Algebra

Luca De Paulis

28 settembre 2020

INDICE

Parte I

ARITMETICA

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

$$\begin{aligned} * : G \times G &\to G \\ (a, b) &\mapsto a * b. \end{aligned} \tag{1}$$

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

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

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 $\mathbb{Z}/^{\times}_{n\mathbb{Z}} \subseteq \mathbb{Z}/_{n\mathbb{Z}}$;

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

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

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

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

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

(v) Legge di cancellazione sinistra:

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

Legge di cancellazione destra:

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

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 $g * (x * y) = (x * y) * g$.

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

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

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

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.

($\implies$) 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

$$\implies m \mid n.$$

($\impliedby$) 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 $\mathrm{ord}_{\mathbb{Z}/_{n\mathbb{Z}}}([1]_n) = n$.

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 $H = \left\langle g^{h_0} \right\rangle$.

($\supseteq$) 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 $\left\langle g^{h_0} \right\rangle \subseteq H$.

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

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

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

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

$$|\mathbb{Z}/_{n\mathbb{Z}}| = |\overline{1}| = \operatorname{ord}_{\mathbb{Z}/_{n\mathbb{Z}}}(\overline{1}) = n. \tag{2}$$

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*

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

Dimostrazione. Sia X_d l'insieme

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

Se $d \not\mid n$ per la proposizione 1.3.10: (i) segue che $X_d = \varnothing$.

Dunque abbiamo che

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

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

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

$\square$

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 $H_d = \left\langle \dfrac{\overline{n}}{d} \right\rangle$.

Infatti ovviamente $H_d \subseteq \left\langle \dfrac{\overline{n}}{d} \right\rangle$. 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 $\overline{x} = \dfrac{\overline{n}}{d} b$ 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

$$f(x * y) = f(x) \star f(y). \tag{3}$$

L'insieme di tutti gli omomorfismi da G_1 a G_2 si indica con $\mathrm{Hom}(G_1, G_2)$.

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) *per ogni* $H \leqslant G_1$ *vale che* $f(H) \leqslant G_2$;

(iv) *per ogni* $K \leqslant G_2$ *vale che* $f^{-1}(K) \leqslant G_1$;

(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

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

(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 $G_1 \simeq G_2$.

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

Allora $G_1 \simeq G_3$.

Dimostrazione. Dato che $G_1 \simeq G_2$ e $G_2 \simeq G_3$ 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 $G_1 \simeq G_3$. □

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* $G \simeq \mathbb{Z}$*;*

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

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 $G \simeq \mathbb{Z}$.

(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.

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

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

$\square$

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

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

Definizione 1.4.14 **Automorfismo.** Sia $(G, \cdot)$ un gruppo e sia $\varphi : G \to G$ un isomorfismo. Allora φ viene detto *automorfismo* e l'insieme di tutti gli automorfismi di un gruppo G si denota con $\mathrm{Aut}(G)$.

Proposizione 1.4.15 **Gruppo degli automorfismi.** *Sia* $(G, \cdot)$ *un gruppo. Allora la struttura* $(\mathrm{Aut}(G), \circ)$ *(dove* $\circ$ *è la composizione di funzioni) è un gruppo.*

Dimostrazione. Mostriamo che valgono gli assiomi di gruppo.

chiusura La composizione di funzioni è un'operazione su $\mathrm{Aut}(G)$ in quanto la composizione di due omomorfismi è un omomorfismo (per la Proposizione 1.4.4) e la composizione di due funzioni bigettive è ancora bigettiva, dunque la composizione di due automorfismi è ancora un automorfismo.

associatività La composizione di funzioni è associativa.

elemento neutro L'elemento neutro di $\mathrm{Aut}(G)$ è

$$\begin{aligned} \mathrm{id}_G : G &\to G \\ g &\mapsto g. \end{aligned}$$

Infatti id_G è un automorfismo di G e inoltre per ogni $f \in \mathrm{Aut}(G)$ vale che

$$\mathrm{id}_G \circ f = f = f \circ \mathrm{id}_G .$$

invertibilità Le funzioni in $\mathrm{Aut}(G)$ sono bigettive, dunque invertibili, e le loro inverse sono ancora automorfismi.

