Relazioni e funzioni

X, Y insiemi $\rightsquigarrow X \times Y = \{(x,y) \mid x \in X, y \in Y\}$
↑ prodotto cartesiano

Nota: $X \times Y \neq Y \times X$ (coppie ordinate)

$\mathcal{R} \subset X \times Y$ relazione da X a Y

$S \subset X \rightsquigarrow \mathcal{R}(S) = \{y \in Y \mid \exists\, x \in S \text{ con } (x,y) \in \mathcal{R}\} \subset Y$
$T \subset Y \rightsquigarrow \mathcal{R}^{-1}(T) = \{x \in X \mid \exists\, y \in T \text{ con } (x,y) \in \mathcal{R}\} \subset X$

$\mathcal{R}_| = \mathcal{R} \cap (S \times T) \subset S \times T$ restrizione di R da S a T

Note: 1) $\mathcal{R} : X \to Y$ notazione diversa per $\mathcal{R} \subset X \times Y$
2) $x \,\mathcal{R}\, y$, $x \overset{\mathcal{R}}{\to} y$, $\mathcal{R} : x \mapsto y$ notazioni diverse per $(x,y) \in \mathcal{R}$

Esempi: 1) $\varnothing, X \times Y$ relazione vuota/piena
2) $\mathrm{id}_X = \Delta X = \{(x,x) \mid x \in X\} \subset X \times X$ identità di X
3) $P = \{\text{punti del piano}\}$, $R = \{\text{rette del piano}\}$
$\mathcal{A} = \{(p,r) \in P \times R \mid p \in r\}$ (rel. di appartenenza)
$\mathcal{I} = \{(r,s) \in R \times R \mid r \cap s = \text{punto}\}$ (rel. di incidenza)
$\mathcal{P} = \{(r,s) \in R \times R \mid r \cap s = \varnothing\}$ (rel. di parallelismo)

$\mathcal{R}$ relazione da X a Y
$\rightsquigarrow \mathcal{R}^{-1} = \{(y,x) \in Y \times X \mid (x,y) \in \mathcal{R}\}$
↑ relazione inversa di $\mathcal{R}$ (da Y a X)

$\mathcal{R}$ relazione da X a Y, $\mathcal{S}$ relazione da Y a Z
$\rightsquigarrow \mathcal{S} \circ \mathcal{R} = \{(x,z) \in X \times Z \mid \exists\, y \in Y \text{ con } (x,y) \in \mathcal{R} \text{ e } (y,z) \in \mathcal{S}\}$
↑ relazione composta di $\mathcal{R}$ e $\mathcal{S}$ (da X a Z)

Note: 1) $(\mathcal{R}^{-1})^{-1} = \mathcal{R}$ e $\mathcal{R} \circ \mathrm{id}_X = \mathcal{R} = \mathrm{id}_Y \circ \mathcal{R}$
2) in generale $\mathcal{R}^{-1} \circ \mathcal{R} \neq \mathrm{id}_X$ e $\mathcal{R} \circ \mathcal{R}^{-1} \neq \mathrm{id}_Y$

Esempi: per le relazioni $\mathcal{A}$, $\mathcal{I}$ e $\mathcal{P}$ definite sopra si ha
$\mathcal{A}^{-1} \circ \mathcal{A} = P \times P$, $\mathcal{A} \circ \mathcal{A}^{-1} = \Delta R \cup \mathcal{I}$, $\mathcal{I} \circ \mathcal{I} = R \times R$
$\mathcal{I} \circ \mathcal{A} = P \times R$, $\mathcal{P} \circ \mathcal{A} = P \times R - \mathcal{A}$, $\mathcal{P} \circ \mathcal{P} = \mathcal{P} \cup \Delta R$

$f : X \to Y$ relazione da X a Y
funzione $\overset{\text{def}}{\iff}$ per ogni $x \in X$ esiste unico $y \in Y$ t.c. $x \xrightarrow{f} y$
(*in tal caso si scrive anche* $f(x) = y$)

Note: 1) $f : X \to Y$, $f : Y \to Z$ funzioni $\Rightarrow g \circ f : X \to Z$ funzione
2) $f : X \to Y$ funzione, $f_| : S \to T$ funzione $\Leftrightarrow f(S) \subset T$

Esempi: P, R *insiemi e* $\mathcal{A}, \mathcal{I}, \mathcal{P}$ relazioni definiti sopra
1) $\rho : P \times P \to R$ definita $((p,q),r) \in \rho \Leftrightarrow \{p,q\} \subset r$
non è una funzione, ma lo è $\rho_| : (P \times P - \Delta P) \to R$
2) $\sigma : R \times R \to P$ definita $((r,s),p) \in \sigma \Leftrightarrow p \in r \cap s$
non è una funzione, ma lo è $\sigma_| : \mathcal{I} \to P$
3) $\tau : P \times R \to R$ definita $((p,r),s) \in \tau \Leftrightarrow p \in s$ e $r \,\mathcal{P}\, s$
non è una funzione, ma lo è $\tau_| : (P \times R - \mathcal{A}) \to R$

$f : X \to Y$ funzione da X a Y
iniettiva $\overset{\text{def}}{\iff}$ per ogni $y \in Y$ esiste al più un $x \in X$ t.c. $x \xrightarrow{f} y$
suriettiva $\overset{\text{def}}{\iff}$ per ogni $y \in Y$ esiste almeno un $x \in X$ t.c. $x \xrightarrow{f} y$
biiettiva $\overset{\text{def}}{\iff}$ per ogni $y \in Y$ esiste unico $x \in X$ t.c. $x \xrightarrow{f} y$

Note: 1) $f : X \to Y$, $g : Y \to Z$ funzioni
f, g *iniettive* $\Rightarrow g \circ f$ *iniettiva* $\Rightarrow f$ *iniettiva*
f, g suriettive $\Rightarrow g \circ f$ suriettiva $\Rightarrow g$ suriettiva
2) f^{-1} funzione $\Leftrightarrow f$ biiettiva $\Leftrightarrow f$ *iniettiva* e suriettiva

