Aritmetica

Luca De Paulis

9 agosto 2020

INDICE

1 | GRUPPI

1.1 INTRODUZIONE AI GRUPPI

Definizione 1.1.1 **Gruppo.** Sia $G \neq \varnothing$ un insieme e sia $*$ un'operazione su G, ovvero

$$*: G \times G \to G$$
$$(a, b) \mapsto a * b.$$

Allora la struttura $(G, *)$ si dice *gruppo* se valgono i seguenti assiomi:

(G1) L'operazione $*$ è *associativa*:
per ogni $a, b, c \in G$ vale che $a * (b * c) = (a * b) * c$.

(G2) Esiste un elemento $e_G \in G$ che fa da *elemento neutro* rispetto all'operazione $*$:
per ogni $a \in G$ vale che $a * e_G = e_G * a = a$.

(G3) Ogni elemento di G è *invertibile* rispetto all'operazione $*$:
per ogni $a \in G$ esiste $a^{-1} \in G$ tale che $a * a^{-1} = a^{-1} * a = e_G$.
Tale a^{-1} si dice *inverso di* a.

Definizione 1.1.2 **Gruppo abeliano.** Sia $(G, *)$ un gruppo. Allora $(G, *)$ si dice *gruppo abeliano* se vale inoltre

(G4) l'operazione $*$ è commutativa, ovvero

$$\forall a, b \in G \quad a * b = b * a.$$

L'elemento neutro di G si può rappresentare come e_G, id_G, 1_G o semplicemente e nel caso sia evidente il gruppo a cui appartiene.

Possiamo rappresentare un gruppo in *notazione moltiplicativa*, come abbiamo fatto finora, oppure in *notazione additiva*, spesso usata quando si studiano gruppi abeliani.

In notazione additiva, ovvero considerando un gruppo $(G, +)$ gli assiomi diventano

(G1) l'operazione $+$ è associativa, ovvero

$$\forall a, b, c \in G. \quad a + (b + c) = (a + b) + c$$

(G2) esiste un elemento $e_G \in G$ che fa da elemento neutro rispetto all'operazione $+$:

$$\forall a \in G. \quad a + e_G = e_G + a = a$$

(G3) ogni elemento di G è invertibile rispetto all'operazione $+$:

$$\forall a \in G \ \ \exists(-a) \in G. \quad a + (-a) = (-a) + a = e_G.$$

Per semplicità spesso si scrive $a - b$ per intendere $a + (-b)$.

(G4) l'operazione $+$ è commutativa, ovvero

$$\forall a, b \in G \quad a + b = b + a.$$

Facciamo alcuni esempi di gruppi.

ESEMPIO 1.1.3. Sono gruppi abeliani $(\mathbb{Z}, +)$ e le sue estensioni $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, come è ovvio verificare.

ESEMPIO 1.1.4. $(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo, definendo l'operazione di somma rispetto alle classi di resto.

ESEMPIO 1.1.5. è un gruppo la struttura $(\mu_n, \cdot)$ dove

$$\mu_n := \{ x \in \mathbb{C} : x^n = 1 \}.$$

Dimostrazione. Infatti

(G0) $\cdot$ è un'operazione su μ_n. Infatti se $x, y \in \mu_n$, ovvero

$$x^n = y^n = 1$$

allora segue anche che

$$(xy)^n = x^n y^n = 1$$

da cui $xy \in \mu_n$;

(G1) $\cdot$ è associativa in $\mathbb{C}$, dunque lo è in $\mu_n \subseteq \mathbb{C}$;

(G2) $1 \in \mathbb{C}$ è l'elemento neutro di $\cdot$ e $1 \in \mu_n$ in quanto $1^n = 1$;

(G3) ogni elemento di μ_n ammette inverso. Infatti sia $x \in \mu_n$, dunque $x \neq 0$ (altrimenti $x^n = 0 \neq 1$) e sia $x^{-1} \in \mathbb{C}$ il suo inverso. Allora

$$(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$$

ovvero $x^{-1} \in \mu_n$;

(G4) inoltre $\cdot$ è commutativa in $\mathbb{C}$, dunque lo è anche in μ_n.

Da ciò segue che μ_n è un gruppo abeliano. □

ESEMPIO 1.1.6. $(\mathbb{Z}^\times, \cdot)$ dove

$$\mathbb{Z}^\times := \{ n \in \mathbb{Z} : n \text{ è invertibile rispetto a } \cdot \} = \{ \pm 1 \}$$

è un gruppo abeliano;

ESEMPIO 1.1.7. $(\mathbb{Z}/n\mathbb{Z}^\times, \cdot)$ dove

$$\mathbb{Z}/n\mathbb{Z}^\times := \{ \overline{n} \in \mathbb{Z}/n\mathbb{Z} : \overline{n} \text{ è invertibile rispetto a } \cdot \}$$

è un gruppo abeliano.

Dimostrazione. Infatti

(G0) $\cdot$ è un'operazione su $\mathbb{Z}/n\mathbb{Z}$. Infatti se $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ allora segue anche che $\overline{xy}$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$ e il suo inverso è $\overline{x^{-1}} \cdot \overline{y^{-1}}$, da cui $\overline{xy} \in \mathbb{Z}/n\mathbb{Z}$;

(G1) $\cdot$ è associativa in $\mathbb{Z}/n\mathbb{Z}$, dunque lo è in $\mathbb{Z}/n\mathbb{Z}^\times \subseteq \mathbb{Z}/n\mathbb{Z}$;

(G2) $1 \in \mathbb{Z}/n\mathbb{Z}$ è l'elemento neutro di $\cdot$ e $1 \in \mathbb{Z}/n\mathbb{Z}^\times$ in quanto 1 è invertibile e il suo inverso è 1;

(G3) ogni elemento di $\mathbb{Z}/n\mathbb{Z}^\times$ ammette inverso per definizione;

(G4) inoltre $\cdot$ è commutativa in $\mathbb{Z}/n\mathbb{Z}$, dunque lo è in $\mathbb{Z}/n\mathbb{Z}^\times \subseteq \mathbb{Z}/n\mathbb{Z}$.

Da ciò segue che $\mathbb{Z}/n\mathbb{Z}$ è un gruppo abeliano. □

Esempio 1.1.8. Se X è un insieme e $\mathcal{S}(X)$ è l'insieme

$$\mathcal{S}(X) := \{ f : X \to X \,:\, f \text{ è bigettiva} \}$$

allora $(\mathcal{S}(X), \circ)$ è un gruppo (dove $\circ$ è l'operazione di composizione tra funzioni).

Dimostrazione. Infatti

(G0) se $f, g \in \mathcal{S}(X)$ allora $f \circ g : X \to X$ è bigettiva, dunque $f \circ g \in \mathcal{S}(X)$;

(G1) l'operazione di composizione di funzioni è associativa;

(G2) la funzione

$$\begin{aligned} \mathrm{id} : X &\to X \\ x &\mapsto x \end{aligned}$$

è bigettiva ed è l'elemento neutro rispetto alla composizione;

(G3) Se $f \in \mathcal{S}(X)$ allora f è invertibile ed esisterà $f^{-1} : X \to X$ tale che $f \circ f^{-1} = \mathrm{id}$. Ma allora f^{-1} è invertibile e la sua inversa è f, dunque f^{-1} è bigettiva e quindi $f^{-1} \in \mathcal{S}(X)$.

Dunque $\mathcal{S}(X)$ è un gruppo (non necessariamente abeliano). □

Esempi di strutture che non rispettano le proprietà di un gruppo sono invece:

- $(\mathbb{N}, +)$ poichè nessun numero ha inverso ($-n \notin \mathbb{N}$);
- $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ e $(\mathbb{C}, \cdot)$ non sono gruppi in quanto 0 non ha inverso moltiplicativo;
- l'insieme
$$\{ x \in \mathbb{C} \,:\, x^n = 2 \}$$
in quanto il prodotto due elementi di questo insieme non appartiene più all'insieme.

Definiamo ora alcune proprietà comuni a tutti i gruppi.

Proposizione 1.1.9 **Proprietà algebriche dei gruppi.** *Sia $(G, \cdot)$ un gruppo. Allora valgono le seguenti affermazioni:*

(i) l'elemento neutro di G è unico;

(ii) $\forall g \in G$ l'inverso di g è unico;

(iii) $\forall g \in G \;\; (g^{-1})^{-1} = g$;

(iv) $\forall h, g \in G \;\; (hg^{-1})^{-1} = g^{-1}h^{-1}$;

(v) Valgono le leggi di cancellazione*: $\forall a, b, c \in G$ vale che*

$$ab = ac \iff b = c \qquad \text{(sx)}$$
$$ba = ca \iff b = c \qquad \text{(dx)}$$

Dimostrazione. (i) Siano $e_1, e_2 \in G$ entrambi elementi neutri. Allora

$$e_1 = e_1 \cdot e_2 = e_2$$

dove il primo uguale viene dal fatto che e_2 è elemento neutro, mentre il secondo viene dal fatto che e_1 lo è.

(ii) Siano $x, y \in G$ entrambi inversi di qualche $g \in G$. Allora per definizione di inverso

$$xg = gx = e = gy = yg.$$

Ma allora segue che

$$\begin{aligned} & x && \text{(el. neutro)} \\ &= x \cdot e && (e = gy) \\ &= x(gy) && \text{(per (G1))} \\ &= (xg)y && (xg = e) \\ &= e \cdot y && \text{(el. neutro)} \\ &= g \end{aligned}$$

ovvero $x = y = g^{-1}$.

(iii) Sappiamo che $gg^{-1} = g^{-1}g = e$. Sia x l'inverso di g^{-1}, ovvero

$$g^{-1}x = xg^{-1} = e.$$

Dunque g è un inverso di g^{-1}, ma per 1.1.9: (ii) l'inverso è unico e quindi $(g^{-1})^{-1} = g$.

(iv) Sia $(hg)^{-1}$ l'inverso di hg. Allora per (G3) sappiamo che

$$\begin{aligned} & (hg)(hg)^{-1} = e && \text{(moltiplico a sx per } h^{-1}\text{)} \\ \iff & h^{-1}hg(hg)^{-1} = h^{-1} && \text{(per (G3))} \\ \iff & g(hg)^{-1} = h^{-1} && \text{(moltiplico a sx per } g^{-1}\text{)} \\ \iff & g^{-1}g(hg)^{-1} = g^{-1}h^{-1} && \text{(per (G3))} \\ \iff & (hg)^{-1} = g^{-1}h^{-1}. \end{aligned}$$

(v) Legge di cancellazione sinistra:

$$\begin{aligned} & ab = ac && \text{(moltiplico a sx per } a^{-1}\text{)} \\ \iff & a^{-1}ab = a^{-1}ac && \text{(per (G3))} \\ \iff & b = c. \end{aligned}$$

Legge di cancellazione destra:

$$\begin{aligned} & ba = ca && \text{(moltiplico a dx per } a^{-1}\text{)} \\ \iff & baa^{-1} = caa^{-1} && \text{(per (G3))} \\ \iff & b = c. && \square \end{aligned}$$

1.2 SOTTOGRUPPI

Definizione 1.2.1 **Sottogruppo.** Sia $(G, *)$ un gruppo e sia $H \subseteq G$, $H \neq \emptyset$.
Allora H insieme ad un'operazione $*_H$ si dice *sottogruppo* di $(G, *)$ se $(H, *_H)$ è un gruppo.
Inoltre se l'operazione $*_H$ è l'operazione $*$, ovvero l'operazione del sottogruppo è indotta da G, allora si scrive $H \leqslant G$.