Dunque $(\mathrm{Aut}(G), \circ)$ è un gruppo. □

1.4.2 Omomorfismi di gruppi ciclici

Studiamo ora gli insiemi $\mathrm{Hom}(G_1, G_2)$ dove G_1 e G_2 sono gruppi ciclici. Per il Teorema 1.4.12 è sufficiente studiare gli omomorfismi tra i gruppi $\mathbb{Z}$ e $\mathbb{Z}/_{n\mathbb{Z}}$ (con $n \in \mathbb{N}$ qualunque).

omomorfismi con dominio $\mathbb{Z}$ Consideriamo l'insieme $\mathrm{Hom}(\mathbb{Z}, G)$ dove $(G, \cdot)$ è un gruppo ciclico qualunque (quindi può essere isomorfo a $\mathbb{Z}$ oppure a $\mathbb{Z}/_{n\mathbb{Z}}$ per qualche $n \in \mathbb{N}$).

Sia $g := f(1)$. Allora possiamo mostrare per induzione che $f(n) = g^n$ per ogni $n \geqslant 0$. Per i negativi siccome f è un omomorfismo vale che

$$f(-n) = f(n)^{-1} = (g^n)^{-1} = g^{-n},$$

da cui segue che gli omomorfismi $\mathbb{Z} \to G$ sono tutti della forma

$$f(k) = g^k \quad \forall k \in \mathbb{Z}$$

e sono tutti identificati univocamente dal valore di $f(1)$.

Viceversa, per ogni $g \in G$ esiste un omomorfismo

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

Questa funzione è un omomorfismo poiché

$$\varphi_g(k_1 + k_2) = g^{k_1+k_2} = g^{k_1} g^{k_2} = \varphi_g(k_1)\varphi_g(k_2).$$

Vi è dunque una bigezione tra $\mathrm{Hom}(\mathbb{Z}, G)$ e G, data dalle due mappe

$$\begin{aligned} \mathrm{Hom}(\mathbb{Z}, G) &\leftrightarrow G \\ f &\mapsto f(1) \\ \varphi_g &\leftarrow g. \end{aligned}$$

1.4.3 Prodotto diretto di gruppi

Definizione 1.4.16 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 1.4.17 **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 1.4.18 **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. □

Proposizione 1.4.19 **Ordine nel prodotto diretto.** *Siano* $(G_1, *)$, $(G_2, \star)$ *due gruppi e sia* $(G_1 \times G_2, \cdot)$ *il loro prodotto diretto. Sia* $(x, y) \in G_1 \times G_2$. *Allora vale che*

$$\operatorname{ord}_{G_1 \times G_2}((x, y)) = \left[\operatorname{ord}_{G_1}(x), \operatorname{ord}_{G_2}(y)\right].$$

Dimostrazione. Sia $n = \operatorname{ord}(x)$, $m = \operatorname{ord}(y)$ e $d = \operatorname{ord}((x, y))$. Mostriamo che $d = [n, m]$.

$d \mid [n, m]$ Vale che

$$(x, y)^{[n,m]} = (x^{[n,m]}, y^{[n,m]}).$$

Siccome $\operatorname{ord}(x) = n \mid [n, m]$ e stessa cosa per $\operatorname{ord}(y) = m$, per la Proposizione 1.3.5: (ii) segue che

$$(x^{[n,m]}, y^{[n,m]}) = (e_1, e_2)$$

da cui (per la Proposizione 1.3.5: (ii)) segue che $d \mid [n, m]$.

$[n, m] \mid d$ Per definizione di potenza intera nel prodotto diretto sappiamo che $(x, y)^d = (x^d, y^d)$. Inoltre dato che d è l'ordine di (x, y) segue che $(x, y)^d = (e_1, e_2)$. Dunque

$$\begin{aligned} & x^d = e_1, \ y^d = e_2 \\ \iff & n \mid d, \ m \mid d \\ \iff & [n, m] \mid d. \end{aligned}$$

Dunque $d = [n, m]$, ovvero la tesi. □

Teorema 1.4.20 **Teorema Cinese del Resto (III forma.)** *Siano* $n, m \in \mathbb{Z}$ *entrambi non nulli. Allora vale che*

$$\mathbb{Z}/_{nm\mathbb{Z}} \simeq \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}} \iff (n, m) = 1.$$

Dimostrazione. Sia $G = \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}$. Siccome $|G| = nm$ in virtù del Teorema 1.4.12 per mostrare che $G \simeq \mathbb{Z}/_{nm\mathbb{Z}}$ è sufficiente mostrare che G è ciclico.

