1 Insiemi e numeri

1.1 Insiemi; relazioni, funzioni

Insiemi e sottoinsiemi Un *insieme* è una collezione di oggetti, che si diranno i suoi *elementi*. Per indicare che a è un elemento dell'insieme A, si usa dire che a *appartiene ad* A, e si denota "$a \in A$" oppure "$A \ni a$"; l'affermazione contraria si denota "$a \notin A$" oppure "$A \not\ni a$". Se si vuole rappresentare il fatto che un insieme A è costituito dagli oggetti a, b, c, ..., si potrà scrivere

Insiemi, elementi

$$A = \{a, b, c, d, ...\} \qquad \text{(rappresentazione } \textit{estensiva} \text{ di un insieme).}$$

Tuttavia, tale rappresentazione può diventare concretamente impossibile quando A abbia una gran quantità di elementi: risulta allora più pratico menzionare che l'insieme è costituito dagli elementi x tali che una determinata proposizione aperta $P(x)$ è vera, scrivendo

$$A = \{x : \mathrm{P}(x)\} \ \text{ oppure } \ A = \{x \mid \mathrm{P}(x)\} \qquad \text{(rappresentazione } \textit{intensiva} \text{ di un insieme).}$$

Per ragioni tecniche, è conveniente assumere che esista un *insieme vuoto* $\varnothing$ privo di elementi. Un insieme si dirà *finito* se ha un numero finito di elementi, *infinito* nel caso contrario. Due insiemi A e B sono *uguali* se e solo se hanno esattamente gli stessi elementi (si scriverà allora $A = B$). Se invece gli elementi di A formano una sottocollezione di quelli di B, si dice che A *è un sottoinsieme di* B, o che A *è contenuto in* B (notazione: $A \subset B$, o $A \subseteq B$ se si ammette che possa anche essere uguale) o che B *contiene* A (notazione: $B \supset A$, $B \supseteq A$). Dato un qualsiasi insieme A, è chiaro che $A \subseteq A$; inoltre, si assume che $\varnothing \subset A$ (i sottoinsiemi di A diversi sia da A che da $\varnothing$ si dicono *propri*). Per definizione, vale $A = B$ se e solo se $A \subset B$ e $B \subset A$,[10] e $\{a\} \subset A$ se e solo se $a \in A$. [11] Quando si vuole descrivere un sottoinsieme A di un dato insieme X tramite una sua *proprietà caratteristica* (ovvero, una proposizione aperta $\mathrm{Q}(x)$ che, per $x \in X$, sia vera se e solo se $x \in A$) la proposizione aperta da inserire nella rappresentazione analitica intensiva sarebbe $\mathrm{P}(x) = (x \in X) \wedge \mathrm{Q}(x)$, ovvero $A = \{x : (x \in X) \wedge \mathrm{Q}(x)\}$, ma si usa scrivere per semplicità

$$A = \{x \in X : \mathrm{Q}(x)\}.$$

Esempi. (1) L'insieme A dei numeri razionali tra -3 (compreso) e 4 (escluso) si può scrivere $A = \{x \in \mathbb{Q} : -3 \leq x < 4\}$: qui la proposizione aperta $\mathrm{Q}(x)$ è, naturalmente, $\mathrm{Q}(x) =$ "$-3 \leq x < 4$". L'insieme

[10] Il modo classico di dimostrare che due insiemi sono uguali è proprio quello di dimostrare che il primo è contenuto nel secondo, e il secondo nel primo.

[11] Si faccia attenzione a non confondere elementi e sottoinsiemi di un dato insieme: $\{a\}$ denota il sottoinsieme di A formato dal solo elemento a, e non va confuso con a.

B dei numeri interi tra -2 (escluso) e 2 (compreso) si può scrivere intensivamente come $B = \{x \in \mathbb{Z} : -2 < x \leq 2\}$, o estensivamente come $B = \{-1, 0, 1, 2\}$: è chiaro che $B \subset A$. **(2)** L'insieme A delle città (capoluoghi di provincia) italiane che sono venete *e* che iniziano per V si scrive intensivamente come $A = \{x : x$ è una città veneta che inizia per V$\}$ o estensivamente come $A = \{$Verona, Venezia, Vicenza$\}$; invece l'insieme B delle città italiane che sono venete *o* che iniziano per V si può scrivere intensivamente come $B = \{x$ città italiana : x è una città veneta oppure inizia per V$\}$ o estensivamente come $B = \{$Belluno, Padova, Rovigo, Treviso, Varese, Venezia, Verbania, Vercelli, Verona, Vibo Valentia, Vicenza, Viterbo$\}$. È chiaro che $B \supset A$ (in generale P$\wedge$Q $\Rightarrow$ P$\vee$Q).

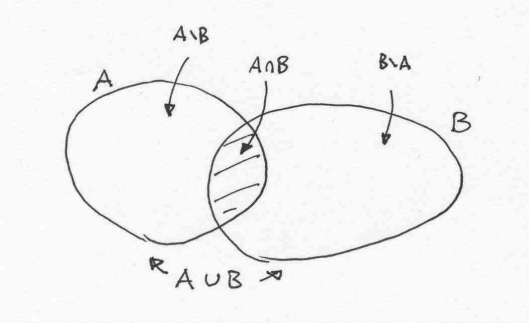

Figura 1.1: Rappresentazione di insiemi tramite i diagrammi di Venn

Unione, intersezione, differenza Introduciamo le operazioni più comuni in teoria degli insiemi, per visualizzare le quali è particolarmente espressiva la rappresentazione con *diagrammi di Venn* (Figura 1.1): l'*unione*, l'*intersezione*, la *differenza*. Dati due insiemi A e B, la loro *unione* è

Operazioni con gli insiemi

$$A \cup B = \{x : (x \in A) \vee (x \in B)\},$$

l'insieme degli elementi che appartengono ad A oppure a B: si tratta di unire, senza ripetizioni, le due collezioni. Vale chiaramente $A \cup B = B \cup A$; se $B \subset A$ allora $A \cup B = A$, in particolare $A \cup \varnothing = A$ per ogni insieme A.[(12)]
L'*intersezione* è

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\},$$

insieme degli elementi che appartengono sia ad A che a B (si prendono solo gli elementi comuni alle due collezioni). Vale chiaramente $A \cap B = B \cap A$; se $B \subset A$ allora $A \cap B = B$. Se $A \cap B = \varnothing$, gli insiemi A e B si diranno *disgiunti* e la loro unione si indicherà anche con $A \sqcup B$, o con $A \dot{\cup} B$.
La *differenza*

$$A \setminus B = \{x : (x \in A) \wedge (x \notin B)\}$$

è l'insieme degli elementi che appartengono ad A ma non a B (dalla collezione degli elementi di A si eliminano quelli che stanno anche in B): ovviamente, se A e B sono disgiunti allora $A \setminus B = A$, mentre se $B \subset A$ allora $B \setminus A = \varnothing$. In generale vale $A \cup B =$

[(12)] Ciò mostra tra l'altro che *l'insieme vuoto è unico*: se infatti ce ne fossero due (diciamo $\varnothing_1$ e $\varnothing_2$) varrebbe $\varnothing_1 = \varnothing_1 \cup \varnothing_2 = \varnothing_2 \cup \varnothing_1 = \varnothing_2$.

$(A \setminus B) \sqcup (A \cap B) \sqcup (B \setminus A)$, da cui se $B \subset A$ si ottiene $A = (A \setminus B) \sqcup B$, e $A \setminus B$ è detto il *complementare di B in A* (si scrive anche $\complement_A B$).

Esempi. (1) Sia A l'insieme degli animali neri, B quello dei gatti. Allora $A \cup B$ è costituito da tutti i gatti e da tutti gli animali neri (dunque un gatto rosso e un alce nero ci stanno, ma non un alce rosso), $A \cap B$ è l'insieme dei gatti neri, $A \setminus B$ sono gli animali neri che non sono gatti (tipo un alce nero), $B \setminus A$ i gatti di colore diverso dal nero. **(2)** Dentro $\mathbb{Q}$ consideriamo $A = \{m \in \mathbb{Z} : m \text{ è pari}\}$ e $B = \{x \in \mathbb{Q} : -4 < x \leq 2\}$. Allora $A \cup B = \{x \in \mathbb{Q} : -4 < x \leq 2 \text{ oppure } x \text{ è un intero pari}\}$ (ad esempio $-874, \frac{7}{4}, -1, -4 \in A \cup B$ ma $53, -5, 3, \frac{9}{4} \notin A \cup B$), $A \cap B = \{-2, 0, 2\}$, $A \setminus B = \{m \in \mathbb{Z} : m \text{ è pari}, m \neq -2, 0, 2\}$ e $B \setminus A = \{x \in \mathbb{Q} : -4 < x \leq 2, x \neq -2, 0, 2\}$ Il complementare di B in $\mathbb{Q}$ è $\complement_{\mathbb{Q}} B = \{x \in \mathbb{Q} : x \leq -4\} \cup \{x \in \mathbb{Q} : x > 2\}$.

Insieme delle parti e prodotto cartesiano Dato un insieme X, si denota con $\mathcal{P}(X)$ l'insieme delle *parti di X*, ovvero l'insieme i cui elementi sono i sottoinsiemi di X:

Insieme delle parti

$$\mathcal{P}(X) = \{Y : Y \subset X\}.$$

Si noti che $\mathcal{P}(X) \neq \varnothing$ per ogni insieme X, perché si avrà sempre $X \in \mathcal{P}(X)$ e $\varnothing \in \mathcal{P}(X)$. Dati due insiemi X e Y, il loro *prodotto cartesiano* $X \times Y$ è l'insieme formato dalle "coppie ordinate" (x, y) con $x \in X$ e $y \in Y$: ovvero,

Prodotto cartesiano

$$X \times Y = \{(x, y) : x \in X \text{ e } y \in Y\}.$$

Se uno tra X e Y è $\varnothing$, si pone $X \times Y = \varnothing$. È chiaro che se X e Y sono insiemi finiti, diciamo rispettivamente con n e m elementi, anche $X \times Y$ è un insieme finito ed ha mn elementi. Non è difficile convincersi anche del fatto che se X è un insieme finito con n elementi, allora anche $\mathcal{P}(X)$ è finito ed ha 2^n elementi.[(13)]

Esempi. Se $X = \{a, b, c\}$ e $Y = \{1, 2, 3, 4\}$, vale $\mathcal{P}(X) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, X\}$, $\mathcal{P}(Y) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, Y\}$ e $X \times Y = \{(a, 1), (a, 2), (a, 3), (a, 4), (b, 1), (b, 2), (b, 3), (b, 4), (c, 1), (c, 2), (c, 3), (c, 4)\}$. Come previsto, essi hanno rispettivamente $2^3 = 8$, $2^4 = 16$ e $3 \cdot 4 = 12$ elementi.

Relazioni Una *relazione* (binaria) in un insieme X è una parentela che può legare o meno tra loro due oggetti qualunque (presi nell'ordine) x_1 e x_2 di X. Essa può essere vista semplicemente come un sottoinsieme $\mathcal{R} \subset X \times X$: perciò, se $(x_1, x_2) \in \mathcal{R}$, si usa scrivere anche $x_1 \mathcal{R} x_2$, e si dirà che x_1 è *in relazione* con x_2; se invece $(x_1, x_2) \notin \mathcal{R}$, si dirà che x_1 non è in relazione con x_2.

Relazioni

Una relazione $\mathcal{R}$ può avere o meno alcune proprietà notevoli, che andiamo ora ad elencare:

(Rifl) *Riflessività*: $x \mathcal{R} x$ per ogni $x \in X$;
(Sym) *Simmetria*: se $x_1 \mathcal{R} x_2$, allora $x_2 \mathcal{R} x_1$;
(ASym) *Antisimmetria*: se $x_1 \mathcal{R} x_2$ e $x_2 \mathcal{R} x_1$, allora $x_1 = x_2$;
(Trns) *Transitività*: se $x_1 \mathcal{R} x_2$ e $x_2 \mathcal{R} x_3$, allora $x_1 \mathcal{R} x_3$.

[(13)] Scegliere un sottoinsieme di X equivale a dire, per ogni elemento $x \in X$, se x ci sta o no: dunque vi sono 2 possibilità per ogni $x \in X$, indipendenti da quelle di tutti gli altri elementi, e pertanto le possibili scelte di sottoinsiemi di X sono $2 \cdot \cdots \cdot 2$ (n fattori), ovvero 2^n.

Una relazione $\mathcal{R}$ in X che soddisfa (Rifl)-(Sym)-(Trns) si dice *equivalenza* in X; due elementi $x_1, x_2 \in X$ legati da una relazione d'equivalenza si diranno anche *equivalenti tra loro*, e si scriverà spesso $x_1 \sim x_2$ o notazioni simili. L'effetto di un'equivalenza in un insieme X è quello di creare una *partizione* di X, ovvero di spezzare X in una famiglia di sottoinsiemi disgiunti (le *classi di equivalenza*, ciascuna formata da elementi in relazione tra loro);[14] viceversa, data una qualsiasi partizione di X si può definire un'associata relazione d'equivalenza in X dicendo che due elementi $x_1, x_2 \in X$ sono equivalenti se appartengono al medesimo sottoinsieme della partizione (la dimostrazione è evidente). Se invece la relazione $\mathcal{R}$ soddisfa (Rifl)-(ASym)-(Trns), essa si dirà un *ordine* in X, perché il suo effetto è quello di creare (proprio grazie a (ASym)) un sistema di "gerarchie" tra gli elementi di X; se una relazione d'ordine soddisfa anche

Equivalenza

Ordine

(Tot) *Totalità*: se $(x_1, x_2) \in X \times X$, allora vale $x_1 \mathcal{R} x_2$ oppure $x_2 \mathcal{R} x_1$,

essa si dirà un *ordine totale* in X.