Proposizione 1.2.2 **Condizione necessaria e sufficiente per i sottogruppi.** *Sia $(G, *)$ un gruppo e sia $H \subseteq G$, $H \neq \emptyset$.*
Allora $H \leqslant G$ se e solo se

(i) $*$ *è un'operazione su* H*, ovvero*

$$a * b \in H \qquad \forall a, b \in H$$

(ii) ogni elemento di H *è invertibile (in* H*), ovvero*

$$h^{-1} \in H \qquad \forall h \in H$$

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Ovvio in quanto se $H \leqslant G$ allora H è un gruppo.

($\Longleftarrow$) Sappiamo che $*$ è associativa poichè lo è in G; dobbiamo quindi mostrare solamente che $e_G \in H$.

Per ipotesi $H \neq \emptyset$, dunque esiste un $h \in H$. Per l'ipotesi 1.2.2: (ii) dovrà esistere anche $h^{-1} \in H$, mentre per l'ipotesi 1.2.2: (i) deve valere che $h * h^{-1} \in H$.

Tuttavia $h * h^{-1} = e_G$, dunque $e_G \in H$ e quindi H è un sottogruppo indotto da G.

Da ciò viene la tesi. □

Un sottogruppo particolarmente importante di qualsiasi gruppo è il *centro del gruppo*:

Definizione 1.2.3 **Centro di un gruppo.** Sia $(G, *)$ un gruppo. Allora si definisce *centro di* G l'insieme

$$Z(G) := \{\, x \in G \,:\, g * x = x * g \;\; \forall g \in G \,\}.$$

Intuitivamente, il centro di un gruppo è l'insieme di tutti gli elementi per cui $*$ diventa commutativa.

Mostriamo che il centro di un gruppo è un sottogruppo tramite la prossima proposizione.

Proposizione 1.2.4 **Proprietà del centro di un gruppo.** *Sia* $(G, *)$ *un gruppo e sia* $Z(G)$ *il suo centro.*

Allora vale che

(i) $Z(G) \leqslant G$*;*

(ii) $Z(G) = G$ *se e solo se* G *è abeliano.*

Dimostrazione. Mostriamo le due affermazioni separatamente

$Z(G)$ **È UN SOTTOGRUPPO** Notiamo innanzitutto che $Z(G) \neq \varnothing$ poichè $e_G \in Z(G)$. Per la proposizione 1.2.2 ci basta mostrare che $*$ è un'operazione su $Z(G)$ e che ogni elemento di $Z(G)$ è invertibile.

(1) Siano $x, y \in Z(G)$ e mostriamo che $x * y \in Z(G)$, ovvero che per ogni $g \in G$ vale che $g * (x * y) = (x * y) * g$.

$$\begin{aligned}
& g * (x * y) && \text{(per (G1))} \\
&= (g * x) * y && \text{(dato che } x \in \mathbb{Z}(G)\text{)} \\
&= (x * g) * y && \text{(per (G1))} \\
&= x * (g * y) && \text{(dato che } x \in \mathbb{Z}(G)\text{)} \\
&= x * (y * g) && \text{(per (G1))} \\
&= (x * y) * g.
\end{aligned}$$

(2) Sia $x \in Z(G)$, mostriamo che $x^{-1} \in Z(G)$.
Per ipotesi

$$\begin{aligned} & g * x = x * g && \text{(moltiplico a sinistra per } x^{-1}\text{)} \\ \iff\ & x^{-1} * g * x = x^{-1} * x * g && \text{(dato che } x^{-1} * x = e\text{)} \\ \iff\ & x^{-1} * g * x = g && \text{(moltiplico a destra per } x^{-1}\text{)} \\ \iff\ & x^{-1} * g * x * x^{-1} = g * x^{-1} && \text{(dato che } x^{-1} * x = e\text{)} \\ \iff\ & x^{-1} * g = g * x^{-1} \end{aligned}$$

da cui $x^{-1} \in Z(G)$.

Per la proposizione 1.2.2 segue che $Z(G) \leqslant G$.

$Z(G) = G$ **SE E SOLO SE** G **ABELIANO** Dimostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Ovvia: $Z(G)$ è un gruppo abeliano, dunque se $G = Z(G)$ allora G è abeliano.

($\Longleftarrow$) Ovvia: $Z(G)$ è l'insieme di tutti gli elementi di G per cui $*$ commuta, ma se G è abeliano questi sono tutti gli elementi di G, ovvero $Z(G) = G$. □

Un altro esempio è dato dai sottogruppi di $(\mathbb{Z}, +)$.

Definizione 1.2.5 **Insieme dei multipli interi.** Sia $n \in \mathbb{Z}$. Allora chiamo $n\mathbb{Z}$ l'insieme dei multipli interi di n

$$n\mathbb{Z} := \{\, nk : k \in \mathbb{Z} \,\}.$$

È semplice verificare che $(n\mathbb{Z}, +)$ è un gruppo per ogni $n \in \mathbb{Z}$. In particolare vale la seguente proposizione.

Proposizione 1.2.6 $n\mathbb{Z}$ **è sottogruppo di** $\mathbb{Z}$. *Consideriamo il gruppo* $(\mathbb{Z}, +)$. *Per ogni* $n \in \mathbb{Z}$ *vale che* $n\mathbb{Z} \leqslant \mathbb{Z}$.

Dimostrazione. Innanzitutto notiamo che $n\mathbb{Z} \neq \varnothing$ in quanto $n \cdot 0 = 0 \in n\mathbb{Z}$.
Mostriamo ora che $n\mathbb{Z} \leqslant \mathbb{Z}$.

(1) Siano $x, y \in n\mathbb{Z}$ e mostriamo che $x + y \in \mathbb{Z}$.
Per definizione di $n\mathbb{Z}$ esisteranno $k, h \in \mathbb{Z}$ tali che $x = nk$, $y = nh$.
Allora $x + y = nk + nh = n(k + h) \in n\mathbb{Z}$ in quanto $k + h \in \mathbb{Z}$.

(2) Sia $x \in n\mathbb{Z}$, mostriamo che $-x \in n\mathbb{Z}$.
Per definizione di $n\mathbb{Z}$ esisterà $k \in \mathbb{Z}$ tale che $x = nk$.
Allora affermo che $-x = n(-k) \in n\mathbb{Z}$. Infatti

$$x + (-x) = nk + n(-k) = n(k - k) = 0$$

che è l'elemento neutro di $\mathbb{Z}$.

Dunque per la proposizione 1.2.2 segue che $n\mathbb{Z} \leqslant \mathbb{Z}$, ovvero la tesi. □

Corollario 1.2.7 *Siano* $n, m \in \mathbb{Z}$. *Allora valgono i due fatti seguenti:*

(i) $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n$;

(ii) $n\mathbb{Z} = m\mathbb{Z} \iff n = \pm m$.

Dimostrazione. Dimostriamo le due affermazioni separatamente.

PARTE 1. Dimostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Supponiamo $n\mathbb{Z} \subseteq m\mathbb{Z}$, ovvero che per ogni $x \in n\mathbb{Z}$ allora $x \in m\mathbb{Z}$.
Sia $k \in \mathbb{Z}$ tale che $(k, m) = 1$ e sia $x = nk$.
Per definizione di $n\mathbb{Z}$ segue che $x \in n\mathbb{Z}$, dunque $x \in m\mathbb{Z}$. Allora dovrà esistere $h \in \mathbb{Z}$ tale che

$$\begin{aligned} & x = mh \\ \iff & nk = mh \\ \implies & m \mid nk \end{aligned}$$

Ma abbiamo scelto k tale che $(k, m) = 1$, dunque

$$\implies m \mid n.$$

($\Longleftarrow$) Supponiamo che $m \mid n$, ovvero $n = mh$ per qualche $h \in \mathbb{Z}$. Allora

$$n\mathbb{Z} = (mh)\mathbb{Z} \subseteq m\mathbb{Z}$$

in quanto i multipli di mh sono necessariamente anche multipli di m.

PARTE 2. Se $n\mathbb{Z} = m\mathbb{Z}$ allora vale che $n\mathbb{Z} \subseteq m\mathbb{Z}$ e $m\mathbb{Z} \subseteq n\mathbb{Z}$, dunque per 1.2.7: (i) $m \mid n$ e $n \mid m$, ovvero n e m sono uguali a meno del segno. □

Proposizione 1.2.8 **Intersezione di sottogruppi è un sottogruppo.** *Sia* $(G, \cdot)$ *un gruppo e siano* $H, K \leqslant G$.
Allora $H \cap K \leqslant G$.

Dimostrazione. Innanzitutto dato che $e_G \in H$, $e_G \in K$ segue che $e_G \in H \cap K$, che quindi non può essere vuoto.
Per la proposizione 1.2.2 è sufficiente dimostrare che $H \cap K$ è chiuso rispetto all'operazione $\cdot$ e che ogni elemento è invertibile.

(i) Siano $x, y \in H \cap K$; mostriamo che $xy \in H \cap K$.
Per definizione di intersezione sappiamo che $x, y \in H$ e $x, y \in K$. Dato che H è un gruppo varrà che $xy \in H$; per lo stesso motivo $xy \in K$; dunque $xy \in H \cap K$.

(ii) Sia $x \in H \cap K$; mostriamo che $x^{-1} \in H \cap K$.
Per definizione di intersezione sappiamo che $x \in H$ e $x \in K$. Dato che H è un gruppo varrà che $x^{-1} \in H$; per lo stesso motivo $x^{-1} \in K$; dunque $x^{-1} \in H \cap K$.

Dunque per la proposizione 1.2.2 segue che $H \cap K \leqslant G$. □

1.3 GENERATORI E GRUPPI CICLICI

Innanzitutto diamo una definizione generale di potenze:

Definizione 1.3.1 **Potenze intere.** Sia $(G, \cdot)$ un gruppo e sia $g \in G$ qualsiasi.

Allora definiamo g^k per $k \in \mathbb{Z}$ nel seguente modo:

$$g^k := \begin{cases} e_G & \text{se } k = 0 \\ g \cdot g^{k-1} & \text{se } k > 0 \\ (g^{-1})^k & \text{se } k < 0. \end{cases}$$

Se il gruppo è definito in notazione additiva, le potenze diventano prodotti per numeri interi.