Un gruppo è ciclico se e solo se esiste $g \in G$ tale che $\operatorname{ord}(g) = |G|$: infatti per ogni $g \in G$ vale che $\langle g \rangle \leqslant G$, dunque se i due insiemi hanno anche la stessa cardinalità devono essere uguali.

Siano $\bar{x} \in \mathbb{Z}/_{n\mathbb{Z}}, \bar{y} \in \mathbb{Z}/_{m\mathbb{Z}}$ tali che $g = (\bar{x}, \bar{y})$. Per la Proposizione 1.4.19 vale che

$$\operatorname{ord}(g) = \operatorname{ord}((\bar{x}, \bar{y})) = [\operatorname{ord}(\bar{x}), \operatorname{ord}(\bar{y})].$$

D'altro canto però $\operatorname{ord}(\bar{x}) = \dfrac{n}{(n, x)}$, $\operatorname{ord}(\bar{y}) = \dfrac{m}{(m, y)}$ (dove x, y sono rappresentanti qualsiasi delle classi $\bar{x}$, $\bar{y}$ rispettivamente), dunque

$$\operatorname{ord}(g) = \left[\frac{n}{(n, x)}, \frac{m}{(m, y)}\right] \leqslant [n, m].$$

Possiamo dunque distinguere i due casi:

1. se $(n, m) = d > 1$ allora per la PROPOSIZIONE DA INSERIRE per ogni $g \in G$ vale che
$$\mathrm{ord}(g) \leqslant [n, m] = \frac{mn}{d} < mn$$
da cui segue che G non può essere ciclico;
2. se $(n, m) = 1$ allora per ogni $g \in G$ vale che
$$\mathrm{ord}(g) \leqslant [n, m] = mn.$$
In particolare se consideriamo $g = (\bar{1}, \bar{1})$ si ha che
$$\mathrm{ord}(()\bar{1}, \bar{1}) = \left[\frac{n}{(n,1)}, \frac{m}{(m,1)}\right] = [m, n] = mn$$
, dunque $G = \langle(\bar{1}, \bar{1})\rangle$, da cui segue che
$$G \simeq \mathbb{Z}/_{nm\mathbb{Z}}$$
per il Teorema 1.4.12. □

Osservazione. Per il Teorema Cinese del Resto (II Forma) sappiamo che la funzione
$$\begin{aligned} \varphi : \mathbb{Z}/_{nm\mathbb{Z}} &\to \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}} \\ [a]_{nm} &\mapsto ([a]_n, [a]_m) \end{aligned} \tag{4}$$
è bigettiva. Inoltre
$$\begin{aligned} \varphi([a]_{nm} + [b]_{nm}) &= \varphi([a+b]_{nm}) \\ &= ([a+b]_n, [a+b]_m) \\ &= ([a]_n + [b]_n, [a]_m + [b]_m) \\ &= ([a]_n, [a]_m) + ([b]_n, [b]_m) \\ &= \varphi([a]_{nm}) + \varphi([b]_{nm}), \end{aligned}$$
ovvero φ è un omomorfismo di gruppi. Dunque φ è un isomorfismo di gruppi e
$$\mathbb{Z}/_{nm\mathbb{Z}} \simeq \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}.$$

Corollario 1.4.21 **Isomorfismo tra i gruppi degli invertibili.** *Siano* $n, m \in \mathbb{Z}$ *entrambi non nulli. Allora se* $(n, m) = 1$ *segue che*
$$\mathbb{Z}/^{\times}_{nm\mathbb{Z}} \simeq \mathbb{Z}/^{\times}_{n\mathbb{Z}} \times \mathbb{Z}/^{\times}_{m\mathbb{Z}}. \tag{5}$$