Esempi: $P, R, \mathcal{A}, \mathcal{I}, \rho, \sigma$ definiti sopra, $(r_1, r_2) \in \mathcal{I}$, $p_0 = \sigma(r_1, r_2)$
$\rho_| : P \times P - \Delta P \to R$ funz. suriettiva non *iniettiva*
$\rho_| : r_1 \times r_2 - \{(p_0, p_0)\} \to R$ funz. *iniettiva* non suriettiva
$\rho_| : r_1 \times r_2 - \{(p_0, p_0)\} \to \mathcal{I}(r_1) \cap \mathcal{I}(r_2) - \mathcal{A}(p_0)$ funz. biiettiva

Relazioni su un insieme

$\mathcal{R} \subset X^n$ relazione n-aria su X

Esempi: 1) $\mathcal{I}$ e $\mathcal{P}$ definite sopra sono relazioni binarie su R
2) $\mathcal{L} = \{(p_1, p_2, p_3) \mid p_1, p_2, p_3$ allineati$\}$ rel. ternaria su P
3) $\mathcal{T} = \{(p_1, p_2, p_3) \mid p_2$ sta tra p_1 e $p_2\}$ rel. ternaria su P

$\mathcal{R}$ relazione binaria su X
riflessiva $\overset{\text{def}}{\iff} \Delta X \subset \mathcal{R}$ (cioè: $x \mathcal{R} x$, $\forall\, x \in X$)
antiriflessiva $\overset{\text{def}}{\iff} \mathcal{R} \cap \Delta X = \varnothing$ (cioè: $x \mathcal{R} y \Rightarrow x \neq y$)
simmetrica $\overset{\text{def}}{\iff} \mathcal{R} = \mathcal{R}^{-1}$ (cioè: $x \mathcal{R} y \Rightarrow y \mathcal{R} x$)
antisimmetrica $\overset{\text{def}}{\iff} \mathcal{R} \cap \mathcal{R}^{-1} = \Delta X$ (cioè: $x \mathcal{R} y \wedge y \mathcal{R} x \Rightarrow x = y$)
transitiva $\overset{\text{def}}{\iff} \mathcal{R} \circ \mathcal{R} \subset \mathcal{R}$ (cioè: $x \mathcal{R} y \wedge y \mathcal{R} z \Rightarrow x \mathcal{R} z$)

Esempi: 1) $\mathcal{I}$ e $\mathcal{P}$ def. sopra sono antiriflessive e simmetriche
2) $\mathcal{Q} = \mathcal{P} \circ \mathcal{P}$ è riflessiva, simmetrica e transitiva

Equivalenze e quozienti

$\mathcal{R}$ relazione binaria su X
equivalenza $\overset{\text{def}}{\iff} \mathcal{R}$ riflessiva, simmetrica e transitiva

Note: 1) $\sim_{\mathcal{R}}$ notazione usuale per equivalenza
2) $f : X \to Y$ funzione $\rightsquigarrow x_1 \sim_f x_2 \Leftrightarrow f(x_1) = f(x_2)$
↖ relaz. di equiv. indotta da f

Esempi: 1) $\mathcal{P}, \mathcal{Q}$ relaz. definite sopra, $\mathcal{P}$ non equiv., $\mathcal{Q}$ equiv.
2) $T = \{\text{triangoli nel piano}\}$
$l : T \to \mathbb{R}^3$ def. $l(t) = (a \leq b \leq c) \rightsquigarrow \sim_l$ congruenza
$a : T \to \mathbb{R}^2$ def. $a(t) = (\alpha \leq \beta) \rightsquigarrow \sim_a$ similidutine
$A : T \to \mathbb{R}$ def. $A(t) = \text{Area}(t) \rightsquigarrow \sim_A$ "equivalenza"
3) $a \equiv_n b \overset{\text{def}}{\iff} n | (a - b)$ equiv. su $\mathbb{Z}$ (congruenza mod n)

$\mathcal{R}$ relazione binaria su X
$\rightsquigarrow \sim_{\mathcal{R}}$ relazione di equivalenza generata da $\mathcal{R}$
$\overset{\text{def}}{=\!=}$ più piccola relaz. di equiv. su X contenente $\mathcal{R}$
$=\!=$ intersez. di tutte le relaz. di equiv. su X contenenti $\mathcal{R}$

Nota: $x \sim_{\mathcal{R}} x' \Leftrightarrow \exists\, x_1, \ldots, x_n \in X$ con $x_1 = x$, $x_n = x'$, $n \geq 1$
t.c. $x_i \mathcal{R} x_{i+1} \vee x_{i+1} \mathcal{R} x_i$, $\forall\, i = 1, \ldots, n-1$

Esempio: per le relazioni $\mathcal{P}$ e $\mathcal{Q}$ definite sopra si ha $\mathcal{Q} = \sim_{\mathcal{P}}$

$\mathcal{R} = \sim_{\mathcal{R}}$ relazione di equivalenza su X
$\rightsquigarrow [x]_{\mathcal{R}} = \{y \in X \mid x \sim_{\mathcal{R}} y\}$ classe di equivalenza di $x \in X$
$\rightsquigarrow X/\mathcal{R} = \{[x]_{\mathcal{R}} \mid x \in X'\}$ insieme quoziente ($X' =$ ins. di rappr.)