Piu' formalmente, se $(G, +)$ è un gruppo e $g \in G$ qualsiasi, allora definiamo ng per $n \in \mathbb{Z}$ nel seguente modo:

$$ng := \begin{cases} e_G & \text{se } n = 0 \\ g + (n-1)g & \text{se } n > 0 \\ (-n)(-g) & \text{se } n < 0. \end{cases}$$

Le potenze intere soddisfano alcune proprietà interessanti, verificabili facilmente per induzione, tra cui

(P1) per ogni $n, m \in \mathbb{Z}$ vale che $g^m g^n = g^{n+m}$,

(P2) per ogni $n, m \in \mathbb{Z}$ vale che $(g^n)^m = g^{nm}$.

Definizione 1.3.2 **Sottogruppo generato.** Sia $(G, \cdot)$ un gruppo e sia $g \in G$.
Allora si dice *sottogruppo generato da* g l'insieme

$$\langle g \rangle := \left\{ g^k : k \in \mathbb{Z} \right\}.$$

Proposizione 1.3.3 **Il sottogruppo generato è un sottogruppo abeliano.** *Sia* $(G, \cdot)$ *un gruppo e sia* $g \in G$ *qualsiasi.*
Allora $\langle g \rangle \leqslant G$. *Inoltre* $\langle g \rangle$ *è abeliano.*

Dimostrazione. Innanzitutto notiamo che $\langle g \rangle \neq \varnothing$ in quanto $g \in \langle g \rangle$. Mostriamo che $\langle g \rangle$ è un sottogruppo indotto da G.

(i) Se $g^n, g^m \in \langle g \rangle$ allora $g^n g^m = g^{n+m} \in \langle g \rangle$ in quanto $n + m \in \mathbb{Z}$;

(ii) Sia $g^n \in \langle g \rangle$. Per definizione di potenza, g^{-n} è l'inverso di g^n e $g^{-n} \in \langle g \rangle$ in quanto $-n \in \mathbb{Z}$.

Dunque per la proposizione 1.2.2 segue che $\langle g \rangle \leqslant G$.
Inoltre notiamo che

$$g^n g^m = g^{n+m} = g^{m+n} = g^m g^n$$

dunque $\langle g \rangle$ è abeliano. □

Notiamo che, al contrario di quanto succede con i numeri interi, può succedere che $g^h = g^k$ per qualche $h \neq k$.

Supponiamo senza perdita di generalità $k > h$. In tal caso

$$\begin{aligned} & g^{k-h} = e_G \\ \implies\ & g^{k-h+1} = g^{k-h} \cdot g \\ & = e_G \cdot g \\ & = g. \end{aligned}$$

Dunque il sottogruppo generato da g non è infinito, ovvero

$$|\langle g \rangle| < +\infty.$$

Questo ci consente di parlare di ordine di un elemento di un gruppo:

Definizione 1.3.4 **Ordine di un elemento di un gruppo.** Sia $(G, \cdot)$ un gruppo e sia $x \in G$. Allora si dice ordine di x in G il numero

$$\operatorname{ord}_G(x) := \min\left\{ k > 0 : x^k =_G e \right\}.$$

Se l'insieme $\left\{ k > 0 : x^k = e_G \right\}$ è vuoto, allora per definizione

$$\operatorname{ord}_G(x) := +\infty.$$

Quando il gruppo di cui stiamo parlando sarà evidente scriveremo semplicemente $\operatorname{ord}(x)$.

Proposizione 1.3.5 **Scrittura esplicita del sottogruppo generato.** *Sia $(G, \cdot)$ un gruppo e sia $x \in G$ tale che $\operatorname{ord}_G(x) = d < +\infty$.*
Allora valgono i seguenti due fatti:

(i) Il sottogruppo generato $\langle x \rangle$ è

$$\langle x \rangle = \left\{ e, x, x^2, \dots, x^{d-1} \right\}.$$

Dunque in particolare $|\langle x \rangle| = d$.

(ii) $x^n = e \iff d \mid n$.

Dimostrazione. Dimostriamo le due affermazioni separatamente.

PARTE 1. Sicuramente vale che

$$\left\{ e, x, \dots, x^{d-1} \right\} \subseteq \langle x \rangle.$$

Dimostriamo che vale l'uguaglianza.
Sia $k \in \mathbb{Z}$ qualsiasi. Allora $x^k \in \langle x \rangle$.
Dimostriamo che necessariamente $x^k \in \left\{ e, x, \dots, x^{d-1} \right\}$.
Per la divisione euclidea esisteranno $q, r \in \mathbb{Z}$ tali che

$$k = qd + r \qquad \text{con } 0 \leqslant r < d.$$

Allora sostituendo $k = qd + r$ otteniamo

$$\begin{aligned} x^k &= x^{qd+r} \\ &= x^{qd} x^r \\ &= e^q x^r \\ &= x^r. \end{aligned}$$

Per ipotesi $0 \leqslant r < d$, dunque $x^r \in \left\{ e, x, \dots, x^{d-1} \right\}$. Dato che $x^r = x^k$ concludiamo che

$$x^k \in \left\{ e, x, \dots, x^{d-1} \right\}$$

e quindi

$$\langle x \rangle = \left\{ e, x, \dots, x^{d-1} \right\}.$$

Ci rimane da mostrare che $|\langle x \rangle| = d$, ovvero che tutti gli elementi di $\langle x \rangle$ sono distinti.

Supponiamo per assurdo che esistano $a, b \in \mathbb{Z}$ con $0 \leqslant a < b < d$ (senza perdita di generalità) tali che $x^a = x^b$.

Da questo segue che $x^{b-a} = e$, ma questo è assurdo poichè $b - a < d$ e per definizione l'ordine è il minimo numero positivo per cui $x^d = e$.

Di conseguenza tutti gli elementi di $\langle x \rangle$ sono distinti, ovvero $|\langle x \rangle| = d$.

PARTE 2. Dimostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Sia $n \in \mathbb{Z}$ tale che $x^n = e$.

Per divisione euclidea esistono $q, r \in \mathbb{Z}$ tali che

$$n = qd + r \qquad \text{con } 0 \leqslant r < d.$$

Dunque $x^n = x^{qd+r} = x^r = e$. Ma questo è possibile solo se $r = 0$, altrimenti andremmo contro la minimalità dell'ordine.

Dunque $x = qd$, ovvero $d \mid n$.

($\Longleftarrow$) Ovvia: se $n = kd$ per qualche $k \in \mathbb{Z}$ allora

$$x^n = x^{kd} = (x^d)^k = e^k = e.$$

□

Definizione 1.3.6 **Gruppo ciclico.** Sia $(G, \cdot)$ un gruppo.
Allora G si dice *ciclico* se esiste un $g \in G$ tale che

$$G = \langle g \rangle.$$

L'elemento g viene detto *generatore* del gruppo G.

Ad esempio $\mathbb{Z}$ è un gruppo ciclico, in quanto $\mathbb{Z} = \langle 1 \rangle$, come lo è $n\mathbb{Z} = \langle n \rangle$. Questi due gruppi sono anche infiniti, in quanto contengono un numero infinito di elementi.

Un esempio di gruppo ciclico finito è $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle$, che è finito in quanto $\operatorname{ord}_{\mathbb{Z}/n\mathbb{Z}}([1]_n) = n$.

Teorema 1.3.7 **Ogni sottogruppo di un gruppo ciclico è ciclico.** *Sia $(G, \cdot)$ un gruppo ciclico, ovvero $G = \langle g \rangle$ per qualche $g \in G$. Sia inoltre $H \leqslant G$ un sottogruppo.*
Allora H è ciclico, ovvero esiste $h \in \mathbb{Z}$ tale che $H = \langle g^h \rangle$.

Dimostrazione. Innanzitutto notiamo che $e_G \in H$.

Se $H = \{ e_G \}$ allora H è ciclico, e $H = \langle e_G \rangle$.

Assumiamo $\{ e \}_G \subset H$. Allora esiste $k \in \mathbb{Z}$, $k \neq 0$ tale che $g^k \in H$. Dato che per (G3) se $g^k \in H$ allora $g^{-k} \in H$ possiamo supporre senza perdita di generalità $k > 0$.

Consideriamo l'insieme S tale che

$$S := \left\{ h > 0 \,:\, g^h \in H \right\} \subseteq \mathbb{N}.$$

Avendo assunto $k \in S$ sappiamo che $S \neq \varnothing$, dunque per il principio del minimo S ammette minimo.

Sia $h_0 = \min S$. Mostro che $H = \langle g^{h_0} \rangle$.

($\supseteq$) Per ipotesi $g^{h_0} \in H$.

Dato che H è un sottogruppo di G tutte le potenze intere di g^{h_0} dovranno appartenere ad H, ovvero $\langle g^{h_0} \rangle \subseteq H$.

($\subseteq$) Sia $n \in \mathbb{N}$ tale che $g^n \in H$. Dimostriamo che $g^n \in \langle g^{h_0} \rangle$.

Per divisione euclidea esistono $q, r \in \mathbb{Z}$ tali che

$$n = qh_0 + r \qquad \text{con } 0 \leqslant r < h_0.$$

Dunque

$$\begin{aligned} g^n &= g^{qh_0 + r} \\ &= g^{qh_0} g^r. \end{aligned}$$

Moltiplicando entrambi i membri per g^{-qh_0} otteniamo

$$\iff g^n g^{-qh_0} = g^r.$$

Ma $g^n \in H$ e $g^{-qh_0} \in H$ (in quanto è una potenza intera di g^{h_0}), dunque anche il loro prodotto $g^r \in H$.
Se $r > 0$ allora esisterebbe una potenza di g con esponente positivo minore di h_0 contenuto in H, che è assurdo in quanto abbiamo assunto che h_0 sia il minimo dell'insieme S.
Segue che $r = 0$, ovvero $n = qh_0$, ovvero che $g^n \in \langle g^{h_0} \rangle$, ovvero $H \subseteq \langle g^{h_0} \rangle$.

Concludiamo quindi che $H = \langle g^{h_0} \rangle$, ovvero H è ciclico. □

Consideriamo i sottogruppi di $\mathbb{Z}$. Tramite la proposizione 1.2.6 abbiamo dimostrato che per ogni $n \in \mathbb{Z}$ allora $n\mathbb{Z} \leqslant \mathbb{Z}$. La prossima proposizione mostra che i sottogruppi della forma $n\mathbb{Z} = \langle n \rangle$ sono gli unici possibili.

Proposizione 1.3.8 **Caratterizzazione dei sottogruppi di $\mathbb{Z}$.** *I sottogruppi di $\mathbb{Z}$ sono tutti e solo della forma $n\mathbb{Z}$ al variare di $n \in \mathbb{N}$.*

Dimostrazione. Nella proposizione 1.2.6 abbiamo mostrato che $n\mathbb{Z} \leqslant \mathbb{Z}$ per ogni $n \in \mathbb{Z}$. Ora mostriamo che è sufficiente considerare $n \in \mathbb{N}$ e che questi sono gli unici sottogruppi possibili.

Dato che $\mathbb{Z}$ è ciclico (poiché $\mathbb{Z} = \langle 1 \rangle$) per il teorema 1.3.7 ogni suo sottogruppo dovrà essere ciclico, ovvero dovrà essere della forma $\langle n \rangle$ per qualche $n \in \mathbb{N}$.

