Iacopo Barsotti

Appunti di Geometria II

(Università di Padova 1972–73)

(Iacopo Barsotti)

Indice

Prefazione

Il testo su cui mi sono basato per questa trascrizione è una dispensa dattiloscritta e ciclostilata che veniva prodotta dall'allora bidello Franco Mazzuccato del Seminario Matematico e venduta agli studenti che seguivano il corso di Geometria II. Una copia di queste dispense è conservata presso la Biblioteca del Seminario Matematico di Padova.

La qualità del contenuto e la brillantezza dello stile espositivo fanno di queste pagine un ottimo testo di lettura per chi voglia approfondire alcuni aspetti, forse oggi ingiustamente trascurati, dei corsi di base di Geometria. Per questo motivo le note sono state riprodotte in una forma più facilmente accessibile, rispetto alle vecchie dispense ciclostilate.

Per quanto riguarda la "composizione tipografica" di queste pagine,possiamo dire che l'utilizzo della macchina da scrivere per la composizione del testo originale presenta notevoli limitazioni rispetto alle possibilità attualmente concesse dal TEX, ma permette comunque, utilizzando eventualmente simboli aggiunti successivamente a mano, di ottenere una sufficiente raffinatezza nelle notazioni, come ben sanno i lettori di testi più o meno contemporanei pubblicati nei Lecture Notes della Springer o di note di seminari. Nella trascrizione si è quindi cercato di mantenersi il più possibile aderenti alle notazioni originali, comprese alcune abitudini tipiche di Barsotti, quali quella di non mettere parentesi sull'argomento di funzioni di una variabile (anche nel volume Appunti di Algebra o in articoli di ricerca da lui pubblicati, si trova fv invece del più consueto $f(v)$). Non si sono invece mantenute le abbreviazioni, molto diffuse nel testo, ed alcune terminologie tipiche, quali l'uso del termine "addittivo" in luogo di "additivo", perché queste ultime mi risultano universalmente accettate e il mantenimento del testo originale a rischio di possibili fraintendimenti. In questi casi, così come per evidenti errori di stampa, le modifiche sono state introdotte senza particolari indicazioni nel testo. In qualche caso si è comunque ritenuto opportuno evidenziare le differenze introdotte rispetto alla lezione originale. Le figure presenti nel testo sono state realizzate con Metapost cercando di riprodurre fedelmente i disegni presenti nella dispensa.

La speranza è quindi che le lezioni di Barsotti possano essere anche per gli studenti di oggi una lettura appassionante ed uno stimolo ad uno studio più approfondito di aspetti pur elementari, ma non per questo banali, della geometria.

Maurizio Candilera

1

Prodotti esterni, norme, spazio affine

1.1 Lezione 1

In tutto il corso, salvo esplicito avviso in contrario, tutti gli spazi vettoriali si intendono di dimensione finita. Il corso presuppone la conoscenza del corso di Algebra; per taluni (pochi) risultati si citerà direttamente, con la sigla [AA], il volume *Appunti di Algebra*, di Iacopo Barsotti (Zanichelli 1968).

Benché la teoria della dualità fra spazi vettoriali si supponga nota dal corso di Algebra, ne daremo qui definizioni e risultati; per le dimostrazioni vedansi le lezioni 42 e 43 di [AA].

Siano V e W spazi vettoriali sul corpo C; un'applicazione $(v, w) \mapsto v \circ w$ di $V \times W$ (prodotto cartesiano) su C è *bilineare* se è separatamente lineare nella v (per ogni w) e nella w (per ogni v); è una *dualità* se intanto è bilineare, e se inoltre accade che l'unico v (risp. l'unico w) che rende $v \circ w = 0$ per ogni w (risp. per ogni v) sia lo 0. Si dice anche che V, W sono duali l'uno dell'altro nella dualità "$\circ$". Altra notazione usata da vari autori (ma mai in questi appunti) in luogo di $v \circ w$ è la $\langle v\,,\, w\rangle$.

Teorema 1.1.1. *Sia V spazio vettoriale su C, e sia $W = \mathrm{Hom}_C(V, C)$. Allora vi è una dualità fra V e W data da $v \circ w = wv$. Se W' è un qualsiasi duale di V, vi è un unico isomorfismo f di W' su tutto W tale che $v \circ fw' = v \circ w'$ per ogni $v \in V$.*

L'(1.1.1) dice che il duale di V è unico a meno di isomorfismi, e che ha la stessa dimensione di V; lo si indicherà in generale con V^*; altre notazioni spesso usate sono $\tilde{V}$, V^t, ${}^tV$ (quella t è iniziale di *trasposto*, che è un altro modo di dire duale). L'(1.1.1) dice anche che $V^{**} \cong V$; questo V^{**} è il *biduale* di V, e di regola viene identificato con V.

Due elementi $v \in V$, $v^* \in V^*$ diconsi *ortogonali* se $v \circ v^* = 0$; se $\{v_1, \ldots, v_n\}$ è base di V, la sua *duale* o *trasposta* è la base $\{v_1^*, \ldots, v_n^*\}$ di V^* tale che $v_i \circ v_j^* = \delta_{ij}$ (simbolo di Kronecker); notare che l'asterisco appiccicato ad un vettore qualsiasi v, non pensato come elemento di una base, non significa proprio nulla.

Se X è sottoinsieme di V, l'*ortogonale* di X è il sottospazio $X^\perp$ (sempre così indicato) di V^* formato dai vettori che sono ortogonali ad ogni $x \in X$;

inoltre $X^{\perp\perp}$ è il minimo sottospazio di V che contiene X. In particolare, se X è già sottospazio, allora $X^{\perp\perp} = X$.

Lemma 1.1.2. *Se U è sottospazio di V, allora* $\dim U + \dim U^{\perp} = \dim V$.

1.2 Lezione 2

Siano V, U spazi vettoriali su C, e sia $f \in \mathrm{Hom}_C(V, U)$. Esiste un'unica $f^* \in \mathrm{Hom}_C(U^*, V^*)$ tale che $v \circ f^* u^* = fv \circ u^*$ per ogni $u^* \in U^*$; la f^* è la *trasposta* di f, e si ha $f^{**} = f$, $(fg)^* = g^* f^*$. Inoltre $\ker f^* = (\operatorname{im} f)^{\perp}$, onde $\operatorname{im} f^* = (\ker f)^{\perp}$.

Sia f legata alla matrice $A = (a_{ij})$ per mezzo della base $\{v_1, \ldots, v_n\}$ di V e della $\{u_1, \ldots, u_m\}$ di U:

$$f(v_i) = \sum_{j=1}^{m} a_{ji} u_j;$$

allora f^* è legata alla *trasposta* A^* di A (ossia $a^*_{ij} = a_{ji}$) per mezzo delle basi duali delle precedenti. Se in particolare $U = V$, ossia se $f \in \mathrm{End}_C V$, allora $f^* \in \mathrm{End}_C V^*$; l'applicazione $f \mapsto f^*$ applica $\mathrm{End}_C V$, che è una C-algebra, su $\mathrm{End}_C V^*$, che è pure una C-algebra; è una reciprocità di algebre.

Parentesi: Se C è un corpo, una C-algebra M è uno spazio vettoriale su C, non necessariamente di dimensione finita, che sia anche un anello, e tale inoltre che $(ca)b = a(cb) = c(ab)$ per $c \in C$ e per $a, b \in M$; si intende che le operazioni di somma in quanto spazio vettoriale e in quanto anello debbano coincidere. Un'applicazione $g : M \to N$ di una C-algebra su un'altra è un *omomorfismo* se è tale sia quando M, N sono considerati come spazi vettoriali, sia quando sono considerati anelli; è un *antiomomorfismo* se è omomorfismo di spazi vettoriali e se inoltre $g(ab) = g(b)g(a)$; è una *reciprocità* se è un antiomomorfismo iniettivo e suriettivo.

Altra parentesi che servirà tra poco: sia G un insieme sul quale è definita l'operazione $+$, associativa e commutativa (per esempio gli interi non negativi). Sia A un anello (risp. una C-algebra); tale A dicesi *graduato*, o *G-graduato*, se è somma diretta di gruppi additivi (risp. di spazi vettoriali su C, non necessariamente di dimensione finita) A_g, indicizzati da un g che percorre tutto G, in maniera che il prodotto di un elemento di A_g per uno di A_h stia in A_{g+h}. Notare che quando si considerano somme dirette di infiniti enti si intende che ogni elemento di A sia somma di un numero finito di elementi scelti negli A_g. Gli elementi di A_g diconsi *omogenei di grado g*; esempio tipico è quello di $A = C[x_1, \ldots, x_n]$, con C corpo ed $x_1, \ldots, x_n$ indeterminate; qui G consiste degli interi non negativi, mentre A_g è l'insieme (spazio vettoriale su C) delle *forme* di grado g, ossia dei polinomi ogni cui monomio ha grado g (ivi compreso il polinomio 0).

1.3 Lezione 3 (cfr. lezione 45 di [AA])

Ricordiamo che il *gruppo simmetrico* di ordine $n!$, indicato con P_n, è il gruppo di tutte le permutazioni di n oggetti; contiene come sottogruppo invariante di indice 2 il *gruppo alternante* A_n, che consiste di quelle permutazioni che sono di *classe pari*, ossia ottenibili mediante un numero pari di scambi. Se gli oggetti sono i numeri $1, 2, \dots, n$ in quest'ordine, per vedere se una certa permutazione $p = (p_1, \dots, p_n)$ è di classe pari o dispari basta contare il numero delle inversioni: si ha una *inversione* ogniqualvolta si ha una coppia (p_i, p_j) con $i < j$, ma $p_i > p_j$; classe pari se c'è un numero pari di inversioni. Chiamiamo *segnatura* di p, in simboli $\mathrm{sgn} p$, il numero 1 se p ha classe pari, e il numero -1 se p ha classe dispari. È come dire che $\mathrm{sgn} p$ è l'immagine, nel gruppo moltiplicativo $\{\pm 1\}$, di p modulo il sottogruppo invariante A_n. Quindi $\mathrm{sgn}(pq) = (\mathrm{sgn} p)(\mathrm{sgn} q)$, e $\mathrm{sgn}(p^{-1}) = \mathrm{sgn} p$. Se $n = 1$ si prende $P_1 = A_1 = \{1\}$, $\mathrm{sgn} 1 = 1$; idem se $n = 0$.

Sia S un insieme; un'applicazione f di $S \times \cdots \times S$ (n volte) su un corpo C è *alternante* se:

1. $f(\dots, s_i, \dots, s_j, \dots) = -f(\dots, s_j, \dots, s_i, \dots)$, ossia f cambia segno scambiando due suoi argomenti,
2. $f(\dots) = 0$ se due degli argomenti sono uguali.

Notare che, se C non ha caratteristica 2, la condizione 2 è conseguenza della 1, in quanto se $s_i = s_j$ la 1 dà $2f(\dots, s_i, \dots, s_j, \dots) = 0$. D'altra parte, se l'$S$ di prima è anche spazio vettoriale su C, e se si richiede che f sia *multilineare* (definizione simile a quella di bilineare, lezione 1), allora per controllare che f sia anche alternante basta verificare la 2; la 1 infatti ne segue nel modo seguente (ove prendiamo $n = 2$ per semplicità):

$$0 = f(u+v, u+v) = f(u,u) + f(u,v) + f(v,u) + f(v,v) = f(u,v) + f(v,u).$$

Al solito, se $n = 0$ o $n = 1$ la definizione precedente cade in difetto; ed allora, se $n = 1$ ogni applicazione di S in C sarà considerata alternante; se $n = 0$ le applicazioni alternanti saranno semplicemente gli elementi di C. Notiamo (donde il nome) che se t è una permutazione di $\{1, \dots, n\}$ si ha

$$f(s_{t_1}, \dots, s_{t_n}) = (\mathrm{sgn} t) f(s_1, \dots, s_n). \tag{1.3.1}$$

Sia V spazio vettoriale di dimensione n su C, e ne sia V^* il duale; indicheremo con E_i, od $E_i(V)$ se si vuole essere pignoli, lo spazio vettoriale su C (per ora non palesemente di dimensione finita) delle applicazioni i-lineari alternanti di $V^* \times \cdots \times V^*$ (i volte) su C; quindi $E_0 = C$, $E_1 = V$. Liberiamoci subito del sospetto sulla dimensione:

Lemma 1.3.2. *Nelle notazioni precedenti, sia $f \in E_i$; allora $f(x_1, \dots, x_i) = 0$ se le $x_1, \dots, x_i$ sono linearmente dipendenti.*

Teorema 1.3.3. *$E_i = 0$ per $i > n$; invece per $0 \le i \le n$ si ha $\dim E_i = \binom{n}{i} = \frac{n!}{i!(n-i)!}$. Se inoltre $v_1^*, \dots, v_n^*$ è base di V^*, una base di E_i è data dalle f_t*

così definite: t è un sottoinsieme ordinato, di cardinalità i, dell'insieme ordinato $\{1, \dots, n\}$; ed f_t manda la i-upla $v_{t_1}^*, \dots, v_{t_i}^*$ su 1, ed ogni altra i-upla di elementi della base, ad indici ordinati, sullo 0.

Dim. Per il (1.3.2): se le x_j sono linearmente dipendenti, una di esse, per esempio l'ultima, è combinazione lineare delle precedenti: $x_i = \sum_{j=1}^{i-1} c_j x_j$, con $c_j \in C$. Ed allora $f(x_1, \dots, x_i) = \sum_{j=1}^{i-1} c_j f(x_1, \dots, x_{i-1}, x_j) = 0$ (perché l'ultima x_j è uguale a qualche precedente x_j).

Per il (1.3.3): il primo asserto discende da (1.3.2), perché in V di dimensione n, non ci sono più di n vettori linearmente indipendenti. Per il resto, basta dimostrare l'asserto sulla base, dato che $\binom{n}{i}$ è proprio il numero delle sotto-i-uple ordinate di una n-upla ordinata.

Sia dunque $f \in E_i$; allora $f = \sum_t f(v_{t_1}^*, \dots, v_{t_i}^*) f_t$: infatti ambo i membri danno lo stesso risultato se applicati ad una i-upla ordinata qualsiasi $v_{s_1}^*, \dots, v_{s_i}^*$; quindi, per la multilinearità, anche se applicati ad una qualsiasi i-upla di elementi di V^* (non necessariamente scelti nella base).

Ciò dimostra che le f_t generano E_i; resta da dimostrare che esse sono linearmente indipendenti. Se allora $\sum_t c_t f_t = 0$, con $c_t \in C$, applicando alla i-upla $v_{s_1}^*, \dots, v_{s_i}^*$ (con s ordinato) si ottiene $c_s = 0$. C.V.D. □

1.4 Lezione 4

Sia $f \in E_i$, $g \in E_j$; definiamo il *prodotto esterno* $f \wedge g$ come l'elemento di E_{i+j} tale che, per $x_1, \dots, x_{i+j} \in V^*$, si abbia:

$$(1.4.1) \quad (f \wedge g)(x_1, \dots, x_{i+j}) = \sum_t (\operatorname{sgn} t) f(x_{t_1}, \dots, x_{t_i}) g(x_{t_{i+1}}, \dots, x_{t_{i+j}}),$$

ove la somma è estesa a tutte le permutazioni t di $\{1, \dots, i+j\}$ per le quali $t_1 < \dots < t_i$ e $t_{i+1} < \dots < t_{i+j}$.

Occorre far vedere che $f \wedge g$ è effettivamente elemento di E_{i+j}; la multilinearità è ovvia; per l'alternanza, suppongasi per esempio $x_h = x_k$ con $h \neq k$; quando nel secondo membro di (1.4.1) tanto h quanto k sono fra i primi i elementi t_s, oppure fra gli ultimi j, quel termine del secondo membro si annulla poiché f e g sono alternanti. Se invece si considera un termine, indicizzato da t, nel quale h cade fra i primi i e k fra gli ultimi j, per vedere bene la cosa spezziamo la permutazione t nei primi i e negli ultimi j elementi: $t = (T_1, T_2)$; e scriviamo il termine così:

$$(1.4.2) \qquad \operatorname{sgn}(T_1, T_2)\, f(x_{T_1}) g(x_{T_2});$$

nella T_1 sostituiamo h con k, ottenendo S_1, e nella T_2 sostituiamo k con h, ottenendo S_2. Ora S_1 ed S_2 sono permutazioni che possono essere non più ordinate (ossia gli elementi non più susseguentesi nell'ordine naturale); ordiniamole, ottenendo Z_1 e Z_2; nella (1.4.1) c'è anche il termine

$$\begin{aligned}
&\operatorname{sgn}(Z_1, Z_2)\, f(x_{Z_1})g(x_{Z_2}) = \\
&\qquad = \operatorname{sgn}(Z_1, Z_2)\, ((\operatorname{sgn} S_1)(\operatorname{sgn} Z_1)\, f(x_{S_1}))\, ((\operatorname{sgn} S_2)(\operatorname{sgn} Z_2)\, g(x_{S_2})) = \\
&\qquad = \operatorname{sgn}(S_1, S_2)\, f(x_{S_1})g(x_{S_2}) = \\
&\qquad = -\operatorname{sgn}(T_1, T_2)\, f(x_{S_1})g(x_{S_2}).
\end{aligned}$$

Ma $f(x_{S_1}) = f(x_{T_1})$, e analogamente per S_2 e T_2. Quindi questo termine elide il (1.4.2), e in conclusione $f \wedge g$ è alternante. □

Fra le seguenti regole solo l'ultima non è ovvia e sarà dimostrata:

$$\begin{aligned}
&f \wedge g = (-1)^{ij} g \wedge f \quad \text{se } f \in E_i \text{ e } g \in E_j; \\
&f \wedge f = 0 \quad \text{se } f \in E_i \text{ con } i \text{ dispari}; \\
&c \wedge f = f \wedge c = cf \quad \text{se } c \in C \text{ e } f \in E_i; \\
&f \wedge (g + h) = f \wedge g + f \wedge h \\
&(f + g) \wedge h = f \wedge h + g \wedge h \\
&f \wedge (g \wedge h) = (f \wedge g) \wedge h \quad (\text{onde si scrive } f \wedge g \wedge h).
\end{aligned} \tag{1.4.3}$$

L'ultima si dimostra così: intanto, se $f \in E_i$, $g \in E_j$, $h \in E_r$, invece di scrivere $x_{t_1}, \ldots, x_{t_i}$ scriviamo x_{T_1}; invece di scrivere $x_{t_{i+1}}, \ldots, x_{t_{i+j}}$ scriviamo x_{T_2}; invece di scrivere $x_{t_{i+j+1}}, \ldots, x_{t_{i+j+r}}$ scriviamo x_{T_3}; e quando la permutazione (T_1, T_2, T_3) è la permutazione naturale (ossia ordinata nell'ordine naturale), chiamiamola (I_1, I_2, I_3):

$$\begin{aligned}
&[f \wedge (g \wedge h)](x_{I_1}, x_{I_2}, x_{I_3}) = \\
&\quad = \sum_{\substack{T_1 \text{ ord} \\ (T_2, T_3) \text{ ord}}} \operatorname{sgn}(T_1, T_2, T_3)\, f(x_{T_1})(g \wedge h)(x_{T_2}, x_{T_3}) = \\
&\quad = \sum_{\substack{T_1 \text{ ord} \\ (T_2, T_3) \text{ ord}}} \operatorname{sgn}(T_1, T_2, T_3)\, f(x_{T_1}) \sum_{\substack{S_2 \text{ ord},\, S_3 \text{ ord} \\ (S_2, S_3) \text{ perm.} \\ \text{di } (T_2, T_3)}} \operatorname{sgn}(S_2, S_3)\, g(x_{S_2})\, h(x_{S_3}) = \\
&\quad = \sum_{\substack{T_1 \text{ ord} \\ S_2 \text{ ord} \\ S_3 \text{ ord}}} \operatorname{sgn}(T_1, S_2, S_3)\, f(x_{T_1})\, g(x_{S_2})\, h(x_{S_3}).
\end{aligned}$$

In questa formula f non compare in modo diverso da g od h, salvo l'ordinamento f, g, h; perciò si raggiunge lo stesso risultato partendo da $(f \wedge g) \wedge h$. C.V.D. □

L'ultima (1.4.3) dà, per $f = c \in E_0 = C$ e tenendo presente la terza,

$$c(g \wedge h) = (cg) \wedge h = g \wedge ch \tag{1.4.4}$$

(l'ultima ottenuta sostituendo f, g, h con, rispettivamente g, c, h).

Ora poniamo $E = E(V) = E_0 \oplus E_1 \oplus \cdots \oplus E_n$; è uno spazio vettoriale su C di dimensione $1 + n + \binom{n}{2} + \cdots + \binom{n}{n-2} + n + 1 = 2^n$; se $e = e_0 \oplus e_1 \oplus \cdots \oplus e_n$ ed $f = f_0 \oplus f_1 \oplus \cdots \oplus f_n$ sono elementi di E, definiamo

$$
\begin{aligned}
e \wedge f = e_0 \wedge f_0 \oplus (e_0 \wedge f_1 + e_1 \wedge f_0) \oplus (e_0 \wedge f_2 + e_1 \wedge f_1 + e_2 \wedge f_0) \oplus \\
\cdots \oplus (e_0 \wedge f_n + \cdots + e_n \wedge f_0).
\end{aligned}
$$

Le (1.4.3), (1.4.4) dicono che E, con questa definizione, è un'algebra graduata su C, detta l'*algebra esterna* su V; gli elementi di E_i sono i suoi elementi omogenei di grado i (lo 0 è omogeneo di ogni grado).

1.5 Lezione 5

Sia $\{v_1, \ldots, v_n\}$ base di V, e al solito sia $\{v_1^*, \ldots, v_n^*\}$ la base duale di V^*; gli elementi f_t del Teorema 1.3.3 non sono altro, per la definizione 1.4.1, che i prodotti $v_{t_1} \wedge \cdots \wedge v_{t_i}$; si può quindi dire:

Teorema 1.5.1. *Se $\{v_1, \ldots, v_n\}$ è base di V, una base di E_i è data dalle $v_{t_1} \wedge \cdots \wedge v_{t_i}$, ove $\{t_1, \ldots, t_i\}$ è un qualsiasi sottoinsieme ordinato di $\{1, \ldots, n\}$.*

ed anche

Teorema 1.5.2. *I vettori $x_1, \ldots, x_i$ di V sono linearmente dipendenti se, e solo se, $x_1 \wedge \cdots \wedge x_i = 0$.*

Dim. del (1.5.2). Se essi sono dipendenti, uno di essi è combinazione lineare degli altri; si ripete allora la prima parte della dimostrazione del Lemma 1.3.2, usando la seconda delle (1.4.3) (tenere presente che $x_j \in E_1$ e che 1 è dispari).

Reciprocamente, se $x_1, \ldots, x_i$ sono indipendenti, essi fanno parte di una base di V, onde il loro prodotto esterno è elemento di una base di E_i per (1.5.1), ed è perciò non nullo. C.V.D. □

Ora, al solito, il giochetto delle applicazioni lineari: siano V, U spazi vettoriali su C, e sia $f \in \mathrm{Hom}_C(V, U)$; definiamo un'applicazione $E_i(f) = f_i = f \wedge \cdots \wedge f$ (i volte) di $E_i(V)$ su $E_i(U)$ mediante la $f_i(x_1 \wedge \cdots \wedge x_i) = fx_1 \wedge \cdots \wedge fx_i$. Si controlla subito che questa è una buona definizione e che $f_i \in \mathrm{Hom}_C(E_i(V), E_i(U))$; quindi $F = E(f) = f_1 \oplus \cdots \oplus f_n \in \mathrm{Hom}_C(E(V), E(U))$, per lo meno in quanto spazi vettoriali; ma F è anche omomorfismo in quanto C-algebre, dato che

$$
\begin{aligned}
F((x_1 \wedge \cdots \wedge x_i) \wedge (y_1 \wedge \cdots \wedge y_j)) &= f_{i+j}(x_1 \wedge \cdots \wedge y_j) = \\
&= f_i(x_1 \wedge \cdots \wedge x_i) \wedge f_j(y_1 \wedge \cdots \wedge y_j) = \\
&= F(x_1 \wedge \cdots \wedge x_i) \wedge F(y_1 \wedge \cdots \wedge y_j).
\end{aligned}
$$

Consideriamo in particolare il caso di f_n quando $f \in \mathrm{End}_C V$ ed $n = \dim V$; è un endomorfismo di $E_n \cong C$; ed ogni endomorfismo di C in quanto spazio vettoriale su C consiste nella moltiplicazione per un elemento di C. In altre parole, $f_n \in C$, e per qualunque base $\{v_1, \ldots, v_n\}$ di V (od anche non-base) si ha

$$
fv_1 \wedge \cdots \wedge fv_n = f_n \, v_1 \wedge \cdots \wedge v_n.
$$

Questo f_n è chiamato il *determinante* di f ed è indicato con $\det f$; poiché le applicazioni $f \mapsto F$, $f \mapsto f_i$, quando f percorre $\mathrm{End}_C V$ sono chiaramente omomorfismi[1] di C-algebre si ha subito il

Teorema 1.5.3 (Teorema di Binet)**.** $\det(fg) = (\det f)(\det g)$.

Inoltre, il Teorema 1.5.2 dice che f è *singolare*, o *degenere* (ossia non iniettiva, o equivalentemente non suriettiva) se, e solo se, $f_n = 0$:

$$\det f = 0 \quad \text{se, e solo se, } f \text{ è singolare.} \tag{1.5.4}$$

I (1.5.3) e (1.5.4) messi insieme danno:

$$\text{se } f \text{ è nonsingolare, si ha } \det f^{-1} = (\det f)^{-1}. \tag{1.5.5}$$

Più preciso del (1.5.4) è il seguente risultato, conseguenza del (1.5.2):

Teorema 1.5.6. *Se $f \in \mathrm{End}_C V$, il rango di f (ossia $\dim fV$) è il massimo i per il quale $E_i(f) = f_i \neq 0$.*

Ed ora leghiamo il prodotto esterno con la dualità: oltre agli $E_i = E_i(V)$ vi sono gli $E_i^* = E_i(V^*)$; l'averli indicati con un asterisco fa pensare che essi siano duali degli E_i, in qualche modo canonico determinato dalla dualità "$\circ$" fra V e V^* (duali in qualche dualità lo sono certamente, visto che hanno la stessa dimensione); ciò è effettivamente vero, come mostra il risultato seguente:

Teorema 1.5.7. *Per ogni i esiste un'unica applicazione bilineare $(a, b) \mapsto a \circ b$ di $E_i \times E_i^*$ su C tale che*

$$(x_1 \wedge \cdots \wedge x_i) \circ (y_1 \wedge \cdots \wedge y_i) = (x_1 \wedge \cdots \wedge x_i)(y_1, \ldots, y_i)$$

per $x_j \in V$, $y_j \in V^*$. Essa è una dualità fra E_i ed E_i^*.

Dim. Si vede subito che se l'applicazione bilineare descritta esiste essa è una dualità. Per controllare che esista, osserviamo intanto che una (unica) applicazione bilineare con la proprietà descritta esiste quando per $x_1, \ldots, x_i$ si prenda un sottoinsieme ordinato di una base ordinata $\{v_1, \ldots, v_n\}$ di V. Per far vedere che tale applicazione gode della stessa proprietà quando le x_j siano arbitrarie, basta far vedere che continua a goderne se una di esse viene cambiata. Ora, per esempio, se la x_i viene sostituita con $\sum_j c_j v_j$, si ha

$$\begin{aligned}(x_1 \wedge \cdots \wedge x_i) \circ y &= \sum_j c_j (x_1 \wedge \cdots \wedge x_{i-1} \wedge v_j) \circ y = \\ &= \sum_j c_j (x_1 \wedge \cdots \wedge x_{i-1} \wedge v_j)(y) = (x_1 \wedge \cdots \wedge x_i)(y).\end{aligned}$$

C.V.D. □

[1] Il testo originale riporta la parola "isomorfismi", ma si tratta di una svista, perché le applicazioni tra $\mathrm{End}_C V$ ed i vari $\mathrm{End}_C E_i(V)$ non sono in generale né iniettive né suriettive.

Agganciando il (1.5.7) a quanto precede si vede che: se $f \in \mathrm{End}_C V$ ed f^* ne è il trasposto, allora $(f^*)_n = (f_n)^*$. Infatti

$$\begin{aligned}
(v_1 \wedge \cdots \wedge v_n) \circ (f^*)_n(v_1^* \wedge \cdots \wedge v_n^*) &= (v_1 \wedge \cdots \wedge v_n)(f^* v_1^*, \ldots, f^* v_n^*) = \\
&= \sum_t (\mathrm{sgn} t)(v_1 \circ f^* v_{t_1}^*) \cdots (v_n \circ f^* v_{t_n}^*) = \\
&= \sum_t (\mathrm{sgn} t)(f v_1 \circ v_{t_1}^*) \cdots (f v_n \circ v_{t_n}^*) = \\
&= (f v_1 \wedge \cdots \wedge f v_n)(v_1^*, \ldots, v_n^*) = \\
&= f_n(v_1 \wedge \cdots \wedge v_n) \circ (v_1^* \wedge \cdots \wedge v_n^*) = \\
&= (v_1 \wedge \cdots \wedge v_n) \circ (f_n)^*(v_1^* \wedge \cdots \wedge v_n^*).
\end{aligned}$$

Ma $f_n = \det f = (\det f)^*$, onde $(f_n)^* = \det f$; morale:

(1.5.8) $$\det f^* = \det f.$$

1.6 Lezione 6

Si è parlato di determinanti, ed è bene far vedere che si tratta proprio della vecchia conoscenza. Sia $f \in \mathrm{End}_C V$, sia $\{v_1, \ldots, v_n\}$ base di V, e sia $A = (a_{ij})$ la matrice legata ad f per mezzo di quella base:

$$f v_i = \sum_j a_{ji} v_j.$$

Questa dà

$$(\det f) v_1 \wedge \cdots \wedge v_n = f v_1 \wedge \cdots \wedge f v_n = \sum_j a_{j_1 1} \cdots a_{j_n n} v_{j_1} \wedge \cdots \wedge v_{j_n},$$

ove la somma è estesa in teoria al variare di ciascun j_i da 1 a n. Ma se due j_i hanno lo stesso valore, il prodotto esterno si annulla, cosicché basta far variare la j su tutte le permutazioni di $\{1, \ldots, n\}$. Ma allora, indicizzando diversamente si ottiene

$$(\det f) v_1 \wedge \cdots \wedge v_n = \left(\sum_{j \in P_n} (\mathrm{sgn} j) a_{j_1 1} \cdots a_{j_n n} \right) v_1 \wedge \cdots \wedge v_n,$$

ossia $\det f = \sum_{j \in P_n} (\mathrm{sgn} j) a_{j_1 1} \cdots a_{j_n n}$. Il secondo membro di questa è proprio il noto $\det A$, determinante della matrice A. Ora i (1.5.3), (1.5.4), (1.5.5), (1.5.8) assumono il solito significato della teoria dei determinanti. Il (1.5.6) invece fa sorgere il sospetto che gli f_i che vi compaiono abbiano a che fare con i minori di A, dato che il rango di f non è che la caratteristica di A, ossia il massimo i per il quale esistono minori non nulli di A di ordine i. Ed infatti, si cerchi la matrice legata ad f_i, nella base di E_i costituita dai $v_{t_1} \wedge \cdots \wedge v_{t_i}$ (cfr. 1.5.1). Se $B = (b_{sr})$ è questa matrice (e le s, r sono ora i-uple ordinate di interi positivi $\leq n$), da una parte si ha

$$f_i\, v_{r_1} \wedge \cdots \wedge v_{r_i} = \sum_s b_{sr} v_{s_1} \wedge \cdots \wedge v_{s_i}, \tag{1.6.1}$$

e dall'altra, come più sopra,

$$f_i\, v_{r_1} \wedge \cdots \wedge v_{r_i} = f v_{r_1} \wedge \cdots \wedge f v_{r_i} = \sum_s a_{s_1 r_1} \cdots a_{s_i r_i} v_{s_1} \wedge \cdots \wedge v_{s_i},$$

ove la somma è estesa a priori al variare di ciascun s_j da 1 a n. Ma di nuovo ci si può limitare a far variare s su tutte le i-uple di interi positivi distinti $\leq n$, ciascuna i-upla presa in tutti i possibili ordinamenti; se infine riordiniamo ciascuna i-upla nell'ordine naturale, il coefficiente di $v_{s_1} \wedge \cdots \wedge v_{s_i}$ nella formula precedente diviene $\sum_t (\mathrm{sgn} t) a_{t_1 r_1} \cdots a_{t_i r_i}$, ove t percorre tutte le permutazioni di $\{s_1, \ldots, s_i\}$. Ora l'espressione precedente è precisamente il minore di A estratto dalle righe $s_1, \ldots, s_i$ e dalle colonne $r_1, \ldots, r_i$. Se lo indichiamo con A_{sr}, un confronto con la (1.6.1) permette di affermare che

1.6.2. *La matrice formata coi minori A_{sr} è legata ad $f_i = f \wedge \cdots \wedge f$ (i volte) mediante la base di E_i descritta nel Teorema 1.5.1.*

Da qui possiamo dedurre la

1.6.3 (Regola di Laplace generalizzata)**.** *Se A è una matrice quadrata $n \times n$, se ne scelgano i colonne di indici $r_1, \ldots, r_i$ (in ordine crescente); per ogni scelta di i righe di indici $s_1, \ldots, s_i$ (in ordine crescente), sia A_{sr} il minore di queste righe e colonne. Siano poi S, R le j-uple (con $j = n - i$) ordinate complementari delle s, r in $\{1, \ldots, n\}$. Allora*

$$\det A = \sum_{s,S} \mathrm{sgn}(s, S)\, \mathrm{sgn}(r, R)\, A_{sr} A_{SR}.$$

Idem scambiando le parole "righe" e "colonne".

Dim. Scriviamo

$$(\det f) v_{r_1} \wedge \cdots \wedge v_{r_i} \wedge v_{R_1} \wedge \cdots \wedge v_{R_j} = f_i(v_{r_1} \wedge \cdots \wedge v_{r_i}) \wedge f_j(v_{R_1} \wedge \cdots \wedge v_{R_j}),$$

e sfruttiamo la (1.6.2) per f_i ed f_j; l'ultima espressione diviene

$$\sum_{s,S} A_{sr} A_{SR} v_{s_1} \wedge \cdots \wedge v_{s_i} \wedge v_{S_1} \wedge \cdots \wedge v_{S_j},$$

ove, al solito, basta prendere come insieme S il complementare di s in $\{1, \ldots, n\}$ (ordinato, naturalmente). Se ora questo $v_{s_1} \wedge \cdots \wedge v_{S_j}$ lo vogliamo scrivere come

$v_{r_1} \wedge \cdots \wedge v_{r_i} \wedge v_{R_1} \wedge \cdots \wedge v_{R_j}$ (come nella prima formula di questa dimostrazione), si acquista il fattore $\operatorname{sgn}(s, S) \operatorname{sgn}(r, R)$. C.V.D. $\square$

Per finire questa esposizione sull'algebra esterna, osserviamo che è bensì vero che ogni elemento di E_i è combinazione lineare di prodotti esterni di i vettori, ma non è in generale vero che sia proprio prodotto esterno di i vettori. Ciò è però vero nel caso speciale $i = 1$ (banale); donde, vista la simmetria delle dimensioni degli E_i, viene il dubbio che debba essere vero anche per $i = n - 1$. Dimostriamolo:

Teorema 1.6.4. *Se $n = \dim V$, ogni elemento di E_{n-1} è prodotto esterno di $n - 1$ elementi di V.*

Dim. Fissato un $0 \neq e \in E_n$, per ogni coppia (e_i, e_{n-i}), con $e_j \in E_j$, esiste un $c \in C$ tale che $e_i \wedge e_{n-i} = ce$. L'applicazione $(e_i, e_{n-i}) \mapsto c$ è una dualità fra E_i ed E_{n-i} (esercizio); la indicheremo, nel caso particolare $i = n - 1$, con un puntino invece del solito tondino: $e_{n-1} \cdot e_1$. Sia allora $0 \neq y_n \in E_{n-1}$, onde y_n è elemento di una base $\{y_1, \ldots, y_n\}$ di E_{n-1}; ne sia $\{v_1, \ldots, v_n\}$ la base duale di $V = E_1$, e pongasi

$$a = (v_1 \wedge \cdots \wedge v_{n-1}) \cdot v_n \neq 0.$$

Ora si ha $y_n \cdot v_i = \delta_{ni}$, ed anche $(v_1 \wedge \cdots \wedge v_{n-1}) \cdot v_i = a\delta_{ni}$. Quindi $y_n = a^{-1}(v_1 \wedge \cdots \wedge v_{n-1})$. C.V.D. $\square$

1.7 Lezione 7

Sia V spazio vettoriale su C, e sia $(x, y) \mapsto g(x, y)$ una applicazione bilineare di $V \times V$ su C, detta anche *forma bilineare* su V. Se la caratteristica di C non è 2, pongasi

$$g_s(x, y) = \frac{1}{2}\left[g(x, y) + g(y, x)\right] \quad \text{e} \quad g_a(x, y) = \frac{1}{2}\left[g(x, y) - g(y, x)\right].$$

Ora g_s è *simmetrica*, ossia $g_s(x, y) = g_s(y, x)$, mentre g_a è alternante, detta anche *antisimmetrica*. Quindi per studiare le forme bilineari su V, basta studiare separatamente le simmetriche e le alternanti, sempre che C non abbia caratteristica 2; nulla naturalmente vieta di dare qualche risultato anche nel caso della caratteristica 2. Sia dunque g simmetrica o alternante; un $x \in V$ dicesi *isotropo* se $g(x, x) = 0$ (se g è alternante, sono tutti isotropi); la g è *degenere* se esiste qualche vettore $x \neq 0$ che è *ortogonale* ad ogni y: $g(x, y) = 0$, onde $g(y, x) = 0$ per ogni y. L'insieme di tali x è un sottospazio di V, detto il *nucleo* ed indicato con $\ker g$. Infine, un sottospazio nel quale la g induca la forma bilineare nulla è detto *isotropo*[2]; quest'ultimo concetto, ma non gli altri, resta significativo anche quando

[2]Segnaliamo la differenza con la terminologia di [D] (Jean Dieudonné, *Sur les groupes classiques*, Publ. Inst. Math. Univ Strasbourg, 1948) ove i sottospazi isotropi sono quelli su cui g induce una forma bilineare degenere, mentre i sottospazi su cui g induce la forma identicamente nulla sono detti "totalmente isotropi". Il testo [MH] (John Milnor e Dale Husemoller, *Symmetric Bilinear Forms*, Springer Verlag 1973) preferisce il termine "self-orthogonal subspaces".

g sia bilineare qualsiasi. Torniamo alla g simmetrica o alternante; se $U = \ker g$, e W è complementare di U in V, la restrizione di g a W è nondegenere: sia infatti $0 \neq x \in W$; se si avesse $g(x, y) = 0$ per ogni $y \in W$, la stessa varrebbe per ogni $y \in V$, onde x apparterrebbe ad U, il che non è. Si può perciò asserire che V è somma diretta di un sottospazio U sul quale la g è nulla, e di un W sul quale è nondegenere. La scelta di U è unica, ma non quella di W; se però W_1, W_2 sono due scelte di W, e se g_1, g_2 sono le restrizioni di g a W_1, W_2 rispettivamente, si può porre fra W_1 e W_2 il seguente isomorfismo: per $x \in W_1$ si scriva $x = z + y$, con $z \in W_2$ ed $y \in U$; la $x \mapsto z$ è l'isomorfismo voluto. Se $x \mapsto z$ ed $x' \mapsto z'$, si ha

$$g_2(z, z') = g(z, z') = g(z + y, z' + y') = g(x, x') = g_1(x, x');$$

insomma, l'isomorfismo di W_1 su tutto W_2 cambia g_1 in g_2. Quindi l'applicazione bilineare (simmetrica o alternante) non degenere legata ad una degenere è unica a meno di isomorfismi, e ci potremo perciò limitare a studiare le nondegeneri.

Diciamo subito che se V, U sono spazi vettoriali su C muniti di forme bilineari g, h, un isomorfismo t di V su tutto U che soddisfa la $h(tx, ty) = g(x, y)$ dicesi una *isometria* (rispetto a g, h); gli spazi diconsi *isometrici*. Con le stesse notazioni, ma senza l'ipotesi di isometria e neppure di uguaglianza di dimensione, lo spazio $V \oplus U$ può essere dotato della forma k così definita:

$$k(v \oplus u, v' \oplus u') = g(v, v') + h(u, u');$$

tale forma sarà indicata con $g \boxplus h$ e chiamata *somma ortogonale*; anche $V \oplus U$, dotato di $g \boxplus h$, sarà indicato con $V \boxplus U$ e chiamato *somma ortogonale*. Se nella formula precedente che definisce k si usa il $-$ in luogo del $+$, si ha la *differenza ortogonale*: $g \boxminus h$, $V \boxminus U$. I $\boxminus g$, $\boxminus V$, sono ovviamente gli $0 \boxminus g$ e $\langle 0 \rangle \boxminus V$, quest'ultimo essendo V dotato di $-g$. Si noti che $g \boxminus g$ e $V \boxminus V$ non sono 0; quest'ultimo è $V \oplus V$ dotato della $k(x \oplus x', y \oplus y') = g(x, y) - g(x', y')$.

Un'applicazione bilineare non degenere è anche una *autodualità*; se è simmetrica si chiama una *norma* su V, e lo spazio V insieme ad una propria norma è uno *spazio normato*.

Le applicazioni bilineari simmetriche sono intimamente legate alle applicazioni o *forme quadratiche* su V. Si chiama così un'applicazione $f : V \to C$ tale che:

1. $f(cx) = c^2 fx$ se $c \in C$ ed $x \in V$;
2. La $(x, y) \mapsto g(x, y) = f(x + y) - fx - fy$ è una forma bilineare, certamente simmetrica.

Come si vede dalla definizione stessa, ad una forma quadratica f è legata una bilineare simmetrica g, dalla quale f è ricostruibile quando la caratteristica di C non sia 2 col porre $f(x) = \frac{1}{2} g(x, x)$; e questa stessa formula dà, per ogni g bilineare simmetrica (ed anche non simmetrica), una f quadratica, sempre che la caratteristica non sia 2. Perciò, se la caratteristica non è 2, alle quadratiche si possono applicare la nomenclatura ed i risultati delle bilineari simmetriche: *nucleo, degenere* o no, *somma* e *differenza ortogonali*, *vettori* e *sottospazi isotropi*.

1.8 Lezione 8

Vediamo la traduzione in matrici del contenuto della lezione precedente. Sia $\{v_1, \ldots, v_n\}$ una base di V; i vettori di V sono gli $x_1v_1 + \cdots + x_nv_n$, con $x_i \in C$, e questi possono essere identificati con le matrici $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ di tipo $n \times 1$; la forma bilineare g è completamente identificata col dare le $a_{ij} = g(v_i, v_j)$. Se A è la matrice a_{ij}, si ha

$$g\left(\sum_i x_i v_i, \sum_j y_j v_j\right) = \sum_{ij} a_{ij} x_i y_j = X^* AY$$

(al solito X^* è la trasposta di X, ossia la matrice $(x_1, \ldots, x_n)$ di tipo $1 \times n$). La g è simmetrica (risp. alternante) se, e solo se, la A è *simmetrica* (ossia $A^* = A$) o rispettivamente *antisimmetrica* (ossia $A^* = -A$)[3]. Se A è simmetrica, la forma quadratica f ad essa legata (se la caratteristica non è 2) è la $X \mapsto \frac{1}{2}X^*AX = \frac{1}{2}\sum_{ij} a_{ij}x_ix_j = f(X)$; questa è proprio una forma nelle indeterminate x_i (quadratica, ossia di grado 2) nel senso della lezione 2.

Se A, B le matrici di due forme bilineari, g, h (su due spazi), la matrice di $g \boxplus h$ è $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$, e quella di $g \boxminus h$ è $\left(\begin{smallmatrix} A & 0 \\ 0 & -B \end{smallmatrix}\right)$.

Sia $\{u_1, \ldots, u_n\}$ un'altra base di V, con la trasformazione di basi data da

$$u_j = \sum_i p_{ij} v_i. \tag{1.8.1}$$

Posto $P = (p_{ij})$, il vettore rappresentato da X nella base v è rappresentato da $P^{-1}X$ nella base u. Se B è la matrice di g nella base u, si dovrà avere $(P^{-1}X)^*BP^{-1}X = X^*AX$; ma $(P^{-1}X)^* = X^*(P^{-1})^*$, onde $X^*P^{*-1}BP^{-1}X = X^*AX$, e infine

$$B = P^*AP. \tag{1.8.2}$$

Due matrici A, B, con elementi in un anello commutativo con identità (in questo caso nel corpo C), che sono legate fra loro dalla (1.8.2), con P matrice ad elementi in quell'anello e invertibile in quell'anello, diconsi *congruenti* in quell'anello; la relazione di congruenza è ovviamente un'equivalenza, ossia è riflessiva, simmetrica e transitiva. Nel caso presente due matrici sono congruenti se, e solo se, sono legate alla stessa forma bilineare (od anche quadratica nel caso delle simmetriche) mediante basi diverse.

[3] Già qui dovrebbe porsi l'ipotesi che la caratteristica sia diversa da 2. Se la caratteristica fosse 2 la definizione data di matrice antisimmetrica coinciderebbe con quella di matrice simmetrica, ma la matrice di una forma bilineare alternante deve soddisfare anche la condizione $a_{ii} = 0$

L'essere g non degenere significa che la validità di $X^*AY = 0$ per ogni Y comporta $X^* = 0$; ma $X^*AY = 0$ per ogni Y è equivalente a $X^*A = 0$; quindi g è non degenere se, e solo se, la $X^*A = 0$ comporta $X^* = 0$; ossia se, e solo se, A è non degenere (= nonsingolare; insomma, se $\det A \neq 0$).

Sappiamo che se g è degenere e simmetrica o alternante, si può scrivere $V = U \boxplus W$, ove g è nulla su U e nondegenere su W; quindi

Teorema 1.8.3. *Ogni matrice A simmetrica o antisimmetrica ad elementi in un corpo è congruente, su quel corpo, ad una matrice del tipo $\left(\begin{smallmatrix} B & 0 \\ 0 & 0 \end{smallmatrix}\right)$, con B nondegenere, ed avente ordine eguale alla caratteristica di A.*

Si può aggiungere che se la forma quadratica f è vista proprio come forma $f(x)$, nelle indeterminate $x_1, \dots, x_n$, uncambiamento di base corrisponde ad una sostituzione lineare nelle indeterminate; se la A di f viene trasformata in una $\left(\begin{smallmatrix} B & 0 \\ 0 & 0 \end{smallmatrix}\right)$, la $f(x)$ diviene una $f'(y)$, ove però, se l'ordine di B è $m < n$, le $y_{m+1}, \dots, y_n$ non compaiono; quindi:

Corollario 1.8.4. *La caratteristica della matrice di una forma quadratica uguaglia il minimo numero di indeterminate (combinazioni lineari delle date) che compaiono effettivamente nella forma.*

Torniamo alla (1.8.2); al solito, la (1.8.1) poteva essere considerata non come un cambiamento di base, ma come un isomorfismo t di V su uno spazio U di base $\{u_1, \dots, u_n\}$; la (1.8.2) dà allora la matrice legata, per mezzo di $\{u_1, \dots, u_n\}$, alla forma bilineare di U che rende t isometria. Facciamo invece di nuovo $U = V$, ma cerchiamo quand'è che questa t è isometria: ora V ha già la g, e quindi occorre che la B definita dall'(1.8.2) coincida con la A:

$$A = P^*AP. \tag{1.8.5}$$

Se vogliamo usare t direttamente si ragiona così: t è isometria se, e solo se, $g(tx, ty) = g(x, y)$; qualora g sia nondegenere, ossia sia autodualità, e si possa quindi scrivere $x \circ y$ in luogo di $g(x, y)$, la precedente diviene $tx \circ ty = x \circ y$. Qui, ricordando la trasposizione delle applicazioni lineari, si sarebbe tentati di scrivere indifferentemente $tx \circ ty = x \circ t^*ty$ oppure $tx \circ ty = t^*tx \circ y$, raggiungendo in ambo i casi il risultato che:

1.8.6. *t è isometria (di uno spazio in sé) se, e solo se, $t^*t = \iota$ (ι=iota, che indicherà sempre l'applicazione identica); ossia se, e solo se, $t^* = t^{-1}$.*

Il risultato è vero, ma è stato raggiunto in modo troppo semplicistico; infatti la t^* definita da $t^*x \circ y = c \circ ty$ non coincide in generale con la $\tilde{t}$, definita da $x \circ \tilde{t}y = tx \circ y$; si ha certamente $(\tilde{t})^* = \tilde{t^*} = t$, ma non si ha né $t^{**} = t$, né $\tilde{\tilde{t}} = t$. Questo è perché i risultati sulla bidualità sono stati raggiunti, nella lezione 2, identificando in modo canonico il biduale di V con V; il modo canonico consisteva nell'identificare la base biduale del biduale di V con la base di partenza. Nel caso presente, il duale di V è già dato, ed è V stesso con la stessa base; la base duale chissà chi è, e la biduale vattelapesca! Comunque, l'(1.8.6) è vero sia come scritto, sia sostituendovi l'asterisco con la tilde. Se però g è o simmetrica, o alternante (oltre che nondegenere), allora $t^* = \tilde{t}$ e non ci sono patemi. Per la matrice P di t, la regola resta l'(1.8.5), anche nel caso degenere.

Se P è matrice di una isometria di V in sé, ed A (ossia g) è nondegenere, prendendo i determinanti di (1.8.5) si ottiene $\det A = (\det P)^2 \det A$, ossia $(\det P)^2 = 1$, $\det P = \pm 1$:

Teorema 1.8.7. *Le (matrici delle) isometrie di uno spazio con forma bilineare non degenere sono* modulari*, ossia con determinante* ± 1.

Quelle con determinante $+1$ sono chiamate *unimodulari* (ma semplicemente modulari da certi autori).

1.9 Lezione 9

Abbiamo visto che ci si può ridurre allo studio delle forme bilineari su V che sono non degeneri, e che inoltre sono o norme (ossia simmetriche), o alternanti. Ora dobbiamo appunto iniziare questo studio; un po' di nomenclatura: una norma su V dicesi *iperbolica* (ed il V munito di essa dicesi *spazio iperbolico*) se V contiene un sottospazio V_1 che è l'ortogonale di se stesso in V; naturalmente tale V_1 è isotropo. Se $n = \dim V$, $m = \dim V_1$, si ha $\dim V_1^{\perp} = n - m$; ma $V_1^{\perp} = V_1$, onde $n - m = m$, $n = 2m$. Quindi gli spazi iperbolici hanno tutti dimensione pari, doppia di quella di un loro qualsiasi sottospazio che sia l'ortogonale di se stesso. Invece, una norma su V dicesi *ellittica* (e lo spazio è *ellittico*)se l'unico vettore isotropo di V è lo 0, ossia se $x \circ x \neq 0$ per $x \neq 0$. Quanto alle forme alternanti nondegeneri, ci limiteremo a stipulare che uno spazio munito di una tale forma sarà detto esso stesso *alternante*. Le isometrie di V in sé prendono anche nomi diversi nei vari casi: per gli spazi normati si chiamano *trasformazioni ortogonali* ; per quelli alternanti si chiamano *trasformazioni simplettiche*. Gli spazi iperbolici e quelli alternanti possono essere trattati in modo simile, come mostra questo primo (e praticamente unico) risultato:

Teorema 1.9.1. *Se C non ha caratteristica 2, uno spazio su C è iperbolico se, e solo se, è somma ortogonale di spazi normati di dimensione 2, ciascuno dei quali ha una base $\{v, w\}$ tale che $v \circ v = w \circ w = 0$, $v \circ w = 1$. Senza ipotesi su C, lo stesso vale per gli spazi alternanti.*

[Il trucco naturalmente sta nel non aver detto chi è $w \circ v$, che sarà $+1$ per gli iperbolici e -1 per gli alternanti].
Dim. Se V è iperbolico, sappiamo già che contiene un sottospazio V_1 che è l'ortogonale di se stesso; ne sia $\{v_1, \dots, v_m\}$ una base. Se V è alternante, sia V_1 un sottospazio isotropo massimale (massimale fra gli isotropi); l'ortogonale $V_1^{\perp}$ di V_1 in V contiene V_1, e non contiene nient'altro: ché se $0 \neq v \in V_1^{\perp} \smallsetminus V_1$, allora $V_1 + \langle v \rangle$ è ancora isotropo, contro l'ipotesi di massimalità. Qui, come sempre nel seguito, indico con $\langle S \rangle$ il minimo spazio vettoriale che contiene S.

