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

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

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

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

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 che B *contiene* A (notazione: $B \supset A$). Dato un qualsiasi insieme A, è chiaro che $A \subset A$; 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 $B \subset A$, e $\{a\} \subset A$ se e solo se $a \in A$. [3] 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 B dei numeri interi tra -2 (escluso) e 2 (compreso) si può scrivere intensivamente come $B = \{x \in \mathbb{Z} :$

[3] 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.

$-2 < x \leq 2\}$, 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).

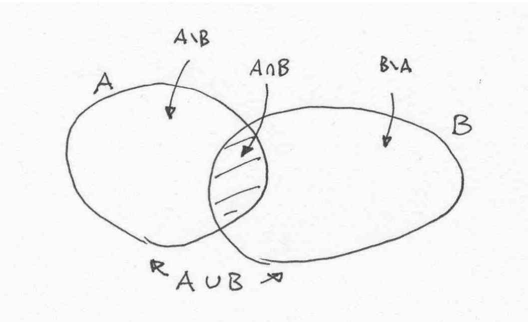

Figura 1.1: *Rappresentazione di insiemi tramite i diagrammi di Venn*

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

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

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.[4]

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 $A \cup B = (A \setminus B) \sqcup (A \cap B) \sqcup (B \setminus A)$, 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 $\complement_A B$).

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

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:

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

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,

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

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.[5]

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.
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 $x_1 \mathcal{R} x_3$.

Una relazione $\mathcal{R}$ in X che soddisfa (Rifl)-(Sym)-(Trns) si dice *equivalenza* in X: il suo effetto è quello di spezzare X in una famiglia di sottoinsiemi disgiunti (le *classi di equiv-*

[5] 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 sono $2 \cdot \dots \cdot 2$ (n fattori), ovvero 2^n.

alenza, ciascuna formata da elementi in relazione tra loro)[6]. 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

(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 decompongono 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.

Siamo X e Y due insiemi diversi da $\varnothing$. Una *funzione* f da X ad Y è una regola che ad ogni elemento $x \in X$ associa uno ed un solo elemento $f(x) \in Y$, detto *immagine* di x tramite f.
Una funzione può essere detta anche *mappa* o *applicazione*; l'insieme di partenza X si chiama *dominio* di f, quello d'arrivo Y *codominio* di f. La notazione più usuale per una funzione è $f : X \to Y$. 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 $x \mapsto f(x)$. Due funzioni $f : X \to Y$ e $g : X \to Y$ si diranno *uguali* (scrivendo $f = g$) se $f(x) = g(x)$ per ogni $x \in X$, ovvero se lavorano allo

[6] 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.

stesso modo.

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 $\mathrm{id}_X(x) = x$.

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

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

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"). 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 $B \cap f(X) = \varnothing$. Va anche notato che, per abuso di notazione, nel caso di $\{y_0\}$ (sottoinsieme di Y costituito dal solo elemento y_0) si usa scrivere spesso $f^{-1}(y_0)$ in luogo del formalmente corretto $f^{-1}(\{y_0\})$ (si chiama anche la *fibra* di f sopra y_0: sono gli elementi di X che vengono mandati in y_0).

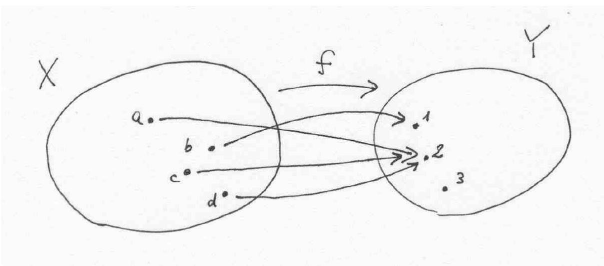

Figura 1.2: *Una funzione deve mandare* ogni *elemento del suo dominio in* uno ed un solo *elemento del suo codominio*

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 $f^{-1}(B_2) = \{a, c, d\}$.

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 $f(A_1) \cap f(A_2) = \{y_0\} \neq \varnothing$.

Data una funzione $f : X \to Y$ ed un sottoinsieme $A \subset X$, si potrà definire la *restrizione di f ad 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 $f(X) \subset B$.