Esempi. **(1)** Sia X l'insieme di tutti gli esseri umani; le relazioni "essere coetanei", "essere figli degli stessi genitori", "essere nati nella stessa nazione" sono tutte relazioni d'equivalenza (e infatti ripartiscono tutto X in "classi d'equivalenza" disgiunte) mentre ad esempio "essere fratelli" (ovvero avere un genitore in comune) e "lavorare nella stessa ditta" non lo sono: infatti "essere fratelli" non soddisfa necessariamente (Trns), mentre "lavorare nella stessa ditta" soddisfa (Sym) e (Trns) ma non (Rifl) (se una persona è disoccupata...). La relazione "essere coetaneo o più anziano" non è d'ordine, perché soddisfa (Rifl) e (Trns) ma non (ASym). La relazione "voler bene a" non soddisfa ne' (Rifl) (pensare ai masochisti) ne' (Sym) (a meno che uno non voglia credere all'affermazione dantesca *Amor ch'a nullo amato amar perdona*, secondo la quale l'Amore alla fine forza chi è amato a contraccambiare il sentimento) ne' (Trns) (anche se Mario vuol bene a Ugo e Ugo vuol bene a Federico, può darsi che Mario detesti Federico). **(2)** Dato un insieme T e considerato l'insieme $X = \mathcal{P}(T)$ delle sue parti, la relazione $\subset$ non è una relazione d'ordine in X (non vale (Rifl)) mentre $\subseteq$ è una relazione d'ordine in X, anche se non totale; quanto alla relazione "avere intersezione non vuota", essa non soddisfa (Trns). **(3)** In $\mathbb{Q}$, la relazione $\leq$ è un ordine totale. **(4)** Fissando un numero naturale $n_0 \in \mathbb{N}$, possiamo dividere ogni numero intero $m \in \mathbb{Z}$ per n_0 usando la *divisione euclidea*: esisterà un'unica coppia di numeri interi (q, r) con $0 \leq r < n_0$ tali che $m = qn_0 + r$: il numero q si dirà "quoziente" ed r "resto" $r \in \mathbb{Z}$ della divisione euclidea. (Ad esempio, se $n_0 = 7$ si ha $0 = 0 \cdot 7 + 0$, $26 = 3 \cdot 7 + 5$, $-37 = (-6)7 + 5$ e $-20 = (-3)7 + 1$.) Consideriamo in $\mathbb{Z}$, la relazione "avere lo stesso resto nella divisione per n_0", o analogamente "differire per multipli interi di n_0": si verifica facilmente che essa è un'equivalenza, e le classi d'equivalenza sono le cosiddette *classi di resto modulo* n_0, ognuna delle quali è costituita da tutti i numeri interi che danno lo stesso resto nella divisione euclidea per n_0 (le classi resto saranno dunque n_0).

Funzioni Quello di "funzione" è il concetto centrale di tutta la Matematica.

Siano X e Y due insiemi diversi da $\varnothing$. Una *funzione* (o anche *mappa*, o *applicazione*) da

Funzione

[14] Infatti, se $\mathcal{R}$ è una relazione d'equivalenza in X, ogni $x \in X$ appartiene una classe d'equivalenza (almeno quella degli elementi in relazione con esso, tra i quali se medesimo grazie a (Rifl)); se poi due classi d'equivalenza hanno un elemento in comune, per (Sym) e (Trns) esse devono coincidere, e dunque sono tutte disgiunte tra loro.

X a Y è una terna ordinata $f = (X, Y, \Gamma)$ ove Γ è un sottoinsieme del prodotto cartesiano $X \times Y$ tale che per ogni $x \in X$ esiste *uno e un solo* $y_x \in Y$ tale che $(x, y_x) \in \Gamma$. L'elemento y_x viene solitamente denotato con $f(x)$, ed è detto *immagine* di x tramite f.[15]
L'insieme "di partenza" X si chiama *dominio* di f, quello "d'arrivo" Y *codominio* di f, mentre $\Gamma = \Gamma_f = \{(x, f(x)) : x \in X\}$ è detto *grafico* di f: due funzioni sono dunque uguali se e solo se hanno gli stessi dominio, codominio e grafico.

Dominio, codominio
Grafico

La definizione appena data di funzione è quella formalmente corretta; tuttavia, come già accennato nei prerequisiti del corso, in termini pratici è utile pensare a una funzione come a una "regola" che ad ogni elemento $x \in X$ associa uno ed un solo elemento $f(x) \in Y$.[16]
La notazione più usuale per una funzione è $f : X \to Y$, oppure $X \xrightarrow{f} Y$. Se $y \in Y$ è l'immagine di x tramite f, si dirà anche che f *manda* $x \in X$ *in* $y = f(x) \in Y$, o si scriverà $x \mapsto f(x)$.

La funzione si dirà *costante* se esiste un elemento $y_0 \in Y$ tale che $f(x) = y_0$ per ogni $x \in X$ (ovvero, f manda tutti gli $x \in X$ nel medesimo $y_0 \in Y$). Se $X = Y$, c'è l'ovvia funzione *identità* $\mathrm{id}_X : X \to X$, con $\mathrm{id}_X(x) = x$.

Costante
Identità

Se $A \subset X$ e $B \subset Y$, si definisce

Immagine, antiimmagine

$$\begin{aligned} f(A) &= \{f(x) \in Y : x \in A\} \quad \subset Y \qquad (\textit{immagine} \text{ di } A \text{ tramite } f) \\ f^{-1}(B) &= \{x \in X : f(x) \in B\} \quad \subset X \qquad (\textit{anti-immagine} \text{ di } B \text{ tramite } f) : \end{aligned}$$

ovvero, $f(A)$ è l'insieme di tutte le immagini dei vari elementi di A (i "luoghi occupati in arrivo partendo da A"), mentre $f^{-1}(B)$ è l'insieme di tutti gli elementi di X la cui immagine sta in B (gli "oggetti del dominio che vengono spediti in B").[17] In particolare, $f(X)$ è detta *immagine* della funzione f, e ovviamente vale $f^{-1}(Y) = X$. Si noti che se $A \neq \varnothing$ allora $f(A) \neq \varnothing$, mentre può benissimo accadere che $f^{-1}(B) = \varnothing$ anche se $B \neq \varnothing$: precisamente, $f^{-1}(B) = \varnothing$ se e solo se $B \cap f(X) = \varnothing$. Nel caso di $\{y_0\}$ (sottoinsieme di Y costituito dal solo elemento y_0), per abuso di notazione si usa scrivere spesso $f^{-1}(y_0)$ in luogo del formalmente corretto $f^{-1}(\{y_0\})$: si tratta della *fibra* di f sopra y_0, ovvero gli elementi di X che vengono mandati in y_0. Si noti che la relazione in X data da "appartenere a una stessa fibra di f" (ovvero $x_1 \sim x_2$ se e solo se $f(x_1) = f(x_2)$) è un'equivalenza, dunque fornisce una partizione dell'insieme X: in altre parole, $X = \bigcup\{f^{-1}(y) : y \in Y\}$ (l'insieme X è unione disgiunta di tutte le fibre di f, al variare di y in Y).

Fibra

Esempio. Sia $X = \{a, b, c, d\}$, $Y = \{1, 2, 3\}$ e $f : X \to Y$ la funzione definita da $f(a) = 2$, $f(b) = 1$, $f(c) = 2$ e $f(d) = 2$ (vedi Figura 1.2). Se $A_1 = \{a, b\} \subset X$ si ha $f(A_1) = \{1, 2\}$, mentre se $A_2 = \{a, c\} \subset X$ si ha $f(A_2) = \{2\}$. L'immagine di f è $f(X) = \{1, 2\}$. Se $B_1 = \{3\} \subset Y$ si ha $f^{-1}(B_1) = \varnothing$ (infatti $B_1 \cap f(X) = \varnothing$) e se $B_2 = \{2, 3\} \subset Y$ si ha $f^{-1}(B_2) = \{a, c, d\}$.

[15] Attenzione: non si è detto che elementi *diversi* $x_1 \neq x_2$ di X devono per forza avere immagini *diverse*: l'importante è che *ogni* elemento $x \in X$ abbia *un e un solo ben chiaro* elemento immagine $f(x) \in Y$.
[16] Si noti che, nella definizione formale di funzione, le nozioni di "funzione" e di "grafico" sono sostanzialmente la stessa cosa (in effetti, dato Γ sono dati ovviamente anche X e Y), mentre invece nelle note dei prerequisiti del corso (vedi pag. 3) abbiamo preferito, a fini didattici, fare una netta distinzione tra esse.
[17] Per l'immagine si usa talvolta la notazione $f^{\rightarrow}(A)$, e per l'antiimmagine la notazione $f^{\leftarrow}(B)$.

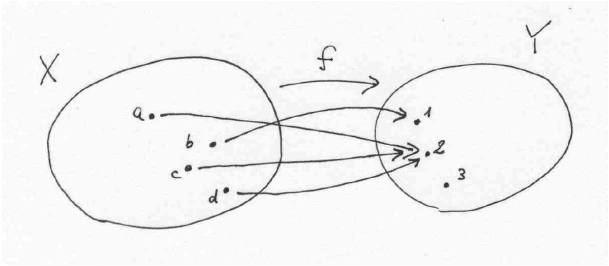

Figura 1.2: Una funzione deve mandare *ogni* elemento del suo dominio in *uno ed un solo* elemento del suo codominio

Esercizio. *Mostrare che se $f : X \to Y$ è una funzione, per ogni $A_1, A_2 \subset X$ si ha*

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2), \qquad f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2),$$

mentre per ogni $B_1, B_2 \subset Y$ vale

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2), \qquad f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2).$$

Risoluzione. Ad esempio, mostriamo che (1) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$ e (2) $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. Per (1), dire $x \in f^{-1}(B_1 \cup B_2)$ è equivalente a dire $f(x) \in B_1 \cup B_2$, cioè $f(x) \in B_1$ oppure $f(x) \in B_2$, cioè $x \in f^{-1}(B_1)$ oppure $x \in f^{-1}(B_2)$, cioè $x \in f^{-1}(B_1) \cup f^{-1}(B_2)$. Per (2), dire che $y \in f(A_1 \cap A_2)$ equivale a dire che esiste $x \in A_1 \cap A_2$ tale che $f(x) = y$. Ma essendo anche $x \in A_1$, si ha allora $y \in f(A_1)$, e analogamente $y \in f(A_2)$: dunque $y \in f(A_1) \cap f(A_2)$, cioè $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. L'inclusione inversa "$\supset$" invece non vale in generale: ad esempio, se x_1 e x_2 sono due elementi distinti di X, e poniamo $A_1 = \{x_1\}$, $A_2 = \{x_2\}$ ed f una funzione costante (diciamo di valore $y_0 \in Y$), allora $f(A_1 \cap A_2) = \varnothing$ (perché $A_1 \cap A_2 = \varnothing$) mentre $f(A_1) \cap f(A_2) = \{y_0\} \neq \varnothing$.

Restrizione, corestrizione, estensione

Data una funzione $f : X \to Y$ ed un sottoinsieme $A \subset X$, si potrà definire la funzione *restrizione di f a A*, denotata $f|_A : A \to Y$, nel modo più naturale: dato $x \in A$, si porrà $f|_A(x) = f(x)$. Se invece $X \subset \widetilde{X}$, una qualsiasi funzione $\tilde{f} : \widetilde{X} \to Y$ tale che $\tilde{f}\Big|_X = f$ si dirà un'*estensione di f*. È chiaro che la restrizione di f ad A è unica, mentre in generale f può ammettere molte diverse estensioni. Altra cosa importante: si può sempre restringere il dominio di una funzione $f : X \to Y$ ad un sottoinsieme $A \subset X$, ma bisogna fare attenzione quando si vuole restringere il codominio di f a $B \subset Y$: per poter continuare ad essere una funzione, bisognerà che l'immagine $f(X)$ sia contenuta in B. Dunque, se $f : X \to Y$ e $B \subset Y$, si potrà considerare la sua *corestrizione* $f|^B : X \to B$ se e solo se $f(X) \subset B$.

Funzione composta

Se $f : X \to Y$ e $g : Y \to Z$ sono due funzioni (in cui dunque il codominio della prima coincide col dominio della seconda), si definisce la *funzione composta* $g \circ f : X \to Z$ tramite la regola $(g \circ f)(x) = g(f(x))$ per ogni $x \in X$.

Esempio. Se $f : \mathbb{R} \to \mathbb{R}$ è data da $f(x) = x^2 + 1$, il grafico Γ_f di f è la parabola $\{(x, y) \in \mathbb{R}^2 : y = x^2 + 1\}$; se $g : \mathbb{R} \to \mathbb{R}$ è data da $g(x) = -x + 3$ il grafico Γ_g di g è la retta $\{(x, y) \in \mathbb{R}^2 : y = x + 3\}$. La composizione $g \circ f : \mathbb{R} \to \mathbb{R}$ è data da $g(f(x)) = -(x^2 + 1) + 3 = -x^2 + 2$, mentre la composizione $f \circ g : \mathbb{R} \to \mathbb{R}$ è data da $f(g(x)) = (-x + 3)^2 + 1 = x^2 - 6x + 10$.

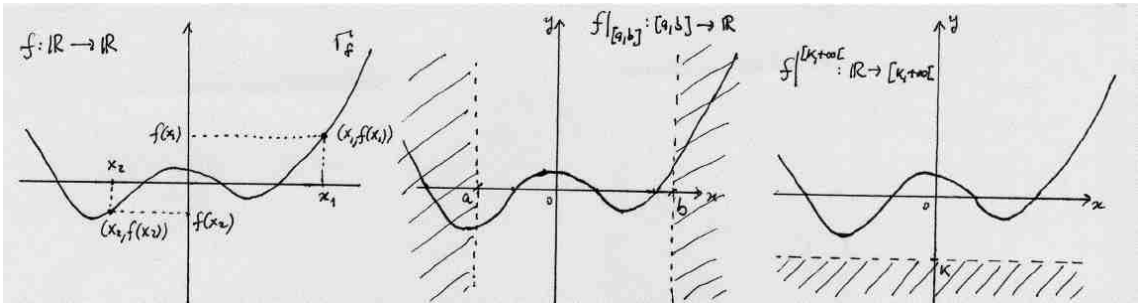

Figura 1.3: Il grafico di una funzione $f : \mathbb{R} \to \mathbb{R}$; la sua restrizione ad un intervallo $[a, b]$; la sua corestrizione alla semiretta $\mathbb{R}_{\geq k}$ (che contiene l'immagine di f).