In ambo i casi, sia $w \in V$ tale che $v_i \circ w = \delta_{i1}$; possibile perché $V \cong V^* \cong \mathrm{Hom}_C(V, C)$; nel caso alternante, w è già isotropo, e se lo si chiama w_1, lo spazio $\langle v_1, w_1 \rangle$ è il primo fra quelli richiesti. Nel caso iperbolico w non è detto che sia isotropo; pongasi allora $w_1 = x v_1 + w$, con $x \in C$; è ancora $v_i \circ w_1 = \delta_{i1}$, ed è anche $w_1 \circ w_1 = 2x + w \circ w$. Dato che la caratteristica di C non è 2, la x può essere scelta in modo che w_1 sia isotropo; e di nuovo $\langle v_1, w_1 \rangle$ è il primo degli spazi cercati. Chiamiamolo, in ambo i casi, U_1, e consideriamo il suo ortogonale $U_1^{\perp}$ in V; questo $U_1^{\perp}$ è ancora alternante o iperbolico, e la funzione di V_1 per esso è assolta da $\langle v_2, \ldots, v_m \rangle$. Quindi si può costruire un $U_2 = \langle v_2, w_2 \rangle$, eccetera. Questo dimostra il teorema in una direzione; nell'altra è ovvio. C.V.D. □

Il (1.9.1) dice che per uno spazio alternante (necessariamente di dimensione pari) la base può essere scelta in modo che la matrice della forma alternante sia

$$\begin{pmatrix} 0 & 1 & & & & & & \\ -1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & -1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & \ddots & & \\ & & & & & & 0 & 1 \\ & & & & & & -1 & 0 \end{pmatrix} \qquad \text{(di ordine } 2m\text{);} \tag{1.9.2}$$

e dice anche che se la caratteristica di C non è 2, la matrice di una forma iperbolica può divenire

$$\begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & 1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & \ddots & & \\ & & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix} \qquad \text{(di ordine } 2m\text{).} \tag{1.9.3}$$

Le due matrici sono state ottenute prendendo la base $v_1, w_1, v_2, w_2, \ldots, v_m, w_m$. Se prendiamo la stessa, ma nell'ordine $v_1, \ldots, v_m, w_1, \ldots, w_m$, le matrici divengono

$$\begin{pmatrix} 0 & \mathbf{1}_m \\ -\mathbf{1}_m & 0 \end{pmatrix} \qquad \text{alternante,} \tag{1.9.4}$$

$$\begin{pmatrix} 0 & \mathbf{1}_m \\ \mathbf{1}_m & 0 \end{pmatrix} \qquad \text{iperbolico,} \tag{1.9.5}$$

ove $\mathbf{1}_m$ vuol dire la matrice identica di ordine m.

Nel caso iperbolico c'è una forma ancora più simpatica: poniamo $x_i = v_i + w_i$, $y_i = v_i - w_i$, e prendiamo la base $x_1, \ldots, x_m, y_1, \ldots, y_m$; la matrice diviene:

$$
(1.9.6) \qquad \begin{pmatrix} 2 & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & 2 & \ddots & & \vdots \\ \vdots & & \ddots & -2 & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \ldots & \ldots & \ldots & 0 & -2 \end{pmatrix} \qquad \begin{array}{l} (m \text{ elementi} = 2 \text{ ed} \\ \ m \text{ elementi} = -2). \end{array}
$$

Se il corpo contiene una radice quadrata di 2, dividendo le x_i, y_i per essa la matrice precedente diviene $\left(\begin{smallmatrix} \mathbf{1}_m & 0 \\ 0 & -\mathbf{1}_m \end{smallmatrix}\right)$.

1.10 Lezione 10

Possiamo trarre alcune conseguenze: intanto il (1.9.6) dice che

$$V = \langle x_1, \ldots, x_m \rangle \boxplus \langle y_1, \ldots, y_m \rangle\,,$$

e inoltre che $\langle y_1, \ldots, y_m \rangle$ è isometrico a $\boxminus \langle x_1, \ldots, x_m \rangle$. Si ha così il "solo se" del risultato seguente:

Lemma 1.10.1. *Se il corpo non ha caratteristica* 2*, uno spazio è iperbolico se, e solo se, è differenza ortogonale di due spazi normati isometrici.*

Dim. del "se". Se $V = U \boxminus U$, con U normato, i vettori $u \oplus u$, quando u percorre U, formano un sottospazio isotropo di V, di dimensione $= \dim U$, che quindi è l'ortogonale di se stesso in V. C.V.D. □

Invece una conseguenza del (1.9.4) è la seguente:

Corollario 1.10.2. *Ogni matrice antisimmetrica di ordine dispari, ad elementi in un anello commutativo con identità, ha determinante nullo. Ogni matrice antisimmetrica di ordine pari, ad elementi in un anello come sopra, ha per determinante il quadrato di un elemento dell'anello.*

Dim. Per ora lasciamo perdere l'anello e rimaniamo nel corpo C. Una matrice antisimmetrica di ordine dispari dà una forma alternante su uno spazio di dimensione dispari, e per quanto visto una tale forma deve essere degenere, cosicché il determinante della matrice è 0. Nel caso pari, sia A la matrice data; se $detA = 0$, bene perché 0 è un quadrato. Se $\det A \neq 0$, lo spazio è alternante, e con base oppportuna la matrice diviene quella del (1.9.4), che indichiamo con B. Ma allora, per (1.8.2), esiste una matrice invertibile P tale che $A = P^* B P$, onde $\det A = (\det P)^2$, come voluto.

Ora prendiamo per C il corpo speciale $\mathbb{Q}(\ldots, t_{ij}, \ldots)$, ove (se $n = \dim V$) le i, j assumono tutti i valori $1, \ldots, n$ con $i < j$, e ove le t_{ij} sono indeterminate; $\mathbb{Q}$ è il corpo razionale. Sia A la matrice antisimmetrica che ha l'elemento t_{ij} nel posto i, j, l'elemento $-t_{ij}$ nel posto j, i, e 0 sulla diagonale. Se allora n è dispari, si deve avere $\det A = 0$. Ma $\det A$ è un polinomio nelle t_{ij} a coefficienti interi, ed è il polinomio 0; tale quindi resta se le t_{ij} vengono sostituite con elementi qualsiansi di un anello commutativo con identità.

Se invece n è pari, sarà $\det A = (q(t))^2$, con $q(t)$ polinomio nelle t a coefficienti razionali; ma il suo quadrato è a coefficienti interi, quindi $q(t)$ stesso è a coefficienti interi (lemma di Gauss, 4.31 di [AA]). Se di nuovo le t_{ij} vengono sostituite con elementi di un anello commutativo con identità, la relazione resta vera. C.V.D. □

Il $q(t)$ di cui si è appena parlato è definito a meno del fattore ± 1; possiamo definirlo completamente col richiedere che esso divenga 1, e non -1, quando la A diviene la (1.9.4). Questo $q(t)$ si chiama il *pfaffiano* di ordine n.

1.11 Lezione 11

Così abbiamo terminato con gli iperbolici e gli alternanti, ed è stato facile trovarli tutti; resta da parlare dei normati non iperbolici. Prima parliamo di fatti generali.

Lemma 1.11.1. *Se C ha caratteristica $\neq 2$, per ogni norma su V esiste qualche vettore non isotropo. In altre parole, un sottospazio di V è isotropo se, e solo se, tale è ogni suo elemento.*

Dim. Se $v, w \in V$ si ha $(v + w) \circ (v + w) = v \circ v + w \circ w + 2v \circ w$; se ogni vettore fosse isotropo, sarebbe $v \circ w = 0$, assurdo. C.V.D. □

Lemma 1.11.2. *In uno spazio normato, vettori non isotropi, a due a due ortogonali, sono linearmente indipendenti.*

Dim. Se $\sum_i c_i v_i = 0$ ($c_i \in C$), si ha $0 = v_j \circ \sum_i c_i v_i = c_j v_j \circ v_j$, onde $c_j = 0$. C.V.D. □

Un vettore v è *normalizzato*, o è un *versore*, se $v \circ v = 1$; una r-upla di vettori è *ortogonale* se essi sono a due a due ortogonali; è *ortonormale* se è ortogonale ed ogni suo elemento è un versore; quindi una *base ortonormale* è una *base autoduale*, ossia duale di se stessa. Una base ortogonale si riconosce dal fatto che la matrice legata alla norma per mezzo di essa è *diagonale*, ossia con elementi tutti nulli fuori della diagonale (principale). La base è ortonormale se questa matrice è addirittura la matrice identica.

Teorema 1.11.3. *Se $\{v_1, \dots, v_n\}$ è base di V, esiste una unica norma di V per la quale quella base è ortonormale. Reciprocamente, ogni spazio normato in caratteristica $\neq 2$ ha basi ortogonali; e se ogni $v \circ v$, per lo meno per i v di una base ortogonale, è quadrato di un elemento del corpo, esistono anche basi ortonormali.*

Dim. Per la prima parte, la norma è quella che nella data base è legata alla matrice identica. Per la seconda, si scelga un vettore non isotropo v_1 (cfr. 1.11.1); l'ortogonale U di $\langle v_1 \rangle$ è normato dalla stessa norma, ed è complementare a v_1. Se allora il teorema era supposto vero per dimensioni minori di $\dim V$ (e lo è per dimensione 1), questo U ha base ortogonale $v_2, \dots, v_n$, che con v_1 dà una base ortogonale di V. Se infine è vera la faccenda dei quadrati, sia $c_i \in C$ tale che $c_i^2 = v_i \circ v_i$; questo c_i è non nullo perché una norma ha nucleo zero; posto $u_i = c_i^{-1} v_i$, la $\{u_1, \dots, u_n\}$ è base ortonormale. C.V.D. $\square$

Teorema 1.11.4. *Sia V spazio normato su C, e sia $f \in \mathrm{End}_C V$. Se C non ha caratteristica 2, la f è trasformazione ortogonale se, e solo se, $fv \circ fv = v \circ v$ per ogni $v \in V$. Se invece V ha basi ortonormali, f è ortogonale se, e solo se, trasforma una data (e quindi ogni) base ortonormale in una base ortonormale.*

Dim. Se $fv \circ fv = v \circ v$ si ha

$$\begin{aligned} 2(fv \circ fw) = f(v+w) \circ f(v+w) - fv \circ fv - fw \circ fw = \\ = (v+w) \circ (v+w) - v \circ v - w \circ w = 2(v \circ w), \end{aligned}$$

e la f è ortogonale. Se invece $\{v_1, \dots, v_n\}$ è base ortonormale, si ha $fv_i \circ fv_j = f^* f v_i \circ v_j$, e questa coincide con $\delta_{ij} = v_i \circ v_j$ se, e solo se, $f^* = f^{-1}$. C.V.D. $\square$

È qui giunto il momento di dire che una *matrice ortogonale* è la matrice P di una trasformazione ortogonale rispetto ad una base ortonormale; deve cioè soddisfare la

$$P^* = P^{-1}. \tag{1.11.5}$$

Invece una *matrice simplettica* è la matrice P (di ordine $2m$) di una trasformazione simplettica rispetto ad una base nella quale la forma alternante abbia la matrice (1.9.4); deve cioè soddisfare (come conseguenza dell'1.8.5) la

$$P^* = \begin{pmatrix} 0 & \mathbf{1}_m \\ -\mathbf{1}_m & 0 \end{pmatrix} P^{-1} \begin{pmatrix} 0 & -\mathbf{1}_m \\ \mathbf{1}_m & 0 \end{pmatrix}. \tag{1.11.6}$$

1.12 Lezione 12

È chiaro che uno spazio normato è ellittico se, e solo se, non contiene nessun sottospazio iperbolico di dimensione positiva (perché gli ellittici non hanno vettori isotropi non nulli, e gli iperbolici ne hanno); invece un iperbolico può benissimo contenere degli ellittici: per esempio, ogni sottospazio generato da un vettore non isotropo è ellittico. Tramite vari lemmi vogliamo far vedere che ogni spazio normato, in caratteristica diversa da 2, è somma ortogonale di un iperbolico ed un ellittico. Anzitutto nella dimostrazione del Teorema 1.9.1 si è visto che ogni sottospazio isotropo massimale di un alternante è l'ortogonale di se stesso; facciamo vedere che ciò vale anche per gli iperbolici:

Lemma 1.12.1. *Se il corpo non ha caratteristica 2, ogni sottospazio isotropo massimale di uno spazio iperbolico è l'ortogonale di se stesso.*

Dim. Sia V iperbolico, e $V = V_1 \oplus V_2$, con V_1, V_2 isotropi e duali l'uno dell'altro nella data norma (cfr. 1.9.5). Sia $n = \dim V_1 = \dim V_2$; sia poi U isotropo massimale, di dimensione m. A priori $m \leq n$ (perché U è contenuto in $U^\perp$); se si dimostra che $m = n$, resta dimostrato che $U = U^\perp$. Sia per assurdo $m < n$, e sia $W = V_1 \cap U$, $r = \dim W$. Se fosse $r = m$, si avrebbe $U \subset V_1$ (il segno $\subset$ vuol dire propriamente contenuto), ed U non sarebbe massimale. Quindi $r < m$ e $W \subset U$; pongasi

$$U = W \oplus W', \qquad W' \text{ non vuoto.}$$

La relazione $V = V_1 \oplus V_2$ dà le due proiezioni pr_1 e pr_2 su V_1 e V_2; sia allora Z l'ortogonale in V_1 della $pr_2 W'$; così W è ortogonale a W' (perché sono ambedue nell'isotropo U) ed a $pr_1 W'$ (perché sono ambedue nell'isotropo V_1), e quindi è anche ortogonale a $pr_2 W'$ (perché un $w' \in W'$ è $w' = pr_1 w' + pr_2 w'$). Di conseguenza W è in V_1, ed è ortogonale a $pr_2 W'$ onde $W \subseteq Z$, e certamente $W \subset Z$, perché $\dim W = r$ e

$$\dim Z = n - \dim pr_2 W' \geq n - \dim W' = n - (\dim U - \dim W) = n - m + r > r.$$

Esiste quindi uno $z \in Z$ che $\notin W$; questo è isotropo (perché è in V_1), è ortogonale a W (stesso motivo), è ortogonale a $pr_2 W'$ (perché è in Z), ed è ortogonale a $pr_1 W'$ (perché sia z che $pr_1 W'$ sono in V_1). Perciò z è ortogonale a W' ed anche a W, ossia è ortogonale ad U. Ma allora $U + \langle z \rangle$ è isotropo ed è più grande di U, perché z, essendo in V_1, ma non in W, non è in U. ciò contrasta con la massimalità di U. C.V.D. $\square$

Lemma 1.12.2. *Se il corpo non ha caratteristica* 2*, uno spazio normato* $V = V_i \boxplus V_e$*, con* V_i *iperbolico e* V_e *ellittico non nullo, non è iperbolico.*

Dim. Sia $V_i = U \oplus U'$, con U, U' isotropi duali l'uno dell'altro nella norma. Dico che U è isotropo massimale anche in V. Se infatti $u \oplus u' \oplus e$ (con $u \in U$, $u' \in U'$, $e \in V_e$) è isotropo e ortogonale ad U, dall'essere $(u \oplus u' \oplus e) \circ u_1 = 0$ per ogni $u_1 \in U$, segue $u' = 0$; e da $(u \oplus e) \circ (u \oplus e) = 0$ segue $e \circ e = 0$, onde $e = 0$. Quindi $u \oplus u' \oplus e = u \in U$.

Se ora V fosse iperbolico, scatterebbe il (1.12.1): U sarebbe l'ortogonale di se stesso in V, e si avrebbe $\dim V = 2 \dim U = \dim V_i$, assurdo perché $\dim V_e \neq 0$. C.V.D. $\square$

Teorema 1.12.3. *Se la caratteristica del corpo non è* 2*, ogni spazio normato è somma ortogonale di uno ellittico ed uno iperbolico.*

Dim. Siano V lo spazio, U un suo sottospazio isotropo massimale, $U^\perp$ l'ortogonale di U in V, e V_e un complementare di U in $U^\perp$. Allora V_e non ha elementi isotropi non nulli, e quindi è normato (1.11.1) ellittico. Se allora $V_i = V_e^\perp$ (in V), è $U \subseteq V_i$, e

$$\begin{aligned} \dim V_i = \dim V - \dim V_e &= \dim V - (\dim U^\perp - \dim U) = \\ &= \dim V - (\dim V - \dim U) + \dim U = 2 \dim U. \end{aligned}$$

Pertanto U è l'ortogonale di se stesso in V_i, e V_i è normato iperbolico. Ne segue che $V_i \cap V_e = \langle 0 \rangle$, ed un computo di dimensioni dice che $V = V_i \boxplus V_e$. C.V.D. $\square$

1.13 Lezione 13

La decomposizione descritta nel Teorema 1.12.3 è chiaramente non unica; la stessa scelta di V_e (che ha il solo dovere di essere complementare di qualcosa) lo mostra. Vogliamo però far vedere che è unica a meno di isometrie.

Lemma 1.13.1. *In caratteristica diversa da* 2*, due spazi normati ellittici* V*,* W *sono isometrici se, e solo se,* $V \boxminus W$ *è iperbolico.*

Dim. Il "solo se" discende dal (1.10.1). Per il "se", sia U sottospazio di $V \boxminus W$ che sia l'ortogonale di se stesso; vogliamo intanto mostrare che $\dim V = \dim W$ ($= \dim U$). Se fosse per esempio $\dim V > \dim W$, si avrebbe $\dim U + \dim V > \dim (V \boxminus W)$, onde $U \cap V \neq \langle 0 \rangle$. Questo spazio sarebbe ellittico (come sottospazio dell'ellittico V) e isotropo (come sottospazio di U), assurdo. Si è così visto che $\dim V = \dim W = \dim U$.

Ora $U \oplus V = U \oplus W = V \boxminus W$, e quindi U (sottinsieme di $V \times W$) è un'applicazione biunivoca f di V su tutto W: precisamente l'applicazione che a $v \in V$ fa corrispondere l'unico $w \in W$ tale che $v \oplus w \in U$. L'essere U isotropo dice che f è isometria: $0 = (v \oplus w) \circ (v' \oplus w') = v \circ v' - w \circ w'$. C.V.D. □

Teorema 1.13.2 (di estensione delle isometrie - Ernst Witt)**.** *Sia* V *uno spazio normato su un corpo di caratteristica diversa da* 2*; sia* U *un sottospazio di* V*, non necessariamente normato, e sia* f *una isometria di* U *su* V *(naturalmente non su tutto* V*, ma semplicemente su* fU*). Allora esiste una trasformazione ortogonale* g *di* V *tale che* $gu = fu$ *per* $u \in U$*.*

Dim. Diremo semplicemente che "la f è estendibile ad una isometria g di V". Fra gli spazi $U' \subseteq V$, ma contenenti U, ai quali f è estendibile ve ne sarà uno massimale; possiamo supporre che questo sia lo stesso U. La dimostrazione si articola poi in tre passi.
(a) Dico che U è normato: se infatti il nucleo di "$\circ$" in U contiene un $u \neq 0$, sia W complementare di $\langle u \rangle$ in U. Sia $v \in V$ ortogonale a W e tale che $v \circ u = 1$; allora $v \notin U$ (perché U è ortogonale ad u), e col metodo usato nella dimostrazione del Teorema 1.9.1 questo v può essere trovato anche isotropo. Sia v' analogamente legato ad fU, fu, fW; si può allora estendere $f : U \to fU$ ad una $f' : U \oplus \langle u \rangle \to fU \oplus \langle v' \rangle$ col richiedere che $f'v = v'$. Ma ciò contrasta con la massimalità di U.
(b) Sia $Z = U^\perp$ (in V) e sia $Z' = (fU)^\perp$ (in V). per (a), Z e Z' sono normati, e complementari in V di U, fU rispettivamente. Per (1.12.3) si può scrivere $Z = Z_i \boxplus Z_e$, $Z' = Z_i' \boxplus Z_e'$; voglio dimostrare che Z_e, Z_e' sono isometrici, per il che, a norma del (1.13.1), basta dimostrare che $Z_e \boxminus Z_e'$ è iperbolico. E infatti, $V \boxminus V = (U \boxminus fU) \boxplus (Z \boxminus Z')$, e $Z \boxminus Z' = Z_i'' \boxplus Z_e''$. Allora $V \boxminus V = (U \boxminus fU) \boxplus Z_i'' \boxplus Z_e''$; ma $V \boxminus V$ e $U \boxminus fU$ sono iperbolici per (1.10.1); tale è allora $(U \boxminus fU) \boxplus Z_i''$; il (1.12.1) comporta dunque che $Z_e'' = \langle 0 \rangle$, ossia che $Z \boxminus Z'$ è iperbolico. Ne segue che anche $(Z_i \boxminus Z_i') \boxplus (Z_e \boxminus Z_e')$ è iperbolico, e il solito ragionamento ci dice che $Z_e \boxminus Z_e'$ è iperbolico, come voluto.
(c) Se Z_e e Z_e' sono isometrici, tali sono anche Z, Z', visto che hanno la stessa dimensione. Sia f' una isometria di Z su tutto Z'; ora la $f : U \to fU$ può essere estesa ad una $g : V = U \boxplus Z \to fU \boxplus Z' = V$ così: $g(u \oplus z) = fu \oplus f'z)$. C.V.D. □

Si noti che questo finale dice che in realtà doveva essere fino da principio $U = V$, $Z = 0$.

Possiamo terminare con il

Teorema 1.13.3. *Se V èspazio normato su un corpo di caratteristica diversa da 2, e se come nel (1.12.3) si scrive $V = V_i \boxplus V_e = V'_i \boxplus V'_e$, con V_i, V'_i iperbolici e V_e, V'_e ellittici, esiste una trasformazione ortogonale f di V tale che $fV_i = V'_i$, $fV_e = V'_e$.*

Dim. Per (1.10.1), $V \boxminus V$ è iperbolico; ma $V \boxminus V = (V_i \boxminus V'_i) \boxplus (V_e \boxminus V'_e)$, onde, per (1.12.2), anche $V_e \boxminus V'_e$ è iperbolico; ma allora, per (1.13.1), esiste una isometria f di V_e su tutto V'_e; questo dice intanto che V_e e V'_e hanno la stessa dimensione, il che a sua volta comporta che anche V_i e V'_i hanno la stessa dimensione; perciò c'è una isometria g di V_i su tutto V'_i. La $f \boxplus g$ è quella chiamata f nell'enunciato. C.V.D. □

1.14 Lezione 14

Siamo così ridotti, per classificare tutti gli spazi normati, alla classificazione degli ellittici. "Classificare" in Matematica significa nella migliore delle ipotesi dare una regola per costruirli tutti, e per riconoscere se due distinti sono o no la stessa cosa (isometrici, nel caso presente). Questo traguardo è raramente raggiunto, ed allora ci si contenta di classificare certi enti col dire (ossia dimostrare) che essi sono in corrispondenza biunivoca con enti già noti, o più facili da studiare. Per questo è spesso utile riuscire a presentare le strutture in istudio sotto "forma canonica", che vuol dire forma di tipo prestabilito, di facile ispezione e confronto. Vediamo il caso degli spazi normati; intanto, un tale ente è uno spazio con una norma; siccome ci sono gli spazi senza norme, ma non le norme senza spazi, parleremo di classificazione delle norme. Poniamo due norme f, g sul corspo C (di caratteristica non 2) nella stessa classe se, e solo se, le loro componenti ellittiche sono isometriche, ed indichiamo con $[f]$ la classe di f; ogni classe contiene una norma ellittica, unica a meno di isometrie. Se W_C è l'insieme delle classi di norme sul corpo C, in W_C si può definire l'operazione $+$ così: $[f] + [g] = [f \boxplus g]$ (verificare che è una buona definizione!). È associativa e commutativa; c'è uno 0 (zero), che è la classe $[0]$ costituita da tutte le norme iperboliche; c'è $-[f] = [\boxminus f]$. Insomma W_C è un gruppo abeliano, il *gruppo di Witt* di C; in generale è arduo il calcolarlo, ma alcuni casi sono semplici (ed ecco visto un esempio di classificazione mediante riduzione a qualcosa di già studiato; in questo caso, un gruppo).

Per esempio, se C è algebricamente chiuso, ogni norma ha basi ortonormali (1.11.3), e quindi tutti gli spazi normati della stessa dimensione sono isometrici: iperbolici se di dimensione pari, e somma ortogonale di un iperbolico e di uno ellittico di dimensione 1 se di dimensione dispari. Quindi:

1.14.1. *Se C è algebricamente chiuso e di caratteristica non 2, il gruppo di Witt W_C è isomorfo al gruppo $\{0, 1\}$, con $1 + 1 = 0$.*

Altro caso facile è quello dei *corpi ordinati*: si chiama così un corpo C che come gruppo additivo sia un gruppo ordinato, e tale inoltre che il prodotto di due positivi sia positivo; ne segue subito che più per meno fa meno, che meno per meno fa più, e che i quadrati (eccetto lo zero) e le loro somme sono positivi; hanno certamente caratteristica 0. Per questi il risultato è meglio espresso direttamente sugli spazi normati:

Teorema 1.14.2 (di Sylvester o Regola d'inerzia)**.** *Sia V spazio normato sul corpo ordinato C; esistono allora degli interi m, n, con $m + n = \dim V$, tali che ogni base ortogonale di V contenga n elementi v per i quali $v \circ v > 0$, ed m per i quali $v \circ v < 0$.*

Dim. Siano $\{v_1, \ldots, v_{n+m}\}$, $\{w_1, \ldots, w_{r+s}\}$ due basi ortogonali, con $v_i \circ v_i > 0$ se $i \leq n$, e < 0 se $i > n$, e con $w_i \circ w_i > 0$ se $i \leq r$, e < 0 se $i > r$; occorre dimostrare che $r = n$. Dico che i vettori $v_1, \ldots, v_n, w_{r+1}, \ldots, w_{r+s}$ sono linearmente indipendenti. Se infatti

$$\sum_{i=1}^{n} x_i v_i = \sum_{j=r+1}^{r+s} y_j w_j,$$

moltiplicando (ossia tondinando) ciascun membro per se stesso si ottiene

$$\sum_{i=1}^{n} x_i^2 v_i \circ v_i = \sum_{j=r+1}^{r+s} y_j^2 w_j \circ w_j;$$

il primo membro è non negativo, il secondo nonpositivo, onde sono ambedue nulli. Ma allora $x_i^2 = y_j^2 = 0$ per l'ordinamento. Ciò dimostra che $n + (n + m - r) \leq n + m$, ossia che $n \leq r$; analogamente $n \geq r$, onde $n = r$. C.V.D. □

Nelle notazioni del Teorema 1.14.2, l'intero $n - m$ dicesi *indice d'inerzia* della norma, o dello spazio od anche della forma quadratica legata alla norma.

Corollario 1.14.3. *Notazioni come nel (1.14.2); se C ha anche la proprietà che ogni suo elemento positivo è un quadrato (come il corpo reale), esistono basi ortogonali tali che $v \circ v = \pm 1$ per ogni loro elemento.*

Dim. Nel (1.14.2) basta dividere ogni v per $(v \circ v)^{1/2}$ se $v \circ v > 0$, o per $(-v \circ v)^{1/2}$ se $v \circ v < 0$ C.V.D. □

Quest'ultimo dice che

Corollario 1.14.4. *Se C è come nel Corollario 1.14.3, il gruppo di Witt W_C è isomorfo al gruppo additivo degli interi razionali.*

Tutte queste cose possono essere dette in termini di matrici o di forme quadratiche, nel qual caso non è più necessario fare l'ipotesi di nondegenerazione che è necessaria per le norme. Sappiamo che una forma quadratica, o una bilineare simmetrica, è determinata dalla propria matrice; e che due forme quadratiche sono isometriche, ossia trasformabili l'una nell'altra mediante sostituzione lineare delle indeterminate, se, e solo se, le loro matrici sono congruenti, e cioè legate dalla $B = P^* A P$ con P invertibile. Ora gli (1.11.3), (1.8.3), (1.14.2), (1.14.3) possono essere riuniti nel seguente

Teorema 1.14.5. *Ogni matrice quadrata simmetrica A ad elementi in un corpo C di caratteristica diversa da 2 è congruente, su C, ad una matrice diagonale, detta la forma canonica per congruenza di A; il numero degli zeri sulla diagonale è invariante, ossia è lo stesso per tutte le forme canoniche di A. Se C è ordinato sono invarianti anche il numero degli elementi diagonali positivi e quello degli elementi diagonali negativi. Se C è algebricamente chiuso, tutti gli elementi diagonali non nulli possono essere scelti uguali ad 1. Se infine C è ordinato, ed ogni suo elemento positivo è un quadrato, vi sono forme canoniche (di Sylvester) in cui gli elementi diagonali assumono solo i valori 0, 1, -1.*

Questo si collega con altre considerazioni: sia C ordinato, e sia

$$f(x) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j \qquad (\text{con } a_{ij} = a_{ji})$$

una forma quadratica vista come polinomio. Se alle x si danno valori y in C, la $y \mapsto f(y)$ è un'applicazione di $C \times \cdots \times C$ in C (funzione di n variabili indipendenti); bene, la forma quadratica è detta:

- *definita positiva* (risp. *negativa*) se $f(y) > 0$ (risp. $f(y) < 0$) per ogni $y \neq 0$;
- *semidefinita positiva* (risp. *negativa* se $f(y) \geq 0$ (risp. $f(y) \leq 0$) per ogni $y \neq 0$;
- *indefinita* negli altri casi.

Al lume del (1.14.5) si può dire che:

1. La forma è definita positiva (risp. negativa) se, e solo se, tutti gli elementi diagonali di una forma canonica per congruenza della sua matrice sono positivi (risp. negativi);
2. La forma è semidefinita positiva (risp. negativa) se, e solo se, tutti gli elementi diagonali di una forma canonica per congruenza della sua matrice sono ≥ 0 (risp. ≤ 0).

Attenzione le norme legate a forme quadratiche definite (positive o negative) sono ovviamente tutte ellittiche; se in C ogni elemento positivo è un quadrato, anche il reciproco è vero; ma in altri corpi può essere falso: per esempio, sul corpo razionale, la forma di matrice $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -2 \end{smallmatrix}\right)$ è ellittica ma non definita! È utile poter riconoscere la definitezza della matrice data senza dover prima trasformarla a forma canonica; il risultato che segue raggiunge appunto questo scopo, e mostra fra l'altro che la definitezza dipende solo dai coefficienti della forma (mentre è chiaro che l'ellitticità dipende anche dal corpo nel quale essi si considerano immersi, e può quindi cambiare con l'ingrandirsi di questo corpo). Ricordiamo che un *minore principale* della matrice quadrata A è il determinante di una matrice B ottenuta da A cancellandovi certe righe e le colonne con gli stessi indici; e una *catena* di tali minori è costituita di $\det B_1, \det B_2, \ldots, \det B_n$, ove B_i ha ordine i (onde $B_n = A$), e B_i è ottenuta da B_{i+1} cancellando una riga e la corrispondente colonna. Ed allora:

Teorema 1.14.6. *Sia C un corpo ordinato, sia f una forma quadratica su C e ne sia A la matrice in una certa base. Allora f è definita positiva se, e solo se, una, e quindi ogni, catena di minori principali di A è costituita di numeri positivi. È definita negativa se $-f$ è definita positiva.*

Dim. Sia f definita positiva e sia $\{v_1, \ldots, v_n\}$ base di V; in $\langle v_1, \ldots, v_i\rangle$ la f induce una forma definita positiva, la cui matrice A_i è estratta dalle prime i righe e colonne della A; pertanto la A_i ha una forma canonica $B_i = P_i^* A_i P_i$ ad elementi diagonali tutti positivi. Ma allora $\det A_i = \det B_i (\det P)^{-2} > 0$.

Reciprocamente, sia f non definita positiva, e sia i il minimo intero tale che la f non sia definita positiva su $\langle v_1, \ldots, v_i\rangle$; lo è però su $\langle v_1, \ldots, v_{i-1}\rangle$, onde A_{i-1} ha forma canonica $B_{i-1} = P_{i-1}^* A_{i-1} P_{i-1}$ ad elementi diagonali positivi. Posto $P_i = \left(\begin{smallmatrix} P_{i-1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$ (di ordine i), la $B_i = P_i^* A_i P_i$ è matrice non definita positiva; ma esiste una sua forma canonica $\begin{pmatrix} B_{i-1} & 0 \\ 0 & b_i \end{pmatrix}$ (dimostrarlo!), onde $b_i \leq 0$ e $\det B_i' \leq 0$, che a sua volta comporta $\det B_i \leq 0$, $\det A_i \leq 0$. C.V.D. □

1.15 Lezione 15

Vi è la nozione di "orientamento" di uno spazio (anche non vettoriale), che in realtà è una nozione di tipo topologico: qui la esporremo in modo algebrico per alcuni casi particolari.

Caso di uno spazio vettoriale V su un corpo ordinato C Fra le *basi ordinate* di V poniamo una relazione di equivalenza (che può essere chiamata *equiorientamento*) col definire

$$(v_1, \ldots, v_n) \sim (w_1, \ldots, w_n) \quad \text{se, e solo se,} \quad \frac{v_1 \wedge \cdots \wedge v_n}{w_1 \wedge \cdots \wedge w_n} > 0;$$

qui, quel rapporto significa $\det f$ se f è l'endomorfismo dato da $f w_i = v_i$. Se L_1, L_2 sono le due classi in cui le basi ordinate vengono suddivise dalla relativa partizione, L_1 ed L_2 sono i due *orientamenti* di V, e V stesso, dotato di uno di essi, è uno *spazio vettoriale orientato*; si noti che in questo caso lo spazio non era supposto normato.

Caso di uno spazio vettoriale normato V con basi ortonormali su un corpo C di caratteristica $\neq 2$ Fra le basi ordinate ortonormali di V poniamo ancora una relazione di equivalenza $\sim$ col definire $(v_1, \ldots, v_n) \sim (w_1, \ldots, w_n)$ se, e solo se, la f del caso precedente, che ora sarà ortogonale, è unimodulare. Valgono le altre definizioni come nel caso precedente; se C è anche ordinato, e V ha basi ortonormali, le due definizioni non si contraddicono.

In ambo i casi è piuttosto ovvio lo stabilire quand'è che un automorfismo f di V ha diritto ad essere chiamato *orientato*, ossia quand'è che f *conserva l'orientamento*: dovra essere $\det f > 0$ nel primo caso, e nel secondo f dovrà essere trasformazione ortogonale unimodulare. Tuttavia in matematica, ingenerale, non appena si è definito un oggetto con una certa struttura ci si pone il problema di definire i sottooggetti che ereditano quella struttura; nel caso presente non è affatto chiaro come un sottospazio di uno spazio orientato V riceva automaticamente un orientamento, neppure nel caso più semplice di sottospazi di dimensione 1 (nel qul caso l'orientamento si chiama anche il *verso*). Questa non chiarezza rispecchia il fatto che non è possibile; il significato di ciò (guardarselo bene, ché le dimostrazioni di impossibilità, di cui questa è un caso minimo, sono state le ultime arrivate nello sviluppo logico dell'uomo) sarà chiarito dall'esempio seguente: spazio di dimensione 3, con orientamento L contenente base ordinata (u, v, w); sottospazio $\langle u, v\rangle$; endomorfismo $f : \begin{cases} u \mapsto v \\ v \mapsto u \\ w \mapsto -w \end{cases}$. Questo f manda L su L ma manda l'orientamento (u, v) nel (v, u).

Torniamo alle definizioni; nel secondo caso (spazio normato con basi ortonormali) si può dire di più. Scelto un orientamento L, sia $(v_1, \dots, v_n)$ una base ortonormale ordinata che gli appartiene; se $(x_1, \dots, x_n)$ è una n-upla ordinata di vettori, il numero

$$(x_1 \wedge \cdots \wedge x_n) \circ (v_1 \wedge \cdots \wedge v_n) = \frac{x_1 \wedge \cdots \wedge x_n}{v_1 \wedge \cdots \wedge v_n} \qquad \text{(cfr.1.5.7)}$$

è indipendente dalla scelta di $(v_1, \dots, v_n)$ in L. Tale numero dicesi il *volume* della n-upla ordinata $(x_1, \dots, x_n)$, ed indicasi con $|x_1, \dots, x_n|$; *area* se $n = 2$, *lunghezza* se $n = 1$. Esso cambia di segno se si cambia l'orientamento.

Teorema 1.15.1. *Nelle ipotesi precedenti, si ha*

$$|x_1, \dots, x_n|^2 = (x_1 \wedge \cdots \wedge x_n) \circ (x_1 \wedge \cdots \wedge x_n).$$

Dim. Se infatti c è il volume, si ha

$$c^2 = (x_1 \wedge \cdots \wedge x_n) \circ c(v_1 \wedge \cdots \wedge v_n) = (x_1 \wedge \cdots \wedge x_n) \circ (x_1 \wedge \cdots \wedge x_n).$$

C.V.D. □

Il (1.15.1) suggerisce che se si ha uno spazio normato V anche senza orientamento, di dimensione n, e se $(x_1, \dots, x_n)$ è una r-upla di suoi vettori, con r qualsiasi, si può chiamare *quadrato del suo volume* ed indicare con $|x_1, \dots, x_r|^2$ il numero $(x_1 \wedge \cdots \wedge x_r) \circ (x_1 \wedge \cdots \wedge x_r)$. Per computarlo in pratica quando V ha basi ortogonali si procede così: sia

$$x_1 \wedge \cdots \wedge x_r = \sum_s a_s v_{s_1} \wedge \cdots \wedge v_{s_r},$$

ove $\{v_1, \dots, v_n\}$ è una base ortonormale di V, ed $(s_1, \dots, s_r$ percorre tutti i sottoinsiemi ordinati di $\{1, \dots, n\}$ di cardinalità r. Allora (avendosi una base ortonormale)

$$(1.15.2) \quad |x_1, \ldots, x_r|^2 = \sum_s a_s^2 (v_{s_1} \wedge \cdots \wedge v_{s_r}) \circ (v_{s_1} \wedge \cdots \wedge v_{s_r}) = \\ = \sum_s a_s^2 (v_{s_1} \circ v_{s_1}) \cdots (v_{s_r} \circ v_{s_r}).$$

Se infine gli x_i sono dati mediante la stessa base, per esempio $x_i = \sum_j b_{ji} v_j$, il numero a_s della (1.15.2) si ottiene così:

$$x_1 \wedge \cdots \wedge x_r = \left(\sum_{j_1} b_{j_1 1} v_{j_1} \right) \wedge \cdots \wedge \left(\sum_{j_r} b_{j_r r} v_{j_r} \right) = \\ = \sum_j b_{j_1 1} \cdots b_{j_r r}\, v_{j_1} \wedge \cdots \wedge v_{j_r} = \sum_s B_s v_{s_1} \wedge \cdots \wedge v_{s_r},$$

ove l'indice j è "disordinato" mentre s è, come prima, ordinato, e ove B_s è il minore delle righe indicizzate da s nella matrice le cui colonne sono le $\begin{pmatrix} b_{1i} \\ \vdots \\ b_{ni} \end{pmatrix}$; perciò $a_s = B_s$.

Forse non è superfluo notare che se la base è ortonormale, la (1.15.2) esprime il fatto che il quadrato del volume è la somma dei quadrati dei volumi delle proiezioni della r-upla data sui sottospazi $\langle v_{s_1}, \ldots, v_{s_r} \rangle$; per $r = 1$ ed $n = 2$ questo è il *teorema di Pitagora*.

Chiudiamo con un collegamento col calcolo vettoriale "pratico": nel solito spazio tridimensionale vi è il "prodotto scalare" di due vettori, indicato con $v \times w$ in Italia e con $v \cdot w$ all'estero (e chiamato *dot product* in inglese); esso non è altro che una norma definita positiva (sui reali), e quindi lo indicheremo col solito tondino; lo spazio può essere ora orientato mediante uno dei due orientamenti. Vi è poi il "prodotto vettoriale o esterno", indicato con $v \wedge w$ in Italia e con $v \times w$ all'estero (e chiamato *cross product* in Inglese), e che ovviamente non è un prodotto esterno nel nostro senso; lo indicheremo con $v \bar{\wedge} w$; che cosa esso sia può essere ricostruito tenendo presente che $u \circ v \bar{\wedge} w$ deve essere il volume di (u, v, w); si ottiene allora:

1.15.3. *Esiste un unico isomorfismo g di E_2 su tutto V tale che $|x, y, z| = x \circ g(y \wedge z)$; quindi $y \bar{\wedge} z = g(y \wedge z)$.*

Dim. Sappiamo che E_2 ha dimensione 3, e che è l'insieme di tutti gli $y \wedge z$ (cfr. Teorema 1.6.4); perciò la $(x, y \wedge z) \mapsto |x, y, z|$ è un'applicazione bilineare di $V \times E_2$ su C. Quindi per ogni scelta di $y \wedge z$ l'applicazione precedente è un elemento di $\mathrm{Hom}_C(V, C)$; ma data la autodualità "$\circ$" di V, questo elemento di $\mathrm{Hom}_C(V, C)$ sarà della forma $v \circ -$, con $v \in V$ dipendente da $y \wedge z$. Se questo v lo chiamiamo appunto $g(y \wedge z)$, la g è lineare e soddisfa la $|x, y, z| = g(y \wedge z) \circ x$. C.V.D. $\square$

1.16 Lezione 16

Premettiamo che se V, U sono spazi vettoriali su corpi C, F, e se $p : c \mapsto c^p \in F$ è un isomorfismo di C su tutto F (scritto come esponente anziché come moltiplicatore a sinistra), un'*applicazione p-semilineare* di V su U è una $f : V \to U$ tale che $f(v + v') = fv + fv'$ e $f(cv) = c^p fv$ per $c \in C$. Se p è l'identità si ricasca nelle solite lineari. La *trasposizione semilineare* è simile alla solita e funziona così:

$$(v \circ f^* u^*)^p = fv \circ u^*. \tag{1.16.1}$$

La f^* è p^{-1}-semilineare

Bene; se p è un automorfismo di C (onde $F = C$ ma p non è necessariamente l'identità), un'applicazione g di $V \times V$ su C che sia lineare nel primo argomento e p-semilineare nel secondo dicesi *p-sesquilineare* (letteralmente, lineare una volta e mezzo). Se essa è nondegenere (solita definizione) la possiamo indicare con $(x, y) \mapsto x \circ y$, ma questa "$\circ$" non è una autodualità, ma una *dualità sesquilineare*. Non si può ovviamente pretendere che essa sia simmetrica; se però p è tale che $p^{-1} = p$, ossia che $p^2 = \iota$, si può richiedere che la dualità sesquilineare sia *hermitiana*, ossia tale che $y \circ x = (x \circ y)^p$; se questo accade si ha, come nel caso simmetrico, che coincidono i due trasposti f^* ed $\tilde{f}$ di un $f \in \mathrm{End}_C V$ dati da $f^* x \circ y = x \circ fy$, $x \circ \tilde{f} y = fx \circ y$ (infatti: $f^* x \circ y = x \circ fy = (fy \circ x)^p = (y \circ \tilde{f} x)^p = (\tilde{f} x \circ y)^{p^2} = \tilde{f} x \circ y$. Si noti però che per $c \in C$ si ha $(cf)^* = c^p f^*$; si noti anche che in una hermitiana il $v \circ v$ appartiene sempre al sottocorpo di C *invariante* per p, ossia formato dai c tali che $c^p = c$.

Di importanza particolare sono le hermitiane nel caso in cui C è il corpo complesso, e p è il *coniugio*: $c^p = \bar{c} =$ complesso coniugato di c; in tal caso $v \circ v$ è sempre nel corpo reale. Non faremo uno studio dettagliato delle hermitiane, ma come collegamento con altre teorie presentiamo un esempio fondamentale che ha però il difetto che lo spazio vettoriale che si costruisce ha dimensione infinita. Dobbiamo premettere il

Lemma 1.16.2 (di Schwarz)**.** *Siano $a_1, \dots, a_n, b_1, \dots, b_n$ numeri complessi; allora*

$$\left| \sum_i a_i \bar{b}_i \right|^2 \leq \left(\sum_i |a_i|^2 \right) \left(\sum_i |b_i|^2 \right).$$

(Qui il simbolo $|\ \ |$ significa valore assoluto).

Dim. Pongasi $k = \left(\sum_i a_i \bar{b}_i\right) \left|\sum_i a_i \bar{b}_i\right|^{-1}$, onde $|k| = 1$. Per x, y reali si ha:

$$0 \leq \sum_i |x\bar{k} a_i + y b_i|^2 = \sum_i (x\bar{k} a_i + y b_i)(xk\bar{a}_i + y\bar{b}_i) =$$

$$= x^2 \sum_i |a_i|^2 + 2xy \left| \sum_i a_i \bar{b}_i \right| + y^2 \sum_i |b_i|^2.$$

Il secondo membro è una forma quadratica in $\mathbb{R}[x, y]$ ($\mathbb{R}$ è il corpo reale), ed è semidefinita positiva; quindi, per (1.14.6, è non negativo il determinante della sua matrice ossia il

$$\left(\sum_i |a_i|^2\right)\left(\sum_i |b_i|^2\right) - \left|\sum_i a_i \bar{b}_i\right|^2 .$$

C.V.D. □

Naturalmente si sarebbe potuto usare un criterio per le equazioni di secondo grado, che è poi la stessa cosa.

Ciò premesso, sia $\mathscr{H}$ l'insieme delle successioni $a = (a_n)_{n\in\mathbb{N}}$ di numeri complessi, tali che $\sum_{n\in\mathbb{N}} |a_n|^2$ esista (finito), ossia converga. Scriviamo $ca = (ca_n)_{n\in\mathbb{N}}$ per $c \in \mathbb{C}$ (corpo complesso), e $a + b = (a_n + b_n)_{n\in\mathbb{N}}$. Questa ha senso se si dimostra che $\sum_{n\in\mathbb{N}} |a_n + b_n|^2$ converge; ma

$$\sum_{k=1}^{n} |a_k + b_k|^2 = \sum_{k=1}^{n} (a_k + b_k)(\bar{a}_k + \bar{b}_k) \leq \sum_{k=1}^{n} |a_i|^2 + \sum_{k=1}^{n} |b_i|^2 + 2\left|\sum_{k=1}^{n} a_k \bar{b}_k\right| ,$$

che per (1.16.2) è minore o uguale di

$$\sum_{k=1}^{n} |a_i|^2 + \sum_{k=1}^{n} |b_i|^2 + 2\left(\left(\sum_{k=1}^{n} |a_i|^2\right)\left(\sum_{k=1}^{n} |b_i|^2\right)\right)^{1/2} ,$$

che è tutta roba limitata quando n tende ad infinito.

Definiamo infine

$$a \circ b = \sum_{n\in N} a_n \bar{b}_n ,$$

che di nuovo esiste per (1.16.2). Questo $\mathscr{H}$ è ora uno spazio vettoriale su $\mathbb{C}$, di dimensione infinita (le $(0, \dots, 0, 1, 0, \dots)$ ne sono una *base topologica*[4], e l'applicazione $(a, b) \mapsto a \circ b$ è una norma hermitiana su $\mathscr{H}$ rispetto al coniugio. Questo $\mathscr{H}$ normato è lo *spazio di Hilbert*. La sua utilità sta in un'altra costruzione che è tipicamente non algebrica e non geometrica, e che tuttavia dà un oggetto algebrico e geometrico. Sia $\mathscr{H}'$ l'insieme di tuttle le funzioni complesse $f(x)$ di variabile reale, definite in un certo intervallo I, e che in I sono *a quadrato sommabile*, e cioè tali che $\int_I |f(x)|^2 dx$ esiste; qui l'integrazione usata deve essere quella di Lebesgue, un po' più generale di quella di Riemann–Mengoli–Cauchy del programma di II anno. Tale $\mathscr{H}'$ è in modo ovvio uno spazio vettoriale su $\mathbb{C}$ (ovvio se si ammette che la somma di due funzioni a quadrato sommabile sia

[4] Ciò significa che il sottospazio vettoriale di $\mathscr{H}$ da esse generato è *denso* in $\mathscr{H}$; ovvero che ogni elemento di $\mathscr{H}$ è limite di una successione di combinazioni lineari finite di elementi della base topologica. Il limite si considera rispetto alla distanza $d(a, b) = \|a - b\| = \sqrt{(a - b) \circ (a - b)}$, che rende $\mathscr{H}$ uno spazio metrico.

ancora a quadrato sommabile); se si pone $f \circ g = \int_I f(x)\overline{g(x)}dx$ (che si dimostra esistere), la $(f,g) \mapsto f \circ g$ è una forma hermitiana su $\mathscr{H}'$, il cui nucleo è lo spazio $\mathscr{H}_0$ delle $f(x)$ *nulle quasi ovunque*, e cioè tali che $\int_I |f(x)|^2 dx = 0$. Quindi il "$\circ$" induce una norma hermitiana su $\mathscr{H} = \mathscr{H}'/\mathscr{H}_0$. Questo $\mathscr{H}$ è lo stesso (o meglio, è isomorfo a quello) definito prima: ad una f basta far corrispondere la $a = (a_n)_{n\in\mathbb{N}}$ tale che le a_n siano le componenti di f rispetto ad un *sistema ortonormale*[5]. Un tipico sistema ortonormale è quello di Fourier, per esempio, quando I è l'intervallo $(0, 2\pi)$; i suoi elementi sono le immagini $\mod \mathscr{H}_0$, delle $f_n(x) = \frac{1}{\sqrt{2\pi}}\exp(nix)$, per $n = 0, \pm 1, \pm 2, \dots$; qui i significa $(-1)^{1/2}$. Alla immagine di $g(x) \in \mathscr{H}'$ in $\mathscr{H}$ corrisponde la successione $(a_0, a_1, a_{-1}, a_2, a_{-2}, \dots)$, ove

$$a_n = g \circ f_n = \int_0^{2\pi} g(x)\overline{f_n(x)}dx;$$

si ha cioè la *serie di Fourier* $g(x) = \sum_n a_n f_n(x) \mod \mathscr{H}_0$.

1.17 Lezione 17

Uno *spazio affine* di dimensione n sul corpo C è la struttura formata da tutti gli oggetti seguenti:

1. Un insieme S non vuoto;
2. Uno spazio vettoriale T su C, di dimensione n;
3. Un'applicazione $(t, P) \mapsto P + t$, di $T \times S$ su S che gode delle proprietà seguenti:
   a) $P + 0 = P$;
   b) $(P + t) + v = P + (t + v)$;
   c) nella relazione $Q = P + t$, se due dei tre oggetti, P, Q, t, sono dati arbitrariamente, il terzo esiste ed è unico.

Uno spazio affine di dimensione 1, o rispettivamente 2, dicesi *retta affine* o rispettivamente *piano affine*. Si scrive anche $Q - P = t$ in luogo di $Q = P + t$; lo spazio vettoriale T è chiamato il *gruppo astratto delle traslazioni* dello spazio affine; gli elementi di S sono i *punti* dello spazio; inoltre, per brevità, spesso si chiama il solo S "lo spazio affine", sottintendendo T e l'applicazione. Fissato un $P \in S$, la $t \mapsto P + t$ è corrispondenza biunivoca fra tutto T e tutto S; pertanto, non appena sia dato T, si può prendere per S il T stesso, privato della struttura di spazio vettoriale e dotato della sola struttura di differenza di (punti, ossia di) vettori.

---

[5] Ovvero una famiglia numerabile $\{ q_n \mid n \in \mathbb{N} \}$ tale che $q_n \circ q_m = \delta_{mn}$ e che il sottospazio vettoriale da essa generato sia denso in $\mathscr{H}$.

Se (T, S) e (T', S') sono spazi affini sui corpi C, C', un'*applicazione affine* del primo sul secondo è un'applicazione g di S su S' per cui esista un'applicazione p-semilineare f di T su T' (con p isomorfismo opportuno di C su C'), con la proprietà $g(P + t) = gP + ft$; questa f, se esiste, è unica, perché appunto $f(P - Q) = gP - gQ$. La f è iniettiva (risp. suriettiva) se, e solo se, tale è la g (dimostrarlo). Le applicazioni affini di un (T, S) su tutto se stesso, per le quali la f è lineare, si chiamano *affinità*, e chiaramente formano un gruppo. Un *sottospazio affine* di (T, S) è un (T', S'), con T' sottospazio vettoriale di T ed S' sottoinsieme di S, tale che l'immersione di T' in T ed S' in S sia un'applicazione affine; se $P' \in S'$, S' consiste di tutti i $P' + t'$ quando t' percorre T'[6]. Siano (T_1, S_1), (T_2, S_2) sottospazi affini di (T, S); se $S_1 \cap S_2$ contiene un punto P, si ha $S_1 = P + T_1$, $S_2 = P + T_2$, onde $S_1 \cap S_2 = P + (T_1 \cap T_2)$; analogamente, se (T_3, S_3) è il minimo sottospazio affine che contiene i due spazi dati, è $S_3 = P + (T_1 + T_2)$; quindi

$$\dim(S_1 \cap S_2) + \dim S_3 = \dim S_1 + \dim S_2. \tag{1.17.1}$$

Due tali sottospazi (che abbiano cioè un punto in comune) diconsi *incidenti*; diconsi invece *paralleli* se uno dei due spazi vettoriali T_1, T_2 è sottospazio dell'altro; quindi se due sottospazi sono incidenti e paralleli, l'uno sarà sottospazio dell'altro; i due sottospazi affini diconsi infine *sghembi* se non sono né incidenti né paralleli[7] Per spazi non incidenti l'analoga della (1.17.1) è:

$$\dim_C(T_1 \cap T_2) + \dim S_3 = \dim S_1 + \dim S_2 + 1; \tag{1.17.2}$$

in quanto $\dim S_3 = \dim(T_1 + T_2) + 1$.

Un sottospazio di dimensione $n - 1$ di uno spazio affine S di dimensione n dicesi un *iperpiano affine* di S.

Se (T, S) è spazio affine, un *riferimento affine* consiste di una base ordinata $(t_1, \ldots, t_n)$ di T e di un punto O (la lettera O, da distinguere dallo 0 di T) di S; questo si chiama l'*origine* del riferimento. Dato un riferimento affine, ogni punto $P \in S$ è univocamente individuato dalle sue *coordinate affini* o *cartesiane* $x_1, \ldots, x_n$, che sono gli elementi di C tali che $P = O + \sum_i x_i t_i$; quando $n = 1$, l'unica x si chiama anche *coordinata ascissa*; quando $n = 2$, le x_1, x_2, in qualche ordine prestabilito, si chiamano anche, rispettivamente, l'*ascissa* e l'*ordinata*. Per dare un riferimento affine si può dare, anziché O e le t_i, l'insieme ordinato delle rette $R_i = O + \langle t_i \rangle$ ed il punto $U = O + \sum_i t_i$, detto *punto unità*. In tal caso

[6] Anche l'insieme vuoto $\varnothing$ si considera un sottospazio affine (di dimensione -1)

[7] Le definizioni in questo ambito differiscono tra i vari autori. Ad esempio, [B] Marcel Berger, *Geometry*, Springer 1987 (2 voll), non da alcuna definizione in proposito e si limita a parlare di sottospazi affini che si intersecano o sono "paralleli" (quando coincidono i sottospazi direttori) o "debolmente paralleli" (quando sono paralleli secondo la definizione data qui) e non dà nomenclatura per le altre possibili situazioni. Per altri autori, le definizioni di incidenti e paralleli coincidono con le presenti, ma i sottospazi sghembi sono quelli per cui $S_1 \cap S_2 = \varnothing$ e $T_1 \cap T_2 = \langle 0 \rangle$ (e quindi sono sghembe –cioè con intersezione vuota– le loro chiusure nello spazio proiettivo). Personalmente, preferisco quest'ultima definizione a quella data qui da Barsotti.

