)$, con $B' \in \mathrm{O}_2(\mathbb{R}) \smallsetminus \mathrm{SO}_2(\mathbb{R})$ (rotazione seguita da una riflessione sul piano di rotazione)?

3.4.5. Si mostri che ogni elemento di $\mathrm{O}_3(\mathbb{R})$ si può scrivere come prodotto di al più 3 elementi di periodo 2 (al più 2 se si tratta di elementi di $\mathrm{SO}_3(\mathbb{R})$?).

3.4.6. Angoli di Eulero. Fissate due basi ortonormali e_1, e_2, e_3 ed E_1, E_2, E_3 esiste un unico elemento φ di $\mathrm{SO}_3(\mathbb{R})$ tale che $\varphi e_i = E_i$ $(i = 1, 2, 3)$ e si può scrivere come composizione di al più tre rotazioni di angoli opportuni intorno a rette. Possiamo considerare i due piani $\langle e_1, e_2 \rangle$ e $\langle E_1, E_2 \rangle$. Se essi coincidono, allora φ è una rotazione attorno alla retta $\langle e_3 \rangle = \langle E_3 \rangle$ (eventualmente preceduta da una rotazione d'angolo π se $E_3 = -e_3$), altrimenti la loro intersezione determina una retta, detta retta dei nodi, di versore diciamo n. Si considerino allora le seguenti rotazioni: rotazione di asse e_3 ed angolo $\psi = \vartheta(e_1, n)$ (precessione), rotazione di asse n ed angolo $\nu = \vartheta(e_3, E_3)$ (nutazione), rotazione di asse E_3 ed angolo $\varrho = \vartheta(n, E_1)$ (rotazione propria). La composizione nell'ordine delle tre rotazioni dà φ.

Si può quindi scrivere la matrice della trasformazione φ in termini dei tre angoli di precessione ψ, di nutazione ν e di rotazione propria ϱ tramite la composizione delle tre matrici:

$$P = \begin{pmatrix} \cos\psi & -\sin\psi & 0 \\ \sin\psi & \cos\psi & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\nu & -\sin\nu \\ 0 & \sin\nu & \cos\nu \end{pmatrix} \qquad R = \begin{pmatrix} \cos\varrho & -\sin\varrho & 0 \\ \sin\varrho & \cos\varrho & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

tenendo conto delle basi in cui sono scritte, e dei cambiamenti di base corrispondenti (P in base iniziale e, N in base $e' = eP$, R in base $e'N = ePN$):

$$(PN)R(PN)^{-1}\ (PNP^{-1})\ P = PNR.$$

qual'è l'evoluzione di e_2? evoluzione del piano $\langle e_1, e_3\rangle$ ...ventaglio di Eulero

♠♠ **3.4.7.** Relazione con il corpo $\mathbb{H}$ dei Quaternioni. Ricordiamo innanzitutto che il sottocorpo dei quaternioni puramente reali, indichiamolo con $\mathbb{H}_0$, è isomorfo al corpo dei numeri reali; e osserviamo subito che il sottinsieme, diciamo $\mathbb{H}'$ dei quaternioni speciali o puramente immaginari, cioè la cui parte reale sia nulla, è uno spazio vettoriale reale di dimensione 3 (generato da i, j, k) e in cui l'operazione di prodotto corrisponde all'operazione di prodotto vettoriale tra vettori di $\mathbb{R}^3$.

Ancora più precisamente, se indichiamo con $z = (a, v)$ e $z' = (a', v')$ due quaternioni, con $a, a' \in \mathbb{R}$ e $v, v' \in \mathbb{R}^3$ (dunque $z = a + (i, j, k)v$ e $z' = a' + (i, j, k)v'$) abbiamo che $z + z' = (a + a', v + v')$, $zz' = (aa' - v \cdot v', av' + a'v + v \times v')$, da cui si vede che il corpo dei quaternioni già "contiene" le due operazioni di prodotto (scalare e vettoriale) tra vettori: infatti il prodotto di due quaternioni speciali è dato da $(0, v)(0, v') = (-v \cdot v', v \times v')$.

Consideriamo ora il sottinsieme dei quaternioni di norma unitaria, sia $\mathbb{H}^1 = \{q \in \mathbb{H} |\, \|q\| = 1\}$. Essi si scrivono unicamente tramite un angolo ϑ (compreso tra 0 e π escluso) e un vettore $u \in \mathbb{S}^2$ di norma 1 nel modo seguente: $q = (\cos(\vartheta), \sin(\vartheta)u)$. Vogliamo vedere che ogni tale quaternione rappresenta un elemento di $\mathrm{SO}_3(\mathbb{R})$, e anche determinare quando due quaternioni determinano la stessa rotazione dello spazio euclideo. Consideriamo allo scopo il prodotto, per ogni $r = (0, v)$:

$$\begin{aligned} qr\overline{q} &= (\cos(\vartheta), \sin(\vartheta)u)(0, v)(\cos(\vartheta), -\sin(\vartheta)u) = \\ &= (\cos(\vartheta), \sin(\vartheta)u)(\sin(\vartheta)v \cdot u, \cos(\vartheta)v - \sin(\vartheta)v \times u) = \\ &= (0, \cos^2(\vartheta)v + 2\sin(\vartheta)\cos(\vartheta)u \times v + \sin^2(\vartheta)(v \cdot u)u - \sin^2(\vartheta)u \times (v \times u)) \ . \end{aligned}$$

Ora, se supponiamo che v sia multiplo di u allora, poiché $u \times v = 0$ e $(v \cdot u)u = v$, otteniamo $qr\overline{q} = r$; mentre se supponiamo che v sia ortogonale a u, poiché allora $u \cdot v = 0$ e $u \times (v \times u) = v$, otteniamo $qr\overline{q} = (0, \cos(2\vartheta)v + \sin(2\vartheta)u \times v) = (0, w)$, ove w è il vettore che si ottiene ruotando v di un angolo pari a 2ϑ attorno all'asse individuato da u.

Mettendo insieme i due risultati, possiamo quindi concludere che per ogni quaternione unitario q la funzione $\varphi_q : \mathbb{H}' \to \mathbb{H}'$ che manda r in $qr\overline{q}$ è una rotazione di $\mathbb{H}'$ (visto come spazio vettoriale euclideo $\mathbb{R}^3$). Abbiamo dunque una funzione $\varphi : \mathbb{H}^1 \longrightarrow \mathrm{SO}_3(\mathbb{R})$ (che manda q in φ_q tale che $(0, \varphi_q(v)) = q(0, v)\overline{q}$) che si controlla essere un omomorfismo di gruppi per le strutture moltiplicative date: $\varphi_1 = \mathbb{I}_3$ e $\varphi_{qq'} = \varphi_q\varphi_{q'}$. Si osservi che la seconda formula per quanto facile dà conseguenze importanti, e in particolare dà un modo quasi immediato per capire che la composizione di due rotazioni è ancora una rotazione, e di determinarne angolo e asse (basta fare il prodotto dei corrispondenti quaternioni: geometricamente non evidente!).

È chiaro che l'omomorfismo φ è suriettivo, poiché ogni elemento di $\mathrm{SO}_3(\mathbb{R})$ è una rotazione attorno ad un fissato asse, e quindi si rappresenta tramite (l'applicazione associata ad) un quaternione. Resta da controllare quali quaternioni determinano la stessa rotazione, e per questo basta vedere quali quaternioni determinano la trasformazione identica: si vede facilmente che sono solo $(\pm 1, 0)$, corrispondenti a rotazioni di angoli 0 e 2π attorno a qualsiasi vettore.

Descrizione esplicita della matrice associata ad un quaternione unitario: dall'espressione prima trovata

$$\varphi_q(v) = \cos^2(\vartheta)v + 2\sin(\vartheta)\cos(\vartheta)u \times v + \sin^2(\vartheta)(v \cdot u)u - \sin^2(\vartheta)u \times (v \times u)$$

possiamo esplicitare la matrice di φ_q in una base data in cui le coordinate di u siano $\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$. In effetti abbiamo

$$\varphi_q(v) = (\cos^2(\vartheta) + 2\sin(\vartheta)\cos(\vartheta)u \times + \sin^2(\vartheta)uu^{\mathrm{t}} + \sin^2(\vartheta)u \times (u\times))v$$

da cui otteniamo che la matrice cercata è la somma

$$\cos^2(\vartheta)\mathbb{I}_2+2\sin(\vartheta)\cos(\vartheta)\begin{pmatrix}0 & -u_3 & u_2\\ u_3 & 0 & u_1\\ u_2 & -u_1 & 0\end{pmatrix}+\sin^2(\vartheta)\begin{pmatrix}u_1^2 & u_1u_2 & u_1u_3\\ u_1u_2 & u_2^2 & u_2u_3\\ u_1u_3 & u_2u_3 & u_3^2\end{pmatrix}+\sin^2(\vartheta)\begin{pmatrix}0 & -u_3 & u_2\\ u_3 & 0 & u_1\\ u_2 & -u_1 & 0\end{pmatrix}^2 .$$

Usando invece coordinate reali $q = (x_0, x_1, x_2, x_3) = (x_0, x)$ per il quaternione unitario, allora la matrice di φ_q si ottiene facilmente da calcoli diretti:

$$\begin{aligned}\varphi_q(v) &= (x\cdot v)x + x_0 v\times x + x\times(v\times x) =\\ &= \begin{pmatrix} x_0^2+x_1^2-x_2^2-x_3^2 & 2(x_1x_2-x_0x_3) & 2(x_1x_3+x_0x_2)\\ 2(x_1x_2+x_0x_3) & x_0^2-x_1^2+x_2^2-x_3^2 & 2(-x_0x_1+x_2x_3)\\ 2(x_1x_3-x_0x_2) & 2(x_0x_1+x_2x_3) & x_0^2-x_1^2-x_2^2+x_3^2\end{pmatrix}\begin{pmatrix}v_1\\ v_2\\ v_3\end{pmatrix}\\ &= \begin{pmatrix} 1-2(x_2^2+x_3^2) & 2(x_1x_2-x_0x_3) & 2(x_1x_3+x_0x_2)\\ 2(x_1x_2+x_0x_3) & 1-2(x_1^2+x_3^2) & 2(-x_0x_1+x_2x_3)\\ 2(x_1x_3-x_0x_2) & 2(x_0x_1+x_2x_3) & 1-2(x_1^2+x_2^2)\end{pmatrix}\begin{pmatrix}v_1\\ v_2\\ v_3\end{pmatrix} .\end{aligned}$$

(ricordando che $x_0^2+x_1^2+x_2^2+x_3^2 = 1$).

La decomposizione in $\mathrm{SO}_3(\mathbb{R})$ secondo gli angoli di Eulero corrisponde ad una fattorizzazione vista per i quaternioni unitari: quale? Cosa corrisponde all'altra fattorizzazione?

elica di Eulero!

♠ **3.5.** Struttura di $\mathrm{O}_n(\mathbb{R})$. Naturalmente una matrice ortogonale non è necessariamente diagonalizzabile su $\mathbb{R}$; però una strategia simile a quella che useremo per il teorema spettrale permette di dimostrare che lo è su $\mathbb{C}$, e anche di verificare il risultato seguente. In generale, data una matrice $A \in \mathrm{O}_n(\mathbb{R})$, esiste una base ortonornale di $V_n(\mathbb{R})$ tale che la matrice in quella base assume la forma

$$\begin{pmatrix}\mathbb{I}_r & 0 & 0 & \cdots & 0\\ 0 & -\mathbb{I}_s & 0 & \cdots & 0\\ 0 & 0 & \Theta_1 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & \Theta_t\end{pmatrix}$$

ove $\Theta_i \in \mathrm{SO}_2(\mathbb{R})$. La trasformazione è diretta o inversa a seconda che il blocco $-\mathbb{I}_s$ abbia ordine pari o dispari.

Si procede osservando che gli autovalori complessi sono tutti di modulo 1, e che se ϑ è un autovalore non reale, anche $\overline{\vartheta}$ lo è, con uguali molteplicità e nullità. Se poi α, β sono autovalori distinti (non necessariamente reali), e $v, w \in \mathbb{C}^n$ sono autovettori rispettivi, allora $\overline{v}^{\mathrm{t}}w = 0$ (in particolare, se sono in $V_n(\mathbb{R})$ risultano ortogonali tra loro): calcolando $(\overline{Av})^{\mathrm{t}}Aw$ si ottiene che $(1-\overline{\alpha}\beta)\overline{v}^{\mathrm{t}}w = 0$. Infine si dimostra la diagonalizzabilità (su $\mathbb{C}$) osservando che se U è sottospazio generato da autovettori, allora $U' = \{w \in \mathbb{C}^n | \overline{w}^{\mathrm{t}}u = 0\ \forall u \in U\}$ è stabile per A, e quindi contiene altri autovettori.

Il passaggio alla forma reale si ottiene "accoppiando" autovettori tra loro coniugati in senso complesso (e quindi relativi ad autovalori coniugati) per formare i blocchi di rotazioni euclidee.

♠ **3.6.** Struttura di $\mathrm{SO}_4(\mathbb{R})$ e rappresentazione tramite quaternioni. Ogni matrice di $\mathrm{SO}_4(\mathbb{R})$ è ortogonalmente simile (in $\mathbb{R}$) ad una matrice del tipo $\left(\begin{smallmatrix}\Theta_1 & \mathbb{O}_2\\ \mathbb{O}_2 & \Theta_2\end{smallmatrix}\right)$ con $\Theta_1, \Theta_2 \in \mathrm{SO}_2(\mathbb{R})$. Detti

ϑ_1, ϑ_2 gli angoli delle rotazioni Θ_1, Θ_2, consideriamo $\alpha,\ \beta$ tali che $\vartheta_1 = \alpha + \beta,\ \vartheta_2 = \alpha - \beta$. Allora, indicando con $\Theta(\alpha), \Theta(\beta)$ le matrici di rotazioni di angoli $\alpha,\ \beta$, risulta che

$$\begin{pmatrix} \Theta_1 & \mathbb{O}_2 \\ \mathbb{O}_2 & \Theta_2 \end{pmatrix} = \begin{pmatrix} \Theta(\alpha) & \mathbb{O}_2 \\ \mathbb{O}_2 & \Theta(\alpha) \end{pmatrix} \begin{pmatrix} \Theta(\beta) & \mathbb{O}_2 \\ \mathbb{O}_2 & \Theta(-\beta) \end{pmatrix} .$$

Le due matrici a destra sono dette (matrici di) rotazioni concordi di angolo α, e rotazioni discordi di angolo β: si tratta di trasformazioni ortogonali consistenti di rotazioni dello stesso angolo, o di angoli opposti, su due piani mutuamente ortogonali. Quindi *ogni trasformazione ortogonale speciale 4-dimensionale è composizione di una rotazione concorde e di una rotazione discorde.*

Questi due tipi di trasformazioni si possono ottenere facilmente a partire dai quaternioni unitari: se $s \in \mathbb{H}^1$ allora la mappa $\mathbb{H} \longrightarrow \mathbb{H}$ data da $q \mapsto sq$ è una rotazione concorde considerando $\mathbb{H} \cong \mathbb{R}^4$ con l'usuale norma quale prodotto scalare. Analogamente, se $r \in \mathbb{H}^1$ allora la mappa $\mathbb{H} \longrightarrow \mathbb{H}$ data da $q \mapsto q\overline{r}$ è una rotazione discorde. Questo si può vedere facilmente usando quaternioni unitari del tipo $(\cos\alpha, \sin\alpha, 0, 0)$ con cui si trovano proprio le matrici standard di rotazioni concordi e discordi, ma è interessante anche provare per un quaternione unitario generale (x_0, y_0, z_0, w_0) e studiare le matrici delle applicazioni lineari che si ottengono tramite moltiplicazione a sinistra/destra.

Quindi l'applicazione $\mathbb{H}^1 \times \mathbb{H}^1 \longrightarrow \mathrm{SO}_4(\mathbb{R})$ che manda (s, r) nella matrice corrispondente (base usuale) alla trasformazione $q \mapsto sq\overline{r}$ è suriettiva; analogamente a prima si vede che rispetta le moltiplicazioni nei due lati, e che il nucleo è formato da $\pm(1, 1)$.

Le fattorizzazioni di quaternioni permettono quindi di concludere che la descrizione di una trasformazione ortogonale diretta 4-dimensionale richiede 6 parametri (analogamente ai 3 angoli di Eulero per le trasformazioni ortogonali dirette 3-dimensionali).

3.7. Definizione-Teorema (Conformità). *Sia φ un automorfismo di $V_n(\mathbb{R})$; le proprietà seguenti sono equivalenti:*
(1) *φ rispetta gli angoli, i.e. $\vartheta(\varphi(v), \varphi(w)) = \vartheta(v, w)$ per ogni $v, w \in V_n(\mathbb{R})$;*
(2) *φ rispetta gli angoli retti, i.e. $\varphi(v) \perp \varphi(w)$ se e solo se $v \perp w$ per ogni $v, w \in V_n(\mathbb{R})$.*
(3) *esiste un numero reale $\alpha > 0$ tale che $\varphi(v) \cdot \varphi(w) = \alpha^2(v \cdot w)$ per ogni $v, w \in V_n(\mathbb{R})$;*
(4) *esiste un numero reale $\alpha > 0$ tale che $\|\varphi(v)\| = \alpha\,\|v\|$ per ogni $v \in V_n(\mathbb{R})$.*
Tali automorfismi si dicono conformità di $V_n(\mathbb{R})$, e il numero α si dice rapporto della conformità.

Dimostrazione. L'equivalenza dei punti (3) e (4) si ottiene ragionando similmente a quanto fatto per le isometrie. Che (1) implichi (2) è evidente. Che (2) implichi sia (3) che (4) si ottiene considerando per ogni coppia di vettori v e w la proiezione ortogonale di uno sull'altro: $(w - \alpha v) \perp v$ se e solo se (ipotesi) $(\varphi w - \alpha\varphi v) \perp \varphi v$, da cui segue $\frac{v \cdot w}{v \cdot v} = \alpha = \frac{\varphi v \cdot \varphi w}{\varphi v \cdot \varphi v}$, e dunque $\frac{\varphi v \cdot \varphi v}{v \cdot v} = \frac{\varphi v \cdot \varphi w}{v \cdot w} = \frac{\varphi w \cdot \varphi w}{w \cdot w}$ (per ogni v, w). Infine, che (3) e (4) implichino (1) segue dalla definizione di (coseno dell')angolo. □

3.7.1. Ovviamente, una conformità è una isometria se e solo se il rapporto di conformità è 1.

3.7.2. È chiaro che ogni conformità è composizione di una trasformazione scalare (pari al rapporto di conformità) con una isometria, nell'ordine preferito.

3.7.3. Osservazioni analoghe a quelle fatte per le trasformazioni ortogonali. Una applicazione insiemistica di $V_n(\mathbb{R})$ in sè che soddisfi alla proprietà...

3.7.4. Matrici conformi. Sia φ una conformità. Ogni matrice A associata usando una base di vettori ortonormali (tali che $v_i \cdot v_j = \delta_{i,j}$) è tale che $A^{\mathrm{t}}A = \alpha^2\mathbb{I}$ per qualche reale $\alpha > 0$. Tali matrici si dicono matrici conformi, e il valore α si dice parametro o rapporto di conformità. Se A è matrice conforme di parametro α, allora $\det A = \pm\alpha^n$. Se $\det A > 0$ la conformità si dice diretta; inversa altrimenti.

Le matrici conformi formano un sottogruppo di $\mathrm{GL}(n, \mathbb{R})$ contenente il gruppo ortogonale.

4. Teorema spettrale reale e sue applicazioni (valori singolari, pseudoinverse).

4.1. Applicazioni aggiunte. In questo paragrafo parleremo soprattutto in termini di matrici, ma può essere utile tener presente un quadro più generale. Se $\varphi : V_m(\Bbbk) \to V_n(\Bbbk)$ è applicazione lineare, allora definiamo una applicazione lineare che è detta aggiunte di φ rispetto al prodotto scalare (o alla base canonica) $\varphi^a : V_n(\Bbbk) \to V_m(\Bbbk)$ definita da $v \cdot \varphi^a(w) = \varphi(v) \cdot w$ per ogni $v \in V_m(\Bbbk)$ e ogni $w \in V_n(\Bbbk)$. (notare che la definizione è implicita e si basa sulla non-degenerazione del prodotto scalare in $V_m(\Bbbk)$: vogliamo definire $\varphi^a(w)$ e diciamo qual è la sua forma contro ogni $v \in V_m(\Bbbk)$).

È facile notare che se A è la matrice in basi canoniche di φ, allora la matrice in basi canoniche di φ^a è A^{t}.

È anche facile capire che, usando le basi canoniche (ovvero il prodotto scalare) per identificare $V_m(\Bbbk)^*$ con $V_m(\Bbbk)$ (e $V_n(\Bbbk)^*$ con $V_n(\Bbbk)$), allora la funzione aggiunta corrisponde alla funzione duale.

La relazione di φ con φ^a identifica vari tipi interessanti di applicazioni lineari:
(1) se $\varphi^a = \varphi$ si dice autoaggiunta (vale $v \cdot \varphi(w) = \varphi(v) \cdot w$ per ogni v, w),
(2) se $\varphi^a = -\varphi$ si dice antiaggiunta (vale $v \cdot \varphi(w) = -\varphi(v) \cdot w$ per ogni v, w),
(3) le isometrie ($\varphi(v) \cdot \varphi(w) = v \cdot w$ per ogni v, w) si riconoscono dalla condizione $\varphi^a = \varphi^{-1}$;
(4) si dicono normali le funzioni tali che $\varphi^a \circ \varphi = \varphi \circ \varphi^a$ (commutano con la loro aggiunta, ovvero $\varphi^a(v) \cdot \varphi^a(w) = \varphi(v) \cdot \varphi(w)$ per ogni v, w).

4.2. Teorema (Spettrale reale (versione matriciale)). *Le matrici reali simmetriche sono ortogonalmente diagonalizzabili, cioè se $A \in M_n(\mathbb{R})$ e $A^{\mathrm{t}} = A$ (simmetrica) allora esiste una matrice ortogonale $P \in \mathrm{O}_n(\mathbb{R})$ tale che $P^{-1}AP = P^{\mathrm{t}}AP$ è matrice diagonale (reale).*

Dimostrazione. Si procede in tre passi:
(1) dimostriamo che tutti gli autovalori di A sono reali: certamente troviamo tutti gli autovalori in $\mathbb{C}$, e sia $\alpha \in \mathbb{C}$ un autovalore con autovettore v; allora dalle uguaglianze

$$\overline{\alpha}(\overline{v}^{\mathrm{t}}v) = (A\overline{v})^{\mathrm{t}}v = \overline{v}^{\mathrm{t}}Av = \overline{v}^{\mathrm{t}}\alpha v = \alpha(\overline{v}^{\mathrm{t}}v)$$

(la seconda uguaglianza è quella fondamentale e usa la simmetria di A, le altre usano il fatto che A è matrice reale: se v è autovettore per α allora $\overline{v}$ è autovettore per $\overline{\alpha}$) e si deduce che $\alpha = \overline{\alpha}$ poiché $\overline{v}^{\mathrm{t}}v \neq 0$. Dunque $\alpha \in \mathbb{R}$.
(2) dimostriamo che gli autospazi sono tra loro ortogonali: se v, w sono autovettori per A relativi agli autovalori α, β diversi tra loro, allora dalle uguaglianze

$$\beta(w^{\mathrm{t}}v) = (Aw)^{\mathrm{t}}v = w^{\mathrm{t}}Av = w^{\mathrm{t}}\alpha v = \alpha(w^{\mathrm{t}}v)$$

(nella seconda uguaglianza si usa la simmetria di A) deduciamo che $(\alpha-\beta)w^{\mathrm{t}}v = 0$ e siccome $\alpha-\beta \neq 0$ otteniamo $w^{\mathrm{t}}v = 0$, cioè che autovettori relativi ad autovalori distinti sono tra loro ortogonale, come si voleva.
(3) dimostriamo ora che esiste una base di autovettori: sia $v_1, \dots, v_r$ un insieme linearmente indipendente massimale di autovettori per A; allora lo spazio $U = \langle v_1, \dots, v_r \rangle$ è stabile per A, ma anche $U^\perp$ lo è, poiché se $v \in V_n(\mathbb{R})$ è ortogonale ai v_i, anche Av lo è, essendo

$$(Av) \cdot v_i = (Av)^{\mathrm{t}}v_i = v^{\mathrm{t}}Av_i = \alpha_i v^{\mathrm{t}}v_i = 0 \ .$$

Ora, se fosse $U^\perp \neq 0$ troveremmo almeno una altro autovalore e un autovettore relativo, indipendente dai precedenti, il che è assurdo per la massimalità ipotizzata. Dunque $U = V_n(\mathbb{R})$ e abbiamo trovato una base di autovettori. □

4.2.1. Si osservi che il teorema si può enunciare come una equivalenza: *una matrice quadrata reale è simmetrica se e solo se è ortogonalmente diagonalizzabile* (il teorema spettrale dà l'implicazione difficile, l'altra è quasi ovvia: farla esplicitamente).

4.2.2. Nella dimostrazione del teorema spettrale è nascosta la seguente osservazione: se A è simmetrica reale, allora $\ker A$ e $\operatorname{im} A$ sono in somma diretta ortogonale: $\mathbb{R}^n = \ker A \boxplus \operatorname{im} A$, ovvero $\operatorname{im} A = (\ker A)^\perp$. Dimostrare direttamente questo fatto.

4.2.3. Qual è la relazione delle matrici simmetriche con il prodotto scalare? Si noti che $A = A^{\mathrm{t}}$ è eqivalente al fatto che per ogni coppia di vettori $v, w \in V_n(\mathbb{R})$ si abbia $(Av) \cdot w = v \cdot (Aw)$. Infatti in generale vale che $(Av) \cdot w = v \cdot (A^{\mathrm{t}}w)$.

4.2.4. Problema. Per capire bene le relazioni tra matrici ortogonali e matrici (reali) simmetriche, si osservi che: vi sono matrici ortogonali non simmetriche, vi sono matrici simmetriche non ortogonali (farsi degli esempi), e infine che *una matrice reale è ortogonale e simmetrica (ovvero ortogonale e ortogonalmente diagonalizzabile) se e solo se è la matrice di una simmetria ortogonale (cioè di una simmetria in cui asse e direzione sono tra loro ortogonali).*

4.3. Problema: teorema di Schur reale. *Una matrice reale è ortogonalmente triangolarizzabile se e solo se ha spettro reale (cioè ha tutti gli autovalori in $\mathbb{R}$).*

Si noti quindi che una matrice reale è triangolarizzabile se e solo se lo è ortogonalmente. Si può vedere sia ripetendo la dimostrazione di triangolarizzabilità (e quando si scelgono complementari, scegliere l'ortogonale...), sia ortonormalizzando (alla Gram-Schmidt) una base triangolarizzante.

Da questo, e con il fatto che le matrici simmetriche hanno spettro reale, si deduce quasi immediatamente il teorema spettrale.

4.4. Problema. È decisamente più difficile, invece, capire quando una matrice è ortogonalmente jordanizzabile: le condizioni ovvie (spettro reale e ortogonalità degli autospazi generalizzati relativi ad autovalori distinti) sono certamente necessarie, ma non sufficienti. Il problema si riduce a: quando una matrice nilpotente (oppure, con un unico autovalore) è ortogonalmente jordanizzabile?

♠♠ **4.5.** Equivalenza ortogonale (valori singolari). Consideriamo ora due matrici $A, B \in M_{n,m}(\mathbb{R})$ non necessariamente quadrate; diciamo che esse sono ortogonalmente equivalenti se esistono $P \in \mathrm{O}_n(\mathbb{R})$ e $Q \in \mathrm{O}_m(\mathbb{R})$ tali che $PAQ = B$. Si tratta di una relazione più sottile della equivalenza di matrici che abbiamo già trattata.

4.5.1. Classificazione per equivalenza ortogonale. *Ogni matrice $A \in M_{n,m}(\mathbb{R})$ è ortogonalmente equivalente ad una matrice pseudodiagonale del tipo*

$$\begin{pmatrix} \Sigma & \mathbb{O}_{r,n-r} \\ \mathbb{O}_{m-r,r} & \mathbb{O}_{m-r,n-r} \end{pmatrix}$$

dove r è il rango di A, $\Sigma \in M_r(\mathbb{R})$ è matrice diagonale con valori diagonali positivi $s_1 \leqslant s_2 \leqslant \cdots \leqslant s_r$ detti i valori singolari di A. I valori singolari s_i sono caratterizzati dal fatto di essere reali positivi e che s_i^2 sono gli autovalori non nulli delle matrici $A^{\mathrm{t}}A$ e AA^{t}; quindi la forma pseudodiagonale è univocamente determinata da A. In particolare il rango e i valori singolari (sequenza non decrescente di $\mathrm{rg}A$ *reali positivi) classificano le matrici per equivalenza ortogonale.*

Poiché $A^{\mathrm{t}}A$ è una matrice simmetrica, possiamo ortogonalmente diagonalizzarla e scrivere $A^{\mathrm{t}}A = P\Sigma^2P^{\mathrm{t}}$ dove Σ^2 ha in diagonale gli autovalori di $A^{\mathrm{t}}A$ che sono non negativi (se $A^{\mathrm{t}}Av = \alpha v$, basta premoltiplicare per v^{t} per ottenere che $\alpha \geqslant 0$) e possiamo pensare ordinati come nell'enunciato. Detti v_i i vettori della base spettrale (sono le colonne di P), abbiamo $A^{\mathrm{t}}Av_i = s_i^2 v_i$ e $v_i \cdot v_j = \delta_{ij}$.

Poniamo $u_i = Av_i$ per $i = 1, \ldots, r$ (gli altri hanno immagini nulle). Si vede subito che $A^{\mathrm{t}}u_i = A^{\mathrm{t}}Av_i = s_i^2 v_i$. Inoltre $u_i \cdot u_j = Av_i \cdot Av_j = v_i \cdot A^{\mathrm{t}}Av_j = s_i^2\delta_{ij}$, e quindi sono ortogonali tra loro. Scegliamo allora una matrice ortogonale Q usando come prime colonne i vettori u_i/s_i, e completando poi ad una base ortonormale del codominio. Quindi abbiamo $AP = Q\Sigma$.

Ora è facile vedere che $Q^{\mathrm{t}}AP$ dà la matrice pseudodiagonale richiesta. □

4.5.2. Caso di matrici quadrate. Si noti che anche se la matrice A è quadrata, in generale i valori singolari non sono in relazione con gli eventuali autovalori della matrice stessa. Solo nel caso di matrici simmetriche c'è una evidente relazione: i valori singolari coincidono con i valori assoluti degli autovalori.

Quale esempio, si considerino le matrici nilpotenti standard, e le matrici standard di Jordan di autovalore 1.

4.5.3. Decomposizione reale polare. È facile, per matrici quadrate, dedurre dal teorema di classificazione per equivalenza ortogonale (e dal teorema spettrale) la cosiddetta decomposizione polare: *ogni matrice reale quadrata $A \in M_n(\mathbb{R})$ si scrive come prodotto $A = SP$ con S matrice simmetrica con autovalori non negativi e P matrice ortogonale; inoltre tale scrittura è unica se A è invertibile. Naturalmente è possibile la scrittura $A = P'S'$ con le stesse condizioni (risulta $S = S'$ se e solo se A è simmetrica?).*

Basta infatti usare $A = Q\Sigma P = (Q\Sigma Q^{\mathrm{t}})(QP)$.

È anche interessante osservare che la decomposizione polare si può trovare usando le stesse tecniche usate nella classificazione per equivalenza ortogonale; inoltre l'esistenza della decomposizione polare permette di ritrovare la classificazione per equivalenza ortogonale.

4.5.4. Curiosità. Ogni endomorfismo di $\mathbb{R}^n$ si decompone come una rigidità seguita da dilatazioni (diverse da asse ad asse) su assi ortogonali tra loro (quasi immediato dalla decomposizione polare).

4.5.5. Usando la decomposizione polare, e osservando che per matrici reali normali (cioè che commutano con la loro trasposta) abbiamo che A è polinomiale in A^{t} (e viceversa), otteniamo il seguente risultato: *due matrici reali normali sono simili se e solo se sono ortogonalmente simili.*

Infatti, se A, B sono simili, abbiamo $B = T^{-1}AT$ con $T \in \mathrm{GL}_n(\mathbb{R})$, e anche $A^{\mathrm{t}} = q(A)$, $B^{\mathrm{t}} = q(B)$ con $q(X)$ polinomio (stesso per entrambe perché dipende solo dagli autovalori, eventualmente complessi, delle due matrici). Da questo si ricava

$$T^{\mathrm{t}}A^{\mathrm{t}}T^{-\mathrm{t}} = B^{\mathrm{t}} = q(B) = q(T^{-1}AT) = T^{-1}q(A)T = T^{-1}A^{\mathrm{t}}T$$

da cui segue che $TT^{\mathrm{t}}A^{\mathrm{t}} = A^{\mathrm{t}}TT^{\mathrm{t}}$ e quindi TT^{t} commuta con A (oltre che con A^{t}). Ora, usando la decomposizione polare di T come SQ con S simmetrica e polinomiale in TT^{t} e Q ortogonale, abbiamo che S commuta con A e quindi $B = T^{-1}AT = (SQ)^{-1}A(SQ) = Q^{-1}S^{-1}ASQ = Q^{-1}AQ$ come si voleva.

♠♠ **4.6.** Pseudoinverse di Moore-Penrose. Esiste una interessante e classica generalizzazione del calcolo delle matrici inverse al caso di matrici rettangolari qualsiasi (e quindi anche per matrici quadrate non invertibili!).

4.6.1. Il problema si presenta geometricamente in questa forma: *data una applicazione lineare $\varphi : V_n(\mathbb{R}) \to V_m(\mathbb{R})$, trovare una applicazione lineare in senso inverso $\psi : V_m(\mathbb{R}) \to V_n(\mathbb{R})$ (che sia di rango minimo e) tale che $\varphi \circ \psi = p^{\perp}_{\operatorname{im}\varphi}$ (proiezione ortogonale sull'immagine di φ) e $\varphi^* \circ \psi^* = p^{\perp}_{\operatorname{im}\varphi^*}$ (proiezione ortogonale sull'immagine di φ^*, pensando lo spazio duale dotato del prodotto scalare nella base duale canonica). La seconda condizione è equivalente a chiedere che $\psi \circ \varphi = p^{\perp}_{(\ker\varphi)^{\perp}}$ (proiezione ortogonale sull'ortogonale del nucleo di φ).*

È chiaro che, se φ è invertibile, l'inversa risponde al problema. È anche ovvio osservare che se φ è una proiezione ortogonale, allora lei stessa risolve il problema.

In generale, decomponendo $V_n(\mathbb{R}) = (\ker\varphi)^{\perp} \boxplus \ker\varphi$ e $V_m(\mathbb{R}) = \operatorname{im}\varphi \boxplus (\operatorname{im}\varphi)^{\perp}$, abbiamo che φ induce un isomorfismo $\tilde{\varphi} : (\ker\varphi)^{\perp} \to \operatorname{im}\varphi$, e quindi le condizioni poste impongono che ψ sia definita come l'inversa di $\tilde{\varphi}$ su $\operatorname{im}\varphi$, e 0 sull'ortogonale (per rendere minimale il rango).

4.6.2. Quindi, data una matrice $A \in M_{n,m}(\mathbb{R})$ diciamo che $A^+ \in M_{m,n}(\mathbb{R})$ è pseudoinversa di Moore-Penrose di A se è l'unica matrice (di rango minimo, necessariamente uguale al rango di A) tale che AA^+ è matrice della proiezione ortogonale sull'immagine di A, e A^+A è matrice della proiezione ortogonale sull'ortogonale del nucleo di A.

Le tre condizioni date sono equivalenti alle seguenti quattro classiche condizioni per definire la pseudoinversa di Moore-Penrose: $AA^+A = A$, $A^+AA^+ = A^+$, AA^+ e A^+A sono matrici simmetriche.

Si osservi comunque che di solito $(AB)^+ \neq B^+A^+$.

4.6.3. Calcolo di pseudoinverse tramite decomposizioni di rango massimo. Se $C \in M_{r,m}$ è di rango r, si vede subito che $C^+ = C^{\mathrm{t}}(CC^{\mathrm{t}})^{-1}$ è la pseudoinversa; analogamente se $B \in M_{n,r}$ è di rango r, si vede subito che $B^+ = (B^{\mathrm{t}}B)^{-1}B^{\mathrm{t}}$ è la pseudoinversa.

In generale, se $A \in M_{n,m}$ è di rango r, allora (e solo allora) si scrive $A = BC$ con $B \in M_{n,r}$ e $C \in M_{r,m}$. Risulta allora facile verificare che $A^+ = C^+B^+$, cioè $A^+ = C^{\mathrm{t}}(CC^{\mathrm{t}})^{-1}(B^{\mathrm{t}}B)^{-1}B^{\mathrm{t}}$.

4.6.4. Calcolo di pseudoinverse tramite decomposizioni singolari. Se invece abbiamo di A una scrittura in termini di valori singolari tramite equivalenza ortogonale, sia $A = P\Sigma Q$ con P e Q ortogonali, allora si vede quasi immediatamente che la matrice $A^+ = Q^+\Sigma^+P^+ = Q^{-1}\Sigma^+P^{-1} = Q^{\mathrm{t}}\Sigma^+P^{\mathrm{t}}$ soddisfa alle condizioni richieste, dove Σ^+ è la matrice pseudodiagonale avente gli inversi dei valori singolari di A nei posti diagonali non nulli.

4.6.5. Altre proprietà. Abbiamo $A^{++} = A$, $A^+ = A^{\mathrm{t}}$ se e solo se A è ortogonale; se U, V sono ortogonali allora $(UAV)^+ = V^+A^+U^+ = V^{\mathrm{t}}A^+U^{\mathrm{t}}$ (falso in generale per matrici solo invertibili).

4.6.6. Applicazioni delle pseudoinverse. Vi sono varie applicazioni della nozione di matrice pseudoinversa; vediamone un paio.

(0) Soluzioni ai minimi quadrati. Se $AX = b$ è sistema lineare reale (incompatibile) allora $AX - b$ ha modulo minimo se e solo se $AX = AA^+b$ (e questo vale se e solo se $A^tAX = A^tb$, condizione già nota), e il valore minimo del modulo di X si ha per $x_0 = A^+b$.
(1) Equazioni matriciali. Date A, B, C opportune matrici reali, il problema $AXB = C$ ha soluzione se e solo se $AA^+CB^+B = C$, e in tal caso le soluzioni sono della forma $X = A^+CB^+ + Y - A^+AYBB^+$ con Y arbitraria. Si osservi comunque che questo problema ha anche una bella interpretazione in termini di applicazioni lineari che ne rende la soluzione più facile di così...
(2) Problemi di regressione.

5. Spazi Vettoriali Euclidei Complessi o Spazi Vettoriali Hermitiani.

5.1. Si può pensare di estendere al caso di spazi vettoriali complessi tutte le strutture (prodotto scalare, norme, angoli, prodotto vettore,...) che abbiamo definito nel primo paragrafo. Un modo ovvio, e utile in certi contesti, ma che porta a spazi molto diversi dagli "usuali" è di definire il prodotto scalare nello stesso modo che per spazi reali: se $v, w \in V_n(\mathbb{C})$ allora $v \cdot w := v^tw = \sum_{j=1}^n z_jz'_j$ se $v = (z_j)^t$ e $w = (z'_j)^t$. Tuttavia questo comporta alcune conseguenze che allontanano dall'intuizione geometrica:

5.1.1. si trovano vettori non nulli "ortogonali a sé stessi": per esempio il vettore $v = \binom{1}{i} \in V_2(\mathbb{C})$ ha la proprietà che $v \cdot v = 1^2 + i^2 = 0$;

5.1.2. si trovano vettori ortogonali tra loro, ma linearmente dipendenti: per esempio i vettori $\binom{1}{i}, \binom{i}{-1} = i\binom{1}{i} \in V_2(\mathbb{C})$;

5.1.3. si trovano vettori il cui prodotto con sé stessi non è un numero reale, e quindi diventa impossibile parlare di positività e difficile parlare di norme: per esempio il vettore $v = \binom{1}{1+i} \in V_2(\mathbb{C})$ ha la proprietà che $v \cdot v = 1^2 + (1+i)^2 = 1 + 2i$.

Quindi questa è una estensione a $V_n(\mathbb{C})$ del prodotto scalare di $V_n(\mathbb{R})$ che fuori dallo "scheletro reale" (in cui le parti immaginarie sono tutte nulle) si comporta in modo bizzarro (ma è comunque utile). Tuttavia un'altra estensione si rivela essere molto più vicina all'intuizione, e risulta estremamente utile.

5.2. Definizione-Teorema (Prodotto Hermitiano). *Sia $V_n(\mathbb{C})$ lo spazio vettoriale standard su $\mathbb{C}$ di dimensione n. Definiamo il prodotto hermitiano di due vettori $v = (z_j)^t$ e $w = (z'_j)^t$ come $v \cdot w := v^t\overline{w} = \sum_j z_j\overline{z'_j}$, ove si sono usate le coordinate nella base canonica.*

Il prodotto hermitiano dà una funzione $V_n(\mathbb{C}) \times V_n(\mathbb{C}) \longrightarrow \mathbb{C}$ che gode delle seguenti proprietà:
$(PH1)$ *hermitianità o emisimmetria: $v \cdot w = \overline{w \cdot v}$ (per ogni $v, w \in V_n(\mathbb{C})$);*
$(PH2)$ *linearità sinistra: $(\alpha_1v_1+\alpha_2v_2)\cdot w = \alpha_1(v_1\cdot w)+\alpha_2(v_2\cdot w)$ e emilinearità destra: $v\cdot(\alpha_1w_1+\alpha_2w_2) = \overline{\alpha_1}(v \cdot w_1) + \overline{\alpha_2}(v \cdot w_2)$ (per ogni $v, v_1, v_2, w, w_1, w_2 \in V_n(\mathbb{C})$, ed ogni $\alpha_1, \alpha_2 \in \mathbb{C}$);*
$(PH3)$ *positività: $v \cdot v \geqslant 0$ (per ogni $v \in V_n(\mathbb{C})$); $v \cdot v = 0$ se e solo se $v = 0$.*
$(PH4)$ *non degenerazione: $v \cdot w = 0$ per ogni $w \in V_n(\mathbb{C})$ (risp. $v \in V_n(\mathbb{C})$) se e solo se $v = 0$ (risp. $w = 0$).*

Lo spazio vettoriale $V_n(\mathbb{C})$ dotato del prodotto hermitiano si dice lo spazio euclideo (complesso) standard di dimensione n o spazio Hermitiano standard di dimensione n.

Si possono allora ripetere molti risultati e definizioni della geometria usuale:

5.3. Definizione (norma). *La norma di un vettore $v \in V_n(\mathbb{C})$ è definita come*

$$\|v\| := \sqrt{v \cdot v}$$

(si usa la positività). Un vettore di norma 1 si dice un versore.

5.4. Teorema (disuguaglianza di Cauchy-Schwarz). *Per ogni $v, w \in V_n(\mathbb{C})$ vale che*

$$|v \cdot w|^2 \leqslant (v \cdot v)(w \cdot w)$$

(si noti che $v \cdot w \in \mathbb{C}$, e usiamo la norma in senso complesso) e dunque

$$|v \cdot w| \leqslant \|v\| \, \|w\| \, .$$

Inoltre vale l'uguaglianza se e solo se v e w sono linearmente dipendenti.

Dimostrazione. Conviene imporre la condizione $u \cdot u \geqslant 0$ ove $u = xv - yw$ e $x = w \cdot w$, $y = v \cdot w$. □

5.5. Teorema (proprietà della norma).
($N1$) $\|v\| = 0$ *se e solo se* $v = 0$;
($N2$) $\|\alpha v\| = |\alpha|\,\|v\|$;
($N3$) $\|v + w\| \leqslant \|v\| + \|w\|$ *(disuguaglianza triangolare);*
($N4$) $\|v \pm w\|^2 = \|v\|^2 \pm 2\Re(v \cdot w) + \|w\|^2$ *(versione complessa del teorema di Carnot);*
($N5$) $\|v + w\|^2 + \|v - w\|^2 = 2\left(\|v\|^2 + \|w\|^2\right)$.

5.6. Definizione (ortogonalità). *Due vettori* $v, w \in V_n(\mathbb{C})$ *si dicono ortogonali e si scrive* $v \perp w$ *se vale* $v \cdot w = 0$ *(il loro prodotto hermitiano è zero).*

5.7. Teorema (Pitagora). *Abbiamo che* $\Re(v \cdot w) = 0$ *(*$v \cdot w$ *è puramente immaginario) se e solo se* $\|v + w\|^2 = \|v\|^2 + \|w\|^2$. *In generale, vedi* ($N4$) *del teorema precedente.*

5.8. Definizione (proiezione ortogonale). *Proiezione ortogonale di un vettore* v *nella direzione di* w:

$$p_w(v) = \frac{v \cdot w}{\|w\|^2} w = \frac{v \cdot w}{w \cdot w} w \ .$$

Risulta che $p_w(v) \perp (v - p_w(v))$.

5.9. Basi ortogonali e ortonormali. Una base di $V_n(\mathbb{C})$ si dice ortogonale se essa è formata di vettori a due a due ortogonali; si dice ortonormale se inoltre i sui vettori hanno tutti norma 1. Se $(v_1, \dots, v_n)$ è una base ortonormale di $V_n(\mathbb{C})$, allora le coordinate di un vettore $v \in V_n(\mathbb{C})$ in quella base sono date da $\begin{pmatrix} v \cdot v_1 \\ \vdots \\ v \cdot v_n \end{pmatrix}$.

Usando la nozione di proiezione ortogonale è sempre possibile, come nel caso euclideo reale, trovare una base ortonormale a partire da un insieme qualsiasi di generatori, tramite il procedimento di Gram-Schmidt.

5.9.1. Formula di Parseval. Se $v_1, \dots, v_n$ è una base ortonormale di $V_n(\mathbb{C})$, allora le coordinate di $v \in V_n(\mathbb{C})$ in questa base ($v = \sum_i x_i v_i$) sono date da $x_i = v \cdot v_i = \overline{v_i \cdot v}$.

Se poi $v, w \in V_n(\mathbb{C})$ allora il prodotto hermitiano si calcola con la formula di Parseval: $v \cdot w = \sum_i (v \cdot v_i)(\overline{w \cdot v_i}) = \sum_i (v \cdot v_i)(v_i \cdot w)$.

5.10. Definizione-Teorema (ortogonali di sottospazi). *Per* S *sottinsieme di* $V_n(\mathbb{C})$ *definiamo l'ortogonale* $S^\perp = \{v \in V_n(\mathbb{C}) \mid v \perp s \ (\forall s \in S)\}$, *che risulta un sottospazio vettoriale. Valgono esattamente le stesse proprietà* (Oi) *per* $i = 0, 1, 2, 3, 4$ *che per l'analoga nozione reale:*
($O0$) $\{0\}^\perp = V_n(\mathbb{C})$, $V_n(\mathbb{C})^\perp = 0$,
($O1$) *Se* $S \subseteq T$ *allora* $T^\perp \subseteq S^\perp$;
($O2$) $\langle S \rangle = (S^\perp)^\perp$; *dunque per* W *sottospazio:* $(W^\perp)^\perp = W$. *Inoltre* $((S^\perp)^\perp)^\perp = S^\perp$.
($O3$) *Se* W *e* W' *sono sottospazi vettoriali di* $V_n(\mathbb{C})$: $(W + W')^\perp = W^\perp \cap W'^\perp$
($O4$) *Se* W *e* W' *sono sottospazi vettoriali di* $V_n(\mathbb{C})$: $(W \cap W')^\perp = W^\perp + W'^\perp$.

5.11. Prodotto vettore. Nello spazio Hermitiano ha ancora senso definire il prodotto vettore come abbiamo fatto per lo spazio vettoriale Euclideo Reale, e possiede ugualmente le proprietà (Ci) per $i = 1, 2, 4, 5$. Tuttavia la proprietà fondamentale ($C3$) diventa ora: il prodotto vettore è ortogonale ai coniugati di ciascuno dei suoi fattori, ovvero $\overline{v_i} \cdot \mathrm{cross}(v_1, \dots, v_{n-1}) = 0$. Per il teorema di Lagrange?

5.12. Equazioni di sottospazi. Si osservi che l'interpretazione hermitiana (o euclidea complessa) delle equazioni di sottospazi diventa ora la seguente: i coefficienti di ogni equazione formano un vettore il cui coniugato è ortogonale al sottospazio stesso. In particolare, in $V_3(\mathbb{C})$, il sottospazio generato da due vettori indipendenti v e w ha come coefficienti dell'equazione le componenti del prodotto vettore $v \times w$ (proprietà affine o vettoriale), ma come vettore ortogonale il coniugato $\overline{v \times w}$ (proprietà metrica, o hermitiana, o euclidea complessa).

5.13. Definizione-Teorema (trasformazioni unitarie o isometrie complesse). *Sia* φ *un automorfismo di* $V_n(\mathbb{C})$ *in sè; le proprietà seguenti sono equivalenti:*
(1) φ *rispetta la struttura hermitiana, i.e.* $\varphi(v) \cdot \varphi(w) = v \cdot w$ *per ogni* $v, w \in V_n(\mathbb{C})$;
(2) φ *rispetta la norma dei vettori, i.e.* $\|\varphi(v)\| = \|v\|$ *per ogni* $v \in V_n(\mathbb{C})$;

(3) *φ manda basi ortonormali (basta per una) in basi ortonormali.*
Tali automorfismi si dicono trasformazioni hermitiane o isometrie complesse di $V_n(\mathbb{C})$.

Per vedere che (2) implica (1) conviene applicare (2) ai vettori $v+w$ (e si ottiene $\Re(\varphi(v)\cdot\varphi(w)) = \Re(v\cdot w)$) e $iv+iw$ (e si ottiene $\Im(\varphi(v)\cdot\varphi(w)) = \Im(v\cdot w)$)

5.13.1. Da controllare. Una applicazione insiemistica di $V_n(\mathbb{C})$ in sè che soddisfi alla proprietà (1) è necessariamente un morfismo lineare; infatti si tratta di verificare che $\varphi(v+\alpha w) - \varphi(v) - \alpha\varphi(w) = 0$, ovvero che il suo prodotto hermitiano con sé stesso è nullo.

D'altra parte un morfismo lineare che rispetti la proprietà (2) è necessariamente biiettivo, e dunque un automorfismo. Infatti da $\varphi v = 0$ segue $\|v\| = \|\varphi v\| = 0$, e dunque $v = 0$.

Quindi il teorema poteva essere enunciato così: *una applicazione insiemistica di $V_n(\mathbb{C})$ in sè rispetta il prodotto hermitiano se e solo se è una applicazione lineare che rispetta la norma; e in tal caso si tratta di una applicazione biiettiva, dunque di un automorfismo.*

5.14. Teorema (Gruppo Unitario). *Sia φ una trasformazione hermitiana. Ogni matrice A associata a φ usando una base di vettori ortonormali (tali che $v_i\cdot v_j = \delta_{i,j}$) risulta una matrice unitaria, i.e. tale che $A^{\mathrm{t}}\overline{A} = \mathbb{I}$ (cioè $\overline{A}^{\mathrm{t}}A = \mathbb{I}$), ovvero $A^{-1} = \overline{A}^{\mathrm{t}}$. Le matrici unitarie formano un sottogruppo (non normale, se $n>1$) di $\mathrm{GL}(n,\mathbb{C})$ che si indica con $\mathrm{U}(n,\mathbb{C})$ o $\mathrm{U}_n(\mathbb{C})$ e si dice il Gruppo Unitario. Se $A\in\mathrm{U}_n(\mathbb{C})$, allora $|\det A| = 1$ ($\det A$ è numero complesso di modulo 1).*

5.14.1. Gruppo Unitario Speciale. Il sottinsieme di $\mathrm{U}_n(\mathbb{C})$ formato dalle matrici di determinante 1 si indica con $\mathrm{SU}(n,\mathbb{C})$ o $\mathrm{SU}_n(\mathbb{C})$ e si dice il gruppo unitario speciale. Si tratta di un sottogruppo normale di $\mathrm{U}_n(\mathbb{C})$, e il quoziente $\mathrm{U}_n(\mathbb{C})/\mathrm{SU}_n(\mathbb{C})$ è isomorfo a $\mathbb{S}^1$ (gruppo moltiplicativo dei complessi di modulo 1).

5.14.2. Si osservi che l'intersezione di $\mathrm{U}_n(\mathbb{C})$ e $\mathrm{SU}_n(\mathbb{C})$ con $\mathrm{GL}_n(\mathbb{R})$ danno rispettivamente $\mathrm{O}_n(\mathbb{R})$ e $\mathrm{SO}_n(\mathbb{R})$

5.14.3. Descrizione esplicita di $\mathrm{U}_2(\mathbb{C})$ e $\mathrm{SU}_2(\mathbb{C})$. Le matrici in $\mathrm{U}_2(\mathbb{C})$ sono tutte e sole le matrici complesse della forma

$$\begin{pmatrix} \alpha & \beta \\ -\varrho\overline{\beta} & \varrho\overline{\alpha} \end{pmatrix} \quad \text{con} \quad |\alpha|^2+|\beta|^2 = 1 \quad \text{e} \quad |\varrho| = 1,$$

mentre le matrici in $\mathrm{SU}_2(\mathbb{C})$ sono tutte e sole le matrici complesse della forma

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \quad \text{con} \quad |\alpha|^2+|\beta|^2 = 1;$$

entrambi i risultati si vedono facilmente esplicitando la condizione $\overline{A}A^{\mathrm{t}} = \mathbb{I}$, e che $\det A = 1$ nel caso speciale. Scrivendo $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ si trova subito $\overline{\alpha}/\overline{\beta} = -\delta/\gamma$ da cui $\delta = \varrho\overline{\alpha}$ e $\gamma = -\varrho\overline{\beta}$; poi dalle condizioni $\alpha\overline{\alpha}+\beta\overline{\beta} = 1 = \gamma\overline{\gamma}+\delta\overline{\delta}$ si deduce che $\varrho\overline{\varrho} = 1$.

♠♠ **5.14.4.** Relazioni tra $\mathrm{SU}_2(\mathbb{C})$ e $\mathrm{SO}_3(\mathbb{R})$. Per $\mathrm{SU}_2(\mathbb{C})$ possiamo ottenere una descrizione più suggestiva usando le componenti reali: se $\alpha = x_0+ix_1$ e $\beta = x_2+ix_3$ otteniamo

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} = x_0\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x_1\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + x_2\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + x_3\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = x_0\mathbb{I}_2 + x_1I + x_2J + x_3K\ .$$

Si osserva subito che lo spazio vettoriale reale di dimensione 4 generato da $\mathbb{I}_2, I, J, K$ in $\mathrm{GL}_2(\mathbb{C})$ ha (considerando il prodotto tra matrici) struttura di corpo isomorfo a quello dei quaternioni; infatti $I^2 = J^2 = K^2 = -\mathbb{I}_2$, $IJ = K = -JI$, $JK = I = -KJ$, $KI = J = -IK$; il quadrato della norma dei quaternioni corrisponde al determinante delle matrici, quindi i quaternioni unitari corrispondono alle matrici unitarie speciali. Di conseguenza possiamo dire che: $\mathrm{SU}_2(\mathbb{C})$ sta a $\mathbb{H}^1$ (sfera tridimensionale in $\mathbb{R}^4$) come $SO_2(\mathbb{R})$ sta a $\mathbb{S}^1$ (sfera unidimensionale in $\mathbb{R}^2$).

Da quanto abbiamo allora visto nella descrizione di $\mathrm{SO}_3(\mathbb{R})$, possiamo concludere che esiste un omomorfismo canonico di gruppi $\mathrm{SU}_2(\mathbb{C})\to\mathrm{SO}_3(\mathbb{R})$, che manda la matrice sopra scritta nella matrice corrispondente al quaternione unitario (x_0,x_1,x_2,x_3). Questo morfismo è suriettivo, e ogni trasformazione euclidea tridimensionale viene determinata da due trasformazioni unitarie speciali (una e l'opposta). Quindi possiamo concludere che dare un elemento di $\mathrm{SU}_2(\mathbb{C})$ consiste nel dare un elemento di $\mathrm{SO}_3(\mathbb{R})$ con un segno ±1; per questo $\mathrm{SU}_2(\mathbb{C})$ viene spesso chiamato il gruppo degli spin.