Funzioni iniettive, suriettive, biiettive

Una funzione $f : X \to Y$ si dirà *iniettiva* se da $x_1 \neq x_2$ in X segue $f(x_1) \neq f(x_2)$ in Y (cioè se manda elementi distinti di X in elementi distinti di Y), o equivalentemente se da $f(x_1) = f(x_2)$ in Y segue $x_1 = x_2$ in X. Una tale funzione esiste quando X è "più piccolo" di Y, e identifica X come un sottoinsieme di Y (in effetti, in questo caso l'immagine $f(X)$ è "una copia fedele" di X dentro Y); infatti l'esempio più semplice di funzione iniettiva è la mappa di *inclusione* di un sottoinsieme $A \subset X$ dentro X, ovvero la funzione $\iota_A : A \to X$ data da $\iota_A(x) = x$.

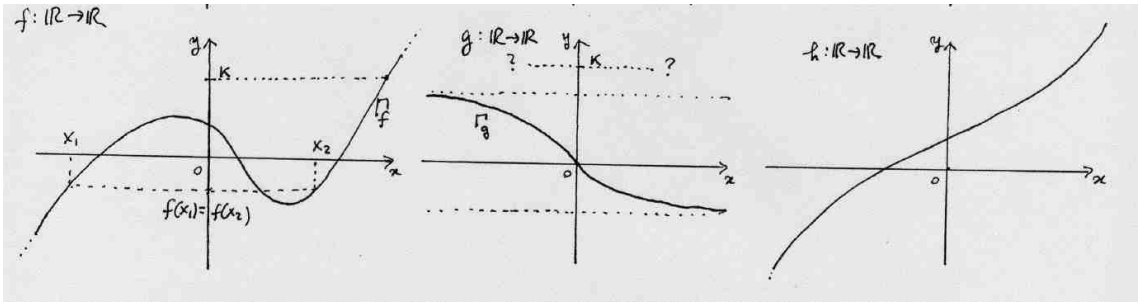

Figura 1.4: f è suriettiva ma non iniettiva; g è iniettiva ma non suriettiva; h è biiettiva.

Una funzione si dirà *suriettiva* se per ogni $y \in Y$ esiste $x \in X$ tale che $f(x) = y$, ovvero $f^{-1}(\{y\}) \neq \varnothing$ per ogni $y \in Y$ (cioè, ciascun elemento di Y è immagine di almeno un elemento di X). Una tale funzione esiste quando X è "più grande" di Y, e "proietta" X sopra tutto Y, infatti l'esempio più ovvio di funzione suriettiva è la mappa costante di un insieme X dentro un insieme con un solo elemento.

Una funzione che sia contemporaneamente iniettiva e suriettiva si dirà essere *biiettiva*, oppure una *biiezione*: essa "identifica" gli insiemi X e Y, perché ogni $y \in Y$ è raggiunto tramite f da uno e soltanto un elemento di X. In tal caso, si potrà definire la funzione *inversa* $f^{-1} : Y \to X$ che associa ad ogni $y \in Y$ il corrispondente $x \in X$ tale che $f(x) = y$, e si avrà allora $f^{-1} \circ f = \mathrm{id}_X$ e $f \circ f^{-1} = \mathrm{id}_Y$. Si faccia attenzione a non confondere il simbolo "f^{-1}" dell'antiimmagine (che si può sempre usare per ogni f) col simbolo "f^{-1}" della funzione inversa (che ha senso se e solo se f è biiettiva).

Funzione inversa

Esempi. **(1)** La funzione $f : X = \{a, b, c, d\} \to Y = \{1, 2, 3\}$ descritta in precedenza non è iniettiva (infatti $a \neq c$ ma $f(a) = 2 = f(c)$) e nemmeno suriettiva (perché $f(X) = \{1, 2\} \subsetneq Y$). Invece la funzione $g : X \to Z = \{5, 6, 7, 8\}$ data da $g(a) = 7$, $g(b) = 5$, $g(c) = 8$ e $g(d) = 6$ è biiettiva, e la sua inversa è la funzione $h = g^{-1} : Z \to X$ data da $h(5) = b$, $h(6) = d$, $h(7) = a$ e $h(8) = c$. **(2)** Sia X l'insieme di tutti gli esseri umani nati dal 1800 in poi, e sia $T = \{x \in X : x \text{ ha avuto almeno un figlio naturale}\}$. La regole $f : X \to X$ (che manda x nella sua madre naturale $f(x)$) e $g : T \to X$ (che manda x nel figlio $g(x)$) non sono funzioni, e per motivi diversi: quanto a f, se x è nato nel 1801 sua madre certamente sarà nata prima del 1800, e dunque non si può definire $f(x)$, mentre per g uno stesso $x \in T$ può avere più di una immagine $g(x)$ (tante quanti i suoi figli). Come "sanare" la situazione? Il problema di f è che il suo codominio è troppo piccolo: così, se ad esempio denotiamo con Y l'insieme di *tutti* gli esseri umani, la stessa regola $f : X \to Y$ stavolta definirà una funzione (ogni persona nata dopo il 1800 viene associata ad una ed una ben individuata persona, che è la madre naturale). Il problema di g, invece, non è la mancanza di immagini, ma il fatto che esse possono essere più d'una: potremo così modificare g dicendo che essa manda $t \in T$ nel suo *primogenito* $g(t)$. Tali funzioni non sono iniettive (se x_1 e x_2 sono due persone diverse che hanno la stessa madre naturale, vale $f(x_1) = f(x_2)$, mentre il padre e la madre dello stesso figlio primogenito hanno la stessa immagine tramite g) né suriettive (l'immagine di f è composta di sole donne, e quella di g di soli primogeniti). Se $y \in Y$, $f^{-1}(y)$ è composta dall'insieme dei figli naturali di y se y è una donna con prole naturale, $f^{-1}(y) = \varnothing$ altrimenti; se $x \in X$, $g^{-1}(x)$ è composta dal padre di x, o dalla madre, o da entrambi se x è stato il primogenito di proprio padre, o della madre, o di entrambi, $g^{-1}(x) = \varnothing$ altrimenti. La funzione composta $f \circ g : T \to Y$ manda t nella madre naturale del proprio primogenito: pertanto, se si considera il sottoinsieme $A = \{t \in T : t \text{ è una madre con prole naturale}\}$, allora la restrizione $h = (f \circ g)|_A : A \to Y$ soddisfa $h(t) = t$, ovvero h è la naturale mappa di inclusione di A dentro Y. **(3)** Altro esempio: se Y è l'insieme di tutti gli esseri umani e $Z \subset Y$ è l'insieme degli esseri umani nati in Sicilia, definiamo $f : Y \to Z$ ponendo $f(y) = y$ se y è nato in Sicilia (dunque se $y \in Z$) e $f(y)$ uguale a "Pippo Baudo" altrimenti. Tale f è una funzione suriettiva ma non iniettiva, perché tutti i "non siculi" vengono mandati in Pippo Baudo. La restrizione $f|_Z$ coincide con id_Z; se $z \in Z$, l'antimmagine $f^{-1}(z)$ è composta dal solo z se questo è un siculo diverso da Pippo Baudo, mentre $f^{-1}(\text{Pippo Baudo})$ è composta da Pippo Baudo e da tutti i "non siculi". **(4)** Sia $f : \mathbb{Q} \to \mathbb{Q}$ data da $f(x) = x^2 + 1$: si tratta di una funzione, né iniettiva (vale $f(1) = f(-1) = 2$) né suriettiva (-5 non fa parte dell'immagine di f, ma nemmeno 3: è così, come sappiamo e come rivedremo tra breve, che sono nati i numeri reali). Invece, posti $A = \mathbb{Q}_{<0}$ e $B = \mathbb{Q}_{>1}$, si ha che $g = f|_A : A \to \mathbb{Q}$ è iniettiva, e $h = f|_A^B : A \to B$ è biiettiva, con inversa $h^{-1}(y) = -\sqrt{y - 1}$ (per ottenerla, basta ricavare l'unica $x \in A$ dall'espressione $y = x^2 + 1$ ove $y \in B$). **(5)** La tangente tg è una biiezione tra $X =]-\frac{\pi}{2}, \frac{\pi}{2}[$ e $Y = \mathbb{R}$, e l'inversa, come detto, è l'arco-tangente arctg.

Metodo della fibra

Data una funzione $f : X \to Y$, il *metodo della fibra* consiste nel calcolare la fibra $f^{-1}(y) \subset X$ al variare di $y \in Y$, ed è un modo molto utile per la verifica concreta di iniettività e suriettività, per il calcolo (ove possibile) della funzione inversa, e per il calcolo dell'immagine di sottoinsiemi del dominio. Si tenga presente che di solito queste sono le cose di più difficile gestione, mentre invece ad esempio il calcolo delle antiimmagini è spesso un conto meccanico. Vediamo come questo metodo si mette in pratica nel seguente esercizio, in cui la semplicità della funzione considerata permette di svolgere i conti in modo completo e di concentrarsi sui concetti.

Esercizio. *Data la funzione* $f : \mathbb{R} \to \mathbb{R}$ *definita da* $f(x) = x^2 - 2x - 3$ *calcolare* $f^{-1}(]0, 5])$ *e*

$f([-2,2[)$. *Dire poi se f è iniettiva, se è suriettiva, e calcolare ove possibile (eventualmente dopo aver ristretto e coristretto f in modo opportuno per renderla biiettiva) la funzione inversa f^{-1}. Infine tracciare il grafico di f, e dare un'interpretazione geometrica dei risultati ottenuti.*

Risoluzione. Il calcolo dell'antiimmagine $f^{-1}(]0,5]) = \{x \in \mathbb{R} : f(x) \in]0,5]\}$ equivale a risolvere il sistema $0 < f(x) \le 5$, ovvero $\begin{cases} x^2-2x-3 > 0 \\ x^2-2x-3 \le 5 \end{cases}$, che dà $-2 \le x < 0$ oppure $3 < x \le 4$: perciò $f^{-1}(]0,5]) = [-2,0[\cup]3,4]$; per le altre domande usiamo il metodo della fibra. Fissato un certo $y \in \mathbb{R}$ nel codominio si ha $f^{-1}(y) = \{x \in \mathbb{R} : f(x) = y\} = \{x \in \mathbb{R} : x^2 - 2x - 3 - y = 0\}$: ora l'equazione $x^2 - 2x - 3 - y = 0$ (nell'incognita x) ha soluzioni se e solo se $\Delta = 4 - 4(-3-y) = 4(y+4) \ge 0$, ovvero se e solo se $y \ge -4$: dunque se $y < -4$ si ha $f^{-1}(y) = \varnothing$, il che mostra che f non è suriettiva (gli $y < -4$ non sono raggiunti da alcun x del dominio tramite f). Se invece $y = -4$ si ottiene la sola soluzione $x = 1$ (dunque $f^{-1}(-4) = \{1\}$), mentre se $y > -4$ si ottengono due soluzioni distinte $x_1(y) = 1 - \sqrt{y+4}$ e $x_2(y) = 1 + \sqrt{y+4}$ (dunque $f^{-1}(y) = \{x_1(y), x_2(y)\}$): e quest'ultimo fatto mostra che f non è nemmeno iniettiva (gli $y > -4$ sono raggiunti da due distinti elementi del dominio tramite f). Per riuscire a invertire f bisognerà prima renderla biiettiva, ovvero far sì che ogni y del codominio abbia esattamente un x tale che $f(x) = y$, ovvero —in termini di fibra— far sì che la fibra di ogni y del codominio abbia uno e un solo elemento: ad esempio, corestringendo f ai soli $y \ge -4$ le fibre diventano non vuote, dunque essa diventa suriettiva; mentre, notando che $x_1(y) < 1 < x_2(y)$, restringendo f ai soli $x \ge 1$ le fibre avranno il solo elemento $x_2(y)$ (si noti che $x_1(-4) = x_2(-4) = 1$): pertanto, così ristretta e coristretta, f diventa biietiva, e la sua inversa è proprio $x_2 : [-4,+\infty[\to [1,+\infty[$. Un'altra scelta possibile sarebbe stata quella di restringere f ai soli $x \le 1$ (e di corestringerla ancora agli $y \ge -4$): in tal caso l'inversa sarebbe stata $x_1(y)$. Se si disegna il grafico di f, ovvero la parabola $y = x^2 - 2x - 3$, tutto quanto trovato appare evidente.

Esercizio. *Se X e Y sono due insiemi finiti con rispettivamente m e n elementi, quante sono, in tutto, le funzioni di X in Y? E quelle iniettive? E quelle biiettive? (Facoltativo: E quelle suriettive?)*

Risoluzione. Tutte le funzioni da X in Y sono n^m: infatti, per ognuno degli m elementi di X si può indipendentemente scegliere l'immagine tra gli n elementi di Y. Tra queste, quelle iniettive (nel solo caso $m \le n$) sono $n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!} = m!\binom{n}{m}$: infatti, se $X = \{x_1, \dots, x_m\}$ vi sono n scelte possibili per $f(x_1)$, poi ne restano $n-1$ per $f(x_2)$ (che deve essere diversa da $f(x_1)$), e così via fino alle restanti $n-(m-1) = n-m+1$ possibili per $f(x_m)$ (che deve essere diversa da $f(x_1)$, ..., $f(x_{m-1})$). Come caso particolare, si ottiene che le biiezioni (nel solo caso $m = n$) sono $n!$, e –com'è naturale– corrispondono al numero di permutazioni di n oggetti. Invece il numero di funzioni suriettive (nel solo caso $m \ge n$) è più complicato da calcolare. Si tratta innanzitutto di ripartire X in n sottoinsiemi disgiunti e non vuoti, e ciò può essere fatto in un numero di modi dato dal *numero di Stirling* $S(m,n)$ definito induttivamente da

$$S(m,1) = S(m,m) = 1, \qquad S(m,n) = S(m-1,n-1) + n\,S(m-1,n) \qquad (\text{se } 2 \le n \le m-1);$$

poi tale numero va moltiplicato per $n!$ (infatti, a ognuno dei sottoinsiemi della partizione va assegnato come immagine un diverso elemento tra gli n di Y, e ciò si può fare in $n!$ modi diversi), ottenendo dunque $n!\,S(m,n)$ che, dopo un po' di lavoro, si dimostra essere uguale a

$$\sum_{j=0}^{n-1} (-1)^j \binom{n}{j} (n-j)^m.$$

Ad esempio per $n = 1$ si ottiene 1 (ovvio: se Y ha un solo elemento c'è la sola funzione costante), per $n = 2$ si ottiene $2^m - 2$, e così via.