O si ritrova come intersezione delle R_i (che hanno l'unico dovere di intersecarsi in un punto e di non stare su uno stesso iperpiano), mentre t_i, o meglio $O + t_i$ è l'intersezione di R_i con l'iperpiano passante per U e parallelo all'iperpiano H_i delle R_j con $j \neq i$; quindi U ha l'unico dovere di non stare su nessuno degli H_i; questi sono gli *iperpiani coordinati*, mentre le R_i sono gli *assi coordinati*.

Sia $(x_1, \dots, x_n)$ un sistema di coordinate cartesiane su S, legate ad un riferimento affine $(O, t_1, \dots, t_n)$; un iperpiano H di S sarà costituito dai punti $Q + V$, ove Q è un punto fissato di H e V è sottospazio vettoriale di T di dimensione $n-1$; se $q_1, \dots, q_n$ sono le coordinate di Q, e se $\sum_i a_i t_i^*$ è una base di $V^\perp$ (nel duale T^* di T), si ha che un punto P, di coordinate $x_1, \dots, x_n$, è su H se, e solo se, $P - Q \in V$, ossia se, e solo se, $\sum_i a_i(x_i - q_i) = 0$, e infine, se, e solo se,

$$\sum_{i=1}^{n} a_i x_i = b \qquad (b = \textstyle\sum_i a_i q_i). \tag{1.17.3}$$

La (1.17.3), unica a meno di un fattore moltiplicativo non nullo in C, è l'*equazione* di H nel sistema $(x_1, \dots, x_n)$; e ogni tale relazione, con le a_i non tutte nulle, è l'equazione di un iperpiano; gli iperpiani H, H' sono paralleli se, e solo se, le a_i dell'uno sono proporzionali a quelle dell'altro. Dato che ogni sottospazio affine di S, di dimensione m, è intersezione di $n - m$ iperpiani (cfr. 1.17.1), si comprende che cosa siano le "equazioni di un sottospazio".

Una *metrica* su uno spazio affine (T, S) (che diviene allora uno *spazio affine metrico*) è una norma su T; se "$\circ$" è tale norma, il *quadrato della distanza* fra P e Q (punti si S) è $|P - Q|^2 = (P - Q) \circ (P - Q)$ (cfr. lez. 15); analogamente per i *quadrati dei volumi*. Si noti che la $P - Q \mapsto |P - Q|^2$, per Q fisso, è una forma quadratica su T[8], la quale, se C non ha caratteristica 2, corrisponde proprio alla forma bilineare "$\circ$"; quindi la metrica su S, ossia la norma su T, è determinata non appena sia data l'applicazione sopra descritta, come è giusto che sia per poterla chiamare "metrica".

Se $t_i \circ t_j = a_{ij}$, e se x, y sono le coordinate di P, Q, avremo

$$|P - Q|^2 = \sum_{1 \le i,j \le n} a_{ij}(x_i - y_i)(x_j - y_j); \tag{1.17.4}$$

e se la base è ortogonale:

$$|P - Q|^2 = \sum_{i=1}^{n} a_{ii}(x_i - y_i)^2; \tag{1.17.5}$$

e se è ortonormale:

$$|P - Q|^2 = \sum_{i=1}^{n} (x_i - y_i)^2. \tag{1.17.6}$$

[8] Per essere pignoli, sarebbe $t \mapsto |(Q + t) - Q|^2$, al variare di $t \in T$.

Allo spazio affine si trasferisce, con cautela, la nomenclatura di T: i sottospazi $P + T_1$, $Q + T_2$ sono *ortogonali* se i due spazi T_1, $T_2^\perp$ sono l'uno sottospazio dell'altro (non importa quale di quale), nel qual caso lo stesso vale per T_2 e $T_1^\perp$. Se C è ordinato, se ogni elemento positivo di C è un quadrato, e se la metrica (ossia la norma) è definita positiva, la radice quadrata non negativa di $|P - Q|^2$ è la *distanza* fra P e Q; con essa lo spazio affine metrico diviene uno spazio metrico nel senso della topologia, chiamato *spazio euclideo* (e *metrica euclidea*).

Se C è ordinato, ovvero se C non ha caratteristica 2 e T ha basi ortonormali, un orientamento L di T si chiama un orientamento di (T, S), e questo si chiama uno *spazio affine orientato* (nel secondo caso sarà anche metrico).

1.18 Lezione 18

Passiamo a trattare delle affinità di (T, S); si è visto che sono le applicazioni biunivoche g di S su tutto S per le quali esiste una (unica) $f \in \mathrm{End}_C T$ tale che $gP = gO + f(P - O)$. Queste f sono elementi invertibili di $\mathrm{End}_C T$; il gruppo di tali elementi, detto *gruppo lineare* di dimensione n su C sarà indicato con $\mathrm{GL}(T)$ o con $\mathrm{GL}_n(C)$[9];

Il gruppo delle affinità sarà indicato con $\mathrm{Aff}T$ o con $\mathrm{Aff}_n(C)$. L'affinità g sopra descritta è univocamente determinata col dare f e gO, quando O sia stato fissato; se $gO - O = t$, si ha

$$gP = O + t + f(P - O); \tag{1.18.1}$$

inoltre la $f \in \mathrm{GL}(T)$ ed il $t \in T$ possono essere dati ad arbitrio. Si sono così identificati gli elementi g di $\mathrm{Aff}T$ con le coppie (f, t), ma la identificazione dipende dalla scelta di O; a rigore, si dovrebbe scrivere $g = (f, t)_O$, e lasciamo al lettore verificare che $(f, t)_Q = (f, t + (Q - O) - f(Q - O))_O$; Nel seguito O sarà fisso, e sarà omesso come indice di (f, t). Il (1.18.1) dà la legge di composizione[10] di queste coppie:

$$\begin{aligned}(f,t)(f',t')P &= (f,t)\big(O + t' + f'(P - O)\big) = \\ &= O + t + f(t' + f'(P - O)) = O + t + ft' + ff'(P - O),\end{aligned}$$

onde

$$(f, t)(f', t') = (ff', t + ft'). \tag{1.18.2}$$

Da qui seguono varie conseguenze:

---

[9] La notazione qui usata è ormai (quasi) universalmente diffusa e quindi la troviamo preferibile alla notazione "Lin" e "Lin(C, n)" utilizzata da Barsotti, che aggiunge "questa notazione, come altre analoghe che seguiranno, è mnemonica e ad hoc per questi appunti; non è standard e non è usata nella letteratura".

[10] Quanto segue si potrebbe riassumere dicendo che "la scelta di O definisce un isomorfismo tra $\mathrm{Aff}T$ ed il prodotto semidiretto $T \rtimes \mathrm{GL}(T)$."

1. Il gruppo Aff$T$ contiene il sottogruppo formato dalle $(f, 0)$ che sarà detto il gruppo delle *affinità centrali di centro* O e isomorfo a $\mathrm{GL}(T)$; i suoi elementi sono quei $g \in \mathrm{Aff}T$ per i quali O è punto unito, ossia tale che $gO = O$. L'immagine del gruppo $\mathrm{GL}(T)$ in Aff$T$, pur essendo sempre isomorfa a $\mathrm{GL}(T)$, dipende chiaramente dalla scelta di O.
2. Il gruppo Aff$T$ contiene il sottogruppo formato dalle (ι_T, t), detto delle *traslazioni* (e si tralascia l'aggettivo "astratte" usato per T); tale gruppo è isomorfio a T ed ogni suo elemento, eccetto l'identità ($t = 0$) è privo di punti uniti. Questo sottogruppo è indipendente dalla scelta di O, perché i suoi elementi sono le applicazioni $P \mapsto P + t$, per $t \in T$.
3. L'applicazione $p : (f, t) \mapsto f$ da origine alla sequenza esatta di gruppi

$$0 \to T \xrightarrow{j} \mathrm{Aff}T \xrightarrow{p} \mathrm{GL}(T) \to \{1\}$$

per cui T è isomorfo al nucleo di p e $\mathrm{GL}(T) \cong \mathrm{Aff}T/T$.

Se lo spazio affine è anche metrico, le affinità g per le quali f è trasformazione ortogonale si chiamano *congruenze* o *movimenti rigidi*; l'(1.11.4) e l'(1.18.1), mostrano che se C non ha caratteristica 2 la g è congruenza se, e solo se, $|gP - gO|^2 = |P - O|^2$ per un dato O e per ogni P, ossia se, e solo se, conserva i quadrati delle distanze. Tutte le traslazioni sono congruenze, mentre sono congruenze solo gli elementi di $\mathrm{GL}(T)$ che corrispondono a trasformazioni ortogonali; questi elementi diconsi *rotazioni* di centro O. Le traslazioni conservano l'orientamento (se c'è), mentre le affinità centrali, e in particolare le rotazioni, sono *dirette* se lo conservano (a determinante positivo, oppure unimodulari), e *inverse* altrimenti. Lo scrivere $(f, t) = (1, t)(f, 0) = (f, 0)(1, f^{-1}t)$ (cfr. 1.18.2) comporta che:

Teorema 1.18.3. *Ogni movimento rigido g di uno spazio affine metrico è ottenibile mediante una traslazione seguita da una rotazione di centro O preassegnato; od anche in ordine inverso. La rotazione è univocamente determinata da g (ed anzi l'elemento di* $\mathrm{GL}(T)$ *che le corrisponde non dipende dalla scelta di O), mentre la traslazione dipende da O.*

Chiudiamo coll'esprimere tutto in matrici:
usiamo in S il riferimento $(O, t_1, \ldots, t_n)$; i punti verranno identificati con le matrici $X = \begin{pmatrix} 1 \\ \hline x_1 \\ \vdots \\ x_n \end{pmatrix}$, $x_i \in C$; gli elementi di $\mathrm{GL}(T)$ con matrici in $\mathrm{GL}_n(C)$ ($n \times n$ ed invertibili ad elementi in C), e gli elementi di T con matrici $n \times 1$. Se allora F è la matrice $n \times n$ di f (legata alla base $\{t_1, \ldots, t_n\}$) ed $a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ è il vettore t (onde $a_1, \ldots, a_n$ sono le coordinate cartesiane di $O + t$), dico che $(f, t) \in \mathrm{Aff}T$ può essere rappresentato dalla matrice (a blocchi)

$$B = \begin{pmatrix} 1 & 0 \\ a & F \end{pmatrix}, \tag{1.18.4}$$

nel senso che se $(f,t)X = Y$, allora

$$Y = BX; \tag{1.18.5}$$

provare per credere! Nel capitolo sullo spazio proiettivo si vedrà il vero motivo di quell'1 che sta in cima alle X, Y.

Naturalmente, al solito, la (1.18.5) può essere interpretata, anziché come una affinità, come formula di trasformazione di coordinate: se si ha un nuovo sistema di riferimento $(O', t'_1, \dots, t'_n)$ nel quale la nuova origine, O', ha come vecchie coordinate $-a_1, \dots, -a_n$, e per le quali la nuova base $\{t'_1, \dots, t'_n\}$ di T è legata alla vecchia mediante le $t_i = \sum_j f_{ji} t'_j$ (ove $(f_{ji})_{1 \le j,i \le n} = F$), allora nella (1.18.5) se le x_i sono le vecchie coordinate di un punto, le y_i ne sono le nuove.

2

Spazi proiettivi

2.19 Lezione 19

Lo spazio affine, costruito nella lezione 17, ha alcune peculiarità che lo rendono un po' scabroso da trattare, nel senso che bisogna sempre fare una casistica minuziosa. Per esempio, se S è affine di dimensione 2, e si vuole trovare l'intersezione tra rette (non coincidenti) $ax + by = c$, ed $a'x + b'y = c'$, occorre trovare la soluzione dei sistema delle due equazioni; ora, se il determinante $\left|\begin{smallmatrix} a & b \\ a' & b' \end{smallmatrix}\right|$ è non nullo, ossia quasi sempre, la soluzione c'è e le rette sono incidenti, mentre se è nullo non c'è e le rette sono parallele; una discussione o dimostrazione che dipendesse dalla soluzione di quel sistema dovrebbe essere divisa in due parti separate. Anche topologicamente (se si opera sui reali) lo spazio affine manca di certe proprietà simpatiche: per esempio non è compatto: gli intervalli aperti $\dots, (0, 2), (1, 3), (2, 4), (3, 5), \dots$ ne sono un ricoprimento con aperti che non contiene nessun ricoprimento finito. Ma torniamo alla faccenda delle parallele, e tanto per non ripeterci troppo usiamo il simbolo $\mathbb{A}^n$ in luogo della frase "spazio affine di dimensione n". Se prendiamo due sottospazi H_r, H_s (r ed s sono le rispettive dimensioni) di un $\mathbb{A}^n$, con $r + s \geq n$, dati per esempio da $H_r = P + W_r$, $H_s = Q + W_s$ (con W_r, W_s sottospazi del T delle traslazioni di $\mathbb{A}^n$), le (1.17.1), (1.17.2) dicono che essi si intersecano, salvo il caso di sottospazi paralleli[1] Il parallelismo appare quindi come una vera e propria eccezione, ed in matematica le eccezioni si tenta sempre di eliminarle. Siccome qui quello che manca è un "punto d'incontro", il modo più semplice per trarsi d'impaccio è quello di inventare nuovi punti, la cui specialità sia di stare su coppie di spazi paralleli. Il modo che si presenta spontaneo è il chiamare "punto improprio" di $\mathbb{A}^n$ ogni *direzione* intendendo con ciò l'insieme di tutte le rette parallele ad una data (rette affini, si intende); un sottospazio H_r "contiene" un certo punto improprio se contiene qualcuna di quelle rette parallele (i soliti punti saranno chiamati "propri"). Se si fa questo si

[1] Come, ad esempio, si ha in $\mathbb{A}^5$ con il riferimento $(O, e_1, \dots, e_5)$, considerando i sottospazi $H_3 = O + \langle e_1, e_2, e_3\rangle$ e $K_3 = O + e_5 + \langle e_2, e_3, e_4\rangle$, ove chiaramente è $H_3 \cap K_3 = \varnothing$. Qui si è modificato il testo originale che contiene un'imprecisione e dice "salvo il caso in cui uno dei W_r, W_s è sottospazio dell'altro, ossia salvo il caso di parallelismo".

vede che gli H_r, H_s sopradescritti s'incontrano sempre, e sono paralleli se, e solo se, la loro intersezione è tutta formata da punti impropri. Il discorso potrebbe essere continuato così (e così è nato storicamente), ma non rimedierebbe al guaio di dover sempre considerare una casistica, in quanti i punti impropri e quelli propri dovrebbero essere trattati diversamente. Daremo quindi una definizione che sembra molto diversa, e faremo poi vedere che si tratta della stessa cosa.

Chiameremo *spazio proiettivo* su C (corpo), di dimensione $n \geq -1$, e indicheremo con (S_n, σ), l'ente costituito dai seguenti oggetti:

1. L'insieme $[V_{n+1}]$ di tutti i sottospazi vettoriali di uno spazio vettoriale V_{n+1} su C (l'indice denota la dimensione come sempre nel seguito);
2. Un'applicazione biunivoca σ di $[V_{n+1}]$ su tutto un insieme $S_n = \sigma[V_{n+1}]$.

Al solito, per "elementi" dello spazio proiettivo si intenderanno gli elementi di S_n, cosicché si dirà generalmente "sia S_n uno spazio proiettivo", sottintendendo il σ; ed anzi, talvolta si prenderà semplicemente $S_n = [V_{n+1}]$ e $\sigma = \iota$ (applicazione identica). Ma per non cadere in certe trappole occorre, almeno finché non si ha pratica con l'argomento, tenere ben distinto S_n da $[V_{n+1}]$.

Dato un S_n, i σV_{m+1}, con V_{m+1} sottospazi vettoriali di dimensione $m+1$ di V_{n+1}, sono gli *elementi di dimensione* m *di* S_n; gli elementi di dimensioni $-1, 0, 1, 2, n-1, n$ si chiamano rispettivamente il *vuoto*, i *punti*, le *rette*, i *piani*, gli *iperpiani*, il *sostegno* di S_n; due elementi σV_i, σV_j *si appartengono* se uno dei due spazi V_i, V_j è sottospazio dell'altro. A loro volta, gli S_{-1}, S_0, S_1, S_2, si chiamano il *vuoto proiettivo*, il *punto proiettivo*, la *retta proiettiva*, il *piano proiettivo*. Notare che il vuoto proiettivo è privo di punti, ma non è l'insieme vuoto perché contiene $\sigma \langle 0 \rangle$.

Si noterà subito una stranezza: l'S_n non è, come tutti gli spazi dabbene, l'insieme dei propri punti, ma è l'insieme del vuoto, dei punti, delle rette, dei piani, ..., degli iperpiani, e del sostegno. Tuttavia l'insieme dei punti di S_n esiste, e si chiama lo *spazio proiettivo punteggiato* o *di punti*, legato ad S_n; quindi c'è il *vuoto punteggiato*, che è l'insieme vuoto, il *punto punteggiato* (di cardinalità 1), la *retta punteggiata*, il *piano punteggiato*.

2.20 Lezione 20

[2] Se $A_r = \sigma U_{r+1}$, $B_s = \sigma W_{s+1}$ sono elementi di S_n, scriveremo $A_r < B_s$ se $U_{r+1} \subset W_{s+1}$, ossia se A_r e B_s si appartengono ed $r < s$; porremo $A_r \cap B_s = \sigma(U_{r+1} \cap W_{s+1})$ = [elemento di dimensione massima fra quelli che sono $\leq A_r$ e $\leq B_s$]; porremo anche $A_r + B_s = \sigma(U_{r+1} + W_{s+1})$ = [elemento di dimensione minima fra quelli che sono $\geq A_r$ e $\geq B_s$]. Se $A_r \cap B_s =$ vuoto, A_r e B_s sono *sghembi* (altrimenti sono *incidenti*); se inoltre $A_r + B_s = sostS_n$, essi sono *complementari*.

[2] In realtà nel testo non compare l'inizio della lezione 20, ma compare nella numerazione delle formule; perciò ne abbiamo posto (arbitrariamente) l'inizio in questo punto

Dato un A_r, esso definisce subito due spazi proiettivi: l'uno è quello che ha A_r come sostegno, e che quindi è formato di tutti gli elementi di S_n che sono $\leq A_r$; consiste dei σV quando $V \subseteq U_{r+1}$, ed è quindi il $\sigma[U_{r+1}]$, di dimensione r; è detto il *sottospazio* di S_n di sostegno A_r, e vedremo in seguito che è veramente un sottospazio. L'altro spazio proiettivo definito da A_r è quello che ha A_r come vuoto, che è quindi formato da tutti gli elementi di S_n che sono $\geq A_r$; consiste dei σV quando $V \supseteq U_{r+1}$, ma questo non mostra che sia spazio proiettivo; per sincerarcene, poniamo $V'_{n-r} = V_{n+1}/U_{r+1}$, chiamiamo h l'omomorfismo naturale di V_{n+1} su V'_{n-r}, e definiamo un σ' di $[V'_{n-r}]$ su S_n così:

$$\sigma' Z = \sigma h^{-1} Z. \tag{2.20.1}$$

Allora lo spazio descritto è $\sigma'[V'_{n-r}]$ ed ha quindi dimensione $n-r-1$; si chiama *stella di centro* A_r (*fascio* se ha dimensione1) in S_n. Notiamo subito che l'essere "sottospazio di" o "stella in" non è una particolarità di questi spazi, ma solo una relazione speciale col dato S_n.

Altra cosa: sia V^*_{n+1} il duale di V_{n+1}, e definiamo un σ^* di $[V^*_{n+1}]$ su S_n cosiì:

$$\sigma^* Z = \sigma Z^{\perp}. \tag{2.20.2}$$

Ora (S_n, σ^*) è uno spazio proiettivo che ha lo stesso insieme S_n di (S_n, σ); sarà indicato con (S^*_n, σ^*) o brevemente S^*_n, e chiamato il *duale*. Se A è elemento di S_n o S^*_n indifferentemente, e se la dimensione di A come elemento di S_n è m, quella come elemento di S^*_n è $n-m-1$; se B è un altro elemento, e se $A < B$ in S_n, sarà $A > B$ in S^*_n; l'elemento $A \cap B$ in S_n è l'elemento $A + B$ in S^*_n; l'elemento $A + B$ di S_n è l'elemento $A + B$ in S^*_n. È $S^{**}_n = S_n$; il vuoto di S_n è il sostegno di S^*_n; i punti di S^*_n sono gli iperpiani di S_n, ecc.. L'insieme dei punti di S^*_n, e quindi degli iperpiani di S_n, è lo *spazio di iperpiani legato ad* S_n (*piano rigato* se $n = 2$, *spazio di piani* se $n = 3$). Se infine A è elemento di S_n, e se A_1, A_2 sono rispettivamente il sottospazio di S_n di sostegno A, e la stella di S_n di centro A, allora A^*_1, A^*_2 sono rispettivamente la stella di S^*_n di centro A ed il sottospazio di S^*_n di sostegno A. A questo punto si può enunciare il

Teorema 2.20.3 (di dualità proiettivo)**.** *Ogni asserto riguardante gli elementi di un S_n e le loro proprietà di appartenenza resta vero quando ogni elemento di dimensione i viene sostituito con uno di dimensione $n-i-1$; in particolare, "punti" con "iperpiani".*

Il (2.20.3) è vago nell'enunciato; per renderlo preciso ci si dovrebbe impegolare nella logica formale; ecco un esempio di ciò che vuol dire e di ciò che non vuol dire: l'asserto "il piano H si appartiene coi punti P, Q" non è dualizzabile perché non ci sono i "duali" di H, P, Q. Invece l'asserto "se tre piani di S_3 non si appartengono con una stessa retta essi si appartengono con esattamente un punto" (in parole povere: se tre piani non hanno in comune una retta s'incontrano in un punto) ha il seguente duale: "se tre punti di S_3 non si appartengono con una stessa retta, essi si appartengono con esattamente un piano" (in parole povere: tre punti non allineati determinano un piano).

2.21 Lezione 21

Siano (S_n, σ), (S'_m, σ') spazi proiettivi sui corpi C, C', con sostegni σV_{n+1}, $\sigma' V'_{m+1}$, e sia f_S un'applicazione di S_n su S'_m; la f_S è un'*applicazione proiettiva* se esiste un'applicazione p-semilineare f_V di V_{n+1} su V'_{m+1} (con p isomorfismo opportuno di C su tutto C') tale che

$$f_S \sigma V_{i+1} = \sigma' f_V V_{i+1} \qquad \text{per ogni } V_{i+1} \subseteq V_{n+1}. \tag{2.21.1}$$

Si ha:

Lemma 2.21.2. *Sia g_V una applicazione q-semilineare di V_{n+1} su V'_{m+1} tale che la (2.21.1) sia soddisfatta dopo la sostituzione di f_V con g_V. Allora $\operatorname{im} g_V = \operatorname{im} f_V$ e $\ker g_V = \ker f_V$; se inoltre f_V ha rango > 1, si ha $p = q$, ed esiste un $a \in C'$ non nullo tale che $g_V v = a f_V v$ per ogni $v \in V_{n+1}$.*

Dim. Sia $U_r = \ker f_V$, e pongasi $V_{n+1} = U_r \oplus W_{n-r+1}$; sia $w_0, \dots, w_{n-r}$ base di W, e pongasi $w = \sum_i w_i$. Da $\sigma' \langle f_V w_i \rangle = f_S \sigma \langle w_i \rangle = \sigma' \langle g_V w_i \rangle$, si ha $\langle f_V w_i \rangle = \langle g_V w_i \rangle$, onde $g_V w_i = a_i f_V w_i$, con $0 \neq a_i \in C'$; analogamente, $g_V w = a f_V w$. Ma $g_V w = \sum_i g_V w_i = \sum_i a_i f_V w_i$, mentre $a f_V w = \sum_i a f_V w_i$. Quindi $a_i = a$ per ogni i. Se poi $u \in U_r$ si ha $\sigma' \langle g_V u \rangle = f_S \sigma \langle u \rangle = \sigma' \langle f_V u \rangle = \sigma' \langle 0 \rangle$, onde $g_V u = 0$, $u \in \ker g$; con ragionamento reciproco si ottiene che $\ker g_V = \ker f_V$; il discorso di prima dà poi che un elemento $\sum_i x_i g_V w_i$ di $\operatorname{im} g_V$ (con $x_i \in C'$) si può scrivere come $\sum_i (a x_i) f_V w_i \in \operatorname{im} f_V$; pertanto $\operatorname{im} f_V = \operatorname{im} g_V$.

Se $\operatorname{im} f_V$ ha dimensione almeno 2, pongasi $z = w_0 + x w_1$, con $x \in C$. Allora, al solito, $g_V z = b f_V z$ per un $b \in C'$; ma $g_V z = g_V w_0 + x^q g_V w_1 = a(f_V w_0 + x^q f_V w_1)$, mentre $b f_V z = b(f_V w_0 + x^p f_V w_1)$. Quindi $a = b$ e $x^q = x^p$. Ora è chiaro che $g_V \sum_i x_i w_i = \sum_i x_i^p a f_V w_i = a f_V \sum_i x_i w_i$. C.V.D. $\square$

Il Lemma 2.21.2 dice che la f_V (detta *soprastante* alla f_S) è essenzialmente unica; la sua dimostrazione prova che:

Lemma 2.21.3. *Una applicazione f_S di S_n su S'_m è proiettiva ed ha applicazione soprastante f_V se, e solo se,*

1. *$f_S \sigma \langle v \rangle = \sigma' \langle f_V v \rangle$ per ogni $v \in V_{n+1}$, o equivalentemente $f_S P = \sigma' f_V \sigma^{-1} P$ per ogni punto P di S_n;*
2. *Se un elemento ed un punto di S_n si appartengono, anche le loro f_S-immagini si appartengono.*

Casi particolari di applicazioni proiettive:

1. $\ker f_V = \langle 0 \rangle$, ossia f_V è iniettiva; accade se, e solo se, S_n non ha punti la cui immagine è il vuoto di S'_m; la f_S dicesi *iniettiva*; è biunivoca tra S_n ed $\operatorname{im} f_S$, e conserva la dimensione.
2. S_n è sottoinsieme di S'_m ed f_S è l'applicazione identica e manda i punti su punti; per 1 la f_S è iniettiva e si chiama l'*immersione* di S_n in S'_m; l'S_n è detto *sottospazio proiettivo* di S'_m.

3. f_V è biiettiva, ossia iniettiva su tutto V'_{m+1}; accade se, e solo se, f_S induce una biiettiva tra spazi punteggiati; allora f_S è biiettiva fra S_n ed S'_m nel solito senso, e conserva la dimensione; viene detta *collineazione*, ed anche *proiettività* quando la f_V sopastante è, o può essere scelta, lineare.
4. Posto $U_r = \ker f_V$, f_V è l'omomorfismo naturale di V_{n+1} su tutto $V'_{m+1} = V_{n+1}/U_r$, onde $r + m = n$. Per ogni elemento Z di $[V_{n+1}]$, l'elemento $f_V Z$ di $[V'_{m+1}]$ è l'insieme dei vettori $v + U_r$ per i quali v può esser scelto in Z; questi sono in corrispondenza biunivoca con gli $Z + U_r$, e richiederemo ulteriormente che σ' sia definita da $\sigma' f_V Z = \sigma(Z + U_r)$, come nella (2.20.1). Con ciò il Lemma 2.21.2 comporta che $f_S \sigma Z = \sigma(Z + U_r) = \sigma Z + \sigma U_r$. La f_S così costruita si dirà la *proiezione di S_n di centro σU_r* oppure *da σU_r*; *proiettare σZ* da σU_r vuol dire appunto costruire $f_S \sigma Z$; e questo oggetto si chiama la *proiezione* di σZ da σU_r. Lo spazio $S'_m = S'_{n-r}$ così costruito non è altro che la stella in S_n di centro σU_r; il $T_{r-1} = \sigma[U_r]$ è un sottospazio proiettivo di S_n, detto il *nucleo* di f_S, e indicato con $\ker f_S$; è l'insieme di tutti gli elementi di S_n la cui f_S-immagine è il vuoto di S'_m; l'S'_m è anche indicato con S_{n+1}/T_{r-1}.
5. Caso generale. Sappiamo che la f_V può essere così decomposta:

$$V_{n+1} \xrightarrow[suriezione]{} V_{n+1}/\ker f_V \xrightarrow[biiezione]{} \operatorname{im} f_V \xrightarrow[immersione]{} V'_{m+1} \ ;$$

   corrispondentemente, f_S si spezza così:

$$S_n \xrightarrow[proiezione]{} S_n/\ker f_S \xrightarrow[collineazione]{} \operatorname{im} f_S \xrightarrow[immersione]{} S'_m \ .$$

Dati S_n ed S'_m, una applicazione proiettiva f_S di S_n su S'_m, con la soprastante f_V, ha naturalmente la *trasposta* f^*, di S'_m su S^*_n, con la soprastante f^*_V (tenere presente la (1.16.1) per la trasposizione semilineare); in particolare, se f_S è immersione, f^*_S è proiezione di centro il sostegno di S_n, mentre se f_S è proiezione di centro A, f^*_S è l'immersione si ${S'_m}^*$ in S^*_n. Se però f_S è collineazione, la f^*_S può anche essere interpretata come collineazione di S'_m su S_n così: da $f^*_S \sigma^* V = \sigma^* f^*_V V$ per (2.21.2) si ottiene $f^*_S \sigma' V^\perp = \sigma(f^*_V V)^\perp$ per (2.20.2); ma $(f^*_V V)^\perp = f_V^{-1} V^\perp$, onde $f^*_S \sigma' V^\perp = \sigma f_V^{-1} V^\perp$, che mostra che

2.21.4. *Se f_S è collineazione di S_n su S'_n, allora f^*_S, come applicazione di S'_n su S_n, coincide con f_S^{-1}.*

Intendiamoci bene: la f^*_S è sempre applicazione di ${S'_m}^* = S'_m$ (come insiemi) su $S^*_n = S_n$; il guaio è che se f_S non è collineazione, quell'applicazione non è proiettiva.

2.22 Lezione 22

Una applicazione proiettiva di S_n su ${S'_m}^*$ si chiama una *reciprocità* di S_n su S'_m; una *autoreciprocità* è una reciprocità di S_n in sé che sia una proiettività di S_n

su S_n^*. Per dare una autoreciprocità basta dare l'f_V soprastante, che è un'applicazione lineare non degenere di V_{n+1} su V_{n+1}^*; ed ormai sappiamo che un tale oggetto identifica V_{n+1} con V_{n+1}^*, cosicché la dualità preesistente fra questi diviene un'autodualità. Si è visto nella prima parte che fra queste sono importanti le norme e le alternanti non degeneri. L'unicità essenziale di f_V (2.21.3) ci dà l'unicità essenziale della autodualità soprastante ad una autoreciprocità; ed allora le autoreciprocità provenienti da norme che non siano anche alternanti (questo va detto per la caratteristica 2) si chiamano *polarità*, mentre quelle provenienti da alternanti si chiamano *sistemi nulli*.

Teorema 2.22.1. *Una autoreciprocità $f_S : S_n \to S_n^*$ è una polarità o un sistema nullo se, e solo se, è vero l'asserto seguente: ogniqualvolta P, Q sono punti di S_n tali che Q si appartenga con $f_S P$, allora P si appartiene con $f_S Q$. La f_S è poi polarità (risp. sistema nullo) se esiste (risp. non esiste) qualche punto P di S_n che non si appartenga con $f_S P$.*

Dim. La autodualità "$\circ$" di V_{n+1} è definita da $v \circ v' = v \circ f_V v'$; dire che $\sigma \langle v \rangle$ si appartiene con $f_S \sigma \langle w \rangle = \sigma^* \langle f_V w \rangle = \sigma \langle f_V w \rangle^\perp$ è equivalente a dire che $v \circ f_V w = 0$, ossia che $v \circ w = 0$. L'altro asserto vuole invece dire $w \circ v = 0$; questo è conseguenza del primo (ossia è vero per tutti i v, w per i quali è vero il primo) se, e solo se, la autodualità soddisfa la $v \circ w = \pm w \circ v$ (dimostrarlo!). Se vale il $+$ o se la caratteristica è 2 si ha una norma; se vale il $-$ e la caratteristica non è 2 si ha l'alternanza. Poi, $\sigma \langle v \rangle$ si appartiene con $f_S \sigma \langle v \rangle$ se, e solo se, $v \circ v = 0$; questo è vero per ogni v se, e solo se, il tondino è alternente (è la definizione dell'alternanza). C.V.D. $\square$

C'è un'ultima operazione da introdurre, che si riattacca a quanto detto subito prima e subito dopo del (2.21.4). Una specialità degli spazi vettoriali, e quindi degli spazi proiettivi, è che ogni sottospazio ha dei complementari; Questo permette di dare degli isomorfismi canonici fra sottospazi e immagini: sia V spazio vettoriale, e ne siano U, U' sottospazi complementari, cosicché $V = U \oplus U'$; posto $V' = V/U$, sia f_V l'omomorfismo naturale di V su V'; questo f_V induce un isomorfismo g_V di V' su tutto U' mediante la $g_V(f_V v) = pr_2 v$; tale g_V è ovviamente il reciproco della restrizione di f_V ad U'. Trasferiamo tutto agli spazi proiettivi $S = \sigma[V]$, $T = \sigma[U]$, $T' = \sigma[U']$, e $S' = S/T =$ (stella in S di centro $sostT$) $= \sigma'[V']$ col σ' del (2.20.1). I sostegni di T e T' sono complementari in S, e l'f_S di S su S' (la proiezione da $sostT$) induce una proiettività g_S di S' su tutto T', che è il reciproco della restrizione di f_S a T'. Questa restrizione fa corrispondere ad un $A \in T'$ l'elemento $A + sostT$ di S, e si noti che A e $sostT$ sono sghembi; quindi g_S fa corrispondere A ad $A + sostT$; ma $A = (A + sostT) \cap sostT'$ (perché $Z = (U \oplus Z) \cap U'$ se Z è sottospazio di U'). Questa proiettività g_S della stella S' sul sottospazio T' che, ripeto, consiste in $B \mapsto B \cap (sostT')$, si chiama *sezione di S' con $sostT'$ in S*; per $B \in S'$ il $B \cap sostT'$ si chiama di nuovo la *sezione di B con $sostT'$ in S*, ed il verbo che si usa per "fare una sezione" è *segare* o *secare*. È bene avvertire che poi in pratica si segano gli elementi di S' anche con dei $sostT'$ che, anziché essere complementari, contengono dei complementari (contengono nel senso di $>$) di $sostT$; con ciò si ottiene una proiettività della stella S' non su tutto T', ma su $\operatorname{im} g_V$, che è la stella in T' di centro $(sostT) \cap (sostT')$; questo non è che il terzo teorema di omomorfismo degli spazi vettoriali trasportato ai proiettivi:

$$\frac{T+T'}{T} = \frac{T'}{T\cap T'}; \tag{2.22.2}$$

in questa formula si sono trasferiti, per comodità, i simboli $+$ e $\cap$ dagli elementi di S ai sottospazi dei quali quegli elementi sono i sostegni; ci sentiremo autorizzati a farlo anche in seguito, e quindi notiamo subito che: *gli elementi di $T+T'$ sono gli $A+A'$, con A, A' elementi di T, T' rispettivamente; gli elementi di $T\cap T'$ sono gli $A\cap A'$.*

Tutto ciò che si può costruire su uno spazio vettoriale ha naturalmente la sua interpretazione proiettiva; una delle cose che conosciamo è l'algebra esterna, o meglio i suoi elementi omogenei $E_0 = C$, $E_1 = V$, $E_2, \dots, E_n, E_{n+1}$ (il V sarà supposto di dimensione $n+1$). Osserviamo che un sottospazio U di dimensione $m+1$ di V è determinato da una sua base $x_0, \dots, x_m$; ed il Teorema 1.5.2 insieme con la multilinearità e l'alternanza del prodotto esterno (1.4.3) mostrano che la corrispondenza $U \mapsto \langle x_0 \wedge \cdots \wedge x_m\rangle$ è biunivoca, ossia che l'elemento a destra dipende unicamente da U e non dalla base scelta. Si può quindi asserire che gli elementi dello spazio proiettivo $S_n = \sigma[V]$ sono i $\sigma\langle h\rangle$, ove h percorre tutti gli elementi di $E = \bigoplus_i E_i$ che sono prodotti esterni di vettori di V; il numero di fattori esterni dà la dimensione. Qui si è naturalmente stipulato di scrivere $\sigma\langle x_0 \wedge \cdots \wedge x_m\rangle = \sigma U$, e si è anche stipulato che 0 sia l'unico elemento di C che è prodotto esterno di vettori di V. Si noti che, per (1.5.2),

2.22.3. *Gli elementi $\sigma\langle h\rangle$, $\sigma\langle k\rangle$ di S_n sono incidenti se, e solo se, $h \wedge k = 0$.*

Nella dimostrazione del Teorema 1.6.4 si è visto che, fissato un $e \in E_{n+1}$ non nullo, l'applicazione $(h,k) \mapsto c \in C$, ove c è dato da $h \wedge k = ce$, è una dualità tra E_{m+1} ed E_{n-m}, dualità che indicheremo con "$\circ$"; si può perciò prendere E_n come duale V^* di V, ed ecco che S_n^* è legato ad E^* come S_n lo è ad E. L'(1.6.4) stesso ci conferma che ogni elemento di E_n è legato ad un iperpiano di S_n, mentre gli elementi di E_i, quando $1 < i < n$, non sono tutti legati ad elementi di S_n.

2.23 Lezione 23

Si era promesso di mostrare che gli spazi proiettivi ora costruiti sono dei "completamenti" di spazi affini, ed è giunto il momento di mantenere la promessa. Partiamo dallo spazio proiettivo (S,σ), di dimensione $n \geq 0$; una proiettività f_S di S in sé è una *omologia* se esiste un iperpiano Z di S tale che f_S induca la proiettività identica sul sottospazio proiettivo di S che ha Z per sostegno; per (2.21.3), è quanto dire che ogni punto che si appartiene con Z deve essere unito per f_S.

Lemma 2.23.1. *Se f_S è omologia, tale è f_S^*.*

Dim. Usiamo $V = \sigma^{-1} sostS$, ed $U = \sigma^{-1}Z$, cosicché, per (2.21.2) e (2.21.3), la f_V soprastante f_S può essere scelta in modo da indurre l'identità in U. Sia

$v_0, \dots, v_n$ base di V, con $\{v_1, \dots, v_n\}$ base di U: $f_V v_i = v_i$ per $i > 0$; presa la base duale v_i^* di V^*, cerchiamo delle $a_i \in C$ tali che, posto $v_i' = v_i^* + a_i v_0^*$ $(i = 1, \dots, n)$, si abbia $f_V^* v_i' = v_i'$ (se le troviamo il teorema è dimostrato). Ora, in effetti è $v_j \circ f_V^* v_i' = f_V v_j \circ v_i^* + a_i f_V v_j \circ v_0^*$, e noi vogliamo che questa, per ogni j, coincida con $v_j \circ v_i^* + a_i v_j \circ v_0^*$. Per $j > 0$ l'identità richiesta è automaticamente verificata perché $f_V v_j = v_j$; per $j = 0$ essa si riduce a $f_V v_0 \circ v_i^* + a_i f_V v_0 \circ v_0^* = a_i$, dalla quale si possono ricavare le a_i se $f_V v_0 \circ v_0^* \neq 1$. Se invece questo è $= 1$, ciò significa che $f_V v_0 = v_0 +$ (elemento di U); in tal caso questo elemento di U può essere preso fra i $v_1, \dots, v_n$, per esempio v_1: $f_V v_0 = v_0 + v_1$ (se quell'elemento fosse 0, f_V sarebbe l'identità ed il risultato sarebbe ovvio). Ora si ha, per $i \neq 1$, $v_j \circ f_V^* v_i^* = f_V v_j \circ v_i^* = v_j \circ v_i^*$; ciò mostra che le $v_0^*, v_2^*, \dots, v_n^*$ hanno ancora la proprietà $f_V^* v_i^* = v_i^*$. Si è così visto che f_S^* è omologia. C.V.D. $\square$

Il significato del Lemma 2.23.1, alla luce del (2.21.4), è il seguente: se f_S è omologia, non solo c'è un iperpiano che è sostegno di un sottospazio su cui f_S induce l'identità; ma c'è anche un punto che è centro di una stella su cui f_S induce l'identità. Ed anzi, per la simmetria del (2.23.1), quest'ultima proprietà caratterizza da sola le omologie. L'iperpiano ed il punto si chiamano l'*asse* ed il *centro di omologia*, e l'omologia è *speciale* se asse e centro si appartengono; ma l'omologia identica è considerata sia speciale che non speciale. Nella dimostrazione del Lemma 2.23.1 l'asse di f_S è $Z = \sigma U$; il centro è l'asse di f_S^*, che nel primo caso (quello con le a_i) è $\sigma \langle v_1', \dots, v_n' \rangle^\perp$, e nel secondo (esclusa l'identità) è $\sigma \langle v_0^*, v_2^*, \dots, v_n^* \rangle^\perp$. Fatti i conti risulta che il centro nel primo caso è $\sigma \langle v_0 - \sum_{i=1}^n a_i v_i \rangle$, che non si appartiene con l'asse, mentre nel secondo è $\sigma \langle v_1 \rangle$, che si appartiene con l'asse. Questo mostra che vi è corrispondenza biunivoca fra le omologie speciali di asse σU da una parte, e l'insieme U dall'altra: all'elemento $u \in U$ corrisponde l'omologia f_S il cui f_V è dato da $f_V v = v$ se $v \in U$, e $f_V v_0 = v_0 + u$. In questa corrispondenza al prodotto di omologie corrisponde la somma dei corrispondenti elementi di U, il che mostra intanto che le omologie speciali di dato asse formano un gruppo abeliano. Inoltre, se u e la corrispondente f_S sono date, a cu (con $c \in C$) corrisponde l'omologia il cui f_V è $f_V v_0 = v_0 + cu$; sarà indicata con cf_S; in tal modo le omologie descritte vengono a formare uno spazio vettoriale su C isomorfo ad U, e il loro prodotto sarà quindi indicato col segno $+$. La corrispondenza trovata dipende dalla scelta di v_0, ma la struttura di spazio vettoriale che ne scaturisce non ne dipende (dimostrazione immediata; ma farsela!). Lo spazio vettoriale delle omologie speciali di asse Z sarà indicato con Om_Z.

Dati dunque S e Z, sia $\mathbb{A}$ l'insieme dei punti di S che non si appartengono con Z, e sia $T = Om_Z$; la coppia $(T, \mathbb{A})$ è uno spazio affine di dimensione n su C se si definisce, per $t \in T$ e $P \in \mathbb{A}$, $P + t =$ [trasformato di P mediante t] (quello che normalmente si indicherebbe con tP): ed infatti le a), b), c) della definizione nella Lezione 17 sono soddisfatte. Questo $(T, \mathbb{A})$ sarà chiamato lo spazio affine ottenuto mediante la scelta dell'*iperpiano improprio* (o *all'infinito*) Z; il sottospazio di S di sostegno Z, ed i suoi elementi, sottospazi e stelle, sono chiamati *impropri* o *all'infinito*; gli altri, *propri* o *al finito* (ma una stella al finito può avere centro all'infinito).

La costruzione non sarebbe molto significativa se non si mostrasse che le applicazioni affini sono tutte e sole le restrizioni agli spazi affini di certe applicazioni proiettive:

Teorema 2.23.2. *Siano S, S' spazi proiettivi su C, C', di dimensioni n, m non negative; siano $(T, \mathbb{A})$ e $(T', \mathbb{A}')$ gli spazi affini ottenuti da S, S' mediante scelta di iperpiani impropri Z, Z'. Un'applicazione proiettiva g_S di S su S' è tale che la sua restrizione $g_{\mathbb{A}}$ ad $\mathbb{A}$ (supposta applicazione di $\mathbb{A}$ su $\mathbb{A}'$) è applicazione affine di $(T, \mathbb{A})$ su $(T', \mathbb{A}')$ se, e solo se, $g_S Z \leq Z'$. Ed ogni g_A proviene nel modo detto da un'unica g_S.*

Dim. Se $g_{\mathbb{A}}$ è applicazione affine, intanto $g_{\mathbb{A}}\mathbb{A} \subseteq \mathbb{A}'$, onde $g_S^{-1}(Z' \cap sost\mathrm{im}\, g_S)$ è un insieme di elementi di S tutti $\leq Z$; quello di massima dimensione dovendo avere dimensione $n-1$, esso coinciderà con Z; ciò mostra che $g_S Z \leq Z'$. Reciprocamente, se g_S ha la proprietà detta, si ha $g_S Z \leq (Z' \cap sost\mathrm{im}\, g_S)$, ed un conto di dimensioni mostra che deve valere l'$=$; quindi di nuovo $g_S^{-1}(Z' \cap sost\mathrm{im}\, g_S)$ contiene un elemento di dimensione $n-1$ che deve coincidere con Z; ed infine $g_S\mathbb{A} \subseteq \mathbb{A}'$. Fissato un $P \in \mathbb{A}$, per ogni $t \in T$ pongasi $g_T t = g_{\mathbb{A}}(P+t) - g_{\mathbb{A}}P$; nelle notazioni della dimostrazione del Lemma 2.23.1 questo è equivalente al dire che se t è data da $v_0 \mapsto v_0 + u$, la $g_T t$ è data da $g_V v_0 \mapsto g_V v_0 + g_V u$; perciò la g_T è semilineare da T a T', e la $g_{\mathbb{A}}$ è affine.

Per ultimo, si vede subito che questa coppia $(g_T, g_{\mathbb{A}})$ poteva essere assegnata, col che il g_V, e quindi il g_S, veniva determinato dall'ultima formula scritta. C.V.D. $\square$

In particolare, nel Teorema 2.23.2 il nucleo di g_S deve aver sostegno che si appartenga con Z; ciò spiega perché non si è mai parlato del nucleo nelle applicazioni affini: esso è fuori dello spazio affine.

Confrontando con la Lezione 18 si vede ora che Aff $\mathbb{A}$ è la restrizione ad $\mathbb{A}$ del gruppo delle proiettività che hanno Z come elemento unito; che T è la restrizione ad $\mathbb{A}$ di Om_Z; e che GL(T) è il gruppo delle restrizioni ad $\mathbb{A}$ delle proiettività di S che hanno Z ed O come elementi uniti. In un'altra parte di queste lezioni vedremo che cosa significa, dal punto di vista proiettivo, introdurre una metrica in $\mathbb{A}$.

2.24 Lezione 24

Diamo un lemma che nel seguito sarà continuamente usato; premettiamo che la scrittura $x_1, \ldots, \widehat{x_i}, \ldots, x_n$ significa $x_1, \ldots, x_n$ saltando x_i.

Lemma 2.24.1. *Sia V spazio vettoriale di dimensione n sul corpo C, e ne sia $\{v_1, \ldots, v_n\}$ una base; sia u un elemento di V che non appartenga al sottospazio $\langle v_1, \ldots, \widehat{v_j}, \ldots, v_n\rangle$ (per ogni j). È allora possibile scegliere $v_1', \ldots, v_n', u'$ in modo che $\langle v_i'\rangle = \langle v_i\rangle$ per ogni i, che $\langle u'\rangle = \langle u\rangle$, e che $u' = v_1' + \cdots + v_n'$; e se $v"_i$, u'' è un'altra tale scelta, esiste un $c \in C$ non nullo tale che $v_i'' = cv_i'$.*

Dim. Sarà $u = \sum_i x_i v_i$, con $x_i \neq 0$ per ogni i; basta prendere $u' = u$, $v_i' = x_i v_i$. Data poi l'altra scelta, e supposto $u'' = cu'$, da $\sum_i v_i'' = \sum_i cv_i'$, e da $v_i'' = c_i v_i'$ (dato che $\langle v_i''\rangle = \langle v_i'\rangle$) si ricava $c_i = c$. C.V.D. $\square$

Dato ora un S_n su C, siano $P_0, \ldots, P_n$ suoi punti; essi formano un $(n+1)$-*edro* (un *triangolo* se $n = 2$) se nessun elemento di S_n, che non sia il sostegno, li contiene tutti; insomma, se $P_0 + \cdot + P_n = sost S_n$. Se $(P_0, \ldots, P_n)$ è un $(n+1)$-edro, sia U un punto di S_n che non si appartenga con nessuno degli iperpiani $P_0 + \cdots + \widehat{P_i} + \cdots + P_n$; l'insieme ordinato $(P_0, \ldots, P_n, U)$ si chiama un *sistema di riferimento* in S_n; in particolare, l'$(n+1)$-edro $(P_0, \ldots, P_n)$ ne è l'$(n+1)$-*edro fondamentale*, ed U ne è il *punto unità*. Il Lemma 2.24.1 mostra che si possono trovare e sono unici, a meno di un fattore non nullo in C, gli elementi $v_0, \ldots, v_n, u$ di $V = \sigma^{-1} sost S_n$, tali che $P_i = \sigma \langle v_i \rangle$, $U = \sigma \langle u \rangle$, e $u = v_0 + \cdots + v_n$. Se P è un punto qualsiasi di S_n, le $x_i \in C$ tali che $P = \sigma \langle \sum_i x_i v_i \rangle$ ne sono le *coordinate proiettive* o *omogenee*; esse sono determinate a meno di un fattore non nullo in C; ed ogni tale $(n+1)$-upla, eccetto quella nulla, dà un punto di S_n; quindi lo spazio punteggiato legato ad S_n è in corrispondenza biunivoca con le matrici $(n+1) \times 1$ $\begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix}$ non nulle ad elementi in C, intendendo però che matrici proporzionali diano lo stesso punto; in particolare, le coordinate di U sono $1, \ldots, 1$, donde il nome di punto unità. Naturalmente, appena è dato un sistema di riferimento in S_n ne è subito dato uno in S_n^*, costituito dagli iperpiani $R_i = P_0 + \cdots + \widehat{P_i} + \cdots + P_n$ di S_n come $(n+1)$-edro fondamentale, e da un punto unità in S_n^* che è l'iperpiano Z di S_n che si appartiene con tutti i punti U_{ij} così definiti: le coordinate di U_{ij} sono tutte 0, eccetto $x_i = 1$ ed $x_j = -1$. Di nuovo, gli iperpiani di S_n sono in corrispondenza biunivoca (a meno del solito fattore di proporzionalità) con tutte le $(n+1)$-uple non nulle di numeri di C, che ora però scriveremo come matrici $1 \times (n+1)$ $(a_0, \ldots, a_n)$; l'iperpiano unità è $(1, \ldots, 1)$. Le a_i sono naturalmente le coordinate proiettive di un punto di S_n^*; ma quando sono viste come coordinate di un iperpiano di S_n sogliono essere chiamate *coordinate plückeriane*. Si ha

Teorema 2.24.2. *Con la precedente scelta di sistemi di riferimento in S_n ed S_n^*, l'iperpiano $a = (a_0, \ldots, a_n)$ ed il punto $x = \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix}$ si appartengono se, e solo se, $ax = 0$.*

Dim. Ci riferiamo alle considerazioni che chiudono la lezione 22, ed al (2.22.3); se i v_i, u sono quelli che sono serviti per costruire il sistema di riferimento in S_n, si ha $R_i = \sigma \langle v_i^* \rangle^{\perp}$, ove $v_i^* = (-1)^i v_0 \wedge \cdots \wedge \widehat{v_i} \wedge \cdots \wedge v_n \in E_n = V^*$ (non farsi spaventare dal -1, che è comodo ma non ha effetto su R_i); si ha anche $Z = \sigma \langle u^* \rangle^{\perp}$, ove $u^* = \sum_i v_i^*$, come si vede sfruttando appunto il (2.22.3), ed il fatto che Z deve appartenersi con gli $U_{ij} = \sigma \langle v_i - v_j \rangle$. Questo mostra che una delle dualità "$\circ$" fra V ed E_n di cui si parla alla fine della lezione 22 è ottenibile mediante $e = v_0 \wedge \cdots \wedge v_n$. I v_i^*, u^*, sono legati fra loro come vuole la definizione di sistema di riferimento, ed i v_i^* formano una base in V^*, duale della $\{v_0, \ldots, v_n\}$. Ora $R_i = \sigma^* \langle v_i^* \rangle$ in quanto elemento di S_n^*, e $Z = \sigma^* \langle u^* \rangle$, il σ^* essendo dato da (2.20.2). La relazione $ax = 0$ viene così a significare $(\sum_i a_i v_i^*) \circ (\sum_i x_i v_i) = 0$, ossia $\sum_j x_j v_j \in \langle \sum_i a_i v_i^* \rangle^{\perp}$, e infine $x < a$ (identificando x ed a col punto e l'iperpiano), per (2.20.2). C.V.D. □

Il (2.24.2) è interpretabile nel solito modo: l'iperpiano a è il "luogo" dei punti x tali che $ax = 0$; questa è ciò che di solito si chiama "l'*equazione*" di a. È anche interpretabile, in S_n^*, alla rovescia: il punto x è "l'*inviluppo*" degli iperpiani a tali che $ax = 0$; questa ha quindi diritto di chiamarsi "l'equazione" del punto x.