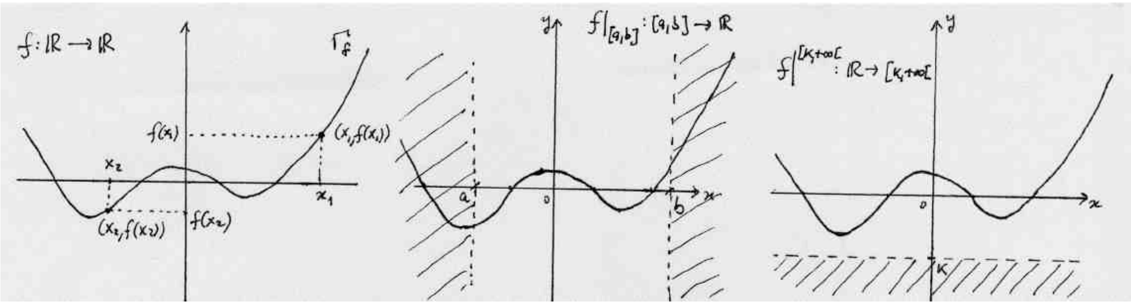

Figura 1.3: *Il grafico di una funzione $f : \mathbb{R} \to \mathbb{R}$; la sua restrizione ad un intervallo $[a, b]$; la sua corestrizione alla semiretta $\mathbb{R}_{\geq k}$ (che contiene l'immagine di f).*

Il *grafico* della funzione $f : X \to Y$ è il sottoinsieme $\Gamma_f \subset X \times Y$ dato da

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

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 $f(g(x)) = (-x + 3)^2 + 1 = x^2 - 6x + 10$.

Una funzione si dirà *iniettiva* se, dati x_1 e x_2 in X con $x_1 \neq x_2$, vale $f(x_1) \neq f(x_2)$ (ovvero, se manda elementi distinti di X in elementi distinti di Y); l'esempio più semplice

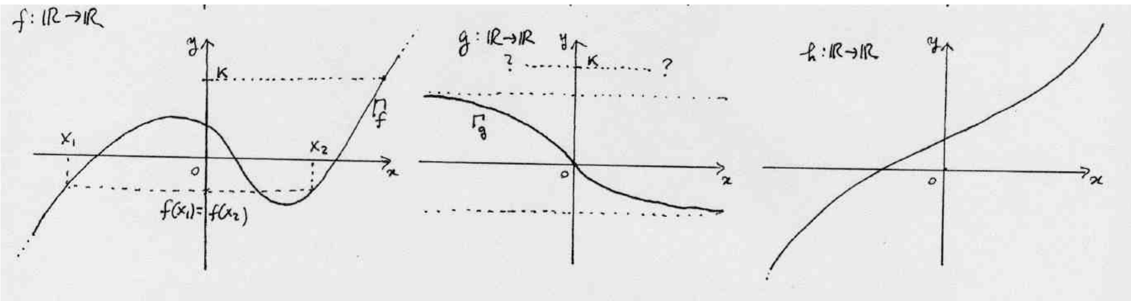

Figura 1.4: f *è suriettiva ma non iniettiva;* g *è iniettiva ma non suriettiva;* h *è biiettiva.*

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 $\iota_A(x) = x$. 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 $y \in Y$: l'esempio più ovvio di funzione suriettiva è la mappa costante di un insieme X dentro un insieme con un solo elemento. Una funzione iniettiva e suriettiva si dirà *biiettiva*: 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 $f \circ f^{-1} = \mathrm{id}_Y$.

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 $f(X) = \{1, 2\} \subsetneq Y$). **(2)** Sia X l'insieme di tutti gli esseri umani nati dal 1800 in poi, e sia $T = \{x \in X : x \text{ ha avuto almeno un figlio}\}$. 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 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. **(2)** 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}(Pippo Baudo) è composta da Pippo Baudo e da tutti i "non siculi". **(3)** Venendo ad un esempio matematico, sia $f : \mathbb{Q} \to \mathbb{Q}$ data da $f(x) = x^2$: si tratta di una funzione, né iniettiva (vale $f(1) = f(-1) = 1$) né suriettiva (-5 non fa parte dell'immagine di f, ma nemmeno 2: è così, come sappiamo e come rivedremo tra breve, che sono nati i numeri reali). Invece $f|_{\mathbb{Q}_{>0}} : \mathbb{Q}_{>0} \to \mathbb{Q}$ è iniettiva.