Per la proposizione 1.2.7: (ii) sappiamo che $n\mathbb{Z} = (-n)\mathbb{Z}$, dunque possiamo considerare (senza perdita di generalità) n positivo o nullo, ovvero $n \in \mathbb{N}$.

Ma $\langle n \rangle = n\mathbb{Z}$, dunque i sottogruppi di $\mathbb{Z}$ sono tutti e solo della forma $n\mathbb{Z}$ al variare di $n \in \mathbb{N}$. □

1.3.1 Il gruppo ciclico $\mathbb{Z}/n\mathbb{Z}$

In questa sezione analizzeremo il gruppo ciclico $(\mathbb{Z}/n\mathbb{Z}, +)$, anche definito da

$$\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle = \langle \overline{1} \rangle.$$

L'ordine di $\overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$ è n. Infatti

$$\begin{aligned} & x \cdot \overline{1} = \overline{0} \\ \iff & x \equiv 0 \pmod{n} \\ \iff & x = nk \end{aligned}$$

con $k \in \mathbb{Z}$. La minima soluzione positiva a quest'equazione è per $k = 1$, dunque $x = n$. Per la proposizione 1.3.5: (i) sappiamo quindi che

$$|\mathbb{Z}/n\mathbb{Z}| = |\overline{1}| = \operatorname{ord}_{\mathbb{Z}/n\mathbb{Z}}(\overline{1}) = n. \tag{1}$$

Proposizione 1.3.9 **Ordine degli elementi di $\mathbb{Z}/n\mathbb{Z}$.** *Sia $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ qualsiasi. Allora vale che*

$$\operatorname{ord}(\overline{a}) = \frac{n}{(a, n)}$$

dove $a \in \mathbb{Z}$ è un rappresentante della classe $\overline{a}$.

Dimostrazione. Per definizione di ordine

$$\operatorname{ord}(\overline{a}) = \min \left\{ k > 0 : k\overline{a} = \overline{0} \right\}.$$

Si tratta quindi di trovare la minima soluzione positiva di $ax \equiv 0 \ (n)$. Divido entrambi i membri e il modulo per a, ottenendo

$$x \equiv 0 \left(\frac{n}{(n,a)}\right) \implies x = \frac{n}{(n,a)}t$$

al variare di $t \in \mathbb{Z}$.

Dato che siamo interessati alla minima soluzione positiva, questa è ottenuta per $t = 1$, da cui segue che

$$\operatorname{ord}(\overline{a}) = \frac{n}{(n,a)}. \qquad \square$$

Corollario 1.3.10 **Conseguenze della proposizione 1.3.9.** *Consideriamo il gruppo* $(\mathbb{Z}/n\mathbb{Z}, +)$. *Valgono le seguenti affermazioni:*

(i) $\forall \overline{a} \in \mathbb{Z}/n\mathbb{Z}. \quad \operatorname{ord}(\overline{a}) \mid n.$

(ii) $\mathbb{Z}/n\mathbb{Z}$ *ha* $\varphi(n)$ *generatori.*

(iii) Sia $d \in \mathbb{Z}$ *tale che* $d \mid n$. *Allora in* $\mathbb{Z}/n\mathbb{Z}$ *ci sono esattamente* $\varphi(d)$ *elementi di ordine* d.

Dimostrazione. (i) Ovvia in quanto (per la proposizione 1.3.9) $\operatorname{ord}(\overline{a}) = \dfrac{n}{(n,a)} \mid n$.

(ii) Sia $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$. Sappiamo che $\overline{x}$ è un generatore di $\mathbb{Z}/n\mathbb{Z}$ se

$$\langle \overline{x} \rangle = \mathbb{Z}/n\mathbb{Z}$$

ovvero se la cardinalità di $\langle \overline{x} \rangle$ è n.

Per la proposizione 1.3.9 $\operatorname{ord}(\overline{x}) = \dfrac{n}{(n,x)}$, dunque $\overline{x}$ è un generatore se e solo se $(n, x) = 1$, ovvero se x è coprimo con n.

Ma ci sono $\varphi(n)$ numeri coprimi con n, dunque ci sono $\varphi(n)$ generatori di $\mathbb{Z}/n\mathbb{Z}$.

(iii) Sia $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ tale che

$$\operatorname{ord}(\overline{a}) = \frac{n}{(n,a)} = d.$$

Allora $(n, a) = \dfrac{n}{d}$, da cui segue che $\dfrac{n}{d} \mid a$.

Sia $b \in \mathbb{Z}$ tale che $a = \dfrac{n}{d}b$. Dato che $(n, a) = \dfrac{n}{d}$ segue che

$$\begin{aligned} &\left(n, \frac{n}{d}b\right) = \frac{n}{d} \\ \iff &\left(\frac{n}{d}d, \frac{n}{d}b\right) = \frac{n}{d} \\ \iff &\frac{n}{d}(d, b) = \frac{n}{d} \\ \iff &(d, b) = 1 \end{aligned}$$

ovvero se e solo se d e b sono coprimi.

Dunque segue che ho $\varphi(d)$ scelte per b, ovvero ho $\varphi(d)$ elementi di ordine d.

$\square$

Questo corollario ci consente di enunciare una proprietà della funzione $\varphi(\cdot)$.

Corollario 1.3.11 **Espressione per n in termini di $\varphi(n)$.** *Sia $n \in \mathbb{Z}$. Allora vale che*

$$n = \sum_{d|n} \varphi(d).$$

Dimostrazione. Sia X_d l'insieme

$$X_d := \{\, \overline{a} \in \mathbb{Z}/n\mathbb{Z} \,:\, \operatorname{ord}(\overline{a}) = d \,\}.$$

Se $d \nmid n$ per la proposizione 1.3.10: (i) segue che $X_d = \varnothing$.
Dunque abbiamo che

$$\mathbb{Z}/n\mathbb{Z} = \bigsqcup_{d|n} X_d.$$

Sfruttando la proposizione 1.3.10: (iii) sappiamo che $|X_d| = \varphi(d)$, dunque passando alle cardinalità segue che

$$|\mathbb{Z}/n\mathbb{Z}| = n = \sum_{d|n} X_d.$$

□

Studiamo ora i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$.

Proposizione 1.3.12 **Caratterizzazione dei sottogruppi di $\mathbb{Z}/n\mathbb{Z}$.** *Studiamo il gruppo $(\mathbb{Z}/n\mathbb{Z}, +)$. Valgono i due seguenti fatti:*

(i) Sia $H \leqslant \mathbb{Z}/n\mathbb{Z}$. Allora H è ciclico e $|H| = d$ per qualche $d \mid n$.

(ii) Sia $d \in \mathbb{Z}$, $d \mid n$. Allora $\mathbb{Z}/n\mathbb{Z}$ ammette uno e un solo sottogruppo di ordine d.

Dimostrazione. (i) Sia $H \leqslant \mathbb{Z}/n\mathbb{Z}$; per il teorema 1.3.7 sappiamo che H deve essere ciclico, ovvero $H = \langle \overline{h} \rangle$ per qualche $\overline{h} \in \mathbb{Z}/n\mathbb{Z}$.
Sia $d = \operatorname{ord}(\overline{h})$. Allora per il corollario 1.3.10: (i) segue che

$$|H| = \operatorname{ord}(\overline{h}) = d \mid n.$$

(ii) Sia H_d l'insieme

$$H_d = \left\{ \overline{0},\ \frac{\overline{n}}{d},\ 2\frac{\overline{n}}{d}, \ldots,\ (d-1)\frac{\overline{n}}{d} \right\}.$$

Mostriamo innanzitutto che $H_d = \left\langle \frac{\overline{n}}{d} \right\rangle$.

Infatti ovviamente $H_d \subseteq \left\langle \frac{\overline{n}}{d} \right\rangle$. Per mostrare che sono uguali basta notare che

$$\left| \left\langle \frac{\overline{n}}{d} \right\rangle \right| = \operatorname{ord}\left(\frac{\overline{n}}{d}\right) = \frac{n}{\left(\frac{n}{d}, n\right)} = \frac{n}{\left(\frac{n}{d}, \frac{n}{d}d\right)} = \frac{n}{\frac{n}{d}(1, d)} = d$$

dunque i due insiemi sono finiti, hanno la stessa cardinalità e il primo è incluso nel secondo, da cui segue che sono uguali.
Sia ora $H \leqslant \mathbb{Z}/n\mathbb{Z}$ tale che $|H| = d$. Per il teorema 1.3.7 segue che $H = \langle \overline{x} \rangle$ per qualche $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ tale che $\operatorname{ord}(\overline{x}) = d$.
Seguendo la dimostrazione di 1.3.10: (iii) possiamo scrivere $\overline{x} = \frac{\overline{n}}{d} b$ con $b \in Z$ tale che $(b, d) = 1$.

Ma $H_d = \left\langle \frac{\overline{n}}{d} \right\rangle$ contiene tutti i multipli di $\frac{\overline{n}}{d}$, dunque deve contenere anche $\overline{x}$.
Dunque dato che $\overline{x} \in H_d$ segue che $H = \langle \overline{x} \rangle \subseteq H_d$. Ma gli insiemi H e H_d hanno la stessa cardinalità, dunque $H = H_d$, ovvero vi è un solo sottogruppo di ordine d. □

1.4 OMOMORFISMI DI GRUPPI

Definizione 1.4.1 **Omomorfismo tra gruppi.** Siano $(G_1, *)$, $(G_2, \star)$ due gruppi. Allora la funzione

$$f : G_1 \to G_2$$

si dice *omomorfismo di gruppi* se per ogni $x, y \in G_1$ vale che

$$f(x * y) = f(x) \star f(y).$$

Esempio 1.4.2. Ad esempio la funzione

$$\begin{aligned} \pi_n : \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto [a]_n \end{aligned}$$

è un omomorfismo tra i gruppi $\mathbb{Z}$ e $\mathbb{Z}/n\mathbb{Z}$. Infatti vale che

$$\pi_n(a + b) = \overline{a + b} = \overline{a} + \overline{b} = \pi_n(a) + \pi_n(b).$$

Questo particolare omomorfismo si dice *riduzione modulo* n.

Esempio 1.4.3. Un altro esempio è la funzione

$$\begin{aligned} f : (\mathbb{R}, +) &\to (\mathbb{R}^+, \cdot) \\ x &\mapsto e^x. \end{aligned}$$

Infatti vale che

$$f(x + y) = e^{x+y} = e^x e^y = f(x)f(y).$$

Proposizione 1.4.4 **Composizione di omomorfismi.** *Siano $(G_1, *)$, $(G_2, \star)$, $(G_3, \cdot)$ tre gruppi e siano $\varphi : G_1 \to G_2$ e $\psi : G_2 \to G_3$ omomorfismi.*
Allora la funzione $\psi \circ \varphi : G_1 \to G_3$ è un omomorfismo tra i gruppi G_1 e G_3.