Note: 1) le classi di equiv. formano una partizione di X
($\cup_{x\in X'}[x]_{\mathcal{R}} = \cup_{x\in X}[x]_{\mathcal{R}} = X$ in quanto $x \in [x]_{\mathcal{R}}\ \forall x \in X$,
$x \sim_{\mathcal{R}} y \Leftrightarrow [x]_{\mathcal{R}} = [y]_{\mathcal{R}} \Leftrightarrow [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} \neq \varnothing$
e quindi $x \not\sim_{\mathcal{R}} y \Leftrightarrow [x]_{\mathcal{R}} \neq [y]_{\mathcal{R}} \Leftrightarrow [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \varnothing$)
2) $\pi_{\mathcal{R}} : X \to X/\mathcal{R}$ proiezione canonica def. $\pi_{\mathcal{R}}(x) = [x]_{\mathcal{R}}$
3) $\mathcal{R}$ coincide con la relaz. di equiv. indotta da $\pi_{\mathcal{R}}$
(infatti: $[x]_{\mathcal{R}} \in X/\mathcal{R} \rightsquigarrow \pi_{\mathcal{R}}^{-1}([x_{\mathcal{R}}]) = [x]_{\mathcal{R}} \subset X$)
4) $f : X \to Y$ funzione $\rightsquigarrow X \xrightarrow{\pi} X/\sim_f \leftrightarrow f(X) \subset Y$

Esempi: 1) $R, \mathcal{Q}$ def. come sopra $\rightsquigarrow R/\mathcal{Q} = \{\text{direzioni del piano}\}$
2) $\mathbb{Z}_n \overset{\text{def}}{=\!=} \mathbb{Z}/\equiv_n = \{[0]_n, \ldots, [n-1]_n\}$ classi di resto mod n
3) $\mathbb{Z} \leftrightarrow (\mathbb{N}\times\mathbb{N})/\sim$ con $(a,b) \sim (a',b') \Leftrightarrow a + b' = a' + b$
3) $\mathbb{Q} \leftrightarrow (\mathbb{Z}\times\mathbb{N})/\sim$ con $(a,b) \sim (a',b') \Leftrightarrow a\,b' = a'b$

Insiemi ordinati

$\mathcal{R}$ relazione binaria su X
ordine $\overset{\text{def}}{\Longleftrightarrow}$ $\mathcal{R}$ riflessiva, antisimmetrica e transitiva
ordine stretto $\overset{\text{def}}{\Longleftrightarrow}$ $\mathcal{R}$ antiriflessiva, antisimmetrica e transitiva
ordine totale $\overset{\text{def}}{\Longleftrightarrow}$ $\mathcal{R}$ ordine t.c. $X^2 - \Delta X \subset \mathcal{R} \cup \mathcal{R}^{-1}$
(cioè: $x \neq y \Rightarrow x\,\mathcal{R}\,y \vee y\,\mathcal{R}\,x$)

Note: 1) $\leq_{\mathcal{R}}$ e $<_{\mathcal{R}}$ notaz. usuali per ordine e ordine stretto
2) $\mathcal{R}$ ordine su $X \leftrightsquigarrow \mathcal{S}$ ordine stretto su X
(infatti: $\mathcal{R} \rightsquigarrow \mathcal{S} = \mathcal{R} - \Delta X$ e $\mathcal{S} \rightsquigarrow \mathcal{R} = \mathcal{S} \cup \Delta X$)

$(X, \leq)$ insieme ordinato (con $\leq$ relazione di ordine su X)
$S \subset X$ limitato inf. $\overset{\text{def}}{\Longleftrightarrow} \exists\, l \in X$ t.c. $l \leq s, \forall\, s \in S$ (l limite inf.)
limitato sup. $\overset{\text{def}}{\Longleftrightarrow} \exists\, l \in X$ t.c. $s \leq l, \forall\, s \in S$ (l limite sup.)
limitato $\overset{\text{def}}{\Longleftrightarrow}$ limitato inf. e sup.
$\rightsquigarrow \min S = s \in S$ t.c. s limite inf. per S (minimo)
$\max S = s \in S$ t.c. s limite sup. per S (massimo)

$\rightsquigarrow \inf S = \max\{l \in X \text{ t.c. } l \text{ lim. inf. per } S\}$ (estremo inf.)
$\sup S = \min\{l \in X \text{ t.c. } l \text{ lim. sup. per } S\}$ (estremo sup.)

Note: 1) $s = \min S \Leftrightarrow s = \inf S \in S$, $s = \max S \Leftrightarrow s = \sup S \in S$
2) $\min S, \max S, \inf S, \sup S$ sono unici (se esistono)
3) $\leq$ ordine totale, $S \neq \varnothing$ finito $\Rightarrow \min S$ e $\max S$ esistono (per induzione su $|S|$ = cardinalità di S)

Esempi: 1) $(\mathbb{N}, \leq)$ totalm. ordinato, limitato inf. ma non sup.
$\varnothing \neq S \subset \mathbb{N} \Rightarrow \exists \min S$ ($\leftsquigarrow$ principio di induzione)
2) $(\mathbb{Z}, \leq)$ totalm. ordinato, illimitato inf. e sup.
$\varnothing \neq S \subset \mathbb{Z}$ limitato inf. (sup.) $\Rightarrow$ esiste $\min S$ ($\max S$)
3) $(\mathbb{Q}, \leq)$ totalm. ordinato, illimitato inf. e sup.
$S = \{q \in \mathbb{Q} \mid q > 0\} \rightsquigarrow \inf S = 0 \notin S$ ($\nexists \min S$)
$S = \{q \in \mathbb{Q} \mid q > \sqrt{2}\} \rightsquigarrow$ non esiste $\inf S$
4) $(\mathbb{R}, \leq)$ totalm. ordinato, illimitato inf. e sup.
$\varnothing \neq S \subset \mathbb{R}$ limitato inf. (sup.) $\Rightarrow$ esiste $\inf S$ ($\sup S$)
5) $(P(X), \subset)$ ordinato non totalm., limitato inf. e sup.
$\varnothing \neq S \subset P(X) \Rightarrow \inf S = \cap_{Y \in S} Y$, $\sup S = \cup_{Y \in S} Y$

$(X, \leq)$ insieme totalmente ordinato
denso $\overset{\text{def}}{\Longleftrightarrow} \forall\, x_1, x_2 \in X,\ x_1 < x_2 \Rightarrow \exists\, x \in X$ t.c. $x_1 < x < x_2$
completo $\overset{\text{def}}{\Longleftrightarrow} \forall \varnothing \neq S \subset X$ limitato inf. (sup.) $\exists \inf S$ ($\sup S$)

Esempi: 1) $(\mathbb{Z}, \leq)$ non denso, ma completo (numerabile)
2) $(\mathbb{Q}, \leq)$ denso, ma non completo (numerabile)
3) $(\mathbb{R}, \leq)$ denso e completo (non numerabile)