Cardinalità Diamo ora un rapido cenno a come le nozioni di "iniettività" e "biiettività"

possano dare un senso generale (anche per insiemi infiniti) alla nozione di "avere lo stesso numero di elementi".

Equipotenza, cardinalità

Si dice che due insiemi A e B *hanno la stessa cardinalità* (oppure *sono equipotenti*, scrivendo $|A| = |B|$) se esiste una biiezione tra essi: è facile verificare che si tratta di una relazione di equivalenza[18]. Nel caso di insiemi finiti, l'equipotenza equivale ad avere lo stesso numero di elementi[19]; ma il maggior interesse della nozione è nel caso di insiemi infiniti, in cui può accadere ad esempio che un sottoinsieme abbia la stessa cardinalità dell'insieme in cui si trova.

Esempio. Gli insiemi $2\mathbb{N} = \{n \in \mathbb{N} : n \text{ è pari}\}$ (numeri naturali pari), $\mathbb{Z}$ (numeri interi) e $\mathbb{Q}$ (numeri razionali) hanno tutti la stessa cardinalità di $\mathbb{N}$, pur essendo rispettivamente un sottoinsieme e due sovrainsiemi di esso. Infatti una biiezione $f : \mathbb{N} \to 2\mathbb{N}$ è data da $f(n) = 2n$; una biiezione $g : \mathbb{N} \to \mathbb{Z}$ è data da $g(n) = \begin{cases} \frac{n}{2} & \text{(se } n \text{ è pari)} \\ -\frac{n-1}{2} & \text{(se } n \text{ è dispari)} \end{cases}$, ovvero $g(1) = 0$, $g(2) = 1$, $g(3) = -1$, $g(4) = 2$, $g(5) = -2$, ... Infine, per ottenere una biiezione tra $\mathbb{N}$ e $\mathbb{Q}$ si rappresentino tutti i numeri razionali scrivendoli senza ripetizioni, in forma di frazioni ridotte, in righe infinite con denominatore via via crescente, in questo modo:

$$\begin{array}{cccccccc} 0 & \frac{1}{1} & -\frac{1}{1} & \frac{2}{1} & -\frac{2}{1} & \frac{3}{1} & -\frac{3}{1} & \dots \\ \frac{1}{2} & -\frac{1}{2} & \frac{3}{2} & -\frac{3}{2} & \frac{5}{2} & -\frac{5}{2} & \frac{7}{2} & \dots \\ \frac{1}{3} & -\frac{1}{3} & \frac{2}{3} & -\frac{2}{3} & \frac{4}{3} & -\frac{4}{3} & \frac{5}{3} & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{array}$$

per poi definire $h : \mathbb{N} \to \mathbb{Q}$ percorrendo via via le antidiagonali corte a partire dall'angolo in alto a sinistra, ovvero $h(1) = 0$; $h(2) = \frac{1}{1}$, $h(3) = \frac{1}{2}$; $h(4) = -\frac{1}{1}$, $h(5) = -\frac{1}{2}$, $h(6) = \frac{1}{3}$; $h(7) = \frac{2}{1}$, $h(8) = \frac{3}{2}$, ...

Gli insiemi infiniti che hanno la stessa cardinalità di $\mathbb{N}$, come quelli dell'esempio qui sopra, si dicono *numerabili*, o che "hanno cardinalità $\aleph_0$" (ove $\aleph$ è la lettera ebraica "aleph"). Si dice anche che $\aleph_0$ è la *cardinalità dell'infinito discreto*.

Dati due insiemi A e B, si dice che A *ha cardinalità minore o uguale a* B (scrivendo $|A| \leq |B|$) se esiste una funzione iniettiva $A \to B$; in tal caso, se non esistono funzioni biiettive si dirà che A *ha cardinalità strettamente minore a* B , e si scriverà $|A| < |B|$.
Mentre l'equipotenza esprimeva in generale l'idea di "avere lo stesso numero di elementi", quest'ultima nozione esprime invece l'idea di "essere più piccolo", "avere meno elementi": infatti, se $A \subset B$ si ha automaticamente $|A| \leq |B|$ (poiché la funzione di inclusione $i : A \to B$ data da $i(x) = x$ è iniettiva). Ciò non toglie, come visto nell'esempio qui sopra, che un sottoinsieme possa essere addirittura equipotente all'insieme. In effetti, tra le varie cardinalità infinite, la cardinalità numerabile $\aleph_0$ è la più piccola, perché non è non è difficile dimostrare[20] il seguente intuitivo fatto: *se X è un insieme infinito, allora esiste una funzione iniettiva $\mathbb{N} \to X$.*
Esistono cardinalità infinite che siano più grandi di $\aleph_0$? La risposta è sì, e per vederlo iniziamo mostrando che l'insieme delle parti di un insieme è sempre più grande dell'insieme stesso:

[18] ...dove? Saremmo a portati a dire *nell'insieme di tutti gli insiemi*, ma questa nozione porterebbe a problemi di logica, nei quali non vogliamo entrare, che obbligano a parlare di una nozione estesa come quella di *classe di tutti gli insiemi*.

[19] si veda infatti l'esercizio qui sopra: esistono biiezioni tra X e Y se e solo se $m = n$.

[20] usando il cosiddetto *assioma della scelta*, per cui rimandiamo a testi più completi.

Proposizione 1.1.1. *Se X è un insieme, allora $|X| < |\mathcal{P}(X)|$.*

Dimostrazione. L'ovvia funzione iniettiva $i : X \to \mathcal{P}(X)$ data da $i(x) = \{x\}$ mostra che $|X| \leq |\mathcal{P}(X)|$: ci resta da mostrare che una funzione iniettiva $f : X \to \mathcal{P}(X)$ non può mai essere biiettiva, ovvero non può mai essere anche suriettiva. In effetti, definiamo $A = \{x \in X : x \notin f(x)\}$: qualunque cosa sia, di certo A è un sottoinsieme di X, ovvero $A \in \mathcal{P}(X)$, e mostriamo che A non può stare nell'immagine $f(X)$ di f (il che dimostra che f non può essere suriettiva). Supponiamo per assurdo che $A \in f(X)$: allora esiste $x_0 \in X$ tale che $A = f(x_0)$. Ora, vi sono due possibilità: $x_0 \in A$ oppure $x_0 \notin A$. Se fosse $x_0 \in A$ si avrebbe $x_0 \notin f(x_0) = A$, assurdo; se invece fosse $x_0 \notin A$ si avrebbe $x_0 \in f(x_0) = A$, pure assurdo. La dimostrazione è terminata. □

Se X è un insieme finito (diciamo con n elementi) già sappiamo che $|X| = n < 2^n = |\mathcal{P}(X)|$; ciò che afferma la Proposizione 1.1.1 è che ciò vale sempre, e in particolare per $X = \mathbb{N}$: dunque $\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$. Si può dimostrare che $\mathcal{P}(\mathbb{N})$ è equipotente all'insieme $\mathbb{R}$ dei numeri reali: la cardinalità $\aleph_1$ di $\mathcal{P}(\mathbb{N})$ (dunque anche di $\mathbb{R}$) esprime la *cardinalità dell'infinito continuo*, ed è strettamente più grande di $\aleph_0$.

1.2 Strutture algebriche fondamentali: gruppi, anelli, corpi, spazi vettoriali

Prima di parlare dei numeri reali e complessi, è utile dare alcuni cenni (che saranno sviluppati nel seguito degli studi, in questo corso e negli altri) sulle proprietà algebriche generali di insiemi dotati di una o più operazioni: in questo modo, guardando le cose un po' dall'alto, ci si potrà meglio rendere conto di che cosa si voglia costruire, e dove si riesca effettivamente ad arrivare.

Operazioni e gruppi La nozione di *operazione* (binaria) ci è nota ormai da lungo tempo: è una regola che, dati due numeri, ne fa saltare fuori un terzo, detto "risultato". Guardiamo ad esempio l'addizione in $\mathbb{Z}$: essa gode di proprietà interessanti, perché è associativa, ha un elemento speciale (lo 0) che sommato a qualsiasi altro lo lascia inalterato, e inoltre, dato un qualsiasi numero intero r ce n'è un altro che, sommato a lui, fa tornare daccapo a 0 (naturalmente, stiamo parlando dell'"opposto" $-r$). La moltiplicazione in $\mathbb{Z}$, invece, è anch'essa associativa, anch'essa ha un elemento (l'1) che lascia inalterati gli altri, ma dato un numero intero r, a meno che non sia $r = \pm 1$ non c'è in $\mathbb{Z}$ un altro numero che, moltiplicato per lui, ci dia 1 (è proprio per questo, d'altronde, che si è creato $\mathbb{Q}$).
Le definizioni che seguono sono solo la generalizzazione di queste idee ad un qualsiasi insieme munito di operazione.

Operazione

Sia G un insieme non vuoto. Un'*operazione* (binaria) su G è una funzione $* : G \times G \to G$: ovvero, ad ogni coppia (x_1, x_2) di elementi di G si associa un elemento (*risultato*) $x_1 * x_2$ di G. Un'operazione "$*$" può avere o meno le seguenti proprietà notevoli:

(Gr_1) *Associatività*: $(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$ per ogni $x_1, x_2, x_3 \in G$;

(Gr_2) *Esistenza dell'elemento neutro*: esiste $e \in G$, detto "elemento neutro per "$*$" in G",

tale che $x * e = e * x = x$ per ogni $x \in G$ (se esiste, tale e è evidentemente unico)[21];

(Gr_3) *Invertibilità* (se vale (Gr_2)): per ogni $x \in G$ esiste $x' \in G$ tale che $x * x' = x' * x = e$ (se vale anche (Gr_2) tale inverso, se esiste, è unico, e si denota con x^{-1});[22]

(Gr_4) *Commutatività*: $x_1 * x_2 = x_2 * x_1$ per ogni $x_1, x_2 \in G$.

Gruppo

Se "$*$" soddisfa (Gr_1), la coppia $(G, *)$ si dirà un *semigruppo*; se soddisfa (Gr_1)-(Gr_2), si dirà *monoide*; se soddisfa (Gr_1)-(Gr_2)-(Gr_3), si dirà *gruppo*; se una di queste strutture soddisfa anche (Gr_4), si aggiungerà l'aggettivo *commutativo*[23].

Proposizione 1.2.1. *In un gruppo* $(G, *)$ *vale la* regola della cancellazione*:*

$$\text{se } \ x * y = x * z \ \text{ oppure se } \ y * x = z * x \ \text{ allora } \ y = z\,. \tag{1.1}$$

Dimostrazione. Se $x * y = x * z$ allora $x^{-1} * (x * y) = x^{-1} * (x * z)$, da cui $(x^{-1} * x) * y = (x^{-1} * x) * z$, da cui $e * y = e * z$, da cui $y = z$; idem se $y * x = z * x$, operando con x^{-1} dall'altra parte. □

Sottogruppo

Sia $(G, *)$ un gruppo. Un sottoinsieme $H \subset G$ si dirà *sottogruppo* se per ogni $x \in H$ si ha $x^{-1} \in H$ e per ogni $x, y \in H$ si ha $x * y \in H$ (ovvero, H è "chiuso" rispetto all'operazione "$*$" ed all'inversione)[24]; è allora chiaro che anche $(H, *)$ è un gruppo (ove si continua ad indicare con "$*$" l'operazione "$*$" indotta su H).

Esempi. (0) Se $(G, *)$ è un gruppo di elemento neutro e, G ha sempre due sottogruppi ovvi: G (se stesso), ed $\{e\}$ (detto anche sottogruppo *banale*). Dati due gruppi $(G_1, *_1)$ e $(G_2, *_2)$, il gruppo *prodotto diretto* è il prodotto cartesiano $G_1 \times G_2$ munito della naturale operazione $(x, y) * (x', y') = (x *_1 x', y *_2 y')$; G_1 (risp. G_2) si identifica col sottogruppo $G_1 \times \{e_2\}$ (risp. $\{e_1\} \times G_2$). **(1)** $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}^\times, \cdot)$ e $(\mathbb{Z}, \cdot)$ sono semigruppi; gli ultimi tre sono anche monoidi. Tutti sono commutativi. **(2)** $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^\times, \cdot)$ sono gruppi commutativi. $(\mathbb{Z}, +)$ è un sottogruppo di $(\mathbb{Q}, +)$; $(\{\pm 1\}, \cdot)$ e $(\mathbb{Q}_{>0}, \cdot)$ sono sottogruppi di $(\mathbb{Q}^\times, \cdot)$; invece il sottoinsieme $\{x \in \mathbb{Q} : 0 < x \leq 1\}$ non è un sottogruppo di $(\mathbb{Q}_{>0}, \cdot)$, perché è chiuso per la moltiplicazione (cioè, se $x, y \in A$ anche $xy \in A$) ma non per il passaggio all'inverso (infatti se $x \in A$ e $x \neq 1$ allora $\frac{1}{x} \notin A$). I sottogruppi di $(\mathbb{Z}, +)$ sono tutti e soli i sottoinsiemi $n\mathbb{Z} = \{nr : r \in \mathbb{Z}\}$ con $n \in \mathbb{Z}$. **(3)** Sia $\mathbb{Z}[x]$ l'insieme dei polinomi a coefficienti in $\mathbb{Z}$: allora $(\mathbb{Z}[x], +)$ è un gruppo commutativo, e $(\mathbb{Z}[x], \cdot)$ un monoide commutativo. Il sottoinsieme $\mathbb{Z}[x]_{\leq m}$ formato dai polinomi di grado $\leq m$ è un sottogruppo di $(\mathbb{Z}[x], +)$. Idem con $\mathbb{Q}$ al posto di $\mathbb{Z}$, o con più variabili. **(4)** Sia X un insieme, e sia $G = \{f : X \to X\}$ l'insieme delle funzioni da X in sè: allora $(G, \cdot)$ (ove "$\cdot$" denota la composizione $f \cdot g = g \circ f$) è un monoide, non commutativo. Considerando il suo sottoinsieme G' dato dalle biiezioni di X in sè, $(G', \cdot)$ diventa un gruppo non commutativo. Un caso particolare è quello in cui X è un insieme finito (diciamo $X = \{1, \dots, n\}$), in cui G' viene detto gruppo delle *permutazioni di n oggetti*, un ente di importanza fondamentale nel calcolo combinatorio. Ad esempio, consideriamo le due permutazioni σ e τ di $X = \{1, 2, 3\}$ date da $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 2$, $\tau(1) = 3$, $\tau(2) = 1$ e $\tau(3) = 2$: allora $(\sigma \cdot \tau)(1) = \tau(\sigma(1)) = 3$, $(\sigma \cdot \tau)(2) = 2$ e $(\sigma \cdot \tau)(3) = 1$, mentre $(\tau \cdot \sigma)(1) = \sigma(\tau(1)) = 2$, $(\tau \cdot \sigma)(2) = 1$ e

[21] Se e ed e' sono due elementi neutri per "$*$", allora $e = e * e' = e'$.