Ora che abbiamo le coordinate è facile vedere chi è il gruppo delle proiettività: è il gruppo quoziente del gruppo moltiplicativo delle matrici $(n+1)\times(n+1)$ ad elementi in C, di determinante non nullo, modulo il sottogruppo delle matrici scalari non nulle; la proiettività di matrice M manda il punto x su Mx, e l'iperpiano a su aM^{-1}.

Se fissiamo $(1, 0, \dots, 0) = R_0$ come iperpiano improprio, lo spazio affine $\mathbb{A}^n$ che si ottiene è costituito dai punti x con $x_0 \neq 0$; il fattore di proporzionalità può essere eliminato col richiedere che $x_0 = 1$, ossia coll'identificare $\begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix}$ con $\begin{pmatrix} x'_0 \\ \vdots \\ x'_n \end{pmatrix}$, ove $x'_i = x_i/x_0$; ecco che le x'_i sono le coordinate cartesiane del punto x, nel sistema di riferimento affine $(P_0, t_1, \dots, t_n)$, ove t_i è l'omologia speciale di asse R_0 che manda P_0 su $\sigma\langle v_0 + v_i\rangle$ (cfr. lezione 17). Per il Teorema 2.23.2, le affinità di $\mathbb{A}^n$ sono le restrizioni ad $\mathbb{A}^n$ delle proiettività aventi matrice M (a determinante non nullo) tale che $(1, 0, \dots, 0)M^{-1} = (1, 0, \dots, 0)$; di tali M sono perciò tutte quelle del tipo $M = \left(\begin{smallmatrix} 1 & {}^t0 \\ b & M' \end{smallmatrix}\right)$, con M' matrice $n \times n$ a determinante non nullo. Questo spiega la strana forma (1.18.4) delle matrici delle affinità.

Per quanto precede, una proiettività manda un sistema di riferimento (di punti o di iperpiani) in un altro, ed è completamente determinata da questa coppia:

Teorema 2.24.3. *Siano $P_0, \dots, P_{n+1}$ punti (o iperpiani) di un S_n, tali che nessuna $(n + 1)$-upla di essi si appartenga con un iperpiano (risp. punto); idem per $P'_0, \dots, P'_{n+1}$ ed S'_n; allora esiste una unica proiettività f_S di S_n su S'_n (se i P, P' sono tutti punti o tutti iperpiani), o una unica reciprocità f_S di S_n su S'_n (se i P son punti ed i P' iperpiani, o viceversa) tale che $f_S P_i = P'_i$ per ogni i.*

2.25 Lezione 25

Per la retta proiettiva S_1 i sistemi di riferimento hanno un carattere particolarmente semplice; intanto un sistema di riferimento consiste di tre punti, che saranno chiamati P_∞ (quello che verrà preso come punto improprio per costruire una retta affine), P_0 (quello che sarà preso come origine), e P_1 (punto unità), a 2 a 2 distinti. Se P è un altro punto, le coordinate proiettive di P si trovano così: $P_\infty = \sigma\langle v_\infty\rangle$, $P_0 = \sigma\langle v_0\rangle$, $P_1 = \sigma\langle v_\infty + v_0\rangle$ per (2.24.1), $P = \sigma\langle x_\infty v_\infty + x_0 v_0\rangle$; e coordinate di P sono x_0, x_∞. Per la retta affine $\mathbb{A}$, con punto improprio P_∞, la coordinata ascissa rispetto a (P_0, t), ove t manda P_0 su P_1 e lascia fisso P_∞, è $x = \frac{x_\infty}{x_0}$. Questo $x \in C$ (oppure $x = \infty$ se $P = P_\infty$; qui si può usare questo simbolo, perché la retta proiettiva ha esattamente un punto in più di quella affine, ed allora a questo punto si può dare una coordinata "affine" che naturalmente non sta in C, per esempio il simbolo ∞) si chiama il *birapporto* dei quattro punti, e si indica con (P_∞, P_0, P_1, P). Si può subito fare una serie di giochetti; poniamo

$$
\text{(2.25.1)} \qquad \begin{cases} (P,Q,R,S) = x; & \text{allora si vede subito che} \\ (Q,P,R,S) = (P,Q,S,R) = \dfrac{1}{x} & \text{(l'ultima se } S \neq P,Q) \\ (P,R,Q,S) = (S,Q,R,P) = 1-x & \text{(l'ultima se } S \neq Q,R) \end{cases} .
$$

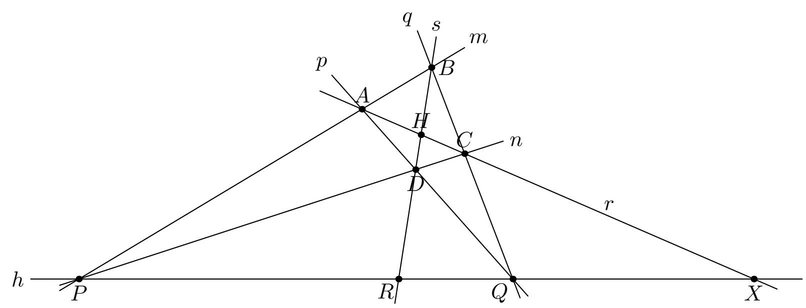
Scambiando in tutti gli altri modi possibili, e purché S sia diverso da P, Q, R, si trovano solo i 6 seguenti valori: x, $\frac{1}{x}$, $\frac{1}{1-x}$, $1 - \frac{1}{x} = \frac{x-1}{x}$, $\frac{1}{1-\frac{1}{x}} = 1 - \frac{1}{1-x} = \frac{x}{x-1}$. Se $x = -1$, questi si riducono ai soli 3 valori -1, 2, $\frac{1}{2}$ (ovvero $1, 0, \infty$ se C ha caratteristica 2); in questo caso l'insieme ordinato $(PQRS)$ si chiama *gruppo armonico* (uso arcaico della parola gruppo), e si dice anche che S è il *quarto armonico* dopo P, Q, R,o infine che R, S (risp. P, Q) *separano armonicamente* P, Q (risp. R, S). Le (2.25.1) permettono di dare significato a (P, Q, R, S) anche quando solo 3 dei 4 punti sono distinti, visto che un significato c'è quando S coincide con P, o Q, od R; ecco i significati che si ottengono: $(P, P, Q, S) = 1$, $(P, Q, P, S) = 0$, $(P, Q, Q, S) = \infty$, oltre naturalmente a $(P, Q, R, P) = \infty$, $(P, Q, R, Q) = 0, (P, Q, R, R) = 1$.

Chiaramente le proiettività conservano i birapporti, mentre le collineazioni applicano ad essi l'isomorfismo p di C legato alla collineazione. Siano allora a, b, c, d quattro elementi di $C \cup \{\infty\}$, di cui almeno tre distinti, per esempio a, b, c, e siano A, B, C, D (questa è un'altra C, ma non si farà confusione) i quattro punti di S che li hanno come coordinate ascisse rispetto a P_∞, P_0, P_1. C'è un'unica proiettività che manda A su P_∞, B su P_0, C su P_1, ed essa manderà D su un X tale che $(A, B, C, D) = (P_\infty, P_0, P_1, X)$. Ogni proiettività ha una matrice $\left(\begin{smallmatrix} r & s \\ r' & s' \end{smallmatrix}\right) = M$, e manda il punto di coordinate proiettive $\left(\begin{smallmatrix} x_\infty \\ x_0 \end{smallmatrix}\right)$ nel punto di coordinate $M \left(\begin{smallmatrix} x_\infty \\ x_0 \end{smallmatrix}\right)$. Quindi manda il punto di coordinata ascissa x in quello di coordinata ascissa $\frac{rx+s}{r'x+s'}$; poiché deve mandare a su ∞, b su 0, c su 1, si ricava $s' = -r'a$, $s = -rb$, e $r(c-b) = r'(c-a)$. Il punto D viene mandato sul punto X di coordinata $\frac{rd+s}{r'd+s'} = \frac{(c-a)(d-b)}{(c-b)(d-a)}$; quindi è questo il valore di $(A, B, C, D) = (P_\infty, P_0, P_1, X)$. Questo valore dipende solo da a, b, c, d e sarà chiamato il *birapporto* di questi quattro elementi di $C \cup \{\infty\}$:

$$
\text{(2.25.2)} \qquad (a, b, c, d) = \frac{(c-a)(d-b)}{(c-b)(d-a)}.
$$

Qui è bene osservare che, per quanto detto prima sul significato del simbolo ∞ come "ascissa" del punto improprio, finché si lavora con birapporti si avvera il sogno del matematico pigro, ossia: $\frac{1}{\infty} = 0$, $\frac{1}{0} = \infty$, ed anche, con cautela, $\frac{\infty}{\infty} = 1$ (ma $\frac{2\infty}{\infty} = 2$) e $\frac{0}{0} = 1$ (ma $\frac{2\cdot 0}{0} = 2$!).

Torniamo ai gruppi armonici per fare un disegnino:



Sono date la retta h ed i punti P, Q, R; si vuole costruire il quarto armonico X dopo questi tre; il disegno si spiega da sé; la figura costituita da $ABCDmnpqrs$ è un *quadrangolo piano completo*: 4 punti (*vertici*) a 3 a 3 non allineati, e le 6 rette (*lati*) che li congiungono a 2 a 2; lati che s'incontrano su un vertice sono *adiacenti* (come p, m); se no, *opposti* (come p, q); i tre punti d'incontro di coppie di lati opposti (ossia P, Q, H) sono i *punti diagonali*. Spiegazione del perché $PQRX$ è gruppo armonico:

$$\begin{aligned}(P,Q,R,X) &= (A,C,H,X) \quad \text{(proiezione di } h \text{ da } B \text{ su } r\text{)}\\ &= (Q,P,R,X) \quad \text{(proiezione di } r \text{ da } D \text{ su } h\text{)}\end{aligned}$$

(dimostrare che queste proiezioni si possono fare, ossia che i centri sono complementari alle rette con cui si sega). Quindi, per (2.25.1), il numero $x = (P,Q,R,X)$ soddisfa alla $x = \frac{1}{x}$, $x^2 = 1$, $x = \pm 1$; se la caratteristica non è 2, non è $x = 1$ perché X non coincide con R (dimostrarlo!); quindi $x = -1$.

Costruzione duale (farsi il disegno): punto H e rette p, q, r per esso; *quadrilatero piano completo* con *lati* $abcd$, *vertici* $PQRSMN$, e *diagonali* p, q, $h =$ retta RS. Retta x per R ed H è quarta armonica dopo p, q, r.

Esercizio: ora che conosciamo birapporti e gruppi armonici, trovare chi sono in realtà i Q_{ij} della lezione 24.

2.26 Lezione 26

Si è visto che le collineazioni cambiano il birapporto solo nel senso che ci applicano il p della semilinearità; l'importante è che vale il reciproco:

Teorema 2.26.1. *Siano S, S' rette proiettive sui corpi C, C'; sia p isomorfismo di C su tutto C', e sia f_S applicazione biunivoca di S su tutto S' con la proprietà seguente: intanto manda sostegno su sostegno e vuoto su vuoto, e poi esistono punti distinti P_∞, P_0, P_1 di S tali che per ogni punto $P \in S$ si abbia $(f_S P_\infty, f_S P_0, f_S P_1, f_S P) = (P_\infty, P_0, P_1, P)^p$. allora f_S è collineazione di S su S'.*

Dim. Sia $V = \sigma^{-1} sostS$, $V' = \sigma'^{-1} sostS'$, e poi $P_\infty = \sigma\langle v_\infty\rangle$, $P_0 = \sigma\langle v_0\rangle$, $P_1 = \sigma\langle v_0 + v_\infty\rangle$, come è possibile a norma del (2.24.1). Scelgo analogamente $f_S P_\infty = \sigma'\langle v'_\infty\rangle$, ecc.; ora $V = \langle v_\infty, v_0\rangle$, e $V' = \langle v'_\infty, v'_0\rangle$, sicché esiste un

p-semiisomorfismo f_V di V su tutto V' tale che $f_V v_\infty = v'_\infty$, $f_V v_0 = v'_0$ onde $f_V(v_0+v_\infty) = v'_0+v'_\infty$. Dico che $f_S \sigma \langle v \rangle = \sigma' \langle f_V v \rangle$ per ogni v, col che sarà dimostrato che f_S è collineazione (cfr. 2.21.1). E infatti $(f_S P_\infty, f_S P_0, f_S P_1, f_S P) = (P_\infty, P_0, P_1, P)^p = (P'_\infty, P'_0, P'_1, P')$, la prima eguaglianza per ipotesi su f_S, e la seconda perché la $\sigma \langle v \rangle \mapsto \sigma' \langle f_V v \rangle$ è collineazione. L'identità del primo e ultimo birapporto dimostrano quanto si voleva. C.V.D. □

Si noterà che ci si va sempre più allontanando da costruzioni "vettoriali" ed avvicinandosi a costruzioni "geometriche", intendendosi con questo quelle costruzioni e dimostrazioni che sfruttano solo le proprietà delle operazioni $+$ e $\cap$ negli spazi proiettivi ed il concetto di dimensione degli elementi (dette anche *proprietà di appartenenza*); del resto ciò non deve sorprendere se si pensa che la geometria proiettiva è nata dalla teoria della prospettiva nel disegno, e che solo recentemente si è inquinata con spazi vettoriali, prodotti esterni e altre diavolerie. Il (2.26.1) caratterizzerebbe le collineazioni fra rette senza ricorso a spazi vettoriali se si potesse definire il birapporto in maniera puramente geometrica. Questo non lo si può in realtà fare, ma si è visto nella lezione 25 che certi birapporti (quelli $= -1$) sono definibili geometricamente. E vi è inoltre un caso speciale nel quale basta conservare questi birapporti per avere una collineazione; il caso è in realtà abbastanza generale, in quanto copre tutte le caratteristiche eccetto 2; acquista però significato geometrico (mediante la costruzione grafica della lezione 25) solo se la retta su cui si considerano i birapporti è già sottospazio di un S_n con $n \geq 2$:

Teorema 2.26.2. *Siano S, S' rette proiettive sul corpo C di caratteristica $\neq 2 >$, e sia f un'applicazione di S su tutto S' che mandi vuoto su vuoto, sostegno su sostegno, e tale che fP, fQ, fM, fN sia gruppo armonico ogniqualvolta tale è P, Q, M, N; allora f è collineazione. Se poi C, come gruppo additivo è ordinato e archimedeo, f è proiettività.*

Dim. (Comessatti). Fissiamo P_∞, P_0, P_1, e $P'_i = fP_i$, sicché su S, S' sono fissate coordinate ascisse, ed f può essere considerata come applicazione di $C \cup \{\infty\}$ su tutto se stesso, che lascia fissi $\infty, 0, 1$; si deve dimostrare che f è automorfismo di C. $(0, 2x, x, \infty) = -1$ per (2.25.2), sicché $(0, f(2x), f(x), \infty) = -1$, onde $f(2x) = 2f(x)$ per (2.25.2). Poi $(2x, 2y, x+y, \infty) = -1$, onde $(2f(x), 2f(y), f(x+y), \infty) = -1$ che dà $f(x+y) = f(x) + f(y)$. Infine $(x, -x, 1, x^2) = -1$, onde $(f(x), f(-x), 1, f(x^2)) = -1$; ma $f(-x) + f(x) = f(-x+x) = f(0) = 0$, sicché $f(-x) = -f(x)$, e la precedente porge $f(x^2) = f(x)^2$; ora

$$\begin{aligned} 2f(xy) = f(2xy) &= f((x+y)^2 - x^2 - y^2) = \\ &= f((x+y)^2) - f(x^2) - f(y^2) = f(x+y)^2 - f(x)^2 - f(y)^2 = \\ &= \big(f(x) + f(y)\big)^2 - f(x)^2 - f(y)^2 = 2f(x)f(y), \end{aligned}$$

e ciò dimostra, con le precedenti, che f è automorfismo di C.

Se C è ordinato e archimedeo come gruppo additivo, esso è sottogruppo ordinato dei reali (2.39 di [AA]); la $f(x^2) = f(x)^2$ dice allora che le f-immagini dei positivi sono positive (2.40 di [AA]), sicché f è applicazione ordinata di C in sé; ma manda 1 su 1 perché è isomorfismo di corpi, sicché per la 2.38 di [AA] essa è l'applicazione identica di C in sé, e proviene quindi da una proiettività di S su S'. C.V.D. □

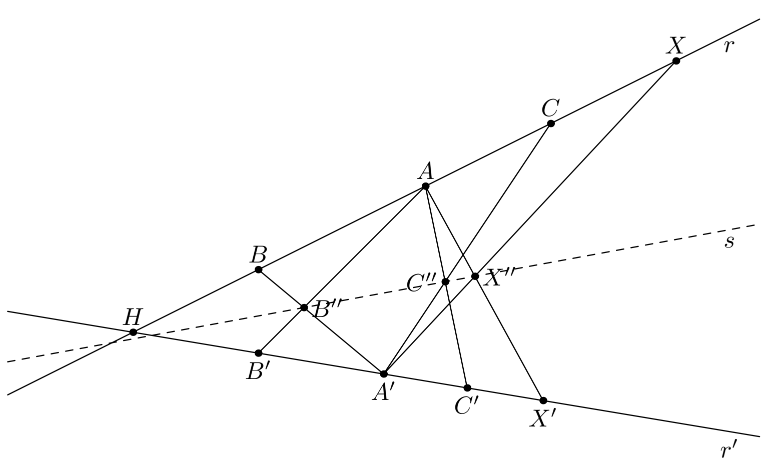
Si noti che in caratteristica $\neq 2$ il (2.26.2) darebbe una notevole semplificazione della prossima dimostrazione del punto 3 del Teorema 2.27.1.

Il Teorema 2.26.2 spiega la preminenza dei gruppi armonici nella geometria proiettiva classica: essa era costruita sul corpo reale, quindi per controllare che un'applicazione biunivoca fra rette fosse una proiettività bastava controllare che conservasse i gruppi armonici. [Fra parentesi, il nome gruppo armonico discende dalla musica: si credeva che un accordo musicale fosse gradevole quando le lunghezze delle corde (supposte ugualmente tese e dello stesso materiale) fossero in progressione armonica, e cioè tali che i loro reciproci (che ora sappiamo essere proporzionali alle frequenze) fossero in progressione aritmetica. Ed i numeri a, x, b sono appunto in progressione armonica se, e solo se, 0 e x separano armonicamente a, b. In pratica l'unica base per la credenza era l'accordo tonale maggiore (do mi sol), ove i rapporti delle frequenze, con 5 decimali esatti, e con la "scala temperata" usata oggigiorno, sono $4,00000 \ : \ 5,03968 \ : \ 5,99324$, abbastanza vicini a $4 : 5 : 6$.]

La speranza di poter fare tutto geometricamente, che fallisce nel caso più semplice (retta) fra i non banali (i banali sono il vuoto proiettivo ed il punto proiettivo), è invece ben riposta per gli spazi di dimensione > 1; a ciò è dedicato il resto di questa parte di lezioni. Prima di enunciare il risultato che segue, avvertiamo che la *proiezione in S di A da B su D* (usata sia come operazione, sia come risultato dell'operazione) significa la proiezione in S di A da B (ossia proiezione di centro B, ristretta ad A), seguita dalla sezione in S con D.

Lemma 2.26.3. *Siano r, r' rette di un piano proiettivo S_2, e siano R, R' i sottospazi proiettivi di S_2 di sostegni r, r'; allora ogni proiettività di R su R' è prodotto di al più tre proiezioni in S_2, di rette da punti su rette.*

Dim. Se $r \neq r'$ la dimostrazione è tutta contenuta nel disegno seguente:



La spiegazione è questa: la proiettività f manda A, B, C su A', B', C', ove A, A' sono diversi da $H = r \cap r'$ (possibile perché una retta ha almeno 3 punti, visto che un corpo ha almeno 2 elementi); per (2.24.3), queste tre coppie determinano la proiettività f. D'altra parte si costruiscano $B'' = (A + B') \cap (A' + B)$ e $C'' = (A + C') \cap (A' + C)$, che sono distinti, e si scriva $s = B'' + C''$ (questa s è detta *asse di collineazione*). Ora una proiettività g di R su R' può essere costruita così: partendo dal punto X di R, lo si proietti da A' su s, in X''; si proietti X'' da A su r', e sia questo $X' = gX$. La g è costruita con due proiezioni, e manda A, B, C in A', B', C'; dunque $g = f$ come voluto.

Se invece $r = r'$, usiamo un $r'' \neq r$, e costruiamo una proiettività h di R' su R'' mediante proiezione su R'' di R da un punto O fuori di r ed r''. Se f era la data da R ad R', la hf è fra R ed R'', onde per quanto precede hf è prodotto di due proiezioni; ma allora $f = h^{-1}hf$ è prodotto di tre. C.V.D. □

Il disegno del Lemma 2.26.3 dà un metodo pratico di costruzione di proiettività. Se la proiettività si può ottenere con una sola proiezione (di R, da un punto D, su R'), viene chiamata anche una *prospettività*, ed il D ne è il *centro di prospettiva*. Dimostrare per esercizio che:

Corollario 2.26.4. *Notazioni come in (2.26.3), ma con $r \neq r'$. Allora la data proiettività è una prospettività se, e solo se, il punto $H = r \cap r'$ corrisponde a se stesso.*

2.27 Lezione 27

Tre punti di un S_n si chiamano *allineati* se si appartengono con una medesima retta. Il risultato seguente è centrale, e dà fra l'altro il motivo del nome "collineazione"; è il primo teorema "sodo" di geometria proiettiva che esponiamo[3]

Teorema 2.27.1. *Siano S, S' piani proiettivi sui corpi C, C'; sia g applicazione biunivoca di S su tutto quello di S' che mandi terne di punti allineati su terne di punti allineati. Allora g è univocamente estensibile ad una collineazione di S su S'.*

Dim. Estendiamo subito la g così (e sarà chiaramente l'unica possibilità di estensione con speranza di rendere la g collineazione): $g(\text{vuoto di } S) = \text{vuoto di } S'$, $g(sostS) = sostS'$; poi, se r è retta di S, e per esempio $r = P + Q$, con P, Q punti, poniamo $gr = gP + gQ$; la condizione sull'allineamento mostra che questa è una buona definizione. Se poi $r \neq s$, è certo $gr \neq gs$: se infatti fosse $gr = gs$, per ogni punto P di S (escluso $r \cap s$) si trovino punti P_r, P_s, appartenentisi con r, s rispettivamente, tali che P, P_r, P_s siano allineati, e che né P_r né P_s coincida

[3] Il teorema seguente, o meglio, la sua successiva generalizzazione a dimensione maggiore, si trova spesso in letteratura con il nome di "Teorema Fondamentale della Geometria Proiettiva" (è questo il caso del libro [GA] Emil Artin, *Geometric Algebra* (Interscience, 1957)) e trova generalizzazioni a spazi proiettivi su anelli. Qui Barsotti si differenzia dalla tradizione e chiama Teorema Fondamentale un successivo teorema sulla decomposizione delle proiettività in una successione di proiezioni.

con $r \cap s$. Allora sono allineati gP, gP_r, gP_s, e inoltre, gP_r, gP_s sono distinti e si appartengono con gr; quindi gP si appartiene con gr, contro l'ipotesi che $\operatorname{im} g$ sia tutto il piano punteggiato. Si conclude che l'estensione di g ora costruita è iniettiva. È anche suriettiva: se infatti,r' è retta di S' e P', Q' sono punti che con essa si appartengono, si ha $r' = g(g^{-1}P' + g^{-1}Q')$.

La dimostrazione si articola in varie parti:

1. Scegliamo 3 punti allineati e distinti P_∞, P_0, P_1 in S e le loro g-immagini P'_i in S', che sono distinte e allineate. Se $r = P_\infty + P_0$ e $r' = gr = P'_\infty + P'_0$, per ogni punto X che si appartenga con r, l'$X' = gX$ si appartiene con r'. Dato allora $x \in C$, si cerchi X tale che $x = (P_\infty, P_0, P_1, X)$, e si ponga $x^p = (P'_\infty, P'_0, P'_1, X')$, ove maturalmente X' significa gX. La $x \mapsto x^p$ è applicazione di C su C'; proviamo anzitutto che essa è su tutto C': dato $x' \in C'$, scelto X' tale che $(P'_\infty, P'_0, P'_1, X') = x'$, basta dimostrare che $X' = gX$ per un X ben determinato. Può questo X non appartenersi con r? Se così fosse, la retta $X + P_0$ sarebbe diversa da r, ma avrebbe come g-immagine la $X' + P'_0 = r' = gr$, contro la dimostrata biunivocità di g anche fra rette.

2. Dimostriamo che l'applicazione p di C su C' costruita in 1 è indipendente dalla scelta di P_∞, P_0, P_1; si scelgano anche dei Q_∞, Q_0, Q_1, e sia q l'applicazione di C su C' che se ne ricava; sia $t = Q_\infty + Q_0$, e sia f la proiettività di R (retta proiettiva di sostegno r) su T (retta proiettiva di sostegno t) che manda P_i su Q_i; posto poi $Q'_i = gQ_i$, sia f' costruita analogamente tra R' e T'. Sia ha

$$\begin{aligned}(Q_\infty, Q_0, Q_1, X)^p = (P_\infty, P_0, P_1, f^{-1}X)^p = \\ = (P'_\infty, P'_0, P'_1, gf^{-1}X) = (Q'_\infty, Q'_0, Q'_1, f'gf^{-1}X);\end{aligned}$$

d'altra parte $(Q_\infty, Q_0, Q_1, X)^q = (Q'_\infty, Q'_0, Q'_1, gX)$, e si sarebbe a cavallo se si potesse dimostrare che $f'gf^{-1} = g$, ossia che $gfg^{-1} = f'$. Ora il (2.26.3) dice che f ed f' si ottengono con al più tre proiezioni; se perciò ogni proiezione (= proiezione e sezione) che si attua in S per costruire la f, viene ripetuta in S' con le g-immagini (dei centri delle proiezioni ecc.), si ottiene in S' la f'; ma d'altra parte la proiettività che si ottiene in S' è anche gfg^{-1}; quindi $gfg^{-1} = f'$, come voluto. resta così provato che $p = q$.

3. Ora mostriamo (seguendo una dimostrazione di Emil Artin) che p è isomorfismo di corpi; ci occorrono gli spazi vettoriali $V = \sigma^{-1} sostS$ e $V' = \sigma'^{-1} sostS'$, di dimensione 3; anzi, possiamo supporre che σ e σ' siano l'identità, cosicché g applica $[V]$ su $[V']$. Sia $V = \langle v_1, v_2, v_3 \rangle$, $V' = \langle v'_1, v'_2, v'_3 \rangle$, con $\langle v'_i \rangle = g \langle v_i \rangle$ e $\langle v'_1 + v'_2 + v'_3 \rangle = g \langle v_1, +v_2 + v_3 \rangle$ (possibile per 2.24.1). Poiché $\langle v_1 + v_2 \rangle$ è allineato con $\langle v_1 \rangle$, $\langle v_2 \rangle$, ed anche con $\langle v_3 \rangle$, $\langle v_1 + v_2 + v_3 \rangle$, lo stesso vale dopo aver applicato g, e ci dice che

$$g \langle v_1 + v_2 \rangle = \langle v'_1, v'_2 \rangle \cap \langle v'_3, v'_1 + v'_2 + v'_3 \rangle = \langle v'_1 + v'_2 \rangle .$$

Analogamente per $\langle v_2 + v_3 \rangle$ e $\langle v'_2 + v'_3 \rangle$. Visto questo, ricordiamo che il dire, per esempio, che $(\langle v_1 \rangle, \langle v_2 \rangle, \langle v_1 + v_2 \rangle, \langle v \rangle) = x \in C$ è equivalente a dire che $\langle v \rangle = \langle v_2 + xv_1 \rangle$. Ora si ha:

3a. $\langle v_1' + v_3' + (x+y)^p v_2' \rangle =$ [punto di S' che ha birapporto $(x+y)^p$ dopo $\langle v_2' \rangle$, $\langle v_1' + v_3' \rangle$, $\langle v_1' + v_2' + v_3' \rangle] =$ [g-immagine del punto di S che ha birapporto $x+y$ dopo $\langle v_2 \rangle$, $\langle v_1 + v_3 \rangle$, $\langle v_1 + v_2 + v_3 \rangle] = g\,\langle v_1 + v_3 + (x+y)v_2 \rangle \subseteq g(\langle v_1 + xv_2 \rangle + \langle v_3 + yv_2 \rangle) = \langle v_1' + x^p v_2' \rangle + \langle v_3' + y^p v_2' \rangle$.
Se ora si esprime il fatto che $v_1' + v_3' + (x+y)^p v_2'$ è combinazione lineare di $v_1' + x^p v_2'$ e $v_3' + y^p v_2'$, si trova che esso è la loro somma, e che perciò $(x+y)^p = x^p + y^p$.

3b. $\langle v_1' + x^p v_3' + (xy)^p v_2' \rangle =$ [punto di S' che ha birapporto $(xy)^p$ dopo $\langle v_2' \rangle$, $\langle v_1' + x^p v_3' \rangle$, $\langle v_1' + v_2' + x^p v_3' \rangle] =$ [g-immagine del punto di S che ha birapporto xy dopo $\langle v_2 \rangle$, $\langle v_1 + xv_3 \rangle$, $\langle v_1 + v_2 + xv_3 \rangle] = g\,\langle v_1 + xv_3 + (xy)v_2 \rangle \subseteq g(\langle v_1 \rangle + \langle v_3 + yv_2 \rangle) = \langle v_1' \rangle + \langle v_3' + y^p v_2' \rangle$.
Se ora si esprime il fatto che $v_1' + x^p v_3' + (xy)^p v_2'$ è combinazione lineare di v_1' e $v_3' + y^p v_2'$, si trova che è la somma del primo con il secondo moltiplicato per x^p, e che perciò $(xy)^p = x^p y^p$, ed è dimostrato che p è omomorfismo di corpi.

4. Resta da dimostrare che esiste un'applicazione p-semilineare h di V su tutto V' tale che $\langle hv \rangle = g\,\langle v \rangle$ per ogni v. Ma ora basta prendere $hv_i = v_i'$ per $i = 1, 2, 3$; infatti, per (2.26.1) e (2.24.3) si avrà $\langle hv \rangle = g\,\langle v \rangle$ per ogni $v \in \langle v_1, v_2 \rangle$; preso poi un $\langle w \rangle \neq \langle v_3 \rangle$, e anche $\neq \langle 0 \rangle$, sia $\langle v \rangle = \langle v_3, w \rangle \cap \langle v_1, v_2 \rangle$. Allora $g\,\langle v \rangle = \langle hv \rangle$ e $g\,\langle v_3 \rangle = \langle hv_3 \rangle$, onde di nuovo $g\,\langle w \rangle = \langle hw \rangle$ perché $\langle w \rangle$ è allineato con $\langle v \rangle$ e $\langle v_3 \rangle$. C.V.D. $\square$

2.28 Lezione 28

Teorema 2.28.1. *Il (2.27.1) resta vero quando S, S' siano spazi proiettivi di dimensione $n \geq 2$.*

Dim. Intanto, l'estensione di g da una applicazione di spazi punteggiati ad una di spazi proiettivi si fa come per il (2.27.1); in essenza consiste nell'identificare ogni $A \in S$ con l'insieme dei punti che con esso si appartengono. Con ciò si dimostra che g manda ogni sottospazio T di dimensione 2 in un T' di S'; e naturalmente nel così fare definisce, per (2.27.1), un isomorfismo p_T di C su tutto C'. La prima cosa da vedere è che questo p_T è in realtà indipendente da T. Se infatti T e Z sono due S_2, e se dim $(T \cap Z) \geq 1$, è certo $p_T = p_Z$, perché nella dimostrazione del Teorema 2.27.1 era bastata una retta per definire il p. Se invece, $T \cap Z$ ha dimensione ≤ 0, costruiamo una catena fra $sostT$ e $sostZ$ nel seguente modo: se $sostT = P_1 + P_2 + P_3$ (punti) e $sostZ = Q_1 + Q_2 + Q_3$, la catena è: $sostT = P_1 + P_2 + P_3$, $P_1 + P_2 + Q_1$ (se non va bene Q_1, ossia se $P_1 + P_2 + Q_1$ è una retta e non un piano, andrà bene Q_2 o Q_3), $P_1 + Q_1 + Q_2$, $Q_1 + Q_2 + Q_3 = sostZ$. Le intersezioni fra due elementi successivi della catena sono rette, onde di nuovo $p_T = \cdots = p_Z$; lo chiameremo p.

Ora occorre trovare l'applicazione p-semilineare f di $V = \sigma^{-1} sostS$ su tutto V' tale che $\langle fv \rangle = g\,\langle v \rangle$ per ogni v, avendo di nuovo supposto $\sigma = \sigma' = \iota$. Si comincia da basi $v_0, \ldots, v_n$ e $v_0', \ldots, v_n'$ tali che $\langle v_i' \rangle = g\,\langle v_i \rangle$, e che $\langle \sum_i v'i \rangle = g\,\langle \sum_i v_i \rangle$ (per 2.24.1), e si definisce $fv_i = v_i'$. Questa f manda una somma di v_i nella somma corrispondente di v_i'; quindi manda v_0, v_1, $v_0 + v_1$

in v_0', v_1', $v_0' + v_1'$; ma la g manda $\langle v_0 \rangle$ su $\langle v_0' \rangle$, $\langle v_1 \rangle$ su $\langle v_1' \rangle$, ed anche $\langle v_0 + v_1 \rangle$ su $\langle v_0' + v_1' \rangle$, perché il punto $\langle v_0 + v_1 \rangle$ è l'intersezione della retta $\langle v_0, v_1 \rangle$ con $\langle v_2, \ldots, v_n, v_0 + \cdots + v_n \rangle$. Quindi $\langle fv \rangle = g \langle v \rangle$ se $v \in \langle v_0, v_1 \rangle$, come nel punto 4 della dimostrazione del Teorema 2.27.1. Poi si prosegue con i $v \in \langle v_0, v_1, v_2 \rangle$, dato che ognuno sta nel $\langle w, v_2 \rangle$ per qualche $w \in \langle v_0, v_1 \rangle$, ecc. C.V.D. □

Siamo così giunti al

Teorema 2.28.2 (T. Fondamentale della Geometria Proiettiva)**.** *Siano T, T' sottospazi propri, della stessa dimensione m, di un S_n con $n \geq 1$; allora ogni proiettività di T su T' è prodotto di un numero finito di proiezioni in S_n (di certi S_r, da certi centri, su certi S_s').*

Dim. Se T, T' sono in uno stesso S_{m+1}, bene; se no, preso un $S_{m+1} \supset T$, proiettiamo T' su S_{m+1}, da un elemento di S_n che sia complementare di $sostS_{m+1}$ in S_n, e sghembo con $sostT'$. La proiezione T'' è contenuta nello stesso S_{m+1} che contiene T, e se il teorema è vero per T e T'' è anche vero per T e T'. Ci si è così ridotti al caso in cui $m = n - 1$. Se poi, in questo caso, $T = T'$, proiettiamo T' da un punto $P \notin T$ su un iperpiano di S_n diverso da T; ora siamo ridotti al caso in cui T e T' hanno sostegni che sono iperpiani diversi, la cui intersezione sarà perciò uno Z di dimensione $m - 1 = n - 2 \geq 0$.

Distinguiamo a questo punto due sottocasi:

1. Ogni punto P che si appartiene con Z corrisponde a se stesso: $fP = P$ se f è la data proiettività; dico allora che f è proiezione di T su T' in S_n da un punto U. Presi infatti punti Q_1, Q_2 di T che non si appartengano con Z, e posto $R = Z \cap (Q_1 + Q_2)$, da $fR = R$ segue che fQ_1, fQ_2, R sono allineati; quindi Q_1, Q_2, fQ_1, fQ_2 si appartengono con lo stesso piano, e le rette $Q_i + fQ_i$ si appartengono con un punto $U \in S_n$. Quando Q percorre i punti di T che non si appartengono con Z, le rette $Q + fQ$ sono incidenti perciò a 2 a 2; se $m > 1$ questo può accadere solo se il loro punto d'incontro è sempre lo stesso U; se invece $m = 1$, si può raggiungere la stessa conclusione nel modo seguente: la proiezione di T su T' da U (l'U trovato per primo) manda Z su Z (che ora è un punto), Q_1 su fQ_1, e Q_2 su fQ_2; quindi, per (2.24.3) essa coincide f.

2. Non ogni punto che si appartiene con Z corrisponde a se stesso; in questo caso la dimostrazione si fa per induzione su m, dato che per $m = 1$ il risultato è già noto (2.26.3). Sia dunque $m \geq 2$, e pongasi $Z' = fZ \in T'$; Sia L un iperpiano di S_n che si appartenga con Z', ma che non sia né $sostT$ né $sostT'$, e pongasi $Z'' = L \cap sostT$, sicché $\dim Z'' = m - 1$; sia g una arbitraria proiettività di T su T', che sia prodotto di proiezioni e mandi Z'' su Z (è facile costruirla). La fg ristretta a Z'' (che per risparmiare simboli sarà identificato col sottospazio che lo ha per sostegno), è proiettività di Z'' su Z', e per l'induzione è quindi costruibile, nello spazio L, mediante proiezioni da punti di L (diciamo $H_1, \ldots, H_r$) di sottospazi di L di dimensione $m-1$ (diciamo $Z_1 = Z'', Z_2, \ldots, Z_r$) su sottospazi della stessa dimensione, diciamo $Z_2, Z_3, \ldots, Z_{r+1} = Z'$. Se prendiamo per ogni Z_i un sottospazio Z_i' di S di dimensione m, che contenga Z_i ma non L, e in particolare, $Z_1' = T$ e $Z_{r+1}' = T'$, le proiezioni degli Z_i' dagli H_i sugli Z_{i+1}' danno una proiettività h, prodotto di proiezioni, che estende da T a T' la restrizione di fg a Z''.

Da $h = fg$ su $Z'' = g^{-1}Z$ si ottien $fg^{-1} = f$ su Z, onde $gh^{-1}f$ è proiettività di T su T' che induce l'identità su Z. Qui si casca nel caso 1, sicché $gh^{-1}f$ è prodotto di proiezioni; ma tali essendo h e g, anche f deve essere prodotto di proiezioni. C.V.D. □

Qui termina la esposizione dei fatti generali della geometria proiettiva; vi è naturalmente una messe di risultati particolari, che un tempo, in mancanza di teorie generali che ne permettessero la dimostrazione con metodi standard, dovevano essere studiati e dimostrati caso per caso. Una parte di questi sarà esposta nella sezione dedicata alle quadriche, sia perché di utilità immediata in altre parti della matematica ed anche in meccanica e fisica, sia perché a loro volta danno un esempio concreto di un'altra larga branca della geometria. Qui vogliamo solo dare l'enunciato (lasciando la dimostrazione come esercizio) di un teorema di notevole importanza storica. Nomenclatura: un *triangolo* consiste di tre punti A, B, C non allineati, e delle tre rette $a = B + C$, $b = A + C$, $c = A + B$. Due triangoli $ABCabc$ e $A'B'C'a'b'c'$ dello stesso S_n sono *omologici* rispetto ad una certa corrispondenza biunivoca (per esempio la $A \mapsto A'$, ecc) se i punti $a \cap a'$, $b \cap b'$, $c \cap c'$, sono allineati; sono invece *prospettivi* se le rette $A + A'$, $B + B'$, $C + C'$ si appartengono con uno stesso punto. Ciò premesso, l'asserto è il seguente:

Teorema 2.28.3 (di Desargues)**.** *Due triangoli sono omologici rispetto ad una certa corrispondenza biunivoca se, e solo se, sono prospettivi rispetto alla stessa corrispondenza.*

3
Matrici

3.29 Lezione 29

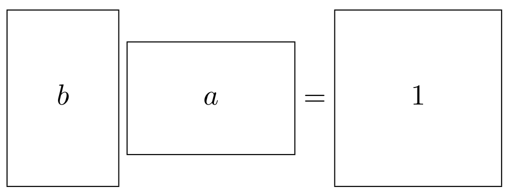
Si è già visto, e si continuerà a vedere nel seguito, che molti risultati sono riducibili a proprietà delle matrici (per esempio la dualità, le norme, le proiettività). Qui ci interessiamo appunto di matrici pure e semplici. In generale si constata che certe relazioni di equivalenza fra matrici sono interessanti, e si cerca allora se fra tutte le matrici equivalenti ad una data ve ne sia una, o alcune, più semplice delle altre; questa matrice più semplice si chiama la *forma canonica* della data rispetto a quella particolare equivalenza.

Un primo tipo di equivalenza è la congruenza (lezione 8), che si è visto essere utile quando si parla di forme quadratiche, norma dualità, ecc.; è una relazione di equivalenza fra matrici ad elementi in un corpo, che però è importante solo quando ci si limita a matrici che siano simmetriche o antisimmetriche, e quando inoltre il corpo non abbia caratteristica 2; la *forma canonica per congruenza* è descritta nei (1.14.5), (1.14.6); quella di una matrice antisimmetrica nei (1.9.4), (1.10.2). Non parleremo quindi più della congruenza.

Prima di parlare di altri tipi di equivalenza ci occorre la nozione di modulo: Sia A un anello, che supporremo sempre commutativo e dotato di identità; un A-*modulo* (sinistro) è un insieme M, con un'operazione $+$ ($m + n \in M$ per $m, n \in M$), ed una operazione di prodotto per scalari ($am \in M$ per $a \in A$ ed $m \in M$) soddisfacenti a tutti gli assiomi che dovrebbero essere soddisfatti se A fosse un corpo ed M uno spazio vettoriale su A; in effetti, se A è un corpo, un A-modulo è proprio uno spazio vettoriale su A. I nostri A-moduli si supporranno sempre *unitari* ossia tali che $1m = m$ per ogni $m \in M$ (1 è l'identità di A). Le definizioni di omomorfismo, isomorfismo, somma, complementare, ecc., di A-moduli possono essere immaginate; valgono i tre teoremi di isomorfismo; si può anche immaginare che cosa sia un insieme di generatori di un A-modulo. Negli A-moduli si può parlare di elementi linearmente dipendenti o indipendenti (su A), e si può parlare di combinazioni lineari; non è però vero che se certi elementi sono linearmente dipendenti, uno di essi debba essere combinazione lineare degli altri; quindi non si può parlare di "base" o di "dimensione".

Un A-modulo generato da elementi indipendenti $x_1, x_2, \dots$ dicesi *libero* o *liberamente generato* (dagli x_i), e gli x_i i suoi *generatori liberi* (il fatto di aver indicizzato gli x con gli interi non sta ad indicare che essi siano al più una infinità numerabile). Un A-modulo generato da un numero finito di elementi dicesi *finitamente generato*, od anche *finito*; uno con un solo generatore dicesi *ciclico*; uno senza sotto-A-moduli propri $\neq \{0\}$ dicesi *semplice*; vale il Teorema di Jordan-Hölder[1].

Sia M un A-modulo finito, generato da $x_1, \dots, x_m$; si chiede se esso è anche generato da $y_1, \dots, y_n$ (suoi elementi). Ciò sarà vero se, e solo se, esistono elementi a_{ij}, b_{rs} in A tali che $y_i = \sum_j a_{ij}x_j$, $x_r = \sum_s b_{rs}y_s$; niente di strano. Suppongasi però ora che tanto le x quanto le y generino M liberamente; allora $x_r = \sum_s b_{rs}y_s = \sum_{sj} b_{rs}a_{sj}x_j$, e $y_i = \sum_j a_{ij}x_j = \sum_{js} a_{ij}b_{js}y_s$, donde, per la libertà, $\sum_s b_{rs}a_{sj} = \delta_{rj}$, $\sum_j a_{ij}b_{js} = \delta_{is}$. Se si sapesse che le matrici (a_{ij}), (b_{rs}) sono quadrate, ossia che $m = n$, queste ultime direbbero che esse sono l'una la reciproca dell'altra; e che esse siano quadrate lo si vede così: se fosse $m > n$, la (a_{ij}) avrebbe meno righe che colonne, e la prima delle relazione precedenti visualmente apparirebbe così:


;

aggiungendo $m - n$ ultime colonne nulle alla b, ed $n - m$ ultime righe nulle alla a, la relazione resterebbe vera, il che è ovviamente impossibile perché ciascuna matrice al primo membro ha ora determinante nullo [parentesi quadra per i pignolissimi: la teoria dei determinanti l'abbiamo svolta per matrici ad elementi in un corpo, mentre queste hanno elementi in un anello; però la definizione di determinante e il teorema di Binet, possono essere trasferiti da un corpo ad un anello col metodo seguito per il pfaffiano: si parte da matrici ad elementi che sono indeterminate, e quindi in un corpo, e poi si applica un omomorfismo che manda queste indeterminate su elementi dell'anello A]. Concludiamo perciò col

Lemma 3.29.1. *Sia M un A-modulo libero finito, e ne sia $\{x_1, \dots, x_m\}$ un insieme di generatori liberi; il numero m dipende solo da M, e le $y_i = \sum_j a_{ij}x_j$ $(i = 1, \dots, m)$ formano un insieme di generatori, certo liberi, di M se, e solo se, la matrice (a_{ij}) è invertibile su A, ossia se, e solo se,* $\det(a_{ij})$ *è una unità di A.*

Il numero m si dirà l'*ordine* di M (se A è un corpo, esso è la dimensione dello spazio vettoriale M). Sia N un sotto-A-modulo finito di M, con generatori liberi $y_1, \dots, y_n$, e sia H la matrice (h_{ij}) tale che $y_i = \sum_j h_{ij}x_j$; se si sostituiscono i generatori liberi x_i con degli x'_i (sempre liberi), e gli y_i con degli y'_i, sarà analogamente $y'_i = \sum_j h'_{ij}x'_j$; ci sono poi le matrici $P = (p_{ij})$, $Q = (q_{ij})$ tali che

[1] Si veda la Lezione 25 di [AA].

$y'_i = \sum_j p_{ij} y_j$, $x_i = \sum_j q_{ij} x'_j$, sicché

$$y'_i = \sum_j p_{ij} y_j = \sum_{jr} p_{ij} h_{jr} x_r = \sum_{jrs} p_{ij} h_{jr} q_{rs} x'_s.$$

La libertà dà ora $H' = PHQ$; notare che: H ed H' sono $n \times m$; P è $n \times n$; Q è $m \times m$; P e Q sono invertibili su A. Morale: se H è una matrice legata ad un sotto-A-modulo libero di M nel modo detto, un cambiamento dei generatori liberi manda H nella $H' = PHQ$, con P, Q invertibili su A. Anche questa è una relazione di equivalenza fra matrici presentatasi in modo naturale; è detta appunto *equivalenza* (in A).

Strettamente legate ad esse sono le *operazioni elementari* (in A) sulle matrici; esse sono le seguenti:

Operazioni elementari *sulle righe* (o *a sinistra*):

1. Moltiplicare una riga (ossia tutti i suoi elementi) per una unità dell'anello A;
2. Scambiare fra loro due righe;
3. Aggiungere ad una riga il prodotto di un'altra per un elemento di A.

Operazioni elementari *sulle colonne* (o *a destra*): stessa roba, ma con le colonne.

Osserviamo che:

1. Moltiplicare la prima riga per $c \in A$ significa moltiplicare la data matrice, a sinistra, per
$$\begin{pmatrix} c & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix};$$
questa è invertibile se c è unità (se fosse stata la i-esima riga, l'elemento c sarebbe andato nel posto (i, i));
2. Scambiare la prima con la seconda riga vuol dire moltiplicare a sinistra per ;
$$\begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix};$$
invertibile su A;
3. Aggiungere alla prima riga la seconda moltiplicata per c vuol dire moltiplicare a sinistra per.
$$\begin{pmatrix} 1 & c & & & \\ 0 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix};$$
anche questa è invertibile su A.

Le operazioni elementari sulle colonne sono analoghe, ma con moltiplicazione a destra. Perciò la matrice ottenuta da H mediante operazioni elementari è equivalente ad H; vedremo che, sotto certe condizioni, vale anche il reciproco.

3.30 Lezione 30

Lemma 3.30.1. *Sia A campo d'integrità a ideali principali, e sia $M = \left(\begin{smallmatrix} a & b \\ a' & b' \end{smallmatrix}\right)$, ad elementi in A; sia d un MCD di a, b, e pongasi $d = pa + bq$, con $p, q \in A$. Posto $V = \begin{pmatrix} p & b/d \\ q & -a/d \end{pmatrix}$, la V è invertibile in A, ed MV (che è equivalente ad M) ha l'elemento d nel posto $(1, 1)$.*

Dim. L'elemento di posto $(1,1)$ in MV è $ap + bq = d$; si ha poi $\det V = -\frac{pa+bq}{d} = -1$. C.V.D. □

Siamo ora in grado di dimostrare il seguente risultato fondamentale:

Teorema 3.30.2 (dei divisori elementari)**.** *Sia A come in (3.30.1), e sia M matrice $m \times n$ ad elementi in A, con, per esempio, $n \leq m$; allora M è equivalente in A ad una matrice in cui tutti gli elementi sono 0 esclusi al più quelli di posto (i, i) $(i = 1, \dots, n)$, che sono uguali a certi e_i, con la proprietà che e_{i+1} è multiplo di e_i. Tali e_i, detti i* fattori invarianti *di M, sono univocamente determinati a meno di fattori unità di A. Ed anzi, $e_1 e_2 \cdots e_i$ è un MCD dei minori di ordine i di M.*

Dim. Per ogni $a \in A$ non nullo sia $h(a)$ il numero dei suoi fattori primi, distinti o no; e per una matrice N sia $h(N)$ il minimo tra gli h degli elementi non nulli di N. Fra le N equivalenti ad M se ne scelga una, per esempio N, il cui $h(N)$ sia minimo; per mezzo di scambi di righe e di colonne si porti al posto $(1, 1)$ un elemento a di N tale che $h(a) = h(N)$ (si chiami ancora N la matrice ottenuta). Ora a divide tutti gli elementi della prima riga di N, ed anche tutti quelli della prima colonna: ché altrimenti, per (3.30.1) (ove la matrice 2×2 che vi compare è un pezzo della N), l'a potrebbe essere sostituito con un d tale che $h(d) < h(a)$, e ciò mediante moltiplicazione a destra o sinistra per una V invertibile. Ciò visto, con l'operazione elementare 3 tutti gli elementi della prima riga e quelli della prima colonna, eccetto l'a al posto $(1, 1)$, possono essere fatti diventare 0; la N è ora equivalente alla $\begin{pmatrix} a & {}^t0 \\ 0 & N_1 \end{pmatrix}$. Ripetiamo con N_1, eccetera, fino ad ottenere la

$$N' = \begin{pmatrix} e_1 & & & \\ & e_2 & & \\ & & \ddots & \\ & & & e_n \\ 0 & \dots & \dots & 0 \\ \vdots & & & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix}.$$

L'e_1 è a; se esso non dividesse e_2, e per esempio un loro MCD fosse d, la $\left(\begin{smallmatrix} e_1 & \\ & e_2 \end{smallmatrix}\right)$ sarebbe equivalente a $\left(\begin{smallmatrix} e_1 & e_2 \\ & e_2 \end{smallmatrix}\right)$, e questa, per (3.30.1), ad una avente d nel posto $(1, 1)$, impossibile; per lo stesso motivo e_2 divide e_3, ecc. Infine è vero che $e_1 e_2 \cdots e_i$ è un MCD dei minori di ordine i di N'; resta da vedere che abbia lo stesso ufficio per M. Ora $M = PN'Q$, ed $N' = P^{-1} M Q^{-1}$; l'asserto deriva allora dal seguente teorema di Binet generalizzato, la cui dimostrazione è conseguenza del (1.6.2): *in un prodotto RS di matrici, il minore formato con le righe*

$i_1, \ldots, i_r$ e le colonne $j_1, \ldots, j_r$ è la somma di tutti i prodotti dei minori di R estratti dalle righe $i_1, \ldots, i_r$ per i corrispondenti minori di S estratti dalle colonne $j_1, \ldots, j_r$ ("corrispondenti" vuol dire che le colonne del primo fattore e le righe del secondo hanno gli stessi indici). C.V.D. □

3.31 Lezione 31

Il Teorema 3.30.2 ci dà la forma canonica rispetto all'equivalenza, ed anche per matrici rettangolari; il nome deriva dalla definizione seguente: si scrive ogni e_i che non sia né unità né 0 come prodotto di potenze di elementi primi distinti:

$$e_i = p_1^{h(i,1)} p_2^{h(i,2)} \cdots p_s^{h(i,s)};$$

dovrà essere $h(i+1,j) \geq h(i,j)$. Gli elementi $p_j^{h(i,j)}$ in cui $h(i,j) > 0$ sono i *divisori elementari* di M. Il (3.30.2) stesso ha un'importante conseguenza per gli A-moduli; ci occorre prima il

Lemma 3.31.1. *Sia A campo d'integrità a ideali principali e sia M un A-modulo libero di ordine m; allora ogni sottomodulo N di M è libero e di ordine $\leq m$. È inoltre possibile scegliere insiemi liberi di generatori $x_1, \ldots, x_m$ di M ed $y_1, \ldots, y_n$ di N tali che $y_i = e_i x_i$, ove $0 \neq e_i \in A$ ed e_i divide e_{i+1}; gli e_i sono univocamente determinati, a meno di fattori che sono unità di A, da M ed N.*

Dim. Primo asserto: per induzione su m, visto che è banalmente vero per $m = 1$ (perché?). Sia $\{x_1, \ldots, x_m\}$ insieme di generatori liberi di M; se $N \subseteq Ax_1 + \cdots + Ax_{m-1}$, esso N è libero per l'induzione. Se no, l'insieme degli $a_m \in A$ per ciascuno dei quali esistono degli $a_1, \ldots, a_{m-1} \in A$ tali che $\sum_{i=1}^m a_i x_i \in N$, è un ideale $(b_m) \neq (0)$ di A. Siano $b_1, \ldots, b_{m-1} \in A$ tali che $y = \sum_{i=1}^m b_i x_i \in N$. Per ogni $x \in N$ esiste un $a \in A$ tale che $x - ay \in N \cap (Ax_1 + \cdots + Ax_{m-1})$ (per la proprietà di b_m); quindi N è somma diretta dell'A-modulo ora scritto, che per la ricorrenza è libero, e di Ay; ne segue che N è libero ed è ovvio che ha ordine $\leq m$ (se si estende tutto sul corpo quoziente di A, gli ordini diventano dimensioni di spazi vettoriali).