Dimostrazione. Consideriamo la funzione
$$\begin{aligned} \varphi^* : \mathbb{Z}/^{\times}_{nm\mathbb{Z}} &\to \mathbb{Z}/^{\times}_{n\mathbb{Z}} \times \mathbb{Z}/^{\times}_{m\mathbb{Z}} \\ [a]_{nm} &\mapsto [a]_n \times [a]_m. \end{aligned}$$
Essa è ben definita: infatti se $[a]_{nm} \in \mathbb{Z}/^{\times}_{nm\mathbb{Z}}$ significa che $(a, mn) = 1$. Siccome per ipotesi $(m, n) = 1$ per la PROPOSIZIONE NON SCRITTA segue che $(m, n) = (a, m) = 1$, ovvero $[a]_n \in \mathbb{Z}/^{\times}_{n\mathbb{Z}}$ e $[a]_m \in \mathbb{Z}/^{\times}_{m\mathbb{Z}}$.

Inoltre questa funzione è una restrizione della φ definita in (4), dunque è iniettiva. Inoltre
$$|\mathbb{Z}/_{nm\mathbb{Z}}| = \varphi(nm) = \varphi(n)\varphi(m) = |\mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}|$$
siccome $(n, m) = 1$, dunque φ è anche surgettiva e quindi è bigettiva.

Tramite passaggi analoghi a quelli visti nell'osservazione precedente si dimostra che φ^* è un omomorfismo, dunque essendo bigettiva è anche un isomorfismo di gruppi, da cui segue la tesi. □

1.4.4 Prodotto di sottogruppi

Definizione 1.4.22 Sia $(G, \cdot)$ un gruppo e siano $H, K \leqslant G$. Allora si definisce il *prodotto tra* H *e* K come

$$HK := \{ h \cdot k \, : \, h \in H, k \in K \}. \tag{6}$$

Analogamente si definisce il *prodotto tra* K *e* H come

$$KH := \{ k \cdot h \, : \, k \in K, h \in H \}. \tag{7}$$

Osservazione. Se il gruppo è in notazione additiva il prodotto di sottogruppi diventa somma di sottogruppi e si indica $H + K$ (o $K + H$).

Proposizione 1.4.23 *[Condizione per cui il prodotto tra sottogruppi è un sottogruppo] Sia* $(G, \cdot)$ *un gruppo e siano* $H, K \leqslant G$.

Allora l'insieme HK *è un sottogruppo di* G *se e solo se* $HK = KH$.

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

($\Longleftarrow$) Siccome entrambi gli insiemi contengono e_G, per la Proposizione 1.2.2 mi basta mostrare che HK è chiuso rispetto all'operazione $\cdot$ e che contiene l'inverso di ogni suo elemento.

CHIUSURA Siano $h_1k_1, h_2k_2 \in HK$. Voglio mostrare che $(h_1k_1) \cdot (h_2k_2) \in HK$. Per associatività, posso scriverlo come

$$h_1 \cdot (k_1h_2) \cdot k_2.$$

Siccome $KH = HK$ esisteranno $h_3 \in H, k_3 \in K$ tali che $k_1h_2 = h_3k_3$. Da ciò segue che

$$h_1 \cdot (k_1h_2) \cdot k_2 = h_1h_3k_3k_2 \in HK.$$

INVERTIBILITÀ Sia $hk \in HK$ e mostriamo che anche il suo inverso $(hk)^{-1} = k^{-1}h^{-1}$ è in HK. Siccome $k^{-1}h^{-1} \in KH$ e $KH = HK$, segue la tesi.

($\Longrightarrow$) Dimostriamo che $HK = KH$ mostrando che $HK \subseteq KH$ e $KH \subseteq HK$.

($KH \subseteq HK$) Banalmente $H \subseteq HK$ (infatti $H \ni h = he_G \in HK$) e $K \subseteq HK$. Ma allora per ogni $h, k \in HK$ segue che $k \cdot h \in HK$ (in quanto $HK \leqslant G$) dunque $KH \subseteq HK$.