[22] Se x'_1 e x'_2 sono entrambi inversi di x, si ha $x'_1 = x'_1 * e = x'_1 * (x * x'_2) = (x'_1 * x) * x'_2 = e * x'_2 = x'_2$.

[23] o *abeliano*, dal nome del matematico Abel.

[24] È anche facile dimostrare che, equivalentemente, H è un sottogruppo se per ogni $x, y \in H$ si ha $x * (y^{-1}) \in H$ (ovvero, H è "chiuso" rispetto alla "divisione").

$(\tau\cdot\sigma)(3)=3$, e dunque $\sigma\cdot\tau\neq\tau\cdot\sigma$. **(5)** Dati due sottoinsiemi A e B di un insieme X, si definisca la loro *differenza simmetrica* come $A\Delta B=(A\setminus B)\sqcup(B\setminus A)=(A\cup B)\setminus(A\cap B)$: verificare che allora $(\mathcal{P}(X),\Delta)$ è un gruppo commutativo (ove si ricorda che $\mathcal{P}(X)$ rappresenta l'insieme delle parti di X).

Morfismo di gruppi

Siano $(G_1,*_1)$ e $(G_2,*_2)$ due gruppi con elementi neutri e_1 ed e_2 rispettivamente. Una funzione $f:G_1\to G_2$ si dirà *morfismo* (o *omomorfismo*) se essa rispetta le operazioni, ovvero se $f(x*_1x')=f(x)*_2f(x')$ per ogni $x,x'\in G_1$ (si noti che, allora, dev'essere $f(e_1)=e_2$ e $f(x^{-1})=f(x)^{-1}$). Se f è un morfismo, si vede facilmente che $\ker(f)=f^{-1}(e_2)=\{x\in G_1:f(x)=e_2\}\subset G_1$ (*nucleo* di f) e $\mathrm{im}(f)=f(G_1)=\{f(x):x\in G_1\}\subset G_2$ (*immagine* di f) sono sottogruppi rispettivamente di G_1 e G_2. La domanda naturale è: dati due gruppi $(G_1,*_1)$ e $(G_2,*_2)$ qualsiasi, esistono morfismi tra essi? Uno, banale, c'è sempre, ed è la funzione costante con valore e_2; non è detto però che ve ne siano altri. Un caso particolarmente importante è quando si riesce a trovare un morfismo biiettivo di gruppi (che si dice *isomorfismo*), perché esso identifica i due gruppi: infatti, oltre a "renderli uguali" come insiemi ne rispetta le operazioni durante il passaggio da una parte all'altra (in questo caso è d'uso denotare $f:G_1\xrightarrow{\sim}G_2$, e dire che i gruppi G_1 e G_2 sono *isomorfi*). In particolare, se $G_1=G_2=G$ si parla di *automorfismi* del gruppo G.

Una particolare classe di automorfismi di G sono le cosiddette *coniugazioni* per un prefissato elemento: preso un $g\in G$, si ha il morfismo $c_g:G\to G$ dato da $c_g(x)=g*x*g^{-1}$ (per $g=e$ si ha l'identità id_G; ed è chiaro che se G è un gruppo commutativo allora $c_g=\mathrm{id}_G$ per ogni $g\in G$). Un sottogruppo H di $(G,*)$ si dirà *normale* (o *invariante*) se esso viene conservato da tutte le coniugazioni, ovvero se $c_g(H)=H$ per ogni $g\in H$: in altre parole, se per ogni $g\in G$ ed ogni $h\in H$ esiste un $h'\in H$ tale che $g*h*g^{-1}=h'$. (Ad esempio, si verifichi se $f:G_1\to G_2$ è un morfismo allora $\ker(f)$ è un sottogruppo normale di G_1.)[(25)] (È chiaro che, se G è commutativo, tutte le coniugazioni sono uguali all'identità, e dunque tutti i sottogruppi di G sono normali.)

Gruppo quoziente

Se H è normale in G, si può costruire un nuovo gruppo G/H a partire da G e H, detto *gruppo quoziente* di G rispetto ad H: l'idea è di "dividere G per H", facendo diventare quest'ultimo come un grosso elemento neutro al fine di "ragionare in G "modulo" (cioè, a meno di) H". Introduciamo dunque una relazione $\mathcal{R}$ in G dicendo che $g\mathcal{R}g'$ se esiste $h\in H$ tale che $g'=g*h$, ovvero se $g'*g^{-1}\in H$: è facile vedere che si tratta di una relazione d'equivalenza (vedi pag. 29). Le classi d'equivalenza, che sono i sottoinsiemi $g*H=\{g*x:x\in H\}$ al variare di g in G, sono dette *classi laterali destre* in G modulo H Nell'insieme delle classi d'equivalenza $G/H=\{g*H:g\in G\}$ definiamo poi un'operazione ponendo semplicemente $(g_1*H)*(g_2*H)=(g_1*g_2)*H$. Il problema è essenzialmente di vedere che questa sia una "buona definizione", cioè che se si rimpiazzano g_1 e g_2 con $g_1'=g_1*h_1$ e $g_2'=g_2*h_2$ (senza dunque cambiare le classi laterali) il risultato del prodotto non cambia: ed è qui che entra in modo decisivo il fatto che H è normale[(26)]

[(25)] Infatti, se $g\in G_1$ e $h\in\ker(f)$ si ha $g*_1h*_1g^{-1}\in\ker(f)$, perché $f(g*_1h*_1g^{-1})=f(g)*_2f(h)*_2f(g^{-1})=f(g)*_2e_2*_2f(g)^{-1}=f(g)*_2f(g)^{-1}=e_2$.

[(26)] Siano infatti $g_1'=g_1*h_1$ e $g_2'=g_2*h_2$: come detto, essendo $g_1'*H=g_1*H$ e $g_2'*H=g_2*H$, bisognerà che valga anche $(g_1'*H)*(g_2'*H)=(g_1*H)*(g_2*H)$, altrimenti l'operazione in G/H sarebbe mal definita. Poiché H è normale, esiste $h'\in H$ tale che $(g_2)^{-1}*h_1*g_2=h'$, ovvero (moltiplicando ambo i membri per g_2) tale che $h_1*g_2=g_2*h'$: allora $(g_1'*H)*(g_2'*H)=(g_1'*g_2')*H=(g_1*h_1*g_2*h_2)*H=$

L'importanza di questa costruzione diventa evidente nel *Teorema di Omomorfismo*, che dice: *un morfismo di gruppi* $f : G_1 \to G_2$ *induce un isomorfismo di gruppi* $G_1/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$ *ponendo* $f(x*\ker(f)) = f(x)$; in particolare, se f è un morfismo suriettivo si ottiene $G_1/\ker(f) \xrightarrow{\sim} G_2$, ovvero, la presenza di un morfismo suriettivo da G_1 a G_2 permette di descrivere il gruppo G_2 tramite un *quoziente* del gruppo G_1.

Esempi. (1) Se $(G, *)$ è un gruppo e $g \in G$, si possono definire le funzioni *traslazione* (sinistra) $\tau_g : G \to G$ e *coniugazione* $c_g : G \to G$ tramite $\tau_g(x) = gx$ e $c_g(x) = gxg^{-1}$. Esse sono biiezioni di G in sè, e come visto c_g è anche un automorfismo di G; invece, τ_g è un morfismo di G in sè se e solo se $g = e$ (nel qual caso $\tau_g = \mathrm{id}_G$), perché $\tau_g(x * y) = \tau_g(x) * \tau_g(y)$ per ogni $x, y \in G$ significa $g * x * y = g * x * g * y$, da cui (cancellando) $g = e$. **(2)** Se H è un sottogruppo di $(G, *)$, la funzione di *inclusione* $H \to G$ è un morfismo di gruppi. **(3)** In $(\mathbb{Z}, +)$, le moltiplicazioni per un dato numero intero n sono morfismi; in realtà questi sono tutti e soli i morfismi di $(\mathbb{Z}, +)$ in sè. **(4)** Per un fissato $n \in \mathbb{Z}$, la funzione di *valutazione* $v_n : \mathbb{Z}[x] \to \mathbb{Z}$, che manda un polinomio $p(x) \in \mathbb{Z}[x]$ nel numero intero $v_n(p) = p(n)$, è un morfismo di $(\mathbb{Z}[x], +)$ in $(\mathbb{Z}, +)$. **(5)** Come vedremo tra breve, denotati con $\mathbb{R}$ i numeri reali e con $\mathbb{R}_0$ i numeri reali positivi, $(\mathbb{R}, +)$ e $(\mathbb{R}_{>0}, \cdot)$ sono gruppi commutativi: è allora chiaro che l'esponenziale $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ è un morfismo tra essi (in realtà, un isomorfismo). **(6)** Diamo qualche esempio di gruppo quoziente. Abbiamo detto che i sottogruppi di $(\mathbb{Z}, +)$ sono i sottoinsiemi $n\mathbb{Z}$ per $n \in \mathbb{Z}$: poiché siamo nel caso commutativo, i sottogruppi sono normali, ed si può considerare il gruppo quoziente $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{r + n\mathbb{Z} : r \in \mathbb{Z}\}$: si tratta di un gruppo finito con n elementi, detto il gruppo degli *interi modulo* n perché in esso gli interi vengono identificati quando differiscono per multipli di n: ad esempio, in $\frac{\mathbb{Z}}{12\mathbb{Z}}$ i numeri $-11, 1, 13, 121$ vengono tutti confusi nella medesima classe $1 + 12\mathbb{Z} = 13 + 12\mathbb{Z} = \cdots$.[27] Altro esempio: $(\mathbb{R}^\times, \cdot)$ è un gruppo abeliano, e sia $(\mathbb{R}_{>0}, \cdot)$ che $(\{\pm 1\}, \cdot)$ sono suoi sottogruppi. La funzione $f : \mathbb{R}^\times \to \mathbb{R}_{>0}$ data da $f(x) = |x|$ è un morfismo suriettivo, con nucleo $\ker(f) = \{\pm 1\}$: per il Teorema di Omomorfismo, il gruppo $\mathbb{R}_{>0}$ è isomorfo al gruppo quoziente $\frac{\mathbb{R}^\times}{\{\pm 1\}}$ (nel quale, infatti, si "ragiona a meno del segno").

Anelli e corpi Sia gli interi $\mathbb{Z}$ che i razionali $\mathbb{Q}$ hanno a disposizione due operazioni (somma e prodotto) che vanno d'accordo tra loro (la seconda è "distributiva" sulla prima); tuttavia, in $\mathbb{Q}$ le cose sembrano andare un po' meglio che in $\mathbb{Z}$, perché ci sono tutti i reciproci (cioè, inversi rispetto al prodotto) dei numeri non nulli. Andiamo dunque a descrivere in generale la situazione di un insieme su cui esistono due operazioni, tenendo bene a mente gli esempi appena dati.

Sia R un insieme dotato di due operazioni $+$ (detta *somma*) e $\cdot$ (detta *prodotto*). Consideriamo le seguenti possibili proprietà per la struttura $(R, +, \cdot)$:

(An_1) $(R, +)$ sia un gruppo commutativo (con elemento neutro denotato 0 e inverso di un elemento x denotato $-x$, e detto *opposto* di x);

(An_2) $(R, \cdot)$ sia un semigruppo;

(An_3) *Distributività*: $(x_1 + x_2) \cdot x' = (x_1 \cdot x') + (x_2 \cdot x')$ e $x' \cdot (x_1 + x_2) = (x' \cdot x_1) + (x' \cdot x_2)$ per ogni $x_1, x_2, x' \in R$;

$(g_1 * h_1 * g_2) * H = (g_1 * g_2 * h') * H = (g_1 * g_2) * H = (g_1 * H) * (g_2 * H)$, come si voleva.

[27] È quello che si fa quando si guarda l'orologio confondendo 13 con 1.

(An_4) *Unitarietà*: esiste un elemento neutro per $\cdot$, denotato 1 (se allora un elemento $x \in R$ ammette inverso x^{-1} rispetto a $\cdot$, tale inverso sarà anche detto *reciproco* di x);

(An_5) *Commutatività*: l'operazione $\cdot$ sia commutativa.

Anello

Se soddisfa (An_1)-(An_2)-(An_3), la terna $(R, +, \cdot)$ si dirà un *anello*; se soddisfa (An_1)-(An_2)-(An_3)-(An_4), si dirà *anello unitario*, o *con unità*; se soddisfa anche (An_5), si aggiungerà l'aggettivo *commutativo*. Si noti che in un anello $(R, +, \cdot)$ vale[(28)]

$$0 \cdot x = x \cdot 0 = 0 \qquad \text{per ogni } x \in R\ .$$

Sottoanello, ideale

Sia $(R, +, \cdot)$ un anello. Un sottoinsieme $A \subset R$ si dirà *sottoanello* se A è un sottogruppo di $(R, +)$ chiuso rispetto all'operazione "$\cdot$"; in particolare, esso si dirà *ideale* sinistro (risp. destro) se è un sottoanello dotato della "proprietà di assorbimento" a sinistra (risp. a destra), ovvero se per ogni $x \in R$ e $a \in A$ si ha $x \cdot y \in A$ (risp. $y \cdot x \in A$). Un ideale sia sinistro che destro si dirà "bilatero" (ovviamente le nozioni distinte di ideale sinistro e destro hanno interesse nel caso di anelli non commutativi).