Operazioni su un insieme

$X^n \to X$ funzione $(x_1, \ldots, x_n) \mapsto x_1 \cdot \ldots \cdot x_n$ operaz. n-aria su X

Esempi: 1) operazioni su $P = \{\text{punti del piano}\}$
$(p_1, p_2) \mapsto p_1 \star p_2 = \text{punto medio}(p_1, p_2)$ oper. binaria
$(p_1, p_2, p_3) \mapsto p_1 \star p_2 \star p_3 = \text{baric.}(p_1, p_2, p_3)$ oper. ternaria
2) $\circ$ operaz. binaria su $\operatorname{Rel} X = \{\mathcal{R} : X \to X \text{ relazione}\}$,
$\operatorname{Fun} X = \{f : X \to X \text{ funz.}\}$ e $\Sigma_X = \{f : X \to X \text{ biiett.}\}$

3) $+$ e $\times$ (usuali) sono operaz. binarie su $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$
4) $-$ (usuale) non è operaz. bin. su $\mathbb{N}$, ma lo è su $\mathbb{Z}$ e $\mathbb{Q}$
5) / (usuale) non è operaz. bin. su $\mathbb{Q}$, ma lo è su $\mathbb{Q}-\{0\}$

$(x_1, x_2) \mapsto x_1 \cdot x_2$ operaz. binaria su X
associativa $\overset{\text{def}}{\iff} x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$, $\forall\, x_1, x_2, x_3 \in X$
commutativa $\overset{\text{def}}{\iff} x_1 \cdot x_2 = x_2 \cdot x_1$, $\forall\, x_1, x_2 \in X$
$e \in X$ elemento neutro $\overset{\text{def}}{\iff} e \cdot x = x = x \cdot e$, $\forall\, x \in X$
$\overline{x} \in X$ elemento inverso di $x \in X \overset{\text{def}}{\iff} \overline{x} \cdot x = e = x \cdot \overline{x}$

Note: 1) operaz. associativa = il risultato di più operazioni non dipende dall'ordine di esecuzione $\rightsquigarrow x_1 \cdot \ldots \cdot x_n$
2) operaz. commutativa = il risultato di un'operazione non dipende dall'ordine degli operandi
3) elemento neutro unico se esiste $(e = e \cdot e' = e')$
associativa $\Rightarrow$ inverso di x unico se esiste
$(\overline{x} = \overline{x} \cdot (x \cdot \overline{x}') = (\overline{x} \cdot x) \cdot \overline{x}' = \overline{x}')$

Esempi: 1) $\star$ op. def. sopra commutativa, ma non associativa
2) $\circ$ (comp. di appl.) associativa, ma non commutativa

Gruppi

$G = (G, \cdot\,)$ gruppo (con $\cdot$ operazione binaria su G)
$\overset{\text{def}}{\iff}$ 1) $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3 \;\; \forall\, x_1, x_2, x_3 \in G$ (associativa)
2) $\exists\, e \in G$ t.c. $e \cdot x = x = x \cdot e$, $\forall\, x \in G$ (elemento neutro)
3) $\forall\, x \in G \;\exists\, \overline{x} \in X$ t.c. $\overline{x} \cdot x = e = x \cdot \overline{x}$ (inverso di x)

$G = (G, \cdot\,)$ gruppo commutativo (o abeliano)
$\overset{\text{def}}{\iff}$ 1),2),3) e 4) $x_1 \cdot x_2 = x_2 \cdot x_1$, $\forall\, x_1, x_2 \in G$ (prop. comm.)

Esempi: 1) $(\mathbb{N}, +)$ non è gruppo ($\nexists$ elemento neutro)
$(\mathbb{Z}, +)$ gruppo comm. (0 elem. neutro, $\overline{x} = -x$ opposto)
2) $(\mathbb{Z}, \cdot\,)$ non è gruppo (1 elem. neutro, ma $\nexists$ inversi)
$(\mathbb{Q}, \cdot\,)$ non è gruppo (1 elem. neutro, ma $\nexists$ inv. di 0)
$(\mathbb{Q}-\{0\}, \cdot\,)$ gruppo comm. (1 elem. neutro, $\overline{x} = x^{-1}$)

3) $(\mathrm{Fun}\, X, \circ)$ e $(\mathrm{Rel}\, X, \circ)$ non sono gruppi
(id_X elem. neutro, ma $\nexists$ inversi: $\mathcal{R} \circ \mathcal{R}^{-1} \neq \mathrm{id}_X$)
$\Sigma_X = (\Sigma_X, \circ)$ gruppo delle permutazioni su X
non commutativo (id_X elem. neutro, $\overline{f} = f^{-1}$)

$H \subset G = (G, \cdot)$ sottogruppo
$\overset{\text{def}}{\iff}$ $H = (H, \cdot)$ gruppo con l'operaz. di G ristretta ad H
$\iff$ 1) $H \neq \varnothing$ $(e \in H)$
2) $x_1, x_2 \in H \Rightarrow x_1 \cdot x_2 \in H$
3) $x \in H \Rightarrow \overline{x} \in H$

$S \subset G$ sottoinsieme $\rightsquigarrow \langle S \rangle \subset G$ sottogruppo generato da S
$\langle S \rangle \overset{\text{def}}{=}$ più piccolo sottogruppo di G contenente S
$=$ intersezione di tutti i sottogruppi di G contenenti S
$= \{x_1 \cdot \ldots \cdot x_n \mid x_i \in S \text{ o } \overline{x}_i \in S\,, n \geq 0\}$

Note: 1) $x \in G \rightsquigarrow \langle x \rangle \subset G$ sottogruppo ciclico generato da x
($\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$ dove $x^0 = e$, $x^k = x \cdot \ldots \cdot x$ se $k > 0$,
$x^k = \overline{x} \cdot \ldots \cdot \overline{x}$ se $k < 0$)
2) notazione moltiplicativa per gruppi: $(x_1, x_2) \mapsto x_1 \cdot x_2$,
$e = 1$ (unità), $\overline{x} = x^{-1}$ (inverso), $x^k = x^{\pm 1} \cdot \ldots \cdot x^{\pm 1}$ (pot.)
notazione additiva per gruppi comm.: $(x_1, x_2) \mapsto x_1 + x_2$,
$e = 0$ (zero), $\overline{x} = -x$ (opposto), $k\,x = \pm x \pm \ldots \pm x$ (mult.)