Secondo asserto: è conseguenza immediata del (3.30.2), e della interpretazione sugli A-moduli dell'equivalenza fra matrici (lezione 29); notare che gli e_i di (3.30.2) che sono uguali a 0 vengono buttati via. C.V.D. □

La conseguenza importante del Teorema 3.30.2 cui si è accennato è la seguente:

Teorema 3.31.2. *Sia A come nel Lemma 3.31.1, e sia M un A-modulo finito; allora M è somma diretta di A-moduli ciclici, e più precisamente $M \cong \sum_i A/e_i A$, ove gli e_i sono non unità di A ed e_{i+1} è multiplo di e_i. Gli ideali (e_i) sono univocamente determinati da queste condizioni.*

Dim. Sia M_0 l'A-modulo libero finito A^m, ove m è la cardinalità di un insieme di generatori di M; se $z_1, \ldots, z_m$ generano M, l'applicazione di M_0 su M che manda $(a_1, a_2, \ldots, a_m)$ su $a_1 z_1 + \cdots + a_m z_m$ è un omomorfismo di M_0 su tutto M. Quindi $M \cong M_0/N$ per un opportuno sotto-A-modulo N di M_0. Scelte in M_0 ed N le x, y come nel (3.31.1), si ha $M_0 = Ax_1 \oplus \cdots \oplus Ax_m$, $N = Ay_1 \oplus \cdots \oplus Ay_n = Ae_1x_1 \oplus \cdots \oplus Ae_nx_n$, onde

$$M \cong A/Ae_1 \oplus \cdots A/Ae_n \oplus Ax_{n+1} \oplus \cdots \oplus Ax_m.$$

Ma per $i > n$ si ha $Ax_i \cong A = A/0A$, ossia si prende $e_i = 0$ per questi casi. Se poi qualche e_i (fra i non nulli) è unità di A, lo si butta via perché in tal caso $A/Ae_i = (0)$; supporremo che non sia stato necessario fare questo, sicché i continua ad avere i valori $1, \ldots, m$.

Resta solo da dimostrare l'unicità degli e_i; osserviamo anzitutto che la somma degli A/Ae_i con $e_i \neq 0$ (ossia per $i = 1, \ldots, n$) corrisponde al sotto-A-modulo M' di M formato dagli elementi *a torsione*, ossia degli x tali che $ax = 0$ per qualche $a \neq 0$. Tale M' è ovviamente ben determinato, e perciò è ben determinato l'ordine di M/M', che è un A-modulo libero, isomorfo alla somma di quelli, fra gli A/Ae_i, per i quali $e_i = 0$; quindi il numero di questi, ossia $m - n$, dipende solo da M. Vediamo ora gli e_i non nulli; per fare questo si lavorerà su M', onde possiamo addirittura supporre che $M = M'$, ossia che M sia *a torsione* (il che vuol dire che ogni suo elemento è a torsione). Intanto M ha una certa lunghezza $h(M)$ nel senso del Teorema di Jordan-Hölder (2.19 di [AA]): essa è la cardinalità, diminuita di 1, di una qualsiasi catena massimale di sotto-A-moduli di M; si vede subito che, espresso il prodotto $e_1, \ldots, e_n$ come prodotto di elementi primi (distinti o no), tale lunghezza è il numero di questi fattori primi [basta tenere presente che una catena massimale in $A/(p_1 \cdots p_r)$, con i p_i primi, è data dagli $A/(p_1 \cdots p_s)$ per $s = 1, \ldots, r$]. Ciò comporta subito che se $h(M) = 1$ esiste il solo e_1, che esso è primo, e che (e_1) è univocamente determinato in quanto esso è l'*annullatore* di M (ossia l'insieme degli $a \in A$ tali che $ax = 0$ per ogni $x \in M$). La dimostrazione può ora farsi per induzione su h: constatato che (e_n) è l'annullatore di M, e che quindi esso è univocamente determinato, sia p un divisore primo di e_n, sia P il sotto-A-modulo di M formato dagli $x \in M$ tali che $px = 0$, e pongasi $Q = M/P$. Se p divide $e_r, \ldots, e_n$, ma non e_{r-1}, si ha

$$P \cong \sum_{i=r}^{n} \frac{(e_i/p)}{(e_i)}, \qquad \text{e} \qquad Q = \sum_{i=1}^{r-1} \frac{A}{(e_i)} \oplus \sum_{i=r}^{n} \frac{A}{(e_i/p)}.$$

Poiché $h(Q) < h(M)$, per la ricorrenza gli (e_i) $(i = 1, \ldots, r-1)$ e gli (e_i/p) $(i = r, \ldots, n)$ sono determinati; anche il numero $n - r + 1$ di questi ultimi è determinato, perché P è isomorfo alla somma diretta di $n - r + 1$ corpi isomorfi ad $A/(p)$. Quindi $(e_1), \ldots, (e_n)$ sono determinati. C.V.D. □

Notare che, come già visto nella dimostrazione, il numero di e_i che sono nulli è l'ordine dell'addendo libero di M.

3.32 Lezione 32

Prima di passare ad altro osserviamo che:

Lemma 3.32.1. *Se A è campo d'integrità euclideo, due matrici ad elementi in A sono equivalenti se, e solo se, sono ottenibili l'una dall'altra mediante operazioni elementari.*

Dim. In una direzione lo sappiamo già (lezione 29). Per l'altra direzione, notiamo che tutta la dimostrazione del (3.30.2) può essere ripetuta per gli euclidei,usando per $h(a)$ il grado di a nel senso euclideo, e usando in luogo della equivalenza la *equivalenza elementare* (ossia la trasformabilità l'una nell'altra per mezzo di operazioni elementari su righe e colonne). Quando si arriva al punto in cui occorre il Lemma 3.30.1, si ragiona così: "ché altrimenti uno di questi elementi, non divisibile per a, potrebbe essere sostituito, con la operazione elementare 3, col resto della propria divisione per a; e ciò contro l'ipotesi su $h(a)$". Tutto il resto fila liscio. Si conclude che una matrice ha la stessa forma canonica per equivalenza o per equivalenza elementare; perciò i due tipi di equivalenza coincidono. C.V.D. □

Una famosa applicazione del (3.31.2):

Teorema 3.32.2. *Ogni gruppo abeliano finito è somma diretta di gruppi ciclici; resta vero se si sostituisce "finito" con "finitamente generato".*

(Dimostrarlo per esercizio).

Ed ora passiamo al terzo ed ultimo tipo di equivalenza fra matrici, quella data da $M' = PMP^{-1}$ (su un corpo C), con P nonsingolare; le matrici M, M' diconsi *simili*; è il tipo di equivalenza che si trova come risposta alla domanda: sotto quali condizioni M ed M' rappresentano lo stesso elemento di $\mathrm{End}_C V$ rispetto a basi diverse? (V è uno spazio vettoriale su C, di dimensione n). Anche la simiglianza è riconducibile a dei moduli: sia x una indeterminata su C, pongasi $K = C[x]$, e si costruisca un K-modulo il cui supporto (=insieme dei suoi elementi) è ancora V, e che quindi verrà ancora indicato con V, nel modo seguente: fissato un $\alpha \in \mathrm{End}_C V$, si porrà $(f(x))v = (f(\alpha))v$ per $v \in V$ e per $f(x) \in K$; la $f(\alpha)$ ha un ovvio significato. Si noti che la definizione precedente è in accordo con la moltiplicazione scalare nello spazio vettoriale V.

Il Teorema 3.31.2 assicura che esistono $v_r, \dots, v_n \in V$, con $r \geq 1$, tali che V sia la somma diretta dei Kv_i, e che l'annullatore di v_i sia l'ideale di K generato da un certo $e_i = e_i(x)$, di grado positivo nella x, e tale che e_i divida e_{i+1} per $r \leq i < n$. Vi è dell'arbitrarietà nella scelta degli e_i, ma la elimineremo col richiedere che essi siano polinomi monici (nessuno di essi è nullo perché V è spazio vettoriale di dimensione finita su C, e quindi non contiene sottospazi isomorfi a K).

L'e_n è particolarmente importante; infatti $e_n(\alpha)v_i = 0$ per ogni i, onde (dato che gli $\alpha^j v_i$ generano V su C) anche $e_n(\alpha)v = 0$ per ogni $v \in V$, sicché $e_n(\alpha) = 0$. D'altra parte, se $f(x) \in K$ è tale che $f(\alpha) = 0$, da $f(\alpha)v_n = 0$ segue che $f(x)$ è multiplo di $e_n(x)$; perciò $e_n(x)$ è il generatore monico dell'ideale formato dagli $f(x) \in C[x]$ tali che $f(\alpha) = 0$; è detto il *polinomio minimo*, o *funzione minima*, di α [che esso dovesse esistere lo si sapeva a priori, perché fra gli $1, \alpha, \alpha^2, \alpha^3, \dots$ ce n'è al massimo n^2 di linearmente indipendenti su C].

3.33 Lezione 33

Continuando, suppongasi che un certo $e_i(x)$, che chiameremo $e(x)$ per risparmiare indici, sia della forma

(3.33.1) $$e(x) = x^s - a_{s-1}x^{s-1} - \cdots - a_0 \qquad (s \text{ dovrebbe essere } s_i);$$

le $\alpha^j v_h$ $(h = r, \ldots, n;\ j = 0, 1, \ldots, s-1)$ formano una base di V su C; dato che α trasforma ogni Kv_h in sé, la matrice B associata ad α per mezzo di quella base è formata di blocchi:

$$B = \begin{pmatrix} B_r & & & \\ & B_{r+1} & & \\ & & \ddots & \\ & & & B_n \end{pmatrix},$$

ove il blocco B_i (sempre la i che si era tralasciato di scrivere) è dato da $B_i = (b_{hj})$, con $\alpha(\alpha^{j-1}v_i) = \sum_{h=1}^{s} b_{hj}(\alpha^{h-1}v_i)$; questa dà $b_{hj} = 0$ eccetto che nei casi seguenti: $b_{j+1,j} = 1$ se $j < s$; $b_{hs} = a_{h-1}$. Visualmente:

(3.33.2) $$B_i = \begin{pmatrix} 0 & \ldots & 0 & a_0 \\ 1 & & & a_1 \\ & \ddots & & \vdots \\ & & 1 & a_{s-1} \end{pmatrix}, \qquad \text{ovvero } B_i = a_0 \text{ se } s = 1.$$

La matrice (3.33.2) si chiama la *compagna* del polinomio (3.33.1). Prima di concludere prendiamo la matrice $x - B_i$ e ne cerchiamo i fattori invarianti in K; il criterio enunciato alla fine del Teorema 3.30.2 dice che essi sono $1, 1, \ldots, 1, \det(x - B_i) = e_i(x)$. Quindi i fattori invarianti di $x - B$, in K, sono $1, \ldots, 1, e_r(x), \ldots, e_n(x)$ (tanti quanti ne occorrono per avere n fattori invarianti). La B è la matrice associata ad α mediante una certa base speciale di V (la $\alpha^j v_h$); in un altra base qualsiasi, α avrà una certa matrice M, simile a B: $B = P^{-1}MP$; le matrici $x - M$, $x - B$ sono legate da $x - B = P^{-1}(x - M)P$, e sono perciò equivalenti su K; ne segue che gli $1, \ldots, 1, e_r(x), \ldots, e_n(x)$ sono anche i fattori invarianti di $x - M$, cosicché abbiamo dimostrato che ogni matrice M ad elementi in C è simile, su C, ad una B del tipo descritto, costruita con le compagne dei fattori invarianti $\neq 1$ della $x - M$ su K. Pertanto M ed M' sono simili se, e solo se, hanno la stessa B, e quindi se, e solo se, $x - M$, $x - M'$ sono equivalenti su K. Morale:

Teorema 3.33.3 (il cui ultimo asserto è il Teorema di Frobenius)**.** *Due matrici M, M', quadrate di ordine n ad elementi nel corpo C, sono simili in C se, e solo se, le $x - M$, $x - M'$ sono equivalenti in $C[x]$, x essendo una indeterminata. Se $e_r(x), \ldots, e_n(x)$ sono i fattori invarianti monici diversi da 1 di $x - M$ in $C[x]$, la M è simile in C ad una matrice fatta di blocchi sulla diagonale, tali blocchi essendo le matrici compagne degli $e_i(x)$. Infine, $e_n(x)$ è il polinomio minimo di M, ed è uguale al rapporto fra* $\det(x - M)$ *ed il MCD in $C[x]$ dei minori di ordine $n - 1$ di $x - M$.*

La matrice simile a B, fatta con le compagne, dicesi la *forma canonica di Jordan* di B, ed è unica (si intende, forma canonica per simiglianza).

3.34 Lezione 34

La forma canonica di Jordan ha l'inconveniente (psicologico) che matrici diagonali possono benissimo avere forme canoniche non diagonali (trovarne qualcuna per esercizio). Si ovvia a questo inconveniente per mezzo di altre forme canoniche che ora descriveremo. Osserviamo dapprima che se $f(x)$, $g(x)$ sono polinomi monici primi fra loro, con le matrici compagne F, G, la matrice $\left(\begin{smallmatrix} F & 0 \\ 0 & G \end{smallmatrix}\right)$ ha come fattori invarianti una sfilza di numeri 1, ed fg (lo si vede col MCD dei minori; per accettata improprietà di linguaggio si parla talvolta dei "fattori invarianti della matrice M" intendendo in realtà i "fattori invarianti della matrice $x-M$"); perciò essa è simile alla compagna di fg. Questo, ed il (3.33.3), danno subito:

Corollario 3.34.1. *Notazioni come nel Teorema 3.33.3; allora B è simile ad una matrice fatta di blocchi diagonali, tali blocchi essendo le matrici compagne dei divisori elementari di $x - B$ in $C[x]$.*

Anche questa è una forma canonica per simiglianza (senza nome). Sia infine $f(x)$ monico irriducibile, e sia F la sua compagna; sia N una matrice quadrata, di ordine r uguale a quello di F, ossia al grado di f, i cui elementi siano tutti 0, eccetto quello della prima riga ed ultima colonna, che è 1; se h è un intero positivo, pongasi

$$G = \begin{pmatrix} F & 0 & \dots & \dots & 0 \\ N & F & \ddots & & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & N & F \end{pmatrix},$$

con h blocchi uguali ad F ed $h-1$ uguali ad N. In G c'è una fila ininterrotta di numeri 1 subito sotto la diagonale principale; quindi i fattori invarianti di $x-G$, eccetto l'ultimo, sono 1; l'ultimo è $\det(x-G) = (\det(x-F))^h = f(x)^h$. Perciò G è simile alla matrice compagna di f^h, e si chiama la *ipercompagna* di f^h. Il (3.34.1) dà ora:

Corollario 3.34.2. *Notazioni come nel Teorema 3.33.3; allora B è simile ad una matrice fatta di blocchi diagonali, tali blocchi essendo le matrici ipercompagne dei divisori elementari di $x - B$ in $C[x]$.*

Questa forma canonica dicesi la *forma canonica razionale*, e dipende in modo essenziale da C (anche la precedente): si nota infatti che se C' è prolungamento[2] di C, i fattori invarianti di C sono gli stessi se computati in $C[x]$ o $C'[x]$; ma i divisori elementari cambiano.

[2]Per Barsotti il termine "prolungamento" è sinonimo di "estensione", ovvero qui si dice che C' è un corpo che contiene C come sottocorpo. [NdR]

Vediamo un'altra cosa; data la M quadrata di ordine n ad elementi in C, il $\det(x-M)=g(x)$ non cambia se M viene sostituita con una simile:

$$\begin{aligned}\det(x-P^{-1}MP) &= \det\left(P^{-1}(x-M)P\right) = \\ &= (\det P^{-1})(\det(x-M))(\det P) = \det(x-M).\end{aligned}$$

Se allora B è la forma canonica di Jordan di M, e se $e_1(x),\dots,e_n(x)$ sono i fattori invarianti di $x-M$ in $C[x]$, si ha

(3.34.3) $$g(x)=\det(x-M)=\det(x-B)=e_1(x)\cdots e_n(x).$$

Il polinomio $g(x)$ ora introdotto si chiama il *polinomio caratteristico* (o *funzione caratteristica* di M; ricordando che $e_n(x)$ era il polinomo minimo, e che gli altri $e_i(x)$ dividono $e_n(x)$, si vede che

3.34.4. *Il polinomio caratteristico è multiplo del polinomio minimo, ma ne ha gli stessi fattori primi, eventualmente con esponenti maggiori. Se n è l'ordine della matrice, il coefficiente di $(-1)^iX^{n-i}$ nel polinomio caratteristico uguaglia la somma dei minori principali di ordine i della matrice (per $i=1$ tale somma è la traccia della matrice).*

Osservando che $e_n(M)=0$ se ne deduce $g(M)=0$, donde il famoso:

Teorema 3.34.5 (di Hamilton-Cayley)**.** *Sia $g(x)$ il polinomio caratteristico di una matrice M (quadrata ad elementi in un corpo). Allora $g(M)=0$.*

Domande: $g(x)$, se C è algebricamente chiuso, ha già n zeri in C, se n è il suo grado; come la mettiamo l'aver trovato un altro zero, ossia M? Perché non si poteva dimostrare il (3.34.5) dicendo semplicemente che $g(M)=[g(x)]_{x=M}=[\det x-M]_{x=M}=\det(M-M)=0$? Si può definire il polinomio caratteristico di un $\alpha\in\mathrm{End}_C V$?

3.35 Lezione 35

La "equazione" $g(x)=0$ si chiama l'*equazione secolare* di M; il nome è dovuto al fatto che fu notata per la prima volta nel problema di sapere come mai l'effetto combinato di tutti i pianeti del sole su uno di essi è di farne avanzare il perielio di un piccolo angolo ogni secolo. Le sue radici in C, ossia gli zeri di $g(x)$ in C, si chiamano gli *autovalori*, o *radici caratteristiche*, di M in C (o di $\alpha\in\mathrm{End}_C V$ se α è associata ad M); i $v\in V$ tali che $\alpha v=cv$ per qualche $c\in C$, ovvero gli $y=\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}$, con $y_i\in C$, tali che $My=cy$, diconsi gli *autovettori* o *vettori caratteristici* di α, o di M; la condizione dà $(c-M)y=0$ onde $\det(c-M)=0$, $g(c)=0$, sicché c è autovalore (si intende, se v o y è non nullo); viceversa, se c è autovalore la $(c-M)y=0$ ha soluzioni $y\neq 0$. Quindi ad ogni autovalore sono associati degli autovettori non nulli; meglio ancora:

Lemma 3.35.1. *Lo spazio vettoriale V_c su C degli autovettori y di M tali che $My = cy$ per un dato c, ha dimensione positiva se, e solo se, c è autovalore di M.*

Lavorando non su $x-M$, ma sulla matrice diagonale i cui elementi diagonali sono i fattori invarianti di $x-M$, il (3.35.1) può essere così precisato (ricordiamo che la nullità di una matrice quadrata è la differenza tra l'ordine e la caratteristica):

Teorema 3.35.2. *Notazioni come nel Lemma 3.35.1, e siano $e_i(x)$ i fattori invarianti di $x-M$; allora*

$$\begin{aligned}\dim V_c &= [\textit{nullità di } c-M] = \\ &= [\textit{numero degli } e_i(x) \textit{ che hanno } c \textit{ come zero}] \leq \\ &\leq [\textit{molteplicità di } c \textit{ come zero del polinomio caratteristico di } M].\end{aligned}$$

La somma dei V_c è diretta, come si vede dal seguente:

Teorema 3.35.3. *Autovettori non nulli appartenenti ad autovalori distinti sono linearmente indipendenti; se la matrice è simmetrica, essi sono a due a due ortogonali (ossia $y_1^* y_2 = 0$).*

Dim. Sia $My_i = c_i y_i$, con i c_i diversi a 2 a 2; se $\sum_{i=1}^r a_i y_i = 0$, moltiplicando a sinistra per $M, M^2, \ldots, M^{r-1}$ si ottiene $\sum_{i=1}^r a_i c_i^j y_i = 0$ per $j = 0, \ldots, r-1$. La matrice dei coefficienti delle $a_i y_i$, ossia la

$$\begin{pmatrix} 1 & 1 & \ldots & \ldots & 1 \\ c_1 & c_2 & & & c_r \\ c_1^2 & c_2^2 & & & c_r^2 \\ \vdots & & & & \vdots \\ c_1^{r-1} & c_2^{r-1} & \ldots & \ldots & c_r^{r-1} \end{pmatrix},$$

è non degenere perché il suo determinante è il *determinante di Vandermonde* $V(c_1, \ldots, c_r)$, che vale $\prod_{1 \leq i < j \leq r}(c_j - c_i) \neq 0$ (dimostrarlo per esercizio, e se non ci si riesce, vedere la dimostrazione alla fine della lezione 37). Quindi $a_i y_i = 0$, ossia $a_i = 0$, e le $y_1, \ldots, y_r$ sono linearmente indipendenti.

Per l'ortogonalità

$$c_2 y_1^* y_2 = y_1^* M y_2 = (y_1^* M y_2)^* = y_2^* M y_1 = c_1 y_2^* y_1 = c_1 y_1^* y_2,$$

onde $y_1^* y_2 = 0$. C.V.D. □

Il (3.35.3) parte prima, applicato ad un $\alpha \in \mathrm{End}_C V$, ha un significato evidente; la parte seconda no, perché non è chiaro cosa voglia dire "ortogonali" se non è stata data una norma (e d'altro canto non è neanche chiaro che cosa voglia dire "simmetrica"). Il suo significato è il seguente:

Corollario 3.35.4. *Se $\alpha \in \mathrm{End}_C V$, e se $\circ$ è una qualsiasi norma su V tale che rispetto ad essa $\alpha^* = \alpha$, e se v_1, v_2 sono autovettori di α appartenenti ad autovalori distinti, allora $v_1 \circ v_2 = 0$.*

Dim. Praticamente la stessa. C.V.D. □

3.36 Lezione 36

Sfruttiamo i risultati precedenti:

Teorema 3.36.1. *Sia M matrice quadrata di ordine n ad elementi nel corpo C; i seguenti asserti sono equivalenti:*

1. *M è simile. in C, ad una matrice diagonale;*
2. *M possiede n autovettori linearmente indipendenti su C;*
3. *Il polinomio minimo di M su C è prodotto di fattori lineari distinti;*
4. *Per ogni autovalore $c \in C$, la sua molteplicità come zero del polinomio caratteristico di M uguaglia la nullità di $c - M$, e la somma di tali molteplicità è n.*

Se le condizioni sono soddisfatte, gli elementi diagonali, nella matrice diagonale simile alla data, sono gli autovalori, ciascuno ripetuto tante volte quanta ne è la molteplicità descritta al punto 4.

Dim. L'asserto non numerato discende dal fatto che il polinomio caratteristico non cambia nella relazione di simiglianza. Per i numerati: $1 \Rightarrow 2$ ovvio: gli autovettori di una diagonale sono i $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$; $2 \Rightarrow 4$ discende da (3.35.2); idem per $4 \Rightarrow 2$. Il (3.35.2) col (3.33.3), dà anche $4 \Leftrightarrow 3$; infine, $3 \Rightarrow 1$ discende da (3.34.1). C.V.D. □

Un ultimo tipo di equivalenza: due matrici quadrate M, M' ad elementi in un corpo sono *ortogonalmente simili* su quel corpo se $M' = P^{-1}MP$, con P ortogonale (cfr. lezione 11) e ad elementi in quel corpo; è una relazione di equivalenza. È chiaro che se M è ortogonalmente simile ad una matrice diagonale, M deve essere simmetrica; è anche chiaro che due matrici ortogonalmente simili sono simili ed anche congruenti. Ciò premesso, si ha:

Teorema 3.36.2. *Sia M matrice simmetrica di ordine n ad elementi in un corpo C di caratteristica $\neq 2$, e tale che in esso ogni somma di n quadrati sia un quadrato. Se allora M è simile, in C, ad una matrice diagonale D, essa è anche ortogonalmente simile, in C, a D.*

Dim. Nello spazio vettoriale numerico di dimensione n su C (che è poi quello di base $\{v_1, \dots, v_n\}$ con

$$v_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad (i - \text{esima componente}),$$

M è matrice di un endomorfismo α; i v_i sono ortonormali nella solita norma $v \circ w = v^* w$. Se M è simile alla diagonale D, per il 2 di (3.36.1) α ha n autovettori

$w_1, \ldots, w_n$ che formano una base, e che sono ortogonali per (3.35.3). Se in C ogni somma di n quadrati è un quadrato, i w_i possono essere scelti normalizzati (cfr. 1.11.3), sicché $\{w_1, \ldots, w_n\}$ è base ortonormale. Ma allora la matrice che trasforma la base v nella w è ortogonale, ed essa trasforma per simiglianza M nella D. C.V.D. □

Corollario 3.36.3. *Sia C un corpo ordinato, tale che in esso la somma di n quadrati sia un quadrato, e che $C[\sqrt{-1}]$ sia algebricamente chiuso. Allora ogni matrice simmetrica di ordine n ad elementi in C è ortogonalmente simile, in C, ad una diagonale.*

Dim. Per (3.36.1) e (3.36.2) basta dimostrare che il polinomio minimo $f(x)$ della matrice simmetrica M è prodotto di fattori lineari distinti in $C[x]$. Se $K = C[\sqrt{-1}]$, quel polinomio minimo è certamente prodotto di fattori lineari in $K[x]$, tali fattori essendo $x - a$, con a autovalore di M in K. Occorre dimostrare che questi a sono veramente in C, e che sono distinti. Se si indica con una sbarra superiore il coniugato di un elemento di K su C, o anche di una matrice, da $My = ay$ (y essendo autovalore non nullo) si ricava $\bar{y}^* My = a\bar{y}^* y$. Prendendo il trasposto coniugato di ambo i membri, e ricordando che $\bar{M}^* = M$, se ne deduce $\bar{a}\bar{y}^* y = a\bar{y}^* y$; ma $\bar{y}^* y = \sum_i \bar{y}_i y_i$, ed ogni $\bar{y}_i y_i$ è somma di due quadrati di elementi di C. Quindi $\bar{y}^* y \neq 0$, ed $a \in C$, come si voleva.

Ora occorre vedere che non ci possono essere fattori lineari ripetuti. Suppongasi che $f(x) = (x - a)^2 h(x)$, e pongasi $k(x) = (x - a)h(x)$; allora $k(x)^2 = f(x)h(x)$, $k(M)^2 = f(M)h(M) = 0$. Ma $N = k(M)$ è simmetrica, ha elementi in C, ed è non nulla, dato che $k(x)$ ha grado minore del grado di $f(x)$; quindi gli elementi della diagonale di N^2 sono somme di quadrati di elementi di C, ed almeno in un caso questi elementi sono non tutti nulli. Ne segue che $N^2 \neq 0$, contraddizione C.V.D. □

3.37 Lezione 37

Lemma 3.37.1. *Sia M matrice quadrata di ordine n ad elementi nel corpo C; sia x indeterminata, e sia $h(x) \in C[x]$; se $r_1, \ldots, r_n$ sono le radici caratteristiche di M, supposte in C, e ciascuna comparente tante volte quante ne è la molteplicità, si ha $\det h(M) = h(r_1) \cdots h(r_n)$.*

Dim. Si prolunghi C in un corpo K tale che $h(x) = k(s_1 - x) \cdots (s_q - x)$, con $k \in C$ ed $s_i \in K$; allora $h(M) = k(s_1 - M) \cdots (s_q - M)$, onde $\det h(M) = k^n \prod_i \det(s_i - M) = k^n \prod_{ij}(s_i - r_j) = \prod_j h(r_j)$, come voluto; ora il K non serve più. C.V.D. □

Teorema 3.37.2. *Notazioni come nel Lemma 3.37.1; allora le radici caratteristiche di $h(M)$ sono le $h(r_1), \ldots, h(r_n)$.*

Dim. Sia y un'altra indeterminata, e si ponga $p(x) = y - h(x) \in (C(y))[x]$; si ha $p(M) = y - h(M)$, onde il (3.37.1), applicato a $p(x)$, dà che

$$\det(y - h(M)) = \det p(M) = \prod_i p(r_i) = \prod_i (y - h(r_i));$$

ma $\det(y - h(M))$ è il polinomio caratteristico di $h(M)$. C.V.D. $\square$

Come promesso nella lezione 35, ecco la dimostrazione del Teorema di Vandermonde: aggiungendo alla i-esima riga ($i > 1$) la $(i-1)$-esima moltiplicata per $-c_1$, il determinante non cambia; d'altra parte la prima colonna della nuova matrice consta di un 1 nel posto $(1,1)$, e di 0 altrove. Cancellandovi prima riga e prima colonna, la matrice che resta ha la colonna i-esima divisibile per $c_{i+1} - c_1$; eseguita la divisione, resta la matrice di Vandermonde delle $c_2, \ldots, c_r$, sicché

$$V(c_1, \ldots, c_r) = (c_2 - c_1)(c_3 - c_1) \cdots (c_r - c_1)\, V(c_2, \ldots, c_r);$$

ne discende per induzione il valore usato nella dimostrazione del Teorema 3.35.3.

4

Quadriche

4.38 Lezione 38

In questa parte lavoreremo sempre in spazi proiettivi; sarebbe pesante mantenere in piena forza la nomenclatura della seconda parte; adotteremo invece la nomenclatura più familiare nella quale "spazio proiettivo" significa "spazio proiettivo punteggiato", e cioè l'insieme dei suoi punti; con ciò le parole 'retta", "piano", ecc. vengono ad indicare dei sottospazi, e non degli elementi di dimensione superiore [questo cambiamento di nomenclatura non è totalmente senza conseguenze; cfr. lezione 38bis].

Sia dunque S_n uno spazio proiettivo sul corpo C, che in questa lezione supponiamo algebricamente chiuso; scelto un sistema di riferimento in S_n, un punto P è assegnato col dare $n+1$ elementi $p_0, \ldots, p_n \in C$, non tutti nulli, e determinati a meno di un fattore non nullo in C; lo chiameremo spesso il punto $(p_0, \ldots, p_n)$, o semplicemente p; qui non occorre porre le p_i in colonna e considerarle come formanti una matrice $(n+1) \times 1$, ma non è vietato farlo.

Siano $x_0, \ldots, x_n$ indeterminate su C; un sottoinsieme U di S è una *varietà (algebrica)* su C se esiste un numero finito di forme $f_1(x), \ldots, f_r(x) \in C[x]$ tali che: $p \in U$ se, e solo se, $f_j(p) = 0$ per $j = 1, \ldots, r$; naturalmente $f_j(p)$ significa $f_j(p_0, \ldots, p_n)$. Notare che l'essere f_j forme garantisce che questa sia una buona definizione, in quanto se $f_j(p) = 0$, anche $f_j(cp) = 0$ per $c \in C$. Per brevità diremo (arcaicamente) che le $f_i(x) = 0$ sono le *equazioni di* U, ma teniamo bene in mente che le $f_i(x)$ si guardano bene dall'essere $= 0$, e che sono le $f_i(p)$ per $p \in U$ che sono $= 0$. La locuzione "le equazioni di U" non comporta che U determini univocamente le proprie equazioni: per esempio, la f_2 può essere sostituita con $f_2^r + f_1^s$ (r, s esponenti interi positivi) senza cambiare U. Spesso diremo anche, per descrivere quanto precede, "siano $x_0, \ldots, x_n$ un sistema di coordinate proiettive su S_n"; è infatti chiaro che, una volta fissate le x_i, un punto P di coordinate $p_0, \ldots, p_n$ può essere identificato con l'omomorfismo di $C[x]$ su C che manda x_i su p_i (e con gli omomorfismi ad esso proporzionali); quindi p_i è il *valore assunto da* x_i *in* P (sempre a meno di un fattore non nullo), e sarà indicato con $x_i(P)$.

Esempi 1. 1. Il vuoto è una varietà: le sue equazioni sono, per esempio, $x_0 = 0, \ldots, x_n = 0$; oppure anche $1 = 0$.

2. Ogni punto P è una varietà: le sue equazioni sono $p_0x_i - p_ix_0$ ($i = 1, \dots, n$), se per esempio $p_0 \neq 0$.

3. Ogni iperpiano è una varietà: la sua equazione è la $a_0x_0 + \cdots + a_nx_n = 0$ che è stata appunto chiamata l'equazione dell'iperpiano nella lezione 24.

4. S_n è una varietà: la sua equazione è $0 = 0$ (unico caso in cui il primo membro è sul serio zero).

5. L'intersezione di due (e quindi di un numero finito) di varietà è una varietà: se $f_i(x) = 0$ e $g_j(x) = 0$ sono rispettivamente le equazioni delle due varietà, quelle dell'intersezione sono $f_i(x) = g_j(x) = 0$.

6. Da 5 e 3 segue che ogni sottospazio di S_n è varietà, le cui equazioni possono essere prese tutte lineari; si chiamano *varietà lineari*.

7. L'unione di due (e quindi di un numero finito di) varietà è una varietà: se $f_i(x) = 0$ e $g_i(x) = 0$ sono rispettivamente le equazioni delle due varietà, quelle dell'unione sono $f_i(x)g_j(x) = 0$.

Sarebbe tentante dire che se F è applicazione proiettiva di S_n su S_m, e U è varietà di S_n, allora FU è una varietà di S_m; peccato che sia falso! È però vero in certi casi importanti; prima di esporli, una osservazione ed una definizione.

L'osservazione è che se una varietà U contiene infiniti punti di una retta R, deve contenere tutti i punti di R: infatti, intanto $U \cap R$ è una varietà in R; se y_0, y_1 è un sistema di coordinate proiettive su R, siano $f_i(y) = 0$ le equazioni di $U \cap R$. Fatto $y_0 = 1$, le $f_i(1, y_1) = 0$ sono soddisfatte da infiniti valori di y_1, sicché i primi membri sono 0; ma allora, per l'omogeneità, $f_i(y_0, y_1) = 0$, ed $U \cap R = R$.

La definizione è la seguente: sia U varietà; la U è un *cono* se esiste un punto $P \in U$ tale che: per ogni $Q \in U$, diverso da P, ogni punto della retta $P + Q$ appartiene ad U. Un P siffatto dicesi "appartenente al vertice di U". Se P e P' appartengono al vertice, ogni punto di $P + P'$ è su U; se poi $Q \neq P, P'$, ogni punto di $P + Q$ e di $P' + Q$ appartiene ad U; ma allora ogni punto di $P + P' + Q$ appartiene ad U, sicché ogni punto di $P + P'$ appartiene al vertice. Si vede così che l'insieme dei punti appartenenti al vertice di U è un sottospazio di S_n detto il *vertice* di U. Ora si ha:

Teorema 4.38.1. *Sia U varietà di S_n e sia F una proiettività di S_n su un S'_n; allora FU è varietà di S'_n. Sia invece U varietà di un $S_m \subset S_n$, e sia S_r sottospazio di S_n sghembo ad S_m; sia F la proiezione di S_n di centro S_r, e sia V l'insieme dei $P \in S_n$ ciascuno dei quali appartiene a qualche punto di FU (ricordare che i punti di FU sono degli S_{r+1}). Allora V è un cono, il cui vertice contiene S_r.*

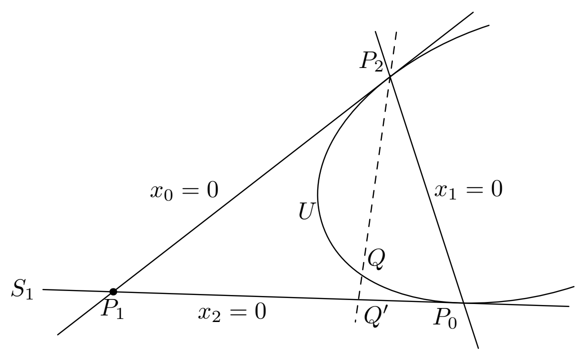
Dim. Per il primo asserto: siano $\{x_0, \dots, x_n\}$ e $\{y_0, \dots, y_n\}$ sistemi di coordinate proiettive su S_n, S'_n rispettivamente, e sia $x_i = \sum_j a_{ij}y_j$ un'applicazione lineare soprastante ad F. Siano $f_S(x) = 0$ le equazioni di U; allora $f_S(\dots, \sum_j a_{ij}y_j, \dots) = 0$ sono quelle di FU, sicché FU è varietà.

Per il secondo asserto: scelgasi un sistema di coordinate proiettive $x_0, \dots, x_n$ tale che le equazioni di S_m siano $x_{m+1} = \cdots = x_n = 0$, e che quelle di S_r siano $x_0 = \cdots = x_{n-r-1} = 0$. Se $f_S(x_0, \dots, x_m) = 0$ sono le equazioni di U, queste stesse sono le equazioni di FU, visto che le $x_0, \dots, x_{n-r-1}$ sono anche un sistema di coordinate proiettive sulla stella S_n/S_r (è $n - r - 1 \geq m$ perché S_r,

S_m sono sghembi). Un punto di FU è un S_{r+1} le cui equazioni sono quelle che esprimono essere le $x_0, \ldots, x_{n-r-1}$ proporzionali a certe $\bar{x}_0, \ldots, \bar{x}_{n-r-1} \in C$ che soddisfano le $f_S(\bar{x}) = 0$; in altre parole, queste stesse equazioni sono le equazioni di V. Che poi V sia cono il cui vertice contiene S_r è palese. C.V.D. $\square$

4.38 Lezione 38bis

Questa lezione è per chi desideri approfondire un po' le motivazioni di certe definizioni; non è necessaria per la comprensione del resto del corso o per l'esame. Intanto, un controesempio all'essere FU varietà: nel piano S_2 fissiamo un sistema di riferimento P_0, P_1, P_2, (Q punto unità); siano x_0, x_1, x_2 le relative coordinate proiettive. Sia S_1 la retta proiettiva $P_0 + P_1$; su questa si fissi il sistema di riferimento P_0, P_1, (punto unità Q' = proiezione di Q da P_2 su S_1), e siano y_0, y_1 le relative coordinate proiettive (l'equazione di S_1 è $x_2 = 0$).



La U sia la varietà di equazione $x_0x_2 - x_1^2 = 0$; sia F l'applicazione proiettiva di S_2 su S_1 che consiste nel proiettare S_2 da P_2 su S_1; allora una F_V soprastante ad $F_S = F$ è data da

(4.38bis.1) $$y_0 = x_0, \quad y_1 = x_1;$$

se $x = (x_0, x_1, x_2)$ percorre U, ossia $x_0x_2 - x_1^2 = 0$, l'$y = Fx$ percorre tutti i punti (y_0, y_1) di S_1 per ciascuno dei quali esiste un punto x tale che $y_0x_2 - y_1^2 = 0$. Fra questi punti non c'è punto $(0, 1) = P_1$, ma ci sono tutti gli altri, sicché FU è tutto S_1 eccetto P_1; questo insieme si è visto non essere una varietà. Ciò mostra che la definizione di "applicazione proiettiva" andava bene per gli spazi proiettivi definiti a suo tempo, ma non per gli spazi proiettivi punteggiati che usiamo ora; ed il perché si può vedere con un esame approfondito dei motivi delle definizioni: una applicazione di un insieme V su uno W è un certo sottoinsieme di $V \times W$; se V, W hanno certe ulteriori strutture, le applicazioni più sensate sono quelle che partecipano di quelle strutture; così, se V, W sono spazi vettoriali, $V \times W$ diventa anch'esso uno spazio vettoriale se lo si indica con $V \oplus W$; ed ora un sottoinsieme F_V di $V \oplus W$ è applicazione lineare se, fra l'altro, è sottospazio vettoriale di $V \oplus W$. Passiamo agli spazi proiettivi $S = [V]$, $T = [W]$; intanto $[V \oplus W]$ non è in corrispondenza biunivoca con $S \times T$, ma perlomeno contiene un sottoinsieme (quello dei $V' \oplus W'$, con V', W' sottospazi di V, W) che è in corrispondenza biunivoca con $S \times T$; identifichiamolo con $S \times T$. Ora l'intersezione di $S \times T$ con $[F_V]$ è ciò che abbiamo chiamato F_S, e la definizione funzionava bene perché questo F_S è appunto un sottoinsieme di $S \times T$, ed è quanto di più vicino ad uno spazio proiettivo si possa acchiappare. Ma se S, T vengono interpretati come spazi proiettivi punteggiati, tutto questo cade, perché se P è punto di S appartenente al nucleo di F_S, l'elemento del vecchio $S \times T$ la cui pr_1 è P è $P \times$ (vuoto di T), e questo non è un elemento del nuovo $S \times T$.

Quindi, per dare una definizione sensata di applicazione proiettiva (che però riceverà il nome di *applicazione razionale lineare*) per spazi proiettivi punteggiati occorre trovare qualcosa di familiare che rappresenti l'$S \times T$; torniamo a V e W: ora $S = [V]_1$ e $T = [W]_1$, ove l'indice 1 vuol dire che si considerano solo i sottospazi di dimensione 1. Il $[V \oplus W]_1$ non ha nessun sottoinsieme in corrispondenza biunivoca canonica con $[V]_1 \times [W]_1$; se però si costruisce $V \otimes W$ (prodotto tensoriale, [AA] lezione 49), ecco che $[V \otimes W]_1$ intanto è uno spazio proiettivo punteggiato, e poi contiene il sottoinsieme dei $\langle v \otimes w \rangle$ ($v \in V, w \in W$, entrambi $\neq 0$), che è appunto in corrispondenza biunivoca con $S \times T$, e che quindi sarà indicato con $S \times T$. Ed anzi, questo sottoinsieme è una varietà di $[V \otimes W]_1$; dimostrazione: se V è identificato con le matrici $(n+1) \times 1$ di elementi di C, e W con le matrici $1 \times (m+1)$, $V \otimes W$ può essere identificato con le matrici $(n+1) \times (m+1)$, ed anzi, $v \otimes w$ con la matrice vw. Si tratta di vedere quando una matrice di tipo $(n+1) \times (m+1)$ sia un prodotto vw; la risposta (esercizio, e comunque ci torneremo in seguito) è "quando abbia caratteristica ≤ 1", sicché le equazioni di $S \times T$ non sono altro che i minori di ordine 2 eguagliati a 0. Più precisamente: partiamo da un $S_{(n+1)(m+1)-1}$ un cui sistema di coordinate proiettive scriviamo con due indici: z_{ij}, $i = 0, \ldots, n$; $j = 0, \ldots, m$; le equazioni $z_{ij} z_{rs} - z_{rj} z_{is} = 0$ danno una varietà in corrispondenza biunivoca con un $S_n \times S_m$ (detta *varietà di Segre*, o *prodotto alla Segre* di S_n ed S_m).

Ora che siamo riusciti a vedere $S \times T$ come qualcosa che ha senso nella teoria che abbiamo in esame, è facile stabilire chi debba essere F_S: l'F_V era un sottoinsieme di $V \times W$; l'immagine di F_V in $V \otimes W$ genera (ma non è) un sottospazio vettoriale di $V \otimes W$, diciamo F'; e l'$[F'] \cap (S \times T)$ è ciò che ora vogliamo chiamare F_S.

Vediamo sull'esempio precedente come questo F_S differisca da quello usato prima; nell'esempio S era S_2, T era S_1; $S \times T$ è la varietà (nell'S_5 di coordinate proiettive z_{ij}, $i = 0, 1, 2$; $j = 0, 1$) formata dai pnti di coordinate $z_{ij} = x_i y_j$, con x, y punti di S, T rispettivamente; F' è generato da tutti gli $\left(\begin{smallmatrix} x_0 \\ x_1 \\ x_2 \end{smallmatrix}\right) \left(\begin{smallmatrix} y_0 & y_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} x_0 y_0 & x_0 y_1 \\ x_1 y_0 & x_1 y_1 \\ x_2 y_0 & x_2 y_1 \end{smallmatrix}\right)$, onde $[F']$ ha equazione $z_{01} - z_{10} = 0$. L'intersezione con $S \times T$ produce perciò l'equazione

$$x_0 y_1 - x_1 y_0 = 0. \tag{4.38bis.2}$$

Ecco che ora il punto incriminato $(0, 1) = P_1$ di T proviene, secondo F_S, da tutti i punti $(0, x_1, x_2)$ di S; e fra questi vi è il $P_2 = (0, 0, 1)$ di U. Nella vecchia F_S

tale P_2 era il centro, e corrispondeva perciò al vuoto di T (ed è per questo che P_1 mancava fra le immagini di punti).

Un'analisi ulteriore rivela che

1. La vecchia F_S esprime, algebricamente, una eguaglianza fra certi x_i ed y_i (la 4.38bis.1); geometricamente esprime che: $F_S P$ è l'intersezione di S_1 con $P_2 + P$;
2. Il nuovo F_S esprime, algebricamente, una proporzionalità fra certi x_i e certi y_i (la 4.38bis.2); geometricamente esprime che: P e P' si corrispondono in F_S se P_2, P, P' sono allineati.
3. Se si analizza ulteriormente l'intersezione di $[F']$ non con $S \times T$, ma con $U \times T$ (che è quella che conta), si vede che essa è unione delle due seguenti varietà D_1 e D_2: la $D_1 = P_2 \times T$ è la corrispondenza fra U e T che fa corrispondere $P_2 \in U$ ad ogni punto di T; invece D_2 ha equazioni $y_0x_1 - x_0y_1 = 0$, $y_0x_2 - x_1y_1 = 0$, e naturalmente $x_0x_2 - x_1^2 = 0$: ad ogni $P \in U$, diverso da P_2 fa corrispondere $F_S P$ (in qualunque interpretazione di F_S); ed a P_2 fa corrispondere P_1 soltanto.

Darò ora, senza dimostrazione, la seguente informazione:

Teorema 4.38bis.3. *Per ogni applicazione razionale lineare, il corrispondente di una varietà è una varietà.*

Notare che le applicazioni razionali lineari sono corrispondenze, ma non necessariamente applicazioni nel vero senso della parola, perché ad un punto del primo spazio possono far corrispondere più di un punto del secondo; è un prezzo che si deve pagare per evitare i maggiori inconvenienti illustrati.

4.39 Lezione 39

C continua ad essere algebricamente chiuso. Una varietà U è una *ipersuperficie* (*curva* per $n = 2$, *superficie* per $n = 3$; le parole superficie e ipersuperficie restano invariate al plurale, anche se ormai sono solo i matematici a saperlo; la parola "specie" è stata più fortunata, e soltanto la rai osa dire "speci"[1]) se può essere definita con una sola equazione; ed in questa espressione includiamo la equazione $1 = 0$ (che dà la *ipersuperficie vuota*) ma non la $0 = 0$ (che darebbe tutto lo spazio, non considerato ipersuperficie). Vorrei anche avvertire, a scanso di equivoci, che mentre la parola ipersuperficie descrive una proprietà di una varietà rispetto allo spazio in cui è immersa, le parole curva e superficie, che qui vengono sate come sinonimi di ipersuperficie in casi speciali, descrivano in realtà, in una teoria più generale che non svolgiamo, delle proprietà di varietà indipendenti dallo spazio in cui sono immerse.

Una varietà è *irriducibile* se non è unione di due sue sottovarietà proprie (*sottovarietà* vuol proprio dire varietà che sia anche sottoinsieme).

[1] ...all'epoca non esistevano ancora le emittenti private. [NdR]

Lemma 4.39.1. *Una ipersuperficie U di equazione $f(x) = 0$, con $f(x)$ irriducibile, è irriducibile; inoltre $f(x)$ genera l'ideale di $C[x]$ formato da tutti i $g(x)$ aventi la proprietà che $g(x(P)) = 0$ per ogni $P \in U$.*

Dim. Sia M quell'ideale (che sia un ideale non c'è dubbio); supponiamo poi che $f(x)$ contenga veramente tutte $x_0, \ldots, x_n$ con grado positivo (se così non fosse, basterebbe applicare una sostituzione lineare invertibile di indeterminate per ottenere che così fosse). Se $0 \neq g(x) \in M$, dico che $g(x)$ ha la stessa proprietà; se infatti $g(x) \in C[x_0, \ldots, x_{n-1}]$, siano $p_0, \ldots, p_{n-1} \in C$ arbitrari, ma non tutti nulli, e sia $p_n \in C$ tale che $f(p) = 0$; questo p_n esiste perché C è algebricamente chiuso e $f(p_0, \ldots, p_{n-1}, x_n) \in C[x_n]$ ha grado positivo[2]. Allora $p \in U$, onde $g(p_0, \ldots, p_{n-1}) = 0$. Essendo $p_0, \ldots, p_{n-1}$ arbitrari, questo dà $g(x) = 0$, contro l'ipotesi.

Ciò premesso, sia $g(x)$ elemento di M di grado minimo nella x_n; questo grado, sia esso s, è certo > 0 per quanto visto. Considerando f e g come elementi di $C(x_0, \ldots, x_{n-1})[x_n]$, si può dividere f per g: $f = gq' + r'$, ove $r' = 0$, ovvero r' ha in x_n grado $< s$. Eliminando il denominatore comune $h(x_0, \ldots, x_{n-1})$ di q', r', si ottiene $hf = gq + r$, con r polinomio nell $x_0, \ldots, x_n$ nullo oppure di grado $< s$ nella x_n. Dato che f e g si annullano su ogni punto di U, r deve fare lo stesso, impossibile se $r \neq 0$ perché il suo grado nella x_n è troppo piccolo. Perciò $r = 0$, e g divide hf. Ma f è irriducibile, onde o g è associato ad f, ovvero g divide h; l'ultima cosa è impossibile, perchè g ha $n + 1$ indeterminate ed h ne ha al più n. Perciò g è associato ad f. La stessa dimostrazione, ora che sappiamo che g è irriducibile, mostra che g, e quindi f, divide ogni elemento di M, e in conclusione che $M = fC[x]$.

Suppongasi ora U riducibile: $U = U_1 \cup U_2$; ad U_i è legato un ideale M_i, e si vede subito che $M = M_1 \cap M_2$; dato che $U_1 \subset U$, ci sono punti p tali che $f(p) = 0$, ma che $f_i(p) \neq 0$ per qualcuna delle equazioni $f_i(x) = 0$ di U_1. Ora $f_1 \in M_1$, e certo $f_1 \notin M$ (altrimenti la $f(p) = 0$ comporterebbe $f_1(p) = 0$); se analogamente, $f_2 \in M_2$, ma $\notin M$, si ha che $f_1 f_2 \notin M$ perché M è primo; ma $f_1 f_2 \in M_1 \cap M_2 = M$, contraddizione. C.V.D. □

Se U è varietà, dicesi *componente (irriducibile)* di U ogni sottovarietà irriducibile U' di U per la quale esista qualche sottovarietà propria U'' di U con la proprietà $U = U' \cup U''$.

Teorema 4.39.2. *Una ipersuperficie non vuota U di equazione $f(x) = 0$ è unione delle ipersuperficie irriducibili le cui equazioni hanno come primi membri i fattori irriducibili di $f(x)$; e queste sono tutte e sole le componenti di U.*

Dim. Se $f = \prod_i g_i^{r_i}$, con i g_i irriducibili a due a due non associati, è $f(p) = 0$ se, e solo se, $g_i(p) = 0$ per qualche i; quindi U è unione delle U_i di equazioni

[2] In realtà, se la $f(p) = 0$ si riducesse ad $h = 0$ con $0 \neq h \in C$, la p_n non esisterebbe. Si può essere sicuri che questo caso cattivo non si avvera se si richiede che $f(x)$ contenga un monomio nella sola x_n, ossia che $f(0, \ldots, 0, 1) \neq 0$; ciò è equivalente al richiedere che U non passi per il punto $(0, \ldots, 0, 1)$ e questo lo si può sempre ottenere con opportuna scelta del sistema di riferimento.

$g_i(x) = 0$; e queste sono irriducibili, ed anche componenti, per (4.39.1). Sia poi U' componente di U; si ha $U' = \bigcup_i (U_i \cap U')$, ove le $U' \cap U_i$ vuote si suppongono non scritte. Essendo U' irriducibile, ciò comporta che qualche $U_i \cap U'$ non è sottovarietà propria di U', sicché $U' \subseteq U_i$ per qualche i. Poi, da $U = U' \cap U''$, con U'' sottovarietà propria di U, si ricava $U_i = (U_i \cap U') \cup (U_i \cap U'')$; l'essere U_i irriducibile ora comporta che o $U' = U_i$, che è quanto si vuole dimostrare, ovvero che $U_i \cap U'' = U_i$, onde $U_i \subseteq U''$. Ma quest'ultima relazione è falsa, perché dà $U = U' \cup U'' \subseteq U''$, e cioè $U = U''$, contro l'ipotesi che U'' fosse sottovarietà propria di U. C.V.D. $\square$

4.40 Lezione 40

C è ancora algebricamente chiuso, ma questa ipotesi sarà abbandonata nel corso di questa lezione. I (4.39.1), (4.39.2) mostrano che vi è corrispondenza biunivoca fra ipersuperficie (di S_n) irriducibili e forme irriducibili di $C[x]$, queste ultime a meno di un fattore non nullo in C; o meglio, fra ipersuperficie irriducibili ed ideali primi principali di $C[x]$; e che la corrispondenza è estensibile fra ipersuperficie (tutte) e forme che sono prodotti di fattori irriducibili distinti, sempre a meno di fattori non non nulloi in C, ed ivi compresa la forma 1, supposta prodotto di zero fattori irriducibili. Possiamo ulteriormente estendere questa corrispondenza se chiamiamo *divisore* (su S_n) ogni elemento del gruppo additivo liberamente generato dalle ipersuperficie irriducibili. Al divisore $D = \sum_i e_i U_i$, con gli e_i interi e le U_i ipersuperficie irriducibili distinte, in numero finito, si fa corrispondere $f(x) = \prod_i f_i(x)^{e_i} \in C(x)$, se $f_i(x) = 0$ è l'equazione di U_i scelta con f_i irriducibile. In questo modo la corrispondenza è biunivoca fra il gruppo additivo dei divisori e il gruppo moltiplicativo $C(x)^*/C_0$, ove $C_0 =$ gruppo degli elementi non nulli di C, e $C(x)^* =$ gruppo degli elementi omogenei non nulli di $C(x)$. Un elemento omogeneo di $C(x)$ è il quoziente fra due forme di $C[x]$, il suo grado essendo la differenza fra quello del numeratore e quello del denominatore.