Dimostrazione. Siano $h, k \in G_1$ e dimostriamo che

$$(\psi \circ \varphi)(h * k) = (\psi \circ \varphi)(h) \cdot (\psi \circ \varphi)(k).$$

Infatti vale che

$$\begin{aligned} (\psi \circ \varphi)(h * k) &= \psi(\varphi(h * k)) && (\varphi \text{ omo.}) \\ &= \psi(\varphi(h) \star \varphi(k)) && (\psi \text{ omo.}) \\ &= \psi(\varphi(h)) \cdot \psi(\varphi(k)) \\ &= (\psi \circ \varphi)(h) \cdot (\psi \circ \varphi)(k) \end{aligned}$$

che è la tesi. □

Dato che un omomorfismo è una funzione, possiamo definire i soliti concetti di immagine e controimmagine.

Definizione 1.4.5 **Immagine e controimm. di un omomorf. attraverso un insieme.** Siano $(G_1, *)$, $(G_2, \star)$ due gruppi e sia $f : G_1 \to G_2$ un omomorfismo.
Siano $H \leqslant G_1$, $K \leqslant G_2$. Allora definiamo l'insieme

$$f(H) := \{\, f(h) \in G_2 \,:\, h \in H \,\} \subseteq G_2$$

detto *immagine di* f *attraverso* H, e l'insieme

$$f^{-1}(K) := \{\, g \in G_1 \,:\, f(g) \in K \,\} \subseteq G_1$$

detto *controimmagine di* f *attraverso* K.
Definiamo inoltre l'*immagine dell'omomorfismo* f come

$$\operatorname{Im} f := f(G_1) = \{\, f(g) \in G_2 \,:\, g \in G_1 \,\}.$$

Per gli omomorfismi definiamo inoltre un concetto nuovo, il *nucleo* o *kernel* dell'omomorfismo.

Definizione 1.4.6 **Kernel di un omomorfismo.** Siano $(G_1, *)$, $(G_2, \star)$ due gruppi e sia $f : G_1 \to G_2$ un omomorfismo.
Allora si dice *kernel* o *nucleo* dell'omomorfismo f l'insieme

$$\ker f := \{\, g \in G_1 \,:\, f(g) = e_2 \,\} \subseteq G_1.$$

Osserviamo che possiamo anche esprimere il nucleo di un omomorfismo in termini della controimmagine del sottogruppo banale $\{\, e_2 \,\}$:

$$\ker f = f^{-1}(\{\, e_2 \,\}).$$

Proposizione 1.4.7 **Proprietà degli omomorfismi.** *Siano* $(G_1, \cdot)$, $(G_2, \star)$ *due gruppi e sia* $f : G_1 \to G_2$ *un omomorfismo.*
Allora valgono le seguenti affermazioni.

(i) $f(e_1) = e_2$;

(ii) $f(x^{-1}) = f(x)^{-1}$;

(iii) $\forall H \leqslant G_1. \quad f(H) \leqslant G_2$;

(iv) $\forall K \leqslant G_2. \quad f^{-1}(K) \leqslant G_1$;

(v) $f(G_1) \leqslant G_2$ *e* $\ker f \leqslant G_1$;

(vi) f *è iniettivo se e solo se* $\ker f = \{\, e_1 \,\}$.

Dimostrazione. (i) $f(e_1) \overset{\text{(el. neutro)}}{=} f(e_1 \cdot e_1) \overset{\text{(omo.)}}{=} f(e_1) \star f(e_1)$.
Applicando la legge di cancellazione 1.1.9: (v) otteniamo

$$e_2 = f(e_1).$$

(ii) Sfruttando il punto 1.4.7: (i) sappiamo che

$$e_2 = f(e_1) = f(x \cdot x^{-1}) = f(x) \star f(x^{-1})$$
$$e_2 = f(e_1) = f(x^{-1} \cdot x) = f(x^{-1}) \star f(x).$$

Dalla prima segue che $f(x^{-1})$ è inverso a destra di $f(x)$, dalla seconda che $f(x^{-1})$ è inverso a sinistra di $f(x)$.
Dunque concludiamo che $f(x^{-1})$ è inverso di $f(x)$, ovvero

$$f(x)^{-1} = f(x^{-1}).$$

(iii) Sia $H \leqslant G_1$. Dato che $H \neq \varnothing$ esisterà un $h \in H$, dunque $f(H)$ non puo' essere vuoto in quanto dovrà contenere $f(h)$ (sicuramente $e_2 \in f(H)$).
Dunque per la proposizione 1.2.2 basta mostrare che $f(H)$ è chiuso rispetto al prodotto e che l'inverso di ogni elemento di $f(H)$ è ancora in $f(H)$.

(1) Mostriamo che se $x, y \in f(H)$ allora $x \star y \in f(H)$.
Per definizione di $f(H)$ dovranno esistere $h_x, h_y \in H$ tali che $x = f(h_x)$ e $y = f(h_y)$. Allora

$$\begin{aligned} x \star y &= f(h_x) \star f(h_y) && (f \text{ è omo}) \\ &= f(h_x \cdot h_y) && H \text{ è sottogr. di } G_1 \\ &\in f(H). \end{aligned}$$

(2) Mostriamo che se $x \in f(H)$ allora $x^{-1} \in f(H)$.
Per definizione di $f(H)$ dovrà esistere $h \in H$ tale che $x = f(h)$. Dato che $H \leqslant G_1$ allora $h^{-1} \in H$.
Dunque $f(h^{-1}) \in f(H)$, ma per il punto 1.4.7: (ii) sappiamo che

$$f(h^{-1}) = f(h)^{-1} = x^{-1} \in f(H).$$

Dunque $f(H) \leqslant G_2$.

(iv) Sia $K \leqslant G_2$. Dato che $e_2 \in K$, sicuramente $f^{-1}(K) \neq \varnothing$, in quanto $e_1 = f^{-1}(e_2) \in f^{-1}(K)$.
Dunque per la proposizione 1.2.2 basta mostrare che $f^{-1}(K)$ è chiuso rispetto al prodotto e che l'inverso di ogni elemento di $f^{-1}(K)$ è ancora in $f^{-1}(K)$.

(1) Mostriamo che se $x, y \in f^{-1}(K)$ allora $x * y \in f^{-1}(K)$.
Per definizione di $f^{-1}(K)$ sappiamo che

$$\begin{aligned} x \in f^{-1}(K) &\iff f(x) \in K \\ y \in f^{-1}(K) &\iff f(y) \in K. \end{aligned}$$

Dato che $K \leqslant G_2$ allora segue che

$$f(x) \star f(y) = f(x * y) \in K$$

ovvero $x * y \in f^{-1}(K)$.

(2) Mostriamo che se $x \in f^{-1}(K)$ allora $x^{-1} \in f^{-1}(K)$.
Per definizione di $f^{-1}(K)$ sappiamo che

$$x \in f^{-1}(K) \iff f(x) \in K.$$

Dato che $K \leqslant G_2$ segue che $f(x)^{-1} \in K$, ma per il punto 1.4.7: (ii) sappiamo che $f(x)^{-1} = f(x^{-1})$, dunque

$$f(x^{-1}) \in K \implies x^{-1} \in f^{-1}(K).$$

Dunque $f^{-1}(K) \leqslant G_1$.

(v) Dato che $G_1 \leqslant G_1$ per il punto 1.4.7: (iii) segue che $\operatorname{Im} f = f(G_1) \leqslant G_2$.
Per definizione $\ker f = f^{-1}(\{ e_2 \})$; inoltre $\{ e_1 \} \leqslant G_2$, dunque per il punto 1.4.7: (iv) segue che $\ker f \leqslant G_1$.

(vi) Dimostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Supponiamo che f sia iniettivo. Allora $\left|f^{-1}(\{ e_2 \})\right| = 1$.

Tuttavia sicuramente $e_1 \in f^{-1}(\{ e_2 \}) = \ker f$ (in quanto $f(e_1) = e_2$), dunque dovrà necessariamente essere $\ker f = \{ e_1 \}$.

($\Longleftarrow$) Supponiamo che $\ker f = \{ e_1 \}$.

Siano $x, y \in G_1$ tali che $f(x) = f(y)$. Moltiplicando entrambi i membri (ad esempio a destra) per $f(y)^{-1} \in G_2$ otteniamo

$$\begin{aligned} & f(x) \star f(y)^{-1} = f(y) \star f(y)^{-1} && \text{(per la 1.4.7: (ii))} \\ \Longleftrightarrow\ & f(x) \star f(y^{-1}) = e_2 && \text{(f è omomorf.)} \\ \Longleftrightarrow\ & f(x * y^{-1}) = e_2 && \text{(def. di $\ker f$)} \\ \Longleftrightarrow\ & x * y^{-1} \in \ker f && \text{(ipotesi: $\ker f = \{ e_1 \}$)} \\ \Longleftrightarrow\ & x * y^{-1} = e_1 && \text{(moltiplico a dx per y)} \\ \Longleftrightarrow\ & x = y. \end{aligned}$$

Dunque $f(x) = f(y)$ implica che $x = y$, ovvero f è iniettivo. □

Proposizione 1.4.8 **Omomorfismi e ordine.** *Siano $(G_1, *)$, $(G_2, \star)$ due gruppi e sia $f : G_1 \to G_2$ omomorfismo.*

Allora valgono le seguenti due affermazioni

(i) per ogni $x \in G$ vale che $\operatorname{ord}_{G_2}(f(x)) \mid \operatorname{ord}_{G_1}(x)$;

(ii) f è iniettivo se e solo se $\operatorname{ord}_{G_2}(f(x)) = \operatorname{ord}_{G_1}(x)$.

Dimostrazione. Innanzitutto diciamo che se $\operatorname{ord}(x) = +\infty$ allora $\operatorname{ord}(f(x)) \mid \operatorname{ord}(x)$ qualunque sia $\operatorname{ord}(f(x))$ (anche se è $+\infty$).

(i) Sia $x \in G_1$. Se $\operatorname{ord}(x) = +\infty$ allora abbiamo finito, dunque supponiamo $\operatorname{ord}(x) = n$ per qualche $n \in \mathbb{Z}$, $n > 0$.

Per definizione di ordine questo significa che $x^n = e_1$. Allora

$$\begin{aligned} f(x)^n &= f(x) \star \cdots \star f(x) && \text{(f è omo.)} \\ &= f(x^n) \\ &= f(e_1) && \text{(prop. 1.4.7: (i))} \\ &= e_2. \end{aligned}$$

Dunque $f(x)^n = e_2$, quindi per la proposizione 1.3.5: (ii) segue che

$$\operatorname{ord}(f(x)) \mid n = \operatorname{ord}(x)\,.$$

(ii) Dimostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Supponiamo f iniettiva.

- Se $\operatorname{ord}(f(x)) = +\infty$ allora per il punto 1.4.8: (i) sappiamo che $+\infty \mid \operatorname{ord}(x)$, dunque $\operatorname{ord}(x) = +\infty = \operatorname{ord}(f(x))$.
- Se $\operatorname{ord}(f(x)) = m < +\infty$ allora

$$f(x)^m = e_2 \iff f(x) \star \cdots \star f(x) = e_2 \iff f(x^m) = e_2,$$

ovvero $x^m \in \ker f$.