$S \subset G$ insieme di generatori $\overset{\text{def}}{\iff} G = \langle S \rangle$
G gruppo ciclico $\overset{\text{def}}{\iff} \exists\, x \in G$ tale che $G = \langle x \rangle$ (x generatore di G)
G finitamente generato $\overset{\text{def}}{\iff} \exists\, S \subset G$ insieme finito di generatori

Esempi: 1) $(\mathbb{Z}, +)$ ciclico infinito (1 e -1 entrambi generatori)
2) $(\mathbb{Z}_n, +)$ ciclico di ordine n ($[k]_n$ gener. $\Leftrightarrow (k, n) = 1$)
3) $(\mathbb{Q}, +)$ e $(\mathbb{R}, +)$ non finitamente generati
4) $\Sigma_n \overset{\text{def}}{=} \Sigma_{\{1,\ldots,n\}}$ gruppo simmetrico di grado n
(costituito da $n!$ permutaz. $(\sigma(1), \ldots, \sigma(n))$, $\sigma \in \Sigma_n$)
non ciclico, finit. gener. da $\{\tau_{i,j}$ trasposizione $\mid i \neq j\}$
($\tau_{i,j}$ def. $\tau_{i,j}(i) = j$, $\tau_{i,j}(j) = i$, $\tau_{i,j}(k) = k$ $\forall\, k \neq i, j$)

$\varphi : G \to H$ applicazione tra $G = (G, \cdot_G)$ e $H = (H, \cdot_H)$ gruppi
omomorfismo $\overset{\text{def}}{\iff} \varphi(x_1 \cdot_G x_2) = \varphi(x_1) \cdot_H \varphi(x_2)$, $\forall\, x_1, x_2 \in G$
isomorfismo $\overset{\text{def}}{\iff} \varphi$ omomorfismo biiettivo

$G \cong H \overset{\text{def}}{\iff} \exists\, \varphi : G \to H$ isomorfismo
$\quad\uparrow$ gruppi isomorfi

Note: 1) $\varphi(e_G) = e_H$, $\varphi(x^{-1}) = \varphi(x)^{-1}$ per ogni $x \in G$
2) $G' \subset G$ sottogruppo $\Rightarrow \varphi(G') \subset H$ sottogruppo
3) $H' \subset H$ sottogruppo $\Rightarrow \varphi^{-1}(H') \subset G$ sottogruppo
4) $\varphi : G \to H$ e $\psi : H \to K$ omo. $\Rightarrow \psi \circ \varphi : G \to K$ omo.
5) $\varphi : G \to H$ isomorfismo $\Rightarrow \varphi^{-1} : H \to G$ isomorfismo
$\quad\hookrightarrow \cong$ è una "relazione di equivalenza" tra gruppi

Esempi: 1) $\exp : (\mathbb{R}, +) \to (\mathbb{R} - \{0\}, \cdot\,)$ definita $\exp(x) = e^x$
2) $\eta : \mathbb{Z}_2 \to (\{-1, 1\}, \cdot\,)$ definita $\eta([n]_2) = (-1)^n$
3) $\pi : \Sigma_n \to \mathbb{Z}_2$ definita $\pi(\sigma) = [\#\{\sigma\text{-scambi}\}]_2$ (parit)
4) $\operatorname{sgn} = \eta \circ \pi : \Sigma_n \to (\{-1, 1\}, \cdot\,)$ (segno)

$H \subset G$ sottogruppo, $x \in G$
$\rightsquigarrow x_1 \sim_H x_2 \overset{\text{def}}{\iff} x_1 \cdot x_2^{-1} \in H$ relaz. di equiv. (congruenza mod H)
$\rightsquigarrow [x]_H = H \cdot x \overset{\text{def}}{=\!=} \{h \cdot x \mid h \in H\}$ laterale (destro) di H in G

$H \subset G$ sottogruppo normale
$\overset{\text{def}}{\iff} H \cdot x = x \cdot H \overset{\text{def}}{=\!=} \{x \cdot h \mid h \in H\}$ per ogni $x \in G$
$\iff H = x \cdot H \cdot x^{-1}$ per ogni $x \in G$ (H invariante per coniugio)
$\rightsquigarrow (H \cdot x_1) \cdot (H \cdot x_2) = H \cdot (x_1 \cdot x_2)$ per ogni $x_1, x_2 \in G$
$\rightsquigarrow G/H = (\{H \cdot x \mid x \in G\}, \cdot\,)$ gruppo quoziente

Nota: G gruppo comm. $\Rightarrow$ ogni sottogruppo di G è normale

Esempi: 1) $(\mathbb{Z}_n, +) \cong (\mathbb{Z}, +)/n\,\mathbb{Z}$ con $n\,\mathbb{Z} = \{n\,k \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$
2) $(\mathbb{R}, +)/2\pi\,\mathbb{Z}$ gruppo degli angoli orientati (rotazioni)

$\varphi : G \to H$ omomorfismo
$\rightsquigarrow \operatorname{Im}\varphi \overset{\text{def}}{=\!=} \varphi(G) \subset H$ sottogruppo (immagine di φ)
$\quad \operatorname{Ker}\varphi \overset{\text{def}}{=\!=} \varphi^{-1}(e_H) \subset G$ sottogruppo normale (nucleo di φ)

Note: 1) $\varphi : G \to H$ omomorfismo $\rightsquigarrow G \xrightarrow{\pi} G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi \subset H$
2) $\varphi : G \to H$ omomorfismo *iniettivo* $\Leftrightarrow \operatorname{Ker}\varphi = \{e_G\}$
$(\varphi(x) = y \Rightarrow \varphi^{-1}(y) = \operatorname{Ker}\varphi \cdot x\,,\ \forall\, x \in G)$