Descrizione diretta della rotazione associata ad un elemento di $\mathrm{SU}_2(\mathbb{C})$: senza passare attraverso il calcolo fatto con i quaternioni, possiamo procedere nel modo seguente. Ogni elemento A di $\mathrm{SU}_2(\mathbb{C})$ determina una isometria φ_A dello spazio vettoriale euclideo reale $\langle I, J, K\rangle_{\mathbb{R}}$, di cui I, J, K formano una base ortonormale (la norma essendo data dal determinante delle matrici), tramite la formula $\varphi_A(X) = AX\overline{A^{\mathrm{t}}}$. Questo determina un omomorfismo di gruppi $\mathrm{SU}_2(\mathbb{C}) \longrightarrow \mathrm{Aut}(\langle I, J, K\rangle_{\mathbb{R}}) = \mathrm{SO}_3(\mathbb{R})$; si tratta di un morfismo suriettivo con nucleo $\{\pm\mathbb{I}_2\}$.

5.15. Teorema (Spettrale Complesso (versione matriciale)). *Una matrice $A \in M_n(\mathbb{C})$ si dice hermitiana se $A^{\mathrm{t}} = \overline{A}$ (la trasposta coincide con la coniugata; se si tratta di matrici reali significa che è simmetrica), ovvero $\overline{A}^{\mathrm{t}} = A$ (la matrice coincide con la propria trsposta coniugata). Ogni matrice hermitiana è unitariamente diagonalizzabile, cioè esiste una matrice $P \in \mathrm{U}_n(\mathbb{C})$ tale che $P^{-1}AP = \overline{P}^{\mathrm{t}}AP$ sia diagonale (reale).*

5.15.1. Tralasciamo la dimostrazione, che è simile a quella svolta nel caso reale. Facciamo invece notare che il viceversa dell'enunciato non è assolutamente vero: esistono matrici che sono unitariamente diagonalizzabili, ma non sono hermitiane. Per esempio una qualsiasi matrice diagonale complessa ma non reale. Un altro esempio sono le matrici antisimmetriche reali: non sono hermitiane, ma lo diventano moltiplicate per i; quindi sono unitariamente diagonalizzabili (autovalori puramente immaginari).

5.15.2. Come per il caso reale, la hermitianità della matrice corrisponde all'uguaglianza $(Av) \cdot w = v \cdot (Aw)$ usando il prodotto hermitiano per ogni coppia di vettori $v, w \in V_n(\mathbb{C})$. In generale infatti vale solo che $(Av) \cdot w = v \cdot (\overline{A}^{\mathrm{t}} w)$.

5.16. (teorema spettrale per) Matrici normali. La stessa tecnica di dimostrazione permette di arrivare a questo risultato: *una matrice complessa A è unitariamente diagonalizzabile se e solo se A e $\overline{A}^{\mathrm{t}}$ commutano per prodotto (i.e. $A\overline{A}^{\mathrm{t}} = \overline{A}^{\mathrm{t}}A$, e matrici con questa proprietà si dicono normali).*

Infatti, prima di tutto si osserva che A e $\overline{A}^{\mathrm{t}}$ hanno lo stesso nucleo (poiché $Av = 0$ sse $\overline{(Av)}^{\mathrm{t}}(Av) = 0$ sse $\overline{(\overline{A}^{\mathrm{t}}v)}^{\mathrm{t}}(\overline{A}^{\mathrm{t}}v) = 0$ sse $\overline{A}^{\mathrm{t}}v = 0$); quindi l'autospazio di A relativo all'autovalore λ coincide con l'autospazio di $\overline{A}^{\mathrm{t}}$ relativo all'autovalore $\overline{\lambda}$: $Av = \lambda v$ sse $\overline{A}^{\mathrm{t}}v = \overline{\lambda}v$ (infatti si ha $\ker(A - \lambda) = \ker(\overline{A}^{\mathrm{t}} - \overline{\lambda})$, poiché $A - \lambda$ commuta con la coniugata trasposta, se lo fa A...).

A questo punto, se v e w sono autovettori di autovalori λ e μ distinti dalle solite uguaglianze $(Av) \cdot w = v \cdot (\overline{A}^{\mathrm{t}} w)$ si ottiene che $\lambda v \cdot w = \mu v \cdot w$, e quindi $(\lambda - \mu)\overline{v}^{\mathrm{t}}w = 0$, da cui l'ortogonalità (hermitiana) di autospazi distinti. Dunque dal solito ragionamento (stabilità di ortogonali di sottospazi stabili, per entrambe A e $\overline{A}^{\mathrm{t}}$) si arriva alla diagonalizzabilità.

5.16.1. Si vede allora che vi sono vari casi interessanti:

(1) una matrice è hermitiana se e solo se è normale (o unitariamente diagonalizzabile) con spettro reale;
(2) una matrice è antihermitiana ($A^{\mathrm{t}} = -\overline{A}$) se e solo se è normale (o unitariamente diagonalizzabile) con spettro puramente immaginario;
(3) una matrice è unitaria se e solo se è normale (o unitariamente diagonalizzabile) con spettro unitario;
(4) una matrice reale è ortogonale se e solo se è normale (o unitariamente diagonalizzabile) con spettro unitario.

Resta comunque che vi sono matrici normali che non appartengono ad alcuna delle classi precedenti...

5.16.2. Come si esprime la normalità in termini del prodotto hermitiano: per ogni coppia di vettori, si ha $(Av) \cdot (Aw) = (\overline{A}^{\mathrm{t}}v) \cdot (\overline{A}^{\mathrm{t}}w)$.

5.16.3. Dalla dimostrazione del teorema spettrale per matrici normali si vede che: *se A è normale, allora* $\ker A = \ker \overline{A}^{\mathrm{t}}$ *e* $\operatorname{im} A = \operatorname{im} \overline{A}^{\mathrm{t}}$. *Da questo segue la decomposizione ortogonale* $V_n(\mathbb{C}) = \ker A \boxplus (\ker A)^{\perp} = \ker A \boxplus \operatorname{im} A$ (perché nell'identificazione di $V_n(\mathbb{C})$ con il suo duale via prodotto hermitiano nella base canonica abbiamo $\operatorname{im} \overline{A}^{\mathrm{t}} = (\ker A)^{\perp}$; si noti che il trasposto viene dalla dualità, il coniugato dal prodotto hermitiano usato per identificare lo spazio con il suo duale...).

5.16.4. Problema. Vi sono varie caratterizzazioni possibili delle matrici normali; ne proponiamo alcune in disordine:

(1) se $A = B + iC$ con B, C matrici hermitiane (è sempre possibile questa scrittura...) allora A è normale se e solo se $BC = CB$;

(2) A è normale se e solo se gli autovettori di A coincidono con quelli di $\overline{A}^{\mathrm{t}}$;

(3) A è normale se e solo se $\overline{A}^{\mathrm{t}} \in \mathbb{C}[A]$ (polinomiale in A); infatti basta considerare il polinomio che calcolato negli autovalori della matrice dà i coniugati (essendo gli autospazi gli stessi);

(4) A è normale se e solo se $\overline{A}^{\mathrm{t}} = AU$ con U matrice unitaria.

5.16.5. Alcune proprietà di stabilità:

(1) se A e B sono matrici normali e $AB = BA$, allora AB è normale;

(2) se A , B e AB sono matrici normali, allora BA è normale.

5.17. Problema: teorema di Schur complesso. *Ogni matrice complessa è unitariamente triangolarizzabile.*

Da questo si deduce quasi immediatamente il teorema spettrale per le matrici hermitiane (se $T = \overline{U}^{\mathrm{t}} AU$ è triangolare con $\overline{A}^{\mathrm{t}} = A$, allora $\overline{T}^{\mathrm{t}} = T$, che è dunque diagonale reale...) e anche l'enunciato per matrici normali (se $T = \overline{U}^{\mathrm{t}} AU$ è triangolare con $A\overline{A}^{\mathrm{t}} = \overline{A}^{\mathrm{t}} A$, allora $T\overline{T}^{\mathrm{t}} = \overline{T}^{\mathrm{t}} T$, da cui si deduce facilmente che T è diagonale: ma si userà che i coefficienti della matrice sono numeri complessi...).

♠ **5.18.** Equivalenza unitaria (valori singolari). Consideriamo ora due matrici $A, B \in M_{n,m}(\mathbb{C})$ non necessariamente quadrate; diciamo che esse sono unitariamente equivalenti se esistono $U \in \mathrm{U}_n(\mathbb{C})$ e $V \in \mathrm{U}_m(\mathbb{C})$ tali che $UAV = B$. Si tratta di una relazione più sottile della equivalenza di matrici che abbiamo già trattata.

5.18.1. Classificazione per equivalenza unitaria. *Ogni matrice $A \in M_{n,m}(\mathbb{C})$ è unitariamente equivalente ad una matrice pseudodiagonale del tipo*

$$\begin{pmatrix} \Sigma & \mathbb{O}_{r,n-r} \\ \mathbb{O}_{m-r,r} & \mathbb{O}_{m-r,n-r} \end{pmatrix}$$

dove r è il rango di A, $\Sigma \in M_r(\mathbb{R})$ è matrice diagonale con valori diagonali positivi $s_1 \leqslant s_2 \leqslant \cdots \leqslant s_r$ detti i valori singolari di A. I valori singolari s_i sono caratterizzati dal fatto di essere reali positivi e che s_i^2 sono gli autovalori non nulli delle matrici $\overline{A}^{\mathrm{t}} A$ e $A\overline{A}^{\mathrm{t}}$; quindi la forma pseudodiagonale è univocamente determinata da A. In particolare il rango e i valori singolari (sequenza non decrescente di rg$A$ *reali non negativi) classifica le matrici per equivalenza unitaria.*

La dimostrazione è del tutto simile a quella del caso reale, e si lascia al lettore.

5.18.2. Caso di matrici quadrate. Cosa si può dire nel caso di matrici quadrate riguardo ai valori singolari?

♠ **5.19.** Decomposizione polare. È facile, per matrici quadrate, dedurre dal teorema di classificazione per equivalenza unitaria (e dal teorema spettrale) la cosiddetta decomposizione polare: *ogni matrice complessa quadrata $A \in M_n(\mathbb{C})$ si scrive come prodotto $A = SU$ con S matrice hermitiana con autovalori non negativi e U matrice unitaria; inoltre tale scrittura è unica se A è invertibile. Naturalmente è possibile la scrittura $A = U'S'$ con le stesse condizioni (risulta $S = S'$ se e solo se A è hermitiana?).*

Basta infatti usare $A = U\Sigma V = (U\Sigma\overline{U}^{\mathrm{t}})(UV)$.

È anche interessante osservare che la decomposizione polare si può trovare usando le stesse tecniche usate nella classificazione per equivalenza unitaria; inoltre l'esistenza della decomposizione polare permette di ritrovare la classificazione per equivalenza unitaria: da $A = SU$ troviamo $A = W\Sigma\overline{W}^{\mathrm{t}} U$ con Σ diagonale (con entrate reali non negative) e $\overline{W}^{\mathrm{t}} U$ unitaria.

Visto che non l'abbiamo fatto nel caso reale, proponiamo l'argomento diretto nel caso complesso: consideriamo una diagonalizzazione unitaria per $\overline{A}^{\mathrm{t}} A = V\Sigma^2\overline{V}^{\mathrm{t}}$ (i termini diagonali di Σ^2 sono non negativi, siano s_i^2 con $s_i \geqslant 0$). Le colonne v_i di V sono una base ortonormale di $V_n(\mathbb{C})$ e le loro immagini tramite A, siano $u_i = Av_i$, sono ortogonali tra loro: $u_i \cdot u_j = (Av_i) \cdot (Av_j) = v_i \cdot (\overline{A}^{\mathrm{t}} Av_j) = s_j^2 (v_i \cdot v_j)$ (si osservi per inciso che se $s_i = 0$ allora $u_i = Av_i = 0$); quindi possiamo completare l'insieme u_i/s_i

per $s_i \neq 0$ ad una base ortonormale di $V_n(\mathbb{C})$, e quindi ottenere (le colonne di) una matrice unitaria W tale che $AV = W\Sigma$. Basta allora osservare che

$$A = AV\overline{V}^{\mathrm{t}} = W\Sigma\overline{V}^{\mathrm{t}} = W\Sigma\overline{W}^{\mathrm{t}}W\overline{V}^{\mathrm{t}} = SU$$

dove $S = W\Sigma\overline{W}^{\mathrm{t}}$ è hermitiana con spettro non negativo, e $U = W\overline{V}^{\mathrm{t}}$ è unitaria, come si voleva.

♠ **5.20.** Pseudoinverse. Anche nel caso complesso esiste la nozione di matrice pseudoinversa di una matrice rettangolare qualsiasi $A \in M_{n,m}(\mathbb{C})$. Si tratta dell'unica matrice A^+ che soddisfa alle tre condizioni seguenti:
(0) $\mathrm{rg}A^+$ è minimo possibile (necessariamente uguale a $\mathrm{rg}A$);
(1) AA^+ è proiezione hermitiana su $\mathrm{im}\,A$;
(1′) A^+A è proiezione hermitiana su $(\ker A)^\perp = \mathrm{im}\,\overline{A}^{\mathrm{t}}$;
o equivalentemente alle quattro condizioni classiche:
(1) $AA^+A = A$ e $A^+AA^+ = A^+$;
(2) A^+A e AA^+ sono hermitiane.

5.20.1. Calcolo. Analogamente al caso reale, le pseudoinverse possono essere calcolate sia tramite decomposizioni di rango massimo: se $A = BC$ con $B \in M_{n,r}$ e $C \in M_{r,m}$, essendo $r = \mathrm{rg}A$, allora $A^+ = C^+B^+ = \overline{C}^{\mathrm{t}}(C\overline{C}^{\mathrm{t}})^{-1}(\overline{B}^{\mathrm{t}}B)^{-1}\overline{B}^{\mathrm{t}}$; sia tramite equivalenza unitaria: se $A = U\Sigma V$ allora $A^+ = V^+\Sigma^+U^+ = \overline{V}^{\mathrm{t}}\Sigma^+\overline{U}^{\mathrm{t}}$.

5.20.2. Altre proprietà. Abbiamo $A^{++} = A$; se U, V sono unitarie allora $(UAV)^+ = V^+A^+U^+$ (falso in generale per matrici solo invertibili), $A^+ = A^{\mathrm{t}}$ se e solo se A è unitaria.

Abbiamo $(A^+)^{\mathrm{t}} = (A^{\mathrm{t}})^+$, se $\alpha \in \mathbb{C}^\times$ allora $\alpha^+ = \alpha/|\alpha|^2$ (o 0 se $\alpha = 0$), se $0 \neq v \in V_n(\mathbb{C})$ allora $v^+ = v^{\mathrm{t}}/\|v\|^2$.

Inoltre $A^+ = (A^{\mathrm{t}}A)^+A = A^{\mathrm{t}}(AA^{\mathrm{t}})^+$.

5.21. Altri prodotti di matrici? Si osservi che non abbiamo mai specificato la struttura degli insiemi di matrici hermitiane (o simmetriche) e antihermitiane (o antisimmetriche) rispetto al prodotto di matrici; questi insiemi infatti sono sottospazi vettoriali delle matrici, ma non sono chiusi per il prodotto usuale. Tuttavia vale la pena forse di osservare, anche se non approfondiremo l'argomento, che vi sono altri "prodotti" di matrici che sono stabili per questi insiemi.

5.21.1. Prodotto antisimmetrico o di Lie. Date due matrici quadrate $A, B \in M_n(\Bbbk)$ definiamo il loro prodotto di Lie, detto anche il loro commutatore, come $[A, B] = AB - BA$. Il nome di commutatore dipende dall'ovvia uguaglianza $AB = BA + [A, B]$. Il prodotto di Lie è bilineare, ma non associativo; tuttavia rispetta la cosiddetta identità di Jacobi:

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$$

(uno spazio vettoriale con un tale prodotto si chiama algebra di Lie su $\Bbbk$).

Gli insiemi delle matrici antisimmetriche reali e antihermitiane complesse sono sottoalgebre di Lie delle matrici.

In particolare l'algebra di Lie delle matrici antisimmetriche reali di ordine 3 è isomorfa all'algebra di Lie formata dallo spazio vettoriale reale standard di dimensione 3 dotato del prodotto vettore (come prodotto di Lie): esplicitare l'isomorfismo.

5.21.2. Prodotto simmetrico o di P.Jordan? Date due matrici quadrate $A, B \in M_n(\Bbbk)$ definiamo il loro prodotto simmetrico come $A \cdot B = AB + BA$. Il prodotto simmetrico è bilineare, ma non associativo; tuttavia rispetta una identità detta alternanza, o proprietà alternativa:

$$(A \cdot B) \cdot A = A \cdot (B \cdot A) \qquad \text{oppure} \qquad (A \cdot A) \cdot B = A \cdot (A \cdot B) \qquad \text{oppure} \qquad (B \cdot A) \cdot A = B \cdot (A \cdot A)$$

(tutte equivalenti tra loro, ed equivalenti al fatto che l'associatore $[A, B, C] = (AB)C - A(BC)$ di tre elementi sia funzione 3-lineare alternante dei suoi argomenti, donde il nome). Uno spazio vettoriale con un tale prodotto si chiama algebra alternativa su $\Bbbk$.

Gli insiemi delle matrici simmetriche reali e hermitiane complesse sono sottoalgebre alternative delle matrici.

5.22. Analogia tra $\mathbb{C}$ e $M_n(\mathbb{C})$. Vi è una simpatica e classica analogia tra numeri complessi e matrici quadrate complesse di cui evidenziamo i primi elementi, e le relazioni con le matrici reali.

5.22.1. Osserviamo prima di tutto che ogni matrice complessa Z si scrive $Z = A+iB$ con A e B matrici hermitiane; infatti basta osservare che $\overline{Z}^{\mathrm{t}} = A - iB$ e ottenere A e B per somma e differenza: $A = \frac{Z+\overline{Z}^{\mathrm{t}}}{2}$ e $B = \frac{Z-\overline{Z}^{\mathrm{t}}}{2i}$ (che si verifica subito essere matrici hermitiane). Questo è analogo alla decomposizione $z = a + ib$ con $a, b \in \mathbb{R}$: quindi le matrici hermitiane sono l'analogo dei numeri reali, le hermitiane con autovalori non negativi (positivi) sono l'analogo dei reali non negativi (positivi).

5.22.2. L'analogo del coniugio complesso $\overline{z} = a - ib$ è $\overline{Z}^{\mathrm{t}} = A - iB$.

5.22.3. La moltiplicazione con i identifica numeri reali e immaginari puri; analogamente la moltiplicazione per i identifica matrici hermitiane e matrici antihermitiane (cioè tali che $\overline{Z}^{\mathrm{t}} = -Z$; si noti che Z è hermitiana sse iZ è antihermitiana). Quindi le matrici antihermitiane sono l'analogo dei numeri puramente immaginari.

L'analogo dei numeri complessi unitari ($z\overline{z} = 1$) è la nozione di matrici unitarie ($U\overline{U}^{\mathrm{t}} = \mathbb{I}$); e la decomposizione polare $z = |z|e^{i\vartheta}$ (unica se $z \neq 0$) diventa la decomposizione polare $Z = SU$ con S hermitiana e U unitaria (unica se Z è invertibile).

Si noti che per i complessi abbiamo $|z|^2 = z\overline{z} = a^2 + b^2$. In generale per una matrice $Z = A + iB$ abbiamo che $Z\overline{Z}^{\mathrm{t}} = (A^2 + B^2)$ se e solo se la matrice Z è normale (altrimenti?); quindi per portare più avanti l'analogia bisogna pensare alle matrici normali come controparte dei numeri complessi (che, come matrici d'ordine uno, sono tutti normali).

5.22.4. Trasformazioni di Cayley. La mappa $z \mapsto \frac{1-z}{1+z}$ manda l'asse immaginario nel circolo unitario tolto -1, e viceversa - essendo tra questi due insiemi una biiezione autoinversa. Analogamente la mappa che manda ogni matrice Z in $\frac{1-Z}{1+Z} = (1-Z)(1+Z)^{-1}$ identifica le matrici antihermitiane con le matrici unitarie prive dell'autovalore -1, e viceversa, essendo autoinversa tra questi due insiemi.

Si osservi che questo si specializza nel caso reale ad una biiezione tra matrici antisimmetriche e matrici ortogonali prive dell'autovalore -1.

Nel caso complesso è ancora interessante notare che matrici hermitiane e matrici unitarie senza autovalore -1 sono in corrispondenza (come, e come si traduce per matrici reali?).

5.22.5. Mappa esponenziale. La mappa $\vartheta \mapsto e^{i\vartheta}$ manda suriettivamente $\mathbb{R}$ sul circolo dei complessi unitari. Analogamente l'esponenziale e^{iA} di una matrice hermitiana è una matrice unitaria, e tutte le matrici unitarie si ottengono come esponenziali (immaginari) di matrici hermitiane.

5.22.6. Possiamo riassumere in uno schema:

contesto :	$\mathbb{C}$ (numeri complessi)	$M_n(\mathbb{C})$(matrici quadr. in $\mathbb{C}$)
sottinsiemi :	$\mathbb{R}$ (reali : $z = \overline{z}$)	H (hermitiane : $A = \overline{A}^{\mathrm{t}}$)
	$\mathbb{R}_{\geqslant 0}$ (reali non neg.)	$H_{\geqslant 0}$ (herm. con spettro non neg.)
	$\mathbb{R}_{>0}$ (reali posit.)	$H_{>0}$ (herm. con spettro posit.)
	$i\mathbb{R}$ (immag. : $z = -\overline{z}$)	iH (antiherm. : $A = -\overline{A}^{\mathrm{t}}$)
	$\mathbb{S}^1$ (unitari : $z\overline{z} = 1$)	U (unitarie : $U\overline{U}^{\mathrm{t}} = \mathbb{I}$)
dec.additt. :	$\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$	$M_n(\mathbb{C}) = H \oplus iH$
dec.polare. :	$\mathbb{C}^\times = \mathbb{R}_{>0} \times \mathbb{S}^1$	$\mathrm{GL}_n(\mathbb{C}) = H_{>0} \times U$
tasf.Cayley :	$i\mathbb{R} \cong \mathbb{S}^1 \smallsetminus \{-1\}$	$iH \cong U(-1 \notin$ spettro)
esponenz. :	$[0, 2\pi[\to \mathbb{S}^1$	H(spettro $\subseteq [0, 2\pi[) \to U$

5.23. Relazioni con il caso reale. L'applicazione biiettiva

$$r : V_n(\mathbb{C}) \longrightarrow V_{2n}(\mathbb{R})$$

cha manda un vettore complesso $v = (z_i)^{\mathrm{t}} = (x_i + iy_i)^{\mathrm{t}}$ nel vettore reale $r(v) = (x_1, \ldots, x_n, y_1, \ldots, y_n)^{\mathrm{t}}$ possiede la proprietà che $\|r(v)\| = \|v\|$ per ogni $v \in V_n(\mathbb{C})$ (norme euclidea nel primo membro, ed hermitiana nel secondo), e più in generale

$$r(v) \cdot r(w) = \Re(v \cdot w)$$

(prodotto scalare euclideo nel primo membro, ed hermitiano nel secondo) per $v, w \in V_n(\mathbb{C})$. In effetti possiamo esplicitare: $v \cdot v' = \sum_{j=1}^n (x_j x'_j + y_j y'_j) + i \sum_{j=1}^n (x_j y'_j - y_j x'_j)$ mentre $r(v) \cdot r(v') = \sum_{j=1}^n (x_j x'_j + y_j y'_j)$.

5.23.1. Applicazioni lineari e Matrici. Se consideriamo la base canonica $e_1, \ldots, e_n$ di $V_n(\mathbb{C})$, allora i vettori $e_1, \ldots, e_n, ie_1, \ldots, ie_n$ sono linearmente indipendenti su $\mathbb{R}$ (ma non su $\mathbb{C}$) e sono

una base di $V_n(\mathbb{C})$ in quanto spazio vettoriale reale, e le coordinate in tale base danno la biiezione precedente. Quanto detto è vero per ogni base di uno spazio vettoriale complesso?

Se ora abbiamo un endomorfismo $\mathbb{C}$-lineare rappresentato dalla matrice $C = A + iB \in M_n(\mathbb{C})$ (con $A, B \in M_n(\mathbb{R})$) in una fissata base, allora lo stesso endomorfismo è anche $\mathbb{R}$-lineare e nella base reale corrispondente ha matrice $\left(\begin{smallmatrix} A & -B \\ B & A \end{smallmatrix}\right) \in M_{2n}(\mathbb{R})$ (e viceversa, ogni matrice di tale forma definisce un endomorfismo $\mathbb{C}$-lineare).

5.23.2. Esplicitare l'isomorfismo tra l'algebra degli endomorfismi $\mathbb{C}$-lineari e la sottoalgebra corrispondente degli endomorfismi $\mathbb{R}$-lineari (usando per esempio le corrispondenti algebre di matrici), specificando la corrispondenza tra automorfismi, trasformazioni unitarie e ortogonali, hermitiane e simmetriche, ecc. In particolare, l'applicazione

$$M_n(\mathbb{C}) \longrightarrow M_{2n}(\mathbb{R}) \text{ definita da } A + iB \longmapsto \left(\begin{smallmatrix} A & -B \\ B & A \end{smallmatrix}\right)$$

è una applicazione iniettiva di algebre, con immagine data dalle matrici che commutano con la "moltiplicazione per i" (cioè con la matrice a blocchi $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$), e che fa corrispondere: a matrici hermitiane le simmetriche, a matrici unitarie le ortogonali (e simplettiche...), a matrici normali le normali...

5.23.3. Sarà di un certo interesse notare che i gruppi $GL_n(\mathbb{C})$, $U_n(\mathbb{C})$, $O_{2n}(\mathbb{R})$ e $Sp_n(\mathbb{R})$ (matrici simplettiche reali d'ordine $2n$, cioè M tali che $M^{\mathrm{t}} \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) M = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ come si vedrà in un futuro capitolo) a due a due si intersecano tutti in $U_n(\mathbb{C})$ (visti in $M_{2n}(\mathbb{R})$).

5.23.4. Che relazioni vi sono tra i determinanti di $A + iB$ e di $\left(\begin{smallmatrix} A & -B \\ B & A \end{smallmatrix}\right)$? In effetti si ha $\det \left(\begin{smallmatrix} A & -B \\ B & A \end{smallmatrix}\right) = |\det(A+iB)|^2$, come si può verificare controllando sulla matrici elementari, oppure sulle matrici triangolari, oppure riducendosi al caso hermitiano (per ogni G complessa, $\overline{G}^{\mathrm{t}} G$ è hermitiana).

Più in generale, che relazioni vi sono tra autovalori e autovettori di $A + iB$ e della controparte reale? Il polinomio caratteristico della seconda è il prodotto del polinomio caratteristico di $A + iB$ e del suo coniugato.

♠ **5.24.** Matrici complesse simmetriche, antisimmetriche e ortogonali. I teoremi spettrali danno condizioni di diagonalizzabilità per matrici reali simmetriche e normali complesse, in particolare hermitiane (antihermitiane, unitarie) complesse. Cosa si può dire in generale di matrici complesse che siano simmetriche, antisimmetriche o ortogonali? Chiaramente non sono normali. I teoremi spettrali sono legati ai prodotti scalare reale ed hermitiano complesso che sonno definiti positivi, e questa proprietà è fondamentale per i teoremi spettrali; il prodotto scalare nel caso complesso è una forma non degenere ma non definita positiva, e quindi non possiamo aspettarci risultati analoghi.

5.24.1. In un certo senso, non solo non è vero che matrici complesse simmetriche, antisimmetriche, ortogonali abbiano particolari proprietà (se non le eventuali restrizioni sugli autovalori) per la loro autoteoria, ma è vero addirittura il contrario:

(1) ogni matrice complessa è simile a una simmetrica complessa, cioè in ogni classe di similitudine esistono matrici complesse simmetriche;

(2) ogni matrice complessa tale che la struttura di Jordan sia stabile passando all'opposto degli autovalori e i blocchi di ordine pari di autovalore nullo siano in numero pari è simile a una antisimmetrica complessa;

(3) ogni matrice invertibile complessa tale che la struttura di Jordan sia stabile passando all'inverso degli autovalori e i blocchi di ordine pari di autovalori ± 1 siano in numero pari è simile a una ortogonale complessa.

In ogni caso i cambiamenti di base da una forma di Jordan a matrici in forme simmetriche, antisimmetriche o ortogonali coinvolgono vettori isotropi (del prodotto scalare in $V_n(\mathbb{C})$).

5.24.2. caso simmetrico: chiaramente possiamo ridurci al caso di matrici di Jordan, standard, nilpotenti N, e mostrare che $N = T^{-1}ST$ con S simmetrica. Da $TNT^{-1} = S = S^{\mathrm{t}} = T^{-\mathrm{t}} J^{\mathrm{t}} T^{\mathrm{t}}$ abbiamo $(T^{\mathrm{t}}T)N = N^{\mathrm{t}}(T^{\mathrm{t}}T)$, e ponendo $-2iV = T^{\mathrm{t}}T$ dobbiamo cercare V tale che $VN = N^{\mathrm{t}}V$. Tali matrici hanno antidiagonali costanti e nulle sopra quella principale, e possiamo per esempio usare quella con antidiagonale costante 1 (e 0 altrove), ovvero la matrice che inverte d'ordine la base canonica. Cercando T simmetrica con $T^2 = -2iV$ possiamo trovare $T = \mathbb{I} - iV$, e quindi

$T^{-1} = \frac{1}{2}(\mathbb{I} + iV)$. Ne risulta allora

$$TNT^{-1} = \frac{1}{2}(\mathbb{I} - iV)N(\mathbb{I} + iV) = \frac{1}{2}(N + VNV) + \frac{i}{2}(NV - VN) = \frac{1}{2}(N + N^{\mathrm{t}}) + \frac{i}{2}(NV - VN)$$
$$= \frac{1}{2}\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ & \ddots & \ddots & \ddots & \\ 0 & \cdots & 1 & 0 & 1 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} + \frac{i}{2}\begin{pmatrix} 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & 1 & 0 & -1 \\ & \iddots & \iddots & \iddots & \\ 1 & 0 & -1 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \end{pmatrix}$$

che è una forma canonica simmetrica per similitudine del blocco nilpotente standard di Jordan.

5.24.3. CASO ANTISIMMETRICO: possiamo ridurci a trattare matrici del tipo:

$$J = \begin{pmatrix} \lambda + N & 0 \\ 0 & -(\lambda + N) \end{pmatrix} \quad \text{simili a} \quad \frac{1}{2}\begin{pmatrix} N - N^{\mathrm{t}} & i(2\lambda V + NV + VN) \\ -i(2\lambda V + NV + VN) & N^{\mathrm{t}} - N \end{pmatrix},$$

e del tipo

$$L = \begin{pmatrix} \vdots & \mathbb{I} & 0 \\ \vdots & 0 & -\mathbb{I} \\ 0 & \cdots & \cdots \end{pmatrix} \quad \text{simili a} \quad \frac{1}{2}(L - L^{\mathrm{t}}) + \frac{i}{2}(LV - VL),$$

usando matrici analoghe a V e T (di taglia opportuna) usate prima.

5.24.4. CASO ORTOGONALE: Ci si può ricondurre al caso antisimmetrico, ricordando che se K è antisimmetrica, allora e^K è ortogonale; quindi basta partire con logaritmi degli autovalori, ed esponenziare le matrici antisimmetriche corrispondenti; nel caso di autovalori ± 1 si useranno matrici $\pm e^L$.

5.24.5. DECOMPOSIZIONE POLARE COMPLESSA. Vi è anche una decomposizione polare complessa usando matrici simmetriche ed ortogonali: *ogni matrice $A \in \mathrm{GL}_n(\mathbb{C})$ si scrive come prodotto $A = SQ$ con S matrice simmetrica complessa, radice quadrata di AA^{t} e polinomiale in AA^{t}, e Q matrice ortogonale complessa; idem per $A = Q'S'$ con S' simmetrica, radice quadrata e polinomiale di $A^{\mathrm{t}}A$; inoltre $SQ = QS$ se e solo se $AA^{\mathrm{t}} = A^{\mathrm{t}}A$ se e solo se $Q'S' = S'Q'$.*

Si può ottenere in modo diretto così: da $A = SQ$ troviamo $A^{\mathrm{t}} = Q^{\mathrm{t}}S^{\mathrm{t}} = Q^{-1}S$, quindi $AA^{\mathrm{t}} = SQQ^{-1}S = S^2$, ed essendo AA^{t} simmetrica invertibile, possiamo trovarne una radice quadrata simmetrica e polinomiale in AA^{t} (da giustificare). Allora definiamo Q come $S^{-1}A$, e si verifica subito che è ortogonale, perché $Q^{\mathrm{t}} = A^{\mathrm{t}}S^{-\mathrm{t}} = A^{\mathrm{t}}S^{-1}$ e quindi $QQ^{\mathrm{t}} = S^{-1}AA^{\mathrm{t}}S^{-1} = S^{-1}S^2S^{-1} = \mathbb{I}$.

6. Esercizi.

6.1. Sia $V = V_n(\mathbb{R})$ lo spazio vettoriale standard di dimensione n su $\mathbb{R}$, dotato del prodotto scalare. Indichiamo con u, v, w elementi di $V_n(\mathbb{R})$ Dire se le seguenti affermazioni sono vere o false, fornendo dimostrazioni o controesempi:
(a) se u è non nullo e $u \cdot v = u \cdot w$ per allora $v = w$;
(b) se $v \cdot w = 0$ per ogni $w \in V$ allora $v = 0$;
(b') se $v \cdot w = 0$ per ogni vettore w di una base di V allora $v = 0$;
(c) se $u \cdot v = u \cdot w$ per ogni $u \in V$ allora $v = w$;
(c') se $u \cdot v = u \cdot w$ per ogni vettore u di una base di V allora $v = w$.

6.2. Sia $V = V_n(\mathbb{R})$ lo spazio vettoriale standard di dimensione n su $\mathbb{R}$, dotato del prodotto scalare. Indichiamo con u, v, w elementi di $V_n(\mathbb{R})$ Dire se le seguenti affermazioni sono vere o false, fornendo dimostrazioni o controesempi:
(a) $\|v + w\| = \|v - w\|$ se e solo se $v \cdot w = 0$;
(b) $\|v + tw\| \geqslant \|v\|$ per ogni $t \in \mathbb{R}$ se e solo se $v \cdot w = 0$;
(c) $\|v + w\|^2 + \|v - w\|^2 = 2(\|v\|^2 + \|w\|^2)$ (interpretazione geometrica?);
(d) $\|v + w\|^2 - \|v - w\|^2 = 4v \cdot w$

6.3. Siano u_1 e u_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione n su $\mathbb{R}$, dotato del prodotto scalare. Sia $v = \alpha_1 v_1 + \alpha_2 v_2$. Poniamo v_1 la proiezione

ortogonale di v lungo u_1 e v_2 la proiezione ortogonale di v lungo u_2. Che relazioni vi sono tra α_1, α_2, v_1 e v_2?

6.4. Siano u_1 e u_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione n su $\mathbb{R}$, dotato del prodotto scalare. Sia $v = \alpha_1 v_1 + \alpha_2 v_2$. Trovare le relazioni tra le aree dei triangolo definiti dalle seguenti coppie di vettori: u_1 e u_2, u_1 e v, v e u_2.

Generalizzare considerando tre vettori e i volumi dei tetraedri.

6.5. Siano v_1 e v_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione n su $\mathbb{R}$, dotato del prodotto scalare. Siano u_2 la proiezione ortogonale di v_2 lungo v_1 e u_1 la proiezione ortogonale di v_1 lungo v_2. Che relazioni vi sono tra le aree A, A_1, A_2, A' dei quattro tetraedri identificati rispettivamente dalle coppie di vettori v_1 e v_2, v_1 e u_1, v_2 e u_2, u_1 e u_2?

6.6. Siano v e w due vettori linearmente indipendenti e sia $u = v - w$. Mostrare che i tre parallelogrammi definiti dalle coppie di vettori v e w, v e u, u e w sono uguali.

6.7. Siano v e w due vettori linearmente indipendenti e sia u la proiezione ortogonale di w su v. Trovate la relazione tra l'area del triangolo definito dai vettori v e w e l'area del triangolo definito dai vettori u e w.

6.8. Siano v_1 e v_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione 2 su $\mathbb{R}$, dotato del prodotto scalare. Sia u un vettore non nullo, e siano u_1 la proiezione ortogonale di u lungo v_1 e u_2 la proiezione ortogonale di u lungo v_2. Mostrare che $u = u_1 + u_2$ se e solo se v_1 è ortogonale a v_2.

È vero lo stesso risultato in uno spazio vettoriale euclideo di dimensione 3? Se no, come si può modificare l'enunciato affinché diventi vero?

E per uno spazio di dimensione n?

6.9. Siano v_1 e v_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione n su $\mathbb{R}$, dotato del prodotto scalare. Mostrare che $\vartheta(v_1, v_1 + v_2) = \vartheta(v_2, v_1 + v_2)$ se e solo se $\|v_1\| = \|v_2\|$ (indichiamo con $\vartheta(v, w)$ l'angolo tra i vettori v e w).

6.10. Siano v e w due vettori linearmente indipendenti (indichiamo con $\vartheta(v, w)$ l'angolo tra i vettori v e w).

(a) mostrare che $\lim_{t\to\infty} \vartheta(v, v + tw) = \vartheta(v, w)$;
(b) mostrare che $\sum_{i=1}^{\infty} \vartheta(v + iw, v + (i+1)w) = \vartheta(v, w)$.

6.11. Nello spazio euclideo $\mathbb{R}^3$ si considerino i vettori $v = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ e $w = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}$.

(a) Si decomponga il vettore v come somma $v_1 + v_2$ ove v_1 sia ortogonale a w, e v_2 parallelo a w.
(b) Si determinino le superfici dei due parallelogrammi aventi come lati i vettori v,v_1 (primo parallelogramma) e v,v_2 (secondo parallelogramma)
(c) Le due superfici del punto precedente risultano uguali: dire se si tratta di un risultato generale (indipendente dai vettori v e w scelti), ed eventualmente giustificarlo e darne una interpretazione in termini di geometria (piana) elementare.

6.12. Nello spazio euclideo $\mathbb{R}^3$ si considerino i vettori $v_1 = \begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix}$ e $v_2 = \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix}$.

(a) determinare il sottospazio ortogonale a $\langle v_1, v_2 \rangle$;
(b) decomporre il vettore $w = \begin{pmatrix} 1 \\ -1 \\ -9 \end{pmatrix}$ come somma $w = w_1 + w_2 + w_3$ ove w_1 sia parallelo a v_1, w_2 sia parallelo a v_2 e w_3 sia ortogonale sia a v_1 che a v_2.
(c) mostrare che i volumi dei tre tetraedri formati rispettivamente da

$$w, w_1, w_2 \quad , \quad w, w_1, w_3 \quad \text{e} \quad w, w_2, w_3$$

sono uguali tra loro (senza calcolarli).

6.13. Nello spazio euclideo $\mathbb{R}^3$ si considerino i vettori $v = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ e $w = \begin{pmatrix} 0 \\ 1 \\ \sqrt{3} \end{pmatrix}$.

(a) calcolare l'angolo formato da v e w;
(b) determinare, se esistono, tutti i vettori che formano due angoli uguali di ampiezza $30°$ con v e w;
(c) determinare, se esistono, tutti i vettori che formano due angoli uguali di ampiezza $60°$ con v e w;
(d) determinare, se esistono, tutti i vettori che formano due angoli uguali di ampiezza $90°$ con v e w;
(e) dire se i tre sottinsiemi di $\mathbb{R}^3$ prima trovati sono o no sottospazi vettoriali.

6.14. Determinare tutte le matrici reali ortogonali di ordini 2, 3 e 4 discutendone autovalori (reali e complessi) e diagonalizzabilità.

6.15. Costruire le matrici delle simmetrie ortogonali e delle proiezioni ortogonali di asse o schermo i seguenti sottospazi di $\mathbb{R}^3$ ed $\mathbb{R}^4$:
(1) $U = \langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \rangle$, $U = \langle \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \rangle$,
(2) $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \rangle$, $U = \langle \begin{pmatrix} 1 \\ 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \rangle$, $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \rangle$.
Cos'hanno in comune queste matrici?

6.16. Dire per quali valori di β la matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \beta & \beta \\ 0 & \beta & -\beta \end{pmatrix}$ è ortogonalmente diagonalizzabile. Per quali valori è ortogonale? È sempre vero che una matrice ortogonale è ortogonalmente diagonalizzabile?

6.17. Mostrare che le matrici in $M_n(\mathbb{R})$ che sono contemporaneamente ortogonali ed ortogonalmente diagonalizzabili sono tutte e sole le matrici di simmetrie ortogonali (nel senso che asse e direzione della simmetria sono ortogonali tra loro). Per ogni n, dare esempi di matrici ortogonali ma non ortogonalmente diagonalizzabili, e di matrici ortogonalmente diagonalizzabili, ma non ortogonali.

6.18. Dire se la matrice $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ è ortogonalmente diagonalizzabile; studiare autovalori ed autospazi.

6.19. Dare un esempio di matrice non simmetrica i cui autospazi siano ortogonali tra loro (attenzione: non può essere una matrice diagonalizzabile: perché?).

6.20. Costruire se possibile una matrice simmetrica e una non simmetrica aventi come autospazi (eventualmente generalizzati) i seguenti sottospazi di $\mathbb{R}^3$ o $\mathbb{R}^4$:
(1) $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \rangle$ e $V = \langle \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \rangle$
(2) $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \rangle$ e $V = \langle \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \rangle$
(3) $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rangle$ e $V = \langle \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \rangle$
(4) $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rangle$ e $V = \langle \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \rangle$

6.21. Radici e Logaritmi di Matrici. Data una matrice A quadrata d'ordine n con coefficienti reali o complessi (eventualmente si considerino anche altri corpi) consideriamo i due problemi inversi usuali dell'elevamento a potenza e della esponenziazione:
(1) per un intero positivo n, sotto quali condizioni su A esistono matrici B tali che $B^n = A$? Tali B si dicono le radici n-esime di A; eventualmente, quante radici n-esime di A si possono trovare?
Si osservi che anche il caso in cui A sia la matrice nulla è interessante!
Se A è la matrice identica in $\mathbb{C}$, quante radici n-esime si trovano?
(1) sotto quali condizioni su A esistono matrici B tali che $A = e^B$? Tali B si dicono i logaritmi di A...

6.22. È una facile osservazione che $v^{\mathrm{t}} A w = 0$ per ogni $v, w \in \Bbbk^n$ implica (ed è equivalente a) che la matrice $A \in M_n(\Bbbk)$ è nulla (perché? e come indebolire l'ipotesi?). In particolare, nei casi reali e complessi abbiamo che una matrice quadrata A tale che $(Av) \cdot w = 0$, per ogni coppia di vettori v, w, è necessariamente nulla.

Cosa succede invece se l'ipotesi si riduce ai casi $v = w$? Dimostrare che:
(1) se $A \in M_n(\mathbb{R})$, allora $(Av) \cdot v = 0$ per ogni $v \in \mathbb{R}^n$ se solo se $A^{\mathrm{t}} = -A$ (cioè A è antisimmetrica);
(2) se $A \in M_n(\mathbb{C})$, allora $(Av) \cdot v = 0$ per ogni $v \in \mathbb{C}^n$ se solo se $A = 0$ (cioè A è nulla);
(si osservi la notevole differenza: nel secondo caso si usa il prodotto hermitiano, naturalmente!).

Si esplori anche il significato geometrico delle condizioni poste: $(Av) \cdot w = 0$ significa che A manda (ogni) v in un vettore ortogonale a (ogni) w, mentre $(Av) \cdot v = 0$ significa che A manda (ogni) v in un vettore a lui ortogonale...

Capitolo VIII

Geometria Euclidea ed Hermitiana

In questo capitolo introdurremo gli spazi euclidei, cioè gli spazi affini reali il cui spazio direttore sia dotato del prodotto scalare.

Estenderemo infine questi argomenti al caso di spazi vettoriali ed affini sul corpo complesso, dando le definizioni fondamentali di Geometria Hermitiana.

1. Spazi Euclidei.

1.1. Definizione (Spazio Euclideo). *Uno spazio euclideo reale è uno spazio affine $\mathbb{E}$ il cui spazio delle traslazioni sia uno spazio vettoriale euclideo reale. Lo spazio euclideo reale standard di dimensione n è $\mathbb{A}^n(\mathbb{R})$ il cui spazio delle traslazioni $V_n(\mathbb{R})$ è dotato del prodotto scalare; si indica con $\mathbb{E}^n(\mathbb{R})$.*

1.2. Riferimenti ortogonali e ortonormali. Un riferimento affine in uno spazio euclideo $\mathbb{E}$ si dice ortogonale (risp. ortonormale) se la base associata di $V_n(\mathbb{R})$ è ortogonale (risp. ortonormale).

1.3. Interpretazione euclidea delle equazioni cartesiane. I coefficienti delle variabili formano dei vettori che sono ortogonali al sottospazio direttore della varietà. Se L è il sottospazio $P_0+\langle v_1,\dots,v_m\rangle$ ed ha equazioni cartesiane date dal sistema $AX-b=0$ con $A\in M_{r,n}(\mathbb{R})$, $b\in\mathbb{R}^r$ ed $r=n-m$, allora risulta che le righe $A^{(1)},\dots,A^{(r)}$ intese come (coordinate di) elementi di $V_n(\mathbb{R})$ sono indipendenti e ortogonali al sottospazio $\langle v_1,\dots,v_m\rangle$. Si ha $V_n(\mathbb{R})=\langle v_1,\dots,v_m\rangle\boxplus\langle A^{(1)},\dots,A^{(r)}\rangle$ (significa che i due sottospazi sono in somma diretta e che sono ortogonali tra loro).

1.4. Definizione-Teorema (Distanza tra punti). *Definiamo la funzione distanza*

$$d:\mathbb{E}^n(\mathbb{R})\times\mathbb{E}^n(\mathbb{R})\longrightarrow\mathbb{R}$$

tramite: $d(P,Q):=\|Q-P\|$. Proprietà della funzione distanza:
$(D1)$ *$d(P,Q)=0$ se e solo se $P=Q$;*
$(D2)$ *simmetria: $d(P,Q)=d(Q,P)$;*
$(D3)$ *disuguaglianza triangolare: $d(P,Q)\leqslant d(P,R)+d(R,Q)$.*
$(D4)$ *invarianza per traslazioni: $d(P+v,Q+v)=d(P,Q)$.*

Dimostrazione. Discende dalle proprietà analoghe viste per il prodotto scalare e la norma di vettori. □

1.5. Definizione-Teorema (Distanza tra punti e sottospazi). *La distanza tra un punto P e il sottospazio L è definita come $d(P,L):=\inf_{Q\in L}d(P,Q)$. Si annulla se e solo se $P\in L$. Se $P\notin L$ allora esiste unico $P'\in L$ tale che $d(P,L)=d(P,P')$, e si chiama il punto di minima distanza. Si trova imponendo al vettore $P-P'$ di essere ortogonale allo spazio direttore di L.*

Dimostrazione. Mostriamo la caratterizzazione del punto di minima distanza: per ogni $Q\in L$ si ha $P-Q=v+v'$ con v appartenente allo spazio direttore di L e v' ortogonale a tale spazio; inoltre tale v' è indipendente da P, come si vede facilmente. Di conseguenza $d(P,Q)=\|v\|^2+\|v'\|^2$, e tale termine è minimo quando $v=0$, dunque quando $P-Q$ è ortogonale allo spazio direttore di L.

Per dimostrare l'esistenza: se $L=Q+W$, basta trovare $w\in W$ tale che $P-(Q+w)\in W^\perp$, e per questo basta decomporre $P-Q=w+w'\in W\oplus W^\perp$. □

1.5.1. Operativamente, si può procedere risolvendo (nelle incognite λ_i) il sistema lineare $((P-Q)+\sum_i\lambda_iw_i)\cdot w_i=0$ (se i w_i sono base di W), che è di Cramer.

1.5.2. Distanza tra punti e rette. Dati un punto P e una retta $r=Q+\langle v\rangle$, abbiamo

$$d(P,r)=\sqrt{\|P-Q\|^2-\frac{((P-Q)\cdot v)^2}{v\cdot v}}=\|P-Q\|\,|\sin\vartheta(P-Q,v)|$$

1.5.3. Distanza tra punti e iperpiani. Dati un punto P di coordinate $(x_1, \dots, x_n)^{\mathrm{t}}$ e un iperpiano π di equazione $a_1X_1 + \cdots a_nX_n + a_0 = 0$, abbiamo

$$d(P, \pi) = \frac{|a_1x_1 + \cdots a_nx_n + a_0|}{\sqrt{a_1^2 + \cdots + a_n^2}} \ .$$

Infatti, ponendo $a = (a_1, \dots, a_n)^{\mathrm{t}}$ abbiamo che a è un vettore ortogonale all'iperpiano, e quindi basta calcolare la proiezione lungo a di un vettore $P{-}Q$ con $Q \in \pi$ qualsiasi:

$$d(P, \pi) = \frac{|a \cdot (P{-}Q)|}{\|a\|} = \frac{|\sum_i a_ix_i - \sum_i a_iy_i|}{\|a\|}$$

ove le y_i sono le coordinate di Q, per cui $-\sum_i a_iy_i = a_0$.

Se l'iperpiano π è dato tramite un punto Q e generatori $v_1, \dots, v_n$ dello spazio direttore, possiamo calcolare la distanza come l'altezza dell'n-parallelepipedo formato da $P{-}Q, v_1, \dots, v_{n-1}$ con base l'$(n{-}1)$-parallelepipedo formato da $v_1, \dots, v_{n-1}$, dunque:

$$d(P, \pi) = \frac{|\det(P{-}Q \ v_1 \cdots v_{n-1})|}{\|\mathrm{cross}(v_1, \dots, v_{n-1})\|} = \frac{|\det(P{-}Q \ v_1 \cdots v_{n-1})|}{\sqrt{\det(v_i \cdot v_j)}} \ .$$

1.6. Definizione-Teorema (Distanza tra sottospazi). *siano L ed L' sue sottospazi di dimensioni m ed m'; la loro distanza è definita da*

$$d(L, L') := \inf_{Q \in L, Q' \in L'} d(Q, Q').$$

Si annulla se e solo se $L \cap L' \neq \varnothing$.

Se $L \cap L' = \varnothing$, allora si possono trovare le coppie di punti di minima distanza $P{\in}L$ e $P'{\in}L'$, cioè tali che $d(L, L') = d(P, P')$, imponendo che $P{-}P'$ sia ortogonale ad entrambi i sottospazi direttori.

I punti di minima distanza sono unici se e solo se le varietà L ed L' sono sghembe.

Dimostrazione. Esercizio, tenendo conto che se $Q{\in}L$ e $Q'{\in}L'$, allora $d(Q, Q') = d(P{+}v, P'{+}v') = \|(P{-}P') + v - v'\|$ e se $P{-}P'$ è ortogonale agli spazi direttori si ha $\|(P{-}P') + v - v'\|^2 = \|P{-}P'\|^2 + \|v - v'\|^2$...

Per dimostrare l'esistenza dei punti di minima distanza basta procedere ad una decomposizione $P - P' = (v + v') + u \in (W + W') \oplus (W + W')^{\perp}$ se $L = P + W$ e $L' = P' + W'$, e allora $P - v \in L$ e $P' + v' \in L'$ sono due tali punti. □

1.6.1. Formule di riduzione. In generale: $d(P+W, P'+W') = d(P, P'+W'+W)$. Questa formula permette di ricondurre il calcolo di distanze tra sottospazi affini ad un calcolo di distanze tra punti e sottospazi.

Ci possiamo sempre ricondurre al calcolo della distanza tra punti e iperpiani nel modo seguente: se $W' = (\langle Q-P\rangle + W)^\perp$, allora $d(P, Q+W) = d(P, Q+(W+W'))$ (e $Q+(W+W')$ è un iperpiano).

1.6.2. Distanze tramite proiezioni ortogonali. Detti $L = P+W$ un sottospazio affine, e Q un punto, possiamo calcolare la distanza $d(Q, L)$ tramite la decomposizione del vettore $Q-P$ in $w+w'$ dove $w \in W$ e $w' \perp W$: $d(Q,L)^2 = \|w'\|^2 = \|Q-P\|^2 - \|w\|^2$. Usando una matrice A le cui colonne siano una base di W, e una matrice B le cui colonne siano una base di $W^\perp$, e tenendo conto delle formule di proiezione ortogonale ($A(A^{\mathrm{t}}A)^{-1}A^{\mathrm{t}}$ è matrice della proiezione ortogonale su W e $B(B^{\mathrm{t}}B)^{-1}B^{\mathrm{t}}$ è matrice della proiezione ortogonale su $W^\perp$), si trovano le formule:

$$d(Q,L)^2 = \|Q-P\|^2 - (Q-P)^{\mathrm{t}}A(A^{\mathrm{t}}A)^{-1}A^{\mathrm{t}}(Q-P)$$

e

$$d(Q,L)^2 = (Q-P)^{\mathrm{t}}B(B^{\mathrm{t}}B)^{-1}B^{\mathrm{t}}(Q-P)$$

(conviene usare quella tra A e B che ha meno colonne; se L è un iperpiano o una retta queste espressioni permettono di trovare le formule classiche).

1.6.3. Altezze e rapporto di volumi. Vi è un facile ragionamento geometrico che permette di calcolare distanze punto-sottospazio e quindi tra sottospazi (senza cercare i punti di minima distanza): la distanza in questione è l'altezza del parallelepipedo determinato dalla congiungente $P'-P$ e dai generatori della giacitura del sottospazio, e quindi si calcola come rapporto tra i volumi dei due parallelepipedi. Se $\mathbb{L} = P + \langle v_1, \dots, v_r\rangle$, allora

$$d(Q,\mathbb{L}) = \frac{\mathrm{Vol}_{r+1}(P-Q\ v_1 \cdots v_r)}{\mathrm{Vol}_r(v_1 \cdots v_r)} = \frac{\sqrt{\det(v_i \cdot v_j)_{0,\dots,r}}}{\sqrt{\det(v_i \cdot v_j)_{1,\dots,r}}}$$

dove $v_0 = P-Q$.

Si specifichi una formula simile per calcolare la distanza tra sottospazi, distinguendo i casi di sottospazi sghembi o meno.

1.6.4. Distanza tra spazi complementari. Per calcolare la distanza tra un sottospazio affine $L = P + \langle v_1, \dots, v_{r-1}\rangle$ di dimensione $r-1$ e un sottospazio affine $M = Q + \langle v_r, \dots, v_{n-1}\rangle$ di codimensione r, possiamo calcolare la distanza di P dal sottospazio affine $Q + \langle v_1, \dots, v_{n-1}\rangle$, che è un iperpiano se e solo se $v_1, \dots, v_{n-1}$ sono linearmente indipendenti. Si ha in tal caso

$$d(L,M) = \frac{|\det(P-Q\ v_1 \cdots v_{n-1})|}{\sqrt{\det(v_i \cdot v_j)}}\ .$$

1.7. Teorema (Volumi di m-edri). *dati $m+1$ punti indipendenti $P_0, \dots, P_m$, detti $v_i = P_i - P_0$, risulta che l'$(m+1)$-edro definito da quei punti ha misura m-dimensionale data da*

$$\mathrm{Vol}_m(\Delta(P_0, \dots, P_m)) = \frac{1}{m!}\sqrt{\det(\,v_i \cdot v_j\,)} = \frac{1}{m!}\|(v_1\ \dots\ v_m)\|$$

ove definiamo che la "norma" di una matrice $m\times n$ con $m \leqslant n$ come la radice quadrata della somma dei quadrati dei minori di ordine m della matrice stessa (si tratta di $\binom{n}{m}$ termini).

Per un insieme di indici $1 \leqslant i_1 < \cdots < i_m \leqslant n$, abbreviato I, indichiamo con $P(I)$ la m-upla delle coordinate di P dei posti in I, e con $P(\widehat{I})$ la $(n-m)$-upla delle coordinate di P dei posti non in I. Allora l'm-volume in questione si scrive come

$$\mathrm{Vol}_m(\Delta(P_0, \dots, P_m)) = \frac{1}{m!}\sqrt{\sum_I \begin{vmatrix} 1 & \cdots & 1 \\ P_0(I) & \cdots & P_m(I) \end{vmatrix}^2}$$

ove la somma è sulle m-uple intere tali che $1 \leqslant i_1 < \cdots < i_m \leqslant n$.