Morfismo di anelli

Un *morfismo di anelli* tra $(R_1, +_1, \cdot_1)$ e $(R_2, +_2, \cdot_2)$, è un morfismo $f : (R_1, +_1) \to (R_2, +_2)$ che rispetta anche le moltiplicazioni, ovvero tale che $f(x \cdot_1 x') = f(x) \cdot_2 f(x')$ per ogni $x, x' \in R_1$; se f è anche biiettiva si dirà *isomorfismo*, e due anelli tra i quali esiste un isomorfismo si diranno *isomorfi*. Si dimostra facilmente che il nucleo (rispetto a $+$) di un morfismo di anelli è un ideale bilatero del dominio, e che l'immagine è un sottoanello del codominio.

Corpo, campo

Un anello unitario $(k, +, \cdot)$ che soddisfa

(Cp) *Invertibilità*: Ogni $x \neq 0$ è invertibile rispetto a $\cdot$ (ovvero, denotando $k^\times = k \setminus \{0\}$, si ha che $(k^\times, \cdot)$ è un gruppo)

si dirà *corpo*; nel caso di corpo commutativo si usa anche il termine *campo*. In un corpo vale la seguente fondamentale proprietà:

Proposizione 1.2.2. (Legge dell'annullamento del prodotto) *Sia k un corpo. Se $x, y \in k$, si ha $x \cdot y = 0$ se e solo se $x = 0$ oppure $y = 0$.*

Dimostrazione. Si abbia $x \cdot y = 0$, ovvero $x \cdot y = x \cdot 0$. Se $x = 0$, siamo a posto; se invece $x \neq 0$ allora basta applicare la regola della cancellazione (1.1). □

Corpo totalmente ordinato

Se si ha un corpo commutativo k dotato di un ordine totale "$\leq$" (ovvero, che soddisfa (Rifl)-(ASym)-(Trns)-(Tot)), si dirà che $(k, +, \cdot, \leq)$ è un *corpo commutativo totalmente ordinato* se soddisfa anche alle seguenti due proprietà di compatibilità dell'ordine con le operazioni:

(CpO_1) se $x_1, x_2 \in k$ e $x_1 \leq x_2$, allora per ogni $x \in k$ vale $x_1 + x \leq x_2 + x$;

[(28)] infatti $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ da cui, cancellando, $x \cdot 0 = 0$.

(CpO_2) se $x_1, x_2 \in k$ e $x_1 \leq x_2$, allora per ogni $x \in k$ tale che $x \geq 0$ vale $x \cdot x_1 \leq x \cdot x_2$.

Esempi. (1) $(\mathbb{Z}, +, \cdot)$ è un anello unitario commutativo. **(2)** I numeri razionali $(\mathbb{Q}, +, \cdot)$, i reali $(\mathbb{R}, +, \cdot)$ e (come vedremo) i numeri complessi $(\mathbb{C}, +, \cdot)$ sono dei campi; i primi due sono anche totalmente ordinati, e sono sottocampi dell'ultimo. **(3)** Fissato un numero naturale $n \in \mathbb{N}$, si è già visto che l'insieme (di n elementi) delle classi di resto $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{r} := r + n\mathbb{Z} : r \in \mathbb{Z}\}$ è un gruppo commutativo con l'operazione di somma; se dotato anche del prodotto, esso diventa una anello commutativo unitario. Ad esempio, in $\frac{\mathbb{Z}}{15\mathbb{Z}}$ si ha $\overline{7} + \overline{9} = \overline{1}$, $\overline{6} \cdot \overline{8} = \overline{3}$ e $\overline{3} \cdot \overline{5} = \overline{0}$: si ricordi infatti che si sta ragionando "modulo 15", ovvero si confondono i numeri che differiscono per multipli di 15. L'ultima uguaglianza ci mostra che $\frac{\mathbb{Z}}{15\mathbb{Z}}$ non può essere un campo, perché nega la legge dell'annullamento (Proposizione 1.2.2): in effetti, non è difficile mostrare che che $\frac{\mathbb{Z}}{n\mathbb{Z}}$ è un campo se e solo se n è un numero primo.[29] **(4)** $(\mathbb{Z}[x], +, \cdot)$ è un anello unitario commutativo, e per ogni $n \in \mathbb{Z}$ le valutazioni $v_n : \mathbb{Z}[x] \to \mathbb{Z}$ (con $v_n(p) = p(n)$) sono morfismi di anello. **(5)** La moltiplicazione per n è un morfismo di gruppo per $(\mathbb{Z}, +)$, ma è un morfismo di anello per $(\mathbb{Z}, +, \cdot)$ se e solo se $n = 0, 1$. **(6)** Come visto, dato un insieme X si ha che $(\mathcal{P}(X), \Delta)$ è un gruppo commutativo; si verifichi anche che $(\mathcal{P}(X), \Delta, \cap)$ è un anello commutativo con unità. **(7)** Dato un insieme X ed un anello $(R, +, \cdot)$, l'insieme $R^X = \{f : X \to R\}$ è un anello definendo $f + g$ e $f \cdot g$ "puntualmente", ovvero $(f + g)(x) = f(x) + g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$. Se $T \subset X$ è un sottoinsieme qualsiasi, il sottoinsieme $R^X_T = \{f : X \to R : f(x) = 0 \text{ per ogni } x \in T\}$ è un ideale bilatero di R^X. Scegliamo ora $X = R = \mathbb{R}$, e consideriamo $\mathbb{R}^{\mathbb{R}}$: allora $\mathbb{R}[x]$ (anello dei polinomi) può essere visto come sottoinsieme di $\mathbb{R}^{\mathbb{R}}$, e come tale è un sottoanello ma non un ideale di $\mathbb{R}^{\mathbb{R}}$.[30] **(8)** Se $(G, *)$ è un gruppo *commutativo*, l'insieme $\mathrm{End}(G)$ costituito dai morfismi $f : G \to G$ è un anello ponendo $(f + g)(x) = f(x) * g(x)$ e $(f \cdot g)(x) = (g \circ f)(x) = g(f(x))$: si chiamerà *anello degli endomorfismi* del gruppo abeliano G. In generale, $\mathrm{End}(G)$ non è commutativo: ad esempio, considerando il gruppo abeliano additivo $G = \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ ed i morfismi $f(m, n) = (n, m)$ e $g(m, n) = (-m, 2n)$, si ha $(f \cdot g)(m, n) = g(f(m, n)) = (-n, 2m)$ mentre $(g \cdot f)(m, n) = f(g(m, n)) = (2n, -m)$, e dunque $f \cdot g \neq g \cdot f$.[31]

Spazi vettoriali Uno *spazio vettoriale* su un corpo k (o un *k-spazio vettoriale*) è un gruppo commutativo $(V, +)$ munito di una "moltiplicazione per scalari" **Spazio vettoriale**

$$k \times V \to V\,, \qquad (\lambda, v) \mapsto \lambda v$$

che sia compatibile con la somma $+$, ovvero tale che

[29] La condizione è necessaria: infatti se n non è un numero primo, scritto $n = ab$ con $a \neq 1$ e $b \neq 1$ si ha che $\overline{a}\overline{b} = \overline{n} = \overline{0}$, il che nega la legge dell'annullamento (ad esempio, nel precedente caso $n = 15$ si erano presi $a = 3$ e $b = 5$). Viceversa, supponiamo che n sia primo, e consideriamo un naturale $m \in \{1, \ldots, n-1\}$: dobbiamo trovare un altro naturale $x \in \{1, \ldots, n-1\}$ tale che $\overline{m}\,\overline{x} = \overline{1}$. A tal fine, se riuscissimo a dimostrare che la funzione $f_m : \frac{\mathbb{Z}}{n\mathbb{Z}} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ data dalla "moltiplicazione per m" è iniettiva, saremmo a posto: infatti, poiché $\frac{\mathbb{Z}}{n\mathbb{Z}}$ è un insieme finito, allora f_m sarebbe anche biiettiva, dunque suriettiva, dunque in particolare esisterebbe di certo $x \in \{1, \ldots, n-1\}$ tale che $\overline{m}\,\overline{x} = \overline{1}$. Mostriamo perciò che f_m è iniettiva: infatti, se per assurdo esistessero $a, b \in \{1, \ldots, n-1\}$ (diciamo con $a > b$) tali che $f_m(\overline{a}) = f_m(\overline{b})$ allora si avrebbe $m\overline{a} = m\overline{b}$, ovvero $\overline{ma} = \overline{mb}$, ovvero $\overline{m(a-b)} = \overline{0}$, ovvero n dividerebbe $m(a-b)$: ma poiché n è primo, bisognerebbe che n dividesse m oppure $a - b$, ma entrambe le cose sono impossibili.

[30] Infatti la famiglia dei polinomi è chiusa rispetto alla moltiplicazione, ma se moltiplico un polinomio per una qualsiasi altra funzione $g : \mathbb{R} \to \mathbb{R}$ ovviamente non è detto che si ottenga un polinomio, anzi!

[31] Questo esempio risulterà chiaro quando si parlerà di endomorfismi di spazi vettoriali di dimensione finita, introducendo il calcolo matriciale.

(SV_1) $\lambda(\mu v) = (\lambda\mu)v$ per ogni $\lambda, \mu \in k$ e ogni $v \in V$;
(SV_2) $(\lambda + \mu)v = \lambda v + \mu v$ per ogni $\lambda, \mu \in k$ e ogni $v \in V$;
(SV_3) $\lambda(v + w) = \lambda v + \lambda w$ per ogni $\lambda \in k$ e ogni $v, w \in V$;
(SV_4) $1\, v = v$ per ogni $v \in V$.

Gli elementi di V sono usualmente chiamati *vettori*, quelli di k *scalari*.

Sottospazio vettoriale

Un sottoinsieme $W \subset V$ tale che $(W, +)$ sia sottogruppo di $(V, +)$ e tale che $\lambda v \in W$ per ogni $\lambda \in k$ e ogni $v \in W$ si dice *sottospazio vettoriale* di V: è facile vedere che ciò equivale a chiedere che per ogni $v, w \in W$ e ogni $\lambda, \mu \in k$ si abbia $\lambda v + \mu w \in W$. Un *morfismo di spazi vettoriali* (sullo stesso corpo k) è un morfismo di gruppi $f : V_1 \to V_2$ che rispetta anche la moltiplicazione per scalari, ovvero (riassumendo entrambe le proprietà) tale che $f(\lambda v + \mu w) = \lambda f(v) + \mu f(w)$ per ogni $\lambda, \mu \in k$ e ogni $v, w \in V_1$; si dimostra facilmente che il nucleo $\ker(f)$ (risp. l'immagine $\mathrm{im}(f)$) è un k-sottospazio vettoriale di V_1 (risp. di V_2).

Morfismo di spazi vettoriali

Algebra

Un anello $(R, +, \cdot)$ si dirà un'*algebra* su k (oppure una k-*algebra*) se è un k-spazio vettoriale (rispetto alla somma) e la moltiplicazione per scalari è compatibile col prodotto:

(Alg) $\lambda(x \cdot y) = (\lambda x) \cdot y = x \cdot (\lambda y)$ per ogni $\lambda \in k$ e ogni $x, y \in R$.

Esempi. (1) L'esempio fondamentale di spazio vettoriale su $k = \mathbb{R}$ è dato da $V = \mathbb{R}^n = \{\vec{v} = (v_1, \dots, v_n) : v_j \in \mathbb{R} \text{ per ogni } j = 1, \dots, n\}$ (la famiglia delle n-uple di numeri reali, che descrive –una volta fissato un sistema cartesiano– uno spazio reale a n dimensioni) con la sua naturale operazione di somma e la sua naturale moltiplicazione per costanti reali. Nel caso $n = 2$ gli elementi di $\mathbb{R}^2$ (coppie di numeri reali) possono essere rappresentati come gli usuali vettori nel piano cartesiano; la somma $\vec{v} + \vec{w}$ è data dalla nota "regola del parallelogramma" (si tratta della diagonale principale del parallelogramma costruito su $\vec{v}$ e $\vec{w}$), e la moltiplicazione $\lambda\vec{v}$ di un vettore $\vec{v}$ per uno scalare $\lambda \in \mathbb{R}$ dà luogo a una dilatazione della lunghezza del vettore $\vec{v}$ di un fattore $|\lambda|$, e il verso è mantenuto o invertito a seconda che $\lambda \gtrless 0$. (Analoga rappresentazione è possibile nello spazio tridimensionale cartesiano per i vettori di $\mathbb{R}^3$.) Una funzione $f : \mathbb{R}^2 \to \mathbb{R}^2$ è un morfismo di $\mathbb{R}$-spazi vettoriali se e solo se esistono dei numeri $\lambda, \mu, \nu, \eta \in \mathbb{R}$ tali che $f(\vec{v}) = (\lambda v_1 + \mu v_2,\ \nu v_1 + \eta v_2)$ per ogni $\vec{v} = (v_1, v_2) \in \mathbb{R}^2$; più in generale, un morfismo $f : \mathbb{R}^n \to \mathbb{R}^m$ è associato univocamente a una *matrice* $m \times n$ (una tabella $F = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} \end{pmatrix}$ con m righe e n colonne di numeri reali λ_{ij} con $1 \le i \le m$ e $1 \le j \le n$) tale che, scritto $f(v_1, \dots, v_n) = (f_1(v_1, \dots, v_n)\,,\ \dots\ ,\ f_m(v_1, \dots, v_n))$ (le m funzioni componenti di f) si abbia $f_i(v_1, \dots, v_n) = \sum_{j=1}^{n} \lambda_{ij} v_j = \lambda_{i1} v_1 + \cdots + \lambda_{in} v_n$ per ogni $i = 1, \dots, m$: si tratta della moltiplicazione della matrice F per il "vettore-colonna" $\vec{v} = (v_1, \dots, v_n)$. **(2)** $\mathbb{R}^X = \{f : X \to R\}$ (le funzioni reali di un certo insieme X) e $\mathbb{R}[x_1, \dots, x_n]$ (i polinomi a coefficienti reali con n indeterminate) sono due esempi di $\mathbb{R}$-algebre commutative.

Gli spazi vettoriali sono l'oggetto di studio dell'*algebra lineare*, che sta ai fondamenti della geometria; per ulteriori elementi su di essi (dipendenza lineare, generatori, basi, ...) rimandiamo dunque a un corso di geometria.