Ma f è iniettiva, dunque per 1.4.7: (vi) $\ker f = \{ e_1 \}$, da cui segue che $x^m = e_1$. Dunque per la proposizione 1.3.5: (ii) segue che

$$\operatorname{ord}(x) \mid m = \operatorname{ord}(f(x)).$$

Inoltre per il punto 1.4.8: (i) sappiamo che $\operatorname{ord}(f(x)) \mid \operatorname{ord}(x)$, dunque $\operatorname{ord}(f(x)) = \operatorname{ord}(x)$.

($\Longleftarrow$) Sia $x \in \ker f$, ovvero $f(x) = e_2$. Allora

$$1 = \operatorname{ord}_{G_2}(e_2) = \operatorname{ord}(f(x)) \overset{\text{hp.}}{=} \operatorname{ord}_{G_1}(x).$$

Ma $\operatorname{ord}(x) = 1$ se e solo se $x = e_1$, ovvero $\ker f = \{ e_1 \}$, dunque per la proposizione 1.4.7: (vi) f è iniettiva.

□

1.4.1 Isomorfismi

Gli omomorfismi bigettivi sono particolarmente importanti e vanno sotto il nome di *isomorfismi*.

Definizione 1.4.9 **Isomorfismo.** Siano $(G_1, *)$, $(G_2, \star)$ due gruppi e sia $\varphi : G_1 \to G_2$ un omomorfismo.

Allora se φ è bigettivo si dice che φ è un *isomorfismo*. Inoltre i gruppi G_1 e G_2 si dicono *isomorfi* e si scrive $G_1 \cong G_2$.

Corollario 1.4.10 **Transitività della relazione di isomorfismo.** *Siano $(G_1, *)$, $(G_2, \star)$, $(G_3, \cdot)$ tre gruppi tali che $G_1 \cong G_2$ e $G_2 \cong G_3$.*

Allora $G_1 \cong G_3$.

Dimostrazione. Dato che $G_1 \cong G_2$ e $G_2 \cong G_3$ dovranno esistere due isomorfismi $\varphi : G_1 \to G_2$ e $\psi : G_2 \to G_3$.

Per la proposizione 1.4.4 la funzione $\psi \circ \varphi$ è ancora un isomorfismo; inoltre la composizione di funzioni bigettive è ancora bigettiva, da cui segue che $\psi \circ \varphi$ è un isomorfismo tra G_1 e G_3 e quindi $G_1 \cong G_3$. □

Due gruppi isomorfi sono sostanzialmente lo stesso gruppo, a meno di "cambiamenti di forma". In particolare gli isomorfismi inducono naturalmente una bigezione sui sottogruppi dei due gruppi isomorfi, come ci dice la seguente proposizione.

Proposizione 1.4.11 **Bigezione tra i sottogruppi di gruppi isomorfi.** *Siano $(G_1, *)$, $(G_2, \star)$ due gruppi e sia $\varphi : G_1 \to G_2$ un isomorfismo.*

Siano inoltre $\mathcal{H}$ e $\mathcal{K}$ tali che

$$\mathcal{H} = \{ H : H \leqslant G_1 \}, \quad \mathcal{K} = \{ K : K \leqslant G_2 \}.$$

Allora la funzione

$$\begin{aligned} f : \mathcal{H} &\to \mathcal{K} \\ H &\mapsto \varphi(H) \end{aligned}$$

è bigettiva.

Dimostrazione. Siccome $H \leqslant G_1$ e φ è un omomorfismo, allora $f(H) = \varphi(H) \leqslant G_2$ (ovvero $f(H) \in \mathcal{K}$) per la proposizione 1.4.7: (iii); dunque f è ben definita.

Definiamo ora una seconda funzione

$$\begin{aligned} g : \mathcal{K} &\to \mathcal{H} \\ K &\mapsto \varphi^{-1}(K). \end{aligned}$$

Anch'essa ben definita per la proposizione 1.4.7: (iv).

Consideriamo ora le funzioni $g \circ f$ e $f \circ g$. Per la bigettività di φ vale che

$$\begin{aligned} (g \circ f)(H) &= \varphi^{-1}(\varphi(H)) = H && \forall H \in \mathcal{H} \\ (f \circ g)(K) &= \varphi(\varphi^{-1}(K)) = K && \forall K \in \mathcal{K} \end{aligned}$$

ovvero la funzione f è bigettiva e definisce quindi una bigezione tra l'insieme dei sottogruppi di G_1 e l'insieme dei sottogruppi di G_2. □

Teorema 1.4.12 **Isomorfismi di gruppi ciclici.** *Sia $(G, \cdot)$ un gruppo ciclico. Allora*

(i) se $|G| = +\infty$ segue che $G \cong \mathbb{Z}$;

(ii) se $|G| = n < +\infty$ segue che $G \cong \mathbb{Z}/n\mathbb{Z}$.

Dimostrazione. Per ipotesi $G = \langle g \rangle = \{ g^k : k \in \mathbb{Z} \}$ per qualche $g \in G$.

(i) Se $|G| = +\infty$ allora $|\langle g \rangle| = +\infty$, ovvero per ogni $k, h \in \mathbb{Z}$ con $k \neq h$ segue che $g^k \neq g^h$. Sia allora

$$\begin{aligned} \varphi : \mathbb{Z} &\to G \\ k &\mapsto g^k. \end{aligned}$$

Per definizione di $G = \langle g \rangle$ questa funzione è surgettiva. Dato che G ha ordine infinito segue che questa funzione è iniettiva. Mostriamo che è un omomorfismo.

$$\varphi(k + h) = g^{k+h} = g^k g^h = \varphi(k)\varphi(h).$$

Dunque φ è un isomorfismo e $G \cong \mathbb{Z}$.

(ii) Dato che $|G| = n$ per la proposizione 1.3.5 sappiamo che $\operatorname{ord}(g) = n$, ovvero che $g^n = e_G$. Sia allora

$$\begin{aligned} \varphi : \mathbb{Z}/n\mathbb{Z} &\to G \\ \overline{a} &\mapsto g^a \end{aligned}$$

dove a è un generico rappresentante della classe $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$.

- Mostriamo che φ è ben definita. Siano $a, b \in \overline{a}$ e mostriamo che $\varphi(\overline{a}) = \varphi(\overline{b})$, ovvero che $g^a = g^b$.
  Per ipotesi $a \equiv b \ (n)$, ovvero $a = b + nk$ per qualche $k \in \mathbb{Z}$. Dunque
  $$g^a = g^{b+nk} = g^b (g^n)^k = g^b$$
  poiché $g^n = e_G$.
- Mostriamo che φ è un omomorfismo.
  $$\varphi(\overline{a} + \overline{b}) = g^{a+b} = g^a g^b = \varphi(\overline{a})\varphi(\overline{b}).$$

- Mostriamo che φ è surgettiva.

$$\mathrm{Im}(\varphi) = \varphi(\mathbb{Z}/n\mathbb{Z}) = \left\{ g^0, g^1, \dots, g^n \right\} = \langle g \rangle = G.$$

Ma $|\mathbb{Z}/n\mathbb{Z}| = |G|$, dunque per cardinalità φ è anche iniettiva e dunque è bigettiva. Quindi φ è un isomorfismo e $G \cong \mathbb{Z}/n\mathbb{Z}$.

□

Corollario 1.4.13 **Sottogruppi del gruppo ciclico.** *Sia $(G, \cdot)$ un gruppo ciclico.*

(i) Se G è infinito e $H \leqslant G$ allora segue che $H = \langle g^n \rangle$ per qualche $g \in G$, $n \in \mathbb{Z}$.

(ii) Se G ha ordine n finito, allora G ammette uno e un solo sottogruppo per ogni divisore di n. Inoltre se $H \leqslant G$ allora H è ciclico.

Dimostrazione. Ricordiamo che

1. i sottogruppi di $\mathbb{Z}$ sono tutti e soli della forma $n\mathbb{Z}$ al variare di $n \in \mathbb{N}$ per la Proposizione 1.3.8,
2. i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ hanno tutti cardinalità che divide n per la punto 1.3.12: (i). Inoltre, per ogni d che divide n vi è uno e un solo sottogruppo di $\mathbb{Z}/n\mathbb{Z}$ di cardinalità d, per la punto 1.3.12: (ii).
3. per la Proposizione 1.4.11 sappiamo che se $f : G_1 \to G_2$ è un isomorfismo, allora

$$\{ K : K \leqslant G_2 \} = \{ f(H) : H \leqslant G_1 \}.$$

Mostriamo le due affermazioni separatamente.

(i) Se G è ciclico ed infinito allora per il Teorema 1.4.12 segue che esiste un isomorfismo

$$\begin{aligned} \varphi : \mathbb{Z} &\to G \\ k &\mapsto g^k. \end{aligned}$$

Per la bigezione tra i sottogruppi di $\mathbb{Z}$ e G allora ogni sottogruppo di G dovrà essere scritto come immagine di qualche sottogruppo di $\mathbb{Z}$, ma come abbiamo osservato sopra i sottogruppi di $\mathbb{Z}$ sono tutti e solo della forma $n\mathbb{Z}$ per qualche $n \in \mathbb{N}$.
Dunque i sottogruppi di G sono

$$\{ K : K \leqslant G \} = \{ \varphi(n\mathbb{Z}) = \langle g^n \rangle : n \in \mathbb{N} \}.$$

(ii) Se G è ciclico ed è finito, allora $G = \langle g \rangle$ per qualche $g \in G$, e inoltre $|G| = \mathrm{ord}(g) = n$ per qualche n finito.
Allora per il Teorema 1.4.12 esiste un isomorfismo

$$\begin{aligned} \psi : \mathbb{Z}/n\mathbb{Z} &\to G \\ \overline{a} &\mapsto g^a. \end{aligned}$$

Per l'osservazione 2) sopra i sottogruppi di $\mathbb{Z}/n\mathbb{Z}$ sono tutti e solo della forma $\langle \overline{d} \rangle$, dunque per l'osservazione 3) segue che

$$\{ K : K \leqslant G \} = \left\{ \psi(\langle \overline{d} \rangle) = \left\langle g^d \right\rangle : d \mid n \right\}. \qquad \square$$

1.4.2 Prodotto diretto di gruppi

Definizione 1.4.14 Siano $(G_1, *)$, $(G_2, \star)$ due gruppi. Consideriamo il loro prodotto cartesiano

$$G_1 \times G_2 = \{ (g_1, g_2) : g_1 \in G_1, g_2 \in G_2 \}$$

e un'operazione $\cdot$ su $G_1 \times G_2$ tale che

$$\begin{aligned} \cdot : (G_1 \times G_2) \times (G_1 \times G_2) &\to (G_1 \times G_2) \\ ((x, y), (z, w)) &\mapsto (x * z, y \star w). \end{aligned}$$

La struttura $(G_1 \times G_2, \cdot)$ si dice *prodotto diretto dei gruppi* G_1 *e* G_2.

Proposizione 1.4.15 **Il prodotto diretto di gruppi è un gruppo.** *Siano* $(G_1, *)$, $(G_2, \star)$ *due gruppi. Allora il prodotto diretto* $(G_1 \times G_2, \cdot)$ *è un gruppo.*

Dimostrazione. Sappiamo già che $\cdot$ è un'operazione su $G_1 \times G_2$, quindi basta mostrare i tre assiomi di gruppo.