Gruppi di trasformazioni

$\varphi : G \times X \to X$ azione del gruppo G sull'*insieme* X
$\overset{\text{def}}{\Longleftrightarrow}$ 1) $\varphi(e_G, x) = x\,,\ \forall\, x \in X$
2) $\varphi(g_1 \cdot g_2, x) = \varphi(g_2, \varphi(g_1, x))\,,\ \forall\, g_1, g_2 \in G\ \forall\, x \in X$
$\Longleftrightarrow \Phi : G \to \Sigma_X$ definito $\Phi(g)(x) = \varphi_g(x) = \varphi(g, x)$ omomorfismo

$\varphi : G \times X \to X$ azione di G su X
effettiva $\overset{\text{def}}{\Longleftrightarrow} \Phi : G \to \Sigma_X$ *iniettiva* $(\Rightarrow G \cong \Phi(G) = T \subset \Sigma_X)$
gruppo di trasformazioni
libera $\overset{\text{def}}{\Longleftrightarrow} \varphi_g(x) \neq x\,,\ \forall\, g \in G - \{e_G\}\ \forall\, x \in X$ $(\Rightarrow$ effettiva$)$
transitiva $\overset{\text{def}}{\Longleftrightarrow} \forall\, x_1, x_2 \in X\ \exists\, g \in G$ tale che $\varphi_g(x_1) = x_2$
semplicemente transitiva $\overset{\text{def}}{\Longleftrightarrow}$ libera e transitiva

Esempi: 1) azione di $G = (\mathbb{R}, +)$ su $X = \{$rette del piano$\}$ con
$\varphi_x : X \to X$ *indotta* da rotaz. di x rad. centrata *in* O
azione non effettiva e non transitiva
2) $G = (\mathbb{R}, +)/2\pi\mathbb{Z} \rightsquigarrow$ azione effettiva, non libera/trans.
3) $X = \{$rette orientate$\} \rightsquigarrow$ azione libera, non transitiva
4) $X = \{$rette orient. per $O\} \rightsquigarrow$ azione sempl. transitiva

$\varphi : G \times X \to X$ azione di G su X
$\rightsquigarrow x_1 \sim_G x_2 \overset{\text{def}}{\Longleftrightarrow} \exists\, g \in G$ tale che $\varphi_g(x_1) = x_2$
relazione di equivalenza *indotta* dall'azione
$\rightsquigarrow \operatorname{Orb}_\varphi(x) \overset{\text{def}}{=\!=} [x]_G = [x]_{\sim_G} = \{\varphi_g(x) \mid g \in G\}$ φ-orbita di $x \in X$
$\rightsquigarrow X/G \overset{\text{def}}{=\!=} X/\sim_G = \{\operatorname{Orb}_\varphi(x) \mid x \in X\}$ insieme delle orbite

Note: 1) $G_x = \{g \in G \mid \varphi_g(x) = x\}$ sottogr. stabilizzatore di x
2) $\operatorname{Orb}_\varphi(x) \leftrightarrow G/G_x =$ *insieme* (non gruppo) quoziente
risp. all'azione naturale di G_x su G

3) φ azione libera $\Leftrightarrow G_x = \{e_G\}$ per ogni $x \in X$
φ azione transitiva $\Leftrightarrow \mathrm{Orb}_\varphi(x) = X$ per ogni $x \in X$

Esempi: 1) T = gruppo di trasformazioni del piano
X = *insieme di figure* (sottoinsiemi) del piano
$\rightsquigarrow$ azione di T su X se $t(x) \in X \ \forall\, t \in T \ \forall\, x \in X$
$\rightsquigarrow X/T \leftrightarrow X' =$ classif. di X rispetto alla T-equiv.
T_x = gruppo delle T-simmetrie di $x \in X$
2) T = gruppo dei "movimenti rigidi", $X = \{\text{triangoli}\}$
x = scaleno,isoscele,equilatero $\Rightarrow T_x \cong \{\mathrm{id}\}, \mathbb{Z}_2, \Sigma_3$

Campi

$K = (K, +, \cdot\,)$ campo (con $+$ e $\cdot$ operazioni binarie su K)
$\overset{\text{def}}{\Longleftrightarrow}$ 1) $(K, +)$ gruppo comm. con elemento neutro 0_K
cioè: 1a) $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$, $\forall\, x_1, x_2, x_3 \in K$
1b) $x + 0_K = x = 0_K + x$, $\forall\, x \in K$
1c) $\forall\, x \in K \ \exists\, -x \in K$ t.c. $x + (-x) = 0_K = (-x) + x$
1d) $x_1 + x_2 = x_2 + x_1$, $\forall\, x_1, x_2 \in K$
2) $(K - \{0_K\}, \cdot\,)$ gruppo comm. con elemento neutro 1_K
cioè: 2a) $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$, $\forall\, x_1, x_2, x_3 \in K - \{0_K\}$
2b) $x \cdot 1_K = x = 1_K \cdot x$, $\forall\, x \in K$
2c) $\forall\, x \in K \ \exists\, x^{-1} \in K$ t.c. $x \cdot x^{-1} = 1_K = x^{-1} \cdot x$
2d) $x_1 \cdot x_2 = x_2 \cdot x_1$, $\forall\, x_1, x_2 \in K$
3) $x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3)$, $\forall\, x_1, x_2, x_3 \in K$
(proprietà distributiva della somma rispetto al prodotto)

Note: 1) $x_1 \cdot x_2 = 0_K \Leftrightarrow x_1 = 0_K \wedge x_2 = 0_K$ (annull. del prododdo)
2) $1_K \neq 0_K \rightsquigarrow \langle 1_K \rangle = \{n_K \overset{\text{def}}{=\!=} n\, 1_K \mid n \in \mathbb{Z}\} \subset (K, +)$
3) $\langle 1_K \rangle \cong \mathbb{Z}_p$ con $p = 0$ o numero primo
$\mathrm{car}\, \mathbb{K} \overset{\text{def}}{=\!=} p$ (caratteristica di K)