1.3 I numeri reali

Nel riassunto delle cose da sapere prima di iniziare il corso avevamo ricordato la descrizione dei numeri reali come "espressioni decimali possibilmente né limitate né periodiche"; il loro insieme $\mathbb{R}$ contiene allora $\mathbb{Q}$, i cui elementi siano visti come espressioni decimali limitate o quantomeno periodiche. Su $\mathbb{R}$ sappiamo essere definite due operazioni, l'*addizione* e la *moltiplicazione*, ed una relazione d'ordine totale "$\leq$" che, considerate assieme, fanno di $(\mathbb{R}, +, \cdot, \leq)$ un *corpo commutativo totalmente ordinato* (ovvero che soddisfa (An_1)-$\cdots$-(An_6)-(CpO_1)-(CpO_2)); a dire il vero, però, le stesse proprietà sono possedute anche da $\mathbb{Q}$, e dunque non sarà per questo che ci apprestiamo ad allargare $\mathbb{Q}$. Il motivo sta invece nell'*impossibilità di assegnare ad alcune lunghezze un numero razionale*:[32] i nuovi enti numerici creati per colmare queste "lacune" dei numeri razionali furono detti numeri *irrazionali*, e il loro insieme $\widetilde{\mathbb{Q}}$, assieme a $\mathbb{Q}$, forma l'insieme dei numeri reali $\mathbb{R}$.
Come si sa, è fondamentale *l'identificazione dei numeri reali con i punti di una retta*: più precisamente, l'assegnare un "sistema di coordinate ascisse" sulla retta (ovvero fissare un punto O detto "origine", un verso di percorrenza detto "positivo" ed un altro punto, in direzione positiva rispetto ad O e da lui diverso, detto "punto unità") dà luogo ad una funzione biiettiva tra $\mathbb{R}$ e la retta stessa, tanto che è normale parlare di *retta reale*, senza di fatto distinguere tra $\mathbb{R}$ e la retta.

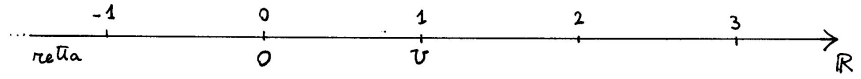

Figura 1.5: Una retta e l'insieme $\mathbb{R}$ dei numeri reali si identificano tramite un sistema di coordinate ascisse.

Poggiando su questa conoscenza di lunga data dei numeri reali, delle loro operazioni, del loro ordine e del loro sostanziale identificarsi con i punti di una retta su cui si sia assegnato un sistema di coordinate ascisse, vogliamo ora esaminarli attraverso le loro proprietà. Oltre ad essere, come visto, un corpo commutativo totalmente ordinato (cosa che però non lo distingue dal suo sottocorpo $\mathbb{Q}$), $\mathbb{R}$ soddisfa anche la seguente proprietà fondamentale:

(Co) (*Completezza*) se U e V sono sottoinsiemi non vuoti di $\mathbb{R}$ tali che $U \leq V$ (ovvero, **Assioma di completezza**

[32] L'esempio storicamente più importante di grandezza irrazionale è quello dell'ipotenusa di un triangolo rettangolo isoscele di lato 1. La sua misura a, in base al teorema di Pitagora, dovrebbe soddisfare $a^2 = 1 + 1 = 2$ (e dunque, per definizione, $a = \sqrt{2}$): se a fosse razionale, si potrebbe scrivere $a = \frac{m}{n}$ con m, n numeri naturali primi tra loro. Se ne dedurrebbe che $m^2 = 2n^2$, perciò m^2 è pari, perciò m è pari, perciò m^2 è divisibile per 4, ma $m^2 = 2n^2$ e perciò n^2 è pari, perciò n è pari (assurdo, perché deve essere primo con m). Generalizzando questo esempio, si può dimostrare che, se $a, n \in \mathbb{N}$ e $\sqrt[n]{a} \notin \mathbb{N}$, allora $\sqrt[n]{a}$ è irrazionale. Altri importanti numeri che si sono dimostrati essere irrazionali sono il numero *pi greco* $\pi = 3,14151\cdots$ (rapporto tra la lunghezza di una circonferenza e quella del suo diametro) ed il *numero di Nepero* $e = 2,71828\cdots$, base naturale della funzione esponenziale.

$x \le y$ per ogni $x \in U$ e $y \in V$), allora esiste $t \in \mathbb{R}$ tale che $U \le t \le V$;

l'elemento t si dice *elemento separatore* tra U e V, ed in generale, ovviamente, esso è lungi dall'essere unico[33]. La proprietà cruciale (Co) è soddisfatta da $\mathbb{R}$ ma non da $\mathbb{Q}$.[34] In altre parole, $\mathbb{R}$ *è un campo totalmente ordinato e completo*; poiché si dimostra (ma noi non ce ne occuperemo) che due campi totalmente ordinati e completi sono necessariamente isomorfi, tale proprietà individua $\mathbb{R}$ "sostanzialmente" (cioè, a meno di isomorfismi).

Figura 1.6: t_1, t_2 e t_3 sono elementi separatori tra U e V; l'intervallo limitato $[a, b[$; la semiretta $\mathbb{R}_{>c}$.

Intervalli Un *intervallo* di $\mathbb{R}$ è un sottoinsieme $I \subset \mathbb{R}$ non vuoto tale che, se $x, y \in I$ e $x \le t \le y$, allora anche $t \in I$ (ovvero, un intervallo è un sottoinsieme di $\mathbb{R}$ "privo di buchi"). Ci si accorge facilmente che gli intervalli sono tutti e soli i sottoinsiemi dei tipi seguenti, ove $a, b \in \mathbb{R}$ con $a \le b$: (1) $[a, b] = \{x \in \mathbb{R} : a \le x \le b\}$ (intervallo chiuso limitato, che si riduce a $\{a\}$ se $a = b$); (2) $[a, b[= \{x \in \mathbb{R} : a \le x < b\}$ e $]a, b] = \{x \in \mathbb{R} : a < x \le b\}$ (intervalli semiaperti limitati); (3) $]a, b[= \{x \in \mathbb{R} : a < x < b\}$ (intervallo aperto limitato); (4) $[a, +\infty[= \{x \in \mathbb{R} : x \ge a\}$, $]a, +\infty[= \{x \in \mathbb{R} : x > a\}$, $]-\infty, b] = \{x \in \mathbb{R} : x \le b\}$ e $]-\infty, b[= \{x \in \mathbb{R} : x < b\}$ (semirette aperte o chiuse, che si denoteranno anche rispettivamente $\mathbb{R}_{\ge a}$, $\mathbb{R}_{>a}$, $\mathbb{R}_{\le b}$ e $\mathbb{R}_{<b}$), (5) lo stesso $\mathbb{R}$.

Intervalli di $\mathbb{R}$

Massimo e minimo. Estremo superiore ed inferiore Una nozione importante in $\mathbb{R}$ è quella di *estremo superiore* e *inferiore*: vediamo di che si tratta. Intanto, dato un sottoinsieme non vuoto $A \subset \mathbb{R}$, si dice che $t \in \mathbb{R}$ è un *massimo* (risp. un *minimo*) di A se soddisfa le seguenti due proprietà:

Massimo, minimo

(1) $t \in A$,

(2) $x \le t$ (risp. $t \le x$) per ogni $x \in A$.

Non è detto che tali massimo e minimo di A esistano, ma, se esistono, sono unici[35], e si denoteranno con $\max A$ e $\min A$. L'insieme dei *maggioranti di* A è il sottoinsieme di $\mathbb{R}$

$$A^* = \{x \in \mathbb{R} : a \le x \text{ per ogni } a \in A\};$$

[33] Ad esempio, se $U = \{x \in \mathbb{R} : x \le -1\}$ e $V = \{x \in \mathbb{R} : x \ge 1\}$ tutti i numeri reali $t \in [-1, 1]$ sono elementi separatori tra U e V.

[34] Se $U = \{x \in \mathbb{Q} : x > 0,\ x^2 \le 2\}$ e $V = \{x \in \mathbb{Q} : x > 0,\ x^2 \ge 2\}$, poichè per $x > 0$ la funzione x^2 è crescente (infatti se $x_2 > x_1 > 0$ allora $x_2^2 - x_1^2 = (x_2 + x_1)(x_2 - x_1) > 0$, ovvero $x_2^2 > x_1^2$), un eventuale elemento $t \in \mathbb{Q}$ tale che $U \le t \le V$ dovrebbe soddisfare $t^2 = 2$, ma come visto ciò è impossibile.

[35] Ad esempio, siano t_1 e t_2 due massimi per A: allora, poiché entrambi devono stare in A, dev'essere $t_1 \le t_2$ e $t_2 \le t_2$, ma allora $t_1 = t_2$ per (ASym).

quello dei *minoranti di* A sarà

$$A_* = \{x \in \mathbb{R} : x \leq a \text{ per ogni } a \in A\}.$$

Se $A^* \neq \varnothing$ (risp. $A_* \neq \varnothing$), si dirà che A è *superiormente limitato* (risp. *inferiormente limitato*), ed un sottoinsieme di $\mathbb{R}$ sia superiormente che inferiormente limitato si dirà, ovviamente, *limitato*. Ora, è chiaro che il miglior maggiorante per A è quello più piccolo possibile: si porrà dunque, se esiste,

Limitatezza

$$\sup A := \min A^*.$$

In quanto minimo di un sottoinsieme, tale elemento, se esiste, sarà unico, e si dirà *estremo superiore* di A. Simmetricamente si definirà, se esiste, l'*estremo inferiore* di A:

Estremo superiore e inferiore

$$\inf A := \max A_*.$$

Si noti che, a differenza di $\max A$ e $\min A$, per $\sup A$ e $\inf A$ non si è richiesta l'appartenenza ad A.

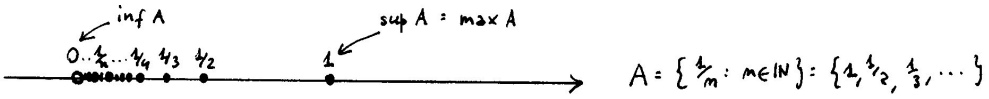

Figura 1.7: Estremo superiore ed inferiore.

La seguente proposizione è importante, e distingue nettamente $\mathbb{R}$ da $\mathbb{Q}$ (si noti che la dimostrazione consiste, in sostanza, nel provare che l'esistenza di sup e inf equivale all'assioma di completezza (Co)).

Proposizione 1.3.1. *Ogni sottoinsieme di* $\mathbb{R}$ *superiormente* (risp. inferiormente) *limitato ammette estremo superiore* (risp. inferiore)*. In particolare, ogni sottoinsieme limitato di* $\mathbb{R}$ *ammette estremo superiore e inferiore.*

Dimostrazione. Sia $A \subset \mathbb{R}$ superiormente limitato, ovvero tale che $A^* \neq \varnothing$. Applichiamo (Co) considerando $U = A$ e $V = A^*$, e sia dunque $A \leq t \leq A^*$ un elemento separatore. Poiché $t \geq A$ si ha $t \in A^*$; poiché inoltre $t \leq A^*$, è proprio $t = \min A^*$. In modo analogo si dimostra l'affermazione per l'estremo inferiore. □

Riassumendo, un sottoinsieme superiormente (risp. inferiormente) limitatato A di $\mathbb{R}$ non ammette sempre il massimo (risp. minimo), ma ammette sempre l'estremo superiore (risp. inferiore) che, se appartiene ad A, chiaramente coinciderà col massimo (risp. col minimo) di A. Concretamente, dati un sottoinsieme A e un numero $\alpha \in \mathbb{R}$, per determinare se sia $\alpha = \sup A$ o no si potrà applicare la seguente

Proposizione 1.3.2. (Proprietà caratteristiche di sup e inf) *Vale* $\alpha = \sup A$ *se e solo se*
(Sup1) $a \leq \alpha$ *per ogni* $a \in A$*;*
(Sup2) *per ogni* $x \in \mathbb{R}$ *tale che* $x < \alpha$ *esiste* $a \in A$ *tale che* $x < a$*.*

Simmetricamente, $\alpha = \inf A$ *se e solo se*

(Inf1) $a \geq \alpha$ *per ogni* $a \in A$*;*

(Inf2) *per ogni* $x \in \mathbb{R}$ *tale che* $x > \alpha$ *esiste* $a \in A$ *tale che* $x > a$*.*

Dimostrazione. Se $\alpha = \sup A$, essendo $\alpha = \min A^*$ vale $\alpha \in A^*$; dato poi $x \in \mathbb{R}$ tale che $x < \alpha$, vale certamente $x \notin A^*$ (appunto perché $\alpha = \min A^*$), e dunque esiste qualche $a \in A$ tale che $x \not\geq a$, ovvero $x < a$. Viceversa, assumiamo che α soddisfi (Sup1) e (Sup2), e supponiamo per assurdo che $\alpha \neq \min A^*$: allora esiste $x \in A^*$ tale che $x \not\geq \alpha$, ovvero $x < \alpha$. Ma allora per (Sup2) esiste $a \in A$ tale che $x < a$, e ciò dice che $x \notin A^*$, contraddizione. Gli stessi ragionamenti provano l'asserto speculare per inf. □

Ciò che afferma la proprietà caratteristica è dunque che "$\sup A$ sta sopra A, ma non appena si prova a scendere ci si lascia davanti qualche elemento di A"; similmente, "$\inf A$ sta sotto A, ma non appena si prova a salire ci si lascia dietro qualche elemento di A".[36]

Esercizio. *Dire se i seguenti sottoinsiemi* $A \subset \mathbb{R}$ *ammettono estremi superiore ed inferiore, massimo e minimo:* **(0)** $\{-2\}$*;* **(1)** $[0, 1[$*;* **(2)** $]-\infty, -5[$*;* **(3)** $\{x \in \mathbb{R} > 0 : \sin(\frac{1}{x}) = 0\}$*;* **(4)** $\{(-1)^n \frac{n-1}{n} : n \in \mathbb{N}\}$*;* **(5)** $\{(-1)^n \frac{n-1}{n} : n \in \mathbb{N}\} \cup \{1\}$*;* **(6)** $\{\frac{xy}{x^2+y^2} : x, y > 0\}$.