ASSOCIATIVITÀ Siano $(x, y), (z, w), (h, k) \in G_1 \times G_2$. Mostriamo che vale la proprietà associativa.

$$\begin{aligned} & (x, y) \cdot ((z, w) \cdot (h, k)) && \text{(def. di } \cdot) \\ = \ & (x, y) \cdot (z * h, w \star k) && \text{(def. di } \cdot) \\ = \ & (x * (z * h), y \star (w \star k)) && \text{(ass. di } * \text{ e } \star) \\ = \ & ((x * z) * h, (y \star w) \star k) \\ = \ & (x * z, y \star w) \cdot (h, k) \\ = \ & ((x, y) \cdot (z, w)) \cdot (h, k). \end{aligned}$$

ELEMENTO NEUTRO Siano $e_1 \in G_1, e_2 \in G_2$ gli elementi neutri dei due gruppi. Mostro che (e_1, e_2) è l'elemento neutro del prodotto diretto.
Sia $(x, y) \in G_1 \times G_2$ qualsiasi. Allora

$$\begin{aligned} (x, y) \cdot (e_1, e_2) &= (x * e_1, y \star e_2) = (x, y) \\ (e_1, e_2) \cdot (x, y) &= (e_1 * x, e_2 \star y) = (x, y). \end{aligned}$$

INVERTIBILITÀ Sia $(x, y) \in G_1 \times G_2$. Mostriamo che (x, y) è invertibile e il suo inverso è $(x^{-1}, y^{-1}) \in G_1 \times G_2$, dove x^{-1} è l'inverso di x in G_1 e y^{-1} è l'inverso di y in G_2.

$$\begin{aligned} (x, y) \cdot (x^{-1}, y^{-1}) &= (x * x^{-1}, y \star y^{-1}) = (e_1, e_2) \\ (x^{-1}, y^{-1}) \cdot (x, y) &= (x^{-1} * x, y^{-1} \star y) = (e_1, e_2). \end{aligned}$$

Dunque il prodotto diretto $(G_1 \times G_2, \cdot)$ è un gruppo. □

Proposizione 1.4.16 **Il centro del prodotto diretto è il prodotto diretto dei centri.** *Siano* $(G_1, *)$, $(G_2, \star)$ *due gruppi e sia* $(G_1 \times G_2, \cdot)$ *il loro prodotto diretto. Allora vale che*

$$Z(G_1 \times G_2) = Z(G_1) \times Z(G_2).$$

Dimostrazione. Per definizione di centro sappiamo che

$$\begin{aligned} Z(G_1 \times G_2) = \{ & (x, y) \in G_1 \times G_2 : \\ & (g_1, g_2) \cdot (x, y) = (x, y) \cdot (g_1, g_2) \quad \forall (g_1, g_2) \in G_1 \times G_2 \}. \end{aligned}$$

Sia $(x, y) \in Z(G_1 \times G_2)$. Allora per ogni $(g_1, g_2) \in G_1 \times G_2$ vale che

$$\begin{aligned}
&(g_1, g_2) \cdot (x, y) = (x, y) \cdot (g_1, g_2) \\
\iff &(g_1 * x, g_2 \star y) = (x * g_1, y \star g_2) \\
\iff &g_1 * x = x * g_1 \text{ e } g_2 \star y = y \star g_2 \\
\iff &x \in Z(G_1) \text{ e } y \in Z(G_2) \\
\iff &(x, y) \in Z(G_1) \times Z(G_2).
\end{aligned}$$

Seguendo la catena di equivalenze al contrario segue la tesi. □

2 | ANELLI E CAMPI

2.1 ANELLI

Definizione 2.1.1 **Anello.** Sia A un insieme e siano $+$ (*somma*), $\cdot$ (*prodotto*) due operazioni su A, ovvero

$$+ : A \times A \to A, \quad (a, b) \mapsto a + b, \qquad \cdot : A \times A \to A. \quad (a, b) \mapsto a \cdot b.$$

Allora la struttura $(A, +, \cdot)$ si dice *anello* se valgono i seguenti assiomi:

(S) La struttura $(A, +)$ è un gruppo abeliano, ovvero:

(S1) Vale la *proprietà commutativa della somma*:
per ogni $a, b \in A$ vale che $a + b = b + a$.

(S2) Vale la *proprietà associativa della somma*:
per ogni $a, b, c \in A$ vale che $(a + b) + c = a + (b + c)$.

(S3) Esiste un elemento $0 \in A$ che è *elemento neutro* per la somma:
per ogni $a \in A$ vale che $a + 0 = 0 + a = a$.
Tale elemento si chiama *zero dell'anello*.

(S4) Ogni elemento di A è *invertibile* rispetto alla somma:
per ogni $a \in A$ esiste $(-a) \in A$ (detto *opposto di* a) tale che $a + (-a) = 0$.

(P) Vale il seguente assioma per il prodotto:

(P1) Vale la *proprietà associativa del prodotto*:
per ogni $a, b, c \in A$ vale che $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(D) Vale la *proprietà distributiva del prodotto rispetto alla somma* sia a destra che a sinistra:
per ogni $a, b, c \in A$ vale che $a(b + c) = ab + ac$ e che $(a + b)c = ac + bc$.

Definizione 2.1.2 **Anello commutativo.** Sia $(A, +, \cdot)$ un anello. Allora $(A, +\cdot)$ si dice anello commutativo se vale inoltre il seguente assioma:

(P2) Vale la *proprietà commutativa del prodotto*:
per ogni $a, b \in A$ vale che $a \cdot b = b \cdot a$.

Definizione 2.1.3 **Anello con unità.** Sia $(A, +, \cdot)$ un anello. Allora $(A, +\cdot)$ si dice anello con unità se vale inoltre il seguente assioma:

(P2) Esiste un elemento $1 \in A$ che è *elemento neutro* per il prodotto:
per ogni $a \in A$ vale che $a \cdot 1 = 1 \cdot a = a$.
Tale elemento si dice *unità dell'anello*.

ESEMPIO 2.1.4. Le strutture $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sono tutti esempi di anelli commutativi con unità.

ESEMPIO 2.1.5. L'insieme delle matrici quadrate $\mathrm{Mat}_{n\times n}(\mathbb{R})$ (con $n \geqslant 2$) è un esempio di anello non commutativo con unità.

ESEMPIO 2.1.6. L'insieme dei numeri pari insieme alle operazioni di somma e prodotto, ovvero $(2\mathbb{Z}, +, \cdot)$, è un anello commutativo ma non ha l'identità.

Definizione 2.1.7 **Insieme degli invertibili.** Sia $(A, +, \cdot)$ un anello con identità. Allora si dice *insieme degli invertibili di* A l'insieme

$$A^\times = \{\, x \in A : \exists y \in A \text{ tale che } xy = yx = 1 \,\}.$$

OSSERVAZIONE. La struttura $(A^\times, \cdot)$ forma sempre un gruppo rispetto al prodotto. Esso viene detto *gruppo moltiplicativo dell'anello* A.

Definizione 2.1.8 **Divisori di zero.** Sia $(A, +, \cdot)$ un anello. Allora $a \in A$ si dice *divisore di zero* se esiste $b \in A$, $b \neq 0$ tale che

$$ab = 0.$$

Proposizione 2.1.9 **Proprietà degli anelli.** *Sia $(A, +, \cdot)$ un anello con unità. Allora valgono le seguenti affermazioni:*

(i) Per ogni $a \in A$ vale che $a \cdot 0 = 0 \cdot a = 0$.

(ii) $(A^\times, \cdot)$ è un gruppo.
In particolare, se A è commutativo allora è un gruppo abeliano.

(iii) Nessun $a \in A$ è contemporaneamente divisore dello zero e invertibile.

Dimostrazione. Dimostriamo separatamente le varie affermazioni.

(i) $a \cdot 0 \overset{(S3)}{=} a \cdot (0+0) \overset{(D)}{=} a \cdot 0 + a \cdot 0$.
Siccome $(A, +)$ è un gruppo, valgono le leggi di cancellazione, dunque segue che
$$0 = a \cdot 0.$$

(ii) Mostriamo che $(A^\times, \cdot)$ è un gruppo.

(G1) Mostriamo che il prodotto di due elementi invertibili di A è ancora in $A^\times$, ovvero è ancora invertibile.
Siano $x, y \in A^\times$ (ovvero essi sono invertibili e i loro inversi sono rispettivamente x^{-1} e y^{-1}); mostro che il loro prodotto $xy \in A$ è invertibile e il suo inverso è $y^{-1}x^{-1}$.

$$\begin{aligned} &(xy)\cdot(y^{-1}x^{-1}) && \text{(per (P1))}\\ &= x(yy^{-1})x^{-1} && \text{(per definizione di inverso)}\\ &= x \cdot x^{-1} && \text{(per definizione di inverso)}\\ &= 1. \end{aligned}$$

Passaggi analoghi mostrano che $(y^{-1}x^{-1}) \cdot xy = 1$, ovvero $y^{-1}x^{-1}$ è l'inverso di xy e quindi $xy \in A^\times$.

(G2) Vale la proprietà associativa del prodotto in quanto vale in A.

(G3) L'elemento neutro del prodotto è 1 ed è in $A^\times$ in quanto $1 \cdot 1 = 1$ (ovvero 1 è l'inverso di se stesso).

(G4) Se l'anello è commutativo, allora $\cdot$ è commutativa su ogni suo sottoinsieme, dunque in particolare lo sarà anche su $A^\times$.

Da ciò segue che $(A^\times, \cdot)$ è un gruppo.

(iii) Supponiamo per assurdo esista $x \in A$ che è invertibile e divisore dello zero. Dato che è un divisore dello zero segue che

$$\exists z \neq 0, z \in A. \quad xz = 0.$$

Siccome è invertibile segue che

$$\exists y \in A. \quad xy = 1.$$

Ma allora

$$\begin{aligned} z &= z \cdot 1 \\ &= z \cdot (xy) && \text{(per (P1))} \\ &= (zx) \cdot y \\ &= 0 \cdot y && \text{(per il punto (i))} \\ &= 0. \end{aligned}$$

Tuttavia ciò è assurdo, in quanto abbiamo supposto $z \neq 0$, dunque non può esistere un divisore dello zero invertibile.

□

OSSERVAZIONE. Notiamo che per il punto 2.1.9: (i) 0 è sempre un divisore dello zero.

Definizione 2.1.10 **Dominio di integrità.** Sia $(A, +, \cdot)$ un anello commutativo con identità. Esso si dice *dominio di integrità* (o semplicemente *dominio*) se l'unico divisore dello zero è 0.

Proposizione 2.1.11 **Annullamento del prodotto.** *Sia $(A, +, \cdot)$ un dominio. Allora vale la legge di annullamento del prodotto, ovvero per ogni $a, b \in A$ vale che*

$$ab = 0 \implies a = 0 \text{ oppure } b = 0.$$

Dimostrazione. Se $a = 0$ la tesi è verificata. Supponiamo allora $a \neq 0$ e dimostriamo che deve essere $b = 0$.