Dimostrazione. Basta ricordare quanto fatto per gli Spazi Vettoriali Euclidei, a cui ci si riconduce immediatamente. □

1.7.1. Teorema (Area di triangoli). *Dati tre punti non allineati P_0, P_1 e P_2, detti* $P_1-P_0 = \begin{pmatrix} l_1 \\ \vdots \\ l_n \end{pmatrix}$ *e* $P_2-P_0 = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$, *l'area del triangolo da essi definito è*

$$A(P_0,P_1,P_2) = \frac{1}{2}\sqrt{\det((P_i-P_0)\cdot(P_j-P_0))} = \frac{1}{2}\sqrt{\sum_{i<j}\begin{vmatrix} l_i & m_i \\ l_j & m_j \end{vmatrix}^2} = \frac{1}{2}\sqrt{\sum_{i<j}\begin{vmatrix} 1 & 1 & 1 \\ P_{0,i} & P_{1,i} & P_{2,i} \\ P_{0,j} & P_{1,j} & P_{2,j} \end{vmatrix}^2}\ .$$

1.7.2. In particolare per $m = n-1$ risulta:

$$\mathrm{Vol}_{n-1}(\Delta(P_0,\dots,P_{n-1})) = \frac{1}{(n-1)!}\sqrt{\sum_{i=1}^{n}\begin{vmatrix} 1 & \cdots & 1 \\ P_0\widehat{(i)} & \cdots & P_{n-1}\widehat{(i)} \end{vmatrix}^2}$$

1.7.3. E per $m = n$ risulta: $\mathrm{Vol}_n(\Delta(P_0,\dots,P_n)) = \frac{1}{n!}|\det\begin{pmatrix} 1 & \cdots & 1 \\ P_0 & \cdots & P_n \end{pmatrix}|$.

1.8. Interpretazione euclidea delle coordinate baricentriche come rapporto di volumi.

1.9. Interpretazione euclidea dei baricentri. Dato un insieme finito di punti nello spazio euclideo, il baricentro (in senso affine, con pesi uguali) di questi punti è il punto dello spazio che minimizza la somma dei quadrati delle distanze dai punti dati. Infatti possiamo supporre (a meno di una traslazione) che il baricentro sia l'origine, e dunque di avere punti di coordinate P_i tali che $\sum_i P_i = 0$. Per ogni punto X dello spazio abbiamo allora

$$\sum_i \|X-P_i\|^2 = \sum_i (X-P_i)\cdot(X-P_i) = \sum_i X\cdot X - 2\sum_i X\cdot P_i + \sum_i P_i\cdot P_i = N\|X\|^2 + \sum_i \|P_i\|^2$$

da cui segue $\sum_i \|X-P_i\|^2 \geqslant \sum_i \|P_i\|^2$ come si voleva.

1.9.1. Problemi di regressione lineare. Dato un insieme finito di punti in uno spazio euclideo, come trovare un iperpiano (o in generale un sottospazio) tale da minimizzare la somma dei quadrati delle distanze dei punti dati dall'iperpiano (sottospazio) in questione? Naturalmente, se l'insieme di punti sta su un iperpiano, quell'iperpiano è la risposta; possiamo quindi supporre che l'insieme dato di punti generi lo spazio.

♠ **1.10.** Ortogonalità tra sottospazi di uno spazio euclideo. Di solito non si definisce una nozione di ortogonalità tra sottospazi affini di uno spazio euclideo, anche se si è soliti dire che due rette sono ortogonali (se i vettori direttori lo sono), o che due piani in $\mathbb{E}^3(\mathbb{R})$ sono ortogonali (che ha un altro significato: i vettori normali ai piani sono tra loro ortogonali; si noti che in questo caso i sottospazi direttori non sono ortogonali in quanto sottospazi vettoriali, perché hanno intersezione non nulla). Vogliamo far vedere quali difficoltà nascono dal tentativo di definire una nozione di ortogonalità che tenga conto dei casi precedenti, e sia ragionevolmente vicina all'intuizione.

1.10.1. Ortogonali relativi. Per due sottospazi $U \leqslant V \leqslant \mathbb{R}^n$, definiamo l'ortogonale relativo di U in V nel modo seguente:

$$U^{\perp_V} = U^\perp \cap V = \{v \in V \ :\ v \perp U\}$$

e abbiamo allora una serie di facili osservazioni del tipo:
(1) $V = U \boxplus U^{\perp_V}$ e $U^\perp = U^{\perp_V} \boxplus V^\perp$; inoltre $\mathbb{R}^n = U \boxplus U^{\perp_V} \boxplus V^\perp$;
(2) $U^{\perp_V\perp_V} = U$;
(3) $U \leqslant \mathbb{W}$ se e solo se $U^{\perp_V} \geqslant \mathbb{W}^{\perp_V}$;
(4) $(U+\mathbb{W})^{\perp_V} = U^{\perp_V} \cap \mathbb{W}^{\perp_V}$ e $(U\cap\mathbb{W})^{\perp_V} = U^{\perp_V} + \mathbb{W}^{\perp_V}$
e così via.

1.10.2. Ora, per due sottospazi $V, W \leqslant \mathbb{R}^n$ usiamo gli ortogonali relativi della situazione $V\cap W \leqslant V, W \leqslant V+W$: otteniamo che

$$\begin{aligned} V &= (V\cap W)\boxplus(V\cap W)^{\perp_V} & V^\perp &= V^{\perp_{V+W}} \boxplus (V+W)^\perp \\ W &= (V\cap W)\boxplus(V\cap W)^{\perp_W} & W^\perp &= W^{\perp_{V+W}} \boxplus (V+W)^\perp \end{aligned}$$

da cui le decomposizioni ortogonali

$$(V\cap W)\boxplus(V\cap W)^{\perp_V}\boxplus V^{\perp_{V+W}}\boxplus(V+W)^\perp = \mathbb{R}^n = (V\cap W)\boxplus(V\cap W)^{\perp_W}\boxplus W^{\perp_{V+W}}\boxplus(V+W)^\perp$$

e

$$(V \cap W) \boxplus (V \cap W)^{\perp_V} \boxplus V^{\perp_{V+W}} = V + W = (V \cap W) \boxplus (V \cap W)^{\perp_W} \boxplus W^{\perp_{V+W}}$$

da cui si ricava che

$$(V \cap W)^{\perp_V} \boxplus V^{\perp_{V+W}} = (V \cap W)^{\perp_W} \boxplus W^{\perp_{V+W}}$$

e siccome $(V \cap W)^{\perp_V}$ e $(V \cap W)^{\perp_W}$ sono in somma diretta:

$$V + W = (V \cap W)^{\perp_V} \boxplus ((V \cap W)^{\perp_V} \oplus (V \cap W)^{\perp_W}) \ ,$$

concludiamo che

$$\dim (V \cap W)^{\perp_V} = \dim W^{\perp_{V+W}} \qquad \text{e} \qquad \dim (V \cap W)^{\perp_W} = \dim V^{\perp_{V+W}}$$

1.10.3. Quindi le seguenti condizioni sono tutte equivalenti tra loro:
(1) $(V \cap W)^{\perp_V}$ e $(V \cap W)^{\perp_W}$ sono ortogonali tra loro;
(2) $(V \cap W)^{\perp_V} \leqslant W^{\perp_{V+W}}$ (e dunque uguali);
(2′) $(V \cap W)^{\perp_W} \leqslant V^{\perp_{V+W}}$ (e dunque uguali);
(3) $(V \cap W)^{\perp} \cap V \leqslant W^{\perp}$;
(3′) $(V \cap W)^{\perp} \cap W \leqslant V^{\perp}$;
(4) $W^{\perp} \cap (V + W) \leqslant V$;
(4′) $V^{\perp} \cap (V + W) \leqslant W$;
e queste sono le condizioni sotto le quali intendiamo definire che due sottospazi affini con quegli spazi direttori si dicono ortogonali tra loro: intuitivamente, quando i complementi ortogonali dell'intersezione sono ortogonali tra loro (in quanto sottospazi vettoriali di $\mathbb{R}^n$).

1.10.4. Si noti che nella definizione proposta, due sottospazi paralleli sono anche ortogonali tra loro! Perché, e come integrare la definizione per evitare questo uso, se desse fastidio?

Nei casi in cui V e W siano complementari, o generatori per $\mathbb{R}^n$, oppure in somma diretta (intersezione nulla), alcune delle condizioni equivalenti si semplificano: esplorare questi casi.

♠ **1.11.** Angoli tra sottospazi di uno spazio euclideo. Siccome sappiamo calcolare l'angolo tra due vettori, sappiamo certamente come definire l'angolo tra due rette incidenti (quello tra i vettori direttori), e anche l'angolo tra iperpiani (quello tra i vettori normali). Possiamo definire gli angoli in una situazione più generale?

1.11.1. Per esempio possiamo definire l'angolo tra due rette qualsiasi in questo modo: considerando la retta ortogonale comune (nello spazio di dimensione 3 generato dalle due rette) e misurando l'angolo tra i due piani del fascio di questa retta e contenenti le due rette iniziali.

1.11.2. Possiamo definire l'angolo tra una retta e un iperpiano (usando l'angolo tra direttore della retta e normale all'iperpiano, o meglio il complementare retto).

1.11.3. Possiamo definire l'angolo tra un sottospazio e un iperpiano (usando il complementare retto dell'angolo massimo/minimo tra vettori direttori del sottospazio e normale all'iperpiano).

1.11.4. Da completare, se possibile, riducendosi al caso di sottovarietà affini incidenti e di sottospazi direttori con intersezione nulla (intersecando con un ortogonale dell'intersezione).

2. Trasformazioni Euclidee.

2.1. Definizione (congruenza). *Una applicazione $F \in \mathrm{Aff}(\mathbb{E})$ si dice una congruenza (o rigidità, o isometria) se l'applicazione φ associata è una trasformazione ortogonale (rispetta la stuttura euclidea, i.e. il prodotto scalare). Indichiamo con* $\mathrm{Rig}(\mathbb{E})$ *questo sottogruppo di* $\mathrm{Aff}(\mathbb{E})$.

2.1.1. Congruenze e affinità. Si osservi che una applicazione insiemistica dello spazio euclideo in sè che rispetti le distanze tra i punti, è necessariamente una biiezione.

D'altra parte una applicazione insiemistica dello spazio euclideo in sè tale da rispettare il prodotto scalare tra i due vettori per ogni terna di punti è necessariamente una affinità, e dunque una congruenza come definita sopra.

2.1.2. Caratterizzazioni. In base a quanto visto per le trasformazioni ortogonali di spazi vettoriali euclidei, possiamo subito dire che essere una rigidità è equivalente ad essere una applicazione insiemistica che rispetta il prodotto scalare per ogni terna di punti, o essere una affinità che conserva le distanze per ogni coppia di punti.

2.1.3. Traslazioni. È immediato che le traslazioni dello spazio affine sono rigidità: dunque $\mathrm{Rig}(\mathbb{E}) \supseteq \mathrm{Trasl}(\mathbb{E})$.

2.1.4. Rigidità centrali. Le rigidità centrali di centro un punto $R \in \mathbb{E}$ sono quelle rigidità che fissano R; definiamo dunque $\mathrm{Rig}_R(\mathbb{E}) := \mathrm{Rig}(\mathbb{E}) \cap \mathrm{Centr}_R(\mathbb{E})$.

2.1.5. Forme matriciali. Si verifica subito che una affinità è una rigidità se e solo se la matrice associata in un riferimento ortonormale di $\mathbb{E}$ è del tipo $A = \left(\begin{smallmatrix} 1 & 0 \\ v & A' \end{smallmatrix}\right)$ ove A' è una matrice ortogonale.

2.2. Teorema (decomposizione di rigidità). *Ogni elemento di* $\mathrm{Rig}(\mathbb{E})$ *si può scrivere come composizione di una traslazione e di una rigidità di centro R preassegnato, e anche in ordine inverso. Il gruppo delle rigidità è il prodotto semidiretto di traslazioni e rigidità centrali (tramite l'azione del coniugio delle seconde sulle prime).*

Dimostrazione. Analoga al caso delle affinità. □

♠ **2.3.** Teorema (classificazione secondo Eulero delle rigidità). *Le rigidità di $\mathbb{E}$ si dividono in:*

(D) dirette (conservano l'orientamento dello spazio):
- *(T) traslazioni;*
- *(m-R) m-rotazioni: composizioni di m rotazioni su piani tra loro ortogonali, ove $m \leqslant [n/2]$ (parte intera di $n/2$);*
- *(T,m-R) glisso-m-rotazioni: composizioni di m rotazioni su piani tra loro ortogonali, ove $m \leqslant [n/2]-1$ se n è pari, $m \leqslant [n/2]$ se n è dispari, con una traslazione parallela allo spazio ortogonale ai piani di rotazione;*

(I) inverse (rovesciano l'orientamento dello spazio):
- *(R) riflessioni di direzione una retta;*
- *(m-R,R) m-roto-riflessioni: composizioni di una m-rotazione e di una riflessione di direzione ortogonale ai piani di rotazione, ove $m \leqslant [n/2]-1$ se n è pari, $m \leqslant [n/2]$ se n è dispari*
- *(T,m-R,R) glisso-m-roto-riflessioni: composizioni di una m-rotazione e di una riflessione di direzione ortogonale ai piani di rotazione, ove $m \leqslant [n/2]-1$, con una traslazione di direzione ortogonale sia ai piani di rotazione, sia alla direzione di riflessione.*

Dimostrazione. Si applica il teorema di decomposizione delle rigidità, il teorema di decomposizione in blocchi per applicazioni lineari (isometrie reali, notando che i blocchi possono avere autovalori ± 1, oppure essere di ordine due ma in $\mathrm{SO}_2(\mathbb{R})$: la rigidità sarà diretta o inversa a seconda che la molteplicità di -1 sia pari o dispari), e si semplifica la traslazione tenendo conto dei blocchi (i blocchi di rotazioni non identiche e l'eventuale riflessione permettono di "cancellare" la corrispondente traslazione). □

2.3.1. Problema. È vero che ogni rigidità è composizione di riflessioni? Quante?

2.4. Definizione-Teorema (similitudini). *Sia f un'affinità di $\mathbb{E} = \mathbb{E}^n_{\mathbb{R}}$ in sè; le seguenti proprietà sono equivalenti:*

(a) f conserva gli angoli retti, cioè per ogni $P, Q \in \mathbb{E}$ si ha $(P-Q) \cdot (P'-Q') = 0$ se e solo se $(f(P)-f(Q)) \cdot (f(P')-f(Q')) = 0$;

(b) esiste un numero reale $\alpha > 0$, tale che per ogni $P, Q \in \mathbb{E}$ si abbia $d(P,Q) = \alpha d(f(P), f(Q))$;

(c) esiste un numero reale $\alpha > 0$, tale che per ogni $P, Q, P', Q' \in \mathbb{E}$ si abbia $(P-Q) \cdot (P'-Q') = \alpha^2 (f(P)-f(Q)) \cdot (f(P')-f(Q'))$;

(d) f conserva gli angoli.

Le affinità di questo tipo si dicono similitudini; il numero α si dice il rapporto di similitudine

Dimostrazione. Analoga al caso delle conformità. □

2.4.1. Le omotetie sono similitudini. Osservazioni simili a quelle per le rigidità.

2.4.2. Forma matriciale. Sia $A = \left(\begin{smallmatrix} 1 & 0 \\ v & A' \end{smallmatrix}\right)$ la matrice di un'affinità f di $\mathbb{E}$ in sè in un riferimento ortonormale. Allora f è una similitudine se e solo se A' è una matrice conforme, i.e. $A'^t A' = \alpha^2 I_n$, per qualche numero reale $\alpha > 0$. Se $\det(A) > 0$ la similitudine si dice diretta, nel caso contrario si dice inversa.

2.4.3. Problema. Si mostri che l'insieme delle similitudini di $\mathbb{E}$ in sè è un sottogruppo del gruppo delle affinità, e che tale sottogruppo contiene il gruppo delle isometrie. Si mostri poi che il sottoinsieme delle similitudini dirette è un sottogruppo del gruppo delle similitudini.

2.4.4. Teorema (decomposizione di similitudini). *Ogni similitudine si scrive come composizione di una rigidità seguita da una omotetia di centro R preassegnato, o anche in ordine inverso*

Dimostrazione. Analoga al caso delle affinità. □

2.4.5. Similitudine di figure. Due figure F_1, F_2 (cioè sottoinsiemi di E) si dicono simili se esiste una similitudine f tale che $f(F_1) = F_2$. Si mostri che due triangoli di $\mathbb{E}$ sono simili se esiste una corrispondenza tra i vertici (o tra i lati) dell'uno e quelli dell'altro, tale che a vertici corrispondenti corrispondano angoli uguali, oppure tale che il rapporto tra le lunghezze dei lati corrispondenti sia costante.

2.5. Riassunto. Abbiamo visto ormai diverse nozioni, via via più restrittive, di trasformazioni in uno spazio affine: affinità, similitudini, rigidità. Di solito si dicono proprietà e nozioni affini (risp. conformi, metriche) le proprietà e nozioni che sono stabili per le affinità (risp. similitudini, rigidità). Per esempio:

(a) sono proprietà affini: dimensioni di (sotto)spazi, allineamento di punti, rapporto semplice, parallelismo, nozione di parallelogramma,...;

(c) sono proprietà conformi: perpendicolarità, misure di angoli, nozione di quadrato, di poligono regolare,...;

(m) sono proprietà metriche le nozioni di lunghezze ed aree, quadrati unitari, ...

È buona norma, per ogni proprietà o nozione geometrica interessante, chiedersi quali sono le sue proprietà di invarianza. Per esempio: triangoli isosceli, equilateri, rettangoli, scaleni? E le varie classi di quadrangoli piani: parallelogrammi, trapezi, rombi, quadrati?

2.6. Invarianti euclidei. Sono invarianti euclidei le proprietà che sono invarianti per isometrie. Per esempio coppie di punti vi è un solo invariante (la distanza); per coppie di rette vi sono due invarianti (distanza ed angolo tra loro, che determinano anche la posizione reciproca affine delle rette); per terne di punti allineati vi sono due invarianti affini, mentre per tre punti non allineati ve ne sono tre (le lunghezze dei lati del triangolo, oppure due lati e l'angolo compreso, oppure un lato e i due angoli adiacenti);

3. Piano euclideo.

3.1. Interpretazione euclidea delle equazioni cartesiane delle rette: la retta r di equazione $aX+bY+c=0$ ha direzione ortogonale al vettore $\binom{a}{b}$, dunque ha vettore direttore $\binom{b}{-a}$.

3.2. Angolo tra rette: L'angolo $\vartheta(r,r')$ tra due rette r ed r' è l'angolo formato dai vettori normali alle due rette, o equivalentemente l'angolo formato dai vettori direttori, e quindi

$$\cos\vartheta(r,r') = \frac{|aa'+bb'|}{\sqrt{a^2+b^2}\sqrt{a'^2+b'^2}} \ .$$

3.3. distanza punto-retta:

$$d(P_0,r) = \frac{|ax_0+by_0+c|}{\sqrt{a^2+b^2}}.$$

Se $r = P_1+\langle v_1\rangle$ e $u_1 = \mathrm{cross}(v_1)$ (i.e. un vettore normale alla retta) allora

$$d(P_0,r) = \frac{|(P_1-P_0)\cdot u_1|}{\|u_1\|}$$

(interpretazione geometrica?).

3.4. asse di un segmento: si tratta della retta dei punti equidistanti dai due punti dati P_0 e P_1; si scrive $(\frac{1}{2}P_0+\frac{1}{2}P_1)+\langle P_1-P_0\rangle^\perp$, oppure tramite l'equazione:

$$(x_1-x_0)\left(X-\frac{x_0+x_1}{2}\right)+(y_1-y_0)\left(Y-\frac{y_0+y_1}{2}\right)=0 \ .$$

3.5. BISETTRICI DI DUE RETTE INCIDENTI: se $r_0 = P_0 + \langle v_0 \rangle$ e $r_1 = P_1 + \langle v_1 \rangle$ e $\|v_0\| = \|v_1\|$, allora le bisettrici sono date da $P + \langle v_0 \pm v_1 \rangle$ ove $P = r_0 \cap r_1$.

Se abbiamo equazioni cartesiane $a_0X + b_0Y + c_0 = 0$ e $a_1X + b_1Y + c_1 = 0$ con $a_0^2 + b_0^2 = a_1^2 + b_1^2$ allora le bisettrici hanno equazioni $(a_0X + b_0Y + c_0) \pm (a_1X + b_1Y + c_1) = 0$.

3.6. AREA DI TRIANGOLI:

$$A(P_0, P_1, P_2) = \frac{1}{2}|\det \begin{pmatrix} 1 & 1 & 1 \\ P_0 & P_1 & P_2 \end{pmatrix}| = \frac{1}{2}|\begin{vmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{vmatrix}| .$$

3.7. DISTANZA TRA RETTE PARALLELE: è la distanza tra una retta e un punto qualsiasi dell'altra retta.

3.8. CONGRUENZE PIANE (SECONDO EULERO). La scelta di un riferimento ortonormale sul piano $\mathbb{A}^2(\mathbb{R})$ determina un isomorfismo del gruppo $\mathrm{Rig}(\mathbb{A}^2(\mathbb{R}))$ delle rigidità del piano con il sottogruppo

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & & \\ b & & A \end{pmatrix} | a, b \in \mathbb{R};\ A \in \mathrm{O}_2(\mathbb{R}) \right\}$$

di $\mathrm{GL}_3(\Bbbk)$. Ricordiamo che le rigidità si distinguono in dirette o inverse a seconda che $\det(A)$ sia 1 o -1. Le rigidità piane si classificano allora nel modo seguente:

3.8.1. ROTAZIONI. Sono le rigidità dirette che hanno un punto unito.

3.8.2. TRASLAZIONI. Sono le rigidità dirette prive di punti uniti.

3.8.3. RIFLESSIONI. Sono le rigidità inverse che hanno punti uniti (una retta, in effetti, di punti uniti).

3.8.4. GLISSORIFLESSIONI. Sono le rigidità inverse prive di punti uniti: si possono sempre scrivere come composizione di una riflessione e di una traslazione parallela all'asse di riflessione.

3.8.5. Questa classificazione si ottiene facilmente studiando le forme matriciali, oppure specializzando il teorema generale. Riassunto schematico:

	dirette	*inverse*
c.p.f.	rotazioni (centro un punto) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & c\alpha & -s\alpha \\ 0 & s\alpha & c\alpha \end{pmatrix}$	riflessioni (asse una retta) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$
s.p.f.	traslazioni $\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}$	glisso-riflessioni $\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$

3.8.6. Che tipo di rigidità piana è la composizione di una rotazione e di una riflessione?

3.8.7. La composizione di due riflessioni è una rotazione o una traslazione: perché, e in quali casi?

3.8.8. Ogni rigidità diretta è composizione (non canonicamente) di riflessioni: come? In particolare ogni rigidità del piano è composizione di riflessioni (e si può ottenere piegando un foglio di carta...).

3.8.9. La composizione di una rotazione e di una traslazione è ancora una rotazione: come determinarne centro e angolo in base ai dati di partenza (centro e angolo della rotazione data, e vettore della traslazione)? Si ragioni sia in termini del piano di Gauss (si tratta di trovare il punto $z \in \mathbb{C}$ tale che $z_0 + (z - z_0)e^{i\vartheta} + t = z$, con le ovvie notazioni e t è la traslazione, da cui si ricava subito che $z = z_0 + \frac{t}{1-e^{i\vartheta}}$), sia in termini del piano euclideo, aiutandosi con un disegno (si può ottenere una formula del tipo $z = z_0 + \frac{1}{2}t - \frac{1}{2}\mathrm{cross}(t)\mathrm{cotg}\frac{\vartheta}{2}$).

3.8.10. La composizione di due rotazioni?

3.9. QUALCOSA DI GEOMETRIA DEI TRIANGOLI. Un triangolo sul piano è il dato di tre punti non allineati detti vertici (e delle tre rette che essi definiscono, dette lati; talvolta si usa il termine lati per indicare i segmenti). Vi sono alcuni risultati classici, e ben noti, che ora possiamo dimostrare in modo piuttosto facile: usiamo A, B, C per indicare i tre vertici.

(0) Ricordiamo solo, perché già visto nel capitolo precedente, che le tre mediane di un triangolo (rette per un vertice e il punto medio del lato opposto) si incontrano in un punto, che è il baricentro del triangolo (nozione affine, di cui ora il lettore dovrebbe cercare l'interpretazione euclidea);

(1) Le tre altezze di un triangolo appartengono ad un fascio, cioè si incontrano in un punto; le altezze sono le rette per un vertice e ortogonali al lato opposto. Infatti le altezze sono le rette $A+\langle B-C\rangle^\perp$, $B+\langle A-C\rangle^\perp$, $C+\langle A-B\rangle^\perp$, le loro equazioni cartesiane sono dunque $(B-C)\cdot X = (B-C)\cdot A$, $(A-C)\cdot X = (A-C)\cdot B$, $(A-B)\cdot X = (A-B)\cdot C$, e si vede subito che la matrice $\begin{pmatrix} (B-C)^{\mathrm{t}} & (B-C)\cdot A \\ (A-C)^{\mathrm{t}} & (A-C)\cdot B \\ (A-B)^{\mathrm{t}} & (A-B)\cdot C \end{pmatrix}$ è di rango 2 (terza riga è la differenza delle prime due). Come esprimere le coordinate dell'ortocentro?

(2) I tre assi di un triangolo appartengono ad un fascio, cioè si incontrano in un punto; gli assi sono le rette per il punto medio d'un lato e ortogonali al lato stesso. Si vede con un ragionamento simile a prima. Come esprimere le coordinare del circocentro?

(3) Le tre bisettrici degli angoli interni di un triangolo appartengono ad un fascio, cioè si incontrano in un punto; le bisettrici interne sono le rette per un vertice e che bisecano l'angolo interno. Si tratta di un risultato più complicato: conviene qui usare il fatto che tre rette $P_i + \langle v_i\rangle$ stanno in un fascio se e solo se esistono scalari λ_i tali che i tre punti $P_i + \lambda_i v_i$ coincidano, ovvero se e solo se il sistema di matrice completa $\begin{pmatrix} v_1 & -v_2 & 0 & P_2-P_1 \\ 0 & -v_2 & v_3 & P_2-P_3 \end{pmatrix}$ ammette soluzione. Applicando questo alle tre bisettrici $A+\langle \frac{B-A}{\|B-A\|} + \frac{C-A}{\|C-A\|}\rangle = A+\langle \|C-A\|(B-A)+\|B-A\|(C-A)\rangle$, ecc. sommando le prime tre colonne si ottiene un multiplo della terza... Come esprimere le coordinare dell'incentro?

(4) Le tre bisettrici degli angoli esterni incontrano i lati opposti in tre punti allineati. Anche questo è un risultato più complicato: conviene intersecare ogni lato con la bisettrice esterna opposta (per esempio usando coordinate baricentriche del triangolo: i punti di $B \vee C$ sono $\beta B + \beta' C$ e quelli della bisettrice in A sono $(1+\lambda(\|C-A\|-\|B-A\|))A - \lambda\|C-A\|B + \lambda\|B-A\|C...)$, e si trovano i tre punti di coordinate baricentriche proporzionali a $\begin{pmatrix} 0 \\ \|C-A\| \\ -\|B-A\| \end{pmatrix}$, $\begin{pmatrix} -\|C-B\| \\ 0 \\ \|A-B\| \end{pmatrix}$, $\begin{pmatrix} \|B-C\| \\ -\|A-C\| \\ 0 \end{pmatrix}$, che sono chiaramente allineati, visto che la somma si annulla. Come esprimere la retta che congiunge quei punti?

Il lettore dovrebbe provare a dimostrare con i metodi imparati alcuni risultati che conosce circa i triangoli euclidei, per esempio:

(0) il teorema della retta di Eulero (baricentro , ortocentro e circocentro sono allineati, e l'incentro appartiene alla retta di Eulero sse il triangolo è isoscele);

(1) il teorema dei seni: dette α_i le misure degli angoli e a_i le misure dei lati rispettivamente opposti, risulta $\frac{a_i}{\sin\alpha_i}$ costante (per $i = 1, 2, 3$) e uguale al diametro del circocentro;

(2) la formula di Erone per l'area del triangolo: dette a_i le misure dei lati e p il semiperimetro, il quadrato dell'area è dato da $p(p-a_1)(p-a_2)(p-a_3)$;

(3) il calcolo del coseno d'un angolo: $\cos\alpha_i = \frac{a_j^2+a_k^2-a_i^2}{2a_ja_k}$;

(4) la somma degli angoli interni...

Vale anche la pena di scrivere baricentro G, ortocentro H, circocentro K e incentro L in coordinate baricentriche usando i vertici del triangolo come riferimento:

$$\begin{aligned} G &= \frac{1}{3}A + \frac{1}{3}B + \frac{1}{3}C \\ H &= \frac{\tan\alpha}{t}A + \frac{\tan\beta}{t}B + \frac{\tan\gamma}{t}C \\ K &= \frac{\sin 2\alpha}{s}A + \frac{\sin 2\beta}{s}B + \frac{\sin 2\gamma}{s}C \\ L &= \frac{a}{p}A + \frac{b}{p}B + \frac{c}{p}C \end{aligned}$$

dove i denominatori sono la somma dei numeratori, e le lettere a, b, c indicano la lunghezza dei lati (opposti del vertice omologo), quindi p è il perimetro. Per verificare in modo elementare queste formule può essere utile la seguente osservazione (interpretazione delle coordinate baricentriche in termini di rapporti di aree): se $P = xA + yB + zC$ con $x + y + z = 1$ allora $x = \mathrm{Area}(PBC)/\mathrm{Area}(ABC)$, ecc. (si osservi per inciso che il rapporto di aree è un invariante affine, anche se le aree sono una nozione metrica euclidea).

4. Spazio euclideo.

4.1. INTERPRETAZIONE EUCLIDEA DELLE EQUAZIONI DEI PIANI E DELLE RETTE: il piano π di equazione cartesiana $aX+bY+cZ+d=0$ è ortogonale al vettore $\left(\begin{smallmatrix} a \\ b \\ c \end{smallmatrix}\right)$; dunque il sottospazio direttore del piano è dato da $\langle \left(\begin{smallmatrix} a \\ b \\ c \end{smallmatrix}\right) \rangle^{\perp}$.

La retta $r = \pi \cap \pi'$ determinata dalle equazioni cartesiane di due piani non paralleli ha direzione ortogonale ai vettori $\left(\begin{smallmatrix} a \\ b \\ c \end{smallmatrix}\right)$ e $\left(\begin{smallmatrix} a' \\ b' \\ c' \end{smallmatrix}\right)$, dunque un suo vettore direttore è dato da $\left(\begin{smallmatrix} a \\ b \\ c \end{smallmatrix}\right) \times \left(\begin{smallmatrix} a' \\ b' \\ c' \end{smallmatrix}\right)$.

4.2. ANGOLI: L'angolo $\vartheta(\pi, \pi')$ tra due piani π e π', corrisponde all'angolo tra i vettori normali, e dunque

$$\vartheta(\pi, \pi') = \frac{|aa'+bb'+cc'|}{\sqrt{a^2+b^2+c^2}\sqrt{a'^2+b'^2+c'^2}} \ .$$

L'angolo tra due rette incidenti si misura come l'angolo tra i vettori direttori. L'angolo tra due rette sghembe si definisce nel modo seguente: si considera l'unica retta incidente ed ortogonale ad entrambe, e si calcola l'angolo tra i piani di asse e contenenti le due rette date.

L'angolo tra un piano π e una retta $r = \pi' \cap \pi''$ si scrive come il complementare dell'angolo tra vettore direttore della retta e vettore normale al piano, quindi

$$\sin \vartheta(\pi, r) = \frac{|(a\ b\ c)v|}{\sqrt{a^2+b^2+c^2}\,\|v\|}$$

se v è un vettore direttore della retta, per esempio $v = \left(\begin{smallmatrix} a' \\ b' \\ c' \end{smallmatrix}\right) \times \left(\begin{smallmatrix} a'' \\ b'' \\ c'' \end{smallmatrix}\right)$.

4.3. DISTANZA PUNTO-PIANO:

$$d(P_0, \pi) = \frac{|ax_0+by_0+cz_0+d|}{\sqrt{a^2+b^2+c^2}}.$$

Se $\pi = P_1+\langle v_1, v_1' \rangle$ allora

$$d(P_0, \pi) = \frac{|(P_1-P_0) \cdot (v_1 \times v_1')|}{\|v_1 \times v_1'\|}$$

(interpretazione geometrica: il numeratore è il volume di un parallelepipedo di cui il denominatore è la base). Il disegno è già stato visto: dove?

4.4. DISTANZA TRA PIANI PARALLELI: si tratta della distanza tra un punto qualsiasi di un piano e l'altro piano.

4.5. DISTANZA RETTA-PIANO: è nulla se non sono paralleli, e se lo sono è la distanza dal piano di un punto qualsiasi della retta.

4.6. DISTANZA RETTA-RETTA: siano $r = P+\langle v \rangle$ e $r' = P'+\langle v' \rangle$;
allora se r ed r' non sono parallele:

$$d(r, r') = \frac{|(P-P') \cdot (v \times v')|}{\|v \times v'\|}$$

(interpretazione geometrica: il numeratore è il volume di un parallelepipedo di cui il denominatore è l'area di base); mentre se sono parallele:

$$d(r, r') = \frac{\|(P-P') \times v\|}{\|v\|}$$

(interpretazione geometrica: il numeratore è area di un parallelogramma di cui il denominatore è la misura della base).

4.7. DISTANZA PUNTO-RETTA: sia $r = P+\langle v\rangle$, allora

$$d(P_0, r) = \frac{\|(P-P_0)\times v\|}{\|v\|}$$

(interpretazione geometrica?).

4.8. ASSE DI UN SEGMENTO: si tratta del piano dei punti equidistanti dai due punti dati P_0 e P_1; si scrive $(\frac{1}{2}P_0 + \frac{1}{2}P_1) + \langle P_1 - P_0\rangle^{\perp}$, oppure tramite l'equazione:

$$(x_1 - x_0)\left(X - \frac{x_0 + x_1}{2}\right) + (y_1 - y_0)\left(Y - \frac{y_0 + y_1}{2}\right) + (z_1 - z_0)\left(Z - \frac{z_0 + z_1}{2}\right) = 0\ .$$

4.9. BISETTRICI DI DUE PIANI INCIDENTI: se abbiamo equazioni cartesiane $a_0X+b_0Y+c_0Z+d_0 = 0$ e $a_1X + b_1Y + c_1Z + d_1 = 0$ con $a_0^2 + b_0^2 + c_0^2 = a_1^2 + b_1^2 + c_1^2$ allora i piani bisettori hanno equazioni $(a_0X + b_0Y + c_0Z + d_0) \pm (a_1X + b_1Y + c_1Z + d_1) = 0$.

4.10. AREA DI TRIANGOLI: $A(P_0, P_1, P_2) = \frac{1}{2}\,\|(P_1-P_0)\times(P_2-P_0)\|$, e si esplicita come

$$\frac{1}{2}\sqrt{\det((P_i-P_0)\cdot(P_j-P_0))} = \frac{1}{2}\sqrt{\begin{vmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{vmatrix}^2 + \begin{vmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ z_0 & z_1 & z_2 \end{vmatrix}^2 + \begin{vmatrix} 1 & 1 & 1 \\ y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{vmatrix}^2}$$

ove le $\begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix}$ sono le coordinate di P_i in un riferimento ortonormale.

4.11. VOLUME DI TETRAEDRI:

$$V(P_0, P_1, P_2, P_3) = \tfrac{1}{6}|\det\begin{pmatrix} 1 & 1 & 1 & 1 \\ P_0 & P_1 & P_2 & P_3 \end{pmatrix}| = \tfrac{1}{6}|\begin{vmatrix} 1 & 1 & 1 & 1 \\ x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ z_0 & z_1 & z_2 & z_3 \end{vmatrix}|$$

ove le $\begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix}$ sono le coordinate di P_i in un riferimento ortonormale.

4.12. CONGRUENZE DELLO SPAZIO SECONDO EULERO. La scelta di un riferimento ortonormale sullo spazio $\mathbb{E}^3(\mathbb{R})$ determina un isomorfismo del gruppo $\mathrm{Rig}(\mathbb{A}^3(\mathbb{R}))$ delle rigidità dello spazio con il sottogruppo

$$\left\{\begin{pmatrix} 1 & 0\ 0\ 0 \\ \begin{matrix} a \\ b \\ c \end{matrix} & A \end{pmatrix} \mid a, b, c \in \mathbb{R};\ A \in \mathrm{GL}_3(\mathbb{R})\right\}$$

di $\mathrm{GL}_4(\mathbb{R})$. Tali rigidità si classificano nel modo seguente:

4.12.1. ROTAZIONI (DI ASSE UNA RETTA). Sono le rigidità dirette con (una retta di) punti uniti.

4.12.2. TRASLAZIONI. Sono rigidità dirette senza punti uniti.

4.12.3. ROTO-TRASLAZIONI O GLISSOROTAZIONI. Sono rigidità dirette senza punti uniti, composizioni di una rotazione di asse una retta e di una traslazione parallela all'asse.

4.12.4. RIFLESSIONI. Sono le rigidità inverse con (un piano di) punti uniti.

4.12.5. ROTO-RIFLESSIONI. Sono le rigidità inverse con un punto unito: composizione di una riflessione e di una rotazione di asse ortogonale al piano di riflessione.

4.12.6. GLISSORIFLESSIONI. Sono le rigidità inverse prive di punti uniti: composizione di una riflessione e di una traslazione di direzione parallela al piano di riflessione.

4.12.7. Anche questa classificazione si ottiene facilmente studiando le forme matriciali, oppure specializzando il teorema generale. Riassuntino schematico:

	dirette	*inverse*
c.p.f.	rotazioni (asse una retta) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & c\alpha & -s\alpha & 0 \\ 0 & s\alpha & c\alpha & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	riflessioni (asse un piano) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$ roto-riflessioni (unico punto fisso) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & c\alpha & -s\alpha & 0 \\ 0 & s\alpha & c\alpha & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
s.p.f.	glisso-rotazioni $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & c\alpha & -s\alpha & 0 \\ 0 & s\alpha & c\alpha & 0 \\ c & 0 & 0 & 1 \end{pmatrix}$ traslazioni $\begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & 0 & 1 & 0 \\ c & 0 & 0 & 1 \end{pmatrix}$	glisso-riflessioni $\begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

4.12.8. Che tipo di rigidità spaziale è la composizione di una rotazione e di una riflessione d'asse parallelo al piano di rotazione?

4.12.9. La composizione di due riflessioni è una rotazione o una traslazione: perché, e in quali casi?

4.12.10. Ogni rigidità diretta è composizione (non canonicamente) di riflessioni: come? In particolare ogni rigidità dello spazio è composizione di riflessioni.

4.12.11. Problema. Discutere in generale le composizioni dei vari tipi di rigidità tra di loro, distinguendo a seconda delle posizioni reciproche degli assi (di rotazione e/o riflessione) e delle traslazioni coinvolte...

Potrebbe essere utile fare alcune osservazioni preliminari, del tipo:

- se una rotazione di asse una retta manda un punto P in un altro punto Q, allora l'asse di rotazione giace sul piano che è asse del segmento tra P e Q.
- se una riflessione di asse un piano manda un punto P in un altro punto Q, allora il piano di riflessione è l'asse del segmento.

4.12.12. Problema. Capire da quanti parametri dipendono le rigidità di un certo tipo: per esempio per determinare una rotazione servono 5 parametri (4 per identificare la retta di rotazione, e 1 per l'angolo), mentre per determinare una glissorotazione ne servono 6, e per una traslazione ne servono 3. Nel caso di rigidità inverse: 3 parametri per una riflessione (servono per identificare il piano), 5 per una glissoriflessione, 6 per una rotoriflessione.

5. Spazio euclideo di dimensione quattro.

La stesura di questo paragrafo è un esercizio per il lettore: indichiamo solo le linee principali.

5.1. Questioni di distanze.

5.1.1. Distanze di punti da iperpiani, piani e rette.

5.1.2. Distanze di rette da iperpiani, piani e rette.

5.1.3. Distanze di piani da iperpiani e piani.

5.2. Questioni di angoli.

5.2.1. Angoli tra rette.

5.2.2. Angoli tra iperpiani.

5.2.3. Angoli tra rette e iperpiani.

5.2.4. Angoli tra piani e rette/piani/iperpiani? È possibile, e come, definire un angolo tra piani e iperpiani? È possibile, e come, definire un angolo tra piani e rette? Da quanti parametri dipende (modulo rigidità) la configurazione di due piani che si intersecano in un punto?

5.3. Congruenze secondo Eulero. Riassuntino schematico:

	dirette	*inverse*
c.p.f.	rotazioni (asse un piano) $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & c\alpha & -s\alpha & 0 & 0 \\ 0 & s\alpha & c\alpha & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ 2-rotazioni (unico punto fisso) $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & c\alpha & -s\alpha & 0 & 0 \\ 0 & s\alpha & c\alpha & 0 & 0 \\ 0 & 0 & 0 & c\beta & -s\beta \\ 0 & 0 & 0 & s\beta & c\beta \end{pmatrix}$	riflessioni (asse un iperpiano) $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$ roto-riflessioni (retta punti fissi) $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & c\alpha & -s\alpha & 0 & 0 \\ 0 & s\alpha & c\alpha & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$
s.p.f.	glisso-rotazioni $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & c\alpha & -s\alpha & 0 & 0 \\ 0 & s\alpha & c\alpha & 0 & 0 \\ c & 0 & 0 & 1 & 0 \\ d & 0 & 0 & 0 & 1 \end{pmatrix}$ traslazioni $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ a & 1 & 0 & 0 & 0 \\ b & 0 & 1 & 0 & 0 \\ c & 0 & 0 & 1 & 0 \\ d & 0 & 0 & 0 & 1 \end{pmatrix}$	glisso-roto-riflessioni $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & c\alpha & -s\alpha & 0 & 0 \\ 0 & s\alpha & c\alpha & 0 & 0 \\ c & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$ glisso-riflessioni $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ a & 1 & 0 & 0 & 0 \\ b & 0 & 1 & 0 & 0 \\ c & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$

6. Spazi Hermitiani.

6.1. Spazi Hermitiani. Uno spazio affine su $V_n(\mathbb{C})$, quest'ultimo dotato della struttura di spazio Hermitiano, permette una trattazione simile a quella fatta per gli Spazi Euclidei reali; lasciamo il compito al lettore, dicendo solo che questi spazi si dicono Euclidei Complessi o Spazi Hermitiani. L'applicazione biiettiva naturale $r : \mathbb{A}^n(\mathbb{C}) \longrightarrow \mathbb{A}^{2n}(\mathbb{R})$ risulta allora una isometria (cioè $d(P, P') = d(r(P), r(P'))$ per ogni $P, P' \in \mathbb{A}^n(\mathbb{C})$).

7. Esercizi.

7.1. Nel piano euclideo $\mathbb{E}^2(\mathbb{R})$ si considerino le tre rette r, s, t di equazioni rispettive

$$X + Y - 4 = 0, \qquad X + 5Y - 26 = 0, \qquad 15X - 27Y - 424 = 0.$$

(i) Si scrivano le equazioni delle rette n_r, n_s, n_t passanti per l'origine e normali a r, s, t, rispettivamente;
(ii) Si verifichi che i tre punti $r \cap n_r$, $s \cap n_s$, $t \cap n_t$ sono allineati.

7.2. Si considerino le rette $r, s \in \mathbb{E}^2(\mathbb{R})$ di equazioni $X + Y - 4 = 0$ e $3X + 2Y = 0$.
(i) Trovare le bisettrici dei quattro angoli formati da r, s ;
(ii) Individuare, tra le due, la bisettrice b dell'angolo più piccolo;
(iii) Per ogni punto $P \in b$, si indichino con P_r e P_s le sue proiezioni ortogonali su r ed s rispettivamente. Si calcoli l'applicazione di r in s che manda P_r in P_s.

7.3. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si considerino la retta r ed il piano α di equazioni rispettive $\frac{X-1}{2} = \frac{Y+1}{3} = \frac{Z-1}{4}$, $X+Y+Z-1 = 0$. Si trovino delle equazioni cartesiane della proiezione ortogonale di r su α.

7.4. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si considerino le rette r ed s di equazioni rispettive $X - 1 = Y, X + Y = Z$; $X = Z, X - Y = 2$.
(i) Trovare la retta n normale ad r ed s ed incidente sia r che s;
(ii) Trovare la distanza tra r ed s;
(iii) Sia P_z il punto di s la cui terza coordinata è z. Calcolare la distanza di P_z da r, in funzione di z.

7.5. Si trovino delle equazioni cartesiane delle rette dello spazio euclideo $\mathbb{E}^3(\mathbb{R})$, che passano per il punto $P = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, distano $1/\sqrt{2}$ dall'origine, e sono parellele al piano di equazione $X - Y + 7 = 0$.

7.6. Determinare le rette contenute nel piano di equazione $37X - 12Y + 41Z - 49 = 0$, che distano 2 ed 1 rispettivamente dalle rette r ed s di equazioni $X = 0, Y = 2$; $X = 3Y = 1$.

7.7. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si considerino quattro punti non complanari, a tre a tre non allineati P_1, P_2, P_3, P_4. Sia $P_i - P_1 = \begin{pmatrix} a_i \\ b_i \\ c_i \end{pmatrix}$, per $i = 2, 3, 4$.

(i) Si calcoli l'area del triangolo (P_1, P_2, P_3) in funzione di $a_1, b_1, c_1, a_2, b_2, c_2$.
(ii) Si calcoli il volume del tetraedro (P_1, P_2, P_3, P_4) in funzione delle coordinate dei vettori $P_i - P_1$;
(iii) Si supponga che sia $P_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$; si trovino le equazioni dei piani luogo dei punti P, tali che $\mathrm{Vol}(P_1, P_2, P_3, P_4) = \mathrm{Vol}(P_1, P_2, P_3, P)$.

7.8. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$, si considerino le rette $r : \begin{cases} x = 1 + t \\ y = 2 + t \\ z = -1 + 2t \end{cases}$, $s : \begin{cases} x = 2 + 2t \\ y = 3 + t \\ z = 1 + t \end{cases}$.

(a) Si mostri che r, s sono incidenti e si trovi un'equazione del piano che le contiene.
(b) Si trovino delle equazioni cartesiane delle rette passanti per $r \cap s$, parallele al piano di equazione $x + y + z = 0$, e formanti angoli uguali con r ed s.

7.9. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si considerino le rette di equazioni $r : \begin{cases} x - y = 0 \\ z = 2 \end{cases}$ $s : \begin{cases} x - y + z = 5 \\ 2x - y = 4 \end{cases}$.

(i) Trovare la retta n normale ad r ed s ed incidente sia r che s;
(ii) Trovare la distanza tra r ed s;
(iii) Sia P_t il punto di r la cui prima coordinata è t. Calcolare la distanza di P_t da s, in funzione di t;
(iv) Si scrivano le equazioni delle proiezioni ortogonali di r, s ed n sul piano passsante per l'origine, parallelo ad r e s.

7.10. Nello spazio euclideo standard $\mathbb{E}^3(\mathbb{R})$ si considerino i seguenti punti: $P = \begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}$, $Q = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$, $R = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$.

(a) Si scrivano le equazioni del luogo dei punti S di $\mathbb{E}^3(\mathbb{R})$ tali che il volume del tetraedro (non orientato) (P, Q, R, S) sia $1/\sqrt{6}$.
(b) Tra i punti S di cui in (a) si trovino quelli la cui proiezione ortogonale sul piano per P, Q, R è il baricentro del triangolo (P, Q, R).

7.11. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ è data la famiglia di rette r_t di equazioni $\begin{cases} X - Y + 2Z = t \\ 2X - 2tY - (1 + t)Z = 2 - 4t, \end{cases}$ al variare di t in $\mathbb{R}$.

(i) Si mostri che le rette r_t sono a due a due sghembe;
(ii) Si mostri che esiste una retta n incidente e normale a tutte le rette della famiglia;
(iii) Si trovi la distanza tra r_0 ed r_1.

7.12. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si consideri la retta r di equazioni $\begin{cases} x - y + z = 1 \\ 2x + y + z = -1. \end{cases}$

(a) Si scrivano le equazioni parametriche della retta s passante per l'origine, parallela al piano di equazione $x - y + z = 1$, ed ortogonale ad r.
(b) Si trovi la distanza tra r ed s.
(c) Si trovino un punto P su r ed un punto Q su s, tali che la distanza tra P e Q sia uguale alla distanza tra r ed s. Si mostri poi che P e Q sono unici.

7.13. Nello spazio euclideo standard $\mathbb{E}^3(\mathbb{R})$ si considerino la retta r di equazioni $\begin{cases} x - y + 2z = 0 \\ 2x - 2y - z = 0 \end{cases}$, il piano π di equazione $x + 2y + z = 1$ ed il punto P di coordinate $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$.

(a) Determinare le rette per P, parallele a π e complanari con r;
(b) Determinare i piani per P, paralleli a r ed aventi distanza 1 da essa;
(c) Determinare le rette per P, parallele a π, la cui distanza da r coincide con la distanza di P da r.

7.14. Nello spazio euclideo standard $\mathbb{E}^2(\mathbb{R})$ si considerino le rette r, s, t con le seguenti equazioni: $r : \begin{cases} x + 3y + z = 0 \\ x + y - z = 2 \end{cases}$, $s : \begin{cases} y + 2z = -1 \\ z = 0 \end{cases}$, $t : \begin{cases} 3x - y - z = 1 \\ x + y - z = -1 \end{cases}$.

(i) Si mostri che s incide sia r che t;
(ii) si ponga $T = t \cap s$ e si mostri che T è il punto di t che ha distanza minima da r;

(iii) siano R' il punto di r che ha distanza minima da t e $R = r \cap s$; determinare l'area del triangolo di vertici R, R', T.

7.15. Nello spazio euclideo standard $\mathbb{E}^3(\mathbb{R})$, ove è stato fissato il riferimento canonico, si considerino le rette r ed s di equazioni $\begin{cases} X+Y-Z &=0 \\ 2X-Y+Z &=0 \end{cases}$ e $\begin{cases} 3X-2Y-2Z &=0 \\ X-Y-3Z &=2 \end{cases}$.

(i) Si verifichi che r ed s sono sghembe.
(ii) Si trovi la distanza d di r da s.
(iii) Si trovi un punto P, tale che le sue distanze da r ed s siano $d/2$.

7.16. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ con riferimento canonico, si considerino le rette r, s di equazioni cartesiane $r : \begin{cases} x-y+z=1 \\ x-2z=1 \end{cases}$, $s : \begin{cases} x-y=-1 \\ x-z=1 \end{cases}$.

(a) Si trovino delle equazioni cartesiane di tutte le rette complanari con r ed s ed incidenti l'asse z;
(b) Si indichi con r_k la retta della famiglia di cui al punto (a) che passa per il punto di coordinate $(0,0,k)$; si chiede se esistono dei k per i quali r_k sia ortogonale ad uno degli assi coordinati.

7.17. Nello spazio euclideo tridimensionale si consideri la retta r per $P = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, e direzione $v = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$.

(a) si scriva l'equazione cartesiana del cilindro $\mathscr{C}$ formato dai punti che distano 1 da r.
(b) Si determinino i punti di intersezione di $\mathscr{C}$ con i tre assi coordinati.
(c) Si calcoli il volume del tetraedro definito dai punti trovati in (b).

7.18. Nello spazio euclideo tridimensionale si consideri la retta r per $P = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ e direzione $v = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$.

(a) Scrivere l'equazione cartesiana del cono $\mathscr{C}$, di asse r, vertice P e semiapertura $\frac{\pi}{3}$.
(b) Trovare i punti di intersezione, Q_1 e Q_2, tra $\mathscr{C}$ e la retta s per $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ e direzione $\begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}$.
(c) trovare l'equazione del piano π contenente s e perpendicolare ad r; sia $R = \pi \cap r$.
(d) Si calcoli il volume del tetraedro di vertici P, Q_1, Q_2, R.

7.19. Determinare centro e angolo della rotazione di $\mathbb{E}^2_{\mathbb{R}}$ avente matrice $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1/2 & -\sqrt{3}/2 \\ 2 & \sqrt{3}/2 & 1/2 \end{pmatrix}$.

7.20. Trovare la matrice della rotazione di $\mathbb{E}^2_{\mathbb{R}}$ di centro $(1,1)$ e angolo $-\pi/4$.

7.21.

(1) Sia $\varphi : \mathbb{E}^3_{\mathbb{R}} \to \mathbb{E}^3_{\mathbb{R}}$ una rotazione (attorno ad un asse r); trovare delle condizioni necessarie e sufficienti affinché $t \circ \varphi$ sia ancora una rotazione (ove t è una traslazione).
(2) Mostrare che ogni isometria di $\mathbb{E}^3_{\mathbb{R}}$ in sè che conserva l'orientamento è del tipo $t \circ \varrho$ ove ϱ è una rotazione e t è una traslazione parallela all'asse di ϱ. È vero che t e ϱ commutano tra loro?
(3) descrivere con un disegno la traiettoria del punto $(1,0,0)$ sotto l'azione di $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\vartheta & -\sin\vartheta & 0 \\ 0 & \sin\vartheta & \cos\vartheta & 0 \\ \vartheta & 0 & 0 & 1 \end{pmatrix}$ al variare di $\vartheta \in \mathbb{R}$.

7.22. Studiare la isometria di matrice $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ -1 & 0 & 0 & 1 \\ -1 & -1 & 0 & 0 \end{pmatrix}$.

7.23. Sia φ la isometria di $\mathbb{E}^3_{\mathbb{R}}$ data dalla composizione della rotazione di angolo $\pi/2$ e asse la retta per $P = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$ e direzione $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ con la traslazione di vettore $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$.

(1) vero che φ è una rotazione?
(2) si calcoli la matrice di φ nel riferimento dato.
(3) scrivere φ come composizione di una rotazione (in particolare determinare l'asse) seguita da una traslazione parallela all'asse.

7.24. La simmetria di $\mathbb{E}^3_{\mathbb{R}}$ di asse una retta r e direzione ortogonale è una isometria che conserva l'orientamento? È vero che si tratta di una rotazione?

Normalmente si dice che "lo specchio scambia la (mano) sinistra con la destra". Che senso ha?

Le composizioni di due riflessioni speculari (simmetrie rispetto ad un piano nella direzione ortogonale al piano) conservano l'orientamento di $\mathbb{E}^3_{\mathbb{R}}$. Di che isometrie si tratta?

7.25. Due rette r, s di $\mathbb{E}^3_{\mathbb{R}}$ si specchiano sul piano $\pi:\ x+y+z=1$. La prima retta ha equazioni $x-3y=3$ e $2y-z=2$, mentre la riflessione della seconda è $\sigma(s):\begin{pmatrix}1\\-1\\1\end{pmatrix}+\langle\begin{pmatrix}0\\1\\-1\end{pmatrix}\rangle$.

(1) r ed s si incontrano?
(2) $\sigma(r)$ ed s si intersecano?
eventualmente trovare i punti di intersezione.

7.26. Una isometria φ di $\mathbb{E}^3(\mathbb{R})$ si rappresenta tramite la matrice $\begin{pmatrix}1&0&0&0\\1&1/2&0&-\sqrt{3}/2\\1&0&1&0\\1&\sqrt{3}/2&0&1/2\end{pmatrix}$ nel riferimento canonico.

(i) dire se è una isometria diretta;
(ii) dire se è una rotazione (di asse una retta);
(iii) scrivere φ come composizione di una rotazione ϱ seguita da una traslazione τ di direzione parallela all'asse di rotazione ($\varphi=\tau\circ\varrho$); in particolare si determini una espressione cartesiana per l'asse della rotazione ϱ.
(iv) è vero che τ e ϱ commutano tra di loro? È vero che φ si può scrivere anche come composizione $\varrho\circ\tau'$ ove τ' è una traslazione di direzione parallela all'asse di ϱ?

7.27. Come il precedente esercizio, usando la matrice $\begin{pmatrix}1&0&0&0\\2&0&0&-1\\1&1&0&0\\0&0&-1&0\end{pmatrix}$

7.28. Consideriamo il piano π di $\mathbb{E}^3(\mathbb{R})$ di equazione $X+Y+Z=3$.

(a) Si determini la matrice nel riferimento canonico della riflessione ortogonale s di asse π.
(b) Si componga s con la traslazione di vettore $\begin{pmatrix}1\\0\\1\end{pmatrix}$, e si descriva tale composizione s' come glisso-riflessione (riflessione di asse π' seguita da traslazione parallela all'asse).
(c) Si determini l'antimmagine tramite s' dei vertici del tertraedro fondamentale di $\mathbb{E}^3(\mathbb{R})$.
($d*$) Che rigidità sono le composizioni $s\circ s'$ e $s'\circ s$? Sono uguali?