Risoluzione. **(0)** Banale: $\sup A = \inf A = \max A = \min A = -2$. **(1)** A è limitato, con $A^* = [1, +\infty[$ e $A_* =]-\infty, 0]$: dunque $\sup A = 1$ e $\inf A = 0$. Poiché $0 \in A$, 0 è anche il $\min A$; invece $1 \notin A$, dunque A non ammette max. **(2)** A non è inferiormente limitato, dunque non ammette inf (e dunque nemmeno min); invece esso è superiormente limitato, con $A^* = [-5, +\infty[$: dunque $\sup A = -5$, ed essendo $-5 \notin A$, non ci sarà max. **(3)** La condizione $\sin(\frac{1}{x}) = 0$ con $x > 0$ è equivalente a $x = \frac{1}{k\pi}$ con $k \in \mathbb{N}$: dunque $A = \{\frac{1}{k\pi} : k \in \mathbb{N}\} = \{\frac{1}{\pi}, \frac{1}{2\pi}, \frac{1}{3\pi}, \dots\}$. Vale $\frac{1}{\pi} \in A$ e $x \leq \frac{1}{\pi}$ per ogni $x \in A$: dunque $\max A = \frac{1}{\pi}$ (ed esso sarà ovviamente anche $\sup A$). Si noti poi che A è inferiormente limitato (perché $0 \in A_* \neq \varnothing$), e dunque ammette estremo inferiore, che vogliamo dimostrare essere 0: a tal fine usiamo le proprietà caratteristiche (Inf1) e (Inf2) dell'inf. (Inf1) lo abbiamo già detto ($0 \in A_*$); preso poi un qualsiasi $x > 0$, si ha $\frac{1}{k\pi} < x$ per k abbastanza grande, e dunque vale anche (Inf2). Dunque $\inf A = 0$; poiché $0 \notin A$, non vi sarà minimo. **(4)** Vale $A = \{0, -\frac{2}{3}, -\frac{4}{5}, -\frac{6}{7}, \dots\} \sqcup \{\frac{1}{2}, \frac{3}{4}, \frac{5}{6}, \dots\}$. Si vede subito che $A \subset]-1.1[$: infatti $\left|(-1)^n \frac{n-1}{n}\right| = \frac{n-1}{n} = 1 - \frac{1}{n} < 1$. Dunque A è limitato, ed ammette perciò estremi superiore e inferiore. Vale $\sup A = 1$: infatti $x \leq 1$ per ogni $x \in A$, e dunque vale (Sup1); preso poi un qualsiasi $x < 1$, si ha $x < \frac{2k-1}{2k} = 1 - \frac{1}{2k}$ per k abbastanza grande, e dunque vale (Sup2). In modo analogo si prova che $\inf A = -1$. Poiché né 1 né -1 stanno in A, non vi saranno massimo e minimo. **(5)** Esattamente come nel caso precedente, solo che stavolta $1 \in A$ e dunque esiste $\max A = 1$. **(6)** Poiché $A \subset \mathbb{R}_{>0}$, si ha $\mathbb{R}_{\leq 0} \subset A_*$ e dunque A è inferiormente limitato: perciò ammette estremo inferiore. Vediamo che vale $\inf A = 0$: infatti vale (Inf1), mentre notiamo che per valori del tipo $(x, 1)$ con $x > 0$ si ottengono i punti $\frac{x}{x+1}$ che possono diventare arbitrariamente vicini a zero quando x tende a 0: dunque, preso un qualunque $0 < t < 1$ esistono di certo degli $x > 0$ tali che $\frac{x}{x+1} < t$ (basta prendere $x < \frac{t}{1-t}$) e dunque vale anche (Inf2). Si noti che $0 \notin A$, e dunque A non ammette minimo. Dalla disuguaglianza $(x-y)^2 \geq 0$ con $x, y > 0$ si ricava subito $\left|\frac{xy}{x^2+y^2}\right| = \frac{xy}{x^2+y^2} \leq \frac{1}{2}$, e dunque A è anche limitato: esso ammetterà anche l'estremo superiore. In realtà, per valori del tipo (x, x) con $x > 0$ si ottiene sempre $\frac{xy}{x^2+y^2} = \frac{x^2}{x^2+x^2} = \frac{1}{2}$, e dunque $\frac{1}{2} \in A$: poiché come visto si ha anche $\frac{1}{2} \geq A$, si avrà $\max A = \frac{1}{2}$ (che coincide ovviamente con $\sup A$).

[36] Si dimostra in realtà che l'esistenza di sup ed inf rispettivamente per sottoinsiemi superiormente ed inferiormente limitati è *equivalente* all'assioma di completezza (Co): infatti, se $A \leq B$ allora A è superiormente limitato, e dunque esiste $t = \sup A = \min A^*$: essendo $B \subset A^*$, si ha anche $t \leq B$, e dunque t è un elemento separatore. È lecito attendersi perciò che $\mathbb{Q}$ non soddisfi tale proprietà: l'esempio è il solito, basta prendere $A = \{x \in \mathbb{Q} : x^2 < 2\}$.

Classi contigue Due sottoinsiemi $U, V \subset \mathbb{R}$ tali che $U \leq V$ (ovvero, come detto, tali che $x \leq y$ per ogni $x \in U$ e $y \in V$) e che per ogni $\varepsilon > 0$ esistono due elementi $x_\varepsilon \in U$ e $y_\varepsilon \in V$ tali che $y_\varepsilon - x_\varepsilon < \varepsilon$, si diranno *classi contigue* di numeri reali: l'idea è che "anche se V sta sopra ad U, ci sono però elementi di U e V vicini quanto si vuole".[37] È allora naturale pensare che

Classi contigue

Proposizione 1.3.3. *Due classi contigue $U, V \subset \mathbb{R}$ di numeri reali ammettono un unico elemento separatore $\xi \in \mathbb{R}$, e vale $\xi = \sup U = \inf V$.*

Dimostrazione. Siano $\alpha = \sup U$ e $\beta = \inf V$ (che di certo esistono perché U e V sono limitati risp. superiormente e inferiormente). Sappiamo anche che esiste qualche elemento separatore tra U e V; poiché ogni elemento separatore $t \in \mathbb{R}$ tra U e V deve soddisfare $\alpha \leq t \leq \beta$, ci basta mostrare che $\alpha = \beta$ per concludere. Infatti, se per assurdo si avesse $\alpha < \beta$, si ha avrebbe allora $U \leq \alpha < \beta \leq V$, e allora per ogni $x \in U$ e $y \in V$ si avrebbe $y - x > \beta - \alpha > 0$: ma ciò contraddirebbe la contiguità di U e V (basta prendere $0 < \varepsilon < \beta - \alpha$). □

Esempi. Siano $r \in \mathbb{N}$ e $\alpha \in \mathbb{Q}$, e poniamo $U = \{x \in \mathbb{R} : x^r < \alpha\}$ e $V = \{x \in \mathbb{R} : x^r > \alpha\}$. Allora U e V sono classi contigue, e il loro elemento separatore è la radice r-esima $\sqrt[r]{\alpha}$; se α non è una "potenza r-esima perfetta", cioè non esiste $\beta \in \mathbb{Q}$ tale che $\alpha = \beta^r$), tale elemento separatore è irrazionale (ciò generalizza il ben noto caso $r = \alpha = 2$).

Densità dei razionali e degli irrazionali nei reali Come ultima cosa, vogliamo ricavare in modo preciso dalle proprietà di $\mathbb{R}$ un fatto già detto in modo un po' vago: che "ogni numero reale si può approssimare a piacere con numeri razionali". Se I è un intervallo di $\mathbb{R}$ e $A \subset I$, diremo che A è *denso* in I se, comunque presi $x, y \in I$ con $x < y$, esiste $t \in A$ tale che $x < t < y$ (in altre parole, se "tra due qualsiasi elementi di I se ne trova sempre qualcuno di A"): dimostreremo allora che sia $\mathbb{Q}$ che $\widetilde{\mathbb{Q}} = \mathbb{R} \setminus \mathbb{Q}$ (insieme dei numeri irrazionali) sono densi in $\mathbb{R}$. A tal fine iniziamo col dimostrare che, come $\mathbb{Q}$, anche $\mathbb{R}$ gode della seguente proprietà:

Densità

Proposizione 1.3.4. (Archimedeità di $\mathbb{R}$) *Se $x, y \in \mathbb{R}$ con $x > 0$, esiste $n \in \mathbb{N}$ tale che $nx > y$. Analogamente, se $x, y \in \mathbb{R}$ con $x > 1$ e $y > 0$, esiste $n \in \mathbb{N}$ tale che $x^n > y$.*

Dimostrazione. Negare la tesi equivale a dire che esistono $\tilde{x}, \tilde{y} \in \mathbb{R}$ con $\tilde{x} > 0$ tali che per ogni $n \in \mathbb{N}$ vale $n\tilde{x} \not> \tilde{y}$, cioè $n\tilde{x} \leq \tilde{y}$: ovvero $A = \{n\tilde{x} : n \in \mathbb{N}\}$ è superiormente limitato perché $\tilde{y} \in A^*$, e dunque esiste $x_0 = \sup A$. Da $\tilde{x} > 0$ si ricava $x_0 - \tilde{x} < x_0$: per la seconda proprietà caratteristica del sup, esisterà $n \in \mathbb{N}$ tale che $x_0 - \tilde{x} < n\tilde{x}$, ovvero $x_0 < (n+1)\tilde{x}$: ma allora x_0 non è un maggiorante di A, assurdo perché $x_0 = \sup A = \min A^*$. Stesso procedimento per la seconda affermazione (ove si usa la moltiplicazione in luogo dell'addizione). □

Ricordiamo le funzioni *parte intera* $[\,\cdot\,] : \mathbb{R} \to \mathbb{Z}$ e *parte frazionaria* $\mathrm{frac} : \mathbb{R} \to [0, 1[$: se $x \in \mathbb{R}$, la sua "parte intera" $[x]$ è il massimo intero $r \in \mathbb{Z}$ tale che $r \leq x$ (dunque, per definizione, vale $[x] \leq x < [x] + 1$), e la sua "parte frazionaria" è $\mathrm{frac}(x) = x - [x] \in [0, 1[$. Ad esempio, vale $[\frac{3}{2}] = 1$, $[-\frac{4}{3}] = -2$, $\mathrm{frac}(\frac{3}{2}) = \frac{3}{2} - 1 = \frac{1}{2}$ e $\mathrm{frac}(-\frac{4}{3}) = -\frac{4}{3} - (-2) = \frac{2}{3}$.

[37] Ad esempio, $U =]0, 1[$ e $V =]1, 5[\cup \{7\}$ sono classi contigue di $\mathbb{R}$, perché, preso un qualsiasi $\varepsilon > 0$, si ha $x_\varepsilon = 1 - \frac{\varepsilon}{3} \in U$, $y_\varepsilon = 1 + \frac{\varepsilon}{3} \in V$ e $y_\varepsilon - x_\varepsilon = \frac{2\varepsilon}{3} < \varepsilon$; anche $U = \{x \in \mathbb{R} : x^2 < 2\}$ e $V = \{x \in \mathbb{R} : x^2 \geq 2\}$, sono classi contigue di $\mathbb{R}$ in quanto, preso un qualsiasi $0 < \varepsilon \ll 1$, si ha $x_\varepsilon = \sqrt{2 - \frac{\varepsilon}{3}} \in U$, $y_\varepsilon = \sqrt{2 + \frac{\varepsilon}{3}} \in V$ e $y_\varepsilon - x_\varepsilon < \frac{2\varepsilon}{3} < \varepsilon$. Invece $U =]0, 1]$ e $V = [2, 4[$ non lo sono: se $0 < \varepsilon < 1$, non esistono $x_\varepsilon \in U$ e $y_\varepsilon \in V$ tali che $y_\varepsilon - x_\varepsilon < \varepsilon$ (tra U e V "c'è largo spazio").

Corollario 1.3.5. *$\mathbb{Q}$ e $\widetilde{\mathbb{Q}}$ sono sottoinsiemi densi di $\mathbb{R}$.*

Dimostrazione. Siano $x, y \in \mathbb{R}$ con $x < y$. Per l'archimedeità di $\mathbb{R}$, essendo $y - x > 0$ esiste $n \in \mathbb{N}$ tale che $n(y-x) > 1$, ovvero $y - x > \frac{1}{n}$. Poniamo ora $m = [nx] + 1 \in \mathbb{Z}$: vale $[nx] \leq nx < [nx] + 1 = m$, da cui $\frac{[nx]}{n} \leq x < \frac{m}{n}$; si ha poi $y = x + (y-x) > x + \frac{1}{n} \geq \frac{[nx]}{n} + \frac{1}{n} = \frac{m}{n}$, e se ne ricava che $x < \frac{m}{n} < y$, come si voleva. Si prenda poi un qualsiasi $\alpha \in \widetilde{\mathbb{Q}} \cap \mathbb{R}_{>0}$ (ad esempio $\alpha = \pi$), e sia $\frac{m'}{n'} \in \mathbb{Q}$ tale che $\frac{x}{\alpha} < \frac{m'}{n'} < \frac{y}{\alpha}$, ovvero $x < \frac{m'}{n'}\alpha < y$: se $m' \neq 0$ allora $\frac{m'}{n'}\alpha \in \widetilde{\mathbb{Q}}$ e siamo a posto, mentre se $m' = 0$ allora $x < 0 < y$ e dunque, preso $n'' \in \mathbb{N}$ tale che $n''y > \alpha$, vale $x < 0 < \frac{\alpha}{n''} < y$, con $\frac{\alpha}{n''} \in \widetilde{\mathbb{Q}}$. □

Esempio. Dati $x = \sqrt{2}$ e $y = \frac{5\sqrt{3}}{6}$ (entrambi numeri irrazionali), notiamo che $x < y$: cerchiamo allora un razionale $\frac{m}{n} \in \mathbb{Q}$ tale che $x < \frac{m}{n} < y$. Moltiplicando per i denominatori e elevando al quadrato si ottiene che un tale $\frac{m}{n}$ (che sappiamo esisterà) deve soddisfare $24n^2 < 12m^2 < 25n^2$. Cerchiamo la buona frazione aumentando via via il denominatore n e controllando se qualche intero m soddisfa quanto richiesto: per $n = 1, 2, 3, 4, 5, 6$ ciò non è possibile, mentre per $n = 7$ si può scegliere $m = 10$ (infatti $1176 < 1200 < 1225$). Dunque $x < \frac{10}{7} < y$.