Esempi: 1) $\mathbb{Z} = (\mathbb{Z}, +, \cdot\,)$ non è campo ($\nexists$ *inverso di* $n \neq \pm 1$)
2) $\mathbb{Z}_p = (\mathbb{Z}_p, +, \cdot\,)$ campo $\Leftrightarrow p$ *numero primo*
3) $\mathbb{Q} = (\mathbb{Q}, +, \cdot\,)$ e $\mathbb{R} = (\mathbb{R}, +, \cdot\,)$ campi

$K = (K, +, \cdot, \leq)$ campo ordinato
$\overset{\text{def}}{\iff}$ 1) $(K, +, \cdot)$ campo
2) $(K, \leq)$ totalmente ordinato
3) $x_1 \leq x_2 \Rightarrow x_1 + x_3 \leq x_2 + x_3$, $\forall\, x_1, x_2, x_3 \in K$
4) $0_K \leq x_1 \wedge 0_K \leq x_2 \Rightarrow 0_K \leq x_1 x_2$, $\forall\, x_1, x_2 \in K$

Note: 1) K campo ordinato $\Rightarrow 0_K < 1_K \Rightarrow \operatorname{car} K = 0$
inoltre $0_k \leq x \Leftrightarrow -x \leq 0_K$ ($\rightsquigarrow$ prodotto dei segni)
2) K campo ordinato $\Rightarrow K$ denso $(x_1 < (x_1 + x_2)/2 < x_2)$

$K = (K, +, \cdot, \leq)$ campo ordinato archimedeo
$\overset{\text{def}}{\iff}$ K campo ordinato t.c. $\forall\, 0_K \leq x \in K$, $\exists\, n_K$ t.c. $x \leq n_K$

Note: 1) K campo ordinato completo $\Rightarrow$ archimedeo
2) $\mathbb{Q} = (\mathbb{Q}, +, \cdot, \leq)$, $\mathbb{R} = (\mathbb{R}, +, \cdot, \leq)$ campi archimedei

Campo dei numeri reali

$(q_n)_{n\geq 1} \subset \mathbb{Q}$ successione di Cauchy
$\overset{\text{def}}{\iff}$ $\forall\, m \geq 1$ $\exists\, n_m \geq 1$ t.c. $|q_i - q_j| < 1/m$ $\forall\, i, j > n_m$
$(q_n)_{n\geq 1} \sim (q'_n)_{n\geq 1}$ successioni di Cauchy equivalenti
$\overset{\text{def}}{\iff}$ $(q_1, q'_1, q_2, q'_2, \ldots, q_n, q'_n, \ldots)$ successione di Cauchy

$\mathbb{R} \leftrightarrow \{(q_n)_{n\geq 1} \subset \mathbb{Q} \text{ successione di Cauchy}\} / \sim$

Note: 1) $(q_n)_{n\geq 1} \subset \mathbb{Q}$ appross. razionali di $r = [(q_n)_{n\geq 1}] \in \mathbb{R}$
2) $\mathbb{Q} \subset \mathbb{R}$ $(q \leftrightarrow [(q)_{n\geq 1}] \in \mathbb{R}$ per ogni $q \in \mathbb{Q})$

$r = [(q_n)_{n\geq 1}]$, $r' = [(q'_n)_{n\geq 1}] \in \mathbb{R}$
$\rightsquigarrow$ $r +_{\mathbb{R}} r' = [(q_n +_{\mathbb{Q}} q'_n)_{n\geq 1}] \in \mathbb{R}$
$r \cdot_{\mathbb{R}} r' = [(q_n \cdot_{\mathbb{Q}} q'_n)_{n\geq 1}] \in \mathbb{R}$
$r \leq_{\mathbb{R}} r' \overset{\text{def}}{\iff} \exists\, m \geq 1$ t.c. $q_n \leq_{\mathbb{Q}} q'_n$ $\forall\, n \geq m$

Note: 1) le operazioni su $\mathbb{R}$ non dipendono dalle successioni
e coincidono con quelle di $\mathbb{Q}$ per $r, r' \in \mathbb{Q} \subset \mathbb{R}$
2) la relazione $\leq$ è un ordine totale denso completo su $\mathbb{R}$
e coincide con l'ordine di $\mathbb{Q}$ per $r, r' \in \mathbb{Q} \subset \mathbb{R}$

Campo dei numeri complessi

$\mathbb{C} = (\mathbb{C}, +, \cdot) \stackrel{\text{def}}{=\!=} \{x + y\,i \mid x, y \in \mathbb{R}\}$ con le operazioni definite:

$$(x + y\,i) + (x' + y'i) = (x + x') + (y + y')\,i$$
$$(x + y\,i) \cdot (x' + y'i) = (x\,x' - y\,y') + (x\,y' + x'y)\,i$$

Note: 1) $\mathbb{R} \subset \mathbb{C}$ $(x \leftrightarrow x + 0\,i$ per ogni $x \in \mathbb{R})$
le operazioni di $\mathbb{C}$ estendono quelle di $\mathbb{R}$
2) $\mathbb{C} = (\mathbb{C}, +, \cdot)$ è un campo (non ordinato)
$((x + y\,i)^{-1} = (x - y\,i)/(x^2 + y^2)\,,\ \forall\, x + y\,i \in \mathbb{C})$
3) $i^2 = i \cdot i = -1$ $(i =$ unità immaginaria$)$

$z = x + y\,i \in \mathbb{C}$
$\rightsquigarrow \operatorname{Re} z = x \in \mathbb{R}$ parte reale di z
$\operatorname{Im} z = y \in \mathbb{R}$ parte immaginaria di z
$\rightsquigarrow \overline{z} = x - y\,i \in \mathbb{C}$ coniugato di z
$\rightsquigarrow |z| = \sqrt{z \cdot \overline{z}} = \sqrt{x^2 + y^2} \in \mathbb{R}$ modulo di z