7.29. Consideriamo la retta r di $\mathbb{E}^3(\mathbb{R})$ data da $\begin{pmatrix}1\\2\\3\end{pmatrix}+\langle\begin{pmatrix}1\\1\\1\end{pmatrix}\rangle$.

(a) Si determini la matrice nel riferimento canonico della rotazione ortogonale ϱ di angolo $\pi/2$ attorno ad r.
(b) Si componga ϱ con la traslazione di vettore $\begin{pmatrix}1\\0\\1\end{pmatrix}$, e si descriva tale composizione ϱ' come glisso-rotazione (rotazione di asse r' seguita da traslazione parallela all'asse).
(c) Si determini l'antimmagine tramite ϱ dei vertici del tertraedro fondamentale di $\mathbb{E}^3(\mathbb{R})$.
($d*$) Che rigidità sono le composizioni $\varrho\circ\varrho'$ e $\varrho'\circ\varrho$? Sono uguali?

7.30. Consideriamo i piani di $\mathbb{E}^3(\mathbb{R})$ dati da $\pi_1: X_1-X_2=1$ e $\pi_2: X_3=0$.

(a) Si determini la matrice nel riferimento canonico della composizione s delle riflessioni ortogonali di assi π_1 e π_2 rispettivamente.
(b) Si determinino i punti uniti di s; che tipo di rigidità è?
(c) Si determinino i piani uniti di s.

7.31. Consideriamo in $\mathbb{E}^3(\mathbb{R})$ il piano π passante per il punto $\begin{pmatrix}1\\1\\1\end{pmatrix}$ e ortogonale al vettore $\begin{pmatrix}1\\0\\1\end{pmatrix}$, e la retta r passante per il punto $\begin{pmatrix}2\\1\\0\end{pmatrix}$ e di direzione data dal vettore $\begin{pmatrix}1\\1\\-1\end{pmatrix}$.

(a) Trovare la matrice nel riferimento canonico della riflessione ortogonale σ di asse π.
(b) Trovare la matrice nel riferimento canonico della rotazione ϱ di angolo 180° e asse r.
(c) Determinare e classificare (come isometrie dello spazio) le due composizioni $\sigma\circ\varrho$ e $\varrho\circ\sigma$.

7.32. Consideriamo in $\mathbb{E}^3(\mathbb{R})$ il piano π passante per il punto $\begin{pmatrix}1\\2\\3\end{pmatrix}$ e ortogonale al vettore $\begin{pmatrix}1\\1\\1\end{pmatrix}$.

(a) Trovare la matrice nel riferimento canonico della riflessione ortogonale σ di asse π.
(b) Trovare la matrice nel riferimento canonico della composizione σ' di σ con la traslazione di vettore $\begin{pmatrix}1\\2\\0\end{pmatrix}$, e decomporre σ' come glisso-riflessione (riflessione di asse π' seguita da una traslazione parallela all'asse).
(c) Determinare le antimmagini tramite σ' dei vertici del tetraedro fondamentale di $\mathbb{E}^3(\mathbb{R})$.

7.33. Nello spazio euclideo $\mathbb{R}^4$, si considerino i piani $\sigma_1 : \begin{cases} x_1 - x_3 = 2 \\ x_2 + 2x_4 = -1 \end{cases}$, $\sigma_2 : \begin{cases} x_1 + 2x_4 = 0 \\ x_2 + x_3 = 1 \end{cases}$ e la retta $r : \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_2 - x_3 = -1 \\ x_1 + 2x_2 - 2x_4 = 0 \end{cases}$.

(a) Si mostri che σ_1 e σ_2 hanno in comune un unico punto P e si determinino le coordinate di tale punto.
(b) Si mostri che la retta r interseca entrambo i piani e si determinino le coordinate dei punti $Q_1 = r \cap \sigma_1$ e $Q_2 = r \cap \sigma_2$.
(c) Si determinino il baricentro G e l'area del triangolo PQ_1Q_2.
(d) Si scrivano le equazioni cartesiane del piano π, passante per G e perpendicolare al piano contenente il triangolo PQ_1Q_2.

7.34. Si considerino nello spazio euclideo $\mathbb{E}^4(\mathbb{R})$ il piano π di equazioni $\begin{cases} X_1 - X_2 + X_3 = 1 \\ X_4 = 3 \end{cases}$ e le rette $r_1 : \begin{pmatrix} 1 \\ 1 \\ 0 \\ 4 \end{pmatrix} + \langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \rangle$, $r_2 : \begin{cases} X_1 - X_2 = 1 \\ X_3 = 3 \\ X_2 - X_4 = 0. \end{cases}$

(a) Discutere le posizioni reciproche a due a due di π, r_1, r_2.
(b) Determinare distanza e punti di minima distanza tra π e r_1 (siano P_1, R_1) e tra π e r_2 (siano P_2, R_2).
(c) Determinare il volume del tetraedro formato dai quattro punti P_1, P_2, R_1, R_2, e l'area dei triangoli di vertici P_1, P_2, R_1 e P_1, R_1, R_2.
($d*$) Sia $S = r_1 \vee r_2$ (minimo sottospazio affine contenente le due rette); determinare S e discuterne la posizione reciproca con π.

7.35. Si considerino nello spazio euclideo $\mathbb{E}^4(\mathbb{R})$ il piano π_1 di equazioni $\begin{cases} X_1 - X_2 = 1 \\ X_1 - X_3 = 2 \end{cases}$, il piano $\pi_2 : \begin{pmatrix} 2 \\ 2 \\ 2 \\ 2 \end{pmatrix} + \langle \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ -1 \end{pmatrix} \rangle$ e la retta $r : \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \rangle$.

(a) Discutere le posizioni reciproche a due a due di π_1, π_2, r.
(b) Determinare distanza e punti di minima distanza tra π_1 e r (siano P_1, R_1) e tra π_2 e r (siano P_2, R_2).
(c) Determinare il volume del tetraedro formato dai quattro punti P_1, P_2, R_1, R_2, e l'area dei triangoli di vertici P_1, P_2, R_1 e P_1, R_1, R_2.
($d*$) Discutere la posizione reciproca di $\pi_1 \vee R_1$ con $\pi_2 \vee R_2$; è vero o falso che la loro intersezione contiene la retta r?

7.36. Si considerino nello spazio euclideo $\mathbb{E}^4(\mathbb{R})$ i piani
$\pi_1 : \begin{cases} X_1 + X_2 = 0 \\ X_2 + X_3 = 1 \end{cases}$, $\pi_2 : \begin{cases} X_3 + X_4 = 0 \\ X_4 = -1 \end{cases}$, $\pi_3 : \begin{cases} X_1 + X_2 + X_3 + X_4 = 1 \\ X_2 + X_3 + X_4 = 0 \end{cases}$,

(a) Calcolare i punti di intersezione $P_1 = \pi_2 \cap \pi_3$, $P_2 = \pi_1 \cap \pi_3$, $P_3 = \pi_1 \cap \pi_2$ ed equazioni cartesiane per i sottospazi $\pi_i \vee P_i$ $(i = 1, 2, 3)$.
(b) Determinare le equazioni del piano passante per il baricentro del triangolo P_1, P_2, P_3 e di spazio direttore ortogonale a quello del piano contenente il triangolo.
(c) Calcolare l'area del triangolo di vertici P_1, P_2, P_3, e determinare l'insieme dei punti $X \in \mathbb{E}^4(\mathbb{R})$ tali che il tetraedro P_1, P_2, P_3, X abbia volume 6.

7.37. Si considerino nello spazio euclideo $\mathbb{E}^4(\mathbb{R})$ le rette
$r_1 = \begin{pmatrix} 2 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \langle \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \rangle$, $r_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \langle \begin{pmatrix} -1 \\ -1 \\ 0 \\ -1 \end{pmatrix} \rangle$, $r_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ -1 \end{pmatrix} + \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 3 \end{pmatrix} \rangle$.

(a) Determinare equazioni cartesiane delle tre rette.
(b) Discutere la posizione reciproca a due a due delle tre rette. Esiste un sottospazio affine di dimensione 3 di $\mathbb{E}^4(\mathbb{R})$ contenente le tre rette date?
(c) Determinare le distanze reciproche tra le tre rette.

7.38. Si considerino nello spazio euclideo $\mathbb{E}^4(\mathbb{R})$ le rette
$r_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \rangle$, $r_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \langle \begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix} \rangle$, e il piano $\pi : \begin{cases} X_2 - X_3 = 0 \\ X_2 - X_4 = 0 \end{cases}$.

(a) Determinare equazioni cartesiane delle due rette ed espressioni vettoriali per π.
(b) Discutere la posizione reciproca delle due rette, calcolandone la distanza e i punti di minima distanza.
(c) Determinare le posizioni reciproche tra ciascuna retta e il piano π, specificandone la distanza. Esiste un sottospazio affine di dimensione 3 contenente le due rette e il piano?

Capitolo IX

Geometria Proiettiva

Questo è uno dei capitoli principali del corso dal punto di vista della Geometria: la nozione di spazio proiettivo (e di trasformazioni proiettive) è quella che permette di dare una visione unificante e d'insieme per le geometrie affini e euclidee (mettendone bene in luce le strutture), e al contempo farà da ambiente per altri tipi di geometrie, in futuri capitoli.

Come al solito, il nostro punto di vista sarà algebrico e non assiomatico: introdurre in modo assiomatico la geometria proiettiva è nettamente meno intuitivo che per la geometria euclidea, e quindi molto più difficile da gestire. Vedremo invece che l'algebra lineare si rivela un strumento prezioso, che al contempo permette di introdurre importanti nozioni geometriche e a sua volta viene chiarificato e giustificato dal significato geometrico che riesce a veicolare.

In questo capitolo si noterà una certa interdipendenza tra i paragrafi: verranno usati degli strumenti prima d'averli introdotti, e altre amenità dello stesso tipo. Non credo vi sia alcun circolo vizioso, solo le cose si presentavano così, e così ho preferito lasciarle piuttosto che spezzare dei discorsi unitari per riprenderli dopo aver introdotto qualche concetto a cui andava dedicato un paragrafo. Il consiglio è di guardare le definizioni anche dei paragrafi successivi quando servono, oppure di saltare in prima lettura quando si trovano termini sconosciuti.

0. Motivazioni.

0.1. Grassmann e parallelismo. In uno spazio vettoriale V su un corpo $\Bbbk$, e per due suoi sottospazi U e W vale la formula di Grassmann che dà una relazione tra le dimensioni:

$$\dim U + \dim W = \dim(U + W) + \dim(U \cap W) \ .$$

Viceversa in uno spazio affine $\mathbb{A}(V)$ di spazio direttore V, e per due sottovarietà affini lineari $\mathbb{L}$ ed $\mathbb{M}$ vale in generale solo la relazione

$$\dim \mathbb{L} + \dim \mathbb{M} \geqslant \dim(\mathbb{L} \vee \mathbb{M}) + \dim(\mathbb{L} \cap \mathbb{M})$$

e l'uguaglianza vale se e solo se $\mathbb{L}$ ed $\mathbb{M}$ sono incidenti oppure sghembe. In generale l'uguaglianza viene rovinata dai fenomeni di parallelismo che si presentano negli spazi affini: due sottovarietà possono avere delle direzioni comuni, pur essendo disgiunte. Se $\mathbb{L}$ ed $\mathbb{M}$ sono disgiunte, ma non necessariamente sghembe, e supponiamo che U e W ne siano i rispettivi spazi direttori, allora vale la relazione

$$\dim \mathbb{L} + \dim \mathbb{M} = \dim(\mathbb{L} \vee \mathbb{M}) + \dim(U \cap W) - 1 \ .$$

Il termine $\dim(U \cap W) - 1$ rappresenta in qualche senso la dimensione di una intersezione "all'infinito" tra $\mathbb{L}$ ed $\mathbb{M}$; come quando si dice che i binari del treno "si incontrano in un punto all'infinito": trattandosi di due rette (dimensione 1) parallele, hanno in comune un punto (dimensione 0) all'infinito, la loro "direzione".

Questo suggerisce che lo spazio affine debba essere "immerso" in un oggetto più grande che comprenda anche dei punti all'infinito, che si otterrà dallo spazio affine aggiungendo per ogni classe di rette parallele un punto all'infinito, da interpretare come il punto comune a tutte quelle rette. È quello che faremo, usando il punto di vista dell'algebra lineare, che si rivela estremamente utile per questo scopo.

In realtà preferiamo definire lo spazio proiettivo completo, un ambiente più grande di quello appena delineato, e dotato di una struttura molto più ricca, di cui lo spazio proiettivo "punteggiato" sopra descritto sarà un sottinsieme. Un risultato importante e particolarmente elegante che seguirà da questo approccio, è il teorema di dualità proiettiva.

0.2. Omogeneizzazione di sistemi lineari. Algebricamente, il problema deriva dal fatto che un sistema lineare non omogeneo $AX = b$ (quello della intersezione tra varietà affini) può non

ammettere alcuna soluzione anche se il sistema omogeneo $AX = 0$ ammette soluzioni non banali (ciò succede esattamente, secondo Rouché-Capelli, quando il rango completo supera quello incompleto). Questo suggerisce di considerare il sistema "omogeneizzato" $AX = bX_0$ (ove X_0 è una nuova variabile). Questo sistema, essendo omogeneo, ha sempre soluzioni (almeno quella banale), e l'insieme delle soluzioni è un sottospazio di $\Bbbk^{n+1}$. Chiaramente per $X_0 = 1$ troviamo le eventuali soluzioni del sistema originario, per $X_0 = 0$ troviamo le soluzioni del sistema omogeneo associato, e le soluzioni del sistema omogeneizzato sono date dal sottospazio vettoriale di $\Bbbk^{n+1}$ generato dall'insieme dei vettori $\binom{1}{x}$ con $Ax = b$ (soluzioni del sistema originario). Più precisamente, l'insieme delle soluzioni del sistema omogeneizzato è unione "disgiunta a parte 0" di due tipi di "rette":
(1) $\langle\binom{1}{x}\rangle$ con $Ax = b$ (soluzioni del sistema originario);
(2) $\langle\binom{0}{y}\rangle$ con $Ay = 0$ (soluzioni del sistema omogeneo associato);
ed inoltre è facile vedere che le soluzioni del secondo tipo vanno considerate come "limiti" di soluzioni del primo tipo. Infatti: anche tutte le $x+\alpha y$ con $\alpha \in \Bbbk$ sono soluzioni del sistema $AX = b$, e lo spazio $\langle\binom{1}{x} + \alpha\binom{0}{y}\rangle = \langle\frac{1}{\alpha}\binom{1}{x} + \binom{0}{y}\rangle$ "tende a" $\langle\binom{0}{y}\rangle$ quando α diventa "grande".

Morale: omogenizzare il sistema porta ad avere una "coordinata in più", le soluzioni dei sistemi si presentano come insiemi di "sottospazi vettoriali di dimensione uno" piuttosto che punti, riconosciamo le soluzioni del sistema originale dall'avere non nulla la coordinata aggiunta, ma otteniamo come nuove soluzioni quelle con coordinata aggiunta nulla: esse rappresentano per la varietà affine di partenza le direzioni dello spazio direttore, e noi siamo interessati a trattarli come "punti all'infinito", limiti dei punti affini.

0.3. Proiezioni di centro affine. Parlando di Geometria Affine, abbiamo introdotto le proiezioni dall'infinito (essenzialmente mutuate dalle proiezioni vettoriali di un sottospazio nella direzione di un suo complementare): si tratta di trasformazioni affini. Abbiamo solo accennato a proiezioni con centro affine (applicazioni che mandano un generico punto X nella intersezione di $X \vee P$ con un opportuno schermo, per un opportuno centro P, schermo e centro essendo sottospazi affini), essenzialmente perché non sono trasformazioni affini: in primo luogo non sono definite per tutti i punti (il sottospazio passante per P e parallelo allo schermo non ha immagine: di nuovo un problema di parallelismo), in secondo luogo una espressione in coordinate comporta dei denominatori, e quindi non danno funzioni lineari (ma lineari fratte, in effetti: verificare).

Non sarà una grande sorpresa capire che l'ambiente in cui queste funzioni sono ben definite è proprio quello della Geometria Proiettiva. Sarà invece di grande interesse capire quali invarianti sono rispettati da questo tipo di trasformazioni: per esempio le trasformazioni affini reali non rispettano in generale le lunghezze euclidee, ma rispettano il rapporto semplice, che si può pensare come rapporto di lunghezze euclidee. In generale le trasformazioni proiettive (tipo le proiezioni) non rispetteranno nemmeno tali rapporti (segmenti di lunghezza uguale su una strada sono "proiettati" in segmenti di lunghezze diverse su una tela da un pittore), ma una più complicata struttura (birapporti).

1. Spazi Proiettivi.

Sia V uno spazio vettoriale di dimensione finita su un corpo $\Bbbk$.

1.1. Definizione (Spazio proiettivo completo associato a V). *Lo spazio proiettivo completo associato a V è l'insieme*

$$\mathbb{S}(V) := \{W \ : \ W \leqslant V\}$$

di tutti i sottospazi di V, dotato delle operazioni di intersezione e somma di sottospazi e l'ordine dell'inclusione. Queste operazioni rendono $\mathbb{S}(V)$ un reticolo, cioè un insieme parzialmente ordinato (tramite la relazione di inclusione) dotato due operazioni binarie di minimo (l'intersezione di sottospazi) e massimo (la somma di sottospazi) e in cui per ogni sottinsieme esistono gli estremi inferiori e superiori (rispettivamente l'intersezione e la somma di tutti i suoi elementi). In particolare $\{0\}$ è l'elemento infimo (e si dice il vuoto proiettivo), e V stesso è l'elemento supremo del reticolo.

1.1.1. Elenchiamo alcune facili osservazioni; siano $W_i \in \mathbb{S}(V)$.
(*a*) $W_1 \subseteq W_2$ se e solo se $W_1 + W_2 = W_2$ se e solo se $W_1 \cap W_2 = W_1$;
(*b*) $(W_1 + W_2) \cap W_3 \supseteq (W_1 \cap W_3) + (W_2 \cap W_3)$, ma in generale non sono uguali;
(*c*) $(W_1 \cap W_2) + W_3 \subseteq (W_1 + W_3) \cap (W_2 + W_3)$, ma in generale non sono uguali.

Le ultime due osservazioni dicono che il reticolo $\mathbb{S}(V)$ *non* è distributivo (contrariamente al reticolo della potenza di un insieme, i.e. il reticolo dei sottinsiemi d'un insieme dato).

1.1.2. Spazi proiettivi punteggiati e fogli(eggi)ati associati a V. L'interesse della definizione di spazio proiettivo completo consiste nella sua struttura di reticolo. Definiamo comunque anche due suoi sottinsiemi: lo spazio proiettivo punteggiato, (risp. lo spazio proiettivo fogliato) associato a V è l'insieme

$$\mathbb{P}(V) := \{W \ : \ W \leqslant V, \ \dim_{\Bbbk} W = 1\} \qquad (\text{risp.} \quad \mathbb{I}(V) := \{W \ : \ W \leqslant V, \ \dim_{\Bbbk} W = \dim_{\Bbbk} V - 1\} \ )$$

delle rette (risp. degli iperpiani) di V. Questi insiemi non hanno struttura di reticolo, ma ogni elemento W di $\mathbb{S}(V)$ può essere identificato con la collezione di elementi di $\mathbb{P}(V)$ contenuti in W (risp. la collezione di elementi di $\mathbb{I}(V)$ contenenti W).

1.2. Definizione (Sottospazi e stelle). *Sia W un sottospazio vettoriale di V. L'insieme $\mathbb{S}(W) \subseteq \mathbb{S}(V)$ si dice il sottoreticolo completo (o sottospazio proiettivo completo) di sostegno W di $\mathbb{S}(V)$, mentre $\mathbb{P}(W) \subseteq \mathbb{P}(V)$ si dice il sottospazio proiettivo punteggiato di sostegno W.*

L'insieme $\mathbb{S}(V/W) \cong \{W' \in \mathbb{S}(V) \ : \ W \leqslant W'\} \subseteq \mathbb{S}(V)$ si dice la stella (proiettiva) completa di asse W, mentre $\mathbb{I}(V/W) \cong \{W' \in \mathbb{I}(V) \ : \ W \leqslant W'\} \subseteq \mathbb{I}(V)$ si dice la stella di iperpiani di asse W.

Vogliamo vedere come la dualità degli spazi vettoriali si traduce nel contesto degli spazi proiettivi completi:

1.3. Proposizione. *Sia $V^* := \mathrm{Hom}_{\Bbbk}(V, \Bbbk)$ lo spazio vettoriale duale di V. La dualità canonica tra V e V^* (la forma bilineare che manda la coppia (v, v^*) in $v^*(v) \in \Bbbk$) induce un antiisomorfismo di reticoli*

$$\tau_V : \mathbb{S}(V) \longrightarrow \mathbb{S}(V^*)$$

dato da $\tau_V(W) := W^{\perp}$. Inoltre per ogni $W \in \mathbb{S}(V)$ il morfismo τ_V induce un antiisomorfismo

$$\mathbb{S}(V/W) \longrightarrow \mathbb{S}(W^{\perp}) \cong \mathbb{S}((V/W)^*) \ ;$$

dunque la dualità τ_V scambia sottospazi di $\mathbb{S}(V^*)$ con stelle di $\mathbb{S}(V)$ (e viceversa).

Dimostrazione. Antiisomorfismo di reticoli significa che si tratta di una biiezione insiemistica che rovescia la struttura d'ordine del reticolo, cioè scambia infimo e supremo, rovescia le inclusioni, scambia estremi inferiori e superiori. Tutte queste proprietà sono ben note per la corrispondenza data dall'ortogonale per la dualità standard. Anche l'ultima asserzione deriva da fatti noti della dualità. □

1.4. Lo spazio proiettivo standard. Lo spazio proiettivo standard di dimensione n su $\Bbbk$ è lo spazio proiettivo associato allo spazio vettoriale standard su $\Bbbk$ di dimensione $n+1$; dunque $\mathbb{S}^n(\Bbbk) := \mathbb{S}(\Bbbk^{n+1})$. Lo spazio proiettivo punteggiato associato è formato dalle rette di $\Bbbk^{n+1}$ (come spazio vettoriale), e quindi può essere identificato con l'insieme quoziente dei suoi vettori non nulli

modulo la relazione di equivalenza data dalla proporzionalità (due vettori determinano la stessa retta vettoriale se e solo se sono proporzionali): $\mathbb{P}^n(\Bbbk) := (\Bbbk^{n+1} \smallsetminus \{0\})/\Bbbk^\times$, tramite la biiezione

$$\alpha : \mathbb{P}(\Bbbk^{n+1}) \longrightarrow \mathbb{P}^n(\Bbbk)$$

che manda ogni sottospazio $\langle v \rangle$ nella classe di equivalenza $[v]$ di un generatore.

I punti di $\mathbb{P}^n(\Bbbk)$ possono essere divisi in due sottinsiemi disgiunti: quelli con prima coordinata X_0 non nulla, e allora possono essere rappresentati unicamente da un vettore con $X_0 = 1$ (dividendo per X_0), e quelli con $X_0 = 0$, e in questo caso le altre coordinate sono ancora definite a meno di una costante moltiplicativa non nulla. Quindi vediamo che

$$\mathbb{P}^n(\Bbbk) = \{\begin{pmatrix} 1 \\ X \end{pmatrix} : X \in \Bbbk^n\} \sqcup \{\langle \begin{pmatrix} 0 \\ X \end{pmatrix} \rangle : X \in \Bbbk^n\} \cong \mathbb{A}^n(\Bbbk) \sqcup \mathbb{P}^{n-1}(\Bbbk)$$

ovvero lo spazio proiettivo standard è unione disgiunta di uno spazio affine della stessa dimensione e di uno spazio proiettivo di dimensione diminuita di 1, che ha il significato geometrico di contenere le direzioni delle rette dello spazio affine. In altri termini: per ogni famiglia di rette parallele viene aggiunto un punto da considerare come punto comune a tutte quelle rette.

In particolare una retta proiettiva si ottiene aggiungendo un punto ad una retta affine (l'unico punto all'infinito di quella retta affine!), e un piano proiettivo si ottiene aggiungendo una retta proiettiva ad un piano affine (i punti della retta proiettiva rappresentano le direzioni delle rette affini di un qualunque fascio improprio; rette parallele nell'affine condividono lo stesso punto all'infinito). Si può osservare subito, quindi, che il prodotto cartesiano di due rette proiettive non è nemmeno in biiezione con il piano proiettivo, nonostante entrambi contengano un piano affine (prodotto cartesiano di due rette affini).

In un certo senso gli spazi proiettivi sono le stelle di 0 in uno spazio vettoriale (di dimensione uno di più), e in questo senso sono già stati incontrati all'interno della geometria affine ogniqualvolta si parlava di fasci, stelle, ecc. di sottospazi affini (per descrivere i quali bisogna in effetti usare parametri omogenei definiti a meno di costanti moltiplicative non nulle, oppure perdere qualche sottospazio...).

1.5. Definizione (Spazio proiettivo). *Un insieme $\mathbb{S}$ dotato di una biiezione*

$$\alpha = \alpha_{\mathbb{S}} : \mathbb{S}(V) \longrightarrow \mathbb{S}$$

si dice uno spazio proiettivo completo di spazio vettoriale sovrastante V. Si solito si indica con $\mathbb{S}$ tutta la terna $(\mathbb{S}, V, \alpha_{\mathbb{S}})$. Per trasporto di struttura tramite la biiezione α, $\mathbb{S}$ risulta munito di una struttura di reticolo: indichiamo con $\leqslant$ la relazione d'ordine (dunque $\alpha(W_1) \leqslant \alpha(W_2)$ se e solo se $W_1 \subseteq W_2$) con $\wedge$ l'operazione di inf (dunque $\alpha(W_1) \wedge \alpha(W_2) = \alpha(W_1 \cap W_2)$) e con $\vee$ l'operazione di sup (dunque $\alpha(W_1) \vee \alpha(W_2) = \alpha(W_1 + W_2)$).

La dimensione di $\mathbb{S}$ *è per definizione* $\dim_{\mathbb{S}} \mathbb{S} := \dim_{\Bbbk} V - 1$*; per ogni* $s = \alpha(W) \in \mathbb{S}$*, la sua dimensione è definita da* $\dim_{\mathbb{S}} s := \dim_{\Bbbk} W - 1$*. Gli elementi di* $\mathbb{S}$ *di dimensioni* -1, 0, 1, 2, $\dim_{\mathbb{S}} \mathbb{S} - 1$ *si dicono rispettivamente vuoto (proiettivo), punti, rette, piani, iperpiani di* $\mathbb{S}$*.*

Il sottinsieme $\mathbb{P} = \{s \in \mathbb{S} \ : \ \dim_{\mathbb{S}} s = 0\}$ *si dice lo spazio proiettivo punteggiato associato ad* $\mathbb{S}$*, ed è in biiezione con* $\mathbb{P}(V)$*; il sottinsieme* $\mathbb{I} = \{s \in \mathbb{S} \ : \ \dim_{\mathbb{S}} s = \dim \mathbb{S} - 1\}$ *si dice lo spazio proiettivo fogliato associato ad* $\mathbb{S}$*, ed è in biiezione con* $\mathbb{I}(V)$*.*

1.5.1. Per esempio, la dimensione dello spazio proiettivo completo associato a V è $\dim_{\mathbb{S}(V)} \mathbb{S}(V) := \dim_{\Bbbk}(V) - 1$, e la dimensione di $W \in \mathbb{S}(V)$ è $\dim_{\mathbb{S}(V)} W := \dim \mathbb{S}(W) = \dim_{\Bbbk}(W) - 1$. Dunque i punti di $\mathbb{S}(V)$ sono i sottospazi di dimensione 1 di V. Il vuoto proiettivo è il sottospazio $\langle 0 \rangle$, si può indicare con $\varnothing_{\mathbb{S}}$ (ma non è l'insieme vuoto), e ha dimensione $\dim_{\mathbb{S}} \varnothing_{\mathbb{S}} = -1$ (ed è l'unico di dimensione -1).

1.5.2. Sottospazi e Stelle. Un sottinsieme L di uno spazio proiettivo punteggiato $\mathbb{P}$ (con α da $\mathbb{P}(V)$) si dice una varietà proiettiva (lineare) se è immagine tramite α di un insieme del tipo $\mathbb{P}(W)$ per un sottospazio W di V; ciò vale se e solo se per ogni coppia di suoi punti contiene la retta che li congiunge.

Allo stesso modo si definiscono le stelle per trasporto di struttura da $\mathbb{P}(V)$: esplicitare.

1.5.3. La definizione di spazio proiettivo può sembrare inutilmente complicata dal fatto di prendere un insieme in biiezione con un $\mathbb{P}(V)$, invece che $\mathbb{P}(V)$ stesso. Il punto è che molto spesso capitano insiemi con struttura di spazio proiettivo che non sono essi stessi associati a spazi vettoriali naturali: per esempio un fascio di rette di centro un punto di un piano affine è una retta proiettiva, ma vi è solo una identificazione naturale con qualche spazio proiettivo associato a uno spazio vettoriale. Allo stesso modo, mentre un sottospazio proiettivo di $\mathbb{P}(V)$ si presenta spontaneamente come $\mathbb{P}(W)$, e quindi è uno spazio proiettivo, una stella anche è uno spazio proiettivo, ma è solo in biiezione (ma canonica...) con un $\mathbb{P}(V/W)$, in quanto la stella è formata da sottospazi di V (contenenti W), e non da sottospazi di V/W.

Per ulteriore esempio, l'insieme delle coniche nel piano (o in generale delle quadriche in spazi proiettivi) forma uno spazio proiettivo (di che dimensione? con quali coordinate?).

1.6. Definizione (Spazio proiettivo duale). *Sia* $(\mathbb{S}, \alpha_{\mathbb{S}})$ *uno spazio proiettivo completo di spazio vettoriale sovrastante* V*. Lo stesso insieme* $\mathbb{S}$*, dotato della biiezione* $\alpha_{\mathbb{S}^*} := \alpha_{\mathbb{S}} \circ \tau_{V^*} = \alpha_{\mathbb{S}} \circ \tau_V^{-1}$ *si dice lo spazio proiettivo duale (di spazio sovrastante (o sottostante)* V^**) e si indica con* $\mathbb{S}^*$*. Dunque se* $\mathbb{S} = (\mathbb{S}, V, \alpha_{\mathbb{S}})$*, allora* $\mathbb{S}^* = (\mathbb{S}, V^*, \alpha_{\mathbb{S}^*})$*.*

1.6.1. Se $s \in \mathbb{S}$ e $\dim_{\mathbb{S}} s = r$, allora abbiamo ($s \in \mathbb{S}^*$ e) $\dim_{\mathbb{S}^*} s = \dim \mathbb{S} - r - 1$, cioè $\dim_{\mathbb{S}^*} s = \dim \mathbb{S} - \dim_{\mathbb{S}} s - 1$ (perché $\dim_{\Bbbk}(W^\perp) = \dim_{\Bbbk} V - \dim_{\Bbbk} W$).

Se $T \subseteq \mathbb{S}$ è il sottospazio di $\mathbb{S}$ di sostegno $t \in \mathbb{S}$, allora $T \subseteq \mathbb{S}^*$ è la stella di $\mathbb{S}^*$ di asse $t \in \mathbb{S}^*$. In particolare i punti di $\mathbb{S}$ *sono* gli iperpiani di $\mathbb{S}^*$: $\mathbb{P} = \mathbb{I}^*$ e $\mathbb{I} = \mathbb{P}^*$.

1.6.2. Esempio: $\mathbb{S}^*(V)$. Lo spazio proiettivo duale dello spazio $\mathbb{S}(V)$ si indica con $\mathbb{S}^*(V)$ (piuttosto che $\mathbb{S}(V)^*$) ed è insiemisticamente identico a $\mathbb{S}(V)$, ma dotato della struttura di spazio proiettivo che eredita dall'isomorfismo $\tau_V : \mathbb{S}^*(V) \to \mathbb{S}(V^*)$ (che manda $W \leqslant V$ in $W^\perp \leqslant V^*$). In particolare, per esempio, il vuoto proiettivo di $\mathbb{S}^*(V)$ è V, il sup di due elementi è l'intersezione dei due, e l'inf ne è la somma.

1.6.3. Osservazione. Limitandosi agli spazi proiettivi standard (associati a spazi vettoriali) potremmo anche definire che lo spazio proiettivo duale sia lo spazio proiettivo associato allo spazio vettoriale duale, e potremmo trarne esattamente gli stessi risultati ed enunciati, se non altro perché vi è una identificazione canonica di $\mathbb{S}^*(V)$ con $\mathbb{S}(V^*)$. Il punto è che per uno spazio proiettivo qualsiasi $\mathbb{S}$ non si saprebbe quale altro insieme usare, se non proprio $\mathbb{S}$ stesso.

1.7. (meta)Teorema (principio di dualità proiettiva). *Sia* $\mathbb{S}$ *uno spazio proiettivo. Ogni asserzione* $\mathscr{A}$ *scritta in termini di elementi di* $\mathbb{S}$ *coinvolgendo solo la struttura di reticolo (cioè usando* $\wedge$, $\vee$, $\leqslant$, $\dim$*) è vera se e solo se risulta vera l'asserzione duale* $\mathscr{A}^*$ *che si ottiene sostituendo* $\wedge$ *con* $\vee$, $\vee$ *con* $\wedge$, $\leqslant$ *con* $\geqslant$ *(relazione duale) e* $\dim$ *con* $\dim \mathbb{S} - 1 - \dim$*.*

Dimostrazione. Se l'affermazione $\mathscr{A}$ è vera per ogni spazio proiettivo $\mathbb{S}$, in particolare essa è vera per lo spazio proiettivo duale $\mathbb{S}^*$; allora basta "tradurre" l'affermazione $\mathscr{A}$ fatta in $\mathbb{S}^*$ in termini di elementi di $\mathbb{S}$. Chiaramente si ottiene l'affermazione $\mathscr{A}^*$, che perciò è vera. Il viceversa segue, visto che $\mathscr{A}^{**} = \mathscr{A}$. $\square$

1.7.1. Facciamo notare esplicitamente, come conseguenza del teorema di dualità proiettiva, che basta dimostrare una delle due affermazioni affinché anche l'altra sia vera. Ma di più: se si dispone di una dimostrazione di $\mathscr{A}$ che sia scritta esplicitamente coinvolgendo solo la struttura di reticolo, allora si può trasformarla in una dimostrazione di $\mathscr{A}^*$ (nello stesso modo in cui $\mathscr{A}^*$ si ricava da $\mathscr{A}$).

1.7.2. Notiamo anche che, come mostreranno gli esempi qui sotto, un analogo principio di dualità non può essere vero per gli spazi affini. Spesso, negli esempi seguenti, i risultati scritti a sinistra sono veri per gli spazi affini, mentre quelli scritti a destra lo sono solo sotto ipotesi di "non-parallelismo".

1.7.3. Una nota terminologica: spesso si usa "simmetrizzare" la relazione $\leqslant$, cioè dire che s ed s' si appartengono se $s \leqslant s'$ oppure $s' \leqslant s$. Per esempio di dice che un punto appartiene ad una retta (e questo è usuale), ma anche che una retta appartiene ad un punto (contiene quel punto, ovvero la retta appartiene alla stella di asse quel punto).

1.8. Esempi in $\dim \mathbb{S} = 2$. Elenchiamo affiancati nozioni e relazioni duali:

vuoto proiettivo (dimensione -1).	piano proiettivo (dimensione 2).
punto (dimensione 0).	retta (dimensione 1).
tre punti sono allineati (appartengono alla stessa retta).	tre rette appartengono allo stesso fascio (si incontrano nello stesso punto).
triangoli: tre punti non allineati e le tre rette che li congiungono.	trilateri: tre rette non in un fascio e i tre punti di intersezione.
quadrangoli: quattro punti 3 a 3 non allineati e le sei rette che li congiungono.	quadrilateri: quattro rette 3 a 3 non in un fascio e i sei punti di intersezione.

(si noti che triangoli e trilateri sono nozioni equivalenti, quadrangoli e quadrilateri no).

Scriviamo affiancati alcuni enunciati duali (dimostrarli per esercizio).

due punti distinti appartengono ad un'unica retta (la congiungente i due punti).	due rette distinte appartengono ad un unico punto (l'intersezione delle due rette).
tre punti non allineati generano il piano proiettivo.	tre rette non passanti per uno stesso punto si incontrano nel vuoto proiettivo.
$d > 2$ punti sono allineati sse due a due generano la stessa retta.	$d > 2$ rette sono in un fascio sse due a due si intersecano nello stesso punto.
ogni quadrangolo determina un triangolo diagonale (con vertici le intersezioni di lati opposti).	ogni quadrilatero determina un trilatero diagonale (con lati le congiungenti di vertici opposti).

1.9. Esempi in $\dim \mathbb{S} = 3$. Elenchiamo affiancati nozioni e relazioni duali:

vuoto proiettivo (dimensione -1).	spazio proiettivo (dimensione 3).
punto (dimensione 0).	piano (dimensione 2).
retta (dimensione 1).	retta (dimensione 1).

(dunque la nozione di retta è autoduale in dimensione proiettiva 3);

tre punti sono allineati (appartengono alla stessa retta).	tre piani appartengono allo stesso fascio (si intersecano nella stessa retta).
quattro punti sono complanari (appartengono allo stesso piano).	quattro piani appartengono alla stessa stella (si intersecano nello stesso punto).
tetraedri: quattro punti non complanari, con le sei rette e i quattro piani che li congiungono.	tetrapiani: quattro piani non di una stella, con le sei rette e i quattro punti in cui si intersecano.

Scriviamo affiancati alcuni enunciati duali (dimostrazioni per esercizio).

due punti distinti appartengono ad un'unica retta (la congiungente i due punti).	due piani distinti appartengono ad un'unica retta (l'intersezione dei due piani).
tre punti non allineati generano un piano (il piano congiungente).	tre piani non passanti per una stessa retta si incontrano in un punto.
un punto e una retta che non si appartengono determinano un unico piano (il congiungente).	un piano e una retta che non si appartengono determinano un unico punto (l'intersezione).
se due punti distinti appartengono ad un piano allora la retta congiungente appartiene a quel piano.	se due piani distinti contengono un punto allora la retta intersezione contiene quel punto.

se due rette si intersecano in un punto allora generano un piano.

se due rette generano un piano allora si incontrano in un punto.

Quindi l'affermazione "due rette generano un piano se e solo se si incontrano in un punto" è autoduale (nello spazio proiettivo di dimensione 3), come pure "due rette generano lo spazio se e solo se si incontrano nel vuoto proiettivo".

se $d > 1$ rette si intersecano due a due, allora appartengono ad uno stesso piano oppure appartengono ad uno stesso punto (o entrambi).

se $d > 1$ rette sono due a due complanari, allora appartengono ad uno stesso punto oppure appartengono ad uno stesso piano (o entrambi).

Si noti che l'enunciato è autoduale.

1.10. Esempi in $\dim \mathbb{S} = 4$. Elenchiamo affiancati nozioni e relazioni duali:

vuoto proiettivo (dimensione -1).	spazio proiettivo (dimensione 4).
punto (dimensione 0).	spazio (dimensione 3).
retta (dimensione 1).	piano (dimensione 2).
tre punti sono allineati (appartengono alla stessa retta).	tre spazi appartengono allo stesso fascio (si intersecano nello stesso piano).
quattro punti sono complanari (appartengono allo stesso piano).	quattro spazi appartengono alla stessa stella (si intersecano nella stessa retta).
due rette si intersecano in un punto.	due piani generano uno spazio.

Scriviamo affiancati alcuni enunciati duali (dimostrazioni per esercizio).

due punti distinti appartengono ad un'unica retta (la congiungente i due punti).	due spazi distinti appartengono ad un'unico piano (l'intersezione dei due spazi).
tre punti non allineati generano un piano (il piano congiungente).	tre spazi non passanti per uno stesso piano si incontrano in una retta.
un punto e una retta che non si appartengono determinano un unico piano (il congiungente).	uno spazio e un piano che non si appartengono determinano un'unica retta (l'intersezione).
se due punti distinti appartengono ad un piano allora la retta congiungente appartiene a qual piano.	se due spazi distinti contengono una retta allora il piano intersezione contiene quella retta.
due rette generano un piano se e solo se si incontrano in un punto.	due piani si intersecano in una retta se e solo se generano uno spazio.
se $d > 1$ rette si intersecano due a due, allora appartengono ad uno stesso piano oppure appartengono ad uno stesso punto (o entrambi).	se $d > 1$ piani si intersecano due a due in rette, allora appartengono ad uno stesso spazio oppure appartengono ad una stessa retta (o entrambi).

Si noti che l'enunciato non è autoduale, ma lo diventa opportunamente generalizzato: in $\mathbb{P}^n$, se $d > 1$ sottospazi di dimensione $r > 0$ si intersecano due a due in sottospazi di dimensione $r - 1$, allora appartengono ad uno stesso spazio di dimensione $r + 1$ oppure ad una stella di centro uno spazio di dimensione $r - 1$ (o entrambi), per ogni n, r, d.

D'ora in poi, il lettore dovrà per ogni nozione o affermazione proiettive esplicitare, se possibile, nozione e asserzione duale, anche se l'estensore delle note se ne dimentica.

1.11. Teorema (Formula di Grassmann proiettiva). *Sia $\mathbb{S}$ uno spazio proiettivo completo. Per ogni $s, t \in \mathbb{S}$ abbiamo che*

$$\dim_{\mathbb{S}}(s) + \dim_{\mathbb{S}}(t) = \dim_{\mathbb{S}}(s \vee t) + \dim_{\mathbb{S}}(s \wedge t)$$

(si osservi inoltre che la formula di Grassman è autoduale, o meglio una disuguaglianza è duale dell'altra).

Dimostrazione. Segue immediatamente dalla analoga formula per gli spazi vettoriali. Se $s = \alpha(U)$ e $t = \alpha(W)$, abbiamo che

$$\dim_{\mathbb{k}}(U) + \dim_{\mathbb{k}}(W) = \dim_{\mathbb{k}}(U + W) + \dim_{\mathbb{k}}(U \cap W)$$

da cui l'affermazione segue (togliendo 2 a entrambi i lati!). □

1.11.1. Esempi. La formula di Grassmann può essere usata per dimostrare che varietà lineari proiettive sufficientemente grandi devono avere una intersezione non vuota. Per esempio:

(a) due rette nel piano proiettivo hanno sempre (almeno) un punto in comune; infatti se x è la dimensione dell'intersezione abbiamo $1 + 1 \leqslant 2 + x$, dunque $x \geqslant 0$; quindi nel piano proiettivo non vale il quinto postulato di Euclide ("per ogni punto esterno ad una retta passa una ed una sola retta parallela alla data"), perché non esistono rette parallele. Moltri altri assiomi degli elementi di Euclide sono falsi negli spazi proiettivi; per esempio gli assiomi d'ordine.

(b) una retta ed un piano nello spazio proiettivo tridimensionale hanno almeno un punto in comune.

(c) due piani si intersecano almeno in una retta in uno spazio proiettivo di dimensione 3, ed almeno in un punto in uno spazio proiettivo di dimensione 4.

(d) qual è la minima dimensione di uno spazio proiettivo in cui due sottovarietà lineari di dimensioni m ed n si incontrino nel vuoto?

(e) qual è la massima dimensione di uno spazio proiettivo in cui due sottovarietà lineari di dimensioni m ed n si incontrino almeno in un punto?

1.11.2. Posizioni reciproche di sottospazi proiettivi. Si osservi anche che due sottospazi proiettivi hanno sempre come intersezione un sottospazio proiettivo (eventualmente il vuoto proiettivo, che è $\alpha(0)$). Identificando allora ogni sottospazio con il proprio supporto punteggiato, possiamo dire che le uniche posizioni reciproche sono l'essere incidenti (per definizione, l'intersezione punteggiata non è vuota), oppure essere sghembi (per definizione, l'intersezione punteggiata è vuota); non vi sono fenomeni di parallelismo.

Diciamo anche che due sottospazi proiettivi sono complementari se sono sghembi e il loro sup è l'intero spazio proiettivo. In particolare la somma delle loro dimensioni dev'essere la dimensione dello spazio proiettivo diminuita di 1 (perché?).

Quali sono le nozioni duali di essere sghembi (generanti), di essere incidenti, di essere complementari?

1.11.3. Inseriamo alcune osservazioni classiche, con le duali, da verificare per esercizio:

In uno spazio proiettivo di dimensione tre, date due rette sghembe e un punto ad esse esterno, esiste una unica retta per quel punto e incidente le due date.

In uno spazio proiettivo di dimensione tre, date due rette sghembe e un piano che non ne contenga nessuna, esiste una unica retta di quel piano e incidente le due date.

(entrambi gli enunciati sono falsi in spazi affini di dimensione 3; quello di destra sembra più facile da dimostrare? In quello di sinistra, la retta cercata viene come intersezione di due piani ovvii, il che garantisce l'unicità: dette r, s le due rette e P il punto, la retta cercata deve essere contenuta sia nel piano $r \vee P$ sia nel piano $s \vee P$, che sono diversi, quindi si intersecano in una retta che è complanare, e quindi incidente, sia con r che con s.)

In uno spazio proiettivo di dimensione 4, dati un piano e una retta sghembi, e un punto ad essi esterno, esiste una unica retta per quel punto e incidente piano e retta dati.

In uno spazio proiettivo di dimensione 4, dati un piano e una retta sghembi, e uno spazio che non contenga nessuno dei due, esiste un unico piano di quello spazio tale che?.

Cosa si può dire per due piani sghembi in uno spazio proiettivo di dimensione 5?

Come si può generalizzare in dimensione n dati due sottospazi sghembi?

1.12. Sistemi di riferimento. In generale scegliere un sistema di riferimento in qualche spazio è equivalente a scegliere un isomorfismo con una forma canonica di tali spazi. Per esempio per spazi vettoriali scegliere una base è come dare un isomorfismo lineare con lo spazio standard $\Bbbk^n$; per spazi affini scegliere un riferimento è come dare una affinità con lo spazio affine standard $\mathbb{A}^n(\Bbbk)$; per spazi euclidei scegliere un riferimento ortogonale è come dare una isometria con lo spazio euclideo standard $\mathbb{E}^n(\Bbbk)$.

Quali dati servono in uno spazio proiettivo per ottenere una corrispondenza biiettiva con lo spazio standard $\mathbb{P}^n(\Bbbk)$?

1.12.1. Proposizione-Definizione (Sistemi di riferimento proiettivi e coordinate omogenee). *Sia $\mathbb{S}$ uno spazio proiettivo di dimensione n e spazio vettoriale sovrastante V. I seguenti dati sono equivalenti tra loro:*

(a) *una base ordinata di V a meno di proporzionalità;*

(*b*) *$n+2$ punti $P_0, \dots, P_n, U$ di $\mathbb{P}$ tali che $n+1$ tra loro non stiano su un iperpiano, ovvero generino tutto $\mathbb{S}$ (i $P_0, \dots, P_n$ formano l'edro fondamentale e U è il punto unità);*

(b^*) *$n+2$ iperpiani $p_0, \dots, p_n, u$ tali che $n+1$ tra loro abbiano sempre intersezione vuota.*

Ogni scelta di tali dati si dice un sistema di riferimento proiettivo su $\mathbb{S}$. Una volta scelto un riferimento proiettivo, ad ogni punto $p \in \mathbb{P}$ resta associata una $n+1$-upla di coordinate omogenee (cioè non tutte nulle e definite a meno di una costante moltiplicativa non nulla).

Dimostrazione. L'equivalenza di (b) e (b^*) è garantita dal teorema di dualità proiettiva. Precisamente abbiamo $p_i = P_i^\perp$ e $u = U^\perp$ (cioè, si usa la base duale nello spazio duale).

Dato (a) scegliamo per (b) i punti P_i determinati dalla base data di V e come punto unità U il punto determinato dalla somma dei vettori della base (chiaramente il tutto è ben definito a meno di proporzionalità). Dato (b) possiamo scegliere una base di V nel modo seguente: siano v_i rappresentanti dei P_i e u rappresentante di U, tali che u sia la somma dei v_i (perché si può fare?); allora i v_i sono la base (perché?) voluta di V, ed è definita a meno di proporzionalità.

Scelto un sistema di riferimento, e normalizzato come sopra per ottenere una base di V, ad ogni punto P di $\mathbb{P}$, rappresentato da un vettore $v \in V$, restano associate le coordinate di v nella base scelta; chiaramente sono definite a meno di un multiplo scalare non nullo (perché la base lo è, e anche il vettore v), e si dicono le coordinate omogenee di P nel riferimento scelto. □

1.12.2. Nota. Dato un riferimento, l'assegnazione delle coordinate dà una biiezione tra lo spazio proiettivo dato $\mathbb{P}$ (di dimensione n) e lo spazio proiettivo standard $\mathbb{P}^n(\Bbbk)$: si osservi esplicitamente che per avere questa biiezione non basta dare $n+1$ punti di $\mathbb{P}$ in posizione generale, ma serve anche il punto unità.

Quindi, per ogni dato problema in $\mathbb{P}$ possiamo ad $n+2$ punti in "posizione generale" associare le coordinate standard del riferimento canonico di $\mathbb{P}^n(\Bbbk)$ se questo è utile per semplificare i conti.

Che relazioni vi sono tra sistemi di riferimento proiettivi in $\mathbb{P}^n(\Bbbk)$ e sistemi di riferimento affini in $\mathbb{A}^n(\Bbbk)$?

1.13. Equazioni cartesiane di sottospazi. Dati $m+1$ punti $P_0, \dots, P_m$ di uno spazio proiettivo $\mathbb{P}$, si dicono in posizione generale se gli $m+1$ vettori che li rappresentano sono linearmente indipendenti, ovvero sse la più piccola varietà proiettiva che li contiene ha dimensione m. In tal caso le equazioni della varietà proiettiva congiungente gli $m+1$ punti sono date dalla condizione $\operatorname{rk}\begin{pmatrix} X & P_0 & \cdots & P_m \end{pmatrix} = m+1$, ove $X = \begin{pmatrix} X_0 \\ \vdots \\ X_n \end{pmatrix}$ sono le coordinate del riferimento scelto in $\mathbb{P}(V)$ e i punti sono espressi con coordinate in quel riferimento.

Si osservi che si tratta in ogni caso di equazioni omogenee, condizione necessaria affinché abbia senso controllarle sulle coordinate di punti dello spazio proiettivo (che sono definite a meno di una costante moltiplicativa non nulla: quindi ha senso dire se un polinomio omogeneo si annulla o meno in quel punto, mentre non ha senso chiedersi quale valore non nullo assuma, poiché cambia cambiando rappresentante del punto).

Le equazioni stesse vanno considerate come punti dello spazio duale (iperpiani dello spazio dato) e il sottospazio proiettivo generato è quello formato da tutti i punti corrispondenti ad equazioni soddisfatte dal sottospazio dato (cioè, a tutti gli iperpiani che lo contengono...).

1.13.1. Problema. Esercizio classico:

In uno spazio proiettivo di dimensione tre, date tre rette a due a due sghembe, per ogni punto di una esiste una unica retta per quel punto e incidente le altre due. Descrivere l'insieme definito dalla unione di queste rette.

In uno spazio proiettivo di dimensione tre, date tre rette a due a due sghembe per ogni piano di asse una delle rette, esiste una unica retta di quel piano e incidente le altre due. Descrivere l'insieme definito dalla unione di queste rette.

Per l'enunciato a sinistra, date le equazioni $r_0(X) = 0 = r_1(X)$ ed $s_0(X) = 0 = s_1(X)$ di due di esse, diciamo r ed s, e due punti $T_0, T_1 \in t$ della rimanente, possiamo descrivere l'insieme $\mathscr{Q}$ formato dalle rette $(T \vee r) \wedge (T \vee s)$ al variare di $T = \lambda_0 T_0 + \lambda_1 T_1$ come l'insieme degli $X \in \mathbb{P}^3$ per cui esistono λ_0, λ_1 non entrambi nulli (cioè un punto di $\mathbb{P}^1$) soluzioni del sistema omogeneo

$$\begin{pmatrix} r_1(T_0)r_0(X) - r_0(T_0)r_1(X) & r_1(T_1)r_0(X) - r_0(T_1)r_1(X) \\ s_1(T_0)s_0(X) - s_0(T_0)s_1(X) & s_1(T_1)s_0(X) - s_0(T_1)s_1(X) \end{pmatrix} \begin{pmatrix} \lambda_0 \\ \lambda_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

(si tratta delle equazioni dei due piani $T \vee r$ e $T \vee s$, rilette in termini dei parametri λ_0, λ_1), e quindi se e solo se è nullo il determinante del sistema, che dà una equazione di secondo grado nelle $X = (X_0, X_1, X_2, X_3)$.

1.13.2. Problema. Trovare la massima generalizzazione in $\mathbb{P}^n$ dell'enunciato dato: per esempio, dati due sottospazi sghembi come descrivere l'unione di tutte le trasversali comuni dai punti di un terzo sottospazio? Quando basterà una equazione, o quante equazioni serviranno, e di che grado?

1.13.3. Problema. Cosa si può dire di tre rette, due a due sghembe, in uno spazio proiettivo di dimensione quattro? Naturalmente, il caso (nuovo) interessante è quando esse generano tutto lo spazio (altrimenti sono contenute in un sottospazio di dimensione tre). Generalizzare (e dualizzare).

1.14. Definizione (Sistema di riferimento duale). *Dato un sistema di riferimento su $\mathbb{S}(V)$, cioè una base di V a meno di proporzionalità, il sistema di riferimento duale sullo spazio proiettivo duale $\mathbb{S}^*(V)$ è dato dalla base duale dello spazio vettoriale V^*. Le coordinate di $\mathbb{S}^*(V)$ nel riferimento duale si dicono le coordinate di Plücker; le coordinate di Plücker di un punto di $\mathbb{S}^*(V)$ si identificano con i coefficienti di una sua equazione in quanto iperpiano di $\mathbb{P}(V)$.*

1.14.1. È quasi ovvio osservare che se un punto $P \in \mathbb{P}$ ha coordinate X in un fissato riferimento, e un iperpiano $\pi \in \mathbb{P}^*$ ha coordinate plückeriane a nel riferimento duale, allora $p \in \pi$ se e solo se $a^{\mathrm{t}} X = 0$ (pensando a come coordinate, si intende un vettore colonna...).

1.15. Lo spazio proiettivo standard. La base canonica di $\Bbbk^{n+1}$ dà un riferimento standard nello spazio proiettivo $\mathbb{P}^n(\Bbbk)$. Se $v \in V$ ha coordinate $X = \begin{pmatrix} X_0 \\ \vdots \\ X_n \end{pmatrix}$ rispetto alla base canonica, il punto $P = \alpha\langle v\rangle$ ha coordinate omogenee $X = \begin{pmatrix} X_0 \\ \vdots \\ X_n \end{pmatrix}$ che sono definite a meno di proporzionalità.

Qual è il riferimento duale nello spazio proiettivo duale?

2. Alcuni modelli per gli spazi proiettivi.

Abbiamo definito gli spazi proiettivi completi come reticoli di sottospazi di uno spazio vettoriale, e gli spazi proiettivi punteggiati come insieme dei sottospazi di dimensione 1 di uno spazio vettoriale. Vogliamo ora realizzare dei modelli più concreti, che presentino gli spazi proiettivi come insiemi di punti, piuttosto che di oggetti più complicati. *Faremo anche delle asserzioni di carattere topologico, che possono essere ignote al lettore (basta saltarle facendo finta di nulla), e delle asserzioni circa gli spazi affini che invece saranno chiarite da un futuro paragrafo.*

Il primo passo è identificare lo spazio proiettivo punteggiato associato a V con l'insieme quoziente $(V \smallsetminus \{0\})/\Bbbk^\times$; dunque i suoi elementi sono classi laterali, e possiamo cercare di rappresentarle mediante degli elementi ben scelti.