Gruppi, anelli e corpi. Prima di parlare dei numeri reali, è utile studiare alcune 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* 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.

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)[7];
(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});[8]
(Gr_4) *Commutatività*: $x_1 * x_2 = x_2 * x_1$ per ogni $x_1, x_2 \in G$.

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*[9]. È importante notare che in un gruppo $(G, *)$ vale la *regola della cancellazione*: se $x * y = x * z$ oppure $y * x = z * x$ allora $y = z$ (basta operare in ambo i membri con x^{-1} dalla parte opportuna).

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)[10]; 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

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

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

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

[10] 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").

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 $(\tau \cdot \sigma)(3) = 3$, 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).

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 $f(x *_1 x') = f(x) *_2 f(x')$ 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.)[11] (È chiaro che, se G è commutativo, tutte le coniugazioni sono uguali all'identità, e dunque tutti i sottogruppi di G sono normali.)

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. 20). 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[12] L'importanza di questa costruzione diventa evidente nel *Teorema di Omomorfismo*, che

[11] Infatti, se $g \in G_1$ e $h \in \ker(f)$ si ha $g *_1 h *_1 g^{-1} \in \ker(f)$, perché $f(g *_1 h *_1 g^{-1}) = f(g) *_2 f(h) *_2 f(g^{-1}) = f(g) *_2 e_2 *_2 f(g)^{-1} = f(g) *_2 f(g)^{-1} = e_2$.

[12] 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

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)** I morfismi di $(\mathbb{Z}, +)$ in sè sono tutte e sole In $(\mathbb{Z}, +)$, le moltiplicazioni per un dato numero intero n sono morfismi; in realtà questi sono tutti e soli i morfismi di $(\mathbb{Z}, +)$. **(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 $1 + 12\mathbb{Z} = 13 + 12\mathbb{Z} = \cdots$.[13] 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 (addizione e moltiplicazione) 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 alla moltiplicazione) 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 *addizione*) e $\cdot$ (detta *moltiplicazione*). 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 $x_1, x_2, x' \in R$;
(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) *Invertibilità* (se vale An_4): Ogni $x \neq 0$ è invertibile rispetto a $\cdot$ (ovvero, denotando $R^\times = R \setminus \{0\}$, si ha che $(R^\times, \cdot)$ è un gruppo);
(An_6) *Commutatività*: l'operazione $\cdot$ sia commutativa.

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 (An_1)-(An_2)-(An_3)-(An_4)-(An_5), si dirà *corpo*; se una di queste strutture soddisfa anche (An_6), si aggiungerà l'aggettivo *commutativo* (in luogo di "corpo commutativo"

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 $(g_1' * H) * (g_2' * H) = (g_1' * g_2') * H = (g_1 * h_1 * g_2 * h_2) * H = (g_1 * h_1 * g_2) * H = (g_1 * g_2 * h') * H = (g_1 * g_2) * H = (g_1 * H) * (g_2 * H)$, come si voleva.

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

si usa anche il termine *campo*). In un anello $(R, +, \cdot)$ vale $0 \cdot x = x \cdot 0 = 0$ per ogni $x \in R$ (infatti $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ da cui, cancellando, $x \cdot 0 = 0$).

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).

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.

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

(CpO_1) se $x_1, x_2 \in R$ e $x_1 \leq x_2$, allora per ogni $x \in R$ vale $x_1 + x \leq x_2 + x$;
(CpO_2) se $x_1, x_2 \in R$ e $x_1 \leq x_2$, allora per ogni $x \in R$ tale che $x \geq 0$ vale $x \cdot x_1 \leq x \cdot x_2$.

Esempi. (1) $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{Q}, +, \cdot)$ sono anelli unitari commutativi; $(\mathbb{Q}, +, \cdot)$ è un campo totalmente ordinato. **(2)** $(\mathbb{Z}[x], +, \cdot)$ 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. **(3)** 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 $n = 0, 1$. **(4)** 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. **(5)** 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 $\mathbb{R}^{\mathbb{R}}$.[14] **(6)** 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 $f \cdot g \neq g \cdot f$.[15]

[14] 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!

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