Note: 1) $z = z_1 + z_2 \Rightarrow \overline{z} = \overline{z}_1 + \overline{z}_2\,,\ \forall\, z_1, z_2 \in \mathbb{C}$
$z = z_1 \cdot z_2 \Rightarrow \overline{z} = \overline{z}_1 \cdot \overline{z}_2\,,\ \forall\, z_1, z_2 \in \mathbb{C}$
$z = \overline{z} \Leftrightarrow z = \operatorname{Re} z \Leftrightarrow z \in \mathbb{R}$
2) $|z| \geq 0\ \forall\, z \in \mathbb{C}$ e $|z| = 0 \Leftrightarrow z = 0$
$z = z_1 + z_2 \Rightarrow |z| \leq |z_1| + |z_2|\,,\ \forall\, z_1, z_2 \in \mathbb{C}$
$z = z_1 \cdot z_2 \Rightarrow |z| = |z_1| \cdot |z_2|\,,\ \forall\, z_1, z_2 \in \mathbb{C}$
$|z| = \pm z \Leftrightarrow z \in \mathbb{R}$

$x = r\cos\vartheta,\ y = r\sin\vartheta$ $(\text{con } r \geq 0 \text{ e } \vartheta \in \mathbb{R}/2\pi\,\mathbb{Z})$
$\rightsquigarrow x + y\,i = r(\cos\vartheta + i\,\sin\vartheta) = r\,e^{i\vartheta}$ (forma esponenziale)
$\rightsquigarrow r\,e^{i\vartheta} \cdot r'e^{i\vartheta'} = (r\,r')e^{i(\vartheta+\vartheta')}$ $(\text{con } \vartheta + \vartheta' \in \mathbb{R}/2\pi\,\mathbb{Z})$
$\rightsquigarrow (r\,e^{i\vartheta})^n = r^n e^{in\vartheta}$ $(\text{con } n \in \mathbb{Z} \text{ e } n\vartheta \in \mathbb{R}/2\pi\,\mathbb{Z})$

Note: 1) $e^{i\pi} + 1 = 0$ (equazione di Eulero)
2) $z = r\,e^{i\vartheta} \Rightarrow \overline{z} = r\,e^{-i\vartheta}$ e $|z| = r$
3) $(\{z \in \mathbb{C} \mid |z| = 1\} = \{e^{i\vartheta} \mid \vartheta \in \mathbb{R}/2\pi\,\mathbb{Z}\},\ \cdot\ ) \cong (\mathbb{R}, +)/2\pi\,\mathbb{Z}$

$z^n = 1 \rightsquigarrow z = e^{2ki\pi/n}$ con $k = 0, \ldots, n-1$ (radici n-esime di 1)

Nota: $C_n = (\{e^{2ki\pi/n} \mid k = 0, \ldots, n-1\}, \cdot\ ) \cong (\mathbb{Z}_n, +)$

Teorema fondamentale dell'algebra

$\mathbb{C} = (\mathbb{C}, +, \cdot\ )$ è un campo algebricamente chiuso, cioè:
$p(z) = a_n z^n + \ldots + a_1 z + a_0 \in \mathbb{C}[z]$ polinomio di grado $n \geq 1$
$\Rightarrow$ l'equazione algebrica $p(z) = 0$ ha soluzione in $\mathbb{C}$

Corol. $p(z) = a_n z^n + \ldots + a_1 z + a_0 \in \mathbb{C}[z]$ polinomio di grado $n \geq 1$
$\Rightarrow \exists\, z_1, \ldots, z_k \in \mathbb{C}$ t.c. $p(z) = a_n \cdot (z - z_1)^{\mu_1} \cdot \ldots \cdot (z - z_k)^{\mu_k}$
($z = z_i$ soluz. di molteplicità μ_i dell'equaz. alg. $p(z) = 0$)

Dim. per induzione su $n \geq 1$ a partire dal caso banale $n = 1$
$p(z_i) = 0 \Rightarrow p(z)$ divisibile per $z - z_i \in \mathbb{C}[z]$ (teor. del resto)
$\Rightarrow p(z) = (z - z_i)q(z)$ con $q(z) \in \mathbb{C}[z]$ di grado $n - 1$

Corol. $p(z) = a_n z^n + \ldots + a_1 z + a_0 \in \mathbb{R}[z]$ polinomio di grado $n \geq 1$
$\Rightarrow p(z)$ è prodotto di polinomi in $\mathbb{R}[z]$ di grado ≤ 2

Dim. per induzione su $n \geq 1$ a partire dal caso banale $n = 1$
$p(z_i) = 0$ con $z_i \in \mathbb{R}$
$\Rightarrow p(z)$ divisibile per $z - z_i \in \mathbb{R}[z]$
$\Rightarrow p(z) = (z - z_i)q(z)$ con $q(z) \in \mathbb{R}[z]$ di grado $n - 1$
$p(z_i) = 0$ con $z_i \notin \mathbb{R}$
$\Rightarrow p(\overline{z}_i) = 0$ $(a_n \overline{z}_i^n + \ldots a_1 \overline{z}_i + a_0 = \overline{a_n z_i^n + \ldots a_1 z_i + a_0} = 0)$
$\Rightarrow p(z)$ divisibile per $(z - z_i)(z - \overline{z}_i) \in \mathbb{R}[z]$
$\Rightarrow p(z) = (z - z_i)(z - \overline{z}_i)q(z)$ con $q(z) \in \mathbb{R}[z]$ di grado $n - 2$

Note: 1) $\mathbb{R}$ non è algebric. chiuso ($x^2 + 1 = 0$ non ha sol. in $\mathbb{R}$),
$\mathbb{C}$ è il più piccolo campo algebric. chiuso contenente $\mathbb{R}$
2) $p(z) \in \mathbb{C}[z]$ irriducibile $\Leftrightarrow$ grado $= 1$
$p(z) \in \mathbb{R}[z]$ irriducibile $\Leftrightarrow$ grado $= 1$ o $= 2$ con $\Delta < 0$
3) $p(z) \in \mathbb{R}[z]$ di grado dispari
$\Rightarrow$ l'equazione algebrica $p(z) = 0$ ha soluzione in $\mathbb{R}$