2.1. Gli spazi proiettivi reali (come sfere modulo antipodia o dischi modulo antipodia del bordo). Consideriamo $\mathbb{P}^n(\mathbb{R})$: sia $\mathbb{S}^n = \{x \in \mathbb{E}^{n+1}(\mathbb{R}) \ : \ \|x\| = 1\}$ la (buccia della) sfera di raggio 1 in $\mathbb{E}^{n+1}(\mathbb{R})$. Sia $\sigma : \mathbb{S}^n \longrightarrow \mathbb{S}^n$ la mappa antipodale $x \mapsto -x$. Allora la mappa evidente $\mathbb{P}^n(\mathbb{R}) \longrightarrow \mathbb{S}^n/\sigma$ è una biiezione; in particolare (potremmo vedere che) si tratta di un isomofismo di spazi topologici, da cui seguirà che $\mathbb{P}^n(\mathbb{R})$ è uno spazio topologico compatto. Intuitivamente questa rappresentazione corrisponde a scegliere come rappresentante del punto $P = [v]$ di $\mathbb{P}^n(\mathbb{R})$ un vettore di modulo unitario (ma dobbiamo ancora identificare v con $-v$, che è proprio quello che fa la mappa antipodale).

In particolare possiamo identificare il piano proiettivo $\mathbb{P}^2(\mathbb{R})$ con la (superficie della) sfera $\mathbb{S}^2$, i punti del piano proiettivo con le *coppie di punti antipodali della sfera*, le rette del piano proiettivo con i *circoli massimi* sulla sfera.

Consideriamo ora il disco $\mathbb{D}^n = \{x \in \mathbb{E}^n(\mathbb{R}) \ : \ \|x\| \leqslant 1\}$, e sia τ la relazione di equivalenza che identifica ogni punto sul bordo con il suo opposto. Consideriamo la semisfera $\mathbb{S}^n_{\geqslant 0} = \{x \in \mathbb{S}^n \ : \ x_1 \geqslant 0\}$ e la mappa $\mathbb{S}^n_{\geqslant 0} \to \mathbb{D}^n$ che "cancella la prima coordinata". Essa induce una biiezione $\mathbb{S}^n/\sigma \cong \mathbb{S}^n_{\geqslant 0}/\sigma \longrightarrow \mathbb{D}^n/\tau$, dunque anche il disco modulo antipodia del bordo è un modello per lo spazio proiettivo reale; di nuovo potremmo vedere che si tratta di un isomofismo di spazi topologici. Da notare però che in questo modello s'è fatta una scelta speciale di un iperpiano (il bordo del disco), da pensare

come iperpiano all'infinito; dunque questo modello identifica piuttosto uno spazio proiettivo dotato di una fissata scelta di uno spazio affine (come vedremo meglio in seguito).

In particolare possiamo identificare il piano proiettivo $\mathbb{P}^2(\mathbb{R})$ con il disco $\mathbb{D}^2$, i punti del piano proiettivo con i punti interni del disco oppure le *coppie di punti antipodali del bordo*; descrivere le rette è più difficile (perché? cosa descrivono sul disco i fasci di rette di centro un punto? si controlli che i circoli massimi della semisfera proiettano sul disco delle semiellissi bitangenti il bordo in punti antipodali).

2.2. La retta proiettiva reale (come circonferenza). Se $n=1$ possiamo identificare un isomorfismo $\mathbb{S}^1 \longrightarrow \mathbb{P}^1(\mathbb{R})$ (tramite la "proiezione dal polo nord" sull'asse X: $\binom{x}{y} \mapsto \frac{x}{1-y}$), ovvero $\binom{x}{y} \mapsto \langle \binom{1-y}{x} \rangle$.

Infatti in questo caso abbiamo un isomorfisno tra il quoziente $\mathbb{S}^1/\sigma$ ed $\mathbb{S}^1$ dato dalla seguente costruzione (un po' complicata perché vi sono anche altre corrispondenze: trovarle!):

Perché non si può fare un discorso analogo per $\mathbb{S}^n$ e $\mathbb{P}^n(\mathbb{R})$ con $n>1$?

Si osservi in particolare che $\mathbb{P}^2(\mathbb{R})$ non è il prodotto $\mathbb{P}^1(\mathbb{R})\times\mathbb{P}^1(\mathbb{R})$, che è un oggetto completamente diverso e molto più semplice (un toro, poiché è isomorfo a $\mathbb{S}^1\times\mathbb{S}^1$).

2.3. Nastro di Moebius e piano proiettivo reale. Presentiamo anche un modello meno preciso, ma più suggestivo di piano proiettivo reale, insieme ad alcune costruzioni preliminari o simili.

2.3.1. Si osservi che dato un quadrato $[0,1]\times[0,1]$ possiamo costruire:

un cilindro (identificando $(x,0)\sim(x,1)$ per ogni $x\in[0,1]$);

un nastro di Mœbius (identificando $(x,0)\sim(1-x,1)$ per ogni $x\in[0,1]$);

la prima figura è orientabile, mentre la seconda no, come si vede seguento il cammino $[1/2,y]$ per $y\in[0,1]$ (che rovescia l'orientamento).

2.3.2. Partendo dal cilindro possiamo costruire tre figure senza bordo:

la sfera (colassando a un punto ciascuno dei due cerchi $[0,y]$ e $[1,y]$),

il toro (identificando $(0,y) \sim (1,y)$ per ogni $y \in [0,1]$),

e l'otre o bottiglia di Klein (identificando $(0,y) \sim (1,1-y)$ per ogni $y \in [0,1]$);

si osservi che quest'ultima superficie non è orientabile, poiché contiene nastri di Mœbius, mentre sfera e toro sono orientabili.

2.3.3. Partendo dal nastro di Mœbius e identificando ulteriormente i bordi rimanenti in ordine inverso (identificando $(0,y) \sim (1,1-y)$ per ogni $y \in [0,1]$), oppure colassando ad un punto il bordo rimasto (che è un circolo), si ottiene il piano proiettivo reale; anch'esso è superficie non orientabile, poiché contiene nastri di Mœbius.

2.3.4. Sfere e piani proiettivi reali si ottengono anche per identificazione dei due lati di un diagono (o bigono, poligono con due lati) nei due modi possibili (se il diagono è un disco unitario, e i due lati sono le semicirconferenze tra polo nord e polo sud, si tratta di $(x,y) \sim (-x,y)$ oppure di $(x,y) \sim (-x,-y)$).

2.3.5. Immersioni di $\mathbb{P}^2(\mathbb{R})$ in $\mathbb{R}^3$ ed $\mathbb{R}^4$. La rappresentazione di $\mathbb{P}^2(\mathbb{R})$ come sfera modulo antipodia, o come disco modulo antipodia del bordo, mostra che questa superficie non si può immergere in $\mathbb{R}^3$ in modo iniettivo, cioè senza fare autointersezioni (punti distinti che sono mappati nello stesso punto); vi sono alcuni modelli classici di quasi-immersioni di $\mathbb{P}^2(\mathbb{R})$ in $\mathbb{R}^3$ (superficie di Boy e superficie romana di Steiner, vi è un libro dedicato di F.Apéry, e Boy compare in un fumetto di J.-P. Petit, Le Topologicon). Invece per esercizio si può studiare la funzione

$$\mathbb{R}^3 \longrightarrow \mathbb{R}^4 \quad \text{data da} \qquad \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} \longmapsto \begin{pmatrix} x_0x_1 \\ x_0x_2 \\ x_1x_2 \\ x_1^2-x_2^2 \end{pmatrix}$$

(immagine? antimmagine per ogni punto del codominio?) e controllare in particolare che ristretta alla sfera unitaria assume lo stesso valore su punti antipodali e ha come immagine quindi una superficie in corrispondenza biunivoca con $\mathbb{P}^2(\mathbb{R})$. Questo dà una immersione di $\mathbb{P}^2(\mathbb{R})$ in $\mathbb{R}^4$.

2.4. Spazio proiettivo reale e matrici ortogonali. Mostrare che esiste una biiezione tra $\mathbb{P}^3(\mathbb{R})$ e $\mathrm{SO}_3(\mathbb{R})$. Conviene usare i quaternioni $\mathbb{H}$, e ricordare che vi è una mappa suriettiva di gruppi con nucleo ± 1 dai quaternioni unitari $\mathbb{H}^1$ verso $\mathrm{SO}_3(\mathbb{R})$.

2.5. La retta proiettiva complessa (come superfice sferica). La proiezione stereografica dal polo nord di $\mathbb{S}^2$ (sul piano $Z=0$: $(x,y,z) \mapsto (\frac{x}{1-z}, \frac{y}{1-z})$) dà un isomorfismo $\mathbb{S}^2 \longrightarrow \mathbb{P}^1(\mathbb{C})$ tramite $(x,y,z) \mapsto [1-z, x+iy]$. Potremmo vedere che si tratta della compattificazione di $\mathbb{C}$ con un punto.

2.5.1. In alternativa, abbiamo una identificazione dei punti della retta proiettiva complessa con i punti di $\mathbb{S}^3 \subseteq \mathbb{R}^4 = \mathbb{C}^2$ modulo la moltiplicazione per elementi di $\mathbb{S}^1 \subseteq \mathbb{C}^\times$, quindi si tratta di una fibrazione in cerchi della sfera in dimensione 4.

2.6. Il piano proiettivo complesso. Nel caso del piano proiettivo complesso, abbiamo una identificazione dei suoi punti con i punti di $\mathbb{S}^5 \subseteq \mathbb{R}^6 = \mathbb{C}^3$ modulo la moltiplicazione per elementi di $\mathbb{S}^1 \subseteq \mathbb{C}^\times$, quindi si tratta di una fibrazione in cerchi della sfera in dimensione 6.

2.7. Spazi proiettivi sui campi finiti (conteggi di punti e sottospazi). È un esercizio intessante contare e se possibile disegnare gli spazi proiettivi sui campi con un numero finito di elementi: sia $\mathbb{F}_q$ (il) campo con q elementi, e sappiamo che $q = p^f$, con p numero primo naturale (in effetti $\mathbb{F}_q$ è il campo delle radici di $X^q - X$ come polinomio a coefficienti in $\mathbb{F}_p$, ricordiamo). Allora:

(0) il punto affine $\mathbb{A}^0(\mathbb{F}_q)$ ha un punto, come pure $\mathbb{P}^0(\mathbb{F}_q)$, e questo vale per campi qualsiasi, veramente... (lo scrivo qui, perché non s'era mai notato, finora);

(1) la retta affine $\mathbb{A}^1(\mathbb{F}_q)$ ha q punti,
mentre la retta proiettiva $\mathbb{P}^1(\mathbb{F}_q)$ ha $q+1=\frac{q^2-1}{q-1}$ punti;

(2) il piano affine $\mathbb{A}^2(\mathbb{F}_q)$ ha q^2 punti e $\frac{q^2(q^2-1)}{q(q-1)}=q(q+1)$ rette,
mentre il piano proiettivo $\mathbb{P}^2(\mathbb{F}_q)$ ha $q^2+q+1=\frac{q^3-1}{q-1}$ punti e altrettante rette (dualità...);

(3) lo spazio affine $\mathbb{A}^3(\mathbb{F}_q)$ ha q^3 punti,
$\frac{q^3(q^3-1)}{q(q-1)}=q^2(q^2+q+1)$ rette
e $\frac{q^3(q^3-1)(q^3-q)}{q^2(q^2-1)(q^2-q)}=q(q^2+q+1)$ piani,
mentre lo spazio proiettivo $\mathbb{P}^3(\mathbb{F}_q)$ ha $q^3+q^2+q+1=\frac{q^4-1}{q-1}$ punti (e altrettanti piani per dualità...)
e $\frac{(q^4-1)(q^4-q)}{(q^2-1)(q^2-q)}=(q^2+1)(q^2+q+1)$ rette;

(4) lo spazio affine $\mathbb{A}^4(\mathbb{F}_q)$ ha q^4 punti,
$\frac{q^4(q^4-1)}{q(q-1)}=q^3(q^3+q^2+q+1)$ rette,
$\frac{q^4(q^4-1)(q^4-q)}{q^2(q^2-1)(q^2-q)}=q^2(q^2+1)(q^2+q+1)$ piani
e $\frac{q^4(q^4-1)(q^4-q)(q^4-q^2)}{q^3(q^3-1)(q^3-q)(q^3-q^2)}=q(q+1)(q^2+1)$ spazi,
mentre lo spazio proiettivo $\mathbb{P}^4(\mathbb{F}_q)$ ha $q^4+q^3+q^2+q+1=\frac{q^5-1}{q-1}$ punti (e altrettanti spazi per dualità...)
e $\frac{(q^5-1)(q^5-q)}{(q^2-1)(q^2-q)}=(q^2+1)(q^4+q^3+q^2+q+1)$ rette (e altrettanti piani per dualità...);

(n) generalizzare, magari facendosi una tabellina e capire come aumentano i sottospazi che si contano.

Nota: in questi casi si osserva che $\mathbb{P}^n$ è diverso da $(\mathbb{P}^1)^n$ anche solo perché non hanno lo stesso numero di punti...

2.7.1. Piano di Fano. Giusto per divertimento, e perché è classico, disegnamo il piano proiettivo su $\mathbb{F}_2$ con le sue sette rette (e sette punti). Evidenziamo anche un piano affine (quattro punti e sei rette) ivi contenuto (trovare gli altri?). È divertente anche dare le coordinate ai punti e alle rette.

2.7.2. Spazi di Fano. Cercare altri simili rappresentazioni delle geometrie finite? Nel caso di spazi su $\mathbb{F}_2$, essendo banale la relazione di proporzionalità, è facile: si dicono geometrie di Fano, e i loro (di $\mathbb{P}^n(\mathbb{F}_2)$) punti si possono rappresentare come i vertici di un $(n+1)$-edro e tutti i baricentri di tutti i sotto-edri. Nel caso $n=3$ dello spazio, è simpatico cercare i 15 piani, e le loro rette:

visione globale di $\mathbf{P}^3(\mathbf{F}_2)$

piano $(0,0,0,1)$ piano $(0,0,1,0)$ piano $(0,1,0,0)$ piano $(1,0,0,0)$

piano $(0,0,1,1)$ piano $(0,1,0,1)$ piano $(1,0,0,1)$ piano $(0,1,1,0)$ piano $(1,0,1,0)$ piano $(1,1,0,0)$

piano $(0,1,1,1)$ piano $(1,0,1,1)$ piano $(1,1,0,1)$ piano $(1,1,1,0)$

piano $(1,1,1,1)$

2.7.3. Partizioni. Ancora per divertimento, si potrebbe cercare quando uno spazio (proiettivo) finito può essere scritto come unione disgiunta di suoi sottospazi di una fissata dimensione (si dice una partizione dello spazio in sottospazi di fissata dimensione). È curioso che la condizione, evidentemente necessaria, che il numero di punti del sottospazio divida il numero di punti dello spazio risulta essere anche condizione sufficiente (ed equivalente a che $r+1$ divida $n+1$ se r è la dimensione dei sottospazi, ed n quella dello spazio).

Per esempio ogni spazio proiettivo di dimensione 3 è unione (disgiunta) di un insieme di (quante?) rette due a due sghembe.

Si possono fare anche partizioni degli spazi affini (con sottospazi sghembi di fissata dimensione)?

3. Applicazioni proiettive e proiettività.

3.1. Definizioni ed esempi

3.1.1. Definizione (Applicazioni proiettive). *Siano $\mathbb{S}$ ed $\mathbb{S}'$ due spazi proiettivi di spazi vettoriali sovrastanti V e V'. Una applicazione proiettiva $\varphi : \mathbb{S} \longrightarrow \mathbb{S}'$ è una funzione indotta da una applicazione lineare $f : V \longrightarrow V'$ tra gli spazi vettoriali sovrastanti, i.e. tale che $\varphi(\alpha(W)) = \alpha'(f(W))$ per ogni $W \in \mathbb{S}(V)$. Ciò significa che φ ed f rendono commutativo il seguente diagramma quadrato:*

$$\begin{tikzcd} \mathbb{S}(V) \arrow[r, "\mathbb{S}(f)"] \arrow[d, "\alpha"'] & \mathbb{S}(V') \arrow[d, "\alpha'"] \\ \mathbb{S} \arrow[r, "\varphi"'] & \mathbb{S}' \end{tikzcd} .$$

Definiamo $\operatorname{im}(\varphi) = \alpha'(\operatorname{im}(f)) \in \mathbb{S}(V')$, *(che identifichiamo con il suo supporto* $\operatorname{im}(\varphi) \subseteq \mathbb{P}'$*) e* $\ker(\varphi) = \alpha(\ker(f))$ *(che identifichiamo con il suo supporto* $\ker(\varphi) \subseteq \mathbb{P}$*) che si chiama il luogo di degenerazione dell'applicazione* φ.

3.1.1.1. Risulta $\dim(\operatorname{im}(\varphi)) + \dim(\ker(\varphi)) = \dim(\mathbb{S}) - 1$.

3.1.1.2. Due applicazioni lineari f, g sono sovrastanti la stessa applicazione proiettiva se e solo se $g = \lambda f$ per $\lambda \in \Bbbk^\times$. Il "se" è banale, e il "solo se" si verifica così: da $\mathbb{S}(f) = \mathbb{S}(g)$ certamente segue che $\ker f = \ker g$, e scegliendo una base $v_1, \dots, v_r$ di un complementare dei nuclei abbiamo che $f(v_i) = \lambda_i g(v_i)$ e anche $f(\Sigma_i v_i) = \lambda g(\Sigma_i v_i)$; poiché i vettori $g(v_1), \dots, g(v_r)$ sono linearmente indipendenti se ne deduce che $\lambda = \lambda_1 = \cdots = \lambda_r$, e allora $f = \lambda g$.

3.1.1.3. L'applicazione proiettiva $\varphi : \mathbb{S} \longrightarrow \mathbb{S}'$ non induce direttamente una applicazione tra gli spazi punteggiati, a causa del luogo di degenerazione, ma induce $\varphi : \mathbb{P} \smallsetminus \ker(\varphi) \longrightarrow \mathbb{P}'$ (con immagine $\operatorname{im}(\varphi)$).

3.1.2. Osservazione. *Data un'applicazione lineare $f : V \longrightarrow V'$ l'applicazione (insiemistica) $\mathbb{S}(f) : \mathbb{S}(V) \longrightarrow \mathbb{S}(V')$ data da $W \mapsto f(W)$, soddisfa alle seguenti proprietà:*

(i) $\mathbb{S}(f)(0) = 0$;
(ii) $\dim_\Bbbk \mathbb{S}(f)(W) \leqslant \dim_\Bbbk W$;
(iii) $\mathbb{S}(f)(W \cap W') \subseteq \mathbb{S}(f)(W) \cap \mathbb{S}(f)(W')$ *(non uguali in generale);*
(iv) $\mathbb{S}(f)(W + W') = \mathbb{S}(f)(W) + \mathbb{S}(f)(W')$.
(v) se $W \leqslant W'$ *allora* $\mathbb{S}(f)(W) \leqslant \mathbb{S}(f)(W')$.
(vi) $\mathbb{S}(f)(W) = \mathbb{S}(f)(W')$ *se e solo se* $W + \ker f = W' + \ker f$.

Inoltre $\mathbb{S}(f) = \mathbb{S}(g)$ *se e solo se* $g = \lambda f$ *ove* λ *è uno scalare non nullo.*

È vero che una funzione $\varphi : \mathbb{S}(V) \longrightarrow \mathbb{S}(V')$ avente le proprietà di non aumentare le dimensioni, di rispettare la somma (di sottospazi) e che l'immagine di due elementi è uguale se solo se coincidono quando sommati con il massimo elemento di immagine nulla, è del tipo $\varphi = \mathbb{S}(f)$ per qualche $f : V \longrightarrow V'$ (lineare)? Inoltre tali f sono determinate a meno di multipli scalari non nulli?

3.1.3. Definizione (Proiettività). *Una proiettività è una applicazione proiettiva di $\mathbb{S}$ in sè il cui nucleo sia il vuoto proiettivo di $\mathbb{S}$, ovvero che abbia immagine tutto $\mathbb{S}$, o ancora tale che una applicazione lineare sovrastante sia un isomorfismo (e allora tutte lo sono). Una proiettività si restringe dunque ad una biiezione tra gli spazi proiettivi punteggiati.*

3.1.4. In particolare ad ogni proiettività di $\mathbb{S} = \mathbb{S}(V)$ resta associata un isomorfismo di V a meno di proporzionalità. Il gruppo delle proiettività di $\mathbb{S}$, sotto l'operazione di composizione, si indica con $\mathrm{PGL}(\mathbb{S})$ ed è isomorfo a $\mathrm{PGL}(V) := \mathrm{GL}(V)/\Bbbk^\times$.

3.1.5. Espressione matriciale: gruppo lineare proiettivo. Scelti dei riferimenti su $\mathbb{P}(V)$ e $\mathbb{P}(V')$, allora ogni applicazione proiettiva $\varphi : \mathbb{P}(V) \longrightarrow \mathbb{P}(V')$ si rappresenta (a meno di proporzionalità per uno scalare non nullo) tramite una matrice $A \in M_{n+1,n'+1}(\Bbbk)$.

La scelta di un sistema di riferimento su $\mathbb{S}$ determina allora una identificazione del gruppo $\mathrm{PGL}(\mathbb{S}(V))$ con il gruppo quoziente $\mathrm{PGL}_n(\Bbbk) = \mathrm{PGL}(n, \Bbbk) := \mathrm{GL}(n+1, \Bbbk)/\Bbbk^\times$.

3.1.6. Esempi fondamentali (proiezioni e sezioni). Siano $t = \alpha(W)$ e $t' = \alpha(W')$ elementi di $\mathbb{S}$. Ricordiamo che si dicono sghembi se $t \wedge t' = \alpha(0)$ (il vuoto di $\mathbb{S}$, ovvero $W \cap W' = 0$), incidenti altrimenti; si dicono complementari se sono sghembi e $t \vee t' = \alpha(V)$ (corrisponde a $W \oplus W' = V$). Indichiamo con T il sottospazio di $\mathbb{S}$ di sostegno t, e con T^* la stella di $\mathbb{S}$ di asse t (si tratta del sottospazio di $\mathbb{S}^*$ di sostegno t).

3.1.6.1. Inclusioni di sottospazi. L'inclusione $T \subseteq \mathbb{S}$ è applicazione proiettiva con applicazione lineare sovrastante l'inclusione $W \leqslant V$ (ogni elemento di T viene mandato in sé stesso, ovvero ogni sottospazio di W viene mandato in sè stesso). In generale è iniettiva, ma non suriettiva. Si noti invece che l'applicazione insiemistica $\mathbb{S} \longrightarrow T$ che manda ogni elemento u in $u \wedge t$ (intersezione dei sottospazi) non è una applicazione proiettiva, poiché per esempio non ammette un sottospazio massimale mandato nel vuoto proiettivo. Cosa succede se si legge questa applicazione insiemistica usando le strutture duali degli spazi $\mathbb{S}$ e T? Comunque l'inclusione ammette delle trasformazioni proiettive che ne sono delle inverse sinistre (come?).

3.1.6.2. Proiezioni su stelle. La proiezione $\mathbb{S} \longrightarrow T^*$ data da $s \mapsto s \vee t$ è applicazione proiettiva di sovrastante la proiezione $V \longrightarrow V/W$ (un sottospazio U viene mandato in $U + W$, eventualmente modulo W). In generale è suriettiva ma non iniettiva. Si noti invece che l'applicazione insiemistica $T^* \longrightarrow \mathbb{S}$ che manda ogni elemento u in u (ogni sottospazio contenente W in sé stesso) non è una applicazione proiettiva, poiché per esempio aumenta la dimensione proiettiva. Cosa succede se si legge questa applicazione insiemistica usando le strutture duali degli spazi T^* e $\mathbb{S}$? Comunque la proiezione ammette delle trasformazioni proiettive che ne sono delle inverse destre (come?).

3.1.6.3. Proiezioni da sottospazi su stelle. Più generalmente la proiezione di t' dal centro t è $T' \longrightarrow T^*$ data dalla composizione della inclusione di T' in $\mathbb{S}$ e della proiezione su T^*, quindi $s \mapsto s \vee t$, di applicazione lineare sovrastante $W' \longrightarrow V/W$ (oppure $W' \longrightarrow (W' + W)/W \cong W'/(W' \cap W)$). Questa applicazione è una proiettività se e solo se t e t' sono complementari, nel qual caso merita un nome:

3.1.6.4. Sezioni di stelle con sottospazi. Se t e t'' sono complementari, allora la sezione della stella di asse t con t'' è $T^* \longrightarrow T''$ data da $u \mapsto u \wedge t''$ di applicazione sovrastante l'isomorfismo canonico $V/W \longrightarrow W''$ (inverso del morfismo canonico $W'' \longrightarrow V/W$).

3.1.6.5. Proiezione tra sottospazi (tramite una stella). Se t e t'' sono complementari, allora la proiezione di t' su t'' di centro t è $T' \longrightarrow T''$ data da $u \mapsto (u \vee t) \wedge t''$ composta di una proiezione $T' \longrightarrow T^*$ e di una sezione $T^* \longrightarrow T''$. Quindi l'applicazione lineare sovrastante è la composizione $W' \longrightarrow V/W \longrightarrow W''$ (ovvero $W' \longrightarrow (W' + W)/W \subseteq V/W \longrightarrow W''$). È quello che fa un pittore: proietta il mondo t' sulla tela t'' con centro t il suo occhio.

3.1.6.6. Decomposizione di applicazioni proiettive. Poiché ogni applicazione lineare $f : V \longrightarrow W$ può essere scritta come composizione di tre applicazioni (la prima suriettiva, la seconda un isomorfismo, la terza iniettiva):

$$V \longrightarrow V/\ker f \longrightarrow \operatorname{im} f \longrightarrow W$$

abbiamo che ogni applicazione proiettiva può essere scritta come composizione di una proiezione, di una proiettività e di una immersione.

Si osservi comunque che solo le ultime due applicazioni si possono scrivere per gli spazi punteggiati.

3.1.7. Teorema. *Dati un riferimento su $\mathbb{P}(V)$ e un riferimento su $\mathbb{P}(V')$, spazi proiettivi della stessa dimensione, esiste unica l'applicazione proiettiva $\varphi : \mathbb{P}(V) \longrightarrow \mathbb{P}(V')$ che manda il primo riferimento ordinatamente nel secondo, e si tratta di una proiettività. In particolare, dati due riferimenti proiettivi su $\mathbb{P}(V)$ esiste una unica proiettività che mandi i punti del primo ordinatamente nei punti del secondo.*

Dimostrazione. È un'ovvia conseguenza dell'analogo teorema per gli spazi vettoriali, visto che un riferimento sullo spazio proiettivo determina una base dello spazio vettoriale corrispondente a meno di proporzionalità. □

3.1.7.1. Problema. Un analogo risultato per le trasformazioni proiettive è invece completamente falso: assegnato un riferimento in $\mathbb{P}(V)$, e assegnati altrettanti punti in $\mathbb{P}(V')$, non è detto che esista una trasformazione proiettiva che porti ordinatamente il riferimento dato nei punti assegnati, e nel caso esista non è detto che sia unica. Questo nonostante sia vero che una applicazione lineare

è unicamente definita dai valori attribuiti ad una base del dominio; il punto è che un insieme arbitrario di punti in uno spazio proiettivo non determina un insieme di vettori dello spazio vettoriale corrispondente, e nemmeno una base dello spazio generato.

Per esempio esistono più trasformazioni proiettive che mandano un intero riferimento in un fissato punto del codominio (esse hanno nuclei diversi, cioè diversi luoghi di degenerazione); d'altro lato non esistono trasformazioni proiettive che mandano i punti fondamentali di un riferimento in un fissato punto e il punto unità altrove.

3.1.7.2. Esempio. Per ogni permutazione σ del gruppo simmetrico S_{n+2} esiste una proiettività φ_σ tale che $\varphi_\sigma(P_i) = P_{\sigma i}$. Questo dà un morfismo di gruppi $S_{n+2} \to \mathrm{PGL}(n, \Bbbk)$: si osservi che le matrici corrispondenti sono matrici di permutazioni (un solo 1 per ogni riga e colonna, altrove 0) solo se l'ultimo punto del riferimento (il punto unità) è mandato in sé. Farsi qualche esempio.

3.1.7.3. Nel caso del piano proiettivo ($n = 2$), ogni permutazione dei quattro punti fondamentali induce una permutazione dei tre punti diagonali (del quadrilatero); abbiamo un morfismo suriettivo di gruppi $S_4 \to S_3$ il cui nucleo è il sottogruppo V di Klein di S_4.

3.1.8. Sistemi di riferimento come proiettività. Un sistema di riferimento in uno spazio proiettivo punteggiato di spazio vettoriale sovrastante V è equivalente al dato di un isomorfismo proiettivo $\varrho : \mathbb{P}(V) \longrightarrow \mathbb{P}^n(\Bbbk)$. Basta infatti mandare la base associata al riferimento nella base canonica di $\Bbbk^{n+1}$. L'immagine di un punto sono esattamente le sue coordinate omogenee.

3.1.9. Definizione (Duali di applicazioni proiettive.). *Data una applicazione proiettiva $\varphi : \mathbb{S} \to \mathbb{S}'$, di applicazione sovrastante $f : V \to V'$, allora definiamo l'applicazione duale (o trasposta) $\varphi^* : \mathbb{S}'^* \to \mathbb{S}^*$ come la trasformazione proiettiva di sovrastante la duale di f, cioè $f^* : V'^* \to V^*$.*

3.1.9.1. Interpretazione geometrica. Una trasformazione proiettiva, per immagine inversa, manda iperpiani del codominio in iperpiani del dominio (o l'intero dominio, se l'iperpiano contiene l'immagine): l'applicazione duale interpreta questa azione come proiettività tra gli spazi duali, ovviamente nella direzione opposta. Ciò si vede subito usando le analoghe proprietà della funzione duale per gli spazi vettoriali; si ricordi invece che l'immagine di un iperpiano per una applicazione lineare di solito non è un iperpiano.

Più in generale dalla formula $f^*(U^\perp) = (f^{-1}U)^\perp$ si ha la stessa interpretazione per ogni sottospazio.

3.1.9.2. Duali di immersioni e proiezioni. Chiaramente, immersioni e proiezioni sono nozioni duali tra loro. Infatti, se W è un sottospazio di V ($i : W \to V$ l'inclusione) e $\iota : \mathbb{P}(W) \to \mathbb{P}(V)$ è l'immersione corrispondente, allora $W^* \cong V^*/W^\perp$ è quoziente di V^*, e $\iota^* : \mathbb{P}(V^*) \to \mathbb{P}(W^*)$ è l'applicazione proiettiva associata alla mappa quoziente $i^* : V^* \to W^*$. Nell'altro senso, da $p : V \to V/W$ che definisce la proiezione $\pi : \mathbb{S}(V) \to \mathbb{S}(V/W)$, abbiamo che $(V/W)^* \cong W^\perp$ è sottospazio di V^* e $\pi^* : \mathbb{S}^*(V/W) \to \mathbb{S}^*(V)$ è l'inclusione definita dall'inclusione $p^* : (V/W)^* \cong W^\perp \to V^*$.

3.1.9.3. Duali di sezioni di stelle. Si tratta di una nozione autoduale.

3.1.9.4. Duali di proiezione tra sottospazi (tramite una stella). Si tratta di proiezioni tra stelle tramite un sottospazio.

3.1.9.5. Proposizione (Proiettività indotta sul duale.). *Data un proiettività $\varphi : \mathbb{S} \to \mathbb{S}$, la stessa funzione φ in quanto funzione tra gli spazi duali (che coincidono insiemisticamente con gli spazi stessi, si ricordi) si scrive $\varphi_* : \mathbb{S}^* \to \mathbb{S}^*$ ed è una proiettività la cui sovrastante è l'inversa della trasposta di una sovrastante di φ. Cioè, se $\varphi(\alpha_{\mathbb{S}} W) = \alpha_{\mathbb{S}}(fW)$, allora $\varphi_*(\alpha_{\mathbb{S}}^* W^*) = \alpha_{\mathbb{S}}^*(f^{-*}W^*)$, dove $f^{-*} = (f^*)^{-1} = (f^{-1})^*$ è l'inversa della trasposta.*

Dimostrazione. Basta chiaramente dimostrare il cioè, e per questo basta ricordare che $\alpha_{\mathbb{S}}^* = \alpha_{\mathbb{S}} \circ \tau$ (τ è il passaggio all'ortogonale). Dunque abbiamo

$$\varphi_*(\alpha_{\mathbb{S}}^* W^*) = \varphi(\alpha_{\mathbb{S}}^* W^*) = \varphi(\alpha_{\mathbb{S}}(W^{*\perp})) = \alpha_{\mathbb{S}}(f(W^{*\perp})) = \alpha_{\mathbb{S}}(f^{-*}(W^*)^\perp) = \alpha_{\mathbb{S}}^* f^{-*}(W^*)$$

poiché chiaramente $f(W^{*\perp}) = (f^{-*}(W^*))^\perp$ (si tratta degli elementi v con $(f^{-1}v) \circ W^* = 0$, cioè con $v \circ f^{-*}(W^*) = 0$). Si osservi per inciso che quest'ultima formula, $f(W^{*\perp}) = (f^{-*}(W^*))^\perp$, equivale a $f(W^{*\perp})^\perp = f^{-*}(W^*)$, e anche a $f^*(f(W^{*\perp})^\perp) = W^*$. □

3.1.9.6. Osservazione. Chiaramente φ_* è la proiettività inversa di φ^*, e questo bastava per dimostrare l'enunciato. Si noti però che questo enunciato non si può estendere ad applicazioni proiettive

che non siano proiettività: il punto è che se $\varphi : \mathbb{S} \to \mathbb{S}'$ è applicazione proiettiva (ma non proiettività) allora la funzione stessa φ pensata tra gli spazi duali (che coincidono insiemisticamente con gli spazi dati) semplicemente non è una applicazione proiettiva, cioè non ammette alcuna sovrastante lineare (perché?).

3.1.9.7. Interpretazione geometrica. Se π è un punto di $\mathbb{P}^*$, allora è un iperpiano di $\mathbb{P}$ e $\varphi_*\pi$ (in quanto punto di $\mathbb{P}^*$) è $\varphi\pi$ in quanto iperpiano di $\mathbb{P}$. Dunque possiamo scrivere $\varphi_*\pi = \bigvee_{P\in\pi} \varphi P$, il che caratterizza l'applicazione φ_*. *Si faccia attenzione che l'applicazione duale φ_* non è l'immagine inversa, quanto piuttosto l'immagine diretta, anche se qualcuno la denota con φ^* per ragioni storiche!*

Un altro modo per dire la stessa cosa è che $\varphi_* : \mathbb{P}^* \to \mathbb{P}^*$ rappresenta la restrizione a $\mathbb{I}$ della $\varphi : \mathbb{S} \to \mathbb{S}$.

♠ **3.1.10.** Reciprocità e sistemi nulli. Una reciprocità è un isomorfismo proiettivo di uno spazio proiettivo sul suo duale $\Phi : \mathbb{P}(V) \to \mathbb{P}^*(V)$. È equivalente ad avere un isomorfismo $V \to V^*$, o anche ad una forma bilineare non degenere $g : V \times V \to \Bbbk$. Una reciprocità si dice una polarità (risp. sistema nullo) se la forma g è simmetrica (risp. alternante).

Una reciprocità determina una corrispondenza biunivoca tra punti e iperpiani di $\mathbb{P}(V)$. Se si tratta di una polarità, un punto $P \in \mathbb{P}(V)$ e l'iperpiano $\Phi(P) \in \mathbb{P}^*(V) \cong \mathbb{I}(V)$ sono detti polo e polare uno dell'altro.

Una reciprocità Φ è polarità o sistema nullo se e solo se per ogni $P, Q \in \mathbb{P}(V)$ si ha $P \in \Phi(Q) \Leftrightarrow Q \in \Phi(P)$ (reciprocità). In tal caso, se la caratteristica del corpo $\Bbbk$ è diversa da 2, Φ è polarità (risp. sistema nullo) se e solo se esiste (risp. non esiste) un punto $P \in \mathbb{P}(V)$ tale che $P \notin \Phi(P)$.

3.2. ♠♠ Teoremi Fondamentali (della Geometria Proiettiva): proiezioni.

Abbiamo dato una definizione in termini di algebra lineare della nozione di trasformazione proiettiva tra spazi proiettivi. Tuttavia si vorrebbe dare un significato più geometrico a questa nozione, caratterizzando le trasformazione proiettiva come mappe (insiemistiche) dotate di certe proprietà, quali per esempio scriversi come composizione di proiezioni, oppure rispettare dati geometrici come l'allineamento di punti. Risultati di questo tipo si indicano come *teoremi fondamentali della Geometria Proiettiva.*

3.2.1. Proiettività e Proiezioni. Nei primi esempi di proiettività abbiamo parlato di proiezioni. Ci si può chiedere se ogni proiettività è una proiezione, o una composizione di proiezioni. Naturalmente per avere risposte affermative bisogna che gli spazi proiettivi in questione siano immersi in spazi più grandi per poter effettuare delle proiezioni tra loro.

3.2.2. Proposizione. *Siano L ed M varietà lineari sghembe in $\mathbb{P}$ della stessa dimensione s; allora ogni proiettività di L su M è una proiezione di centro una varietà lineare di dimensione s.*

Dimostrazione. Si considerino un sistema di riferimento proiettivo (P_i) su L e la sua immagine (Q_i) su M; per ogni retta $r_i = P_i \vee Q_i$ si scelga un punto R_i distinto dai due dati. Con questi punti si può costruire una varietà lineare, sghemba ad entrambe L ed M, ed avente la proprietà richiesta (la proiezione da L a M di quel centro dà la proiettività iniziale). Si osservi che il centro di proiezione non è unico... □

3.2.2.1. Esempi. Le proiettività tra rette sghembe (possiamo supporre nello spazio) sono tutte proiezioni di centro un'altra retta (sghemba con entrambe le date). Le proiettività tra piani sghembi (possiamo supporre nello spazio proiettivo di dimensione 5) sono tutte proiezioni di centro un altro piano (sghembo con entrambi i dati).

3.2.3. Proposizione. *Siano L ed M varietà lineari della stessa dimensione in $\mathbb{P}$ spazio proiettivo di dimensione abbastanza grande; allora ogni proiettività di L su M è composizione di al più due proiezioni.*

Dimostrazione. Basta scegliere una terza varietà della stessa dimensione e sghemba con entrambe (per questo occorre una condizione sulla dimensione dello spazio ambiente), componendo la proiettività data con una proiezione qualsiasi, applicando poi il risultato precedente alla composizione. □

3.2.4. Proposizione. *Siano L, M ed N varietà lineari in $\mathbb{P}$ tali che N sia sghemba con le altre due e $L \vee N = M \vee N$. Allora $P \mapsto (P \vee N) \wedge M$ induce una proiettività di L su M che è l'identità su $L \wedge M$. Inoltre si può supporre $N = N \wedge (L \vee M)$, ovvero $N \leqslant (L \vee M)$, e quindi che l'intera costruzione sia fatta in $L \vee M$. Viceversa, una proiettività di L su M che sia l'identità su $L \wedge M$ è proiezione di M su L da un centro di dimensione* $\dim(L) - \dim(L \wedge M) - 1$.

Dimostrazione. Problema. □

3.2.5. Proposizione. *Siano L ed M varietà lineari della stessa dimensione s in $\mathbb{P}$; sia data una proiettività di L su M che sia l'identità ristretta a $N \subseteq L \wedge M$ di dimensione $s - i$ $(1 \leqslant i \leqslant s+1)$. Allora la proiettività è composizione di al più i proiezioni da punti.*

Ogni proiettività tra varietà lineari di dimensione s in $\mathbb{P}$ è prodotto di al più $s + 2$ proiezioni da punti.

Dimostrazione. Problema. □

3.3. ♠♠ Teoremi Fondamentali (della Geometria Proiettiva): collineazioni.

3.3.1. Proiettività e Collineazioni. Si osserva facilmente che le proiettività sono collineazioni, cioè che trasformano terne di punti allineati in terne di punti allineati. Ci si può chiedere se il viceversa è vero, cioè se ogni collineazione è una proiettività. In generale è falso. Questo è dovuto a due ordini di ragioni:

(*i*) nel caso della retta proiettiva, $\dim \mathbb{S} = 1$, la struttura dell'insieme ordinato $\mathbb{S}(V)$ è troppo povera: essendo tutti i punti allineati, ogni applicazione è una collineazione; per caratterizzare le proiettività della retta troveremo un invariante geometrico più fine (il concetto di birapporto e di armonia);

(*ii*) se $\sigma \neq \mathrm{id}_{\Bbbk}$ è un automorfismo del corpo $\Bbbk$, l'applicazione φ di $\Bbbk^n$ in sè definita da $(x_1, \dots, x_n) \mapsto (\sigma(x_1), \dots, \sigma(x_n))$ non è un automorfismo dello spazio vettoriale $\Bbbk^n$, ma induce una collineazione di $\mathbb{P}^n(\Bbbk)$ in sè.

3.3.2. Definizione. *Se $\sigma : \Bbbk \longrightarrow \Bbbk'$ è un isomorfismo di corpi, e V, V' spazi vettoriali su $\Bbbk$, $\Bbbk'$ risp., una applicazione di gruppi $f : V \longrightarrow V'$ si dice σ-lineare se $f(cv) = c^\sigma f(v)$ per ogni $c \in \Bbbk$ e $v \in V$. Una applicazione σ-lineare biiettiva si dice un σ-isomorfismo. Una applicazione $\mathbb{P}(V) \longrightarrow \mathbb{P}(V')$ si dice una σ-proiettività se è indotta da un σ-isomorfismo.*

3.3.2.1. Come si vede, le applicazioni lineari sono particolari applicazioni σ-linari ($\sigma = \mathrm{id}_{\Bbbk}$). Da notare inoltre che se $\Bbbk = \Bbbk' = \mathbb{R}$, allora l'unico automorfismo di corpo è l'applicazione indentica (dipende dalla struttura d'ordine dei reali). Se invece $\Bbbk = \Bbbk' = \mathbb{C}$, allora esistono due automorfismi di corpo: l'identità ed il coniugio.

3.3.2.2. Per le applicazioni σ-linari possiamo sviluppare le stesse tecniche di calcolo matriciale che per le applicazioni lineari.

3.3.3. Teorema. *Siano $\mathbb{P}$ e $\mathbb{P}'$ spazi proiettivi di dimensione $n \geqslant 2$ sui corpi $\Bbbk$ e $\Bbbk'$ e di spazi sovrastanti V e V' rispettivamente. Una applicazione $\psi : \mathbb{P} \longrightarrow \mathbb{P}'$ è una collineazione (i.e. una biiezione che conservi l'allineamento dei punti) se e solo se è una σ-proiettività per un ben determinato isomorfismo di corpi $\sigma : \Bbbk \to \Bbbk'$ (che dipende da ψ). Se $\Bbbk = \Bbbk' = \mathbb{R}$: le proiettività tra spazi di dimensione $n \geqslant 2$ sono le collineazioni.*

Dimostrazione. Lunga e complicata! Vedi Barsotti, oppure Candilera, oppure Gerotto. □

3.4. Teoria di Jordan delle proiettività (omologie, involuzioni....)

In questo paragrafo proponiamo la classificazione delle proiettività per retta, piano e spazio proiettivi su un corpo algebricamente chiuso. Nel caso della retta studieremo anche il caso del corpo reale, e il caso di un corpo arbitrario.

Siano V uno spazio vettoriale sul corpo $\Bbbk$, $\mathbb{P} = \mathbb{P}(V)$ uno spazio proiettivo di dimensione n, φ una proiettività di $\mathbb{P}(V)$ in sè e f uno degli automorfismi di V che induce φ. La proiettività φ induce una applicazione biiettiva di $\mathbb{S} = \mathbb{S}(V)$ in sè che indicheremo ancora con φ, o con $\mathbb{S}(f)$, se è necessario essere più precisi.

3.4.1. Definizione (Elementi uniti di una Proiettività). *Data una proiettività $\varphi : \mathbb{S} \longrightarrow \mathbb{S}$, un elemento $s \in \mathbb{S}$ si dice unito per φ (o sotto φ) se $\varphi(s) = s$. Si dice elemento di punti uniti se $\varphi(P) = P$ per ogni punto $P \leqslant s$, nel qual caso tutti gli elementi di s sono uniti (e anzi, di punti uniti).*

3.4.1.1. Ad esempio un punto P è unito per φ se viene mandato in sè stesso: $\varphi(P) = P$. Una retta r è unita se $\varphi(r) = r$; si dice invece una *retta di punti uniti* se $\varphi(P) = P$ per ogni $P \in r$. Ovviamente una retta di punti uniti è una retta unita; il viceversa essendo in generale falso.

Studiamo come cercare punti uniti ed iperpiani uniti di una proiettività.

3.4.2. Punti uniti e autovettori. Scelto un riferimento su $\mathbb{P}$, possiamo rappresentare i suoi punti con coordinate omogenee X, e $\varphi : \mathbb{P} \longrightarrow \mathbb{P}$ con una matrice $A \in \mathrm{PGL}(n, \Bbbk)$ (cioè una matrice quadrata invertibile d'ordine $n+1$ a meno di proporzionalità). Che un punto $P = \langle v \rangle$ sia unito per φ significa allora che v è un autovettore per l'applicazione f, ovvero che le sue coordinate x_P sono un autovettore della matrice A. Infatti poiché $P = \langle v \rangle$, abbiamo $\varphi(P) = \langle f(v) \rangle$ cosicché

$$\varphi(P) = P \qquad \text{se e solo se} \qquad f(v) = \lambda v$$

ovvero

$$\varphi(P) = P \qquad \text{se e solo se} \qquad Ax_P = \lambda x_P$$

per qualche autovalore λ (necessariamente non nullo).

Dunque: *cercare i punti uniti di una proiettività equivale a cercare gli autovettori di una applicazione lineare f sovrastante φ, ovvero di una matrice che rappresenti la proiettività.*

3.4.3. Proposizione. *Ogni proiettività che abbia tutti i suoi autovalori in $\Bbbk$ (se $\Bbbk$ è algebricamente chiuso allora ogni proiettività) ammette almeno una bandiera (i.e. una catena $L_0 \subset L_1 \subset \cdots \subset L_{n-1}$) di varietà unite, e ogni varietà unita si inserisce in una tale bandiera.*

Dimostrazione. Basta ricondursi alla forma di Jordan? □

3.4.4. Osserviamo che, scelto un riferimento proiettivo, la matrice A è determinata a meno di moltiplicazione per uno scalare (come pure l'applicazione f), dunque i suoi autovalori *non* sono invarianti della proiettività; i rapporti tra gli autovalori invece lo sono, cioè non dipendono dalla matrice scelta per rappresentare la proiettività. Quindi la frase "il punto unito P è associato all'autovalore λ" ha senso solo se si fissa la matrice A; invece la frase "i punti fissi P e Q sono associati allo stesso autovalore (oppure: a due autovalori distinti, oppure: a due autovalori opposti)" ha senso indipendentemente dalla matrice scelta per rappresentare la proiettività.

Osserviamo che se due punti uniti distinti sono associati allo stesso autovalore, allora tutta la retta congiungente è fatta di punti uniti associati a quello stesso autovalore; cioè si tratta di una retta di punti uniti. Se invece due punti uniti sono associati a due autovalori distinti (e dunque sono due punti distinti), allora la retta che li congiunge è una retta unita, ma non una retta di punti uniti (e anzi gli unici punti uniti di quella retta sono i due dati). Generalizzare l'affermazione a tre o più punti.

3.4.5. Iperpiani uniti e autovettori della matrice trasposta. Un iperpiano π di $\mathbb{P}$ è definito da una equazione $a_\pi X = 0$, una volta fissato un riferimento in $\mathbb{P}$ (ricordiamo che a_π si dicono le coordinate plückeriane di π, e sono le sue coordinate in quanto punto dello spazio proiettivo duale, usando il riferimento duale di quello scelto in $\mathbb{P}$). Questo significa che

$$\pi = \{P \in \mathbb{P} \text{ tali che } a_\pi x_P = 0\} \ .$$

L'immagine di π tramite φ è data dall'iperpiano $\varphi(\pi)$:

$$\begin{aligned}
\varphi(\pi) &= \{Q \in \mathbb{P} \text{ tali che } Q = \varphi(P) \text{ con } P \in \pi\} \\
&= \{Q \in \mathbb{P} \text{ tali che } x_Q = Ax_P \text{ e } a_\pi x_P = 0\} \\
&= \{Q \in \mathbb{P} \text{ tali che } A^{-1}x_Q = x_P \text{ e } a_\pi x_P = 0\} \\
&= \{Q \in \mathbb{P} \text{ tali che } a_\pi A^{-1} x_Q = 0\} \ .
\end{aligned}$$

che è dunque definito dalla equazione $(a_\pi A^{-1})X = 0$, cioè ha coordinate plückeriane $a_\pi A^{-1}$. Si osservi per inciso, con conti simili, che l'antimmagine tramite φ di un iperpiano π di coordinate a_π è l'iperpiano di coordinate $a_\pi A$.

Dunque un iperpiano di equazione $aX = 0$ è unito se e solo se abbiamo $aA^{-1} = \mu a$ per qualche $\mu \in \Bbbk$ (necessariamente diverso da zero), cioè se e solo se $aA = \lambda a$ per qualche λ (necessariamente diverso da zero), o infine se e solo se a^{t} è un autovettore di A^{t}.

Conclusione: *cercare gli iperpiani uniti di una proiettività equivale a cercare gli autovettori della trasposta di una matrice che rappresenti la proiettività*

3.4.6. Relazioni tra punti uniti e iperpiani uniti. È utile avere dei criteri per capire quando un punto unito ed un iperpiano unito si appartengano. Un risultato è facile:

(1) *se un punto unito ed un iperpiano unito sono associati ad autovalori distinti, allora si appartengono (cioè il punto appartiene all'iperpiano).* Infatti, sia P il punto unito con $Ax_P = \lambda x_P$ e sia π l'iperpiano unito con $a_\pi A = \mu a_\pi$, e sia $\lambda \neq \mu$; allora

$$(\lambda - \mu)a_\pi x_P = \lambda a_\pi x_P - \mu a_\pi x_P = a_\pi A x_P - a_\pi A x_P = 0$$

da cui $a_\pi x_P = 0$, cioè $P \in \pi$.

Nel caso invece in cui punto e piano sono associati allo stesso autovalore, la situazione è più complicata; se l'autovalore ha molteplicità algebrica uno, allora ha associati un unico punto unito ed un unico iperpiano unito che non si appartengono. Dunque:

(2) *se un punto unito ed un iperpiano unito sono associati allo stesso autovalore e si appartengono, allora l'autovalore ha molteplicità maggiore di uno.*

Più precisamente:

(3) *se un autovalore ha associati un unico punto unito ed un unico iperpiano unito, allora questi si appartengono se e solo se l'autovalore ha molteplicità maggiore di uno.*

Facendo riferimento alla forma di Jordan, possiamo dire che *ogni blocco elementare di Jordan ha associati un unico punto unito e un unico iperpiano unito, e il punto unito appartiene a tutti gli iperpiani uniti associati agli altri blocchi elementari (siano o no dello stesso autovalore), ed appartiene al piano unito del suo stesso blocco elementare se e solo se il blocco stesso ha ordine maggiore di* 1. Si vede subito esplicitando le coordinate nel riferimento in cui si ha la forma di Jordan.

3.4.7. Dualità. Un punto di vista migliore per studiare i fenomeni precedenti è il seguente. Ad ogni proiettività φ di $\mathbb{P}(V)$ in sè corrisponde canonicamente la proiettività φ_* di $\mathbb{P}^* = \mathbb{P}^*(V)$ in sè (nella stessa direzione!), univocamente determinata dalla condizione $\varphi_*(\pi) = \bigvee_{P\in\pi} \varphi(P)$ (immagine dell'iperpiano π).

Se si fissa un riferimento su $\mathbb{P}(V)$, la proiettività φ è descritta da una matrice $A \in \mathrm{GL}_{n+1}(\Bbbk)$, determinata a meno di un fattore non nullo, nel modo seguente: $x_{\varphi P} = Ax_P$, ove $x = x_P$ indica la matrice colonna $(x_0, \dots, x_n)^{\mathrm{t}}$ delle coordinate di P, per ogni $P \in \mathbb{P}(V)$. Poi, se su $\mathbb{P}^*(V)$ si fissa il riferimento duale, cosicché l'iperpiano di $\mathbb{P}(V)$ di equazione $a_0X_0 + \ldots + a_nX_n = 0$ abbia coordinate $a = (a_0 \ldots a_n)$, la proiettività φ_* è descritta dalla matrice A^{-1}, nel modo seguente: $a_{\varphi_*\pi} = a_\pi A^{-1}$, ove $a = a_\pi$ indica la matrice riga $(a_0, \dots, a_n)$ delle coordinate di π, per ogni $\pi \in \mathbb{P}^*(V)$.

Queste affermazioni si verificano facilmente osservando che:

$$P \in \pi \quad \text{sse} \quad a_\pi x_P = 0 \quad \text{sse} \quad (a_\pi A^{-1})(Ax_P) = 0 \quad \text{sse} \quad \varphi(P) \in \varphi^*(\pi).$$

3.4.7.1. Lemma. *Se la matrice $A \in M_n(\Bbbk)$ ha tutti gli autovalori in $\Bbbk$, allora A è simile in $\Bbbk$ ad A^{t}; in particolare A e A^{t} hanno gli stessi autovalori con uguali molteplicità e nullità (ma in generale gli autospazi sono diversi).*

Dimostrazione. Ci si riconduce subito a mostrare che ogni matrice di Jordan è simile alla propria trasposta, il che è quasi ovvio (basta rovesciare l'ordine della base di ogni blocco di Jordan). □

3.4.7.2. Quindi ad ogni autovalore ϱ di A restano associate una sottovarietà lineare U_ϱ di $\mathbb{P}(V)$ i cui punti sono uniti per φ, ed una sottovarietà lineare V_ϱ^* di $\mathbb{P}^*(V)$ (che, detto per inciso, è una stella di iperpiani di centro un sottospazio V_ϱ di $\mathbb{P}(V)$) i cui punti sono uniti per φ_*, entrambe di dimensione $\mathrm{N}(\varrho) - 1$.

Questa affermazione si verifica osservando che gli elementi uniti di φ_* e $\varphi^* = (\varphi_*)^{-1}$ coincidono, e che A^{t} è una delle matrici di $(\varphi_*)^{-1}$, cioè: $a^{\mathrm{t}}_{(\varphi_*)^{-1}(\pi)} = A^{\mathrm{t}} a^{\mathrm{t}}_\pi$.

Si può dire questo in modo suggestivo, anche se impreciso, dicendo che *ogni proiettività ha la stessa configurazione di punti e di iperpiani uniti.*

3.4.7.3. Supponiamo che ϱ_1, ϱ_2 siano due autovalori distinti di A. Siano P_j un punto unito associato a ϱ_j e I_j un iperpiano unito associato a ϱ_j, ove $j = 1, 2$; allora $P_1 \in I_2$.

Supponiamo ora che ϱ sia un autovalore di A e $\mathrm{N}(\varrho) = 1$. Siano P ed I il punto e l'iperpiano uniti corrispondenti a ϱ; allora $P \in I$ se e solo se $\mathrm{M}(\varrho) > 1$.

Più in generale, le sottovarietà U_ϱ e V_ϱ^*, dei punti uniti di $\mathbb{P}(V)$ e $\mathbb{P}^*(V)$ associate a ϱ, si appartengono se $\mathrm{M}(\varrho) > \mathrm{N}(\varrho)$. Più precisamente, possiamo discutere la posizione reciproca del sottospazio di punti fissi U_ϱ e del centro V_ϱ della stella V_ϱ^*: la dimensione dell'intersezione è pari al numero di blocchi di Jordan relativi a ϱ e d'ordine strettamente maggiore di uno, o in modo più intrinseco alla dimensione dell'autospazio di ϱ quando si passa al quoziente modulo U_ϱ...

3.4.8. Involuzioni. Le involuzioni sono le proiettività φ non identiche tali che φ^2 sia l'identità. Se $\Bbbk$ è algebricamente chiuso (o anche solo chiuso per radici quadrate), una proiettività è una involuzione sse esistono due sottospazi complementari L ed M di punti uniti, e associati a due autovalori uno opposto dell'altro (infatti l'applicazione lineare sovrastante è di quadrato scalare, quindi ha polinomio minimo che divide $X^2 - k$). Per ogni retta $P \vee Q$ con $P \in L$ e $Q \in M$ la proiettività indotta è una involuzione avente P e Q come punti uniti.

3.4.8.1. Nel caso delle rette proiettive: una proietività è una involuzione sse esiste una coppia di punti involutoria ($P \neq Q$ tali che $\varphi(P) = Q$ e $\varphi(Q) = P$: si vede subito usando le matrici che il quadrato è scalare); inoltre esiste unica l'involuzione una volta assegnate due coppie involutorie (in particolare se vengono assegnati due punti fissi distinti).