Scriveremo $D = \operatorname{div} f(x)$, o $\operatorname{div}_{S_n} f(x)$ per maggiore precisione; l'ipersuperficie $\bigcup_i U_i$ (unione delle *componenti* di D che compaiono con *molteplicità* e_i non nulla) è il *supporto* di D, eccetto che $D = 0$ ha per supporto l'ipersuperficie vuota. Se gli e_i sono tutti ≥ 0, ed uno almeno è > 0, D si chiama *positivo* o *effettivo*, ogni D può essere scritto come differenza di due divisori positivi: $D = D_1 - D_2$; se $D = \operatorname{div} f$, D_1 e D_2 si chiamano rispettivamente lo *zero* ed il *polo* di f, sempreché D_1 e D_2 non abbiano componenti comuni; i divisori effettivi sono perciò i $\operatorname{div} f$ con $f \in C[x]$.

Un divisore di tipo $1U$, con U ipersuperficie irriducibile, si chiama un *divisore primo*, e viene spesso indicato con la stessa lettera U che indica il suo supporto; ma è una cosa diversa: il supporto è un insieme di punti, mentre il divisore primo è soltanto un elemento di un certo gruppo, e non ha punti.

Ora abbandoniamo l'ipotesi che C sia algebricamente chiuso, e indichiamo con $\bar{C}$ la sua chiusura algebrica; se S_n è definito su C, la sua estensione a $\bar{C}$ sarà indicata con $\bar{S}_n$; le *varietà* in S_n, dette anche varietà in $\bar{S}_n$ *definite su* C, sono quelle varietà in $\bar{S}_n$ che possono essere definite da equazioni i cui primi membri appartengano a $C[x]$; un divisore su S_n, detto anche un *divisore su* $\overline{S}_n$ *razionale su* C, è un divisore su $\bar{S}_n$ del tipo $\operatorname{div} f(x)$, ove $f(x) \in C(x)$; resta vero che il gruppo dei divisori su S_n è isomorfo a $C(x)^*/C_0$. Notare che con queste definizioni un punto di S_n è proprio un punto di $\bar{S}_n$ definito su C, ossia tale che le sue coordinate possano essere scelte in C; lo si chiama anche, in analogia con i divisori, *razionale su* C.

Alcuni esempi:

1. C corpo reale, $\bar{C}$ complesso, $D = \operatorname{div}(x_1^2 + x_2^2 - x_0^2)$, in $\bar{S}_2$; è razionale su C; la $x_1^2 + x_2^2 - x_0^2 = 0$ dà una ipersuperficie irriducibile U in $\bar{S}_2$ (curva), definita su C; $D = 1U$ è primo, e la U ha infiniti puti "reali", ossia razionali su C, il cui insieme non è una varietà.
2. Come prima, ma con $x_1^2 + x_2^2 + x_0^2$; U è ancora irriducibile, e $D = 1U$ primo, benché U sia definita su C e irriducibile, non ha punti reali.
3. Sempre in $\bar{S}_2$, $D = \operatorname{div}(x_1^2 + x_2^2)$; la $x_1^2 + x_2^2 = 0$ è una curva riducibile di $\bar{S}_2$, con componenti U_1 di equazione $x_1 + \sqrt{-1}x_2 = 0$, e U_2 di equazione $x_1 - \sqrt{-1}x_2 = 0$ (due rette); benché $x_1^2 + x_2^2$ sia irriducibile in $C[x]$, il divisore D non è primo, ma è uguale a $1U_1 + 1U_2$; la curva $U_1 \cup U_2 = \operatorname{supp} D$ ha un unico punto reale, e precisamente $(0, 0, 1)$; a differenza del caso 1, questo punto è una varietà, ma non una curva.

Gli esempi precedenti mostrano che benché una varietà di S_n possa avere punti razionali su C, l'insieme di tali punti può non essere una varietà, oppure se è varietà può non essere una ipersuperficie anche se la data lo è. Nel caso di una varietà lineare $\bar{H}$ di S_n, ossia di un sottospazio $\bar{H}$ di $\bar{S}_n$ definito da equazioni a coefficienti in C, l'insieme dei suoi punti razionali su C è ancora un sottospazio H di S_n, della stessa dimensione di $\bar{H}$ in quanto definito dalle stesse equazioni; ma è un caso fortunato.

La differenza fra il grado del numeratore e quello del denominatore di $f(x)$, ossia il grado di omogeneità di $f(x)$, si chiama l'*ordine* di $D = \operatorname{div} f(x)$; se S_m è sottospazio di S_n, ma non di $\operatorname{supp} D$, siano $\sum_{j=0}^n a_{ij}x_j = 0$ $(i = 1, \ldots, n - m)$ le sue equazioni; da esse si possono ricavare, per esempio, le $x_{m+1}, \ldots, x_n$ come combinazioni lineari delle rimanenti; se le sostituiamo in $f(x)$, otteniamo un $g(x_0, \ldots, x_m)$ che è $\neq 0$ (ed anche $\neq \infty$, ossia col denominatore $\neq 0$; si intende che $f(x)$ va prima ridotta ai minimi termini). Il divisore di $g(x)$ su S_m è l'*intersezione* di D con S_m, in simboli $D \cap S_m = S_m \cap D$; il suo supporto è proprio $\bar{S}_m \cap \operatorname{supp} D$ se D è divisore effettivo. Chiaramente $\operatorname{ord} D = \operatorname{ord}(D \cap S_m)$, sicché $\operatorname{ord} D$ è, per $m = 1$, il numero di punti di quest'intersezione, ogni punto contato con la molteplicità con la quale le sue coordinate compaiono come zero del polinomio $g(x_0, x_1)$; meglio ancora, se p è il punto e $p_0 \neq 0$, la molteplicità che conta è quella di p_1 come radice di $g(p_0, x_1)$. Questo mostra che il passaggio dalle ipersuperficie ai divisori è analogo al passaggio dalle radici pure e semplici di una equazione alle radici con le loro molteplicità.

4.41 Lezione 41

Una *quadrica*, in S_n sul corpo C (*conica* se $n = 2$), è un divisore effettivo di ordine 2; e quindi un $\operatorname{div} f(x)$, ove $f(x) = \sum_{ij} a_{ij}x_ix_j$, con gli a_{ij} elementi di C non tutti nulli; qui stiamo evidentemente parlando di forme quadratiche, sicché per prudenza supporremo d'ora in poi, e per tutta questa parte quarta, che C *non abbia caratteristica* 2. Si può allora supporre che la matrice $A = (a_{ij})$ sia simmetrica, visto che la parte antisimmetrica non ha influenza su $f(x)$. La A determina la quadrica Q, e ne è determinata a meno di un fattore non nullo in C; inoltre siamo in un caso in cui non solo Q determina $\operatorname{supp} Q$, ma in cui $\operatorname{supp} Q$ determina Q; infatti, dovendo Q avere ordine 2, possono darsi solo i tre casi seguenti:

1. Q è un divisore primo; allora $\operatorname{supp} Q$ è una ipersuperficie irriducibile;
2. Q è somma di due divisori primi distinti, ciascuno di ordine 1; ognuno di questi, essendo di ordine 1, ha come supporto un iperpiano di $\bar{S}_n$, sicché $\operatorname{supp} Q$ è l'unione di due iperpiani;
3. Q è due volte un divisore primo di ordine 1; in tal caso $\operatorname{supp} Q$ è un iperpiano, che a priori è iperpiano di $\bar{S}_n$, ma che vedremo essere in realtà ipersuperficie in S_n.

In tutti e tre i casi, appena vediamo chi è $\operatorname{supp} Q$ sappiamo come ricostruire Q.

La $f(x)$ precedente si può scrivere x^*Ax, se al solito $x = \begin{pmatrix} x_0 \\ \vdots \\ x_n \end{pmatrix}$; lo studio delle quadriche è perciò lo studio delle forme quadratiche, o il che è lo stesso, delle bilineari simmetriche, sullo spazio vettoriale V tale che S_n sia lo spazio proiettivo punteggiato legato a $[V]$; o più precisamente, delle forme quadratiche a meno di proporzionalità: ecco perché di queste forme quadratiche interessano solo gli zeri, mentre gli altri valori, che avrebbero significato su V (cfr. parte prima), perdono ogni significato in S_n.

I casi $1, 2, 3$ precedenti devono essere riconosciuti da A, o dalla forma quadratica; eccone il modo, in ordine inverso:

3. A ha caratteristica 1: se infatti l'equazione dell'iperpiano $\operatorname{supp} Q$ è $a^*x = 0$, con a matrice non nulla $(n+1) \times 1$ ad elementi in $\bar{C}$, si ha $f(x) = (a^*x)^2 = x^*(aa^*)x$, ed $A = \rho aa^*$, con ρ coefficiente di proporzionalità in $\bar{C}$, ha caratteristica 1 (ogni riga è proporzionale ad a^*). Ora si può vedere che $\operatorname{supp} Q$ è definito su C: infatti ρaa^* deve avere elementi in C; se uno degli elementi non nulli di a viene fatto uguale ad 1, una certa riga di A diviene proprio uguale a ρa^*, sicché ρa ha elementi in C; quindi $\rho \in C$ ed a ha elementi in C.
2. A ha caratteristica 2: se infatti le equazioni dei due iperpiani che sono le componenti di $\operatorname{supp} Q$ sono $a^*x = 0$ e $b^*x = 0$, con a, b ad elementi in $\bar{C}$, sarà $f(x) = (a^*x)(b^*x) = x^*(ab^*)x$, onde $A = \frac{1}{2}(ab^* + ba^*)$; questa ha caratteristica 2, perché intanto ogni riga è combinazione lineare di a^* e b^*, sicché la caratteristica è ≤ 2; e poi se $\Delta = \begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix}$ è un minore di (a, b) non nullo, il minore delle righe e colonne i, j di A è uguale a $-\Delta^2/4$ (fare il conto), ed è quindi non nullo; quindi la caratteristica è proprio 2 e non 1. C'è anche da

osservare, in questo caso, che ogni riga di A è combinazione lineare di a^* e b^*, sicché se r, s sono due tali righe indipendenti, e certo ad elementi in C, le $rx = 0$, $sx = 0$ sono le equazioni dell'$\bar{S}_{n-2}$ intersezione dei due iperpiani componenti di $\operatorname{supp} Q$; pertanto tale intersezione è definita su C.

1. A ha caratteristica maggiore di 2: se infatti la caratteristica è $m < n + 1$, la forma quadratica $f(x)$ su V ha nucleo di dimensione uguale alla nullità di A (cfr. lezione 7, e 1.8.3), e quindi uguale a $n + 1 - m$; ed allora, per quanto detto dopo l'(1.8.3), con una trasformazione lineare invertibile di coordinate a coefficienti in C la $f(x)$ diviene una forma che contiene solo m indeterminate; per il (4.38.1) (e soprattutto per la sua dimostrazione) la $f(x) = 0$ è un cono il cui vertice è un sottospazio di $\bar{S}_n$, definito su C, di dimensione uguale al numero di indeterminate che mancano, diminuito di 1, ossia $n - m$. Se ora $m \leq 2$, questo numero è $\geq n - 2$; se la dimensione è $n - 1$, il cono è un iperpiano, caso 3 e non 1; se la dimensione è $n - 2$ (del vertice s'intende), il cono è due iperpiani distinti, caso 2 e non 1. Quindi, nel caso 1 la caratteristica di A è maggiore di 2 come annunciato all'inizio.

Le quadriche il cui supporto è un cono si chiamano *coni quadrici*; si è così visto che:

Teorema 4.41.1. *Una quadrica in S_n è un cono quadrico se, e solo se, la sua matrice è singolare; ed in tal caso il vertice è un sottospazio di $\bar{S}_n$ di dimensione uguale alla nullità della matrice diminuita di* 1*; tale vertice è poi definito su C.*

Le quadriche a matrice singolare sono dette *quadriche degeneri*, e le quadriche descritte ai punti 2 e 3 si chiamano *quadriche spezzate*. Dato che, per (4.38.1), il supporto di una quadrica degenere non è altro che la proiezione (nel senso più preciso del 4.38.1) dal proprio vertice del supporto di una quadrica non degenere di uno spazio di dimensione minore, basta limitarsi allo studio delle quadriche nondegeneri. Notare che se $n = 1$ (retta), ogni quadrica (somma di due punti) è spezzata; le degeneri sono i punti con molteplicità 2; la parola "cono" perde significato (l'unico cono è la retta stessa).

4.42 Lezione 42

Quando un S_n è considerato, come nel caso presente, spazio punteggiato, il suo *duale* S_n^* sarà lo spazio di iperpiani formato dai suoi iperpiani; converremo che l'iperpiano di equazione $ax = 0$, con $a = (a_0, \ldots, a_n)$, abbia $a_0, \ldots, a_n$ come coordinate proiettive (plückeriane), in accordo con quanto detto nella lezione 24. D'ora in poi parleremo prevalentemente di quadriche non spezzate in due iperpiani coincidenti, sicché sarà inopportuno insistere ferocemente nella distinzione fra quadrica e suo supporto.

Sia $x^*Ax = 0$ l'equazione di una quadrica non degenere; la $x \mapsto (Ax)^* = x^*A$ è una proiettività di S_n su S_n^*, ossia una autoreciprocità di S_n (lezione 22), che indicheremo con π. Se x, y sono due punti tali che y appartenga a πx, si ha $(x^*A)y = 0$, onde $(y^*A)x = 0$, il che significa che x appartiene a πy. Questo, ed il (2.22.1), mostrano che π è polarità, in quanto di punti x che non appartengano a

πx ce ne sono a bizzeffe (tutti quelli che non appartengono alla quadrica). Questo π sarà detto la *polarità legata alla quadrica*; se $a = \pi x$, a è la *polare* di x, ed x il *polo* di a. Le quadriche non degeneri appaiono così come i luoghi dei punti che, per una data polarità, stanno sulla propria polare; tali punti da essere presi in $\bar{S}_n$, salvo che taluni di essi saranno razionali su C. Naturalmente una polarità su S_n di matrice A è anche una polarità su S_n^* di matrice A^{-1}, per (2.21.4); in altre parole, se $a = \pi x = x^* A$, allora $x = (aA^{-1})^*$. Quindi π, o A, determina una quadrica non degenere in S_n^*, i cui "punti" sono i πx quando x percorre la quadrica in $\bar{S}_n$. Quindi la quadrica di S_n, detta *quadrica-luogo*, è il luogo dei punti (di $\bar{S}_n$) che appartengono alla propria polare, mentre quelle di S_n^*, detta *quadrica inviluppo*, è il luogo degli iperpiani (di $\bar{S}_n$) che passano per il proprio polo; le due quadriche, luogo e inviluppo, saranno dette *duali* l'una dell'altra; se una è chiamata Q, l'altra sarà Q^*.

Strettamente legata alla polarità è la questione della tangenza: abbandoniamo per un po' l'ipotesi che C non abbia caratteristica 2, e sia D un divisore effettivo in S_n; un punto $P \in \operatorname{supp} D$ dicesi *semplice* su D se esiste qualche retta R di $\bar{S}_n$, passante per P ma non contenuta in $\operatorname{supp} D$, tale che P compaia con molteplicità 1 in $D \cap R$; dicesi *multiplo* o *singolare* altrimenti; se $n = 1$ la definizione ha ancora senso, ma vuol dire semplicemente che P è semplice se compare con molteplicità 1 in D. Un $\bar{S}_m \subseteq \bar{S}_n$ è *tangente a D in P* se intanto $P \in \bar{S}_m$, e se inoltre o $\bar{S}_m \subseteq \operatorname{supp} D$, ovvero P è punto singolare di $D \cap \bar{S}_m$; questo comporta subito che se $\bar{S}_m$ è tangente a D in P, e se $\bar{S}_r \subseteq \bar{S}_m$ passa per P, anche $\bar{S}_r$ è tangente a D in P. Il risultato generale è:

Teorema 4.42.1. *Sia $D = \operatorname{div} f(x)$ divisore effettivo su S_n, e sia $P \in \operatorname{supp} D$; sia a_i il valore, in $\bar{C}$, che $\frac{\partial f}{\partial x_i}$ assume in P, e pongasi $a = (a_0, \ldots, a_n)$; allora:*

1. *P è singolare su D se, e solo se, $a = 0$; in tal caso ogni $\bar{S}_m$ passante per P è tangente a D in P;*
2. *Se P non è singolare, un $\bar{S}_m$ passante per P è tangente a D in P se, e solo se, è contenuto nell'iperpiano $ax = 0$.*

Dim. Pongasi $f_i(x) = \frac{\partial f}{\partial x_i}$, sicché $a_i = f_i(P)$. Su una retta R per P, si scelgano le coordinate proiettive t, y in modo che P abbia coordinate $t = 1$, $y = 0$. L'immersione di R in $\bar{S}_n$ è un'applicazione proiettiva una cui applicazione lineare soprastante sarà del tipo $x = p_i t + b_i y$, con le $b_i \in \bar{C}$ non tutte nulle, o brevemente $x = Pt + By$. La R sarà quindi tangente a D in P se, e solo se, il $\operatorname{div}_R f(Pt+By)$ ha come componente, con molteplicità maggiore di 1, il punto P di $\bar{S}_n$, ossia il punto $(1, 0)$ di R (oppure se $f(Pt + By) = 0$). Essendo $P = \operatorname{div}_R y$, ciò accadrà se, e solo se, $f(Pt+By)$ è divisibile per y^2. Ora, la $f(Pt+By)$, come polinomio nella y a coefficienti in $\bar{C}[t]$, ha il termine noto $f(Pt) = 0$ e il termine di primo grado uguale a $\sum_i a_i b_i t^{r-1} y$ se $r = \deg f(x) = \operatorname{ord} D$: infatti tale termine è

$$y \left[\frac{\partial f(Pt + By)}{\partial y} \right]_{y=0} = y \sum_i b_i f_i(Pt) = y \sum_i b_i a_i t^{r-1}.$$

Poiché la divisibilità richiesta significa che tale termine di primo grado è 0, si vede che se $a = 0$ ogni R è tangente, sicché P è singolare. Se invece $a \neq 0$,

R è tangente se, e solo se, $\sum_i a_i b_i = 0$; dato che $\sum_i a_i p_i = rf(P) = 0$ (è una proprietà di tutte le forme), la precedente significa $\sum_i a_i(p_i t + b_i y) = 0$, e questa a sua volta vuol dire che R appartiene all'iperpiano di equazione $ax = 0$. Il passaggio da R ad un qualsiasi $\bar{S}_m$ è ovvio. C.V.D. □

Corollario 4.42.2. *Il luogo dei punti singolari di D è una varietà definita su C.*

Dim. Le sue equazioni sono $f(x) = 0$, $\frac{\partial f}{\partial x_0} = 0, \ldots, \frac{\partial f}{\partial x_n} = 0$. C.V.D. □

Nel caso 2 del (4.42.1), l'iperpiano $ax = 0$ è l'*iperpiano tangente* a D in P.

4.43 Lezione 43

Torniamo alle quadriche, e quindi alla convenzione che C non abbia caratteristica 2. Possiamo applicare il Teorema 4.42.1 alla $f(x) = x^* Ax$ di una quadrica Q; le f_i del (4.42.1) sono le $f_i(x) = 2\sum_j a_{ij}x_j$ elemento di indice i in $2Ax$; quindi, per un punto $p \in \mathrm{supp}Q$ le a_i del (4.42.1) formano, a meno del fattore 2, la matrice $1 \times (n+1)$ data da p^*A, che è quella delle coordinate plückeriane della polare di p, quando questa esiste. Perciò il punto p è singolare su Q se, e solo se, $p^*A = 0$ (il che fra l'altro include l'essere $p^*Ap = 0$, ossia $p \in \mathrm{supp}Q$); e di tali P ne esistono se, e solo se, A è singolare come matrice; questi p, come vettori, sono quelli del nucleo della forma quadratica, e come punti sono quelli del vertice di Q [Quest'ultimo fatto, dato qui come conseguenza di quanto già sappiamo sul vertice, si vede anche elegantemente così: se p è singolare, ogni retta per p ha in p intersezione almeno doppia con Q, e quindi esattamente doppia perché $\mathrm{ord}Q = 2$, oppure giace su $\mathrm{supp}Q$; se tale retta passa per un altro punto di $\mathrm{supp}Q$, ma non giace su $\mathrm{supp}Q$, interseca Q in un divisore di ordine almeno 3, assurdo perché $\mathrm{ord}Q = 2$; quindi deve giacere su $\mathrm{supp}Q$]. Si è così visto:

Teorema 4.43.1. *Una quadrica ha punti singolari se, e solo se, è degenere; ed in tal caso i suoi punti singolari sono tutti e soli quelli del vertice.*

Per le non degeneri si ha:

Teorema 4.43.2. *Un iperpiano di $\bar{S}_n$ è tangente alla quadrica non degenere Q di S_n se, e solo se, contiene il proprio polo p; ed in tal caso p è l'unico punto di tangenza. In altre parole, dato $p \in Q$, l'iperpiano tangente a Q in p è la polare di p.*

Dim. Il (4.42.1) dice subito che l'iperpiano tangente a Q in p è la polare a di p; questo stesso iperpiano non può essere tangente a Q altrove, perché un punto diverso da p ha una polare diversa da a. C.V.D. □

Se si mettono insieme i (4.43.1), (4.43.2) si vede che se Q è degenere con vertice $\bar{S}_m$, e se P è un suo punto semplice, l'iperpiano tangente a Q in P è tangente a Q anche in tutti i punti di $\bar{S}_m + P$, e solo in questi.

Tutto questo può naturalmente essere ripetuto per le quadriche inviluppo, ossia per quelle di S_n^*; esse avranno "punti tangenti"; da notare che la duale Q^* di una Q di S_n^* esiste quando Q è non degenere, ed è l'insieme degli iperpiani tangenti a Q, sicché Q è l'insieme dei "punti tangenti" a Q^*. Se Q è degenere, l'insieme dei suoi iperpiani tangenti è una varietà ma non il supporto di una quadrica: per esempio, in S_2, se $Q = R_1 + R_2$ (rette distinte), quell'insieme consiste di tutte le rette per $R_1 \cap R_2$; e cioè una "retta" di S_2^*. Ciò non toglie che le quadriche degeneri di S_n^* esistano: scimmiottando la loro costruzione mediante vertice e quadrica non degenere di un sottospazio, si fà così: si sceglie un S_{n-m-1}^* sghembo con S_m^* (stella di S_n di centro un S_m sghembo al precedente S_{n-m-1}; notare che qui l'asterisco apposto ai simboli di sottospazio sta solo a ricordare che sono sottospazi di S_n^*, e non comporta la loro dualità con gli stessi simboli non asteriscati); in S_{n-m-1}^* si prende una quadrica non degenere H^* (che consisterà quindi degli iperpiani L di S_n che contengono S_m e tali che $L \cap S_{n-m-1}$ sia tangente ad una quadrica non degenere H di S_{n-m-1}); la nostra quadrica degenere Q^* sarà allora l'insieme degli iperpiani K di S_n ciascuno dei quali appartiene ad un fascio il cui centro è l'intersezione di uno qualunque dei precedenti L con un iperpiano qualunque contenente S_{n-m-1}. Si constata con un po' di pensamenti che questo vuol dire solamente che: $K \in \operatorname{supp} Q^*$ se, e solo se, o K contiene S_{n-m-1}, ovvero $K \cap S_{n-m-1}$ è tangente ad H. Casi speciali:

1. Per $n = 1$: il solito punto contato due volte.
2. Per $n = 2$:
   (a) matrice di caratteristica 2: due fasci di rette con centri distinti;
   (b) matrice di caratteristica 1: un fascio di rette contato due volte.
3. per $n = 3$:
   (a) matrice di caratteristica 3: si sceglie una conica non degenere H su un piano T; la Q^* è l'insieme formato da T (vertice) e da tutti i piani $K \neq T$ tali che $K \cap T$ sia tangente ad H;
   (b) matrice di caratteristica 2: due stelle (di piani) con centri distinti;
   (c) matrice di caratteristica 1: una stella di piani contata due volte.

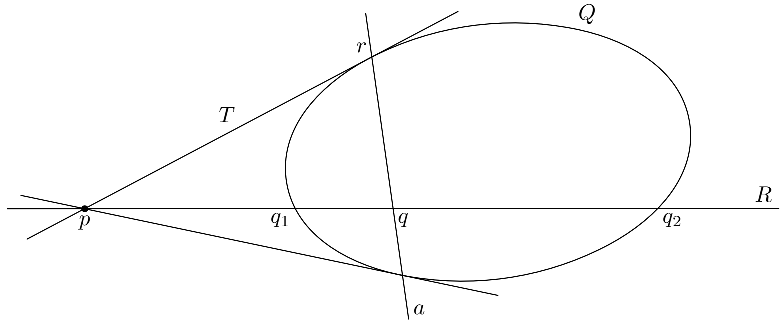
4.44 Lezione 44

La teoria delle quadriche, e soprattutto delle coniche, ha contribuito profondamente alla creazione della geometria proiettiva; vi è quindi una messe di risultati che un tempo erano di dimostrazione un po' riposta, ma che ora possono essere considerati dei semplici esercizi. Taluni di questi meritano di essere conosciuti, sia per l'eleganza che per l'utilità; eccone alcuni.

Ne premettiamo uno riguardante le proiettività sulla retta: una tale proiettività π di una retta R (su $\bar{C}$) in sé, è una *involuzione* se è anche una polarità, ossia $\pi^2 = 1 =$ proiettività identica; la matrice M, di tipo 2×2, di π dovrà dunque essere tale che $M^2 = c =$ matrice scalare non nulla, sicché, se π non è l'identità, il suo polinomio caratteristico sarà $z^2 = c$, e per (3.36.1) M sarà simile a $\left(\begin{smallmatrix} b & 0 \\ 0 & -b \end{smallmatrix}\right)$, ove $b \in \bar{C}$ è una radice quadrata di c. Supposto che M abbia già questa forma, i *punti uniti* di π (quelli che corrispondono a se stessi) sono $(0, 1) = u$ e $(1, 0) = v$; una coppia di punti corrispondenti sarà $x = (x_0, x_1)$ e $y = (x_0, -x_1)$. Ora si vede che il birapporto $(u, v, x, y) = (\infty, 0, x_1/x_0, -x_1/x_0)$ vale -1 sicché:

Lemma 4.44.1. *In una involuzione sulla retta su $\bar{C}$, che non sia l'identità, i punti uniti sono due (distinti), e separano armonicamente ogni coppia di punti corrispondenti.*

Sia Q una quadrica non degenere di S_n, e π la polarità legata ad essa; se S_m è sottospazio di $\bar{S}_n$ non tangente a Q, o rispettivamente se T_m è stella di $\bar{S}_n$ con centro L non tangente a Q (che se questo centro è un punto vuol dire che non deve stare su Q), allora la $Q \cap S_m$, o rispettivamente la $Q^* \cap T_m$, è quadrica non degenere di S_m, o rispettivamente di T_m, e come tale induce una polarità π' in S_m, o rispettivamente in T_m, detta la *polarità indotta* da Q; se S_m è una retta, o rispettivamente T_m è un fascio, la π' è una involuzione. Geometricamente si trova così: dato $p \in S_m$, o rispettivamente, dato $a \in T_m$ (a iperpiano di $\bar{S}_n$), è $\pi' p = S_m \cap \pi p$, o rispettivamente $\pi' a = L + \pi a$.



In particolare, sia Q quadrica non degenere di S_n; sia $p \notin Q$ un punto in $\bar{S}_n$ (e tutti gli enti che seguono sono pure in $\bar{S}_n$), e sia a la polare di p; sia poi R una retta per p non tangente a Q; allora $R \cap Q = q_1 + q_2$, con q_1, q_2 punti distinti; e inoltre $R \cap a = q$ è un punto $\neq p$ e $\neq q_1, q_2$ (se fosse $q = q_1$ la polare di q passerebbe per q, e naturalmente per p, sicché conterrebbe R, ed R sarebbe tangente). Sia π' l'involuzione su R indotta da Q, ossia π. I punti uniti di π' sono q_1, q_2, mentre p, q è coppia di punti corrispondenti; quindi per (4.44.1):

Teorema 4.44.2. *Nelle notazioni descritte (vedasi schizzo), i punti p, q separano armonicamente i punti q_1, q_2.*

Continuiamo con lo stesso disegno; la $Q' = a \cap Q$ è quadrica su a, ma non degenere perché a non è tangente a Q; preso un suo punto r, sia T la retta per p ed r; dico che T è tangente a Q. Se così non fosse, T potrebbe essee presa come la R precedente; senonché ora i punti p, q, q_1, q_2 sono sostituiti da p, r, r, e qualche a che con i tre scritti dovrebbe avere birapporto -1; ma è impossibile avere un gruppo armonico di tal fatta, salvo il caso $s = r$. Perciò:

Teorema 4.44.3. *Nelle notazioni descritte (vedasi schizzo), T 1'e tangente a q in r.*

Altra cosa:

Teorema 4.44.4. *Siano F_1, F_2 fasci di rette di S_2, con centri C_1, C_2; sia f una proiettività di F_1 su F_2, che se $C_1 = C_2$ non sia l'identità: si indichi con $\bar{f}$ la ovvia estensione di f da $\bar{F}_1$ a $\bar{F}_2$. Allora l'unione degli $z \cap \bar{f} z$, quando z percorre*

$\bar{F}_1$, è il supporto di una conica Q di S_2; la Q è degenere (=spezzata nel caso di S_2) solo nei casi seguenti:

1. *$C_1 \neq C_2$ ma f è una prospettività; in tal caso le componenti (distinte) di Q sono la retta per C_1 e C_2, e l'asse di prospettività;*
2. *$C_1 = C_2$ ed f ha due rette unite distinte: Q è spezzata in quelle due rette;*
3. *$C_1 = C_2$ ed f ha una sola retta unita: Q è quella retta, ma con molteplicità 2.*

Reciproco parziale: Sia Q una conica non degenere di S_2, e siano C_1, C_2 suoi punti razionali su C; ad ogni retta z di S_2 per C_1 si faccia corrispondere la z' per C_2 tale che $Q \cap z' - C_2 = Q \cap z - C_1$; allora la $z \mapsto z'$ è proiettività del fascio di centro C_1 (in S_2 su quello di centro C_2.

Dimenticavo di dire che l'*asse di prospettività* è per i fasci di rette quello che il centro di prospettività è per le rette (lezione 26).

Dim. I casi 2 e 3 sono ovvii; per il caso 1, e per il reciproco, conviene il metodo analitico. Prendiamo $C_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $C_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, sicché le rette per C_1 sono le $a = (a_0, 0, a_2)$, e quelle per C_2 le $b = (b_0, b_1, 0)$; la proiettività f sarà data da $b = aM$, per una matrice M opportuna 3×3 (è in realtà una 2×2 gonfiata per tener conto degli zeri fissi in a e b). Il punto x è su Q se, e solo se, è soluzione comune di $ax = 0$ ed $aMx = 0$ per qualche $a \neq 0$, ossia se, e solo se, il sistema precedente, nelle incognite a_0, a_2 ammette soluzione non nulla. Ciò accade se, e solo se, il minore delle righe 0 e 2 della matrice dei coefficienti è nullo; ma tale minore è quadratico omogeneo non nullo in x_0, x_1, x_2, onde Q è conica. Lo spezzamento di Q darebbe che f è prospettività.

Per il viceversa basta ragionare così: dato z, lo $z \cap Q$ si ottiene risolvendo una equazione quadratica; ma una soluzione è già nota (il punto C_1), sicché basta risolvere una equazione lineare; trovata l'altra intersezione p, la retta z' si trova linearmente; in tal modo si passa da z a z' linearmente, e l'applicazione è un'applicazione proiettiva, che è necessariamente una proiettività perché la sua immagine contiene più di uno z'. C.V.D. $\square$

Chiamiamo p il punto $Q \cap z' - C_2 = Q \cap z - C_1$ descritto nel (4.44.4); la corrispondenza $p \mapsto z$ è biunivoca, e permette quindi di considerare Q stessa, o meglio $\operatorname{supp} Q$, come un $\bar{S}_1$, dato che $\bar{F}_1$ è un $\bar{S}_1$; ed anzi, i puntidi $\operatorname{supp} Q$ che sono razionali su C sono in corrispondenza con le rette di F_1, sicché il loro insieme può essere considerato come un S_1. Questo sarebbe però vano se la identificazione dipendesse dalla scelta di C_1; il (4.44.4) dice appunto che così non è. In altre parole, se p_1, p_2, p_3, p_4 sono punti di Q, di cui almeno 3 distinti, e se ci proponiamo di definire il loro birapporto per mezzo di $(p_1, p_2, p_3, p_4) = (z_1, z_2, z_3, z_4)$, il (4.44.4) assicura che questa è una buona definizione. Ora si può dire che:

Teorema 4.44.5. *Ogni conica non degenere razionale su C è uno spazio proiettivo punteggiato di dimensione 1 (retta) su $\bar{C}$ (non, naturalmente, un sottospazio dell'$\bar{S}_2$ che la contiene). Se poi Q ha almeno un punto razionale su C, l'insieme di tali punti è uno spazio proiettivo punteggiato di dimensione 1 su C.*

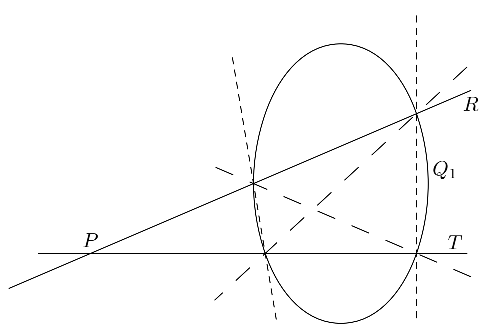
I (4.44.4), (4.44.5) permettono di risolvere graficamente “con la sola riga” problemi di secondo grado, purché sia data una conica (o con riga e compasso se la conica non è data).

4.45 Lezione 45

Se A_0, A_1 sono le matrici di due quadriche distinte Q_0, Q_1 nello stesso S_n, la $A = t_0A_0 + t_1A_1$, con $t_0, t_1 \in C$, non ambedue nulli, è la matrice di una quadrica Q di S_n; tutte queste quadriche Q, in corrispondenza biunivoca con i punti della retta C su cui t_0, t_1 sono coordinate proiettive, formano un *fascio di quadriche* su C; esso è quindi uno spazio proiettivo di dimensione 1 su C. Se si permette a t_0, t_1di assumere valori in $\bar{C}$, si ottiene naturalmente l'estensione su $\bar{C}$ del fascio descritto (ma le quadriche non saranno più tutte razionali su C). Se P è punto di $\operatorname{supp} Q_0 \cap \operatorname{supp} Q_1$, esso appartiene anche a $\operatorname{supp} Q$ per ogni Q; vi è una relazione molto stretta fra i fasci di quadriche e l'intersezione fra due di esse; è però abbordabile, con quanto è a nostra disposizione, solo per le coniche.

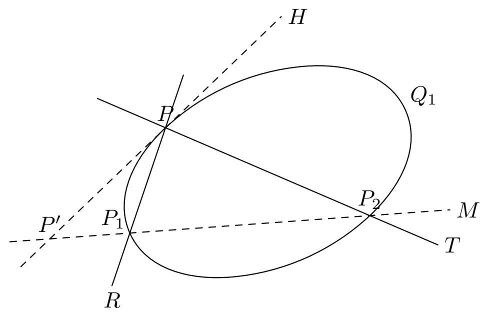
Sia dunque F un fascio di coniche su C, due distinte delle quali sono le Q_0, Q_1 di prima. Se queste sono ambedue spezzate, ed hanno una componente comune, quella componente è comune a tutte le Q (dimostrarlo), sicché ogni Q è spezzata; questo è un caso poco interessante (ed accade anche quando le Q_i sono ambedue spezzate ed hanno in comune un punto del vertice), e lo escluderemo. In tal caso Q è spezzata se, e solo se, $\det A = \det(t_0A_0 + t_1A_1) = 0$; il $\operatorname{div}_F \det A$ è una ipersuperficie di ordine 3 in F, che è perciò somma di tre “punti” L_1, L_2, L_3 di $\bar{F}$, ciascun punto essendo naturalmente una conica $Q \in F$ spezzata. Due di queste, o tutte e tre, possono coincidere, e studieremo i vari casi in dettaglio. Dato che una degenere nel fascio c'è certamente (la L_1), possiamo prendere $Q_0 = L_1$; la Q_1 sarà presa non spezzata.

1. $L_1 = R + T$ rette distinte, con $P = R \cap T \notin \operatorname{supp} Q_1$, ed R, T non tangenti a Q_1; ora $\operatorname{supp} L_1 \cap \operatorname{supp} Q_1$ consta di 4 punti a 3 a 3 non allineati; vogliamo dimostrare che il fascio consta di tutte le coniche passanti per questi 4 punti:



si osservi infatti che l'equazione di una conica in $\bar{S}_2$ contiene 6 coefficienti, determinati dalla conica a meno di proporzionalità; quindi l'insieme di tutte le coniche forma un $\bar{S}_5$; quelle che passano per un punto formano un $\bar{S}_4$; per 2, un $\bar{S}_3$; per 3, un $\bar{S}_2$ (rete), e per 4 non allineati, un fascio. Nel caso presente, le tre coppie di lati opposti del quadrangolo piano completo (lezione 25) che ha i quattro punti come vertici sono le 3 coniche spezzate, tutte distinte.

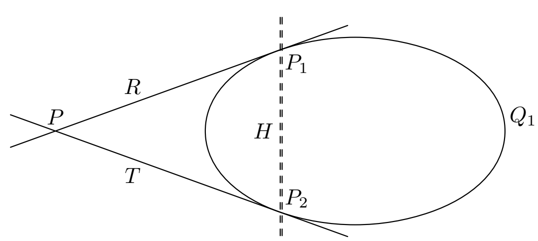
2. $L_1 = R + T$, con $P = R \cap T \in \operatorname{supp} Q_1$, ed R, T non tangenti a Q_1; ora $\operatorname{supp} Q_1 \cap \operatorname{supp} L_1$ consta di 3 punti, P e altri due P_1, P_2, non allineati;



L_1 e Q_1 hanno in comune la tangente H in P, sicché ciò resta vero per ogni $Q \in \bar{F}$ (dimostrarlo). Dato che l'imposizione di una tangente data in un dato punto è, nell'$\bar{S}_5$ del caso 1, due condizioni lineari, il dare 3 punti e la tangente in uno di essi dà 4 condizioni lineari, sicché $\bar{F}$ consta di tutte le coniche passanti per i tre punti e aventi in P tangente H. Una di queste è L_1, che possiamo prendere come divisore di x_1x_2; un'altra è $L_2 = H +$ (retta M per P_1 e P_2, che possiamo prendere come divisore di $(x_1 + x_2)x_0$. Ora Q è il divisore di $t_0x_1x_2 + t_1(x_1 + x_2)x_0$, sicché $\det A = t_0t_1^2$, donde si vede che $L_3 = L_1$. Due qualunque coniche del fascio si chiamano *tangenti* in P.

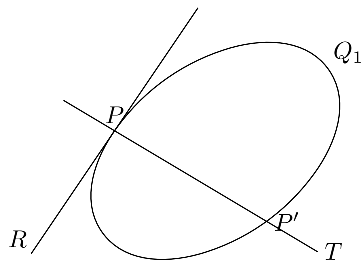
3. (vedasi figura del caso 2). $L_1 = H + M$, con $P' = H \cap M \notin \operatorname{supp} Q_1$, ed H, ma non M, tangente a Q_1 in un punto P certo $\neq P'$; 3 punti di intersezione, e cioè P e i due P_1, P_2 di $M \cap Q_1$; di nuovo H è tangente comune, onde $L_2 =$ somma delle due rette R (per P e P_1) e T (per P e P_2); idem come caso 2 con L_1, L_2 scambiate.

4. $L_1 = R + T$, con $P = R \cap T \notin \operatorname{supp} Q_1$, ma R, T tangenti a Q_1 in P_1, P_2 rispettivamente; 2 punti d'intersezione, e ivi due tangenti date, distinte;



le $Q \in \bar{F}$ sono determinate da queste proprietà, $L_2 = 2$(retta H per P_1, P_2); $L_1 = \operatorname{div} x_1x_2$; $L_2 = \operatorname{div} x_0^2$; $Q = \operatorname{div}(t_0x_1x_2 - t_1x_0^2)$; $\det A = t_0^2t_1$, sicché $L_3 = L_1$.

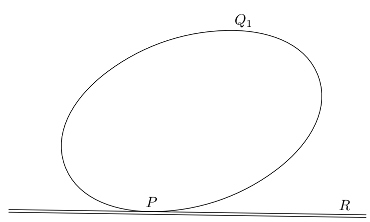
5. $L_1 = R + T$, $P = R \cap T \in \operatorname{supp} Q_1$, R tangente a Q_1 in P; due punti di intersezione P e P'; due qualunque coniche del fascio sono *osculatrici* in P.



Se $L_2 \neq L_1$, P deve essere sul vertice di L_2, col che le equazioni sia di $\operatorname{supp} L_1$ che di $\operatorname{supp} L_2$ possono essere espresse in modo da contenere solo, per esempio, x_0 ed x_1; lo stesso sarà vero di ogni Q, onde ogni Q è spezzata, caso escluso. Questo basta a dire che $L_2 = L_1$, e quindi $= L_3$.

6. (Vedasi figura del caso 4). $L_1 = 2H$, H non tangente a Q_1; se $P_1 + P_2 = H \cap Q_1$, tutte le Q passano per P_1, P_2, ed hanno ivi le tangenti R, T di Q_1; è come il caso 4.

7. $L_1 = 2R$, R tangente a Q_1 in P; un punto d'intersezione ed ivi data tangente;



due qualunque coniche del fascio sono *iperosculatrici* in P. Stesso discorso del caso 5, sicché $L_1 = L_2 = L_3$.

C'è un premio come conseguenza di tutta questa discussione: chiamiamo *ciclo* (di dimensione zero) su $\bar{S}_n$ ogni elemento del gruppo additivo liberamente generato dai punti; per i cicli si adotta la nomenclatura dei divisori: l'unione dei punti è il *supporto*; poi ci sono le *componenti*, le *molteplicità*, i cicli *effettivi* o *positivi*, e l'*ordine* del ciclo (=somma delle molteplicità). Ora l'*intersezione* $Q \cap Q'$ di due coniche qualunque del fascio (ma due coniche stanno sempre in un fascio) può essere definita come ciclo effettivo di ordine 4 nel modo seguente (i numeri si riferiscono ai casi elencati):

1. La somma dei quattro punti;
2. e 3. $2P + P_1 + P_2$;
4. e 6. $2P_1 + 2P_2$;
5. $3P + P'$;
7. $4P$.

4.46 Lezione 46

Prima di proseguire, non voglio passare sotto silenzio l'enunciato (senza dimostrazione) di un famoso teorema di cui la definizione che chiude la lezione precedente è un minimo esempio. Vi è un metodo, che non descrivo, di definire l'intersezione di n divisori di $\bar{S}_n$ quando l'intersezione dei loro supporti consta di un numero finito di punti. Il risultato è il seguente:

Teorema 4.46.1 (di Bezout)**.** *Se $D_1, \ldots, D_n$ sono divisori di $\bar{S}_n$, di ordini $r_1, \ldots, r_n$, e se $\bigcap_i \operatorname{supp} D_i$ è un insieme finito, allora $\bigcap_i D_i$ è un ciclo di ordine $\prod_i r_i$.*

Questo teorema è, fra l'altro, un modo di esprimere correttamente un teorema sulle equazioni, un cui enunciato abbastanza comune, ma falso, è il seguente: se n equazioni algebriche in n incognite hanno un numero finito di (sistemi di) soluzioni, tale numero è uguale al prodotto dei loro gradi. Esempio della falsità di questo enunciato: $x = 0$, $xy = 1$; gradi 1, 2; soluzioni: nessuna; traduzione geometrica: $x_0 = 0, x_0x_1 = x_2^2$; sono retta e conica; intersezione, ossia soluzioni: punto $(0, 1, 0)$ con molteplicità 2.

Passiamo ad altro, e precisamente alla classificazione delle quadriche non degeneri. Non dimentichiamo che se $S_n = [V]_1$, i punti della quadrica (perlomeno quelli razionali su C) sono i $\langle v\rangle$ generati dai $v \in V$ non nulli e isotropi nella norma la cui matrice è la matrice della quadrica; stiamo perciò studiando le norme, e ci dobbiamo aspettare le difficoltà connesse col gruppo di Witt. Cominciamo con la *classificazione proiettiva*; significa che data una Q non degenere, occorre trasformarla, mediante proiettività, in una la cui matrice sia "canonica"; equivalentemente: occorre trovare un nuovo sistema di riferimento proiettivo nel quale la matrice della Q sia canonica. Le matrici delle quadriche si trasformano per congruenza, sicché il (1.14.5) dice che ogni quadrica non degenere può ridursi alle forme:

$$\text{(4.46.2)} \qquad C \text{ arbitrario} : \sum_{i=0}^{n} c_i x_i^2 = 0, \qquad 0 \neq c_i \in C;$$

$$\text{(4.46.3)} \qquad C \text{ algebricamente chiuso} : \sum_{i=0}^{n} x_i^2 = 0;$$

(4.46.4) $\quad C$ ordinato con ogni elem. positivo un quadrato :

$$\sum_{i=0}^{r} x_i^2 - \sum_{i=r+1}^{n} x_i^2 = 0; \qquad \begin{array}{l} 2r \geq n-1; \\ r \text{ univocamente determinato.} \end{array}$$

Il (4.46.2) dà poche informazioni, perché se ci imbattiamo in due quadriche con dei c_i diversi, non sappiamo dire se esse siano o no la stessa quadrica in sistemi di riferimento diversi; i (4.46.3) e (4.46.4) invece danno informazioni totali: il primo dice che, per quei corpi, vi è una sola quadrica, a meno di trasformazioni proiettive; il secondo dice che, per quei corpi, vi è un numero finito di quadriche (sempre a meno di ...), riconoscibili dal numero r che è un invariante.

Casi particolari:

4.46.5. *C come nel (4.46.4), $n = 2$, $r = 1$: $x_0^2 + x_1^2 - x_2^2 = 0$; coniche con punti razionali su C; idem, $r = 2$: $x_0^2 + x_1^2 + x_2^2 = 0$; coniche senza punti razionali su C.*

4.46.6. *C come nel (4.46.4), $n = 3$, $r = 1$: $x_0^2 + x_1^2 - x_2^2 - x_3^2 = 0$; quadriche a punti iperbolici; infiniti punti razionali su C; idem, $r = 2$: $x_0^2+x_1^2+x_2^2-x_3^2 = 0$; quadriche a punti ellittici; infiniti punti razionali su C; idem, $r = 3$: $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$; quadriche senza punti razionali su C.*

Il motivo della nomenclatura sui punti è il seguente: se C è ordinato, ogni coppia di piani distinti a, b spezza il complementare di $a \cup b$ in S_3 in due parti; precisamente la parte formata dai punti p per i quali il rapporto $\frac{ap}{bp}$ è positivo, e quella per la quale è negativo. Si può anche dire che se $\mathbb{A}_3$ è lo spazio affine per il quale b è il piano improprio, il complementare di a in $\mathbb{A}_3$ è spezzato in due da a; precisamente il pezzo formato dai punti p con $ap > 0$, e quello con $ap < 0$, avendo scelto le coordinate di p, come è solito per gli spazi affini, in modo che $bp = 1$. Notare che un piano solo non spezza S_3; il tutto è ripetibile per S_n qualunque. L'ordinamento in C rende C spazio topologico; quindi $\mathbb{A}_3$ è anch'esso topologico in quanto omeomorfo a $C \times C \times C$; se b è un altro piano, e $\mathbb{A}_3'$ è il corrispondente spazio affine, le topologie di $\mathbb{A}_3 \cap \mathbb{A}_3'$ indotte da quella di $\mathbb{A}_3$ e da quella di $\mathbb{A}_3'$, coincidono; questo permette di parlare di "intorni del punto q" in S_3, intendendosi che essi siano presi in qualsiasi $\mathbb{A}_3$ il cui piano improprio non contenga q.

Premesso tutto questo, si consideri la quadrica Q del (4.46.6), $r = 1$. La metrica data dalla sua matrice (nello spazio vettoriale V_4 soprastante il proiettivo S_3) è iperbolica, onde, per (1.9.3), con un cambiamento di coordinate l'equazione della quadrica diviene $y_0y_1 + y_2y_3 = 0$; il cambiamento è $y_0 = x_0 + x_3$, $y_1 = x_0 - x_3$, $y_2 = x_1 + x_2$, $y_3 = x_1 - x_2$; consideriamo un suo punto p razionale su C nel quale, per esempio, $p_0 \neq 0$, sicché si può supporre $p_0 = 1$; in un intorno di esso in S_3 è anche $y_0 \neq 0$, onde di nuovo $y_0 = 1$, e l'equazione in coordinate cartesiane diviene $y_1 + y_2y_3 = 0$. La polare a di p (solo i suoi punti razionali su C) ha equazione $p_1 + y_1 + p_3y_2 + p_2y_3 = 0$; si vede quindi che le rette R_p , $T_p$intersezioni di a con i piani $y_2 = p_2$ e $y_3 = p_3$ sono distinte e sono su $Q \cap S_3$; perciò $Q \cap a = R_p + T_p$. Le rette R_p, T_p, al variare di p, sono le due *schiere di rette* di Q, e si constata facilmente che ogni R_p interseca ogni T_q (ma non coincide con essa), mentre due R_p (idem per due T_p) sono sghembe se non coincidono. Il fatto che $Q \cap a$ abbia, in un intorno di p, dei punti razionali su C mostra già, intuitivamente, che la a "attraversa" Q in un intorno p, ossia che i punti di Q razionali su C in un intorno di p, stanno alcuni in uno, e altri nell'altro, di quei due pezzi di $\mathbb{A}_3$ di cui si è parlato prima; si esprime ciò appunto col dire che ogni p è *punto iperbolico*. Per vederlo bene cerchiamo il segno di $p_1+y_1+p_3y_2+p_2y_3$ quando y appartiene a $Q \cap \mathbb{A}_3$[3] ed è vicino a p. La $y \in Q$ significa $y_1 = -y_2y_3$, sicché cerchiamo il segno di $p_1 - y_2y_3 + p_3y_2 + p_2y_3$ quando $y_i = p_i + \varepsilon_i$, $\varepsilon_i \in C$ piccoli; sostituendo si ottiene $-\varepsilon_2\varepsilon_3$, che effettivamente assume valori positivi e negativi.

Vediamo cosa succede per la Q del (4.46.6), $r = 2$; ora la metrica non è iperbolica, ma lo diventa su $\bar{C}$ per (1.14.2) (basta sostituire x_2 con ix_2, ove $i^2 =$

[3] $Q \cap S_3$ nel testo.

-1); cambiando dalle x alle y (ma ora $y_2 = x_1 + ix_2$, $y_3 = x_1 - ix_2$) si trovano ancora le due schiere di rette, che però sono in $\bar{S}_3$ e non definite su C. Ora interessa ancora il segno di $p_1 + y_1 + p_3y_2 + p_2y_3$ nell'intorno di p in S_3; e questa espressione è ancora $-\varepsilon_2\varepsilon_3$; senonché ora $\varepsilon_2 = \eta_1 + i\eta_2$, $\varepsilon_3 = \eta_1 - i\eta_2$, con $\eta_1, \eta_2 \in C$; pertanto $-\varepsilon_2\varepsilon_3 = -\eta_1^2 - \eta_2^2 < 0$: i punti di Q, razionali su C, vicini a p, stanno in uno solo dei due pezzi in cui a separa $\mathbb{A}_3$.

4.47 Lezione 47

Passiamo alla *classificazione affine*. Ora in S_n si è fissato un iperpiano Z, per esempio $x_0 = 0$, come iperpiano improprio, ottenendo uno spazio affine $\mathbb{A}_n$; le trasformazioni permesse sono le affinità (lezione 17), ossia (lezioni 23 e 24) le $A \mapsto M^*AM$ con M di tipo (1.18.4) (ripetuto nella lezione 24):

$$M = \begin{pmatrix} 1 & 0 & \dots & 0 \\ b_1 & & & \\ \vdots & & M' & \\ b_n & & & \end{pmatrix}. \tag{4.47.1}$$

Se la Q non è degenere, ovvero è degenere ma non spezzata in $Z+$iperpiano, l'equazione di Q nelle coordinate affini $y_i = \frac{x_i}{x_0}$ $(i = 1, \dots, n)$ resta di secondo grado, sebbene non più omogenea. La si può ottenere indifferentemente dalla $x^*Ax = 0$ sia dividendo per x_0^2, sia ponendo $x_0 = 1$.