Dato che $a \neq 0$ segue che a non è un divisore dello zero (poiché A è un dominio), dunque se $ab = 0$ l'unica possibilità è $b = 0$. □

Dall'annullamento del prodotto seguono le leggi di cancellazione del prodotto:

Corollario 2.1.12 **Leggi di cancellazione per il prodotto.** *Sia $(A, +, \cdot)$ un dominio di integrità e siano $a, b, x \in A$ con $x \neq 0$. Allora*

$$ax = bx \implies a = b.$$

Dimostrazione. Aggiungiamo ad entrambi i membri l'opposto di bx:

$$\begin{aligned} & ax - bx = bx - bx \\ \iff & ax - bx = 0 && \text{(per (D))} \\ \iff & (a - b)x = 0 && \text{(per 2.1.11)} \\ \iff & a - b = 0 \text{ oppure } x = 0. \end{aligned}$$

Ma per ipotesi $x \neq 0$, dunque deve seguire che $a - b = 0$, ovvero $a = b$. □

Definizione 2.1.13 **Campo.** Sia $(\mathbb{K}, +, \cdot)$ un anello commutativo con identità. Allora $\mathbb{K}$ si dice campo se $\mathbb{K}^\times = \mathbb{K} \setminus \{ 0 \}$.

OSSERVAZIONE. Un campo è una struttura $(\mathbb{K}, +, \cdot)$ tale che:

(S) La struttura $(\mathbb{K}, +)$ è un gruppo abeliano.

(P) La struttura $(\mathbb{K} \setminus \{ 0 \}, \cdot)$ è un gruppo abeliano.

(D) Vale la *proprietà distributiva del prodotto rispetto alla somma*:
per ogni $a, b, c \in \mathbb{K}$ vale che $a(b + c) = ab + ac$.

Proposizione 2.1.14 **Ogni campo è un dominio.** *Sia $(\mathbb{K}, +, \cdot)$ un campo. Allora $\mathbb{K}$ è anche un dominio di integrità.*

Dimostrazione. Per 2.1.9: (iii) i divisori dello zero non possono essere invertibili, quindi devono essere un sottoinsieme di $\mathbb{K} \setminus \mathbb{K}^\times$. Ma per definizione di campo $\mathbb{K}^\times = \mathbb{K} \setminus \{ 0 \}$, dunque l'unico possibile divisore dello zero è 0, ovvero $\mathbb{K}$ è un dominio. □

Proposizione 2.1.15 **Ogni dominio finito è un campo.** *Sia $(A, +, \cdot)$ un dominio di integrità con un numero finito di elementi. Allora A è un campo.*

Dimostrazione. Sia $x \in A \setminus \{ 0 \}$. Devo mostrare che x è invertibile. Costruisco la mappa

$$\begin{aligned} \varphi_x : A &\to A \\ a &\mapsto ax. \end{aligned}$$

Ora mostro che φ_x è bigettiva.

φ_x È INIETTIVA Supponiamo che per qualche $a, b \in A$ valga che $\varphi_x(a) = \varphi_x(b)$ e mostriamo che segue che $a = b$.
Per definizione di φ_x l'ipotesi equivale ad affermare che $ax = bx$, ma siccome $x \neq 0$ e A è un dominio possiamo applicare la legge di cancellazione per il prodotto, da cui segue che $a = b$, ovvero φ_x è iniettiva.

φ_x È SURGETTIVA Poiché la cardinalità del dominio e del codominio di φ_x è la stessa ed è finita segue che φ_x è anche surgettiva.
Dunque φ_x è bigettiva. Dato che $1 \in A = \varphi_x(A)$ segue che esiste un $y \in A$ tale che

$$xy = 1 (= yx),$$

ovvero x è invertibile e A è un campo. □

Definizione 2.1.16 **Omomorfismo di anelli.** Siano $(A, +, \cdot)$, $(B, \oplus, \odot)$ anelli con unità. Allora la funzione $\varphi : A \to B$ si dice omomorfismo di anelli se

(i) $\varphi(1_A) = 1_B$.

(ii) Per ogni $a, b \in A$ vale che $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$.

(iii) Per ogni $a, b \in A$ vale che $\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$.

2.2 ANELLO DEI POLINOMI

Definizione 2.2.1 **Polinomi a coefficienti in un anello.** Sia $(A, +, \cdot)$ un anello commutativo con identità e consideriamo una successione (a_i) di elementi di A che sia definitivamente nulla, ovvero tale che esista un $n \in \mathbb{N}$ tale che

$$a_m = 0 \quad \text{per ogni } m > n.$$

Allora si dice *polinomio nell'indeterminata* X la scrittura formale

$$p = p(X) = \sum_{i=0}^{\infty} a_i X^i.$$

Gli a_i si dicono *coefficienti del polinomio*.

L'insieme dei polinomi a coefficienti in A si indica con $A[X]$.

Dato che la successione che definisce il polinomio è definitivamente nulla, possiamo scrivere il polinomio come una sequenza finita di termini: basta prendere i termini fino al massimo indice per cui a_i è diverso da 0. Diamo però alcune definizioni preliminari.

Innanzitutto d'ora in avanti $(A, +, \cdot)$ è un anello commutativo con identità a meno di ulteriori specifiche.

Definizione 2.2.2 **Polinomio nullo.** Si dice *polinomio nullo in* $A[X]$ il polinomio definito dalla successione costantemente nulla, e lo si indica come $p(X) = \mathbf{0}$.

Definizione 2.2.3 **Grado di un polinomio.** Sia $p \in A[X]$, $p(X) \neq \mathbf{0}$. Allora si dice grado di p il numero

$$\deg p = \max\{\, n \in \mathbb{N} \,:\, a_n \neq 0 \,\}.$$

Il polinomio $\mathbf{0}$ non ha grado.

Notiamo che i polinomi di grado 0 sono tutti e solo della forma $p(X) = a_0$ per qualche $a_0 \in A$; ovvero sono tutte e sole le costanti dell'anello A.

Definizione 2.2.4 **Uguaglianza tra polinomi.** Siano $p, q \in A[X]$. Allora i polinomi p e q sono uguali se e solo se tutti i loro coefficienti sono uguali.

Definiamo ora le operazioni di somma e prodotto tra polinomi.

Definizione 2.2.5 **Somma tra polinomi.** Siano $p, q \in A[X]$. Allora definisco l'operazione di somma

$$\begin{aligned} + : A[X] \times A[X] &\to A[X] \\ (p, q) &\mapsto p + q \end{aligned}$$

nel seguente modo:

$$\text{se } p(X) = \sum_{i=0}^{\infty} a_i X^i, \quad q(X) = \sum_{i=0}^{\infty} b_i X^i, \text{ allora } (p+q)(X) = \sum_{i=0}^{\infty} (a_i + b_i) X^i.$$

Definizione 2.2.6 **Prodotto tra polinomi.** Siano $p, q \in A[X]$. Allora definisco l'operazione di prodotto tra polinomi

$$\begin{aligned} \cdot : A[X] \times A[X] &\to A[X] \\ (p, q) &\mapsto p \cdot q \end{aligned}$$

nel seguente modo:

$$\text{se } p(X) = \sum_{i=0}^{\infty} a_i X^i, \quad q(X) = \sum_{j=0}^{\infty} b_j X^j, \text{ allora } (p \cdot q)(X) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_i b_j X^{i+j}.$$

Teorema 2.2.7 **L'insieme dei polinomi è un anello.** *La struttura $(A[X], +, \cdot)$ è un anello commutativo con identità (dove l'identità è il polinomio $\mathbf{1}(X) = 1_A$).*

Proposizione 2.2.8 **Grado della somma e del prodotto.** *Siano $p, q \in A[X] \setminus \{ \mathbf{0} \}$. Allora vale che*

(i) $\deg(p+q) \leqslant \max\{ \deg p, \deg q \}$.

(ii) se A è un dominio, allora $\deg(pq) = \deg p + \deg q$.

Dimostrazione. Siano i due polinomi

$$p(X) = \sum_{i=0}^{\infty} a_i X^i, \quad q(X) = \sum_{i=0}^{\infty} b_i X^i.$$

e siano $n = \deg p$, $m = \deg q$.

GRADO DELLA SOMMA Sia $k = \max n, m$. Allora per ogni $i > k$ varrà che $a_i = b_i = 0$, ovvero $a_i + b_i = 0$, da cui $\deg(p+q) \leqslant k$.

GRADO DEL PRODOTTO Il termine di grado massimo di $(pq)(X)$ deve essere quello in posizione $n+m$.

Mostriamo che per ogni $i > n$, $j > m$ vale che il coefficiente del termine di grado $i+j$ è uguale a 0. Infatti per definizione di grado segue che $a_i, b_j = 0$ se $i > n$ o $j > m$, dunque il prodotto $a_i \cdot b_j$ sarà 0, ovvero il coefficiente di grado $i+j$ sarà nullo. Da ciò segue che $\deg(pq) \leqslant n+m$.

Inoltre essendo A un dominio il termine $a_n b_m$ deve essere diverso da 0, in quanto altrimenti uno tra a_n e b_m dovrebbe essere 0, contro la definizione di grado.

Dunque $\deg(pq) = \deg p + \deg q$. □

Corollario 2.2.9 *Se A è un dominio, allora $A[X]$ è un dominio.*

Dimostrazione. Siano $p, q \in A[X] \setminus \{ \mathbf{0} \}$, con $\deg p = n \geqslant 0$, $\deg q = m \geqslant 0$. Allora per la Proposizione 2.2.8 vale che

$$\deg(pq) = \deg p + \deg q = n + m \geqslant 0.$$

Dunque il polinomio $(pq)(X)$ non può essere il polinomio nullo (che non ha grado), da cui segue che in $A[X]$ non vi sono divisori dello zero. □

Corollario 2.2.10 *Se A è un dominio, allora gli invertibili di $A[X]$ sono tutti e soli gli elementi invertibili di A, ovvero*

$$A[X]^\times = A^\times.$$

Dimostrazione. Sia $p \in A[X]^\times$ e sia $q \in A[X]$ il suo inverso, ovvero tale che $(pq)(X) = 1_A$.

Notiamo che $p, q \neq \mathbf{0}$. Infatti se uno dei due fosse il polinomio nullo per la punto 2.1.9: (i) il loro prodotto dovrebbe essere il

polinomio nullo e non l'unità. Allora esistono $\deg p, \deg q \geqslant 0$ e vale che

$$\deg(pq) = \deg p + \deg q \overset{!}{=} \deg 1 = 0.$$

Dato che i gradi di p e q sono positivi o nulli, il grado del prodotto è 0 se e solo se entrambi i polinomi p e q sono di grado zero, ovvero se e solo se sono elementi dell'anello A.

Siano $a, b \in A$ tali che $f(X) = a$e $q(X) = b$. Allora $(pq)(X) = a \cdot b = 1$, ovvero a è invertibile, cioè $a \in A^\times$. □