3.4.8.2. Come si scrivono le involuzioni in termini di trasformazioni di Moebius? Sono matrici del tipo $\begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix}$ (basta imporre che il quadrato sia multiplo dell'identità), quindi $\varphi(X) = \frac{\gamma - \alpha X}{\alpha + \beta X}$.

In particolare quella che fissa $a, b \in \Bbbk$ è $\varphi(X) = \frac{2ab - (a+b)X}{(a+b) + 2X}$; quella che fissa ± 1 è $\varphi(X) = 1/X$. Quella che fissa $0, \infty$ è $\varphi(X) = -X$.

L'affinità che scambia $a, b \in \Bbbk$ è $\varphi(X) = (a + b) - X$; la proiettività che scambia 0 e ∞ è $\varphi(X) = 1/X$, in generale quella che scambia a e ∞ è $\varphi(X) = a + 1/(X - a)$.

3.4.8.3. Una volta introdotta la nozione di birapporto, potremo vedere chiaramente la relazione tra involuzioni e simmetrie affini: ma si può subito osservare che, nelle usuali coordinate, se uno dei due sottospazi di punti uniti è contenuto nell'iperpiano all'infinito $X_0 = 0$, allora l'involuzione è la affinità data dalla simmetria avente quella direzione e con asse l'altro sottospazio di punti uniti...

3.4.8.4. Duali delle involuzioni. Si vede immediatamente che l'applicazione duale di una involuzione è ancora una involuzione.

3.4.9. Omologie. Una omologia è una proiettività non identica con un iperpiano di punti uniti, detto asse di omologia; per dualità esiste un punto unito centro di una stella di iperpiani uniti, detto centro di omologia; l'omologia si dice speciale o generale a seconda che il centro appartenga o no all'asse. La matrice di una omologia in un riferimento che estenda un riferimento dell'asse è del tipo

$$\begin{pmatrix} \mu & 0 \cdots 0 \\ 0 & \\ \vdots & \lambda\mathbb{I} \\ 0 & \end{pmatrix} \qquad \text{ovvero} \qquad \begin{pmatrix} \lambda & 1 \cdots 0 \\ 0 & \\ \vdots & \lambda\mathbb{I} \\ 0 & \end{pmatrix}$$

a seconda che sia generale (il centro è il primo punto del riferimento), e allora il rapprto μ/λ si dice l'invariante dell'omologia e per ogni punto P fuori dell'asse e diverso dal centro si ha $(C\ H\ P\ \varphi(P)) = \mu/\lambda$; ovvero speciale (l'ulteriore punto del riferimento appartiene ad una retta unita esterna all'asse, il centro è il primo punto del riferimento, l'asse è $P_0 \vee P_2 \vee \cdots \vee P_n$).

3.4.9.1. Costruzione grafica delle omologie. Una volta noti asse a e centro C di una omologia, essa è determinata dall'immagine φP di un qualunque punto non unito P. Infatti le rette del fascio di centro C sono rette unite (non di punti uniti), e questo permette le seguenti costruzioni

grafiche:

cioè: per Q arbitrario si trova φQ come intersezione tra la retta unita $Q \vee C$ (unita perché contiene C, quindi appartiene al fascio di rette unite), e la retta immagine di $Q \vee P$, che si ottiene come retta passante per φP (noto) e l'intersezione di $Q \vee P$ con l'asse (che è un punto fisso).

La costruzione funziona per punti Q che non appartengono a $P \vee C$; come costruire graficamente le immagini dei punti di $C \vee P$?

3.4.9.2. Composizione delle omologie. In generale la composizione di due omologie non è una omologia, e anzi ci si può chiedere se ogni proiettività è composizione di omologie. Tuttavia:

(1) la composizione di due omologie di ugual asse è ancora una omologia; commutano tra loro? cosa si può dire della posizione reciproca dei tre centri? Discutere i casi sia speciali che non.
(2) per la composizione di due omologie di ugual centro?

3.4.9.3. Duali delle omologie. Si vede immediatamente che l'applicazione duale di una omologia è ancora una omologia (dello stesso tipo).

3.4.10. Proiettività della Retta. Una proiettività $\varphi : \mathbb{P}^1(\Bbbk) \to \mathbb{P}^1(\Bbbk)$, scelto un sistema di riferimento proiettivo, si rappresenta tramite una matrice invertibile A d'ordine 2 a meno di proporzionalità.

3.4.10.1. Caso di un corpo algebricamente chiuso. Se $\Bbbk$ è algebricamente chiuso, le forme canoniche di Jordan classificano le proiettività di $\mathbb{P}^1(\Bbbk)$ in sè. Si hanno solo tre forme:

(1) l'identità (di matrice $\lambda\mathbb{I}$ con $\lambda \neq 0$); questo caso si verifica quando il polinomio caratteristico della matrice A ha un unico autovalore, dunque di molteplicità algebrica 2, e che abbia molteplicità geometrica 2, cioè che abbia due autovettori indipendenti;
(2) l'omologia generale con due punti uniti distinti; questo caso si verifica quando il polinomio caratteristico della matrice A ha due autovalori distinti $\lambda \neq \mu$, e dunque due autovettori indipendenti (in un riferimento di autovettori, la matrice di φ diventa $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \mu\end{smallmatrix}\right)$ con $\lambda \neq \mu$ non nulli),
(3) l'omologia speciale con un solo punto unito; questo caso si verifica quando il polinomio caratteristico della matrice A ha un unico autovalore, dunque di molteplicità algebrica 2, e che abbia molteplicità geometrica 1, cioè che abbia autospazio di dimensione 1 (in questo caso si può scegliere un riferimento in cui φ è rappresentato dalla matrice $\left(\begin{smallmatrix}\lambda & 1\\ 0 & \lambda\end{smallmatrix}\right)$ con $\lambda \neq 0$).

Questi casi concludono la classificazione su un corpo algebricamente chiuso, poiché non vi sono altre possibilità per gli autovalori e le loro molteplicità.

3.4.10.2. Caso di un corpo arbitrario. Se $\Bbbk$ è qualsiasi, definiamo $\Delta(A) := \operatorname{tr}(A)^2 - 4\det(A)$; Si tratta del discriminante del polinomio di secondo grado

$$X^2 - \operatorname{tr}(A)X + \det(A)$$

che è il polinomio caratteristico della matrice A.

Una proiettività non identica si dice parabolica se $\Delta(A) = 0$, iperbolica se $\Delta(A)$ è quadrato in $\Bbbk$, ellittica se $\Delta(A)$ non è quadrato in $\Bbbk$ (queste condizioni dipendono solo dalla proiettività e non dalla matrice che la rappresenta). Tenendo conto che gli autovalori si calcolano con la classica formula

$$x_{1,2} = \frac{\operatorname{tr}(A) \pm \sqrt{\Delta(A)}}{2}$$

si vede che per una proiettività parabolica il polinomio caratteristico ha un unico autovalore, di molteplicità algebrica 2 e geometrica 1 (altrimenti la proiettività sarebbe identica); per proiettività

iperboliche vi sono due autovalori distinti in $\Bbbk$; per proiettività ellittiche non vi sono autovalori in $\Bbbk$ (dunque si tratta di matrici che non sono nemmeno triangolarizzabili in $\Bbbk$), ma vi sono due autovalori distinti in $\Bbbk[\sqrt{\Delta}]$.

Una proiettività è parabolica, iperbolica, ellittica a seconda che abbia un unico punto unito (necessariamente razionale su $\Bbbk$), due punti uniti distinti in $\mathbb{P}^1(\Bbbk)$, nessuno punto unito razionale su $\Bbbk$ (e allora ha due punti uniti in $\mathbb{P}^1(\Bbbk[\sqrt{\Delta}])$).

Conclusione: le proiettività si classificano come segue:

(1) l'identità;

(2) proiettività iperboliche (hanno due autovalori distinti in $\Bbbk$, dunque due punti uniti distinti in $\mathbb{P}^1(\Bbbk)$, e si riconoscono dal fatto che $\Delta(A)$ sia quadrato in $\Bbbk$);

(3) proiettività paraboliche (hanno un solo autovalore, necessariamente in $\Bbbk$, dunque un solo punto unito, necessariamente in $\mathbb{P}^1(\Bbbk)$, e si riconoscono dal fatto che $\Delta(A) = 0$);

(4) proiettività ellittiche (sono prive di autovalori in $\Bbbk$ e hanno due autovalori distinti in $\Bbbk[\sqrt{\Delta}]$; dunque non hanno alcun punto unito in $\mathbb{P}^1(\Bbbk)$, e hanno due punti uniti distinti in $\mathbb{P}^1(\Bbbk[\sqrt{\Delta}])$, e si riconoscono dal fatto che $\Delta(A)$ non sia quadrato in $\Bbbk$).

3.4.10.3. Studio delle involuzioni. Se $\Bbbk$ è un corpo di caratteristica 2, allora tutte le proiettività paraboliche sono involuzioni (con un unico punto unito), e viceversa ogni involuzione è parabolica. Se invece la caratteristica del corpo è diversa da due, allora non esistono involuzioni paraboliche, e le involuzioni sono ellittiche o iperboliche a seconda che $\det(A)$ sia un quadrato o no in $\Bbbk$.

3.4.10.4. Caso del corpo reale. In questo caso abbiamo che $\Delta(A)$ è un quadrato se e solo se $\Delta(A) \geqslant 0$. Dunque la proiettività è iperbolica, ellittica, parabolica a seconda che $\Delta(A)$ sia positivo, negativo o nullo.

Se poi si tratta di una involuzione, allora non è parabolica, ed è ellittica o iperbolica a seconda che $\det(A)$ sia positivo o negativo.

Osservazione. Se P, Q sono punti distinti, non uniti e non uno l'immagine dell'altro per l'involuzione φ, allora φ è ellittica o iperbolica a seconda che il birapporto $(P\ \varphi(P)\ Q\ \varphi(Q))$ sia negativo o positivo.

3.4.10.5. Esercizi. Studiare le proiettività di matrici

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 3 & 1 \\ 7 & -3 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & -1 \\ 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix},$$

sulle rette proiettive sopra i corpi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

3.4.11. Proiettività del Piano. Se $\Bbbk$ è algebricamente chiuso, le forme canoniche di Jordan classificano le proiettività di $\mathbb{P}^2(\Bbbk)$ in sè. Si hanno sei forme:

(*i*) l'identità (di matrice $\lambda\mathbb{I}$ con $\lambda \neq 0$);

(*ii*) $\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \mu \end{pmatrix}$ con $\lambda \neq \mu$ non nulli, è l'omologia generale (centro P_0 e asse $P_1 \vee P_2$);

(*iii*) $\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$ con $\lambda \neq 0$, è l'omologia speciale (centro P_0 e asse $P_0 \vee P_2$);

(*iv*) $\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \nu \end{pmatrix}$ con λ, μ, ν distinti e non nulli, vi sono tre punti e tre rette unite;

(*v*) $\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix}$ con $\lambda \neq \mu$ non nulli, vi sono due punti uniti P_0 e P_2, e due rette unite $P_0 \vee P_1$ e $P_0 \vee P_2$;

(*vi*) $\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$ con $\lambda \neq 0$, vi è un unico punto unito P_0 e un'unica retta unita $P_0 \vee P_1$.

3.4.12. Proiettività dello Spazio. Se $\Bbbk$ è algebricamente chiuso, le forme canoniche di Jordan classificano le proiettività di $\mathbb{P}^3(\Bbbk)$ in sè. Si hanno quattordici forme (non facciamo l'elenco di tutti i sottospazi uniti: per esercizio, determinare piani e rette uniti in ogni caso, e specificare che tipi di proiettività vi vengono indotte):

(*i*) l'identità (di matrice $\lambda\mathbb{I}$ con $\lambda \neq 0$);

(*ii*) $\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$ omologia speciale di asse $P_0 \vee P_2 \vee P_3$ e centro P_0; sono uniti i piani e le rette passanti per il centro;

(*iii*) $\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$ la retta $P_0 \vee P_3$ è di punti uniti, la retta $P_0 \vee P_1$ è unita, il piano $P_0 \vee P_1 \vee P_2$ è unito;

(*iv*) $\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$ $P_0 \vee P_2$ è retta di punti uniti, le rette $P_0 \vee P_1$ e $P_2 \vee P_3$ sono unite, i piani $P_0 \vee P_1 \vee P_2$ e $P_0 \vee P_2 \vee P_3$ sono uniti;

(*v*) $\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$ il punto P_0, la retta $P_0 \vee P_1$ e il piano $P_0 \vee P_1 \vee P_2$ sono uniti;

(*vi*) $\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix}$ con $\lambda \neq \mu$; $P_0 \vee P_1$ e $P_2 \vee P_3$ sono rette di punti uniti, e sono uniti i piani dei fasci di asse quelle due rette;

(*vii*) $\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix}$ con $\lambda \neq \mu$; la retta $P_2 \vee P_3$ è di punti uniti, la retta $P_0 \vee P_1$ e i piani che la contengono sono uniti;

(*viii*) $\begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \mu & 1 \\ 0 & 0 & 0 & \mu \end{pmatrix}$ con $\lambda \neq \mu$; i punti P_0 e P_2, le rette $P_0 \vee P_1$ e $P_2 \vee P_3$, i piani $P_0 \vee P_1 \vee P_2$ e $P_0 \vee P_2 \vee P_3$ sono uniti;

(*ix*) $\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix}$ con $\lambda \neq \mu$; è l'omologia generale di asse $P_1 \vee P_2 \vee P_3$ e centro P_0;

(*x*) $\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \mu & 1 & 0 \\ 0 & 0 & \mu & 0 \\ 0 & 0 & 0 & \mu \end{pmatrix}$ con $\lambda \neq \mu$; i punti P_0 e quelli della retta $P_1 \vee P_3$, sono uniti; il piano $P_1 \vee P_2 \vee P_3$ e le rette di quel piano contenenti P_1 sono uniti;

(*xi*) $\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \mu & 1 & 0 \\ 0 & 0 & \mu & 1 \\ 0 & 0 & 0 & \mu \end{pmatrix}$ con $\lambda \neq \mu$; i punti P_0 e P_1, la retta $P_1 \vee P_2$ ed il piano $P_1 \vee P_2 \vee P_3$ sono uniti;

(*xii*) $\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \nu & 0 \\ 0 & 0 & 0 & \nu \end{pmatrix}$ con λ, μ e ν distinti; P_0, P_1 e i punti della retta $P_2 \vee P_3$ sono uniti; sui piani uniti $P_0 \vee P_2 \vee P_3$ e $P_1 \vee P_2 \vee P_3$ sono indotte omologie generali;

(*xiii*) $\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \nu & 1 \\ 0 & 0 & 0 & \nu \end{pmatrix}$ con λ, μ e ν distinti; P_0, P_1 e P_2 sono punti uniti, la retta $P_2 \vee P_3$ è unita; i piani $P_0 \vee P_2 \vee P_3$ e $P_1 \vee P_2 \vee P_3$ sono uniti;

(*xiv*) $\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 \\ 0 & 0 & \nu & 0 \\ 0 & 0 & 0 & \xi \end{pmatrix}$ con i quattro autovalori distinti; i quattro punti fondamentali sono uniti, come pure i quattro iperpiani e i sei assi; sono tutti e soli i sottospazi uniti.

4. Spazi Proiettivi, Spazi Affini e Spazi Euclidei.

4.1. Caso Standard. L'immersione standard

$$\mathbb{A}^n(\Bbbk) \longrightarrow \mathbb{P}^n(\Bbbk) \qquad \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \longmapsto \begin{pmatrix} 1 \\ X_1 \\ \vdots \\ X_n \end{pmatrix}$$

determina un isomorfismo di $\mathbb{A}^n(\Bbbk)$ sul sottinsieme (aperto) $U_0 = \{X \in \mathbb{P}^n(\Bbbk) \ : \ X_0 \neq 0\}$ di $\mathbb{P}^n(\Bbbk)$. L'applicazione inversa è

$$U_0 \longrightarrow \mathbb{A}^n(\Bbbk) \qquad \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_n \end{pmatrix} \longmapsto \begin{pmatrix} X_1/X_0 \\ \vdots \\ X_n/X_0 \end{pmatrix} .$$

4.1.1. Descrizione ricorsiva di $\mathbb{P}^n(\Bbbk)$. Tenendo conto che $\mathbb{P}^n(\Bbbk) \smallsetminus U_0$ è un iperpiano di $\mathbb{P}^n(\Bbbk)$ (di equazione $X_0 = 0$), e dunque isomorfo a $\mathbb{P}^{n-1}(\Bbbk)$, possiamo vedere che $\mathbb{P}^n(\Bbbk)$ è unione disgiunta di uno spazio affine $\mathbb{A}^n(\Bbbk)$ della stessa dimensione e di uno spazio proiettivo di dimensione di uno minore $\mathbb{P}^{n-1}(\Bbbk)$ che svolge il ruolo di "orizzonte" per lo spazio affine. Ricorsivamente abbiamo:

$$\begin{aligned} \mathbb{P}^n(\Bbbk) &= \mathbb{A}^n(\Bbbk) \sqcup \mathbb{P}^{n-1}(\Bbbk) \\ &= \mathbb{A}^n(\Bbbk) \sqcup \mathbb{A}^{n-1}(\Bbbk) \sqcup \mathbb{P}^{n-2}(\Bbbk) \\ &= \cdots \\ &= \mathbb{A}^n(\Bbbk) \sqcup \mathbb{A}^{n-1}(\Bbbk) \sqcup \cdots \sqcup \mathbb{A}^1(\Bbbk) \sqcup \mathbb{A}^0(\Bbbk) \ . \end{aligned}$$

Questa descrizione indica bene che $\mathbb{P}^n$ non è il prodotto cartesiano di copie di $\mathbb{P}^1$ (contrariamente ad $\mathbb{A}^n$ che invece è $(\mathbb{A}^1)^n$). In effetti sia $\mathbb{P}^n$ che $(\mathbb{P}^1)^n$ sono compattificazioni di $\mathbb{A}^n$ (nel senso che sono spazi compatti contenenti $\mathbb{A}^n$), ma di forma molto diversa (e il primo contiene meno punti, aggiungendo ad $\mathbb{A}^n$ solo le direzioni delle sue rette).

4.2. Teorema (Affinità e Proiettività). *Una matrice $A \in \mathrm{PGL}(n, \Bbbk)$ di una proiettività di $\mathbb{P}^n(\Bbbk)$ si restringe ad una affinità di $\mathbb{A}^n(\Bbbk)$ se e solo se è (proporzionale a una) della forma $B = \left(\begin{smallmatrix} 1 & 0 \\ a & B' \end{smallmatrix}\right)$ con $B' \in \mathrm{GL}(n, \Bbbk)$, ovvero se e solo se lascia (globalmente) stabile l'iperpiano "all'infinito" di equazione $X_0 = 0$. Viceversa ogni affinità di $\mathbb{A}^n(\Bbbk)$ si estende unicamente ad una proiettività di $\mathbb{P}^n(\Bbbk)$ della forma suddetta.*

Dimostrazione. Essenzialmente ovvio: se la prima riga della matrice non fosse di quella forma, si troverebbero punti "affini" (prima coordinata 1) mandati in punti impropri (prima coordinata 0), e quindi l'applicazione non sarebbe stabile sulla parte affine. □

4.3. Teorema (Traslazioni). *Le traslazioni di $\mathbb{A}^n(\Bbbk)$ sono le (restrizioni di) proiettività che lasciano puntualmente fermo l'iperpiano all'infinito e non hanno altri punti uniti. Sono dunque le omologie speciali di asse l'iperpiano improprio, e il centro dell'omologia corrisponde alla direzione della traslazione.*

Dimostrazione. Basta ricordare che le traslazioni (di vettore v) hanno matrici del tipo $\left(\begin{smallmatrix} 1 & 0 \\ v & \mathbb{I}_n \end{smallmatrix}\right)$, che sono appunto le omologie speciali di asse $X_0 = 0$ e di centro il punto improprio $\binom{0}{v}$. □

4.4. Esempi. La simmetria (affine) di asse V e direzione U è la proiettività involutoria con V e U spazi di punti uniti complementari e U contenuto nell'iperpiano all'infinito; in particolare se V è un punto (dunque che è U?), si tratta della simmetria centrale di centro quel punto.

4.5. Definizione (Completamento proiettivo e scheletro affine). *Data una varietà lineare affine L di equazione $AT + a = 0$, definiamo il suo completamento proiettivo come la varietà lineare proiettiva $\overline{L}$ di equazione omogenea $(\,a \quad A\,)\,X = 0$. È chiaro che $L \subseteq \overline{L}$, e che i punti di $\overline{L} \smallsetminus L$ sono contenuti in $\mathbb{P}^n(\Bbbk) \smallsetminus \mathbb{A}^n(\Bbbk)$, vale a dire sono punti "all'infinito" di coordinate $\binom{0}{T}$ ove $AT = 0$, dunque sono le direzioni della varietà lineare affine L. Potremmo anche definire $\overline{L}$ come al più piccola varietà lineare proiettiva contenente L (intersezione di tutti gli iperpiani proiettivi contenenti L).*

Nell'altro senso, per ogni varietà lineare proiettiva M, definiamo il suo scheletro affine come $M \cap \mathbb{A}$ (intersezione con lo spazio affine).

4.5.1. Si vede subito che lo scheletro del completamento è il sottospazio di partenza ($\overline{L} \cap \mathbb{A} = L$) e che il completamento dello scheletro è il sottospazio iniziale se non era contenuto nell'iperpiano improprio ($\overline{M \cap \mathbb{A}} = M$ sse $M \cap \mathbb{A} \neq \varnothing$), nel qual caso ha scheletro, e quindi completamento, vuoto.

Dunque, scheletro affine e completamento proiettivo danno una corrispondenza biunivoca tra sottospazi affini e sottospazi proiettivi non contenuti nell'iperpiano improprio. A livello di (equazioni di) iperpiani, si tratta della corrispondenza tra equazioni affini ed equazioni omogenee diverse da $X_0 = 0$ (in generale, ogni polinomio si può omogeneizzare aggiungendo una variabile X_0, e ogni polinomio omogeneo si può calcolare in $X_0 = 1$ ottenendo un polinomio, in generale non più omogeneo: studiare queste due funzioni e le loro composizioni).

4.5.2. Parallelismo. Due varietà affini in $\mathbb{A}^n(\Bbbk)$ sono parallele se e solo se i loro completamenti proiettivi hanno intersezione (solo) lungo l'iperpiano all'infinito e una contenuta nell'altra.

4.6. Teorema. *Dati uno spazio proiettivo punteggiato $\mathbb{P}$ e un iperpiano $H \subseteq \mathbb{P}$, l'insieme $\mathbb{P} \smallsetminus H$ resta munito in modo canonico di una struttura di spazio affine (della stessa dimensione di $\mathbb{P}$) con spazio delle traslazioni associato*

$$T := \{\psi \in \mathrm{PGL}(\mathbb{P}) \ : \ \psi_H = \mathrm{id}_H, \psi(x) \neq x \ \forall x \notin H\}$$

(si tratta delle omologie speciali di asse $H = \alpha(U)$). Scegliendo un riferimento in modo che $H = V(X_0)$, i quozienti $(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0})$ si dicono le coordinate affini associate su $\mathbb{P} \smallsetminus H$.

Dimostrazione. Dapprima si osserva che T è uno spazio vettoriale di dimensione uguale a $\dim \mathbb{P}$ (somma: composizione di omologie; gli scalari si rappresentano come omologie generali di asse H; prodotto per gli scalari: azione per coniugio delle omologie generali su quelle speciali), poi che $\mathbb{P} \smallsetminus H$ è uno spazio affine con spazio delle traslazioni T. Si può ricondurre tutto il calcolo al caso standard con una opportuna scelta di riferimento: le omologie speciali hanno matrici del tipo $\left(\begin{smallmatrix} 1 & 0 \\ x & \mathbb{I} \end{smallmatrix}\right)$ e le omologie generali del tipo $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mathbb{I} \end{smallmatrix}\right)$. □

4.6.1. Problema. Date due rette nel piano proiettivo, è sempre possibile scegliere un piano affine (complementare di una opportuna retta del piano proiettivo) tale che esse risultino parallele? Dato un quadrilatero nel piano proiettivo, è sempre possibile scegliere un piano affine (complementare di una opportuna retta del piano proiettivo) tale che il quadrilatero sia un parallelogramma?

4.6.2. Esempi. Consideriamo le rette di equazione $X_1 = 0$ ed $X_0 + X_1 = 0$ nel piano proiettivo con coordinate omogenee X_0, X_1, X_2. Una persona nel piano affine definito da $X_0 \neq 0$ e che usa coordinate affini $T_1 = X_1/X_0$, $T_2 = X_2/X_0$, vede le due rette di equazione $T_1 = 0$ ed $1 + T_1 = 0$, e dice che sono parallele. Una persona nel piano affine definito da $X_1 \neq 0$ e che usa coordinate affini $T_0 = X_0/X_1$, $T_2 = X_2/X_1$, vede la seconda retta di equazione $T_0 + 1 = 0$, mentre non vede la prima, di "equazione" $1 = 0$, e dirà che si tratta dell'"orizzonte". Una persona nel piano affine definito da $X_2 \neq 0$ e che usa coordinate affini $T_0 = X_0/X_2$, $T_1 = X_1/X_2$, vede le due rette di equazione $T_1 = 0$ ed $T_0 + T_1 = 0$, e dice che si incontrano nell'origine.

4.7. Caso Standard Euclideo. Nello spazio affine reale standard, si può considerare la struttura di spazio euclideo usuale, usando il prodotto scalare sullo spazio vettoriale delle traslazioni.

4.7.1. Assoluto euclideo e punti ciclici. I punti di $\mathbb{P}^n(\mathbb{C})$ che annullano l'espressione $\sum_{i=0}^n X_i^2$ per definizione danno il supporto dell'assoluto euclideo (si noti che nessuno appartiene a

$\mathbb{P}^n(\mathbb{R})$), e i punti impropri di questo si dicono punti ciclici euclidei. Per esempio se $n = 1$ non ci sono punti ciclici, se $n = 2$ i punti ciclici sono $\begin{pmatrix} 0 \\ 1 \\ \pm i \end{pmatrix}$, se $n = 3$ i punti ciclici sono $\begin{pmatrix} 0 \\ x \\ y \\ z \end{pmatrix}$ con $x^2 + y^2 + z^2 = 0$.

4.7.2. Unità di misura. La conoscenza dei punti ciclici permette di ricostruire il prodotto scalare a meno di una costante moltiplicativa non nulla; per fissare questa basta fissare un segmento di lunghezza 1, ovvero una coppia di punti. Di solito la scelta di una coppia di punti si dice una unità di misura.

4.7.3. Come si scrivono allora gli invarianti euclidei (lunghezze ed angoli) in termini dell'invariante proiettivo dato dal birapporto? Per la distanza tra due punti A e B, si consideri sulla retta che li congiunge un punto A' tale che il segmento tra A e A' sia unitario; calcolare (∞, A, A', B) dove ∞ è il punto improprio della retta.

4.7.4. Formula di Laguerre. Vediamo il legame tra la nozione di angolo fra due rette incidenti sul piano euclideo e la nozione proiettiva di birapporto; se p e q sono due rette incidenti, e consideriamo i, j le rette cicliche per $p \wedge q$ (sono le rette per $p \wedge q$ e i punti ciclici: dunque due rette complesse coniugate il cui unico punto reale è $p \wedge q$), allora risulta

$$(p\,q\,i\,j) = e^{-2i\vartheta} = \cos 2\vartheta - i \sin 2\vartheta$$

dove ϑ è l'angolo tra le due rette. In particolare, p e q dividono armonicamente le rette cicliche se e solo se sono ortogonali tra loro. Il calcolo è un semplice esercizio: conviene scegliere coordinate proiettive in modo che p e q intersechino la retta impropria nei punti di coordinate (affini su quella) 0 e $\tan\vartheta$; risulta allora

$$(p\,q\,i\,j) = (0, \tan\vartheta, i, -i) = \frac{i + \tan\vartheta}{i - \tan\vartheta} = \frac{\cos\vartheta - i\sin\vartheta}{\cos\vartheta + i\sin\vartheta} = \frac{e^{-i\vartheta}}{e^{i\vartheta}} = e^{-2i\vartheta}$$

come si voleva. Si chiama di solito formula di Laguerre la relazione

$$\vartheta = \frac{i}{2}\log(p\,q\,i\,j)$$

(si intende la determinazione principale del logaritmo complesso).

È utile osservare che la nozione di angolo non dipende dall'unità di misura, ma solo dell'assoluto; in effetti è un invariante di geometria conforme, più che euclidea (basta specificare la quadrica assoluto, cioè la forma quadratica a meno di multipli scalari non nulli).

4.7.5. Ortogonalità, bisettrici ed armonia. Cosa c'entra questo con il fatto che le bisettrici di p e q sono ortogonali tra loro? Si osservi che due rette p, q sono ortogonali sse $(p\,q\,i\,j) = -1$, cioè sse separano armonicamente i punti ciclici. D'altra parte, l'involuzione che scambia p con q fissa le bisettrici, e (essendo indotta da una rigidità inversa) scambia i con j. Dunque le bisettrici di p e q sono la coppia involutoria comune alle involuzioni del fascio per $p \wedge q$ che hanno come punti fissi p, q (involuzione indotta dalle due rette) e i, j (involuzione degli angoli retti).

4.7.6. Questioni di angoli e circonferenze. È un risultato ben noto di geometria elementare che per due punti di una circonferenza l'angolo formato con qualsiasi altro punto della circonferenza non dipende dal punto scelto, ed è metà dell'angolo al centro. Questo si può dimostrare in coordinate sia usando la definizione di coseno dell'angolo, sia usando la formula di Laguerre.

È più interessante notare che questo risultato è un caso particolare di un risultato di geometria proiettiva che riguarda qualsiasi conica non degenere (equazione di secondo grado omogenea in tre variabili che non si fattorizzi in due lineari, cioè che non sia unione di due rette). Il risultato è il seguente: sia $\mathscr{C}$ una conica irriducibile nel piano proiettivo, sia C un punto non appartenente a $\mathscr{C}$, siano T, S i punti di tangenza di rette per C tangenti a $\mathscr{C}$ (nel fascio di C vi sono due rette che sono tangenti a $\mathscr{C}$, cioè che intersecano $\mathscr{C}$ in un punto doppio), siano P, Q due qualsiasi punti di $\mathscr{C}$. Allora: per oni punto X di $\mathscr{C}$ abbiamo che il birapporto delle rette per X e P, Q, T, T' non dipende da X, e il suo quadrato è il birapporto delle rette per C e P, Q, T, T'. Il caso della circonferenza si ottiene usando come C il centro, e allora i punti T, T' sono esattamente i punti ciclici del piano, da cui segue la formula per gli angoli.

4.7.7. Angoli interni di un triangolo. Dati tre vettori u, v, w del piano reale, consideriamo gli angoli $\vartheta_w = \vartheta(u, -v)$, $\vartheta_u = \vartheta(v, -w)$ e $\vartheta_v = \vartheta(w, -u)$ (si tratta dei tre angoli di ogni triangolo i cui lati siano paralleli ai tre vettori; si faccia attenzione: non sono gli angoli tra le rette generate dai vettori...). Allora è facile vedere che $e^{2i(\vartheta_u + \vartheta_v + \vartheta_w)} = 1$, e quindi che la somma $\vartheta_u + \vartheta_v + \vartheta_w$ è (un

multiplo di) π. Un calcolo in termini della definizione di cos (tramite prodotto scalare) sarebbe (non molto) più difficile. Provarci?

4.7.8. Naturalmente, la definizione di prodotto scalare dipende dalla base scelta nello spazio vettoriale, e basi diverse danno luogo a funzioni diverse, e dunque a supporti dell'assoluto diversi tra loro; studieremo una generalizzazione di questi problemi in un futuro capitolo; lo dico solo per rendere sensato il problema seguente, che conviene comunque saltare (per ritornarci dopo lo studio delle quadriche).

4.7.9. Problema. Date due rette nel piano proiettivo, è sempre possibile scegliere un piano affine (complementare di una opportuna retta del piano proiettivo) e un assoluto tale che esse risultino perpendicolari? Dato un quadrilatero nel piano proiettivo, è sempre possibile scegliere un piano affine (complementare di una opportuna retta del piano proiettivo) e un assoluto tale che il quadrilatero sia un rettangolo, un rombo, un quadrato? Si noti comunque che la nozione di quadrato non è euclidea ma conforme (riguarda solo gli angoli).

5. Retta proiettiva e birapporti.

5.1. Trasformazioni di Mœbius. La retta proiettiva standard $\mathbb{P}^1(\Bbbk)$ si può identificare con la retta affine $\mathbb{A}^1(\Bbbk)$ a cui s'è aggiunto un punto all'infinito: $\Bbbk \cup \{\infty\}$ ove ∞ è un simbolo fuori di $\Bbbk$.

Una proiettività φ della retta proiettiva standard (nel riferimento standard è data da una matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}(2,\Bbbk)$ che agisce mandando il punto P di coordinate omogenee $\left(\begin{smallmatrix} X_0 \\ X_1 \end{smallmatrix}\right)$ nel punto $\varphi(P)$ di coordinate omogenee

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \end{pmatrix} = \begin{pmatrix} aX_0 + bX_1 \\ cX_0 + dX_1 \end{pmatrix} .$$

In coordinate affini $X = X_1/X_0$ si può scrivere come

$$\varphi(X) = \frac{c + dX}{a + bX}$$

e si dicono trasformazioni lineari fratte, o trasformazioni di Mœbius, o omografie; si tratta di affinità se si scrivono $\varphi(X) = c + dX$.

5.1.1. Dati tre elementi distinti $a, b, c \in \Bbbk \cup \{\infty\}$, la proiettività che agisce con $\varphi(a) = \infty$, $\varphi(b) = 0$ e $\varphi(c) = 1$ si scrive come

$$\varphi(X) = \frac{(c-a)(X-b)}{(c-b)(X-a)} .$$

5.1.2. Definiamo come birapporto dei quattro elementi $a, b, c, x \in \Bbbk \cup \{\infty\}$ il valore $\varphi(x)$ della trasformazione precedente, cioè il numero

$$\mathrm{CR}(a, b, c, x) = (a\ b\ c\ x) := \frac{(c-a)(x-b)}{(c-b)(x-a)} .$$

Si tratta di un invariante per trasformazioni di Mœbius, proprietà fondamentale che dovrebbe essere chiara dalla definizione stessa (se φ è proiettività che manda a, b, c in $\infty, 0, 1$, e ψ è una proiettività qualsiasi, allora la proiettività che manda $\psi a, \psi b, \psi c$ in $\infty, 0, 1$ è $\varphi\psi^{-1}$ e ovviamente $\varphi\psi^{-1}(\psi(X)) = \varphi(X)$), ma che si può anche dimostrare con un calcolo diretto: se $\psi(X) = \frac{\gamma+\delta X}{\alpha+\beta X}$ è una tale trasformazione, allora

$$(\psi(a)\ \psi(b)\ \psi(c)\ \psi(x)) = \frac{(\psi(c)-\psi(a))(\psi(x)-\psi(b))}{(\psi(c)-\psi(b))(\psi(x)-\psi(a))} = \cdots = \frac{(c-a)(x-b)}{(c-b)(x-a)} = (a\ b\ c\ x)$$

(riempire i $\cdots$).

5.1.3. In particolare $(\infty, 0, 1, \lambda) = \lambda$ e $(\infty, 0, \mu, \lambda) = \frac{\lambda}{\mu}$.

5.2. Definizione (Birapporto). *Dati quattro punti A, B, C, X (i primi tre distinti) di $\mathbb{P}^1(\Bbbk)$ o di una qualunque retta proiettiva il birapporto (cross ratio) della quaterna ordinata è definito da:*

$$\mathrm{CR}(A, B, C, X) = (A\ B\ C\ X) = \frac{x_0}{x_1}$$

ove $\left(\begin{smallmatrix} x_0 \\ x_1 \end{smallmatrix}\right)$ sono le coordinate omogenee di X nel riferimento sulla retta costituito dai punti A, B, C.

5.2.1. Per la terminologia, come birapporto (cross-ratio) viene introdotto da Mœbius, come rapporto doppio da Steiner, e come rapporto anarmonico da Chasles.

5.2.2. Se A, B, C, X si rappresentano in coordinate affini tramite elementi $a, b, c, x \in \Bbbk \cup \{\infty\}$ (i primi tre distinti), allora il birapporto dei quattro punti $(A\ B\ C\ X)$ è calcolato dal birapporto dei quattro numeri $(a\ b\ c\ x)$.

5.2.3. Relazione tra il birapporto e i rapporti semplici per quattro punti affini allineati: si ha che $\mathrm{CR}(A, B, C, X) = \frac{\mathrm{DR}(A,B,C)}{\mathrm{DR}(A,B,X)}$ se $\mathrm{DR}(A, B, X) = \frac{X-A}{X-B}$.

In particolare, se $X = \infty$ (punto all'infinito della retta, intersezione della retta con l'iperpiano improprio), allora $\mathrm{CR}(A, B, C, \infty) = \mathrm{DR}(A, B, C)$.

5.2.4. Invarianza proiettiva. È evidente dalla definizione che il birapporto è invariante per proiettività, ovvero che il birapporto di una quaterna ordinata coincide con il birapporto della sua immagine tramite qualsiasi proiettività. È il più semplice e il più importante degli invarianti. In un certo senso è anche l'unico: se φ è una biiezione insiemistica di $\Bbbk \cup \{\infty\}$ in sè che rispetta i birapporti, allora è necessariamente una trasformazione di Mœbius.

L'invarianza proiettiva permette poi varie possibilità per il calcolo:

$$(\pi_0\,\pi_1\,\pi_2\,\pi_3) = (P_0\,P_1\,P_2\,P_3) = (r_0\,r_1\,r_2\,r_3) = (P'_0\,P'_1\,P'_2\,P'_3)$$

5.2.5. Precursore proiettivo del teorema di Talete. Dati quattro iperpiani $\pi_0, \pi_1, \pi_2, \pi_3$ di un fascio, e considerate due rette r, s sghembe con il centro del fascio, allora esse intersecano i quattro iperpiani in quattro punti distinti (siano $R_i = r \wedge \pi_i$ ed $S_i = s \wedge \pi_i$), e i birapporti di tali quaterne coincidono ($\mathrm{CR}(R_0, R_1, R_2, R_3) = \mathrm{CR}(S_0, S_1, S_2, S_3)$). Nello spazio affine in cui π_3 è l'iperpiano all'infinito, i tre iperpiani affini π_0, π_1, π_2 sono paralleli, e la precedente uguaglianza di birapporti diventa l'usuale teorema di Talete di uguaglianza di rapporti semplici $\mathrm{DR}(R_0, R_1, R_2) = \mathrm{DR}(S_0, S_1, S_2)$ (perché su una retta affine abbiamo $\mathrm{CR}(A, B, C, \infty) = \mathrm{DR}(A, B, C)$).

5.2.6. Significato intuitivo per punti allineati nel piano (Pappo). Può essere utile un approccio intuitivo, e forse quello originale, alla nozione di birapporto, che mette in luce la relazione con i problemi di proiezione di segmenti, confondendo le idee circa proprietà metriche, affini e proiettive degli oggetti che consideriamo. Comunque sia, partendo dal teorema dei seni ($a/b = \sin\alpha/\sin\beta$, e $a'/b' = \sin\alpha'/\sin\beta' = \sin\alpha'/\sin\beta$ nella figura sottostante

notare che il rapporto delle lunghezze a e a' varia al variare della retta secante il fascio: $\frac{a}{a'} = \frac{b}{b'}\frac{\sin\alpha}{\sin\alpha'}$) applicato un paio di volte alla figura seguente:

si trova

$$\frac{(C-A)/(B-C)}{(D-A)/(B-D)} = \frac{\sin\alpha/\sin(\beta+\gamma)}{\sin(\alpha+\gamma)/\sin\beta} = \frac{\sin\alpha}{\sin(\alpha+\gamma)}\frac{\sin\beta}{\sin(\beta+\gamma)}$$

da cui si vede che il complicato rapporto di lunghezze (il quale ha una interpretazione puramente affine, trattandosi di rapporti tra vettori dipendenti) non dipende più dalla retta secante il fascio di

centro O, ma solo dagli angoli tra le quattro rette scelte: proiettando da centro O i quattro punti su un'altra retta, la quantità scritta rimane invariante (il che è falso per rapporti semplici, chiaramente!).

5.3. Proposizione. *In coordinate qualsiasi, se* $A = \binom{a_0}{a_1}$, $B = \binom{b_0}{b_1}$, $C = \binom{c_0}{c_1}$, *allora*

$$(A\ B\ C\ X) = \frac{\begin{vmatrix} a_0 & a_1 \\ c_0 & c_1 \end{vmatrix}}{\begin{vmatrix} b_0 & b_1 \\ c_0 & c_1 \end{vmatrix}} \Big/ \frac{\begin{vmatrix} a_0 & a_1 \\ x_0 & x_1 \end{vmatrix}}{\begin{vmatrix} b_0 & b_1 \\ x_0 & x_1 \end{vmatrix}} .$$

Dimostrazione. Farsi il conto. □

5.4. Teorema (Azione delle permutazioni). *Se* $(A\ B\ C\ D) = \lambda$, *allora:*

$$\begin{aligned}
(A\ B\ C\ D) &= (B\ A\ D\ C) = (D\ C\ B\ A) = (C\ D\ A\ B) = \lambda \\
(B\ A\ C\ D) &= (A\ B\ D\ C) = (D\ C\ A\ B) = (C\ D\ B\ A) = \frac{1}{\lambda} \\
(A\ C\ B\ D) &= (C\ A\ D\ B) = (D\ B\ C\ A) = (B\ D\ A\ C) = 1-\lambda \\
(C\ B\ A\ D) &= (B\ C\ D\ A) = (D\ A\ B\ C) = (A\ D\ C\ B) = \frac{\lambda}{\lambda-1} \\
(C\ A\ B\ D) &= (A\ C\ D\ B) = (D\ B\ A\ C) = (B\ D\ C\ A) = \frac{1}{1-\lambda} \\
(B\ C\ A\ D) &= (C\ B\ D\ A) = (D\ A\ C\ B) = (A\ D\ B\ C) = \frac{\lambda-1}{\lambda} .
\end{aligned}$$

Dimostrazione. Si osservi che, una volta identificati i primi due valori non identici, gli altri seguono per composizione. I primi due sono immediati: scambiando i primi due punti si scambiano tra loro le coordinate omogenee (quindi si inverte il loro rapporto), scambiando i punti centrali, la prima coordinata omogenea viene cambiata nella differenza tra la seconda e la prima.

In alternativa, posto $(\infty, 0, 1, \lambda) = \lambda$, abbiamo $(0, \infty, 1, \lambda) = \frac{(1-0)(\lambda-\infty)}{(1-\infty)(\lambda-0)} = 1/\lambda$ e $(\infty, 1, 0, \lambda) = \frac{(0-\infty)(\lambda-1)}{(0-1)(\lambda-\infty)} = 1-\lambda$.

Allo stesso modo si verifica che i "doppi scambi" disgiunti non modificano il birapporto. La prima osservazione, e quest'ultima, dovrebbero permettere allo studente di ricostruire e di ricordare l'intera tavola delle trasformazioni! □

5.4.1. A titolo mnemonico, si può osservare che $(A\ B\ C\ D)(A\ B\ D\ C) = 1$ (lo scambio degli ultimi, o dei primi, due), e $(A\ B\ C\ D) + (A\ C\ B\ D) = 1$ (lo scambio dei due centrali, o estremi). Il primo è ovvio, il secondo può dedursi dall'espressione di Eulero: $(B-A)(D-C) + (C-A)(B-D) + (D-A)(C-B) = 0$ (più o meno formale).

5.4.2. Osservazione. Quindi in realtà il gruppo Σ_4 delle permutazioni sui 4 punti agisce tramite un gruppo isomorfo a Σ_3 (permutazioni su tre oggetti), che è il quoziente di Σ_4 con il sottogruppo normale generato dai doppi scambi. Si noti che il sottogruppo di Σ_4 che fissa D è isomorfo ad un Σ_3, ma non è un sottogruppo normale di Σ_4.

Nel caso dei birapporti, il punto è che i possibili valori del birapporto, visti come trasformazioni di Mœbius, formano un gruppo d'ordine 6 isomorfo a Σ_3 (scrivere le matrici corrispondenti!), e il morfismo suriettivo da Σ_4 a questo gruppo ha nucleo formato dai doppi scambi disgiunti.

5.4.3 Il birapporto è nullo se $X = B$, 1 se $X = C$ e ∞ se $X = A$. Nel caso $\Bbbk = \mathbb{R}$ il valore di $(A\ B\ C\ X)$ risulta negativo se i primi due punti separano gli ultimi due, positivo altrimenti. Moralmente, il valore -1 si ottiene per il punto che divide "un tratto tra A e B" nella "stessa proporzione" con cui C divide l'altro tratto.

Per quali valori del birapporto λ le permutazioni non danno sei valori distinti?

5.4.4. I sei valori per permutazioni del birapporto tra quattro fissati punti non sono tutti distinti se $\lambda = 1$ (allora i valori sono $1, 0, \infty$ e vi sono solo tre punti distinti), oppure $\lambda = -1$ (allora i valori sono $-1, 2, 1/2$, i quattro punti sono distinti e si dicono una quaterna armonica) oppure se

$\lambda^2-\lambda+1=0$ (e allora i valori possibili sono le due radici seste primitive dell'unità, ovvero le due radici cubiche di -1 diverse da -1, i quattro punti sono distinti e si dicono una quaterna equianarmonica; su $\mathbb{R}$ non esistono quaterne equianarmoniche, su $\mathbb{C}$ sì).

5.5. Quaterne armoniche. *Una quaterna A, B, C, X si dice armonica se* $(A\ B\ C\ X) = -1$. In tal caso si dice anche che i punti C, X separano (o sono separati) armonicamente dai punti A, B, o anche che X è il quart'armonico dopo A, B, C. Si osservi che la condizione di armonia comprende varie nozioni già note al lettore:

(*i*) il quarto armonico dopo a, b, ∞ è la media aritmetica $\frac{a+b}{2}$, o equivalentemente il quarto armonico dopo due punti e il punto improprio è il punto medio;

(*ii*) il quarto armonico dopo $a, b, 0$ è la media armonica $\frac{2ab}{a+b}$ (inverso della media aritmetica degli inversi, cioè $\frac{2}{\frac{1}{a}+\frac{1}{b}}$), come si ottiene facilmente dal precedente usando la proiettività data dalla inversione ($X \mapsto 1/X$ in coordinata affine);

(*iii*) chi è il quarto armonico dopo $a, b, 1$?

(*iv*) abbiamo $(a, -a, c, d) = -1$ se e solo se $cd = a^2$, cioè la media geometrica di c e d dà separatori armonici comuni alla coppia 0 e ∞;

(*v*) abbiamo $(0, \infty, x, -x) = -1$;

(*vi*) abbiamo $(1, -1, x, 1/x) = -1$ e in generale $(a, -a, x, a^2/x) = -1$.

5.5.1. L'origine musicale del nome di quaterna armonica si vede nel secondo esempio: era credenza comune che suoni gradevoli (armonici) venissero dalla sovrapposizione di suoni di frequenza multipla; considerando la lunghezza delle corde usate per produrre il suono (la cui frequenza è inversamente proporzionale alla lunghezza), questo si traduce appunto nella media armonica...

5.5.2. Alcuni degli esempi sopra riportati hanno delle interpretazioni classiche in termini metrici (distanza tra punti su una retta euclidea): siano A, B, C, D una quaterna armonica:

(*i*) (Teorema della media aritmetica) detto M il punto medio tra A e B, abbiamo $\|A-M\| = \|B-M\|$ (usare $C = \infty$);

(*ii*) (Teorema della media armonica) usando A come origine: $\frac{2}{\|B-A\|} = \frac{1}{\|C-A\|} + \frac{1}{\|D-A\|}$;

(*iv*) (Teorema della media geometrica) usando M, punto medio tra A e B, come origine: $\|A-M\|^2 = \|C-M\|\ \|D-M\|$.

♠ **5.5.3.** Sequenze armoniche. Una sequenza di punti $A_1, A_2, A_3, \ldots$ su una retta proiettiva si dice armonica rispetto ad un fissato punto P della stessa retta se P e ogni punto della successione sono separati armonicamente dai due punti precedente e successivo, cioè per ogni indice i abbiamo che P e A_i sono separati armonicamente da A_{i-1} e A_{i+1}, o ancora che per ogni i risulti $(P\ A_i\ A_{i-1}\ A_{i+1}) = -1$, ovvero $(P\ A_{i-1}\ A_i\ A_{i+1}) = 2$.

Per esempio, se P è il punto improprio di una retta euclidea, allora i punti A_i sono tra loro equidistanti. Se invece P è l'origine di un riferimento di una retta euclidea, allora le coordinate in quel riferimento dei punti A_i formeranno una successione armonica.

Si osservi che una successione armonica rispetto a P è determinata dalla conoscenza di due punti in successione (verificarlo per bene, quando sarà nota la costruzione del quarto armonico tramite quadrangoli).

Inoltre, non c'è bisogno di dire che le sequenze armoniche rispetto ad un punto sono trasformate da qualsiasi proiettività in sequenze armoniche rispetto all'immagine di quel punto: si pensi alle strisce bianche su una strada rettilinea. Qualche disegno può aiutare l'immaginazione:

Problema. Data una sequenza di punti allineati, come fare per vedere se si tratta di una sequenza armonica rispetto ad un punto P della retta? Suggerimento: proiettare su una retta affine in modo che il punto P vada all'infinito. Vi sono esempi classici di sequenze armoniche per simulare la prospettiva, per esempio nella chiesa di S.Maria in S.Satiro di Bramante a Milano, oppure nel teatro Olimpico di Palladio (e Scamozzi) a Vicenza.

♠ **5.6.** Quaterne equianarmoniche. Dati tre punti distinti sulla retta proiettiva complessa, quanti sono i quarti anarmonici dopo i tre dati?

Quali sono i quarti equianarmonici dopo ∞, 0 e 1 (disegnarli sul piano di Gauss e confrontarli con il quarto armonico).

E dopo a, b e ∞? E dopo a, b e 0?

5.7. Teorema (Armonia ed involuzioni). *Se φ è una involuzione di $\mathbb{P}^1(\Bbbk)$ (cioè una proiettività non identica tale che $\varphi^2 = \mathrm{id}$) con due punti uniti A e B, allora per ogni punto P distinto dai punti uniti vale $(A\ B\ P\ \varphi(P)) = -1$. Viceversa dati due punti A e B di $\mathbb{P}^1(\Bbbk)$ e $c \in \Bbbk \smallsetminus \{0, \infty\}$, esiste una unica proiettività con punti fissi A e B e definita su $P \neq A, B$ da $(A\ B\ P\ \varphi(P)) = c$; si tratta di una involuzione sse $c = -1$.*

Dimostrazione. Esercizio. Più in generale, si osservi che se P, Q sono punti uniti di φ, e $R \in P \vee Q \smallsetminus \{P, Q\}$, allora il valore di $(P\ Q\ R\ \varphi(R))$ non dipende da R, ed è il rapporto tra gli autovalori di P e Q in un qualsiasi riferimento (il rapporto tra autovalori è un invariante della proiettività, contrariamente agli autovalori delle matrici che rappresentano la proiettività stessa...). □

5.7.1. Involuzioni, armonie e simmetrie affini. Si osservi che data una involuzione, e considerato un iperpiano contenente uno dei due spazi di punti uniti, nello spazio affine complementare l'involuzione è classificata come una simmetria affine: di direzione quel sottospazio, e di asse l'altro sottospazio di punti uniti. Basta infatti osservare che, essendo il punto medio quarto armonico dopo due punti e l'infinito, in ogni retta per un punto dell'asse e un punto della direzione due punti corrispondenti sotto l'involuzione hanno come punto medio quello dell'asse...

5.7.2. Problema. Data una involuzione di una retta proiettiva, si chiamano coppie involutorie le coppie di punti che si scambiano tra loro nell'involuzione (ogni punto sta in una coppia involutoria, ovviamente con la sua immagine). Date due involuzioni, se esse hanno in comune due coppie involutorie, allora coincidono.

Due involuzioni distinte, hanno sempre una coppia involutoria in comune?

Due coppie involutorie definiscono completamente l'involuzione: come trovarne graficamente i punti uniti? Come trovare la coppia involutoria comune di due involuzioni date? Si tratta di trovare separatori armonici comuni...

5.7.3. Problema. Generalizzare il teorema sulle involuzioni a spazi di dimensione n usando due sottospazi sghembi di punti fissi.

5.7.4. Problema. Usando il rapporto semplice $(A\ B\ X) = \frac{X-A}{X-B}$, mostrare che tre coppie A, A', B, B', C, C' di punti tutti allineati sono tre coppie involutorie di una involuzione se e solo se $(A\ B\ C')(B\ C\ A')(C\ A\ B') = 1$.

5.8. Teorema (fondamentale delle proiettività della retta). *Sia $\sigma : \Bbbk \to \Bbbk'$ un isomorfismo di corpi. Una applicazione suriettiva $\varphi : \mathbb{P}^1(\Bbbk) \longrightarrow \mathbb{P}^1(\Bbbk')$ tale che $(\varphi A\ \varphi B\ \varphi C\ \varphi D) = (A\ B\ C\ D)^\sigma$ per ogni quaterna di punti distinti, è una σ-proiettività. Se $\Bbbk = \Bbbk'$, $\sigma = \mathrm{id}$: le proiettività tra rette sono le applicazioni biunivoche che conservano il birapporto.*

Viceversa, siano $\Bbbk$ e $\Bbbk'$ corpi di caratteristica diversa da due; una applicazione suriettiva $\varphi : \mathbb{P}^1(\Bbbk) \longrightarrow \mathbb{P}^1(\Bbbk')$ tale che conserva le quaterne armoniche è una σ-proiettività per un ben determinato $\sigma : \Bbbk \longrightarrow \Bbbk'$ iso di corpi (che dipende da φ). Se $\Bbbk = \Bbbk' = \mathbb{R}$: le proiettività tra rette sono le applicazioni biunivoche che conservano l'armonia.

Dimostrazione. Vedi Barsotti, o Gerotto. □

5.8.1. Dai teoremi precedenti discendono le seguenti asserzioni:

Una collineazione tra due spazi proiettivi $\mathbb{P}(V)$, $\mathbb{P}(W)$ è una proiettività se e solo se conserva i birapporti (delle quaterne ordinate di punti allineati).

Una collineazione tra due spazi proiettivi $\mathbb{P}(V)$, $\mathbb{P}(W)$ è una σ-proiettività se e solo se conserva l'armonia (delle quaterne ordinate di punti allineati).

5.9. Birapporti e numeri complessi. Segnaliamo prima di tutto una possibile fonte di confusione. Siamo abituati a identificare $\mathbb{C}$ con $\mathbb{R}^2$, ma quando pensiamo a $\mathbb{A}^1(\mathbb{C})$ e $\mathbb{A}^2(\mathbb{R})$ (che sono in biiezione!) immergiamo il primo in $\mathbb{P}^1(\mathbb{C})$ (che è isomorfo alla sfera via proiezione stereografica) e il secondo in $\mathbb{P}^2(\mathbb{R})$ (isomorfo alla sfera modulo antipodia del bordo), che non sono nemmeno in biiezione, e portano strutture geometriche molto diverse.

Per esempio per quattro numeri complessi pensati come elementi di $\mathbb{P}^1(\mathbb{C})$ ha senso calcolare il birapporto (sono allineati...), mentre pensati come elementi di $\mathbb{A}^2(\mathbb{R}) \subseteq \mathbb{P}^2(\mathbb{R})$ non ha nemmeno senso in generale (potrebbero non essere allineati).

Ricordiamo che le trasformazioni di Moebius, cioè le razionali fratte, conservano i birapporti. Invece passare al coniugio coniuga i birapporti, come pure le inversioni rispetto a cerchi.

5.9.1. Coclicità. Diciamo cicli le rette e le circonferenze. Allora per tre numeri complessi distinti passa un ciclo, e quattro numeri sono cociclici (stanno su uno stesso ciclo) sse il loro birapporto è reale. Suggerimento: usare la trasformazione di Moebius che porta i primi tre punti sulla retta reale. In particolare, l'equazione del ciclo per z_1, z_2, z_3 è data da $(z_1\ z_2\ z_3\ z) \in \mathbb{R}$ (annullamento della parte immaginaria).

Cosa si può dire della posizione reciproca dei quattro punti se il loro birapporto è puramente immaginario?