Una prima classificazione delle non degeneri è fra le tangenti a Z, dette *paraboloidi* (*parabole* se $n = 2$), e le altre, dette *quadriche a centro*; il *centro* è il polo di Z; naturalmente un'affinità non cambia la proprietà di esser paraboloide o a centro. Sia $Q' = Q \cap Z$, sicché Q è paraboloide o a centro secondoché Q' è degenere o no; la matrice A' di Q' è ottenuta dalla A di Q cancellandovi la prima riga e la prima colonna; l'M' del (4.47.1) può essere scelto in modo che la A' assuma forma canonica diagonale; la A diviene allora

$$\begin{pmatrix} a_0 & a_1 & \dots & a_n \\ a_1 & c_1 & & \\ \vdots & & \ddots & \\ a_n & & & c_n \end{pmatrix}.$$

Si noti che, per quanto detto alla lezione 29, la trasformazione $A \mapsto M^*AM$, con M del tipo (4.47.1), permette di fare su righe e colonne di A tutte le operazioni elementari (le stesse sulle righe che si fanno sullle colonne) ad eccezione delle seguenti: 1) moltiplicazione della prima riga (colonna) per un numero $\neq 1$; 2) scambio della prima riga (colonna) con altra; 3) aggiunta della prima riga (colonna), moltiplicata per un numero $\neq 0$ ad altra riga (colonna). Se allora le c_i sono tutte non nulle, ossia se Q è a centro, operazioni elementari permesse annullano le $a_1, \dots, a_n$, ma non certo a_0 perché Q è non degenere; resta la forma canonica:

4.47.2. *Q a centro; C arbitrario: $\sum_{i=0}^{n} c_i x_i^2 = 0$; $c_i \in C$, $c_i \neq 0$;*

4.47.3. *Q a centro; C algebricamente chiuso: $\sum_{i=0}^{n} x_i^2 = 0$;*

4.47.4. *Q a centro; C ordinato e con ogni positivo un quadrato: $\sum_{i=0}^{r} x_i^2 - \sum_{i=r+1}^{n} x_i^2 = 0$; r univocamente determinato e ≥ 0 (ossia x_0^2 deve aver coefficiente $+1$).*

L'ultimo caso si è ottenuto così: la a_0 la si fa diventare 1 dividendo tutto per a_0; le c_i si fanno diventare ± 1 mediante operazioni elementari permesse, che ora in C sono possibili perché i positivi sono quadrati. Il centro nelle (4.47.2,3,4), è $(1, 0, \ldots, 0)$. Come nella classificazione proiettiva, i c_i del (4.47.2) non sono unici, sicché il (4.47.2) dice poco; invece il (4.47.3) dice che vi è un sol tipo di quadriche a centro, ed il (4.47.4), ove r è univocamente determinato, dà i vari tipi di quadriche a centro. Casi particolari del (4.47.4) (cfr. 4.46.5 e 4.46.6):

4.47.5. • *Come (4.47.4), ma $n = 2$, $r = 0$: $x_0^2 - x_1^2 - x_2^2 = 0$;* ellisse *con infiniti punti razionali su C; la $Q' = Q \cap Z$ non ha punti razionali;*
- *idem, $r = 1$; $x_0^2 + x_1^2 - x_2^2 = 0$;* iperbole*; ha infiniti punti razionali su C; la $Q' = Q \cap Z$ ha due punti razionali (distinti);*
- *idem, $r = 2$; $x_0^2 + x_1^2 + x_2^2 = 0$;* ellisse senza punti razionali *su C.*

4.47.6. • *Come (4.47.4), ma $n = 3$, $r = 0$: $x_0^2 - x_1^2 - x_2^2 - x_3^2 = 0$;* ellissoide *con infiniti punti razionali su C; la $Q' = Q \cap Z$ non ha punti razionali;*
- *idem, $r = 1$; $x_0^2 + x_1^2 - x_2^2 - x_3^2 = 0$;* iperboloide iperbolico*, o* a una falda *(perché?); infiniti punti razionali su C; $Q' = Q \cap Z$ ha punti razionali;*
- *idem, $r = 2$; $x_0^2 + x_1^2 + x_2^2 - x_3^2 = 0$;* iperboloide ellittico*, o* a due falde *(perché?); infiniti punti razionali su C; $Q' = Q \cap Z$ ha punti razionali;*
- *idem, $r = 3$; $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$;* ellissoide senza punti razionali *su C.*

Nelle quadriche a centro, le rette per il centro sono i *diametri*, e gli iperpiani per il centro sono gli *iperpiani diametrali*; nel fascio (per $n = 2$) o stella (per $n > 2$) di centro nel centro della quadrica, la polarità indotta dalla quadrica (lezione 44) si chiama l'*involuzione dei diametri coniugati*; per $n = 2$ è veramente un'involuzione; i due elementi corrispondenti si chiamano *coniugati*. Se il corpo C è come nel (4.47.4), la distinzione (delle quadriche a centro) in iperboloidi e ellissoidi è valida per qualunque dimensione dello spazio; Q è *iperboloide* se $Q \cap Z$ ha punti razionali su C; è *ellissoide* altrimenti. Per il (4.44.3), fra i diametri vi sono le rette tangenti a Q e passanti per il centro, che sono poi le rette per il centro e per i punti di $Q \cap Z$; sono rette di $\bar{S}_n$, ma se Q è iperboloide, e solo allora, alcune di esse contengono due punti razionali su C (il centro e il punto di tangenza quando questo è razionale su C), e sono quindi estensioni su $\bar{C}$ di rette di S_n tutte queste rette, anche quando non sono definite su C, sono gli *asintoti* di Q; per $n = 2$, le ellissi hanno due asintoti non definiti su C; le iperboli ne hanno due definiti su C. Per $n > 2$ gli asintotiti sono tutte le rette (generatrici) di un cono quadrico proiettante $Q \cap Z$ dal centro di Q, detto il *cono asintotico*; la sua equazione si ottiene ponendo $x_0 = 0$ nell'equazione della quadrica.

Veniamo al caso in cui $Q' = Q \cap Z$ è degenere, sicché Q è un paraboloide. La forma di A che precede il (4.47.2) è ancora valida, ma ora uno dei $c_i = 0$ (ma non due perché in tal caso A stessa sarebbe singolare). Mediante operazioni elementari permesse, si può supporre che $c_n = 0$; si può poi annullare $a_0, a_1, \ldots, a_{n-1}$ perché $a_n \neq 0$; infine, a_n diventa 1 mediante proporzionalità. Quindi

4.47.7. *Q paraboloide; C arbitrario:* $2x_0x_n + \sum_{i=1}^{n-1} c_i x_i^2 = 0$*;* $c_i \in C$*,* $c_i \neq 0$*;*

4.47.8. *Q paraboloide; C algebricamente chiuso:* $2x_0x_n + \sum_{i=1}^{n-1} x_i^2 = 0$*;*

4.47.9. *Q paraboloide; C ordinato e con ogni positivo un quadrato:* $2x_0x_n + \sum_{i=1}^{r} x_i^2 - \sum_{i=r+1}^{n-1} x_i^2 = 0$*; r univocamente determinato.*

Casi speciali:

4.47.10. *Come (4.47.9), ma* $n = 2$*:* $2x_0x_2 + x_1^2 = 0$*;* parabola *infiniti punti razionali su C;*

4.47.11. • *Come (4.47.9), ma* $n = 3$*,* $r = 1$*:* $2x_0x_3 + x_1^2 - x_2^2 = 0$*;* paraboloide iperbolico*, o* a sella*; infiniti punti razionali su C;*
• *idem, ma* $r = 2$*;* $2x_0x_3 + x_1^2 + x_2^2 = 0$*;* paraboloide ellittico*; infiniti punti razionali su C.*

4.48 Lezione 48

Passiamo alla *classificazione metrica*; se $\mathbb{A}_n$ è lo spazio affine ottenuto prendendo Z, ossia $x_0 = 0$ come iperpiano improprio, e il gruppo T delle omologie speciali di asse Z come gruppo delle traslazioni (lezione 23), bisogna anzitutto dare una metrica su $\mathbb{A}_n$, e cioè una norma su T (lezione 17). Questa sarà determinata da una matrice simmetrica non degenere H di tipo $n \times n$. Come si è visto alla lezione 23, T è isomorfo (sebbene non canonicamente) allo spazio vettoriale i cui sottospazi di dimensione 1 sono i punti di Z, sicché diremo addirittura che $Z = [T]_1$; se quindi ci si contenta di dare la matrice H a meno di proporzionalità, ossia di dare la metrice a meno dell'unità di misura, basta dare la quadrica non degenere $x'^*Hx' = 0$ su Z, ove x' significa $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Tale quadrica, che come ripeto è equivalente alla metrica esclusa l'unità di misura, si chiama l'*assoluto*, ed i suoi punti si chiamano i *punti ciclici*; il motivo sta nel fatto che, come vedremo, nel caso $n = 2$, una conica è un cerchio se, e solo se, passa per i due punti ciclici. Invece le rette di $\bar{\mathbb{A}}_n$ che, in quanto rette di $\bar{S}_n$ contengono qualche punto ciclico, si chiamano le *rette isotrope*; in generale, si chiamano *isotropi* tutti i sottospazi di $\bar{\mathbb{A}}_n$ che in quanto sottospazi di $\bar{S}_n$, hanno con Z una intersezione tangente all'assoluto. Ed allora, l'insieme di tutti gli iperpiani isotropi, più Z è una quadrica inviluppo (quadrica di S_n^*) degenere (cfr. la fine della lezione 43); anche questa viene spesso chiamata l'*assoluto*. La sua equazione, in coordinate plückeriane, è

$$a \begin{pmatrix} 0 & 0 \\ 0 & H^{-1} \end{pmatrix} a^* = 0. \tag{4.48.1}$$

L'assoluto dà una polarità su Z (*polarità assoluta*): $x' \mapsto (Hx')^*$; se proiettiamo x' e la sua polare $(Hx')^*$ da un punto P di $\bar{\mathbb{A}}_n$, che senza perdità di generalità possiamo supporre essere $(1, 0, \ldots, 0)$, le x' e $(Hx')^*$ sono coordinate rispettivamente di un "punto" e di un "iperpiano" della stella di centro P, sicché la

$x' \mapsto (Hx')^*$ diviene una polarità in quella stella. Un punto y' della stella, ossia una retta di $\bar{S}_n$, appartiene all'iperpiano $(Hx')^*$ se $x'^* Hy' = 0$. Ma questa è la condizione di ortogonalità dei vettori x', y' di $\bar{T}$, sicché la polarità della stella è quella che fa corrispondere ad ogni retta per P l'iperpiano per P ad essa ortogonale; si chiama perciò l'*involuzione degli angoli retti* (ma è una involuzione solo se $n = 2$).

Sia Q una quadrica non degenere di S_n; per poterne ridurre la matrice ad una forma canonica occorre anzitutto che il sistema di riferimento di partenza $(x_0, \ldots, x_n)$ sia in qualche modo canonico rispetto alla metrica; e l'unico modo che conosciamo è quello di richiedere che i vettori (nello spazio T delle traslazioni) che mandano $(1, 0, \ldots, 0)$ sugli $(1, 0, \ldots, 0, 1, 0, \ldots, 0)$ (1 nei posti 0 ed i) formino una base in qualche modo canonica; ciò possiamo ottenere se C è algebricamente chiuso richiedendo base ortonormale, e cioè $H = \mathbf{1}$; o se C è ordinato, con ogni positivo un quadrato, richiedendo che H sia del tipo

$$\begin{pmatrix} h_1 & & & \\ & h_2 & & \\ & & \ddots & \\ & & & h_n \end{pmatrix}, \qquad \text{con } h_i = \pm 1.$$

Supporremo allora sempre nel seguito di essere in uno di questi due casi; dopodiché, se A è la matrice di Q, i movimenti rigidi trasformano A in M^*AM, con M avente la forma (4.47.1), ove però ora la M' deve essere matrice di una trasformazione ortogonale (le M, M' sono rispettivamente le B, F del (1.18.4); quest'ultima condizione significa, per (1.8.5),

$$M'^* HM' = H. \tag{4.48.2}$$

Se C è algebricamente chiuso si è visto che $H = 1$, sicché le trasformazioni ortogonali sono date da matrice ortogonali; dopodiché non sappiamo andare avanti, perché non sappiamo nulla sulla forma canonica della matrici simmetriche rispetto alla simiglianza ortogonale nel caso di corpi algebricamente chiusi. Ad esempio, per $n = 2$, se $A = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1+i & 1 \\ 0 & 1 & 1-i \end{smallmatrix}\right)$, con $i^2 = -1$ (corpo complesso), la conica è a centro, ma la sua matrice non è riducibile a forma diagonale mediante movimenti rigidi del piano: infatti $\left(\begin{smallmatrix} 1+i & 1 \\ 1 & 1-i \end{smallmatrix}\right)$ ha l'unico autovalore 1 (cfr. 3.36.1). Perciò abbandoniamo l'impresa, e passiamo ad investigare l'unico caso per il quale abbiamo un risultato utile: il corpo C ordinato, tale che ogni suo elemento positivo sia un quadrato, e tale che $C[\sqrt{-1}]$ sia algebricamente chiuso; *questa convenzione è in forza fino alla lezione* 50 *compresa.*

Anche sotto questa ipotesi, se H non è definita (positiva o negativa) non si riesce sempre a diagonalizzare l'A' della matrice di una conica. Se per esempio, $A' = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$, non esiste una M' ad elementi in C tale che $M'^* A' M'$ sia diagonale e che la (4.48.2) sia soddisfatta con $h_1 = 1$, $h_2 = -1$: se infatti poniamo $M' =$

$\left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right)$, le precedenti relazioni significano

$$\begin{cases} xy + zt + 2(xt + yz) = 0 \\ xy = zt \\ x^2 - z^2 = 1 \\ y^2 - t^2 = -1 \end{cases}$$

Ora, dalle prime due segue $zt + xt + yz = 0$, che moltiplicata per x e tenendo conto della seconda dà $t(xz + x^2 + z^2) = 0$; è $t \neq 0$ (altrimenti $y^2 = -1$ dall'ultima), onde $xz + x^2 + z^2 = 0$, che insieme alla terza dà $xz + 2x^2 = 1$. Di nuovo $x \neq 0$ (per la terza), sicché $z = (1 - 2x^2)/x$, che sostituita nella terza dà $3x^4 - 3x^2 + 1 = 0$, e questa equazione non può dare un x^2 reale. *Supporremo quindi d'ora in poi, e fino alla lezione 50 compresa, che H sia definita, ed anzi che $H = \mathbf{1}$ (spazio euclideo).* Il caso $H = -\mathbf{1}$ è perfettamente analogo; il caso di H non definito (positivo o negativo) è anch'esso riducibile, per computi pratici, al caso $H = \mathbf{1}$ mediante trasformazioni del tipo $x_j \mapsto \sqrt{-1}\, x_j$ per certe j.

Con le convenzioni fatte, le isometrie sono date dalle M con M' matrice ortogonale; e sappiamo da (3.36.2) che A' è ortogonalmente simile ad una matrice diagonale; si può cioè supporre

$$A = \begin{pmatrix} ? & & ? & \\ & c_1 & & \\ ? & & \ddots & \\ & & & c_n \end{pmatrix}.$$

Ora, il solito discorso fatto per la classificazione affine: con una M del tipo (4.47.1), ma con $M' = \mathbf{1}$, la A può essere ridotta alla forma

$$B = \begin{pmatrix} a & 0 & \dots & 0 & b \\ 0 & a_1 & & & \\ \vdots & & \ddots & & \\ 0 & & & \ddots & \\ b & & & & a_n \end{pmatrix} \tag{4.48.3}$$

ove $a = -1$, $b = 0$, $a_i \neq 0$ per le quadriche a centro, mentre $a = 0$, $b = -1$, $a_i \neq 0$ se $i \neq n$, $a_n = 0$ per i paraboloidi; morale:

4.48.4. *C ordinato, con ogni positivo un quadrato, e con $C[\sqrt{-1}]$ algebricamente chiuso; spazio euclideo; quadriche a centro:*

$$\sum_{i=1}^{n} a_i x_i^2 = x_0^2;$$

gli $a_i \in C$ univocamente determinati;

4.48.5. *C idem; spazio euclideo; paraboloidi:*

$$\sum_{i=1}^{n-1} a_i x_i^2 = 2x_0 x_n;$$

gli $a_i \in C$ univocamente determinati a meno di un cambiamento complessivo del segno.

4.49 Lezione 49

Proseguiamo con la classificazione metrica. Intanto interessa saper trovare i valori degli a_i dei (4.48.3, 4.48.4, 4.48.5) dalla A originale; cominciamo dalle quadriche a centro. Per passare da A a B si è applicata prima una simiglianza ortogonale alla A'; poi si è applicata alla A una congruenza con una M a determinante 1 che lascia A' invariata; e infine si è diviso per un $\rho \in C$ non nullo. I c_i erano gli autovalori di A', e gli $a_i = \rho^{-1} c_i$ sono quelli di B', sicché $\rho a_i = c_i$; poi,

$$\det A' = \prod_i c_i = \rho^n \prod_i a_i \quad \text{mentre} \quad \det A = \rho^{n+1} \det B = -\rho^{n+1} \prod_i a_i,$$

sicché $\rho = -\frac{\det A}{\det A'}$, e infine

4.49.1. *Nella (4.48.4), gli a_i sono gli autovalori della matrice A' moltiplicati per $-\frac{\det A'}{\det A}$.*

Per i paraboloidi il discorso è simile, ma le formule sono:

$$(\text{prodotto autovalori non nulli di } A') = \rho^{n-1} \prod_{i \neq n} a_i,$$
$$\det A = \rho^{n+1} \det B = -\rho^{n+1} \prod_{i \neq n} a_i,$$

sicché $\rho^{-2} = -\frac{\text{prodotto autovalori non nulli di } A'}{\det A}$:

4.49.2. *Nella (4.48.5) gli a_i uguagliano gli autovalori non nulli della matrice A' moltiplicati per la radice quadrata (una qualunque delle due) del rapporto fra il loro prodotto e $-\det A$.*

Un po' di nomenclatura riguardante le (4.48.4, 4.48.5). I nomi per le coniche e quadriche (se $n = 2, 3$) sono gli stessi che nei casi (4.47.5, 4.47.6) e (4.47.10, 4.47.11); resta da dare dei nomi (per n qualunque) ai coefficienti stessi: nel caso (4.48.4) (quadriche a centro) gli a_i^{-1} sono i *quadrati dei semiassi* (vedremo perché), sicché i semiassi sono i $\pm a_i^{-1/2}$; è però invalso l'uso di chiamare *semiasse* la radice quadrata positiva, in C, di $\pm a_i^{-1}$ (il $\pm$ scelto in modo che $\pm a_i > 0$); tale semiasse è poi chiamato *reale* se $a_i > 0$, e *trasverso* altrimenti. Nel (4.48.5), gli a_i^{-1} si chiamano semplicemente *parametri*; sono determinati, come si è visto, a meno del segno; se però lo spazio affine, oltre che metrico, è orientato, il cambiamento di segno non è più permesso se si vuol mantenere l'orientamento, ed i parametri restano univocamente determinati.

Un punto x di $\bar{\mathbb{A}}_n$ ha da un punto fisso P, che prendiamo uguale a $(1, 0, \dots, 0)$, un quadrato della distanza dato da $r^2 \neq 0$ se, e solo se, $\sum_{i=1}^{n} r^{-2} x_i^2 = x_0^2$, il luogo di tutti i punti di $\bar{S}_n$ soddisfacenti a questa è una ipersuperficie irriducibile, supporto di una quadrica. Tale quadrica è detta *sfera* (*cerchio* o *circolo* se $n = 2$) di *centro* P e *quadrato del raggio* r^2; ciò vale per un corpo C qualunque e metrica arbitraria[4]; ma nel nostro caso si vede che una sfera è un ellissoide il cui centro (come quadrica a centro) è proprio il centro della sfera, e i cui quadrati dei semiassi sono tutti uguali (al quadrato del raggio). Notare che una quadrica non degenere è sfera se, e solo se, la sua intersezione con l'iperpiano improprio è l'assoluto. Per $r = 0$ si ottengono le *sfere degeneri*, che sono i *coni isotropi* di vertice nel centro della sfera; e volendo uno può anche parlare della "sfera di raggio infinito", che è l'iperpiano improprio di $\bar{S}_n$ con molteplicità 2.

Sia T un iperpiano diverso da Z, ne sia p il polo rispetto a Q, e sia R una retta per p, non su Z e non tangente a Q; se $q = R \cap T$, e se $q_1 + q_2 = R \cap Q$, il (4.44.2) dice che $(p, q, q_1, q_2) = -1$; se $p \in Z$, ossia se T è iperpiano diametrale, e se si sceglie su R una coordinata affine tale che p, q, q_1 abbiano coordinate ∞, 0, 1, si constata che q_2 ha coordinata -1. L'avere q_1, q_2 coordinate di segno opposto dice (come vedremo nell'ultima lezione) che se p viene considerato "esterno" al "segmento" q_1, q_2, allora q è "interno". Poi, se si sceglie un sistema di coordinate cartesiane ortogonali di origine in q, per le quali l'assoluto abbia ancora matrice $H = \mathbf{1}$, e tale che q_1 sia il punto $(1, c, 0, \dots, 0)$ [possibile per il 1.13.2], il punto q_2 avrà un $-c$ in luogo di c sicché i quadrati delle distanze di q da q_1 e q_2 sono uguali (ed uguali a c^2). Tutto ciò si esprime col dire che

Teorema 4.49.3. *In una quadrica a centro, ogni iperpiano diametrale dimezza le corde aventi direzione coniugata (ossia passanti per il suo polo). Resta vero per i paraboloidi, ove in luogo di "iperpiano diametrale" si legga "iperpiano proprio con polo improprio", il che vuol dire "iperpiano proprio passante per il punto di tangenza del paraboloide con l'iperpiano improprio".*

Fra gli iperpiani descritti (diametrali per le quadriche a centro, o passanti per ecc. ecc. per i paraboloidi) vogliamo cercare quei T il cui polo p è tale che ogni retta propria R per p (tutte parallele fra loro) sia ortogonale a T; occorre che p e $T \cap Z$ siano polo e polare nella polarità assoluta; se $b = (b_0, b')$ (con $b' \neq 0$) sono le coordinate plückeriane di T, il polo p è $p = A^{-1}b^*$ (ma richiediamo che $p_0 = 0$); $T \cap Z$ è l'iperpiano b' di Z, e noi vogliamo che $p' = H^{-1}b'^* = b'^*$. Ora $Ap = b^*$, e da $p_0 = 0$ segue $A'p' = b'^*$, $p' = A'^{-1}b'^*$, sicché $\rho A'^{-1}b'^* = b'^*$, $\rho b' = b'A'$. I b' sono perciò gli autovettori non nulli di A': nel caso (4.48.4) la condizione $p_0 = 0$ dà $b_0 = 0$, ossia T è iperpiano diametrale, come ci si aspettava; i b' si ottengono scegliendo un dato a_i in (4.48.4) come autovalore, poi tutti gli $a_j =$

[4] Ovviamente, cambiando metrica, cambierà la forma dell'equazione del luogo di punti equidistanti da un punto dato. [NdR]

a_i, e siano per esempio $a_i = a_{i_1}, a_{i_2}, \ldots, a_{i_s}$, e prendendo come b' qualunque $(b_1, \ldots, b_n) \neq 0$ in cui tutti i b_j con indice fuori dell'insieme $(i_1, \ldots, i_s)$ sono nulli; in generale quando tutti gli a_i sono distinti si trovano esattamente n tali b'; ma in un caso estremo (sfera) tutti gli iperpiani diametrali vanno bene. Comunque sia, i diametri coniugati agli iperpiani diametrali del tipo descritto si chiamano *assi* della quadrica a centro; essi coincidono con le intersezioni di $n-1$ qualunque fra quegli iperpiani diametriali speciali distinti. Mettendo insieme questo col (4.49.3) si ottiene che:

Teorema 4.49.4. *Ogni quadrica a centro in S_n ha almeno una n-upla di assi fra loro ortogonali. I quadrati dei suoi semiassi sono i quadrati delle distanze dal centro dei punti in cui la quadrica interseca i propri assi.*

Passiamo a trattare dei paraboloidi (4.48.5); i conti fatti prima vanno modificati: continua ad essere vero che il polo p di T è $p = A^{-1}b^*$; ma ora la condizione $p_0 = 0$ dà $b_n = 0$; il resto dei conti va bene, ed i b' sono gli autovettori non nulli di A' per i quali $b_n = 0$; per ottenere b occorre usare un b_0 desunto da $b^* = Ap$, ossia (per 4.48.3) $b_0 = b_n = 0$. Il resto del caso precedente, con la descrizione dei rimanenti b_i, va bene. Ora si vede che tutti gli iperpiani trovati passano per i punti $(1, 0, \ldots, 0)$ e $(0, \ldots, 0, 1)$, sicché essi contengono la retta passante per quei due punti; questa è l'*asse* del paraboloide, ed il primo punto descritto ne è il *vertice* (parola usata in senso del tutto diverso da quello del vertice di un cono; notare che il secondo punto è proprio il vertice del cono $Q \cap Z$).

4.50 Lezione 50

C'è un'ultima cosa che è bene sapere sulle coniche, dal punto di vista metrico; essa è valida per qualunque H, e quindi fino alla formula (4.50.1) l'H sarà supposto arbitrario. Ho detto coniche e non quadriche perché per $n > 2$ il discorso che sto per fare non funziona in generale; il punto in cui non funzionerebbe lo indicherò con un asterisco (*), lasciando il perché come esercizio. È dunque $n = 2$; prendiamo un punto proprio $p = (1, p')^*$; nel fascio di centro p, ad ogni retta b la Q fa corrispondere, per involuzione indotta nel fascio, una retta R; questa involuzione π può essere ottenuta così: si trasla l'origine nel punto p mediante la M del (4.47.1) con $b_i = p_i$ e $M' = \mathbf{1}$; la matrice di Q diviene M^*AM, e quella di Q^* è $(M^*AM)^{-1}$ quella dell'assoluto resta H perché una traslazione è un movimento rigido). La π è l'involuzione (= polarità) legata alla intersezione della conica inviluppo Q^* con $b_0 = 0$; la matrice di tale intersezione è quella delle ultime due righe e colonne in $(M^*AM)^{-1} = M^{-1}A^{-1}M^{*-1}$.

Se $A^{-1} = \left(\begin{smallmatrix} d_0 & d^* \\ d & D \end{smallmatrix}\right)$, la matrice descritta è la $d_0 p' p'^* - (p'd^* + dp'^*) + D$. Bene: noi cerchiamo dei punti propri p (che chiameremo *fuochi* della conica) per i quali l'involuzione π coincida con l'involuzione degli angoli retti. Quest'ultima è data dalla matrice H, sicché noi vogliamo che, per un opportuno $\rho \neq 0$ in C, si abbia

$$d_0 p' p'^* - (p'd^* + dp'^*) = \rho H - D. \tag{4.50.1}$$

Queste sono tre equazioni fra tre incognite (*), le p_1, p_2, ρ, ed hanno sempre soluzioni (*). Vediamo di risolverle esplicitamente nei casi (4.48.4) e (4.48.5), sicché ora H torna ad essere $= \mathbf{1}$.

Caso (4.48.4): nella (4.50.1) si ha $d_0 = -1$, $d_{ii} = a_i^{-1}$, e gli altri elementi di A^{-1} sono 0; quindi le (4.50.1) divengono

$$\begin{cases} -p_1^2 = \rho - a_1^{-1} \\ -p_1 p_2 = 0 \\ -p_2^2 = \rho - a_2^{-1} \end{cases} .$$

Dalla seconda si ha $p_1 = 0$, oppure $p_2 = 0$; nel primo caso la prima dà $\rho = a_1^{-1}$, e la terza dà $p_2^2 = a_2^{-1} - a_1^{-1}$; analogamente nell'altro caso; perciò:

Teorema 4.50.2. *Un cerchio ha un solo fuoco, che è il centro; un'ellisse o iperbole non cerchio di equazione (4.48.4) ha quattro fuochi, e precisamente* $(1, 0, \pm[a_2^{-1} - a_1^{-1}]^{1/2})$ *e* $(1, \pm[a_1^{-1} - a_2^{-1}]^{1/2}, 0)$. *Di questi, due sono razionali su C e due no.*

Caso (4.48.5): si ha $d_2 = -1$, $d_{11} = a_1^{-1}$, e gli altri elementi di A^{-1} sono nulli; perciò le (4.50.1) divengono

$$\begin{cases} 0 = \rho - a_1^{-1} \\ p_1 = 0 \\ 2p_2 = \rho \end{cases} .$$

Dalla prima, $\rho = a_1^{-1}$, sicché $p_2 = \frac{1}{2a_1}$:

Teorema 4.50.3. *Una parabola di equazione (4.48.5) ha un solo fuoco; esso è razionale su C, ed è dato da* $(1, 0, \frac{1}{2a_1})$.

4.51 Lezione 51

In quanto precede, specie nella lezione 48, l'S_1 è piuttosto trascurato; l'assoluto di S_1 dovrebbe essere una quadrica in Z, ma Z è un punto, il solito P_∞, e non ha quadriche; ciò è giusto, perché una metrica nello spazio affine $\mathbb{A}^1$ è data, a meno dell'unità di misura, non appena sia dato P_∞, per il semplice motivo che in uno spazio vettoriale di dimensione 1 vi è una sola norma a meno di proporzionalità; ed anzi, ogni tale spazio è orientabile, sicché si può definire non solo il quadrato della lunghezza di ogni vettore, ma anche la lunghezza, che è ciò che sarebbe chiamato il volume in dimensione > 1 (parlo sempre di un C ordinato). Se si prende la distanza fra un P_0 ed un P_1 come unità di misura, ecco che $x = (P_\infty, P_0, P_1, X)$ è la lunghezza del vettore $t = X - P_0 \in T$.

Questo è in accordo con la nostra intuizione quando l'S_1 lo pensiamo proprio come retta; ma fra gli S_1 ci sono anche i fasci di rette del piano, e per questi S_1 la costruzione descritta sarebbe la seguente: si fissa una retta r_∞, poi l'"angolo" $r_0 r_1$ come unità di misura; dopodiché la "lunghezza" di un angolo $r_0 x$ è (r_∞, r_0, r_1, x).

La misura così ottenuta non è però affatto quella normalmente usata; diviene una talvolta usata quando r_∞ ed r_0 siano ortogonali (nel senso familiare solito), e r_1 sia la bisettrice di $r_\infty r_0$: allora la misura descritta è il cosiddetto *coefficiente angolare* di $r_0 x$, ossia $\tan r_0 x$. L'altra misura, quella in gradi o in radianti, non salta affatto fuori dalle nostre lucubrazioni; ed anzi, gli unici angoli dei quali si è parlato nel corso sono i retti. Questo ci fa sospettare che negli S_1 ci debba essere un altro tipo di "metrica", che non rientra fra quelle sulle quali abbiamo speso tanto tempo.

Osserviamo che, fissata in S_1 una quadrica $Q = P_1 + P_2$, con $P_1 \neq P_2$, e tre punti X, Y, Z, si ha

$$(P_1, P_2, X, Y)(P_1, P_2, Y, Z) = (P_1, P_2, X, Z),$$

come conseguenza di (2.25.2). Perciò questo birapporto (P_1, P_2, X, Y) ha quasi la proprietà di una "distanza", nel senso che la distanza fra X e Z è il prodotto, invece che la somma, della distanza fra X e Y e di quella fra Y e Z. Il trucco per passare dai prodotti alle somme è il logaritmo; mettiamoci quindi nel caso in cui $C = \mathbb{R}$, e scriviamo $d(X, Y) = k \log (P_1, P_2, X, Y)$, con k numero complesso non nullo per ora arbitrario; questa espressione ha sempre significato se l'insieme $\{P_1, P_2, X, Y\}$ consta di almeno tre punti distinti (si intende che $\log \infty = \infty$ e $\log 0 = -\infty$). Ora i casi sono due:

1. P_1 e P_2 reali, ossia razionali su C; essi dividono S_1 in due *segmenti* così definiti: scelto un $X \in S_1$, $X \notin \{P_1, P_2\}$, un segmento è formato dagli $Y \notin \{P_1, P_2\}$ tali che $(P_1, P_2, X, Y) > 0$; l'altro da quelli per cui quel birapporto è < 0; si controlla subito che la definizione è indipendente dalla scelta di X. Nel secondo caso diremo che X, Y *separano* P_1, P_2 (questo è lo stesso discorso fatto nella lezione 46, ove due piani spezzano S_3 in due pezzi). Se X, Y sono sullo stesso segmento, vi è un solo $\log (P_1, P_2, X, Y)$ reale, determinato a meno del segno (per 2.25.1) perché nella quadrica Q non si sa chi sia P_1 e chi P_2. Preso per k un reale non nullo, e fissato un orientamento col dire quale sia P_1 e quale P_2 (questo dà proprio un orientamento dello spazio vettoriale soprastante ad S_1, nel senso della lezione 15), la $d(X, Y)$ funziona benissimo come distanza. Due punti dello stesso segmento hanno distanza reale, che è nulla se, e solo se, $X = Y$; è $d(X, Z) = d(X, Y) + d(Y, Z)$; poi $d(P_1, X) = -\infty$, $d(P_2, X) = +\infty$; se invece X, Y sono in segmenti diversi, il $k \log (P_1, P_2, X, Y)$ è complesso non reale, ed è determinato a meno di multipli interi di $2k\pi i$, ove $i^2 = -1$ e π è il numero di Archimede. Una siffatta definizione di distanza dà una *metrica iperbolica* di S_1.
2. P_1, P_2 non reali, e quindi con ascisse complesse coniugate; il (2.25.2) dà allora che, per ogni coppia X, Y di punti reali, e quindi diversi da P_1, P_2, il birapporto (P_1, P_2, X, Y) è il rapporto fra due numeri complessi coniugati non reali; il suo logaritmo è perciò puramente immaginario, e definito a meno di multipli interi di $2\pi i$ (ed anche a meno del fattore ± 1 se non si stabilisce chi sia P_1 e chi P_2). Scelto $k = hi$ con h reale, e fissati P_1, P_2, ecco che $d(X, Y)$ è reale, ma è definita a meno di multipli interi di $2h\pi$. Una siffatta distanza dà una *metrica*

ellittica su S_1, e $2h\pi$ è l'*ampiezza* di S_1. È questa, con $h = 1$ la metrica (in radianti) usualmente adottata per la misura degli angoli.

Le due metriche descritte si chiamano *non euclidee*; tutte quelle descritte nel resto di questo corso sono *euclidee*, ovviamente in un senso diverso da quello dato nela lezione 17. Le euclidee possono anche essere chiamate *paraboliche*, in quanto casi limite (per $P_1 = P_2$) delle non euclidee. Facciamolo vedere, partendo per esempio dal caso iperbolico (la partenza da quello ellittico funziona nello stesso modo).

Le coordinate ascisse di P_1, P_2 siano z e $-z$, con $z > 0$; quelle di X, Y, siano x, y; e si prenda $k = hz$; si ha

$$d(X, Y) = k \log (z, -z, x, y) = hz \log \frac{(x - z)(y + z)}{(x + z)(y - z)},$$

che è reale se $|x|$, $|y|$ sono ambedue $< z$. Quando z tende a ∞ (col che P_1, P_2 vengono a coincidere con P_∞), questa espressione tende al valore $2h(y - x)$ (regola di l'Hospital), che è appunto la distanza fra x ed y in una metrica delle solite.

In tutto il corso, riferendosi al caso $n = 2$, si è data una metrica nel piano per mezzo di un assoluto consistente in una conica inviluppo degenere, a supporto riducibile; essa definisce su ogni retta non appartenente alla conica una metrica parabolica, fissata dal punto improprio (intersezione della retta col vertice dell'assoluto) e da una unità di misura variabile da retta a retta, e determinata dalla posizione del punto improprio rispetto ai punti ciclici; mentre su ogni fascio a centro proprio definisce una metrica non euclidea, ellittica se i punti ciclici sono non reali, e iperbolica altrimenti. Si sarebbe potuto invertire il ruolo retta-fascio, dando come assoluto una conica non degenere (ed allora che sia luogo o inviluppo non interessa più), si ottengono metriche non euclidee sia sulle rette che sui fasci. Sono queste le *metriche non euclidee* del piano, che sono ellittiche o iperboliche secondoché l'assoluto non ha o ha punti reali. Da notare che sono metriche non di un piano affine, ma di tutto il piano proiettivo, esclusi, nel caso iperbolico, i punti reali (risp. le rette reali) dell'assoluto come centri di fasci (risp. come sostegni di punteggiate). Tuttavia, sempre nel caso iperbolico, per evitare punti con distanze non reali, si preferisce limitarsi a considerare solo la porzione di piano formata dai punti interni all'assoluto (o meno frequentemente solo da quelli esterni); le definizioni sono le seguenti: un punto (retta) è *interno* a Q se intanto $\notin Q$ ($\notin Q^*$), e se inoltre le due rette di Q^* (i due punti di Q) per il punto (sulla retta) non sono reali; è *esterno* se non è né interno, né su Q (su Q^*). Se Q ha punti reali, ogni retta (punto) per un punto interno (su una retta interna) è esterno, e reciprocamente.

Nel caso ellittico, due rette qualunque s'incontrano sempre, ossia non ci sono parallele; nel caso iperbolico (ma solo punti interni), ogni retta R ha, per un punto P fuori di essa, due "parallele", che sono le rette passanti per P e per, rispettivamente, le due intersezioni di R con l'assoluto.

Storicamente, le geometrie non euclidee nacquero dal tentativo, sempre andato a vuoto, di far discendere il quinto postulato di Euclide (quello delle parallele) dai precedenti; i postulati venivano considerati “verità palesi”, ed il quinto sembrava meno palese degli altri (ora sappiamo che sono tutti arbitrari). Falliti tutti i tentativi, nel secolo scorso un rampollo di famiglia militare ungherese (Bolyai) e un insegnante di matematica russo (Lobacevski) si provarono a spingere alle estreme conseguenze la negazione del quinto postulato; il primo non ammettendo nessuna parallela[5], ed il secondo ammettendone due. Ottennero, invece del paradosso in cui speravano, la geometria ellittica e iperbolica rispettivamente; si seppe poi che Gauss, il più insigne dei matematici allora viventi, aveva già trovato, con metodi differenziali, quei due risultati e molti altri; diciamo anzi che il non raggiungimento di paradossi da parte di Bolyai e Lobacevski non bastava affatto a dimostrare che le loro geometrie erano possibili; per fare questo occorreva una costruzione basata su enti di provata serietà, quali i numeri reali; è appunto ciò che il metodo di Gauss (o quello esposto in questo corso) riuscì ad ottenere.

[5]Non è vero che Bolyai non ammettesse nessuna parallela; sia lui che Lobacevski ne ammettevano due, e trovavano la geometria iperbolica (nota dell’Autore).

A

La versione del 1969/70

La dispensa trascritta nelle pagine precedenti è una sorta di "punto d'arrivo" dei tentativi compiuti da Barsotti –giunto a Padova nel 1968– per definire e delimitare i contenuti del corso di Geometria 2. Una prima versione fu la dispensa dell'Anno Accademico 1969/70, che circolò con varie aggiunte e correzioni. Quella dispensa conteneva 60 lezioni così suddivise:

parte I, *Complementi sugli spazi vettoriali*; lezz.1–12;
parte II, *Algebra Omologica*; lezz. 13–25;
parte III, *Spazio Proiettivo*; lezz. 26–37;
parte IV, *Matrici*; lezz 38–48;
parte V, *Quadriche*; lezz. 49–60.

Come si vede la gran parte degli argomenti è stata ripresa con modifiche e ampliamenti nella versione che abbiamo riportato, con l'esclusione dei contenuti della parte II a cui Barsotti ha dovuto rinunciare, credo per motivi di tempo, vista anche la riduzione operata nel numero delle lezioni. Riprodurre qui tutta la dispensa mi sembrerebbe uno scrupolo filologico degno di miglior causa; può essere invece interessante riproporre la sezione omessa per evidenziare anche in questo caso l'originalità e la abilità nella presentazione della materia che caratterizzano lo stile di Barsotti.

A.13 Lezione 13

Questo titolo (Algebra Omologica) descrive un metodo per maneggiare certe situazioni un po' complicate che si presentano spesso; il metodo in sé non costruisce nulla, ed è essenzialmente un linguaggio; solo i primissimi elementi vengono qui esposti. Premettiamo qualche definizione che fa parte di altre teorie (cfr. lezioni 33, 34, 37, 38 di [AA]). Sia A un anello, che supporremo sempre commutativo e dotato di identità; un A-modulo (sinistro) è un insieme M, con una operazione $+$ ($m + n \in M$ per $m, n \in M$), ed una operazione di prodotto scalare ($am \in M$ per $a \in A$ ed $m \in M$) soddisfacenti a tutti gli assiomi che dovrebbero venire soddisfatti se A fosse un corpo ed M uno spazio vettoriale su A; in effetti, se A è un corpo, un A-modulo è proprio uno spazio vettoriale. I nostri A-moduli si supporranno sempre *unitari*, ossia tali che $1m = m$ per $m \in M$ (1 è l'identità di A). Le definizioni di omomorfismi, isomorfismi, somma complementare, ecc., di A-moduli possono essere immaginate; valgono i tre teoremi di omomorfismo; si può anche immaginare cosa sia un insieme di generatori di un A-modulo. Negli A-moduli si può parlare di elementi linearmente dipendenti o indipendenti (su A), e si può parlare di combinazioni lineari; non è però più vero che se certi elementi sono linearmente dipendenti, uno di essi debba essere combinazione lineare degli altri; quindi non si può parlare di "base" o di "dimensione".

Un A-modulo generato da elementi indipendenti $x_1, x_2, \dots$ dicesi *libero* o *liberamente generato* dagli x_i, e gli x_i sono i suoi *generatori liberi* (il fatto di aver indicizzato gli x con gli interi non sta ad indicare che essi siano al più un'infinità numerabile). Un A-modulo generato da un numero finito di elementi dicesi *finitamente generato*, od anche *finito*; uno con un solo generatore dicesi *ciclico*; uno senza sotto-A-moduli propri $\neq \{0\}$ dicesi *semplice*; vale il teorema di Jordan-Hölder.

Nell'algebra omologica conviene spesso pensare ad un omomorfismo f di un A-modulo M in uno N come ad un ente che porta con sé i moduli di partenza e di arrivo; l'immagine fM sarà allora indicata con $\operatorname{im} f$; pertanto la restrizione di f da M ad $\operatorname{im} f = fM$ è un altro omomorfismo (se $\operatorname{im} f \subset N$), per esempio g; tale g è suriettivo, mentre f non lo era. Una successione (finita o no)

$$\dots M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \dots,$$

ove gli M_i sono A-moduli e gli f_i omomorfismi, dicesi *esatta* se per ogni i per il quale f_i ed f_{i+1} esistono si ha $\operatorname{im} f_i = \ker f_{i+1}$; per esempio, la

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

è esatta se, e solo se, f è iniettivo, g è suriettivo, e $P = N/M$ dopo opportune identificazioni.

A.14 Lezione 14

Premesso tutto questo, e premesso anche che spesso chiamemremo *freccia* un omomorfismo, si ha:

Lemma A.14.1. *Se nel diagramma*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & P \arrow[r] \arrow[d] & 0, \\
0 \arrow[r] & M' \arrow[r] & N' \arrow[r] & P' \arrow[r] & 0
\end{tikzcd}$$

in cui le successioni orizzontali sono esatte, manca la prima, o l'ultima, freccia verticale, ed il diagramma quadrato rimanente è commutativo, allora la freccia mancante può essere introdotta in modo unico se si richiede che tutto il diagramma ottenuto sia commutativo.

Dim. banale. C.V.D. □

Un A-modulo *graduato* è un modulo M che sia somma diretta di A-moduli M_i: $M = \cdots \oplus M_{i-1} \oplus M_i \oplus M_{i+1} \cdots$ (la somma può essere finita da una parte o da ambedue se ci si mettono degli zeri); gli elementi di M_i diconsi di *grado* i (talvolta di *dimensione* i). Un *omomorfismo di grado* r dell'A-modulo graduato M sull' M' è un omomorfismo f che mandi M_i su M'_{r+i}; la restrizione di f ad M_i si usa indicare con f_i.

Un *complesso* (o A-complesso) è un A-modulo graduato M, dotato di un endomorfismo d di grado 1 (o -1), tale che $dd = 0$, ossia tale che $\operatorname{im} d_{i-1} \subseteq \ker d_i$:

$$\cdots \longrightarrow M_{i-1} \xrightarrow{d_{i-1}} M_i \xrightarrow{d_i} M_{i+1} \longrightarrow \cdots .$$

Vi è una nomenclatura psicologica legata ai complessi: spesso se le frecce si scrivono con la punta a destra (ossia se d ha grado 1) si parla di "coomologia", e se con la punta a sinistra (ossia se d ha grado -1) di "omologia"; di fatto, se si fa una teoria e poi la si dualizza, si premette un "co" a tutte le parole, o si toglie se c'era già; si usano anche scrivere gli indici in alto quando c'è il "co", e in basso quando non c'è; non sempre useremo queste convenzioni.

Gli elementi di M_i diconsi le *catene* (*cocatene*) di dimensione i; i d_i sono gli operatori di *bordo* o *contorno* (*cobordo* o *cocontorno*), od anche le *differenziazioni* (*codifferenziazioni*). Se gli M_i sono liberi; e in ognuno è fissato un insieme di generatori liberi, questi si chiamano talvolta le *celle* o *simplessi* di dimensione i. Si pone $Z_i(M) = \ker d_i \subseteq M_i$, ed i suoi elementi si chiamano i *cicli* (*cocicli*) di dimensione i; si pone anche $B_i(M) = \operatorname{im} d_{i-1} \subseteq M_i$, e i suoi elementi si chiamano i *bordi* (*cobordi*) di dimensione i. L'A-modulo $Z_i/B_i = H_i(M)$ è l'i-*esimo gruppo di omologia* (*coomologia*). Sono quindi esatte la riga e la colonna del seguente diagramma, dove d_B è la restrizione di d da M a B.

$$\begin{tikzcd}
 & 0 \arrow[d] & & & \\
 & B_i \arrow[d] & & & \\
0 \arrow[r] & Z_i \arrow[r] \arrow[d] & M_i \arrow[r, "d_B"] & B_{i+1} \arrow[r] & 0 \\
 & H_i \arrow[d] & & & \\
 & 0 & & &
\end{tikzcd} .$$

La somma diretta degli H_i è un A-modulo graduato che si indica con $H(M)$ e si chiama l'*omologia* (*coomologia*) di M:

$$
\begin{tikzcd}
 & 0 \arrow[d] & & & \\
 & B \arrow[d] & & & \\
0 \arrow[r] & Z \arrow[r] \arrow[d] & M \arrow[r, "d_B"] & B \arrow[r] & 0 \\
 & H \arrow[d] & & & \\
 & 0 & & &
\end{tikzcd}
\quad \text{(riga e colonna esatte).}
$$

Se in una teoria si usano sia delle omologie, con indice in basso, che delle coomologie, con indice in alto, l'H omologico si indica con H_*, quello coomologico con H^*.

Un *omomorfismo* g *di grado* r di un complesso M su uno M' è un omomorfismo siffatto di moduli graduati che renda commutativo il diagramma

(A.14.2)
$$
\begin{tikzcd}
M \arrow[r, "d"] \arrow[d, "g"'] & M \arrow[d, "g"] \\
M' \arrow[r, "d'"'] & M'
\end{tikzcd}
$$

Per mezzo di essi si definiscono i *sottocomplessi* (bisogna che $0 \longrightarrow M \xrightarrow{g} M'$ sia esatta), e le *immagini* (bisogna che $M \xrightarrow{g} M' \longrightarrow 0$ sia esatta); notare che 0 è il complesso con $M_i = 0$ per ogni i.

A.15 Lezione 15

L'operatore H fa passare dai complessi agli A-moduli graduati; esso è "funtoriale", nel senso che fa anche passare dagli omomorfismo fra complessi agli omomorfismi fra A-moduli graduati, come ora spieghiamo: abbiasi l'omomorfismo $M \xrightarrow{g} M'$, e consideriamo il diagramma

(A.15.1)
$$
\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d, "g_B"] & Z \arrow[r] \arrow[d, "g_Z"] & H \arrow[r] \arrow[d, "g_H"] & 0 \\
0 \arrow[r] & B' \arrow[r] & Z' \arrow[r] & H' \arrow[r] & 0
\end{tikzcd}
,
$$

ove il g_H a priori manca; qui, g_B è la restrizione di g a B, che esiste per la commutatività di (A.14.2), e g_Z quella di g a Z. Poiché le righe sono esatte, il g_H esiste per (A.14.1) se si vuole che il diagramma resti commutativo (lo è senza il g_H); questo g_H è appunto l'omomorfismo di H su H' che corrisponde al g di M su M'.

Teorema A.15.2 (fondamentale dell'omologia)**.** *Sia*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

una successione esatta, con M*,* M'*,* M''*, complessi, ed* f, g *di grado* 0*; se allora* σ *è l'omomorfismo canonico di* Z *su* H*, esiste l'omomorfismo* $h = \sigma' f_Z^{-1} d g_Z^{-1} \sigma''^{-1}$ *di* H'' *in* H'*, ed esso ha grado* 1 *e rende esatta la successione*

$$\begin{tikzcd} H' \arrow[r, "f_H"] & H \arrow[d, "g_H"] \\ & H'' \arrow[ul, "h"] \end{tikzcd} \quad .$$

Dim. Se $z'' \in Z''$, sia $y \in g^{-1}z'' \in M$, determinato a meno di elementi in $\ker g = \operatorname{im} f$; inoltre $d''gy = d''z = 0$, onde $gdy = 0$, e $dy \in \ker g = \operatorname{im} f$, determinato a meno di elementi di $d(\operatorname{im} f) = fB'$. Esiste uno $z' \in M'$ tale che $fz' = dy$, ed è determinato a meno di elementi di B', ed anzi, $fd'z' = dfz' = ddy = 0$, sicché $z' \in Z'$. L'immagine di z' in H' è ora univocamente determinata, e si è così definito un omomorfismo h^* di Z'' in H', di grado 1. Si può così scrivere il seguente diagramma commutativo a righe esatte (ove h è stato aggiunto a norma del (A.14.1), e ι è l'identità):

$$\begin{tikzcd} 0 \arrow[r] & B'' \arrow[r] \arrow[d] & Z'' \arrow[r] \arrow[d, "h^*"] & H'' \arrow[r] \arrow[d, "h"] & 0 \\ 0 \arrow[r] & 0 \arrow[r] & H' \arrow[r, "\iota"'] & H' \arrow[r] & 0 \end{tikzcd}$$

che ci dà la costruzione di h.

Ora per l'esattezza del diagramma dell'enunciato:

1. È $g_H f_H = \sigma'' g_Z \sigma^{-1} \sigma f_Z \sigma'^{-1} = \sigma'' g_Z f_Z \sigma'^{-1}$, per (A.15.1); questo è 0 perché $g_Z f_Z = 0$; quindi $\operatorname{im} f_H \subseteq \ker g_H$. Poi, se $\sigma x \in \ker g_H$, con $x \in Z$, deve essere $\sigma'' g_Z x = g_H \sigma x = 0$, $g_Z x \in B'' = gB$, $x \in Z \cap [B + fM'] = Z \cap fM' = fZ'$, onde $\sigma x \in \sigma f Z' = f_H \sigma' Z' = \operatorname{im} f_H$.
2. È $h g_H = \sigma' f_Z^{-1} d g_Z^{-1} \sigma''^{-1} \sigma'' g_Z \sigma^{-1} = \sigma' f_Z^{-1} d \sigma^{-1} = 0$ perché $d\sigma^{-1} = 0$; perciò $\operatorname{im} g_H \subseteq \ker h$. Poi se $\sigma'' gx \in \ker h$, con $x \in g^{-1}Z''$, si deve avere $\sigma' f^{-1} dx = \{0\}$, $f^{-1}dx \subseteq B'$, $dx \in fB' = fd'M' = dfM'$, $x \in fM' + Z$, $gx \in gZ$, $\sigma gx \in \sigma g Z = g_H H = \operatorname{im} g_H$.

3. È $f_H h = \sigma f_Z \sigma'^{-1}\sigma' f_Z^{-1} d g_Z^{-1} \sigma''^{-1} = \sigma d g_Z^{-1} \sigma''^{-1} = 0$ perché quindi $\operatorname{im} h \subseteq \ker f_H$. Se poi $\sigma' x \in \ker f_H$, con $x \in Z'$, si avrà $\sigma f x = 0$, $f x \in B$, $x \in f^{-1}[dM \cap fZ']$. Consideriamo un $y \in M$ tale che $dy \in fZ'$; per un tale y è $d'' g y = g d y = 0$, onde $g y \in Z''$, $y \in g^{-1} Z''$; pertanto $x \in f^{-1} d g^{-1} Z''$, e $\sigma' x \in \sigma' f^{-1} d g^{-1} \sigma''^{-1} H'' = \operatorname{im} H$.

C.V.D. □

A.16 Lezione 16

Per parecchi moduli è definita un'applicazione ord, dei moduli stessi sugli interi, o in generale su un gruppo abeliano Γ, che soddisfa la condizione seguente: se $0 \to M \to N \to P \to 0$ è esatta, $\operatorname{ord} N$ esiste se, e solo se, esistono $\operatorname{ord} M$ ed $\operatorname{ord} P$; e si ha inoltre $\operatorname{ord} N = \operatorname{ord} M + \operatorname{ord} P$. Esempi sono l'ordine di un gruppo finito abeliano (che è un A-modulo con $A =$ anello degli interi); la dimensione di uno spazio vettoriale di dimensione finita.