5.9.2. Per quattro punti su $\mathbb{C}$ allineati come punti reali, chiaramente il birapporto è lo stesso calcolato in quanto elementi di $\mathbb{C}$ o in quanto elementi del piano (ci si riduce subito al caso di quattro numeri reali). Per quattro punti su una circonferenza: possiamo ricondurci alla circonferenza unitaria, usare la trasformazione di Moebius $\frac{1+iZ}{i+Z}$, che dà la prioiezione stereografica tra retta reale e circonferenza unitaria usando come centro di proiezione $-i$. Il birapporto in quanto elementi di $\mathbb{C}$ coincide con quello dei quattro punti reali corrispondenti, quindi con quello delle quattro rette spiccate da $-i$, quindi al birapporto dei quattro punti in quanto punti della circonferenza (che per definizione è il birapporto delle quattro rette spiccate da un punto qualsiasi della circonferenza ai quattro dati, definizione che si può dare per ogni conica).

5.9.3. Trasformazioni. Esiste una trasformazione di Moebius che manda z_1, z_2, z_3, z_4 ordinatamente in w_1, w_2, w_3, w_4 sse i birapporti delle due quaterne coincidono.

La trasformazione di Moebius che manda z_1, z_2, z_3 in w_1, w_2, w_3 si ottiene esplicitando w dall'equazione

$$\frac{w-w_2}{w-w_1}\,\frac{w_3-w_1}{w_3-w_2} = \frac{z-z_2}{z-z_1}\,\frac{z_3-z_1}{z_3-z_2}$$

(perché?).

5.9.4. Angoli. Dati tre punti ordinati, scrivere l'angolo formato come argomento di un rapporto semplice. Usando il limite della differenza di due angoli, mostrare che le trasformazioni di Moebius sono conformi (rispettano gli angoli tra cicli), riconducendo tale differenza a un birapporto.

Le inversioni rispetto a cicli sono trasformazioni conformi?

5.10. Problema: calcolo di birapporti. Dati quattro punti allineati A, B, C, D in $\mathbb{P}^n(\Bbbk)$, usando le coordinate dei punti in un riferimento fissato (diciamo p_i le coordinate del punto P, per $i = 0, \dots, n$), è vero che esiste un indice i tale che $(A\ B\ C\ D) = (a_i\ b_i\ c_i\ d_i)$? (no.) È vero che esiste una coppia di indici i, j tali che $(A\ B\ C\ D) = (a_i/a_j\ b_i/b_j\ c_i/c_j\ d_i/d_j)$? (si, ma non vale per tutte le coppie di indici: come giustificare la scelta degli indici?). Si osservi che la definizione stessa di birapporto (normalizzare i primi due punti usando il terzo e poi calcolare le coordinate del quarto) richiede di risolvere problemi con due sole incognite, per cui bastano due equazioni lineari indipendenti, quindi bastano due indici tali che la matrice $\begin{pmatrix} a_i & b_i \\ a_j & b_j \end{pmatrix}$ sia invertibile; il fatto che i quattro punti siano allineati fa sì che il risultato non dipenda dagli indici scelti (purché soddisfino la condizione di rango).

6. Piano proiettivo e costruzioni classiche.

6.1. Costruzione grafica del quarto armonico dopo tre punti: siano A, B, C punti di una retta proiettiva r immersa nel piano $\mathbb{P}^2(\Bbbk)$; si traccino due rette distinte $m, n(\neq r)$ per A e una retta $h(\neq r)$ per C; si consideri poi la seguente costruzione:

$M := m \cap h$ e $N := n \cap h$;
$u := M \vee B$ e $v := N \vee B$;
$U := u \cap n$ e $V := v \cap m$;
$k := U \vee V$.
Il quarto armonico è $X := k \cap r$.

Infatti si consideri la proiettività φ di r in sè composta della proiezione di r su h di centro V e della proiezione di h su r di centro U. Si vede subito che X e C sono punti fissi di φ, e che φ scambia A con B. Dunque φ è una involuzione di r in sè, e quindi la quaterna (A, B, C, X) è armonica.

6.2. Costruzione del quarto armonico dopo tre rette di un fascio: siano a, b, c rette di unfascio di centro R immerso nel piano $\mathbb{P}^2(\Bbbk)$; si traccino due punti distinti $M, N(\neq R)$ di a e un punto $H(\neq R)$ di c; poi:

$m := M \vee H$ e $n := N \vee H$;
$U := m \wedge b$ e $V := n \wedge b$;
$u := U \vee N$ e $v := V \vee M$;
$K := u \wedge v$;
il quarto armonico è $x := K \vee R$.

Si tratta semplicemente della costruzione duale della precedente; le rette di un fascio costituiscono una retta proiettiva (dello spazio duale). Riconoscere nella figura a lato la involuzione del fascio di asse R come nella dimostrazione precedente.

6.3. Quadrangolo piano completo: è la figura piana formata da quattro punti, a tre a tre non allineati, detti vertici e dalle sei rette che li congiungono, dette lati. I punti di intersezione di coppie di lati opposti si dicono i punti diagonali. Le rette passanti per due punti diagonali si dicono le diagonali del quadrangolo; in ogni diagonale i punti diagonali separano armonicamente i punti di intersezione con i rimanenti due lati.

Giustificare l'affermazione precedente in termini della costruzione grafica del quarto armonico, e riconoscere in quella costruzione la presenza di un quadrangolo piano completo. Quante quaterne armoniche di punti e rette contiene un quadrangolo?

6.3.1. Relazioni quadrangoli-triangoli. Si osservi che ogni quadrangolo determina il suo triangolo diagonale (tre punti e tre rette). Viceversa, dato un triangolo ed un punto ad esso esterno (cioè che non appartiene ad alcuna retta del triangolo), esiste un unico quadrangolo con quel vertice ed avente quel triangolo come triangolo diagonale: costruirlo.

In generale quindi, ogni triangolo è triangolo diagonale di più quadrangoli.

6.3.2. Studio elementare dei quadrangoli piani completi. Tutto quello che abbiamo visto (quaterne armoniche di punti su lati e diagonali, di rette per vertici e diagonali, ricostruzione del quadrangolo dato il triangolo diagonale e un vertice) si può ottenere in modo elementare in coordinate. Possiamo scegliere un riferimento che usi i quattro vertici come punti fondamentali del

piano, e calcolare tutti gli altri dati del problema: i vertici sono

$$P_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \ P_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \ P_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \ P_3 = U = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

i lati sono le rette

$$r_{01} = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}, \ r_{02} = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}, \ r_{03} = \begin{pmatrix} 0 & 1 & -1 \end{pmatrix}, \ r_{12} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \ r_{13} = \begin{pmatrix} 1 & 0 & -1 \end{pmatrix}, \ r_{23} = \begin{pmatrix} 1 & -1 & 0 \end{pmatrix},$$

i punti diagonali sono

$$D_{01} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \ D_{02} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \ D_{03} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$$

e le rette diagonali sono

$$d_{03} = \begin{pmatrix} -1 & 1 & 1 \end{pmatrix}, \ d_{02} = \begin{pmatrix} 1 & -1 & 1 \end{pmatrix}, \ d_{01} = \begin{pmatrix} 1 & 1 & -1 \end{pmatrix},$$

e si possono trovare subito le quaterne armoniche trovando anche gli ulteriori punti di intersezione tra lati e diagonali: esercizio.

6.4. Quadrilatero piano completo: è la figura piana formata da quattro rette, a tre a tre non appartenenti ad un fascio, detti lati e dai sei punti di intersezione, detti vertici. Le rette congiungenti coppie di vertici opposti si dicono le diagonali del quadrilatero. I punti di intersezione di due diagonali si dicono i punti diagonali, e il fascio di rette di quei centri si dicono i fasci diagonali. In ogni fascio diagonale, le due diagonali separano armonicamente le rette passanti per i rimanenti due vertici.

Giustificare l'affermazione precedente in termini della costruzione grafica del quarto armonico dopo tre rette d'un fascio, e riconoscere in quella costruzione la presenza di un quadrilatero piano completo. Quante quaterne armoniche di punti e rette contiene un quadrilatero?

6.4.1. Relazioni quadrilateri-trilateri. Dualizzare le affermazioni su quadrangoli-triangoli.

6.4.2. Studio elementare dei quadrilateri piani completi. Dualizzare lo studio esplicito dei quadrangoli.

6.5. Quadrangolo piano semplice: è la figura formata da una quaterna ordinata di punti complanari, a tre a tre non allineati (detti i vertici) e dalle quattro rette congiungenti punti (circolarmente) consecutivi (dette i lati). Dati quattro punti complanari a tre a tre non allineati, quanti quadrangoli piani semplici distinti si possono formare? È vero che sono tutti proiettivamente equivalenti tra loro (cioè che possono essere scambiati ciascuno negli altri tramite proiettività del piano)?

Dualizzare (quadrilatero piano semplice).

♠ **6.5.1.** Separatori armonici comuni. Dati due punti distinti della retta proiettiva, vi sono infinite coppie che separano armonicamente i punti dati: infatti per ogni terzo punto distinto dai dati si può trovare il quarto armonico.

Date due coppie di punti distinti della retta proiettiva, esiste una unica coppia di punti che separa armonicamente entrambe le coppie date (servono ipotesi sul corpo di base?). Per verificarlo conviene supporre che i punti della prima coppia abbiano coordinate 0 e ∞ (cosicché le coppie armoniche sono formate da punti di coordinate opposte), e della seconda coppia abbiano coordinate 1 e a (arbitraria).

Nel caso di $\mathbb{R}$, mostrare che i separatori armonici di due coppie di punti reali sono reali se e solo se le due coppie non si separano tra loro (cioè se hanno birapporto positivo usando prima una coppia, poi l'altra). In particolare non sarà possibile dare una costruzione grafica lineare dei separatori armonici comuni; per una costruzione grafica serviranno almeno delle circonferenze: a partire dai quattro punti A, B, C, D si tracciano due circonferenze per trovare il punto medio M dei separatori armonici comuni;

poi la tangente da M a uno dei due cerchi permette di trovare i separatori comuni:

$$\|T-M\|^2 = \|A-M\|\,\|B-M\| = \|P-M\|\,\|Q-M\| = \|C-M\|\,\|D-M\|$$
$$(U,V,\infty,M) = (A,B,U,V) = (C,D,U,V) = -1$$

(che proprietà si stanno usando dei cerchi? Dati una circonferenza e un punto esterno, il prodotto delle sue distanze dai punti in cui una retta del suo fascio taglia la circonferenza non dipende dalla retta...).

6.6. Polarità di Poncelet di una coppia di rette rispetto ad un punto. Siano u, u' rette distinte in un piano proiettivo, P un punto ad esse esterno:

6.6.1. per ogni $r, r' \in P^*$ (rette distinte del fascio per P) i punti intersezione di $((r \wedge u) \vee (r' \wedge u'))$ e $((r \wedge u') \vee (r' \wedge u))$ sono tutti allineati, e formano una retta passante per $u \wedge u'$ (detta retta polare di u, u' rispetto a P);

6.6.2. per ogni $r \in P^*$ (retta del fascio per P) i quarti armonici, se esistono, dopo P, $r \wedge u$, $r \wedge u'$ sono tutti allineati: è la retta polare?

6.6.3. ogni retta per $u \wedge u'$ si può ottenere come polare rispetto a qualche punto?

6.6.4. l'omologia involutoria di centro P e asse la retta polare manda u in u' secondo la proiezione di centro P;

6.6.5. se un esagono ha i vertici pari in u, e quelli dispari su u', allora i lati opposti si incontrano in tre punti allineati; il viceversa è falso (vedi Pascal);

6.6.6. le polari di P rispetto alle coppie di lati di un triangolo incontrano i lati opposti in tre punti allineati (e tale retta si dice retta polare del triangolo rispetto a P);

6.6.7. e dualizzare tutto!

6.7. Osservazione: inserisco qui una osservazione che permette di meccanizzare certi calcoli successivi. Dati quattro punti distinti A, B, A', B' (che confonderemo con le loro coordinate in un sistema di riferimento scelto) del piano, vogliamo calcolare l'intersezione $r \wedge r'$ delle due rette $r = A \vee B$ e $r' = A' \vee B'$. Bene: le coordinate plückeriane delle due rette (nel riferimento duale) sono date da $r = A \times B$ e $r' = A' \times B'$, e il loro punto di intersezione ha coordinate $r \times r' = (A \times B) \times (A' \times B')$. Qui il $\times$ è il prodotto vettore (in quanto elementi di $\Bbbk^3$).

Generalizzare a n iperpiani di uno spazio di dimensione n usando il cross-product.

6.8. Teorema di Pappo (Asse di collineazione). *Date due rette distinte r, r' del piano, e su ciascuna tre punti distinti, siano $A, B, C \in r$ e $A', B', C' \in r$, diversi da $r \wedge r'$; allora i tre punti $(A \vee B') \cap (B \vee A')$, $(A \vee C') \cap (C \vee A')$ e $(B \vee C') \cap (C \vee B')$ sono allineati, la retta a che li congiunge si dice asse di collineazione. Inoltre, l'asse di collineazione contiene $r \wedge r'$ se e solo se le tre rette $A \vee A'$, $B \vee B'$, $C \vee C'$ sono concorrenti in un punto, e anche se e solo se i birapporti $(A\ B\ C\ r \wedge r')$ e $(A'\ B'\ C'\ r \wedge r')$ coincidono.*

Dimostrazione. Si tratta di un facile conto, usando un sistema di riferimento in cui i punti A, B, C abbiano coordinate $\begin{pmatrix}1\\0\\a\end{pmatrix}, \begin{pmatrix}1\\0\\b\end{pmatrix}, \begin{pmatrix}1\\0\\c\end{pmatrix}$ e i punti A', B', C' $\begin{pmatrix}1\\a'\\0\end{pmatrix}, \begin{pmatrix}1\\b'\\0\end{pmatrix}, \begin{pmatrix}1\\c'\\0\end{pmatrix}$ (in effetti basta scegliere due rette come fondamentali, e abbiamo ancora ampia scelta per specializzare il riferimento e precisare le coordinate dei punti; non lo facciamo solo per mantenere eleganza e simmetria del procedimento di calcolo). Si noti che a, b, c, a', b', c' sono tutti non nulli. Allora i tre punti di intersezione

cercati sono le colonne della matrice

$$\begin{pmatrix} aa'-bb' & aa'-cc' & bb'-cc' \\ a'b'(a-b) & a'c'(a-c) & b'c'(b-c) \\ ab(a'-b') & ac(a'-c') & bc(b'-c') \end{pmatrix}$$

che evidentemente ha determinante nullo, poiché la somma a segni alterni delle colonne moltiplicate rispettivamente per cc', bb', aa' dà il vettore nullo. Similmente si dimostra l'inoltre. □

6.8.1. Una dimostrazione alternativa, senza coordinate, può essere data anticipando un po' il punto seguente. Vi è una unica proiettività φ di r in r' che manda i tre punti A, B, C ordinatamente in A', B', C'. Ora, fissando ad esempio A, consideriamo la retta che congiunge $(A \vee B') \cap (B \vee A')$ con $(A \vee C') \cap (C \vee A')$, chiamiamola a. Allora la composizione delle proiezioni da r ad a di centro A' e da a a r' di centro A dà esattamente la proiettività φ detta. Quindi questa retta contiene tutti i punti del tipo $(P \vee \varphi Q) \cap (Q \vee \varphi P)$ per ogni $P, Q \in r$ (in particolare per B, C).

Conviene anche osservare che la retta a è l'unica passante per immagine e antimmagine tramite φ del punto $r \wedge r'$ (se non è un punto unito), e che la scrittura di φ come composizione di proiezioni non è unica (dipende dal punto A scelto) mentre la retta attraverso cui passano le proiezioni è sempre a, unica.

6.8.2. Variazioni sul teorema di Pappo. Variando l'ordine dei punti possiamo trovare 6 rette di collineazione, e si distribuiscono in due gruppi di 3 in fasci (configurazione duale di Pappo?).

6.9. Proiettività tra rette immerse nel piano: una proiettività tra due rette distinte del piano si scrive come composizione di al più due proiezioni da rette a rette di centri opportuni. Infatti, se $\varphi : r \longrightarrow r'$, e $A, B, C \in r$ distinti, allora i tre punti $(A \vee \varphi B) \cap (B \vee \varphi A)$, $(A \vee \varphi C) \cap (C \vee \varphi A)$ e $(B \vee \varphi C) \cap (C \vee \varphi B)$ sono allineati, la retta a che li congiunge si dice asse di collineazione per φ, e la proiettività si scrive come composizione della proiezione $r \longrightarrow a$ di centro φA e della proiezione $a \longrightarrow r'$ di centro A.

Si osservi anche che una proiettività tra due rette distinte è una proiezione se e solo se il punto di intersezione è unito.

6.9.1. Una proiettività di una retta in sè si scrive come proiezione di al più tre proiezioni da rette a rette di centri opportuni. Il punto è che basta comporre con una proiezione su un'altra retta, e poi decomporre la composizione come prodotto di due proiezioni (l'inversa di una proiezione è una proiezione, ovviamente?).

6.9.2. Dualizzare: studiare le proiettività tra fasci di rette del piano.

6.9.3. Problema. Siano r, r' due rette complanari, e C un punto non appartenente alle due rette. Sia $\varphi : R \to r'$ la proiezione da r ad r' di centro C (definita da $\varphi(R) = (R \vee C) \wedge r'$ per ogni $R \in r$). Mostrare che tutti i punti definiti da $(A \vee \varphi(B)) \wedge (B \vee \varphi(A))$ al variare di A, B in r sono tutti appartenenti ad una retta a passante per $r \wedge r'$. Mostrare che le quattro rette $r, r', a, C \vee (r \wedge r')$ formano una quaterna armonica. Dedurre che la retta a rimane la stessa per tutti i punti di $C \vee (r \wedge r')$ (ma la proiezione φ cambia cambiando il punto).

Dualizzare.

6.10. Triangoli prospettivi e omologici. Due triangoli A, B, C e A', B', C' in $\mathbb{P}^n(\Bbbk)$ (di lati a, b, c e a', b', c', ove una minuscola congiunge le due maiuscole diverse) si dicono prospettivi se le rette $A \vee A'$, $B \vee B'$ e $C \vee C'$ si incontrano in un punto (ovvero vertici omologhi generano tre rette convergenti in un punto); si dicono omologici se i tre punti $a \wedge a'$, $b \wedge b'$ e $c \wedge c'$ sono allineati (lati omologhi si incontrano in tre punti allineati).

Per due triangoli in un piano, essere omologici è duale di essere prospettivi.

6.10.1. Teorema di Desargues. *Una coppia di triangoli è prospettiva se e solo se è omologica (nel piano si tratta di un'affermazione autoduale: una implicazione è duale dell'altra; in*

dimensioni maggiori?).

Dimostrazioni. Osserviamo che se i triangoli sono prospettivi, oppure omologici, allora essi sono contenuti in uno spazio proiettivo di dimensione al più tre. Inoltre, per dualità, nel caso piano basta dimostrare che due triangoli prospettivi sono omologici.

6.10.2. Proponiamo una prima dimostrazione usando esplicitamente delle coordinate proiettive. Supponiamo che i triangoli non siano complanari; poiché i triangoli sono prospettivi, possiamo scegliere il punto di prospettività come origine e i tre punti di un triangolo come gli altri punti fondamentali del riferimento. Dunque un triangolo ha vertici di coordinate $A = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, B = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, C = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$, mentre l'altro ha vertici di coordinate $A' = \begin{pmatrix} 1 \\ a \\ 0 \\ 0 \end{pmatrix}, B' = \begin{pmatrix} 1 \\ 0 \\ b \\ 0 \end{pmatrix}, C' = \begin{pmatrix} 1 \\ 0 \\ 0 \\ c \end{pmatrix}$, (cioè sono prospettivi nell'origine). I lati dei due triangoli hanno equazioni

$$\begin{aligned} a:&\ X_0 = 0 = X_1 & \qquad a':&\ X_1 = 0 = bcX_0 - cX_2 - bX_3 \\ b:&\ X_0 = 0 = X_2 & \qquad b':&\ X_2 = 0 = acX_0 - cX_1 - aX_3 \\ c:&\ X_0 = 0 = X_3 & \qquad c':&\ X_0 = 0 = abX_0 - bX_1 - aX_2 \end{aligned}$$

e quindi i tre punti di intersezione sono dati da

$$a \wedge a' = \begin{pmatrix} 0 \\ 0 \\ b \\ -c \end{pmatrix} \qquad b \wedge b' = \begin{pmatrix} 0 \\ a \\ 0 \\ -c \end{pmatrix} \qquad c \wedge c' = \begin{pmatrix} 0 \\ a \\ -b \\ 0 \end{pmatrix} .$$

Per verificate che i tre punti sono allineati basta osservare che la loro somma con segni alterni è nulla. Il viceversa, ovvero che triangoli omologici sono prospettivi si fa in modo analogo: scegliendo un riferimento proiettivo avente un vertice di ciascun triangolo in un punto fondamentale, e l'intersezione dei lati non omologhi di quei vertici come ulteriori punti fondamentali.
Usando $A = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $A' = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$, $b \wedge b' = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, $c \wedge c' = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$,
abbiamo che $B = \begin{pmatrix} 1 \\ 0 \\ b \\ 0 \end{pmatrix}$, $B' = \begin{pmatrix} 0 \\ 0 \\ b' \\ 1 \end{pmatrix}$, $C = \begin{pmatrix} 1 \\ c \\ 0 \\ 0 \end{pmatrix}$, $C' = \begin{pmatrix} 0 \\ c' \\ 0 \\ 1 \end{pmatrix}$, con $\det \begin{pmatrix} b & b' \\ c & c' \end{pmatrix} = 0$ (perché?). Si vede subito allora che si ha un punto di prospettività.

6.10.3. Lasciamo per esercizio il caso di triangoli complanari; in questo caso possiamo scegliere un riferimento in cui il punto di prospettività è il punto unità, ed i tre vertici di un triangolo sono i punti fondamentali. Un facile disegno (o un facile conto) dà allora il risultato. □

6.10.4. Proponiamo una seconda dimostrazione che è valida se supponiamo che i triangoli non siano complanari e non fa uso di coordinate. Siano π e π' i piani su cui giacciono i triangoli, e sia $\varrho : \pi \to \pi'$ la proiezione di centro il punto di prospettività dei triangoli. Allora i punti della retta $\pi \wedge \pi'$ sono (i soli) uniti per ϱ, e contengono i tre punti di intersezione dei lati (perché? un lato e la sua immagine, che è il lato omologo, devono intersecare $\pi \wedge \pi'$ nello stesso punto...).

Per il viceversa, conviene cercare una proiettività, tra i due piani contenenti i triangoli, che mandi i vertici del primo in quelli del secondo e che fissi puntualmente la retta di intersezione: sarà allora una proiezione di centro un punto, e i due triangoli prospettivi. Per definire tale proiettività si può sia mandare i vertici nei vertici, e un punto della retta $\pi \wedge \pi'$ in sè (allora bisogna dimostrare che i tre punti di intersezione dei lati omologhi sono punti uniti, possibile con un facile argomento di birapporti), sia mandare due punti di un triangolo nei corrispondenti dell'altro e fissare i punti di intersezione dei lati

omologhi in $\pi \wedge \pi'$ (allora bisogna dimostrare che il terzo vertice va nel terzo vertice, e che anche il terzo punto di intersezione di lati in $\pi \wedge \pi'$ è unito, entrambe cose facili). $\square$

6.10.5. Infine proponiamo una terza dimostrazione che è valida se supponiamo che i triangoli siano complanari e non fa uso di coordinate. Poiché i triangoli sono prospettivi possiamo considerare la proiettività del piano che fissa il punto di prospettività O e manda i vertici di un triangolo nei corrispondenti dell'altro. Si tratta di una omologia di centro O, poiché il fascio di rette di centro O ha tre rette unite, e quindi è unito. Dunque esiste una retta di punti uniti, che necessariamente contiene tutti i punti uniti distinti da O; in particolare contiene le tre intersezioni di lati corrispondenti (perché si tratta di punti uniti? sono punti che stanno su un lato e sulla retta per O e sè stessi...). $\square$

6.10.6. Variazioni sulla dimostrazione. Nel caso del piano possiamo anche dimostrare il teorema mostrando che per due triangoli le condizioni di prospettività e di omologia equivalgono alla stessa condizione algebrica. Possiamo supporre che il primo triangolo abbia vertici P_0, P_1, P_2 punti del riferimento canonico, e il secondo triangolo generico $A' = \left(\begin{smallmatrix} x_0 \\ x_1 \\ x_2 \end{smallmatrix}\right)$, $B' = \left(\begin{smallmatrix} y_0 \\ y_1 \\ y_2 \end{smallmatrix}\right)$, $C' = \left(\begin{smallmatrix} z_0 \\ z_1 \\ z_2 \end{smallmatrix}\right)$. Allora la condizione di prospettività è l'annullamento del determinante (dato dalle coordinate plückeriane delle rette per vertici corrispondenti):

$$0 = \det \begin{pmatrix} 0 & -y_2 & -z_1 \\ -x_2 & 0 & z_0 \\ x_1 & y_0 & 0 \end{pmatrix} = x_2 y_0 z_1 - x_1 y_2 z_0$$

mentre la condizione di omologia si ottiene usando i punti di intersezione dei lati corrispondenti, che sono le tre colonne della matrice

$$\begin{pmatrix} y_2 \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} - x_2 \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix} & z_1 \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} - x_1 \begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix} & z_0 \begin{pmatrix} y_0 \\ y_1 \\ y_2 \end{pmatrix} - y_0 \begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix} \end{pmatrix}$$

il cui determinante si calcola facilmente, per multilinearità sulle colonne, essere:

$$-(x_2 y_0 z_1 - x_1 y_2 z_0) \det \begin{pmatrix} x_0 & y_0 & z_0 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{pmatrix}$$

e si conclude dunque che le due condizioni sono equivalenti. Si possono anche calcolare punto di prospettività e retta di omologia.

6.10.7. Variazioni sul teorema di Desargues. Giocare con tre triangoli prospettivi dallo stesso punto, e con tre triangoli due a due prospettivi. Come si distribuiscono le rette di omologia, ci sono casi in cui coincidono? Distinguere i casi di piano e spazio. Se il punto di prospettività è lo stesso, si può applicare tre volte anche il teorema di Pappo: che relazioni ci sono tra le rette di omologia e quelle di collineazione?

6.10.8. Desargues e pentagoni. Nel teorema di Desargues compaiono dieci punti e dieci rette (configurazione di Desargues). Mostrare che possono essere divisi in due pentagoni ciascuno inscritto nell'altro (ogni vertice di ciascuno appartiene ad un lato dell'altro).

♠ **6.11.** Nota culturale. I teoremi di Pappo e Desargues (nel piano) sono molto importanti anche per una loro caratterizzazione algebrica, che qui non dimostriamo, ma che possiamo facilmente enunciare, anche se in modo un po' impreciso. Costruendo la geometria proiettiva piana in termini assiomatici (per poi costruire qualche struttura algebrica di base canonicamente associata per identificare la geometria assiomatica con costruzioni di algebra lineare), oppure definendola in termini di algebra lineare ma usando strutture algebriche di base più deboli di un campo, si può vedere che: vale il teorema di Desargues sse la struttura di base è un corpo (non necessariamente commutativo, ma l'associatività del prodotto è essenziale) e vale il teorema di Pappo sse la struttura di base è un campo (cioè la commutatività del prodotto è essenziale). In particolare, Pappo implica Desargues (e non viceversa). Per esempio un piano proiettivo sui quaternioni rispetta il teorema di Desargues, ma non quello di Pappo; un piano proiettivo sugli ottonioni non verifica nessuno dei due teoremi.

Possiamo mostrare direttamente che il teorema di Pappo implica quello di Desargues nel modo seguente, nel piano: dati A, B, C e A', B', C' triangoli prospettivi da O, definiamo $D = BC \wedge B'C'$, $E = AC \wedge A'C'$ e $F = AB \wedge A'B'$ (dobbiamo mostrare che sono allineati). Usiamo i punti: $U = OA \wedge BC'$, $X = AB \wedge A'C'$, $Y = OX \wedge BC$, $Z = OX \wedge B'C'$. Allora:

(1) usando Pappo sulle terne ordinate O, C, C' e B, X, A otteniamo che Y, U, E sono allineati, in particolare $E \in UY$;
(2) usando Pappo sulle terne ordinate O, B, B' e C', A', X otteniamo che U, Z, F sono allineati, in particolare $F \in UZ$;
(3) usando Pappo sulle terne ordinate B, C', U e Z, Y, X otteniamo che D, F, E sono allineati, come si voleva.

♠ **6.12.** Altri esempi classici: prospettività tra quadrangoli.

Se due quadrangoli piani completi, senza vertici o lati comuni, sono tali che cinque lati omologhi hanno intersezioni su una retta, allora anche la sesta coppia di lati omologhi si interseca in quella retta, e le quattro rette che uniscono vertici omologhi appartengono ad un fascio.

Se due quadrilateri piani completi, senza vertici o lati comuni, sono tali che cinque vertici omologhi generano rette d'un fascio, allora anche la sesta coppia di vertici omologhi genera una retta di quel fascio, e i quattro punti di intersezione di lati omologhi sono allineati.

6.13. Proiettività tra rette sghembe nello spazio proiettivo: si tratta di proiezioni di centro una retta (si può scegliere qualsiasi retta distinta da r ed r' che sia complanare con le tre rette $A \vee \varphi A$, $B \vee \varphi B$ e $C \vee \varphi C$: basta confrontare proiettività e proiezione sui tre punti scelti). Si tratta di una costruzione già incontrata? Le rette che si possono usare come asse che figura formano?

Dualizzare: studiare le proiettività tra fasci di piani (di asse una retta) nello spazio. Ovvero?

♠ **6.14.** Altri esempi classici: duale spaziale di Desargues? Si noti che il duale nello spazio tridimensionale della nozione di triangolo (3 punti, le 3 rette e il piano generati) è la nozione di triplano (3 piani, le 3 rette e il punto segati), quindi una figura geometrica che di solito non si studia. Si può comunque per una coppia di triplani dare le nozioni di essere omologici (intersezione di facce omologhe sono rette complanari), di essere prospettivi (sup di lati omologhi sono piani di un fascio), ed enunciare il teorema come: una coppia di triplani è prospettiva se e solo se è omologica.

Si generalizza senza difficoltà al caso n-dimensionale.

♠ **6.14.1.** Analogo spaziale di Desargues: teorema di Poncelet. In uno spazio proiettivo di dimensione 3, un tetraedro è il dato di 4 punti in posizione generale, delle 6 rette e 4 piani da essi generati. Due tetraedri sono detti prospettivi se vertici omologhi generano rette d'un fascio, e sono detti omologici se facce omologhe si incontrano in rette complanari. Il teorema di Poncelet, che afferma che una coppia di tetraedri è prospettiva se e solo se è omologica, è autoduale (in dimensione 3; è vero, ma non autoduale in dimensioni superiori), e va pensato come la generalizzazione tridimensionale di Desargues.

Anche qui non vi sono ostacoli per trovare la generalizzazione n-dimensionale di Desargues.

♠ **6.15.** Problema. Si pensi lo spazio euclideo come spazio affine immerso nello spazio proiettivo. Sappiamo allora che le rigidità (trasformazioni euclidee) rispettano le distanze tra due punti; le affinità non rispettano le distanze tra due punti, ma rispettano il rapporto delle distanze tra tre punti allineati; e infine che le proiettività rispettano (quando ha senso) il birapporto delle distanze per quattro punti allineati, ma in generale non strutture più semplici.

Trovare invarianti proiettivi n-dimensionali; per esempio nel caso del piano: ogni rigidità rispetta l'area del triangolo dato da tre punti; in generale le affinità cambiano le aree, ma cosa lasceranno invariato? e le proiettività, appunto?

♠ **6.16.** Nota culturale. Riguardando a ritroso le diverse geometrie finora incontrate (spazi vettoriali, spazi affini, spazi euclidei, spazi proiettivi) si può capire lo spirito del cosiddetto "programma di Erlangen" in cui si definisce lo studio della geometria come lo studio degli invarianti sotto un gruppo di trasformazioni prefissato:
(0) per uno spazio vettoriale V è il gruppo degli automorfismi di V (isomorfismi lineari $\mathrm{GL}(V)$);

(1) per uno spazio proiettivo $\mathbb{P}(V)$ è il gruppo delle proiettività ($\mathrm{PGL}(V)$);
(2) per uno spazio affine complementare di H_∞ in $\mathbb{P}(V)$ è il gruppo delle proiettività che stabilizzano globalmente H_∞ (affinità);
(3) per uno spazio conforme complementare di H_∞ in $\mathbb{P}(V)$ e con una scelta di una quadrica Ω in H_∞ è il gruppo delle affinità che stabilizzano globalmente Ω (conformità rispetto a Ω);
(4) per uno spazio pseudoeuclideo complementare di H_∞ in $\mathbb{P}(V)$ e con una scelta di una forma quadratica q su H_∞ è il gruppo delle affinità che rispettano q (rigidità, isometrie di q).

Negli ultimi casi siamo abituati ad usare forme definite positive (casi euclidei), ma si può fare altrimenti. Più grande è il gruppo delle trasformazioni ammesse, meno sono gli invarianti geometrici che si possono trovare e definire, ma più semplici e chiari tendono ad essere i risultati essenziali.

♠ **6.17.** Problema-Gioco (per sviluppare l'immaginazione). Dato un triangolo di vertici A, B, C (lati a, b, c ciascuno opposto al vertice omonimo), e un triangolo inscritto di vertici $A_1 \in a, B_1 \in b, C_1 \in c$, si può trovare un altro triangolo inscritto in quello iniziale usando come vertici le intersezioni dei lati del secondo: $A_2 = a_1 \wedge a, B_2 = b_1 \wedge b, C_2 = c_1 \wedge c$; poi si procede usando il secondo triangolo, e per induzione si trova una successione di triangoli tutti inscritti in quello iniziale. Questo procedimento può fermarsi o prosegue dando sempre triangoli diversi? Se non si ferma, che cosa succede al limite della successione di triangoli?

Non dimenticarsi di dualizzare.

♠ **6.18.** Altro problema-gioco (per sviluppare l'immaginazione). Nel piano proiettivo sono date tre rette distinte r, s, t di un fascio per un punto O. Siano R_0, S_0, T_0 punti sulle rette r, s, t rispettivamente, non allineati (triangolo). Definiamo una sequenza di triangoli costruendo $R_{i+1}, S_{i+1}, T_{i+1}$ a partire da R_i, S_i, T_i intersecando i lati con le rette r, s, t (in altri termini costruiamo l'unico triangolo che è prospettivo da O e inscritto nel precedente) per ogni $i \in \mathbb{N}$. Determinare il limite per $i \to \infty$ dei punti R_i, S_i, T_i.

Definire con un processo inverso una sequenza di triangoli R_i, S_i, T_i per $i \in -\mathbb{N}$ (triangoli ricorsivamente prospettivi e circoscritti al successivo), e determinare il limite per $i \to -\infty$ dei punti R_i, S_i, T_i.

Studiare le rette di omologia delle coppie di triangoli prospettivi del problema.

6.19. Problema: versioni proiettive di Menelao e Ceva. I teoremi affini di Menelao e Ceva danno condizioni di allineamento o di convergenza a partire da punti sui lati di un triangolo; essendo un problema su un piano affine, si può pensare come problema su un piano proiettivo con una fissata retta (da usare come retta impropria nella versione affine).

6.19.1. Si possono quindi enunciare i seguenti due risultati: dato un triangolo di vertici A, B, C (lati a, b, c) e una retta u generica (interseca i lati in punti distinti dai vertici) e considerati tre punti A', B', C' su a, b, c rispettivamente (diversi da tutti i precedenti), allora:

(Menelao) A', B', C' sono allineati se e solo se $(A\ B\ C'\ c\wedge u)(B\ C\ A'\ a\wedge u)(C\ A\ B'\ b\wedge u)=1$;

(Ceva) $A\vee A'$, $B\vee B'$, $C\vee C'$ sono in un fascio sse $(A\ B\ C'\ c\wedge u)(B\ C\ A'\ a\wedge u)(C\ A\ B'\ b\wedge u)=-1$.

Dimostrare direttamente questi enunciati. Verificare inoltre che il secondo enunciato è equivalente al duale del primo (in particolare dualizzare entrambi gli enunciati!); nel fare questo, può essere utile usare il seguente fatto (da dimostrare): dati $A', A'' \in a$, $B', B'' \in b$, $C', C'' \in c$ che siano separatori armonici dei vertici, allora A', B', C' sono allineati se solo se $A\vee A''$, $B\vee B''$, $C\vee C''$ sono in un fascio.

6.19.2. Si possono dedurre i risultati precedenti dal seguente: dato un triangolo di vertici A, B, C (lati a, b, c) e dati $A', A'' \in a$, $B', B'' \in b$, $C', C'' \in c$ (generici, cioè distinti tra di loro e dai vertici), allora esiste una proiettività del piano cha manda ordinatamente A, B, C, A', B', C' in A, B, C, A'', B'', C'' se solo se risulta $(A\ B\ C'\ C'')(B\ C\ A'\ A'')(C\ A\ B'\ B'')=1$.

Dimostrare direttamente l'enunciato, e dedurne i teoremi precedenti.

7. Problemi.

7.1. Problemi di geometria proiettiva.

7.1.1. Discutere le soluzioni di $aX + bY = c$ nel piano affine, e del sistema omogeneizzato. Descrivere le soluzioni del secondo, la loro relazione con le soluzioni del primo e fare un disegno che spieghi i risultati.

7.1.2. Discutere le soluzioni del sistema $\begin{cases} X+Y=0 \\ X+Y=2 \end{cases}$ e del sistema omogeneizzato, confrontandone le soluzioni e facendo un disegno dei risultati. È possibile disomogeneizzare il sistema ottenuto in modo da ottenere due rette in un piano affine che si intersechino?

7.1.3. Discutere le soluzioni del sistema $\begin{cases} X+Y=1 \\ X-Y=1 \end{cases}$ e del sistema omogeneizzato, confrontandone le soluzioni e facendo un disegno dei risultati. È possibile disomogeneizzare il sistema ottenuto in modo da ottenere due rette in un piano affine che siano parallele?

7.1.4. Discutere il sistema di equazioni di due piani distinti in $\mathbb{A}^3(\mathbb{R})$ ed il suo omogeneizzato, esplicitando i ranghi delle varie matrici, e confrontando le soluzioni dei due sistemi. Possibilmente fare un disegno che spieghi i risultati.

7.1.5. Discutere il sistema di equazioni di un piano ed una retta (non contenuta nel piano) in $\mathbb{A}^3(\mathbb{R})$ ed il suo omogeneizzato, esplicitando i ranghi delle varie matrici, e confrontando le soluzioni dei due sistemi. Possibilmente fare un disegno che spieghi i risultati.

7.1.6. Discutere il sistema di equazioni di due rette distinte in $\mathbb{A}^3(\mathbb{R})$ ed il suo omogeneizzato, esplicitando i ranghi delle varie matrici, e confrontando le soluzioni dei due sistemi. Possibilmente fare un disegno che spieghi i risultati.

7.1.7. Perché un sistema che sia già omogeneo non coincide con il proprio omogeneizzato? Confrontarne le soluzioni, facendo qualche esempio, con dei disegni esplicativi.

7.1.8. Discutere il sistema dei due piani $P + \langle v, w\rangle$ e $Q + \langle v, u\rangle$ ove $P = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, Q = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ sono punti in $\mathbb{A}^4(\mathbb{R})$ e $v = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, w = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, u = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$ sono vettori di $\mathbb{R}^4$, ed il suo omogeneizzato. Disomogeneizzare il nuovo sistema in modo da trovare due piani (in uno spazio affine di dimensione 4) che si intersecano (in un punto?).

7.1.9. Discutere il sistema dei due piani $P + \langle v_1, v_2\rangle$ e $Q + \langle w_1, w_2\rangle$ ove $P = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, Q = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$ sono punti in $\mathbb{A}^4(\mathbb{R})$ e $v_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, w_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, w_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ sono vettori di $\mathbb{R}^4$, ed il suo omogeneizzato. È vero che i due piani sono contenuti in un sottospazio di dimensione tre?

7.1.10. Date due rette nel piano proiettivo, è sempre possibile scegliere un piano affine (complementare di una opportuna retta del piano proiettivo) tale che esse risultino parallele?

Consideriamo una figura quadrilatera (formata da quattro punti ordinati, a tre a tre non allineati, e dalle quattro rette che congiungono ogni punto col successivo, e l'ultimo con il primo) nel piano proiettivo. È sempre possibile scegliere un piano affine (complementare di una opportuna retta del piano proiettivo) tale che la figura in questione diventi un parallelogramma?

7.1.11. In $\mathbb{P}^3(\mathbb{R})$ siano $P = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ e α il piano di equazione $\alpha : 2X_0 - X_1 + X_3 = 0$. Sia π la proiezione di centro P verso α. Determinare $\pi(Q)$ per $Q = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}$.

7.1.12. Verificare se le rette

$$r : \begin{cases} X_0 - X_1 + X_2 = 0 \\ X_1 - 2X_2 + X_3 = 0 \end{cases} \qquad \text{e} \qquad s : \begin{cases} X_0 + X_2 - 3X_3 = 0 \\ X_0 - 2X_1 - 2X_2 = 0 \end{cases}$$

di $\mathbb{P}^3(\mathbb{R})$ sono sghembe oppure incidenti.

7.1.13. Come vengono descritte dagli abitanti di $\mathbb{P}^*(V)$ le quaterne ordinate di punti allineati di $\mathbb{P}(V)$?

7.1.14. Siano r ed s due rette sghembe di $\mathbb{P}^3(\mathbb{R})$. Verificare che per ogni punto P di $\mathbb{P}^3(\mathbb{R})$ non contenuto né in r né in s, esiste un'unica retta t per P incidente sia r che s.

7.1.15. È vero o falso che in uno spazio proiettivo di dimensione maggiore o uguale a 3 è possibile trovare tre rette a due a due sghembe? E quattro? Ed n? E infinite?

7.1.16. Siano H un iperpiano ed L una varietà lineare di dimensione r di un dato spazio proiettivo, non contenuta in H. Calcolare la dimensione di $H \wedge L$. Che cosa si può dire se H ha codimensione 2 (invece che 1)?

7.1.17. Sia $\Bbbk$ un corpo. Siano L, M ed N tre rette a due a due sghembe in $\mathbb{P}^4(\Bbbk)$ e si supponga che $\dim(L \vee M \vee N) = 4$. Dimostrare che esiste una ed una sola retta trasversale comune alle rette L, M ed N date.

Trovare l'enunciato duale e darne una dimostrazione diretta.

7.1.18. Sia $\Bbbk$ un corpo. Siano L, M ed N tre rette a due a due sghembe in $\mathbb{P}^5(\Bbbk)$ e si supponga che $\dim(L \vee M \vee N) = 5$. Dimostrare che per ogni punto P di $\mathbb{P}^5(\Bbbk)$ non appartenente a $(L \vee M) \cup (L \vee N) \cup (M \vee N)$ esiste uno ed un solo piano passante per P ed intersecante ciascuna delle rette L, M ed N date.

Trovare l'enunciato duale e darne una dimostrazione diretta.

7.1.19. Sia $\Bbbk$ un corpo. Siano date $n+1$ rette $L_0, L_1, \ldots, L_n$ in posizione generale in $\mathbb{P}^{2n}(\Bbbk)$ (i.e. $\dim(L_0 \vee L_1 \vee \ldots \vee L_n) = 2n$ e $\dim(L_0 \vee \ldots \vee \widehat{L_i} \vee \ldots \vee L_n) = 2n-1$ per ogni i). È vero che esiste una ed una sola varietà lineare T di $\mathbb{P}^{2n}(\Bbbk)$ di dimensione $n-1$ trasversale a tutte le rette $L_0, L_1, \ldots, L_n$ date? Esplicitare per n piccoli.

Dualizzare.

7.1.20. Sia $n \geqslant 3$ un intero. Sia $\mathscr{R}$ un insieme di rette di $\mathbb{P}^n(\Bbbk)$ contenente almeno tre elementi. Si supponga che per ogni $r, s \in \mathscr{R}$ si abbia $r \wedge s \neq \varnothing$ (ogni due rette in $\mathscr{R}$ siano incidenti). È vero o falso che tutte le rette di $\mathscr{R}$ sono contenute in uno stesso piano oppure passano per uno stesso punto?

Dualizzare per $n = 3$, $n = 4$, $n > 4$.

7.1.21. Un $n+1$-edro (triangolo se $n = 2$, tetraedro se $n = 3$) $\mathscr{T}$ in $\mathbb{P}^n(\Bbbk)$ è l'insieme di varietà lineari di $\mathbb{P}^n(\Bbbk)$ formato da $n+1$ punti $P_0, P_1, \ldots, P_n$ in posizione generale (i.e. $\dim(P_0 \vee P_1 \vee \ldots \vee P_n) = n$) detti vertici e dalle varietà lineari, dette facce, che si ottengono congiungendo in tutti i modi possibili i vertici. Diremo che un $n+1$-edro $\mathscr{T}'$ di vertici $P'_0, P'_1, \ldots, P'_n$ è circoscritto a $\mathscr{T}$ se per ogni i si ha che $P_i \in P'_0 \vee \ldots \vee \widehat{P'_i} \vee \ldots \vee P'_n$ e P_i non appartiene ad alcuna faccia di $\mathscr{T}'$ di dimensione minore di $n-1$.

(0) Capire la definizione.
(1) È possibile trovare due triangoli circoscritti ciascuno all'altro?
(2) È possibile trovare due tetraedri circoscritti ciascuno all'altro? (può essere utile pensare a matrici antisimmetriche?)

Si generalizzi, se possibile.

7.1.22. Nello spazio proiettivo $\mathbb{P}^3(\Bbbk)$ si considerino quattro punti P_1, P_2, P_3, P_4. Mostrare che essi non sono complanari se e solo se per ogni permutazione σ di $\{1, 2, 3, 4\}$ le due rette $P_{\sigma 1} \vee P_{\sigma 2}$ e $P_{\sigma 3} \vee P_{\sigma 4}$ sono sghembe.

Dualizzare l'enunciato.

Come si generalizzano l'enunciato e il suo duale in $\mathbb{P}^n(\Bbbk)$?

7.1.23. Siano dati un piano π e una retta r tra loro sghembi in $\mathbb{P}^4(\Bbbk)$.

(a) Mostrare che per ogni punto P non appartenente né ad r né a π, esiste una unica retta p per P incidente sia r sia π.
(b) Se il punto P varia su una retta, come si può descrivere l'unione di tutte le rette p che si ottengono nel punto precedente?
(c) Dualizzare l'enunciato del punto (a).

7.1.24. Siano dati un piano π e una retta r tra loro sghembi in $\mathbb{P}^4(\Bbbk)$.

(a) Mostrare che, per ogni retta s contenuta π, $r \vee s$ è uno spazio di dimensione 3 la cui intersezione con π è esattamente s.

(*b*) È vero o falso che ogni iperpiano della stella di r si ottiene come $r \vee s$ per qualche retta (unica?) s contenuta in π?
(*c*) Dualizzare l'enunciato del punto (*a*).

7.1.25. Siano dati un piano π e una retta r tra loro sghembi in $\mathbb{P}^4(\Bbbk)$.
(*a*) Mostrare che, per ogni punto R di r, $R \vee \pi$ è uno spazio di dimensione 3 la cui intersezione con r è esattamente R.
(*b*) È vero o falso che ogni iperpiano della stella di π si ottiene come $R \vee \pi$ per qualche punto (unico?) R contenuto in r?
(*c*) Dualizzare l'enunciato del punto (*a*).

7.1.26. In un piano proiettivo siano date tre rette distinte r_1, r_2, r_3 passanti per un punto O, e due rette p, q non contenenti O e la cui intersezione non appartenga alle tre rette precedenti. Detti P_1, P_2, P_3 le intersezioni di p con r_1, r_2, r_3, e Q_1, Q_2, Q_3 le intersezioni di q con r_1, r_2, r_3:
(*a*) i quarti armonici S_i dopo O, P_i, Q_i (per $i = 1, 2, 3$) sono allineati;
(*b*) la retta contenente S_1, S_2, S_3 passa per $p \cap q$.
(*c*) Dualizzare la costruzione e i risultati precedenti.

7.1.27. Dualizzare e "dimostrare o confutare tramite controesempi" le seguenti affermazioni:
(*a*) Dati due piani π_1, π_2 e una retta r in $\mathbb{P}^3(\Bbbk)$, allora $\pi_1 \wedge \pi_2$ è sghembo con r se e solo se $\pi_1 \wedge r \neq \pi_2 \wedge r$.
(*b*) Dati due piani π_1, π_2 e una retta r in $\mathbb{P}^4(\Bbbk)$, allora $\pi_1 \wedge \pi_2$ è sghembo con r se e solo se $\pi_1 \wedge r \neq \pi_2 \wedge r$.
(*c*) Dati tre piani π_1, π_2 e σ in $\mathbb{P}^4(\Bbbk)$, allora $\pi_1 \wedge \pi_2$ è sghembo con σ se e solo se $\pi_1 \wedge \sigma$ è sghembo con $\pi_2 \wedge \sigma$.

7.1.28.
(*a*) Siano r una retta P_1, P_2 punti distinti non in r di $\mathbb{P}^3(\Bbbk)$. Mostrare che $P_1 \vee P_2$ è sghemba con r se e solo se $P_1 \vee r \neq P_2 \vee r$. Dualizzare l'enunciato.
(*b*) Generalizzare l'enunciato a $\mathbb{P}^n(\Bbbk)$ usando un sottospazio L e due sottospazi M_1, M_2 (della stessa dimensione e sghembi tra loro) che siano sghembi con L: quando $M_1 \vee M_2$ è sghembo con L?

7.1.29.
(*a*) Siano date quattro rette a due a due sghembe in $\mathbb{P}^3(\mathbb{R})$. Esistono ed eventualmente quante (rette) trasversali comuni?
(*b*) Dualizzare la domanda e la soluzione del punto precedente.

7.1.30. Dato un riferimento P_0, P_1, P_2, U di un piano proiettivo, determinare i punti Q del piano tali che le rette $Q \vee P_0, Q \vee P_1, Q \vee P_2, Q \vee U$ formano una quaterna armonica (nell'ordine dato).

7.1.31. Siano dati tre punti distinti A, B, C su una retta proiettiva, e siano X, Y, Z i quarti armonici delle terne (A, B, C), (B, C, A) e (C, A, B).
(*a*) Determinare i quarti armonici dopo X, Y, Z nei vari ordini possibili.
(*b*) Quali sono le immagini di X, Y, Z tramite la proiettività che manda ordinatamente A, B, C in X, Y, Z?

7.1.32. Date due rette incidenti distinte r, r', siano A, B, C tre punti su r e A', B', C' tre punti su r' tutti distinti e diversi da $r \wedge r'$.
(*a*) Dimostrare che $A \vee A'$, $B \vee B'$, $C \vee C'$ sono rette concorrenti in un punto se e solo se $(A\ B\ C\ r \wedge r') = (A'\ B'\ C'\ r \wedge r')$.
(*b*) Dualizzare l'enunciato nel piano e nello spazio.

7.1.33. (*Una costruzione dello spazio affine.*) Siano V uno spazio vettoriale di dimensione $n+1$ sul corpo $\Bbbk$ e I un suo sottospazio di codimensione 1. Sia G l'insieme degli automorfismi φ di V con le seguenti proprietà:

$$a)\quad \varphi_{|I} = \mathrm{id}_I; \qquad b)\quad \text{se} \quad \varphi\langle v\rangle = \langle v\rangle \quad \text{e} \quad v \notin I, \quad \text{allora} \quad \varphi = \mathrm{id}_V.$$

(i) Si mostri che G è un sottogruppo di $\mathrm{GL}(V)$.
(ii) Si mostri che per ogni vettore $v \notin I$ e per ogni $\varphi \in G$, si ha $\varphi(v) = v + w$, ove $w = w(v, \varphi) \in I$ è un vettore che dipende da v e φ.
(iii) Si fissi un vettore $v \notin I$ e si mostri che l'applicazione $F_v : G \to I$ definita da $\varphi \mapsto w(v, \varphi)$ è un isomorfismo del gruppo G sul gruppo $(I, +)$. Si indichi con G_v lo spazio vettoriale il cui gruppo soggiacente è G e in cui la moltiplicazione per gli scalari è definita da $\alpha\varphi = F_v^{-1}(\alpha w(v, \varphi))$.

(iv) Si mostri che se $v_1, v_2 \notin I$, allora gli spazi vettoriali G_{v_1}, G_{v_2} sono isomofi; più precisamente si mostri che $F_{v_1} F_{v_2}^{-1}$ è un'omotetia dello spazio vettoriale I.

(v) Sia E l'insieme dei sottospazi di dimensione 1 di V che non sono contenuti in I. Si mostri che l'immagine di ogni elemento P di E tramite ogni elemento φ di G è ancora un elemento di E. Si mostri infine che, comunque si fissi $v \notin I$, l'azione di G su E munisce quest'ultimo di una struttura di spazio affine su G_v.

7.1.34. (*Completamento dello spazio affine*). Sia V uno spazio vettoriale di dimensione n su $\Bbbk$ munito della struttura canonica di spazio affine su se stesso. Si considerino lo spazio proiettivo $\mathbb{P}(\Bbbk \oplus V)$ e l'applicazione $\mathscr{A} : V \to \mathbb{P}(\Bbbk \oplus V)$ definita da $v \mapsto \langle (1, v) \rangle$.

(i) Si mostri che $\mathscr{A}$ è un'affinità dello spazio affine V sullo spazio affine $\mathbb{P}(\Bbbk \oplus V) \setminus I$, ove I è l'iperpiano $\{0\} \oplus V$.

(ii) Si supponga che sia $V = \Bbbk^n$. In questo caso, sia lo spazio affine $\Bbbk^n$, che lo spazio proiettivo $\mathbb{P}(\Bbbk \oplus V)$, sono muniti di riferimenti canonici. Si confrontino le coordinate dei punti $v \in V$ e $\mathscr{A}(v) \in \mathbb{P}(\Bbbk \oplus V)$.

(iii) Sia $L = v + U$ una sottovarietà lineare dello spazio affine V. Si trovi la minima sottovarietà lineare W di $\mathbb{P}(\Bbbk \oplus V)$ che contiene $\mathscr{A}(L)$, e si mostri che se un punto $P \in \mathbb{P}(W) \setminus \mathscr{A}(L)$, allora $P \in \mathbb{P}(I)$. In particolare si mostri che se L è una retta, allora esiste un unico punto in $P \in \mathbb{P}(W) \setminus \mathscr{A}(L)$.

7.2. Problemi sulle proiettività.

7.2.1. Verificare che esiste un'unica autoproiettività φ di $\mathbb{P}(\mathbb{R})$ tale che $\varphi\binom{1}{1} = \binom{1}{-1}$, $\varphi\binom{2}{0} = \binom{1}{1}$, $\varphi\binom{1}{-1} = \binom{2}{1}$. Dare una matrice di φ rispetto al sistema di riferimento canonico.

7.2.2. Determinare le autoproiettività φ di $\mathbb{P}^2(\mathbb{R})$ che soddisfano le seguenti condizioni: $\varphi\begin{pmatrix}1\\2\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\end{pmatrix}$, $\varphi(r) = r'$, $\varphi(s) = s'$, dove $r : X_0 - X_1 = 0$, $r' : X_0 + X_1 = 0$, $s : X_0 + X_1 + X_2 = 0$, $s' : X_1 + X_2 = 0$.

7.2.3. Determinare i punti uniti ed i piani uniti delle seguenti autoproiettività di $\mathbb{P}^2(\mathbb{R})$:

$$f : \begin{pmatrix}X_0\\X_1\\X_2\end{pmatrix} \mapsto \begin{pmatrix}-X_0 + 15X_1 + 6X_2\\-2X_0 + 8X_1 + 2X_2\\4X_0 - 18X_1 - 5X_2\end{pmatrix} \quad , \quad g : \begin{pmatrix}X_0\\X_1\\X_2\end{pmatrix} \mapsto \begin{pmatrix}X_0 - X_1\\X_0 + 3X_1\\2X_2\end{pmatrix}.$$

7.2.4. Sia $f : \mathbb{P}^3(\Bbbk) \to \mathbb{P}^3(\Bbbk)$ una proiettività non identica. Si supponga che f non sia una omologia e che esista una retta r di punti uniti ($f(P) = P$ per ogni $P \in r$). È vero allora che esiste un fascio di piani uniti per f (cioè una retta s tale che per ogni piano π contenente s si ha $f(\pi) = \pi$)? Dualizzare l'enunciato.