Bene, se M è un complesso, e se vi è un'applicazione "ord" per i suoi H_i, e se inoltre gli H_i sono *quasi tutti* 0 (ossia tutti eccetto al più un numero finito), l'elemento di Γ dato da

$$\chi(M) = \sum_i (-1)^i \operatorname{ord} H_i \tag{A.16.1}$$

si chiama la *caratteristica di Eulero-Poincaré* di M; l'$\operatorname{ord} H_i$ è l'i-esimo *numero di Betti* di M.

Teorema A.16.2. *Nelle notazioni precedenti, se* $\operatorname{ord} M_i$ *esiste per ogni* i*, se è nullo per quasi tutti gli* i*, e se* $H_i = 0$ *per quasi tutti gli* i*, si ha* $\chi(M) = \sum_i (-1)^i \operatorname{ord} M_i$.

Dim. L'esattezza di $0 \to Z_i \to M_i \to B_{i+1} \to 0$ dice che esistono $\operatorname{ord} Z_i$ ed $\operatorname{ord} B_{i+1}$, e che $\operatorname{ord} M_i = \operatorname{ord} Z_i + \operatorname{ord} B_{i+1}$. Poi, l'esattezza di $0 \to B_i \to Z_i \to H_i \to 0$ dice che $\operatorname{ord} H_i$ esiste, e che $\operatorname{ord} Z_i = \operatorname{ord} B_i + \operatorname{ord} H_i$. In conclusione, $\operatorname{ord} M_i = \operatorname{ord} B_i + \operatorname{ord} H_i + \operatorname{ord} B_{i+1}$; moltiplicando per $(-1)^i$ e sommando si ha il risultato. C.V.D. □

A.17 Lezione 17

Possiamo subito dare un esempio, semplice ma fondamentale, di quanto precede; basta munirsi di un anello A e di un insieme finito F; occorre però prima una definizione: fra gli ordinamenti di F può porsi una relazione di equivalenza col definire $\alpha \sim \beta$ se, e solo se, la permutazione che cambia α in β è pari, ossia di segnatura 1 (cfr. lezione 45 di [AA]). Le due classi in cui questa equivalenza ripartisce F si dicono gli *orientamenti* di F, ed F con un orientamento è un *insieme orientato*. Da notare che un orientamento di F non definisce (a differenza degli ordinamenti) degli orientamenti nei sottoinsiemi: gli ordinamenti (a, b, c),

(b, c, a) di $\{a, b, c\}$ appartengono allo stesso orientamento, ma inducono in $\{a, c\}$ ordinamenti appartenenti a orientamenti diversi. Per $i = 0$ ed $i = 1$ la definizione cade; diremo che $\varnothing$ non ha orientamenti, e che gli insiemi di cardinalità 1 hanno un solo orientamento. Dati allora A ed F, cominciamo con l'ordinare F, e consideriamo l'A-modulo M'_i i cui generatori liberi sono i sottoinsiemi ordinati di F di cardinalità $i + 1$; questo per $i = 0, 1, \ldots, n$ se $n + 1 = \operatorname{card} F$; poniamo anche $M'_i = \{0\}$ per gli altri valori di i. Posto $M' = \bigoplus_i M'_i$, M' diviene un complesso col definire il bordo d_* (di grado -1) così:

$$d'_*(s_0, \ldots, s_i) = \sum_j (-1)^j (s_0, \ldots, \widehat{s_j}, \ldots, s_i),$$

ove il cappuccio su s_j significa che s_j va saltato (si verifichi che $d'_* d'_* = 0$). Non è però questo il complesso che ci interessa; se indichiamo con $(s_0, \ldots, s_i)$ non l'insieme ordinato, ma quello orientato (secondo l'orientamento cui quell'ordinamento appartiene), e se inoltre identifichiamo $(s_1, s_0, \ldots, s_i)$ con $-(s_0, \ldots, s_i)$, quando $i \geq 1$, in luogo di M'_*, d'_* otteniamo gli M_*, d_*; verificare che il d_* è ben definito dalla stessa formula[1], ossia dalla

(A.17.1) $$d_*(s_0, \ldots, s_i) = \sum_j (-1)^j (s_0, \ldots, \widehat{s_j}, \ldots, s_i).$$

Gli $(s_0, \ldots, s_i)$ orientati (con ciascuno dei due orientamenti, ossia i $\pm(s_0, \ldots, s_i)$ se $i > 0$) sono i *simplessi* del complesso costruito (detto talvolta *complesso simpliciale discendente* di F).

Facciamo un altro giochetto: sia M^i l'A-modulo delle applicazioni alternanti di $S \times \cdots \times S$ ($i + 1$ fattori) su A (ed $M^i = 0$ se $i < 0$); una ϕ dicesi *alternante* se cambia segno quando si scambiano fra loro due argomenti, e se inoltre vale 0 quando due argomenti coincidono (questo va detto per il caso della caratteristica 2); se $i = 0$ ogni ϕ si considera alternante. Questo M^i non è altro che $\mathrm{Hom}_A(M_i, A)$, e ne è il *duale* secondo una definizione di dualità fra A-moduli perfettamente analoga a quella per spazi vettoriali (cfr. lezione 42 di [AA]); anzi, essendo i moduli in questione liberi e finiti, resta anche vero (esercizio!) che il duale di M^i è M_i. Posto $M^* = \bigoplus_i M^i$, il $M_* \xrightarrow{d_*} M_*$ ha un duale $M^* \xleftarrow[d^*]{} M^*$ dato da $d^* x \circ y = x \circ d_* y$ ($x \in M^*$, $y \in M_*$; "$\circ$" è l'operazione di dualità), ossia da:

(A.17.2) $$(d^*\phi)(s_0, \ldots, s_i) = \sum_j (-1)^j \phi(s_0, \ldots, \widehat{s_j}, \ldots, s_i).$$

Questo d^* è un operatore di cobordo di grado 1, ed M^* è un complesso, *duale* di M, detto *complesso simpliciale ascendente* di F; i *simplessi* di M^i sono i ϕ che mandano un $(s_0, \ldots, s_i)$ su 1 e tutti gli altri, escluso $-(s_0, \ldots, s_i)$, su 0.

[1] [Nota dell'Autore]: tutto questo si può dire più ampollosamente ma meno chiaramente se si vuole evitare l'uso della parola imprecisa "identificare"; provarcisi per esercizio

Le definizioni precedenti possono essere messe in altra luce sfruttando i prodotti esterni; questi sono stati definiti solo per gli spazi vettoriali, ma è chiaro che le loro prime proprietà valgono anche per gli A-moduli liberi finiti. L'insieme orientato $(s_0, \ldots, s_i)$ non è altro che il prodotto esterno $s_0 \wedge \cdots \wedge s_i$ di elementi di M_0; insomma, $M_i = M_0 \wedge \cdots \wedge M_0$, $i+1$ volte; se $F = (x_0, \ldots, x_n)$, orientato, la base duale, in M^0, della $\{x_0, \ldots, x_n\}$, è data dagli $x^0, \ldots, x^n$ tali che $x^i \circ x_j = \delta_{ij}$ (scriviamo $x^i \circ x_j$ in luogo di $x^i x_j$); ed allora $M^i = M^0 \wedge \cdots \wedge M^0$ ($i+1$ volte), con la dualità $(s^0 \wedge \cdots \wedge s^i) \circ (t_0 \wedge \cdots \wedge t_i) = (s^0 \wedge \cdots \wedge s^i)(t_0, \ldots, t_i)$ (cfr. l'analogo 1.5.7). Posto $y^* = x^0 + \cdots + x^n \in M^0$, la (A.17.2) diviene

A.17.3. *Per $x^* \in M^*$, si ha $d^* x^* = y^* \wedge x^*$.*

La (A.17.1) non si presta ad interpretazione altrettanto semplice senza introdurre nuovi concetti. Comunque la (A.17.3) ci permette di trovare subito la coomologia di M^*; infatti, scegliamo intanto come insieme di generatori liberi di M^0 gli elementi $y^*, x_1^*, \ldots x_n^*$ (il che è possibile); allora:

Z^0 è liberamente generato da y^*, $B^0 = \{0\}$ onde $H^0 \cong Z^0$;
Z^i (per $0 < i \leq n$) è liberamente generato dagli $y^* \wedge x_{\sigma_1}^* \wedge \cdots \wedge x_{\sigma_i}^*$ con $(\sigma_1, \ldots, \sigma_i)$ sottoinsieme ordinato di $(1, \ldots, n)$, $B^i = Z^i$, onde $H^i = \{0\}$.

Dualizziamo (è possibile in questo caso particolare):

$Z_0 = M_0$, $B_0 =$(ortogonale di y^* in M_0) $=$ modulo liberamente generato da $x_1, \ldots, x_n$, onde $H_0 \cong A$;
$Z_i =$(ortogonale di B^i in M_i) è liberamente generato dagli $x_{\tau_1} \wedge \cdots \wedge x_{\tau_i}$ per $0 < i < n$, $B_i = Z_i$, onde $H_i = \{0\}$. $Z_n = \{0\}$, $B_n = \{0\}$, onde $H_n = \{0\}$.

Vediamo che cos'è la caratteristica di Eulero-Poincaré di M^* ed M_*; intanto occorre una funzione "ord" valida per gli M_i, Z_i, B_i, H_i; ora, in generale una tale funzione non c'è; ma se, come in questo caso, i moduli sono tutti liberi finiti, e inoltre si richiede la validità della $\operatorname{ord} N = \operatorname{ord} M + \operatorname{ord} P$ solo per quelle $0 \to M \to N \to P \to 0$ esatte per le quali $N = M \oplus P$ (ed è così in questo caso), si può prendere $\operatorname{ord} M =$ numero dei suoi generatori liberi. Allora si vede subito, per (A.16.1), che

$$\chi(M_*) = \chi(M^*) = 1. \tag{A.17.4}$$

Controlliamo il (A.16.2): si dovrebbe avere

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

e infatti la somma è $1 - (1-1)^{n+1} = 1$.

A.18 Lezione 18

Quanto esposto nella Lezione 17 è, sì, un'applicazione della omologia, ma in sé può sembrare un gioco complicato su enti piuttosdto semplici, gli insiemi finiti. La sua vera applicazione è quella che segue, che è poi quella che ha originato tutta la teoria. Si dovrebbe cominciare con uno spazio affine, ma siccome non ne abbiamo ancora parlato prenderemo uno spazio vettoriale V di dimensione $n+1$ sui reali $\mathbb{R}$; se $v_0, \ldots, v_i$ sono suoi elementi linearmente indipendenti (onde $i \leq n$), chiameremo *simplesso* in V (di dimensione i), con *scheletro* $\{v_0, \ldots, v_i\}$, quello che in uno spazio affine sarebbe l'$(i+1)$-edro di vertici $v_0, \ldots, v_i$ e che qui definiamo così: il simplesso è l'insieme

$$\{\, x \mid x \in V, x = \alpha_0 v_0 + \cdots + \alpha_i v_i, \alpha_j \in \mathbb{R}, \alpha_j > 0, \alpha_0 + \cdots + \alpha_i = 1 \,\}\,;$$

invece, un *simplesso orientato* sarà l'insieme di un simplesso e di un orientamento del suo scheletro. Le *facce* del simplesso sono i simplessi il cui scheletro è sottoinsieme non vuoto dello scheletro del simplesso (ivi compreso il simplesso stesso ed i suoi *vertici*).

Pongasi in V una norma ellittica definita positiva (cfr. lezione 14); l'applicazione $v \mapsto \sqrt{v \circ v}$ (≥ 0) diviene una metrica in V nel senso della topologia, che rende V omeomorfo a $\mathbb{R} \times \cdots \times \mathbb{R}$ ($n+1$ fattori; prodotto topologico; $\mathbb{R}$ con la solita topologia). In tal caso si vede subito che la chiusura di un simplesso non è altro che l'unione di tutte le sue facce.

Sia allora S uno spazio topologico; diremo *cella di dimensione* i di S l'ente costituito da:

1. L'immagine omeomorfa E' di un simplesso E di dimensione i (di qualche V di dimensione $\geq i+1$), in un omeomorfismo α di $\bar{E}$ (chiusura di E) su S;
2. L'insieme delle α-immagini dei vertici di E, detto lo *scheletro* della cella;

notare che la cella non è l'unione di 1 e 2, ma è l'insieme di 1 e 2; spesso chiameremo "cella" semplicemente l'aperto descritto in 1.

Una *triangolazione* K su S è un insieme finito di celle $E''_j = (E'_j, \text{scheletro})$ tale che gli E'_j siano a 2 a 2 disgiunti, e che se una cella appartiene a K, anche ogni sua faccia vi appartenga. Se K è una triangolazione, l'unione degli scheletri delle sue celle E''_j è una unione di simplessi nel senso della lezione 17 (di questa appendice); si può costruire l'A-modulo libero K_* che li ha per generatori liberi, e tale K_* diviene un complesso nel senso della lezione 14 (sempre di questa appendice) per mezzo del d_* di (A.17.1); analogamente si definisce il K^* col (A.17.2); essi danno (mediante gli H_* ed H^*) l'*omologia* e *coomologia* di K; se K *copre* tutto S, ossia se S è l'unione degli E'_j, l'omologia e la coomologia di K sono ovviamente degli invarianti per omeomorfismo di S; se capita che questi invarianti siano indipendenti dalla scelta della triangolazione, ovvero indipendenti da tale scelta purché la triangolazione soddisfi a certe condizioni topologiche, allora tali invarianti sono invarianti topologici di S, e l'omologia e coomologia sono l'*omologia* e *coomologia* di S.

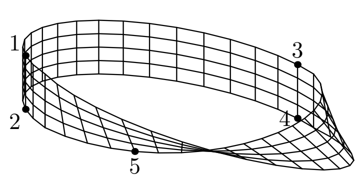
Vediamo qualche caso in cui ciò accade; ci limitiamo al caso delle triangolazioni "di dimensione pura", "fortemente connesse", e "poliedrali", dette anche *poliedri*. Definizioni: *di dimensione pura* $n > 0$ vuol dire che esiste un n tale che ogni cella sia faccia di una cella di dimensione n; *poliedrale* vuol dire che intanto ogni cella di dimensione $n-1$ è faccia di al più due celle di dimensione n. e poi che se due celle E, F di dimensione n hanno a comune una faccia, allora quella faccia è faccia di una faccia comune di dimensione $n-1$ (in tal caso le E, F sono *adiacenti*); *fortemente connesso* vuol dire che se E, F sono due celle di dimensione n, esistono celle $E_1 = E, E_2, \ldots, E_r = F$ tali che, per $i = 1, \ldots, r-1$, le E_i, E_{i+1} abbiano a comune una faccia (certo di dimensione $n-1$ se poliedrale). Se K indica un poliedro, K_* indicherà il complesso (su qualche anello che va specificato) in cui K_i è liberamente generato dagli scheletri orientati delle celle di dimensione i di K; invece K^* ne indicherà il duale.

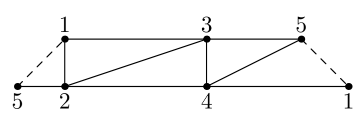
Intanto, un poliedro è *orientabile* se le varie celle n-dimensionali che lo formano sono orientabili in modo che per due celle adiacenti $(s_0, s_1, \ldots, s_n)$, $(s'_0, s_1, \ldots, s_n)$, le orientazioni scritte siano l'una quella scelta e l'altra no; invece la *frontiera* è la triangolazione formata da quelle facce di dimensione $n-1$ che sono facce di una sola cella n-dimensionale, e dalle loro facce (le altre celle $(n-1)$-dimensionali sono facce di esattamente 2 celle n-dimensionali). Si ha il risultato seguente, la cui facile dimostrazione si lascia come esercizio:

Teorema A.18.1. *Sia A anello di caratteristica diversa da 2. Un poliedro K di dimensione $n > 0$, senza frontiera, è orientabile se, e solo se, il suo gruppo di omologia H_n è isomorfo ad A; è non orientabile se, e solo se, $H_n = \{0\}$. Se invece vi è frontiera F non vuota, e se M_*, N_* sono i complessi su A di K, F rispettivamente, i risultati precedenti valgono per l'H_n di M_*/N_*. Per il (A.15.2) si può anche dire: se F è la frontiera di K, K è orientabile se, e solo se: $H_n(K) = \{0\}$, e inoltre $Z_{n-1}(F) \cap B_{n-1}(K) = \{0\}$.*

A.19 Lezione 19

La striscia di Moebius: È il poliedro di dimensione 2 le cui celle sono (dando numeri anziché nomi ai vertici) 123, 234, 345, 145, 125 (vedi figura):

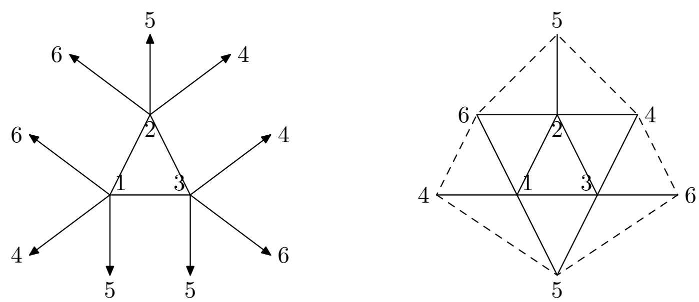




Frontiera: 13, 24, 35, 14, 25, che è poliedro di dimensione 1.

Cerchiamo lo Z_2 di Moebius/frontiera; i bordi dei 5 generatori scritti di Moebius, modulo frontiera, sono $(2,3) + (1,2)$, $(3,4) + (2,3)$, $(4,5) + (3,4)$, $(4,5) - (1,5)$, $(1,2) - (1,5)$; se A non ha caratteristica 2, nessuna combinazione lineare di questi è 0; quindi $Z_2 = H_2 = \{0\}$, e Moebius non è orientabile.

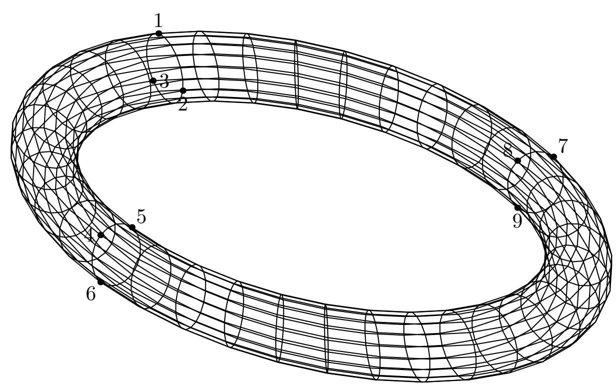
Il piano proiettivo reale: Una sua triangolazione è la seguente



ove i vertici con freccia sono sulla retta impropria[2]; ecco le celle: 123, 135, 234, 126, 256, 245, 346, 356, 145, 146. Frontiera vuota; $Z_2 = \{0\}$ (facile); quindi non orientabile.

La sfera: È la superficie di un tetraedro: 123, 134, 124, 234; frontiera vuota; $Z_2 \neq \{0\}$, e la sfera è orientabile.

Il toro: È fatto così (camera d'aria):



una triangolazione è 128, 278, 279, 239, 139, 189, 578, 457, 467, 679, 569, 589, 124, 145, 156, 136, 236, 246. Controllare che è senza frontiera, orientabile.

L'otre di Klein: Può essere realizzato nello spazio di dimensione 4; in quello tridimensionale ci si deve contentare di farne un modello che interseca se stesso, contro la definizione di complesso; è un fiasco il cui collo si piega, entra all'interno da un lato (e questa intersezione non conta), e si salda a un buco in fondo;

[2]Abbiamo aggiunto a fianco un'altra rappresentazione della stessa triangolazione, ove la retta impropria compare tratteggiata perché, come nel caso del nastro di Moebius, i lati con vertici omonimi vanno identificati. [NdR]

per triangolarlo basta tagliare il toro con un taglio in 123, e riincollarlo in modo che l'123 su un moncone vada a combaciare con l'132 sull'altro; ecco perciò la triangolazione: 128, 278, 279, 239, 139, 189, 578, 457, 467, 679, 569, 589, 134, 145, 156, 126, 236, 346. Frontiera vuota, non orientabile.

A.20 Lezione 20

Prendiamo per A il corpo razionale; allora tutti gli A-moduli finiti sono spazi vettoriali, e la loro dimensione funge da funzione "ord" (lezione 16); esiste perciò la caratteristica di Eulero-Poincaré, ed esistono i numeri di Betti. Premesso che chiamiamo *superficie chiusa* l'unione di tutte le celle di un poliedro di dimensione 2 senza frontiera, vale il seguente risultato fondamentale (la cui dimostrazione non diamo, ma metà della quale, e cioè il "solo se", è facile e può essere fatta come esercizio):

Teorema A.20.1. *Due superficie sono omeomorfe se, e solo se, scelti dei poliedri K, K' che le ricoprano, essi sono intanto o ambedue orientabili o ambedue non orientabili, e se inoltre le caratteristiche di Eulero-Poincaré di K_*, K'_* sul corpo razionale coincidono.*

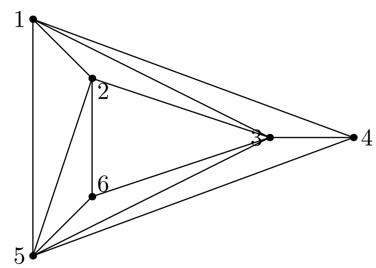
Si hanno anche i seguenti fatti che diamo per informazione e senza dimostrazione: per una superficie non orientabile, la caratteristica χ di Eulero-Poincaré può assumere i valori $1, 0, -1, -2, \ldots$; per una orientabile i valori $2, 0, -2, -4, \ldots$; posto allora $\chi = 1-p$ per le prime, e $\chi = 2-2p$ per le seconde, l'intero p può assumere i valori $0, 1, 2, \ldots$, e si chiama il *genere* della superficie. Inoltre, il numero $2 - \chi$, che coincide con $p + 1$ per le non orientabili, o con $2p$ per le orientabili, è l'*ordine di connessione* della superficie, e coincide con il massimo intero h tale che si possano fare sulla superficie h "tagli" senza "rompere la connessione", ossia senza che essa divenga un insieme sconnesso. E infine, la superficie campione orientabile di genere p è la *sfera con p manichi*[3], e cioè una sfera nella quale si siano fatti $2p$ buchi circolari, ogni coppia dei quali viene congiunta con un "manico". Invece la superficie campione non orientabile di genere p è una "*sfera con p striscie di Moebius*", ossia una sfera con p buchi circolari, i quali sono saldati alle frontiere di altrettante striscie di Moebius (notare che la frontiera di una striscia di Moebius è omeomorfa ad un circolo). Per esempio:

Il toro è omeomorfo a una sfera con 1 manico;
L'otre di Klein è omeomorfo a una sfera con 2 striscie di Moebius;
Il piano proiettivo è omeomorfo ad una sfera con 1 striscia di Moebius.

Vi è poi un altro risultato inteessante, che siamo perfettamente in grado di dimostrare; consideriamo un poliedro di dimensione n, senza frontiera, che sia immerso in uno spazio vettoriale (o affine) di dimensione $> n$, e le cui celle siano proprio simplessi nel senso della lezione 18, e non loro immagini omeomorfe (per

[3] letterale. [NdR]

$n = 2$, un solito poliedro della geometria elementare se lo spazio ha dimensione 3; per $n = 1$ un poligono, piano o gobbo). Ragioniamo per $n = 2$ per semplicità: se prendiamo un piano che contenga una cella di dimensione 2, tutte le celle di dimensione 2 di quel poliedro, appartenenti a quel piano, formano un numero finito di poliedri; se in uno di questi cancelliamo dalla lista delle celle di dimensione 1 (segmenti) una tale cella a che appartenga a 2 celle di dimensione 2 (adiacenti) b, c, il numero delle celle di dimensione 1 diminuisce di 1; se però nel contempo le due celle adiacenti le riuniamo, e chiamiamo "cella di dimensione 2" l'unione $b \cup a \cup c$, anche il numero complessivo di celle di dimensione 2 diminuisce di 1. Quindi le nuove "celle" di dimensione 1 non sono più dei simplessi, ma sono a loro volta gli interni di poliedri piani; il giochetto può continuare finché non ci si imbatta in una a la distruzione della quale non fa diminuire di uno il numero delle celle di dimensione 2;



nel disegno le celle di dimensione 2 siano le 123, 134, 125, 256, 356, 345; possiamo distruggere 13, 25, 35, 12, 34, ma non 56, perché così facendo non diminuirebbe il numero delle nuove "celle" di dimensione 2. Fatto questo sulle celle di dimensione 1, lo ripetiamo su quelle di dimensione 0 che risultino su una stessa retta. Alla fine il nostro poliedro risulta fatto di "facce" ciascuna delle quali è una unione di celle nel senso iniziale della parola; le operazioni fatte non hanno alterato la somma a secondo membro nel (A.16.2), e ovviamente quella a primo membro è ancora $\chi(M)$ (per A corpo razionale). Se allora il numero delle "facce" di dimensione i è indicato con F_i, si ha

(A.20.2) $$\chi = \sum_i (-1)^i F_i,$$

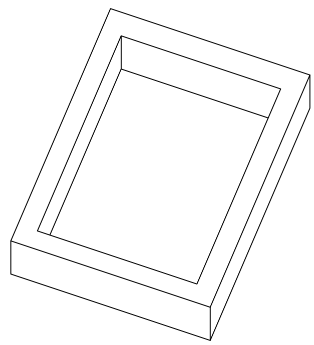
che è una famosa formula di Eulero.

Esempi:

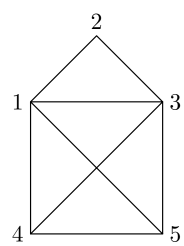
- *Tetraedro* (quattro triangoli equilateri); $\chi = 2$, per (A.20.1) (omeomorfo alla sfera); $F_2 = 4$, $F_1 = 6$, $F_0 = 4$; e infatti $4 - 6 + 4 = 2$.
- *Cubo* (esaedro; 6 quadrati); $\chi = 2$; $F_2 = 6$, $F_1 = 12$, $F_0 = 8$; e infatti $6 - 12 + 8 = 2$.
- *Dodecaedro* (12 pentagoni regolari); $\chi = 2$; $F_2 = 12$, $F_1 = 30$, $F_0 = 20$; e infatti $12 - 30 + 20 = 2$.
- *Ottaedro* (8 triangoli equilateri); $\chi = 2$; $F_2 = 8$, $F_1 = 12$, $F_0 = 6$; e infatti $8 - 12 + 6 = 2$.

- *Icosaedro* (20 triangoli equilateri); $\chi = 2$; $F_2 = 20$, $F_1 = 30$, $F_0 = 12$; e infatti $20 - 30 + 12 = 2$.

Questi sono tutti i *poliedri regolari*; perché non ce ne possono essere altri?
La cornice (vedi figura); $\chi = 0$ (omeomorfa al toro);



$F_2 = 12$, $F_1 = 28$, $F_0 = 16$; e infatti $12 - 28 + 16 = 0$.
Altri giochetti. Si può fare la casetta senza mai alzare la matita e senza tornare indietro?



Questa non è un poliedro (3 celle di dimensione 1 hanno una faccia comune); però il poter fare quello che si è detto è molto simile all'"orientare"; significa attribuire ai simplessi di dimensione 1 il coefficiente 1 o -1, in modo che il bordo della somma ottenuta sia del tipo $a - b$ (b partenza, a arrivo). Osservato che il bordo di una tale somma non potrà mai essere $a+b$, si vede che, se il problema è risolubile, deve accadere che, preso per A il corpo di cardinalità 2, il bordo della somma di tutti i simplessi di dimensione 1 sia un $a + b$. Ma $d_*(p, q) = p + q$, cosicché il bordo in questione è la somma di quei vertici in cui s'incontra un numero dispari di segmenti; quindi se il giochetto è risolubile di tali vertici ce ne sono o nessuno o due (come in questo caso). Si controlli che la condizione è anche sufficiente (supponendo che l'insieme sia connesso, s'intende).

Avvertenza. La Lezione 17 (di questa appendice) descrive certi complessi basati su simplessi che sono semplicemente insiemi finiti; le 18, 19, 20 ne danno un'applicazione topologica, ove quegli insiemi vengono interpretati come punti di uno spazio topologico. Questo è il modo in cui la topologia è nata [questa parte della topologia si è chiamata "analysis situs" prima e "topologia combinatoria" poi; ora si chiama “topologia algebrica”]. È però bene avvertire che ad iniziare dal 1932, per poter trattare spazi topologici completamente slegati dai numeri reali si è adottato un metodo diverso: gli insiemi finiti usati per i simplessi sono non più insiemi di punti, ma insiemi di aperti di uno spazio; la trattazione è meno visuale, ma più semplice e più generale. Non ne parliamo.

A.21 Lezione 21

Per dare un'altra applicazione dell'algebra omologica dobbiamo introdurre alcuni nuovi concetti. Sia A un anello (commutativo con identità); una *derivazione* D *di* A è un'applicazione di A in sé (e in teorie più minuziose anche di A in qualcos'altro), tale che $D(x+y) = Dx + Dy$, $D(xy) = xDy + yDx$. Se ne deduce subito $D0 = 0$, $D(x-y) = Dx - Dy$, e $D1 = D(-1) = 0$. L'insieme delle derivazioni di A è un A-modulo se si definisce xD mediante la $(xD)y = x(Dy)$.

Lemma A.21.1. *Se A è campo d'integrità con corpo quoziente C, e se D è derivazione di A, esiste un'unica derivazione di C che induce D in A.*

Dim. Basta porre $D(\frac{x}{y}) = \frac{Dx}{y} - \frac{xDy}{y^2}$; questa è l'unica perché $0 = D1 = D(y\frac{1}{y}) = yD(\frac{1}{y}) + \frac{1}{y}Dy$. C.V.D. □

Un $a \in A$ tale che $Da = 0$ è una *costante* rispetto a D; le costanti rispetto a D formano un sottoanello A_0 di A contenente il sottoanello fondamentale, e formano un sottocorpo se A è corpo; la D è A_0-lineare, ossia $D(ax) = aDx$ per $a \in A_0$. Certe volte conviene parlare solo delle D il cui anello delle costanti contiene un dato anello B, ossia delle D che inducono in B la derivazione 0 (o *banale*); esse saranno chiamate le derivazioni *di* A *su* B.

Lemma A.21.2. *Sia A un campo d'integrità, e siano $x_1, \dots, x_n$ indeterminate su A; allora esistono, e sono uniche, le derivazioni $D_1, \dots, D_n$ di $A[x]$ su A tali che $D_i x_j = \delta_{ij}$; esse formano un insieme di generatori liberi dell'A-modulo delle derivazioni di $A[x]$ su A.*

Dim. Le D_i esistono perché

$$D_i\left(\sum_r a_r x_1^{r_1}\cdots x_i^{r_i}\cdots x_n^{r_n}\right) = \sum_r r_i a_r x_1^{r_1}\cdots x_i^{r_i-1}\cdots x_n^{r_n};$$

questa dà anche l'unicità. Se poi D è qualsiasi, si ha $D = \sum_i (Dx_i)D_i$; le D_i sono generatori liberi perché da $\sum_i y_i D_i = 0$ si ottiene, applicando ad x_j, che $y_j = 0$. C.V.D. □

Le D_i del (A.21.2) si denotano spesso con $\frac{\partial}{\partial x_i}$, notazione che ha senso solo quando sia ben chiaro chi sia A e chi siano le $x_1, \dots, x_n$; si usa scrivere $\frac{\partial y}{\partial x_i}$ in luogo di $\left(\frac{\partial}{\partial x_i}\right) y$; si dice *derivare rispetto* ad x_i in luogo di “applicare D_i”.

Un polinomio in una indeterminata, a coefficienti in un corpo, è *separabile* se non ha radici di molteplicità > 1 (in una chiusura algebrica del corpo).

Lemma A.21.3. *Sia C un corpo, x una indeterminata su C, ed $f = f(x)$ un polinomio in $C[x]$. Allora f è separabile se, e solo se, $f(x)$ e $\frac{\partial f}{\partial x}$ sono primi fra loro. Inoltre: se C ha caratteristica 0, ogni f irriducibile è separabile; se C ha caratteristica $p \neq 0$, un tale f è separabile se, e solo se, $f(x) \notin C[x^p]$.*

Dim. La $D = \frac{\partial}{\partial x}$ può ovviamente essere estesa ad una derivazione di $K[x]$ su K, con K chiusura algebrica di C. Se allora $f(x) = a\prod_i(x-k_i)$, con $k_i \in K$, si ha $Df = \sum_j a\prod_{i\neq j}(x-k_i)$; i fattori irriducibili di f (in $K[x]$) sono gli $x-k_i$; uno di questi, per esempio $x-k_1$, compare certamente in tutti i termini di $\sum_j$ con $j > 1$; compare anche nel primo termine se, e solo se, $k_1 = k_j$ per qualche $j \neq 1$, ossia se e solo se f non è separabile; ciò dimostra la prima parte. Per la seconda si scriva $f = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, onde $Df = na_nx^{n-1} + (n-1)a_{n-2}x^{n-1} + \cdots + a_1$, e si applichi la prima parte. L'f è già irriducibile, onde è primo con tutti i polinomi eccetto lo 0; quindi f è inseparabile se, e solo se, $Df = 0$; ne segue l'asserto. C.V.D. □

A.22 Lezione 22

Lemma A.22.1. *Sia C un corpo, D una derivazione di C, e $K = C[\theta]$ un prolungamento finito semplice separabile di C (ossia tale che il polinomio minimo di θ su C sia separabile). Allora esiste una derivazione Δ di K che induca D in C.*

Dim. Sia $f(x)$ il polinomio minimo di θ su C, onde $f(\theta) = 0$; pongasi $g(x) = (\frac{\partial}{\partial x})f(x)$, con la $\frac{\partial}{\partial x}$ computata come derivazione in $K[x]$ su K; se la Δ esiste, si deve avere $\Delta f(\theta) = 0$; ma se $f(x) = \sum_{i=0}^n c_ix^i$, è

$$\Delta f(\theta) = \sum_{i=0}^{n}(Dc_i)\theta^i + g(\theta)\Delta\theta.$$

Ora, $g(x)$ è un polinomio di grado $< n$, e non è nullo perché f è separabile; perciò $g(\theta) \neq 0$, e $\Delta\theta = -\sum_i(Dc_i)\theta^i/g(\theta)$; quindi Δ, se esiste, è unica. Per far vedere che esiste basta prendere per $\Delta\theta$ l'espressione trovata, col che il Δy per ogni $y \in K$ è determinato per linearità, e basta far vedere che la Δ così definita è proprio una derivazione. Lo lasciamo come esercizio.4 C.V.D. □

Dai (A.21.2), (A.21.3), (A.22.1), segue:

Teorema A.22.2. *Sia K un prolungamento del corpo C, di trascendenza finita n su C, e si supponga che K possieda su C una* base separante *$x_1, \ldots, x_n$; ciò significa che le $x_1, \ldots, x_n$ sono algebricamente indipendenti su C, che K è algebrico su $C(x_1, \ldots, x_n)$, e che ogni elemento di K ha su questo corpo un polinomio minimo separabile (sempre vero se, per esempio, C ha caratteristica 0). Allora le derivazioni di K su C formano uno spazio vettoriale su C di dimensione n.*

Ci poniamo ora nelle condizioni del (A.22.2); lo spazio vettoriale delle derivazioni sarà indicato con $\operatorname{der} K/C$; il suo duale sarà indicato con $\Omega^1_{K/C}$, e i suoi elementi si chiamano i *differenziali di K su C, di dimensione* 1*, o semplici*. Lo spazio E_r su $\Omega^1_{K/C}$, che è quindi lo spazio delle applicazioni r-lineari alternanti di $\mathrm{der} \times \cdots \times \mathrm{der}$ (r volte) su C, è indicato con $\Omega^r_{K/C}$, e i suoi elementi sono i *differenziali (di K su C) di dimensione r, o r-upli*; si pone anche $\Omega^0_{K/C} = K$. Il 3.42 di [AA] dice dunque che $\Omega^r_{K/C}$ ha dimensione $\binom{n}{r}$, e che gli Ω^r con $r > n$ sono $= \{0\}$; poniamo $= \{0\}$ anche gli Ω^r con $r < 0$. Se $\Omega_{K/C} = \bigoplus_r \Omega^r_{K/C}$, trasformeremo questo spazio vettoriale graduato (su K) in un complesso (lezione 14 di questa appendice) di C-moduli (ossia di spazi vettoriali su C, di solito di dimensione infinita), e non, si noti bene, di K-moduli. Per fare questo vi definiremo un $d = d_{K/C}$ di grado 1; la definizione è la seguente, ove $\omega_r \in \Omega^r_{K/C}$, e quindi $\omega_r(D_1, \ldots, D_r) \in K$:

$$
\begin{aligned}
(d\omega_r)(D_0, \ldots, D_r) = &\sum_{i=0}^{r} (-1)^i D_i \omega_r(D_0, \ldots, \widehat{D_i}, \ldots, D_r) + \\
&+ \sum_{i<j} (-1)^{i+j} \omega_r([D_i, D_j], D_0, \ldots, \widehat{D_i}, \ldots, \widehat{D_j}, \ldots, D_r).
\end{aligned}
\tag{A.22.3}
$$

Qui occorre spiegare che $[D_i, D_j]$ significa $D_i D_j - D_j D_i$, ossia che per $x \in K$ si ha $[D_i, D_j]x = D_i(D_j x) - D_j(D_i x)$; si controlla subito che $[D_i, D_j]$ è una derivazione di K su C.

A.23 Lezione 23

Occorre far vedere intanto che il $d\omega_r$ definito da (A.22.3) è veramente multilineare alternante. Ora, se $r = 0$, onde $\omega_r = x \in K$, la (A.22.3) dice che

$$(dx)D = Dx, \tag{A.23.1}$$

e questa applicazione, $D \mapsto Dx$ è effettivamente lineare; per ogni r, inoltre, ciascun termine del II membro di (A.22.3) è K-lineare in ciascuna D_h, onde tale è $d\omega_r$. Per l'alternanza, se per esempio $D_0 = D_1$, nella $\sum_i$ se ne vanno tutti i termini contenenti sia D_0 che D_1 in parentesi, e resta solo

$$D_0 \omega_r(D_1, D_2, \ldots) - D_1 \omega_r(D_0, D_2, \ldots) = 0;$$

invece nella $\sum_{i<j}$ (che esiste solo se $r > 1$) se ne vanno di nuovo i termini contenenti sia D_0 che D_1 (ossia dove D_0 e D_1 non hanno il cappuccio), e resta

$$
\begin{aligned}
-\omega_r([D_0, D_1], D_2, \ldots) + &\sum_{j>1} (-1)^j \omega_r([D_0, D_j], D_1, \ldots, \widehat{D_j}, \ldots, D_r) \\
&+ \sum_{j>1} (-1)^{j+1} \omega_r([D_1, D_j], D_0, D_2, \ldots, \widehat{D_j}, \ldots, D_r) = 0.
\end{aligned}
$$

Quindi $d\omega_r$ è alternante, onde $\in \Omega^{r+1}_{K/C}$. Poi, l'applicazione $\omega \mapsto d\omega$ è C-lineare, come si vede subito dal (A.22.3); vediamo come si comporta rispetto alla moltiplicazione per un $x \in K$; il (A.22.3) dice subito che

(A.23.2) $$d(x\omega_r) = d(x \wedge \omega_r) = dx \wedge \omega_r + x \wedge d\omega_r$$

(cfr. 3.40 e 3.41 di [AA]).

Questo ci fa ricordare che $\Omega_{K/C}$ è anche un'algebra, e ci suggerisce di ricercare la relazione tra d e $\wedge$. Se allora $x_1, \ldots, x_n$ è una base separante di K su C (cfr. A.22.2), pongasi $L_i = \frac{\partial}{\partial x_i}$; le $dx_1, \ldots, dx_n$ appartengono a $\Omega^1_{K/C}$, e sono linearmente indipendenti su K, perché se $\sum_i y_i dx_i = 0$, è $0 = (\sum_i y_i dx_i)\, L_j = y_j$; quindi le dx_i sono una base di $\Omega^1_{K/C}$ su K. Prima di proseguire notiamo per inciso una conseguenza immediata del primo fatto, che è poi una formula ben nota in Analisi:

A.23.3. *se $y \in K$, è $dy = \sum_i \frac{\partial y}{\partial x_i} dx_i$*

(basta applicare ambo i membri ad L_i). Continuiamo; intanto per $y \in K$ la (A.22.3) comporta che

$$(ddy)(D_0, D_1) = D_0 D_1 y - D_1 D_0 y - [D_0, D_1]y = 0,$$

ossia $ddy = 0$; dico allora che:

(A.23.4) $$d(\omega_r \wedge \omega_s) = (d\omega_r) \wedge \omega_s + (-1)^r \omega_r \wedge (d\omega_s)$$

se $\omega_i \in \Omega^i_{K/C}$, per $r = 0$ o $s = 0$ questa è la (A.23.2); poi se ω_r, ω_s sono elementi della base descritta, ossia prodotti esterni di vari dx_i, questa si riduce a $0 = 0$ (basta osservare che per un tale ω_r, se nella (A.22.3) si prendono delle L_j in luogo delle D_h, tutto nel secondo membro va a 0, dato che le L_j commutano fra loro); attesa allora la C-linearità di ambo i membri, basta dimostrare la (A.23.4) quando ω_r, ω_s sono multipli, a coefficienti in K, di elementi della base descritta: $\omega_r = y\omega'_r$, $\omega_s = z\omega'_s$. Il primo membro diviene $d(yz\omega'_r \wedge \omega'_s) = d(yz) \wedge \omega'_r \wedge \omega'_s$ per (A.23.2); il secondo diviene

$$zdy \wedge \omega'_r \wedge \omega'_s + (-1)^r y\omega'_r \wedge dz \wedge \omega'_s = zdy \wedge \omega'_r \wedge \omega'_s + ydz \wedge \omega'_r \wedge \omega'_s$$

per 3.41 di [AA]; ma queste coincidono, come richiesto.

E ora finalmente possiamo vedere che $dd = 0$, ossia che $dd\omega_r = 0$ per ogni ω_r; infatti $dd(y\omega'_r) = d(dy \wedge \omega'_r) = 0$ per (A.23.4), perché $ddy = d\omega'_r = 0$. Quindi $\Omega_{K/C}$ è un complesso nel quale vale la (A.23.4).

A.24 Lezione 24

Ora che abbiamo il complesso $\Omega_{K/C}$ possiamo considerare i cocicli Z^r e i cobordi B^r; gli $\omega_r \in Z^r$ sono quelli per cui $d\omega_r = 0$, e si chiamano differenziali *chiusi*;

gli $\omega_r \in B^r$ sono quelli per cui esiste un ω_{r-1} tale che $\omega_r = d\omega_{r-1}$, e si chiamano differenziali *esatti*. Se si prendono due elementi di $\Omega^n_{K/C}$, essi saranno del tipo $\sigma_1 \wedge \cdots \wedge \sigma_n$ e $\sigma'_1 \wedge \cdots \wedge \sigma'_n$; si sa inoltre che il secondo è multiplo del primo se questo è non nullo; il coefficiente $J \in K$ tale che $\sigma'_1 \wedge \cdots \wedge \sigma'_n = J\sigma_1 \wedge \cdots \wedge \sigma_n$ si chiama l'*jacobiano* di $\sigma'_1 \wedge \cdots \wedge \sigma'_n$ rispetto a $\sigma_1 \wedge \cdots \wedge \sigma_n$, e si indica con una delle notazioni

$$\frac{\sigma'_1 \wedge \cdots \wedge \sigma'_n}{\sigma_1 \wedge \cdots \wedge \sigma_n}, \qquad J\begin{pmatrix} \sigma'_1, \ldots, \sigma'_n \\ \sigma_1, \ldots, \sigma_n \end{pmatrix}.$$

Se $\sigma_i = dx_i$ e $\sigma'_i = dx'_i$ si scrive anche

$$\frac{d(x'_1, \ldots, x'_n)}{d(x_1, \ldots, x_n)}, \qquad J\begin{pmatrix} x'_1, \ldots, x'_n \\ x_1, \ldots, x_n \end{pmatrix}.$$

L'applicazione K-lineare f di $\Omega^n_{K/C}$ tale che $\sigma'_i = f\sigma_i$ è data, nel secondo caso, da $dx'_i = fdx_i$, ossia da $fdx_i = \sum_j \frac{\partial x'_i}{\partial x_j} dx_j$; quindi $J\binom{x'}{x} = \det f = \det(\frac{\partial x'_i}{\partial x_j})$, che è la solita definizione dell'jacobiano in Analisi; si vede anche che $J \neq 0$ se, e solo se, le dx'_i sono linearmente indipendenti su K, ossia se, e solo se, le x'_i sono una base separante ("variabili indipendenti" dell'Analisi). Se $n = 1$ si ha in particolare $\frac{\partial x'}{\partial x} = J\binom{x'}{x} = \frac{dx'}{dx}$, noto simbolo per le derivate "totali"; si noti che questo è un vero rapporto di differenziali.

Che cosa ci se ne fa di tutta questa costruzione? Finché si vuole usare tutto il $\Omega_{K/C}$, poco, in quanto esso è canonicamente legato a K e C, e quindi non può contenere informazioni nuove. L'utilità sta quando o si usano dei sottocomplessi di $\Omega_{K/C}$ che siano anche sottoalgebre e che siano spazi vettoriali su C di dimensione finita, ovvero quando tutta la teoria sia fatta non partendo da un corpo C, ma da un anello; o infine quando K è di sua natura ignoto, e si usa tutto il macchinario esposto per studiarlo. Ciò che in ogni caso è estremamente interessante è il fatto che le due applicazioni dell'algebra omologica qui esposte (topologia e differenziali) sono intimamente legate tra loro, come ora faremo vedere, senza però dare dimostrazioni.

Diamo solo degli esempi per illustrare l'affermazione precedente.

A.25 Lezione 25

Si prenda per C il corpo reale (anche il complesso andrebbe bene); ci interessa un poliedro K di dimensione n, e con K_* si indicherà il complesso sul corpo reale; chiamiamo F la C-algebra delle "funzioni differenziabili su K"; funzioni su K vuoldire applicazioni di $\overline{K}$ (unione delle celle di K) su C; dato poi l'omeomorfismo usato per definire le celle, esse saranno funzioni reali di n variabili reali, e come tali ha senso parlare di differenziabilità. Porremo $F^i = \Omega^i_{F/C}$, e $F^* = \bigoplus_i F^i$; indicheremo con d sia il d_* di K_* che il d^* di F^*. Si può definire un'applicazione C-bilineare $(S, \omega) \mapsto S \circ \omega \in C$ di $K_i \times F^i$ su C nel modo seguente, per approssimazioni successive; intanto basta definirla quando S, ω sono simplessi, ossia basta definire la $S \circ (dx_1 \wedge \cdots \wedge dx_i)$; ora, S è una cella, ossia l'immagine omeomorfa di un simplesso in uno spazio vettoriale V su C, di dimensione $m \geq n$; i suoi vertici sono le immagini di certi vettori $v_0, \ldots, v_i$; le $x_1, \ldots, x_i$ sono i coefficienti con cui certi vettori $w_1, \ldots, w_i$ (che generano lo stesso spazio generato dai $v_j - v_0$) compaiono nell'espressione di un punto della cella S; usando la base duale $w_1^*, \ldots, w_i^*$ prenderemo allora, come prima approssimazione di $S \circ \omega$, la

$$(i!)^{-1}(w_1^* \wedge \cdots \wedge w_i^*)(v_1 - v_0, \ldots, v_i - v_0).$$

La seconda approssimazione consiste nel suddividere S in tante celle $S'_1, S'_2, \ldots$ di dimensione i, nel computare gli $S'_j \circ \omega$ nel modo detto, e nel farne la somma. Si può dimostrare che se le suddivisioni sono fatte con giudizio, queste approssimazioni tendono ad un limite, che è appunto l'$S \circ \omega$; esso è comunemente denotato con $\int_S \omega$, e chiamato l'*integrale* di ω su S. Se $i = 0$, $\int_S \omega$ è semplicemente la somma dei valori che ω (elemento di K) assume nei punti di S (che sono un numero finito).

Nei casi più simpatici (qui naturalmente non diamo dettagli) l'applicazione

$$(S_i, \omega_i) \mapsto \int_{S_i} \omega_i$$

(ora gli indici danno la dimensione) è una dualità; ma il più bello è che in essa le d di K_* ed F^* sono trasposte l'una dell'altra:

$$\int_{dS_i} \omega_{i-1} = \int_{S_i} d\omega_{i-1} \qquad \text{(formula di Green-Stokes)}. \tag{A.25.1}$$

Quindi H^* (coomologia di F^*) è il duale di H_* (omologia su K_*), e le proprietà di K possono essere trovate studiando H^*.

Esempi. 1. K è il segmento aperto (a, b), e le sue facce sono a e b; F è fatto di funzioni differenziabili in (a, b). La (A.25.1) scritta con un simbolismo più comune in questo caso, dice semplicemente che $\int_a^b df(x) = f(b) - f(a)$.

2. Prendiamo per K la regione fra due circonferenze concentriche, triangolata come si vuole; se si prende per S un cerchio tutto contenuto in K (tutto il suo interno), onde dS è la circonferenza, la (A.25.1) dice che

$$\int_{dS} f dx + g dy = \int_S \left(\frac{\partial g}{\partial x} - \frac{\partial f}{\partial y} \right) dx \wedge dy$$

(usualmente indicato con $\iint_S (\ldots) dx\, dy$). Ma questo può non esser vero se il cerchio S non è tutto in K (per esempio, se è concentrico colle due circonferenze che delimitano K); per esempio, $\omega = \frac{ydx - xdy}{x^2+y^2}$, che è chiuso ma non esatto, ha integrale nullo lungo le curve chiuse il cui interno è tutto in K, ma non lungo quelle senza questa proprietà; il suo "integrale" fatto con la testa nel sacco è $-\arctan(y/x)$, che *non è* un elemento di F.

3. Esercizio. Chi conosce gli operatori vettoriali $grad$, rot può cercare il loro significato nel contesto di questa teoria.

Elenco dei simboli

$\mathbb{N}$	numeri naturali, 0 incluso	
$\mathbb{Z}$	numeri interi	
$\mathbb{Q}, \mathbb{Q}_{>0}$	numeri razionali, risp. numeri razionali positivi	
$\mathbb{R}, \mathbb{R}_{>0}$	numeri reali, risp. numeri reali positivi	
$\mathbb{C}$	numeri complessi	
$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$	elementi invertibili in $\mathbb{Q}$, risp. $\mathbb{R}, \mathbb{C}$	
V^*	spazio duale di V	1
V^{**}	spazio biduale di V	1
$X^\perp$	sottospazio ortogonale in V^*	1
f^*	applicazione lineare trasposta	2
A^*	matrice trasposta	2
P_n	gruppo simmetrico di ordine $n!$	3
$\mathrm{sgn} p$	segnatura della permutazione p	3
$E_i(V)$	spazio delle forme i-lineari alternanti su V^*	3
$f \wedge g$	prodotto esterno di applicazioni multilineari alternanti	4
$E(V)$	algebra esterna su V	6
$v_{t_1} \wedge \cdots \wedge v_{t_i}$	vettori della base di $E_i(V)$ associata ad una base di V	6
$E_i(f)$	omomorfismo associato ad $f : V \to U$	6
$g \boxplus h$	somma ortogonale di due forme bilineari	11
$V \boxplus U$	somma ortogonale di due spazi	11
$g \boxminus h$	differenza ortogonale di due forme bilineari	11
$V \boxminus U$	differenza ortogonale di due spazi	11
$\langle S \rangle$	minimo sottospazio che contiene S	14
W_C	gruppo di Witt del corpo C	21
$v \bar{\wedge} w$	prodotto vettoriale	26
(T, S)	spazio affine	29
$(O, t_1, \dots, t_n)$	riferimento affine	30
$\mathbb{A}^n$	spazio affine di dimensione n	35
(S_n, σ)	spazio proiettivo di dimensione n	36
$[V]$	insieme dei sottospazi vettoriali di V	36
$sostS$	sostegno di uno spazio vettoriale in S_n	36
$A_r < B_s$	relazione di appartenenza (nello spazio proiettivo)	36
$A_r \cap B_s$	intersezione fra elementi dello spazio proiettivo	36
$A_r + B_s$	elemento generato da A_r e B_s nello spazio proiettivo	36
(S_n, σ^*)	spazio proiettivo duale di (S_n, σ)	37
(f_S, f_V)	applicazione proiettiva	38

Om_Z	spazio vettoriale delle omologie speciali di asse Z 42
$(P_0,\dots,P_n,U)$	sistema di riferimento in S_n 44
(P_∞,P_0,P_1,P)	birapporto di quattro punti allineati 46
(a,b,c,d)	birapporto di quattro elementi di $C\cup\{\infty\}$ 46
$V(c_1,\dots,c_r)$	determinante di Vandermonde 65
$x_i(P)$	valore assunto in P dalla coordinata x_i 69
$D=\sum_i e_iU_i$	divisore (su S_n) 75
$\operatorname{div}_{S_n} f(x)$	divisore di una funzione razionale 75
$\operatorname{supp} D$	supporto di un divisore 75
$\bar{S}_n$	estensione di S_n (def. su C) a $\bar{C}$ 75
$Z_i(M)$	cicli di dimensione i 103
$B_i(M)$	bordi di dimensione i 103
$H_i(M)$	i-esimo gruppo di omologia del complesso M 103
$\operatorname{der} K/C$	spazio vettoriale delle derivazioni di K su C 116
$\Omega^1_{K/C}$	differenziali di K su C 116