7.2.5.

(*a*) Sia φ proiettività tra due rette r, s distinte del piano proiettivo, con $\varphi(r \wedge s) = r \wedge s$; mostrare che si tratta di una proiezione da r a s di centro un opportuno punto.

(*b*) Dualizzare l'enunciato precedente.

(*c*) Sia φ proiettività tra due piani π, σ distinti dello spazio proiettivo con $\varphi(P) = P$ per ogni $P \in \pi \wedge \sigma$. è vero che si tratta di una proiezione da π a σ di centro un opportuno punto (dimostrazione o controesempio)?

7.2.6. Determinare le possibili forme di Jordan di proiettività di $\mathbb{P}^3$ aventi una (unica) retta di punti uniti. Per tali proiettività, determinare la configurazione delle rette unite.

7.2.7. Sia φ una proiettività di $\mathbb{P}^3(\Bbbk)$ in sè con due sole rette complementari di punti uniti.

(*a*) Determinare le possibili forme di Jordan per φ, e mostrare che per ogni punto P (non unito) dello spazio la retta $P \vee \varphi(P)$ è unita.

(*b*) Per le rette r unite per φ, e per ogni coppia di punti distinti P, Q di r non uniti per φ: si determini il birapporto $(P\ \varphi(P)\ Q\ \varphi(Q))$; esistono quaterne di questo tipo armoniche?

7.2.8. Sia φ una proiettività di $\mathbb{P}^3(\Bbbk)$ in sè con due soli punti uniti.

(*a*) Determinare le possibili forme di Jordan per φ, e le configurazioni delle rette unite.

(*b*) Per le rette r unite per φ, e per ogni coppia di punti distinti P, Q di r non uniti per φ: si determini il birapporto $(P\ Q\ \varphi(P)\ \varphi(Q))$; esistono quaterne di questo tipo armoniche?

7.2.9. Sia φ una proiettività di $\mathbb{P}^3(\Bbbk)$ in sè con esattamente tre punti uniti.
(a) Determinare le possibili forme di Jordan per φ, e le configurazioni delle rette unite.
(b) Per le rette r unite per φ, e per ogni coppia di punti distinti P, Q di r non uniti per φ: si determini il birapporto $(P\ Q\ \varphi(P)\ \varphi(Q))$; esistono quaterne di questo tipo armoniche?

7.2.10. Sia φ una proiettività di $\mathbb{P}^3(\Bbbk)$ in sè avente come punti uniti esattamente quelli di una retta e un punto esterno ad essa.
(a) Determinare le possibili forme di Jordan per φ, e le configurazioni delle rette unite.
(b) Per le rette r unite per φ, e per ogni coppia di punti distinti P, Q di r non uniti per φ: si determini il birapporto $(P\ Q\ \varphi(P)\ \varphi^{-1}(Q))$; esistono quaterne di questo tipo armoniche?

7.2.11. Sia φ una proiettività di $\mathbb{P}^3(\Bbbk)$ in sè avente come punti uniti esattamente quelli di una retta.
(a) Determinare le possibili forme di Jordan per φ, e le configurazioni delle rette unite.
(b) Per le rette r unite per φ, e per ogni coppia di punti distinti P, Q di r non uniti per φ: si determini il birapporto $(P\ Q\ \varphi^{-1}(P)\ \varphi^{-1}(Q))$; esistono quaterne di questo tipo armoniche?

7.2.12. Date due rette sghembe r, s in $\mathbb{P}^3(\Bbbk)$, per ogni punto P non appartenente alle due rette, definiamo il punto P' sulla retta che interseca P, r, s e tale che il birapporto dei quattro punti R, S, P, P' sia $\lambda \in \Bbbk$ fissata costante diversa da $0, 1$ (R ed S sono i punti di intersezione con r ed s risp.).
(a) Dimostrare che la mappa che manda P in P' si estende ad una proiettività di $\mathbb{P}^3(\Bbbk)$, e determinarne le possibili forme di Jordan.
(b) Dualizzare l'enunciato. Generalizzare l'enunciato in $\mathbb{P}^n(\Bbbk)$.

7.2.13. Una proiettività φ di $\mathbb{P}^3$ in sè ha una retta r di punti uniti, e una retta unita s (non di punti uniti) incidente r, e non ha punti uniti fuori di r ed s.
(a) Trovare tutte le possibili forme di Jordan di φ.
(b) Per ciascuna di esse, discutere la configurazione delle rette unite.

7.2.14. Sia φ una proiettività di $\mathbb{P}^3(\Bbbk)$ in sè avente tre rette unite (non di punti uniti) complanari, e nessun altro punto unito fuori del piano delle tre rette.
(a) Determinare le possibili forme di Jordan per φ, e, per ciascuna, le configurazioni delle rette unite.
(b) In quali dei casi precedenti vi sono dei piani in cui φ induce una involuzione?

7.2.15. Sia $\Bbbk$ un corpo algebricamente chiuso, e sia f una proiettività non identica di $\mathbb{P}^1(\Bbbk)$ in sè. Si supponga che esista un intero N tale che $f^N = \mathrm{id}$.

È vero che se $\Bbbk$ ha caratteristica nulla allora f ha due punti uniti distinti?

È vero che se $\Bbbk$ ha caratteristica positiva p e p non divide N allora f ha due punti uniti distinti?

È vero che se $\Bbbk$ ha caratteristica positiva p allora esistono f con un solo punto unito tali che $f^p = \mathrm{id}$?

7.2.16. Sia $\Bbbk$ un corpo algebricamente chiuso di caratteristica diversa da due, e sia f una proiettività di $\mathbb{P}^1(\Bbbk)$ in sè. Si supponga che esistano due punti distinti P e Q tali che $f(P) = Q$ e $f(Q) = P$. È vero che f è necessariamente una involuzione?

7.2.17. Sia $\Bbbk$ un corpo di caratteristica diversa da due. Siano $\{a, a'\}$, $\{b, b'\}$ e $\{c, c'\}$ le tre coppie di lati opposti di un fissato quadrangolo piano completo. Sia r una retta del piano non passante per alcuno dei vertici del quadrangolo. Poniamo $A = r \wedge a$, $A' = r \wedge a'$, $B = r \wedge b$, ecc. È vero che esiste una ed una solo involuzione di r in sè che manda ordinatamente A, B, C in A', B', C'?

7.2.18. Siano $\mathbb{P}$ e $\mathbb{P}'$ due spazi proiettivi della stessa dimensione sul corpo $\Bbbk$. Siano $f, g : \mathbb{P} \longrightarrow \mathbb{P}'$ due proiettività. Siano L ed M due varietà lineari di $\mathbb{P}$, nessuna contenuta nell'altra tali che $\dim(L \wedge M) \geqslant 0$. Si supponga che $f(P) = g(P)$ per ogni $P \in L \cup M$. È vero o falso che allora $f(P) = g(P)$ per ogni $P \in L \vee M$?

Cosa cambia se $\dim(L \wedge M) < 0$? Che possibilità ci sono?

7.2.19. Sia f una proiettività di $\mathbb{P}^1(\mathbb{R})$ in sè. Dimostrare che i determinanti delle matrici associate ad f hanno tutti lo stesso segno. Che cosa si può dire di f e dei suoi punti uniti se tali determinanti sono negativi?

7.2.20. Siano f e g due omologie in uno spazio proiettivo di dimensione $n \geqslant 2$ sul corpo $\Bbbk$. Cosa si può dire delle posizioni reciproche dei centri e degli assi se risulta $f \circ g = g \circ f$?

7.2.21. Sia V uno spazio vettoriale di dimensione $2n$ sul corpo $\Bbbk$. Siano W, Z sottospazi di V della stessa dimensione, tali che $W \oplus Z = V$, sia $\varphi : W \to Z$ un isomorfismo e si ponga $\Gamma = \{w + \varphi(w) : w \in W\}$.

(i) Si mostri che Γ è un sottospazio vettoriale di V con le seguenti proprietà: $\dim \Gamma = \dim W$, $\Gamma \cap W = \Gamma \cap Z = 0$.

(ii) Si mostri che ogni sottospazio vettoriale di V con le proprietà di Γ determina un isomorfismo di W su Z.

(iii) Si supponga $n = 2$; si mostri che ogni proiettività tra due rette sghembe r ed s di $\mathbb{P}(V)$ si ottiene proiettando r su s da una opportuna retta t, sghemba sia con r che con s.

(iv) Si mostri che la retta t di cui in (iii) non è unica; ed anzi, che in generale, vi sono infinite rette che determinano la stessa proiettività.

(v) Si dica cosa vede un abitante di $\mathbb{P}^*(V)$ quando guarda 2 rette sghembe di $\mathbb{P}(V)$, e come descrive la costruzione delle proiettività tra di esse.

7.2.22. Siano I e J due iperpiani distinti e P un punto di $\mathbb{P}(V)$; si supponga che $P \notin I, J$. Si consideri la corrispondenza che ad ogni sottovarietà lineare U di I associa la sottovarietà lineare $\pi(U) = (U \vee P) \wedge J$. Le corrispondenze del tipo di $U \mapsto \pi(U)$ si dicono *prospettività* di $\mathbb{P}(I)$ in $\mathbb{P}(J)$ e P si dice il *centro* della prospettività..

(i) Si mostri che le prospettività sono proiettività, e che però esistono proiettività tra iperpiani di $\mathbb{P}(V)$ che non sono prospettività.

(ii) Che cosa accade se si fa la costruzione precedente tra 2 iperpiani di uno spazio affine?

7.3. Problemi dagli esami.

7.3.1. Dato un riferimento P_0, P_1, P_2, U di un piano proiettivo, determinare i punti Q del piano tali che le rette $Q \vee P_0, Q \vee P_1, Q \vee P_2, Q \vee U$ formano una quaterna armonica (nell'ordine dato).

7.3.2. Siano dati tre punti distinti A, B, C su una retta proiettiva, e siano X, Y, Z i quarti armonici delle terne (A, B, C), (B, C, A) e (C, A, B).

(a) Determinare i quarti armonici dopo X, Y, Z nei vari ordini possibili.

(b) Quali sono le immagini di X, Y, Z tramite la proiettività che manda ordinatamente A, B, C in X, Y, Z?

7.3.3. Siano π, σ piani distinti in $\mathbb{P}^3(\Bbbk)$ e $\varphi : \pi \to \sigma$ una proiettività. Se $\varphi(P) = P$ per ogni $P \in \pi \cap \sigma$ allora esiste un unico punto C (di $\mathbb{P}^3(\Bbbk)$) tale che φ è la proiezione (da π a σ) di centro C?
Generalizzare a due piani in $\mathbb{P}^4(\Bbbk)$ che si intersecano in un punto.
Generalizzare a due piani sghembi in $\mathbb{P}^5(\Bbbk)$.
Dualizzare.

7.3.4. Si consideri in un piano proiettivo un triangolo di vertici A, B, C (punti non allineati). Siano A'', B'', C'' tre punti rispettivamente sui lati $a = B \vee C$, $b = A \vee C$, $c = A \vee B$ (diversi dai vertici), e siano A', B', C' i quarti armonici rispettivamente dopo B, C, A'' su a, A, C, B'' su b, A, B, C'' su c.

(a) Mostrare che A'', B'', C'' sono punti allineati se e solo se $A \vee A'$, $B \vee B'$, $C \vee C'$ sono rette concorrenti.

(b) Dualizzare la costruzione e l'enunciato del punto precedente.

(c) L'enunciato del punto (a) rimane vero se invece dei quarti armonici si costruiscono i tre punti A', B', C' in modo che i birapporti (B, C, A'', A'), (A, C, B'', B'), (A, B, C'', C') siano (non banali e) uguali tra loro?

7.3.5. Si considerino in un piano proiettivo due triangoli prospettivi di vertici A, B, C e A', B', C' (lati a, b, c e a', b', c' come usuale), e sia O il punto di prospettività. Poniamo

$$\begin{array}{lcl} \overline{A} = OA \wedge BC & & \overline{A}' = OA' \wedge B'C' \\ \overline{B} = OB \wedge AC & \text{e} & \overline{B}' = OB' \wedge A'C' \\ \overline{C} = OC \wedge AB & & \overline{C}' = OC' \wedge A'B' \end{array}$$

(si tratta dei punti di intersezione dei lati dei triangoli con le rette da O).

(a) Mostrare che

$$(\overline{A}\ B\ C\ a \wedge a') = (\overline{A}'\ B'\ C'\ a \wedge a')$$

e analogamente per gli altri lati (scrivere le uguaglianze).

(b) Mostrare che la retta di omologia (passante per $a \wedge a'$, $b \wedge b'$, $c \wedge c'$) passa per il punto di prospettività O se e solo se

$$(\overline{A}\ B\ C\ a \wedge a') = (A\ \overline{B}\ C\ b \wedge b') = (A\ B\ \overline{C}\ c \wedge c')$$

(basta una delle uguaglianze?).

(c) Nel caso precedente, trovare condizioni necessarie e sufficienti affinché i quattro punti sulla retta di omologia formino una quaterna armonica (in qualche ordine).

7.3.6. Siano dati due triangoli A, B, C e A', B', C' del piano proiettivo.

(a) Determinare tutte le proiettività che mandano ordinatamente il primo triangolo nel secondo.

(b) In quali casi tra le proiettività precedenti vi sono omologie (speciali e/o generali)?

(c) In quali casi tra le proiettività precedenti vi sono involuzioni?

Nota post-compito sulla soluzione: nel primo punto era importante accorgersi che le proiettività in questione non erano uniche, ma dipendevano da due parametri.

Il secondo punto ha chiaramente a che fare con il teorema di Desargues sui triangoli prospettivi/omologici.

Il terzo punto si può scrivere bene in termini di birapporti.

Naturalmente le migliori risposte dovevano essere scritte in termini "geometrici", cioè in termini dei triangoli di partenza e delle loro relazioni.

7.3.7. Si considerino in un piano proiettivo tre triangoli prospettivi Δ_i, di vertici A_i, B_i, C_i, per $i = 1, 2, 3$ (lati a_i, b_i, c_i come usuale) con punto di prospettività comune O. Siano r_{ij} le rette di omologia di Δ_i e Δ_j (per $i \neq j$).

(a) Mostrare che le rette r_{12} ed r_{13} coincidono se e solo se

$$(O\ A_1\ A_2\ A_3) = (O\ B_1\ B_2\ B_3) = (O\ C_1\ C_2\ C_3)$$

e in tal caso coincidono con la retta r_{23}.

(b) In generale, mostare che le tre rette r_{ij} appartengono ad un fascio. Che cosa si può dire, di più, se vale solo una delle uguaglianze del punto precedente?

(c) Dualizzare la costruzione e gli enunciati precedenti.

Ci si aspettava una soluzione con conti espliciti, usando un riferimento con i punti fondamentali nel primo triangolo e il punto unità nel punto di prospettività; qualche ragionamento per permutazioni permetteva di evitare i conti più pesanti (comunque non impossibili).

Suggerimenti per una soluzione senza conti: per il primo punto, usare il teorema di Pappo (ultima parte) per mostrare che i lati a_1, a_2, a_3 sono concorrenti in un punto (idem per i b_i e i c_i, e la retta per quei tre punti passa per O); per il secondo punto conviene considerare i tre triangoli di lati a_i, b_i e c_i che sono per costruzione omologici, quindi prospettivi per Desargues, e le rette che uniscono vertici corrispondenti sono esattamente le tre rette di omologia dei triangoli di partenza. Una uguaglianza del primo punto fa degenerare uno dei triangoli, che diventa il punto di intersezione delle tre rette.

7.3.8. Siano dati due triangoli prospettivi Δ, Δ' (di vertici A_1, A_2, A_3 e A'_1, A'_2, A'_3) in un piano proiettivo (sul campo $\mathbb{C}$), sia O il loro punto di prospettività.

(a) Sia Δ'' il triangolo (di vertici A''_1, A''_2, A''_3) tale che $(O\ \Delta\ \Delta'\ \Delta'') = -1$ (cioè $(O\ A_i\ A'_i\ A''_i) = -1$ per $i = 1, 2, 3$). Qual è la relazione tra le tre rette di omologia delle tre coppie di triangoli?

(b) Viceversa, dati tre triangoli prospettivi dallo stesso punto, cosa si può dire dei tre triangoli se le tre rette di omologia coincidono?

(c) Dualizzare la costruzione e i due punti precedenti.

7.3.9. Si considerino in un piano proiettivo due triangoli prospettivi Δ, Δ', di vertici A, B, C e $A'B'C'$ (lati a, b, c e a', b', c' come usuale) con punto di prospettività O e retta di omologia r.

(a) Variando la scelta dei sei punti per formare due triangoli, mostrare che vi sono quattro coppie di triangoli prospettivi dal punto O, e determinare le quattro rette di omologia corrispondenti e le loro relazioni reciproche.

(b) Dualizzare il punto precedente: variando la scelta dei sei lati, mostrare che vi sono quattro coppie di triangoli omologici dalla retta r, e determinare le relazioni reciproche dei quattro punti di prospettività corrispondenti.

(c) Poniamo $A'' = (O \vee A) \wedge r$, $B'' = (O \vee B) \wedge r$, $C'' = (O \vee C) \wedge r$. Verificare che
$$(O\ A\ A'\ A'') = (O\ B\ B'\ B'') = (O\ C\ C'\ C'')\ .$$
Mostrare che le quattro rette del punto (a) coincidono se e solo se i quattro punti del punto (b) coincidono se e solo e le quaterne precedenti di punti sono armoniche in qualche ordine (quale?).

Le quattro coppie di triangoli sono $(ABC, A'B'C')$, $(ABC', A'B'C)$, $(AB'C, A'BC')$, $(A'BC, AB'C')$. *Le quattro rette di omologia sono o in posizione generale o coincidenti. Per il terzo punto: le quaterne sono proiettate una sull'altra da opportuni fasci di rette; la coincidenza delle rette di omologia capita quando* O *ed* r *separano armonicamente le coppie* A, A', B, B' *e* C, C' *(farsi un disegno con* O *punto all'infinito).*

Nota: la condizione del punto (c) *si presenta se e solo se i sei punti vertici dei due triangoli stanno su una conica.*

7.3.10. Si considerino in un piano proiettivo due rette distinte r, s, sia O il punto di intersezione. e tre punti distinti e diversi da O su ciascuna, siano $R_1, R_2, R_3 \in r$ e $S_1, S_2, S_3 \in s$.

(a) Applicando il teorema di Pappo alle 6 coppie (di terne ordinate) $R_1, R_2, R_3 \in r$ e $S_{\pi(1)}, S_{\pi(2)}, S_{\pi(3)} \in s$, per π nel gruppo delle permutazioni di $\{1, 2, 3\}$, si ottengono in generale 6 rette di collineazione; mostrare che in generale le sei rette appartengono a due fasci; siano H e K i punti centri dei fasci. *[sugg.: se* π *è un ciclo d'ordine* 3*, allora* $\pi, \pi^2, \pi^3 (= \mathrm{id})$ *danno tre rette d'un fascio.]*

(b) Determinare sotto quali condizioni, in termini dei due birapporti (O, R_1, R_2, R_3) e (O, S_1, S_2, S_3), le rette di uno dei fasci coincidono tra loro.

(c) Mostrare che se $(O, R_1, R_2, R_3) = (O, S_1, S_2, S_3)$ allora le tre rette di uno dei due fasci (quale?) formano con $H \vee K$ una quaterna armonica; vale il viceversa? In quali casi in entrambi i fasci le tre rette formano una quaterna armonica con $H \vee K$?

Risultati (variazioni sul teorema di Pappo). Il primo punto si può fare sia in modo astratto, sia tramite conti in coordinate, che poi aiutano a risolvere i successivi punti.

Astratto: consideriamo il 3*-ciclo* $(1, 2, 3)$ *e le sue potenze; siccome le rette di collineazione sono determinate dai tre punti* $R_1S_{\pi 2} \wedge R_2S_{\pi 1}$, $R_1S_{\pi 3} \wedge R_3S_{\pi 1}$, $R_2S_{\pi 3} \wedge R_3S_{\pi 2}$, *abbiamo che le tre rette associate sono determinate dai tre punti delle righe di*
$$\begin{array}{lll} R_1S_2 \wedge R_2S_1 & R_1S_3 \wedge R_3S_1 & R_2S_3 \wedge R_3S_2 \\ R_1S_3 \wedge R_2S_2 & R_1S_1 \wedge R_3S_2 & R_2S_1 \wedge R_3S_3 \\ R_1S_1 \wedge R_2S_3 & R_1S_2 \wedge R_3S_3 & R_2S_2 \wedge R_3S_1 \end{array}$$
e prendendo due triangoli scegliendo i vertici uno da ciascuna riga, verifichiamo subito che sono omologici (usando il teorema di Pappo, si tratta dei tre punti della retta di collineazione di una delle altre permutazioni!), e di conseguenza prospettivi, il che dimostra che le tre rette di collineazione sono concorrenti. Per le altre tre rette segue applicando uno scambio di indici.

In coordinate: usiamo
$O = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $R_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $S_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, $R_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, $S_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $R_3 = \begin{pmatrix} 1 \\ x \\ 0 \end{pmatrix}$, $S_3 = \begin{pmatrix} 1 \\ 0 \\ y \end{pmatrix}$.

Qualche facile conto dà che le rette di collineazione per $\mathrm{id}, (123), (132)$ *sono*
$\begin{pmatrix} y-x \\ 1-y \\ x-1 \end{pmatrix}$, $\begin{pmatrix} y-1-xy \\ 1 \\ x \end{pmatrix}$, $\begin{pmatrix} x-1-xy \\ y \\ 1 \end{pmatrix}$, *visibilmente concorrenti, e* $H = \begin{pmatrix} 1-xy \\ (1-y)(x^2-x+1) \\ (1-x)(y^2-y+1) \end{pmatrix}$.

Per le altre tre permutazioni $(12), (1, 3), (2, 3)$ *otteniamo le tre rette*
$\begin{pmatrix} xy-x-y \\ 1 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1-x-y \\ y \\ x \end{pmatrix}$, $\begin{pmatrix} 1-xy \\ y-1 \\ x-1 \end{pmatrix}$, *visibilmente concorrenti, e* $K = \begin{pmatrix} y-x \\ (y-1)(x^2-x+1) \\ (1-x)(y^2-y+1) \end{pmatrix}$.

Siccome $x = (O, R_1, R_2, R_3)$ *e* $y = (O, S_1, S_2, S_3)$*, le tre rette per* H *coincidono tra loro sse i due birapporti sono uno inverso dell'altro ed equianarmonici (cioè equianarmonici discordi), e le tre rette per* H *coincidono tra loro sse i due birapporti sono uguali ed equianarmonici (cioè equianarmonici concordi).*

Calcolando il birapporto delle rette per H *nel caso* $x = y$ *si trova sempre* $1/2$*, quindi la quaterna è armonica, e viceversa. Perché anche l'altro birapporto (rette per* K*) sia armonico si deve avere anche la condizione* $(O, R_1, R_2, R_3) = (O, S_1, S_3, S_2)$*, quindi* $xy = 1$ *(e* $x = y$*), da cui segue* $x = y = -1$*, cioè servono quaterne armoniche in partenza, nel qual caso i punti* H *e* K *sono sulla retta per* R_1 *ed* S_1 *e ne sono separatori armonici.*

7.3.11. Dato un triangolo di vertici A, B, C (lati a, b, c) in un piano proiettivo, e dati $A', A'' \in a$, $B', B'' \in b$, $C', C'' \in c$ (generici, cioè distinti tra di loro e dai vertici), mostrare che: esiste una

proiettività del piano cha manda ordinatamente A, B, C, A', B', C' in A, B, C, A'', B'', C'' se solo se risulta $(A\ B\ C'\ C'')(B\ C\ A'\ A'')(C\ A\ B'\ B'') = 1$.

Dedurre dalla proprietà precedente che: se A'', B'', C'' sono allineati, allora A', B', C' sono allineati se e solo se $(A\ B\ C'\ C'')(B\ C\ A'\ A'')(C\ A\ B'\ B'') = 1$. Dedurre da questo il teorema di Menelao affine.

Dualizzare gli enunciati precedenti.

7.3.12. In uno spazio proiettivo di dimensione 3 sono dati tre triangoli non complanari e prospettivi dallo stesso punto. Mostrare che le tre rette di omologia (delle tre coppie di triangoli prospettivi) sono sempre concorrenti in un punto, e caratterizzare i casi in cui coincidono (sugg.: considerare i birapporti sulle tre rette di prospettività).

7.3.13. In uno spazio proiettivo (di dimensione 3) sono date tre rette non complanari e concorrenti in un punto O, e su ciascuna retta tre punti distinti e distinti da O. Applicando il teorema di Pappo alle tre coppie di rette si ottengono tre rette di collineazione (su tre piani diversi). Discutere le posizioni reciproche di queste rette, in particolare caratterizzare i casi un cui sono in un fascio, o in cui due si intersecano (risposta in termini di birapporti dei punti sulle rette date).

7.3.14. In uno piano proiettivo sono date due rette a, b concorrenti in un punto $O = a \wedge b$, e su ciascuna retta tre punti distinti $A_0, A_1, A_2 \in a$, $B_0, B_1, B_2 \in b$ e distinti da O. Applicando il teorema di Pappo si ottiene la retta di collineazione c contenente i tre punti $C_0 = (A_1 \vee B_2) \wedge (A_2 \vee B_1)$, $C_1 = (A_0 \vee B_2) \wedge (A_2 \vee B_0)$, $C_2 = (A_0 \vee B_1) \wedge (A_1 \vee B_0)$. Siano infine $O_a = c \wedge a$, $O_b = c \wedge b$. Determinare la retta di collineazione per i punti $A_0, A_1, A_2 \in a$ e $C_0, C_1, C_2 \in c$ e per i punti $B_0, B_1, B_2 \in b$ e $C_0, C_1, C_2 \in c$. Discutere le relazioni tra i birapporti delle quaterne di punti in cui il primo punto è uno tra O, O_a, O_b e i successivi tre una terna tra $A_0, A_1, A_2 \in a$, $B_0, B_1, B_2 \in b$, $C_0, C_1, C_2 \in c$ (quando hanno senso?).

7.3.15. In un piano proiettivo sono date due rette a, b, sia $O = a \wedge b$, e un punto esterno C. Per ogni coppia $A_0, A_1 \in a$ di punti in a distinti e diversi da O, siano $B_0, B_1 \in b$ i punti di b che si ottengono proiettando da C (cioè $B_i = b \wedge (C \vee A_i)$). Mostrare che tutti i punti $(A_0 \vee B_1) \wedge (A_1 \vee B_0)$ sono allineati su una retta c passante per O.

Mostrare che la retta c è quarta armonica dopo a, b e $O \vee C$ (nel fascio di centro O).

7.3.16. Sono dati due triangoli di vertici A, B, C e A', B', C' in un piano proiettivo, prospettivi dallo stesso punto O, senza vertici né lati comuni. Sia r la retta di omologia e siano $\tilde{A}, \tilde{B}, \tilde{C}$ le intersezioni di r con i raggi OA, OB, OC rispettivamente. Su ogni raggio OA, OB, OC siano A_1, B_1, C_1 le intersezioni con i lati a, b, c rispettivamente, e siano A'_1, B'_1, C'_1 le intersezioni con i lati a', b', c' rispettivamente. Scelto un opportuno sistema di riferimento proiettivo:

(1) Determinare i birapporti $(O\ X\ X'\ \tilde{X})$ per $X \in \{A, B, C\}$, e giustificare perché risultano uguali;
(2) Determinare i birapporti $(O\ X\ X'\ X_1)$ e $(O\ X'\ X\ X'_1)$ per $X \in \{A, B, C\}$, e determinare in quali casi non sono tutti distinti;
(3) Trovare condizioni necessarie e sufficienti in termini dei birapporti del punto (2) affinché i birapporti del punto (1) risultino armonici,
(4) Dualizzare gli enunciati precedenti.

7.3.17. In uno spazio proiettivo di dimensione 3 sono date tre rette r_0, r_1, r_2 due a due sghembe, e tre rette trasversali comuni s_0, s_1, s_2 distinte. Siano $A_{ij} = r_i \wedge s_j$, per $i, j = 0, 1, 2$ i nove punti di intersezione.

Per punti $R_i \in r_i$, per $i = 0, 1, 2$: mostrare che essi sono allineati se e solo se i tre birapporti $(A_{i0}\ A_{i1}\ A_{i2}\ R_i)$ coincidono per $i = 0, 1, 2$.

Definiamo $\mathcal{S}$ l'insieme delle rette trasversali comuni a r_0, r_1, r_2. Mostrare che le rette di $\mathcal{S}$ sono del tipo $R_0 \vee R_1$ dove $R_0 \in r_0$, $R_1 \in r_1$ sono tali che $(A_{00}\ A_{01}\ A_{02}\ R_0) = (A_{10}\ A_{11}\ A_{12}\ R_1)$.

Definiamo $\mathcal{R}$ l'insieme delle rette trasversali comuni a s_0, s_1, s_2. Mostrare che ogni retta di $\mathcal{S}$ interseca ogni retta di $\mathcal{R}$ ma che due rette in $\mathcal{S}$ (o in $\mathcal{R}$) sono sempre sghembe.

7.3.18. In un piano proiettivo sono dati tre punti P_0, P_1, P_2 in posizione generale, siano r_i le rette generate dai punti P_j con $j \neq i$, e un punto O non appartenente alle rette r_i. Definiamo P'_i per $i = 0, 1, 2$ i punti di intersezione di $O \vee P_i$ con r_i; siano r'_i le rette generate dai punti P'_j con $j \neq i$.

Per punti $Q_i \in O \vee P_i$, per $i = 0, 1, 2$: mostrare che essi sono allineati se e solo se i tre birapporti $(O\ P_i\ P'_i\ Q_i)$ hanno somma 1.

Mostrare che i punti dati dalle intersezioni $r_i \wedge r'_i$ per $i = 0, 1, 2$ sono allineati, e siano S_i i punti di intersezione di tale retta con le rette $O \vee P_i$; determinare i birapporti $(O\ P_i\ P'_i\ S_i)$.

Dualizzare costruzione e risultati precedenti.

7.3.19. In uno spazio proiettivo di dimensione 3 sono dati quattro punti P_0, P_1, P_2, P_3 in posizione generale, siano π_i i piani generati dai punti P_j con $j \neq i$, e un punto O non appartenente ai piani π_i. Definiamo P'_i per $i = 0, 1, 2, 3$ i punti di intersezione di $O \vee P_i$ con π_i, e π'_i i piani generati dai punti P'_j con $j \neq i$.

Per punti $Q_i \in O \vee P_i$, per $i = 0, 1, 2, 3$: mostrare che essi sono complanari se e solo se i quattro birapporti $(O\ P_i\ P'_i\ Q_i)$ hanno somma 1.

Mostrare che le rette date dalle intersezioni $\pi_i \wedge \pi'_i$ per $i = 0, 1, 2, 3$ sono complanari, e siano S_i i punti di intersezione di tale piano con le rette $O \vee P_i$; determinare i birapporti $(O\ P_i\ P'_i\ S_i)$.

Dualizzare costruzione e risultati precedenti.

7.3.20. In uno spazio proiettivo di dimensione 3 sono dati quattro punti P_0, P_1, P_2, P_3 in posizione generale, siano π_i i piani generati dai punti P_j con $j \neq i$, e un punto O non appartenente ai piani π_i. Siano P'_i per $i = 0, 1, 2, 3$ punti sulle rette $O \vee P_i$ distinti da quelli già dati e π'_i i piani generati dai punti P'_j con $j \neq i$.

Mostrare che le rette date dalle intersezioni $\pi_i \wedge \pi'_i$ per $i = 0, 1, 2, 3$ sono complanari, sia σ tale piano.

Siano S_i i punti di intersezione del piano σ con le rette $O \vee P_i$; mostrare che i birapporti $(O\ P_i\ P'_i\ S_i)$ sono tutti uguali per $i = 0, 1, 2, 3$.

Dualizzare costruzione e risultati precedenti.

7.3.21. In uno spazio proiettivo di dimensione 3 è dato un riferimento P_0, P_1, P_2, P_3, U, e (per ogni $i = 0, 1, 2, 3$) sia P'_i il punto dato dalla intersezione della retta $U \vee P_i$ con il piano generato dai P_j per $j \neq i$.

Mostrare che anche i punti $P'_0, P'_1, P'_2, P'_3, U$ formano un riferimento.

Dati quattro punti $Q_i \in U \vee P_i$, per $i = 0, 1, 2, 3$: mostrare che essi sono complanari se e solo se i birapporti $(U\ P_i\ P'_i\ Q_i)$ hanno somma 1.

Determinare i punti $R_i \in U \vee P_i$, per $i = 0, 1, 2, 3$, che siano complanari e tali che i birapporti $(U\ P_i\ P'_i\ R_i)$ siano uguali tra loro.

Dualizzare costruzione e risultati precedenti.

7.3.22. Sono date due rette r, s in un piano proiettivo, e su ciascuna tre punti distinti $R_0, R_1, R_2 \in r$, $S_0, S_1, S_2 \in s$ e distinti dall'intersezione $O = r \wedge s$. Applicando il teorema di Pappo si ottiene la retta di collineazione u passante per i tre punti $U_i = (R_j \vee S_k) \wedge (R_k \vee S_j)$ per $\{i, j, k\} = \{1, 2, 3\}$. Poniamo $T_i = u \wedge (R_i \vee S_i)$,

(1) Supponiamo che $O \in u$; allora le tre rette $R_i \vee S_i$ concorrono in un punto A, e mostrare che le quattro rette $r, s, u, O \vee A$ formano una quaterna armonica.
(2) Sotto l'ipotesi del punto precedente, trovare condizioni necessarie e sufficienti affinché la retta $R_0 \vee S_0$ sia la retta di collineazione per le terne di punti R_1, T_1, S_1 e R_2, T_2, S_2. *[sugg.: i birapporti sulle rette sono uguali ed armonici] [sugg.: considerare i birapporti* $(O\, R_0\, R_1\, R_2)$ *e* $(O\, S_0\, S_1\, S_2)$*]*
(3) Supponiamo che $O \notin u$; determinare sotto quali condizioni la retta $R_0 \vee S_0$ sia la retta di collineazione per le terne di punti R_1, T_1, S_1 e R_2, T_2, S_2. *[sugg.: i birapporti sulle rette sono diversi ed equianarmonici] [sugg.: come sopra, considerare i birapporti dei punti dati sulle rette* r, s*]*
(4) Sotto le condizioni del punto precedente, mostrare che il triangolo di vertici O, R, S e il triangolo di lati $R_i \vee S_i$ sono prospettivi (da quanti e quali punti?).

7.3.23. Sono date tre rette r, s, t due a due sghembe in uno spazio proiettivo di dimensione 3. Presi quattro punti distinti T_0, T_1, T_2, T_3 di t, siano u_0, u_1, u_2, u_3 le rette per quei punti e incidenti sia r sia s, e siano $R_0, R_1, R_2, R_3 \in r$ e $S_0, S_1, S_2, S_3 \in s$ i punti di incidenza.

(1) mostrare che le quattro trasversali u_i sono due a due sghembe, e che i birapporti $(T_0\, T_1\, T_2\, T_3)$, $(R_0\, R_1\, R_2\, R_3)$, $(S_0\, S_1\, S_2\, S_3)$ sono uguali.
(2) Determinare quali piani intersecano le quattro rette u_0, u_1, u_2, u_3 in punti allineati, e mostrare che il birapporto di tali punti è sempre lo stesso;
(3) Dualizzare tutti gli enunciati trovati.

7.3.24. In un piano proiettivo su $\mathbb{C}$ sono dati due triangoli di vertici A, B, C e A', B', C' prospettivi dal punto O. Siano A'', B'', C'' le intersezioni dei raggi OA, OB, OC con i lati BC, AC, AB rispettivamente.

Trovare condizioni necessarie e sufficienti in termini dei birapporti dei punti dati sulle tre rette OA, OB, OC affinché il triangolo A, B, C sia prospettivo anche con i triangoli ottenuti da A', B', C' scambiando due vertici. Come sono disposti i tre nuovi centri di prospettività?

Trovare condizioni necessarie e sufficienti in termini dei birapporti dei punti dati sulle tre rette OA, OB, OC affinché il triangolo A, B, C sia prospettivo anche con i triangoli ottenuti da A', B', C' applicando tutte le permutazioni possibili. In questo caso mostrare che vi sono sei centri di prospettività, i quali formano due triangoli che sono a loro volta prospettivi da sei diversi punti.

7.3.25. Sono date due rette r, s in un piano proiettivo, e su ciascuna tre punti distinti $R_0, R_1, R_2 \in r$, $S_0, S_1, S_2 \in s$ e distinti dall'intersezione $O = r \wedge s$.

Usando i sei punti iniziali, si possono formare coppie di triangoli non degeneri del tipo R_i, S_j, S_k e S_i, R_j, R_k per $\{i, j, k\} = \{0, 1, 2\}$ (un vertice su una retta, gli altri due sull'altra); trovare condizioni necessarie e sufficienti in termini dei birapporti sulle due rette affinché qualche coppia di tali triangoli (variando anche la corrispondenza dei vertici) sia prospettiva.

Determinare nei casi precedenti le rette di omologia delle coppie di triangoli omologici trovati. Dualizzare tutti gli enunciati.

7.3.26. In un piano proiettivo è dato un triangolo di vertici A_0, B_0, C_0 (lati a_0, b_0, c_0) e un punto O non appartenente ai lati del triangolo.

Siano $A_1 = a_0 \wedge OA_0$, $B_1 = b_0 \wedge OB_0$, $C_1 = c_0 \wedge OC_0$ (e indichiamo con a_1, b_1, c_1 i lati di questo triangolo). Mostrare che i due triangoli sono prospettivi da O, e che la loro retta di omologia h_0 (passante per $P = a_0 \wedge a_1, Q = b_0 \wedge b_1, R = c_0 \wedge c_1$) non contiene O.

Siano A'_0, B'_0, C'_0 le intersezioni di h_0 con i tre raggi OA_0, OB_0, OC_0 rispettivamente. Mostrare che i birapporti $(O\ A_0\ A_1\ A'_0)$, $(O\ B_0\ B_1\ B'_0)$, $(O\ C_0\ C_1\ C'_0)$ sono uguali e determinarne il valore.

Mostrare che la quaterna Q, B_1, A_0, C_0 è armonica. Trovare tutte le quaterne armoniche con i punti dati.

Dualizzare costruzione e risultati precedenti.

Continuare il procedimento definendo i trinagoli A_i, B_i, C_i per $i \in \mathbb{N}$ e determinare il limite per $i \to \infty$. Idem per $i \in -\mathbb{N}$.

7.3.27. In un piano proiettivo sono dati due triangoli di vertici A_0, B_0, C_0 (lati a_0, b_0, c_0) e A_1, B_1, C_1 (lati a_1, b_1, c_1) prospettivi da un punto O.

Siano A, B, C rispettivamente i quarti armonici sulle tre rette OA_0, OB_0, OC_0 dopo i punti O, A_0, A_1 ecc. Mostrare che A, B, C sono allineati se e solo se per essi passa la retta di omologia dei due triangoli prospettivi dati.

Determinare una condizione necessaria e sufficiente in termini dei punti iniziali (suggerimento: usare dei birapporti...) per cui si verifica la situazione del punto precedente.

Se i punti A, B, C non sono allineati, essi formano un triangolo prospettivo ai due iniziali; determinare la relazione tra le tre rette di omologia per le coppie di triangoli.

Appendice A

Esercizi per sviluppare l'Immaginazione.

1. Il nuovo appartamento (F. Baldassarri). Un Tizio compra un nuovo appartamento, sottinsieme dello spazio euclideo reale 4-dimensionale, della forma:

$$A = \left\{ x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in \mathbb{E}^4(\mathbb{R}) \text{ tali che } x_i \in [0,1] \text{ per ogni } i \text{ e } x_i \in \{0,1\} \text{ per almeno un } i \right\}$$

(si tratta della "buccia tridimensionale" dell'ipercubo unitario $[0,1]^4$ di $\mathbb{E}^4(\mathbb{R})$).

Diciamo che una stanza sia un insieme in biiezione con $[0,1]^3$, e una parete sia un insieme in biiezione con $[0,1]^2$.

1.1. Quante stanze vi sono nell'appartamento A? Per ciascuna stanza trovare una biiezione con $[0,1]^3$ che rispetti le strutture metriche (distanze ed angoli).

1.2. Se ogni parete (compresi soffitti e pavimenti) di ogni stanza dell'appartamento ha una porta, quante porte ci sono? Quante porte di ingresso?

1.3. Tizio vuole dipingere le stanze, in modo che stanze adiacenti abbiano colori diversi, usando il minimo numero possibile di colori. Quanti ne occorrono?

1.4. Fare un disegno dell'appartamento in cui si possano controllare i risultati precedenti.

Una possibile immagine è la seguente:

(questo è un modo di disegnare l'ipercubo su un foglio che generalizza il modo di disegnare un cubo: cioè disegnare un quadrato, un suo traslato e poi unire i vertici corrispondenti con altrettanti segmenti; qui siamo partiti da un cubo...)

Qualcuno preferisce vedere l'ipercubo in questo modo:

(il cubetto centrale e il cubone totale sono due stanza opposte e disgiunte dell'ipercubo).

Suggerimenti e sviluppi.

1.5. Può essere utile pensare all'esercizio che un matematico bidimensionale darebbe ai propri studenti circa la buccia bidimensionale del cubo tridimensionale (per loro una "stanza" è un quadrato e una "parete" è un segmento).

1.6. La buccia tridimensionale dell'ipercubo in dimensione 5 è una villa.

2. La divisione dell'appartamento. Tizio decide di dividere l'appartamento in due unità, e sta considerando le seguenti possibilità:

(1) $A = A_0 \cup A_1$ ove

$$A_0 = \{x \in A \text{ tali che } x_i = 0 \text{ per almeno un } i\}$$
$$A_1 = \{x \in A \text{ tali che } x_i = 1 \text{ per almeno un } i\}$$

(2) $A = B \cup C$ ove

$$B = \{x \in A \text{ tali che } x_i \in \{0,1\} \text{ per almeno un } i \in \{1,2\}\}$$
$$C = \{x \in A \text{ tali che } x_i \in \{0,1\} \text{ per almeno un } i \in \{3,4\}\}$$

2.1. È vero che in entrambi i casi l'appartamento è diviso in parti uguali e senza sovrapposizioni? Per entrambe le possibilità, fare un disegno delle due parti.

2.2. Quale divisione bisognerà scegliere per minimizzare il numero di porte di comunicazione tra le due parti?

2.3. Quale divisione bisognerà scegliere affinché in entrambe le parti siano presenti stanze di tutti i colori possibili (avendo colorato le stanze come nell'esercizio precedente)?

3. Parallelepipedi e tetraedri. Dati m vettori linearmente indipendenti in $\mathbb{R}^n$ (quindi $n \geqslant m$)), ricordiamo che:

(1) il parallelepipoide m-dimensionale o m-parallelepipoide (parallelogramma se $m = 2$, parallelepipedo se $m = 3$) da essi generato è l'insieme delle loro combinazioni lineari con coefficienti compresi tra 0 e 1;

(2) il simplesso m-dimensionale o $(m+1)$-simplesso o $(m+1)$-edro (triangolo se $m = 2$, tetraedro se $m = 3$) da essi generato è l'insieme delle loro combinazioni lineari con coefficienti compresi tra 0 e 1 sottoposti alla condizione che la somma sia minore o uguale a 1;

(2′) per alcuni aspetti è meglio identificare il simplesso $(m-1)$-dimensionale o m-simplesso o m-edro come l'insieme delle loro combinazioni lineari con coefficienti compresi tra 0 e 1 sottoposti alla condizione che la somma sia uguale a 1 (verificare che le definizioni sono equivalenti?).

Di solito i simplessi m-dimensionali sono descritti meglio in geometria affine dicendo che si tratta dell'inviluppo convesso di $m+1$ punti (donde $(m+1)$-simplesso o $(m+1)$-edro), e nella descrizione vettoriale uno dei punti è l'origine (gli altri essendo gli estremi dei vettori).

3.1. Ogni m-parallelepipoide ha come facce (bloccando a 0 o 1 qualcuno dei combinatori) dei parallelepipoidi di dimensione inferiore: per ogni dimensione, contare quante facce ci sono e cercare di capire la combinatorica della geometria: per esempio, quante facce di dimensione r sono comuni a facce di dimensione $r+1$? Farsi dei disegni da cui si possa dedurre il conteggio.

3.2. Ogni simplesso m-dimensionale ha come facce (bloccando a 0 qualcuno dei combinatori, oppure con la somma esattamente 1, usando la prima descrizione) dei simplessi di dimensione inferiore: per ogni dimensione, contare quante facce ci sono e cercare di capire la combinatorica della geometria: per esempio, quante facce di dimensione r sono comuni a facce di dimensione $r+1$? Farsi dei disegni da cui si possa dedurre il conteggio.

4. Volumi di m-parallelepipoidi e $(m+1)$-edri. Si sa che il volume m-dimensionale di un m-parallelepipoide è $m!$ (m fattoriale) volte quello dell'$(m+1)$-edro (simplesso m-dimensionale) generato dagli stessi vettori. Come si giustifica "intuitivamente" questo fatto?

4.1. per $m = 2$ possiamo dividere il parallelogramma in due triangoli congruenti, ed in effetti sovrapponibili.

4.2. per $m = 3$ possiamo dividere il parallelepipedo in sei tetraedri congruenti tra loro, ma non necessariamente sovrapponibili. Fare un disegno della situazione e costruirsi un modellino di parallelepipedo (di polistirolo o gommapiuma) così sezionato.

4.3. per $m = 4$ possiamo dividere il parallelepipoide in 24 simplessi 4-dimensionali (pentaedri) congruenti tra loro, ma non necessariamente sovrapponibili. Fare un disegno della situazione.

4.4. in base agli esempi precedenti proporre un metodo ricorsivo per dividere un m-parallelepipoide in $m!$ $(m+1)$-edri (simplessi m-dimensionali) tra loro congruenti.

Per procedere in modo induttivo conviene osservare che un $(m+1)$-edro S_m (simplesso m-dimensionale) ha esattamente $m+1$ facce che sono m-edri (simplessi $(m-1)$-dimensionali); quando

si considera un $(m+1)$-parallelepipoide visto come prodotto $P_m \times I$, questo contiene $m!$ oggetti del tipo $S_m \times I$ (dove I è intervallo reale $[0,1]$ per esempio), il quale ha quindi $m+1$ componenti del tipo $S_{m-1} \times I$. Quindi per dividere queste componenti in simplessi m-dimensionali, bisogna ottenere $m+1$ simplessi $(m+1)$-dimensionali. Quindi in totale in P_{m+1} avremo $(m+1) \cdot m!$ simplessi $(m+1)$-dimensionali.

Per esempio conviene osservare i primi passi: il parallelogramma P_2 si divide in due triangoli S_2 (ciascuno dei quali con tre lati!); Il parallelepipedo 3-dimensionale P_3 è quindi formato da due solidi $S_2 \times I$, le cui facce 2-dimensionali laterali sono 3, e quindi ciascuno si divide in 3 simplessi 3-dimensionali S_3; in totale P_3 contiene 6 simplessi S_3.

Quindi un 4-parallelepipoide P_4 contiene 6 solidi 4-dimensionali del tipo $S_3 \times I$, ciascuno dei quali ha 4 facce del tipo $S_2 \times I$, e quindi si divide in 4 simplessi 4-dimensionali S_4.

5. Nidi di vespe. Le vespe di una certa specie costruiscono un nido della forma

$$\{x \in \mathbb{R}^3 | \|x\| \leqslant 1\}$$

(una sfera unitaria) diviso in un certo numero di celle dai piani coordinati di $\mathbb{R}^3$.

5.1. Quante celle vi sono? Quante pareti? Quante pareti ha ogni cella? Quante interne e quante esterne?

5.2. Con quante altre celle comunica ogni cella? Ogni parete è in comune a quante celle?

5.3. Quanti colori bisogna usare per colorare le celle in modo che ogni cella abbia un colore diverso da tutte quelle adiacenti?

Ora una vespa progetta un iper-nido della forma seguente:

$$\{x \in \mathbb{R}^4 | \|x\| \leqslant 1 \text{ ed esiste un indice } i \text{ con } x_i = 0 \}$$

(intersezione della palla unitaria di $\mathbb{R}^4$ con gli iperpiani coordinati), e si chiede:

5.4. quanti nidi del tipo precedente vi sono nell'iper-nido?

5.5. quante celle vi sono? quante pareti? quante pareti ha ogni cella? Quante interne e quante esterne?

5.6. con quante altre celle comunica ogni cella? ogni parete è in comune a quante celle?

5.7. quanti colori bisogna usare per colorare le celle in modo che ogni cella abbia un colore diverso da tutte quelle adiacenti?

5.8. vero che ogni cella ha la sua uscita verso l'esterno?

Esaminare analogamente il caso:

$$\{x \in \mathbb{R}^5 | \|x\| \leqslant 1 \text{ ed esistono due indici } i \neq j \text{ con } x_i = x_j = 0 \} .$$

Provare a fare dei disegni dei progetti.

Anche qui può essere utile pensare all'esercizio di un matematico bidimensionale.

Che relazioni ci sono con l'esercizio dell'ipercubo?

6. Conteggi di dimensioni e parametri.

6.1. Per determinare un punto in uno spazio affine di dimensione n servono esattamente n coordinate, quindi n parametri indipendenti.

6.2. Per determinare l'insieme degli iperpiani in uno spazio affine di dimensione n possiamo cercare di contare le equazioni lineari (non omogenee, quindi con $n+1$ coefficienti), ma dobbiamo tener conto che equazioni proporzionali danno luogo allo stesso iperpiano, quindi considerare questo insieme di $(n+1)$-uple a meno di moltiplicazione per scalari non nulli (cioè si tratta di una spazio proiettivo di dimensione n, come si vedrà in futuro se si continua a studiare Matematica). Questo ragionamento porta a pensare che l'insieme degli iperpiani affini dipenda da n parametri liberi, ma in realtà non si tratta di uno spazio affine di dimensione n: per lo stesso motivo per cui le rette di un fascio per un punto nel piano non sono (in corrispondenza con) una retta affine (in questo caso manca solo un punto: in generale mancano i punti di uno spazio proiettivo di dimensione $n-1$).

6.3. Per determinare invece l'insieme delle rette in uno spazio affine di dimensione n bisogna considerare le coppie di punti (quindi $2n$ parametri), ma dobbiamo tener conto del fatto che coppie diverse di punti possono determinare la stessa retta: ogni punto sulla retta è determinato da un parametro, quindi in totale i parametri necessari per determinare una retta saranno $2n-1-1 = 2n-2 = 2(n-1)$. Ma che tipo di spazio geometrico formino questi parametri non è facile da capire, e nemmeno come identificare un tale set di parametri. Il primo caso non banale è quello delle rette nello spazio affine tridimensionale: dipendono da 4 parametri che possono essere identificati come punti di una ipersuperficie quadratica in uno spazio di dimensione 5.

Pensare allo stesso problema (rette in uno spazio affine di dimensione n) usando le equazioni cartesiane lineari (ne servono $n-1$ indipendenti) porta agli stessi risultati in un modo più complicato, facile solo nei casi $n = 2, 3$.

Naturalmente, il caso delle rette nel piano ricadeva nel punto precedente.

6.4. Conteggio del numero di parametri da cui dipendono i sottospazi di dimensione m in uno spazio affine di dimensione n?

6.5. Si può anche cercare di classificare i possibili sottospazi o configurazioni di sottospazi a meno di certe trasformazioni (per esempio affinità, conformità, isometrie), ovvero considerando equivalenti due configurazioni se esiste una trasformazione del tipo voluto che trasforma una configurazione nell'altra: si tratta di classificare gli elementi dell'insieme quoziente delle configurazioni date modulo le trasformazioni volute.

6.5.1. due sottospazi di dimensione uguale possono essere sempre trasformati uno nell'altro con trasformazioni isometriche, quindi anche conformi e affini; quindi a meno di isometrie, o di conformità, o di affinità, i sottospazi di una fissata dimensione sono tutti equivalenti, e l'insieme quoziente è fatto da un punto.

6.5.2. se prendiamo invece la configurazione formata da due rette, vediamo che a meno di affinità vi sono tre classi possibili: rette incidenti, rette parallele e rette sghembe; a meno di conformità vi sono infinite classi di rette incidenti (dipendenti da un invariante che parametrizza le classi: l'angolo tra le rette), una classe di rette parallele, e infinite classi di rette sghembe (con invariante un parametro: l'angolo tra le rette); a meno di isometria vi sono infinite classi di rette incidenti (dipendenti da un invariante che parametrizza le classi: l'angolo tra le rette), infinite classi di rette parallele (dipendenti da un invariante che parametrizza le classi: la distanza tra le rette), e infinite classi di rette sghembe (dipendenti da due invarianti che parametrizzano le classi: la distanza e l'angolo tra le rette).

In altri termini, date due coppie di rette: esse possono essere trasformate una (coppia) nell'altra con affinità se e solo se entrambe le coppie hanno le stesse posizioni reciproche (incidenti, parallele, sghembe); possono essere trasformate con conformità sse hanno le stesse posizioni reciproche e formano lo stesso angolo; possono essere trasformate con isometrie sse (hanno le stesse posizioni reciproche e) hanno la stessa distanza e formano lo stesso angolo.

6.5.3. La configurazione di due iperpiani?

6.5.4. La configurazione di due piani in spazi affini di dimensione 3? In dimensione 4? In dimensione 5?

7. Forme frattali vie iterazioni di affinità. Si consideri una figura F (sottinsieme, diciamo compatto) del piano euclideo, e un insieme finito di trasformazioni affini $T_1, \ldots, T_m$. Si ponga $F_0 = F$, e per ogni i sia ricorsivamente F_{i+1} la figura che si ottiene facendo l'unione di $T_1(F_i), \ldots, T_m(F_i)$. Per esempio $F_1 = T_1(F_0), \ldots, T_m(F_0)$ (unione dei trasformati della figura di partenza). Sotto opportune condizioni sulle trasformazioni, il procedimanto "converge" ad una figura limite F_∞ che dipende solo dalle trasformazioni usate e non dalla figura di partenza. Spesso F_∞ ha un aspetto frattale, cioè di figura con parti che si ripetono indefinitamente simili. Spesso anche la figura data dalla unione di tutte le F_i ha un suo interesse, perlomeno estetico.

7.1. La figura di controcopertina si chiama Albero di Pitagora e si ottiene (a parte il riflesso, che ha puro scopo estetico: perché un albero con il riflesso sembra più bello di un albero e basta?) a partire dal quadrato grande tramite due trasformazioni affini. Capire quali. (nel disegno, il colore si scurisce man mano che i cresce; in effetti il disegno riporta F_i per $i = 0, 1, \ldots, 9$).

Anche la figura di copertina (Arbusto di Pitagora) si ottiene (a parte il riflesso, come prima) a partire dal quadrato grande tramite due trasformazioni affini. Capire quali. Questa figura è stata prodotta per inserire in mezzo il logo del libro. Perché albero e arbusto di Pitagora si somigliano molto?

7.2. A partire da un triangolo, ed iterando due trasformazioni affini, si possono ottenere queste due figure:

o anche queste due:

Capire quali trasformazioni si stanno usando e i rapporti tra la quattro figure. Perché non se ne sono costruite quattro usando il quadrato?

7.3. Un esempio con tre trasformazioni di un pentagono:

(e riflessione).

7.4. Per vedere l'indipendenza dalla forma iniziale, possiamo mostrare una successione di iterazioni usando tre trasformazioni uguali (capire quali) su diverse forme iniziali:

7.5. È abbastanza classico con questi procedimenti costruire degli alberi, il che fa capire come alcune forme comuni in natura si possono ottenere come ripetizione di azioni sempre simili:

Capire come si generano i rami.

7.6. Anche costruire dei cristalli può aver a che fare con affinità iterate; qui abbiamo tentato alcuni bi- e tri-cristalli, con alterne fortune:

7.7. Infine, sono classiche anche alcune figure dette di Sierpinski (ma il triangolo si dice anche di Tartaglia, modulo 2 perché fatto in bianco/nero):

Come si possono generare?

7.8. Provare ad immaginare frattali tridimensionali generati da iterazioni di trasformazioni affini, per esempio alberi e arbusti di Pitagora solidi (a partire da un cubo).

7.9. Naturalmente, nulla proibisce di usare trasformazioni lineari generali, cioè di prevedere anche deformazioni delle figure tramite le iterazioni successive.