($HK \subseteq KH$) Consideriamo la funzione

$$\begin{aligned} f : HK &\to KH \\ x &\mapsto x^{-1}. \end{aligned}$$

Questa funzione è ben definita, in quanto se $x \in HK$, ovvero se $x = hk$ per qualche $h \in H, k \in K$ allora

$$x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$$

poiché $k^{-1} \in K$ e $h^{-1} \in H$. Inoltre questa funzione è ovviamente iniettiva, da cui segue che $HK \subseteq KH$.

Dunque HK è sottogruppo se e solo se $HK = KH$. □

1.5 CLASSI LATERALI E GRUPPO QUOZIENTE

Sia $(G, \cdot)$ un gruppo e sia $H \leqslant G$. Consideriamo la seguente relazione sugli elementi di G: diciamo che $x \sim_L y$ se e solo se $y^{-1}x \in H$.

Questa relazione è una relazione di equivalenza, infatti

- $\sim_L$ è riflessiva: $x^{-1}x = e_G \in H$, dunque $x \sim_L x$.
- $\sim_L$ è simmetrica: se $x \sim_L y$, ovvero $y^{-1}x \in H$, allora il suo inverso $(y^{-1}x)^{-1} = x^{-1}(y^{-1})^{-1} = x^{-1}y \in H$, dunque $y \sim_L x$.
- $\sim_L$ è transitiva: supponiamo che $x \sim_L y$ e $y \sim_L z$ e mostriamo che $x \sim_L z$. Dalla prima sappiamo che $y^{-1}x \in H$, mentre dalla seconda segue che $z^{-1}y \in H$. Dato che H è un sottogruppo, il prodotto di suoi elementi è ancora in H, dunque
$$z^{-1}y \cdot y^{-1}x = z^{-1}x \in H$$
da cui segue che $x \sim_L z$.

Questa relazione di equivalenza forma delle classi di equivalenza che partizionano G: in particolare la classe di $x \in G$ sarà della forma

$$\begin{aligned}[C_x]_L &= \{\, g \in G \,:\, g \sim_L x \,\} \\ &= \left\{\, g \in G \,:\, x^{-1}g \in H \,\right\} \\ &= \left\{\, g \in G \,:\, x^{-1}g = h \text{ per qualche } h \in H \,\right\} \\ &= \{\, g \in G \,:\, g = xh \text{ per qualche } h \in H \,\}.\end{aligned}$$

Notiamo che gli elementi della classe di x sono quindi tutti e soli gli elementi del sottogruppo h moltiplicati a sinistra per x. Diamo dunque la seguente definizione.

Definizione 1.5.1 **Classe laterale sinistra.** Sia $(G, \cdot)$ un gruppo e $H \leqslant G$ un suo sottogruppo. Sia inoltre $x \in G$.

Allora si dice *classe laterale sinistra di* H *rispetto a* x l'insieme

$$xH := \{\, xh \,:\, h \in H \,\}.$$

Osservazione. Nel caso di gruppi additivi le classi laterali si scrivono in notazione additiva, ovvero nella forma $x + H$ per $x \in G$, $H \leqslant G$.

Esempio 1.5.2. Ad esempio le classi laterali di $n\mathbb{Z} \leqslant \mathbb{Z}$ sono della forma

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

La classe $a + n\mathbb{Z}$ denota tutti i numeri congrui ad a modulo n.

Allo stesso modo possiamo definire un'altra relazione di equivalenza $\sim_R$ tale che

$$x \sim_R y \iff xy^{-1} \in H.$$

Le classi di equivalenza di questa relazione sono della forma

$$[C_x]_R = \{\, g \in G \,:\, g = hx \text{ per qualche } h \in H \,\}.$$

Possiamo dunque definire anche le classi laterali destre nel seguente modo.

Definizione 1.5.3 **Classe laterale destra.** Sia $(G, \cdot)$ un gruppo e $H \leqslant G$ un suo sottogruppo. Sia inoltre $x \in G$.

Allora si dice *classe laterale destra di* H *rispetto a* x l'insieme

$$Hx := \{\, hx \,:\, h \in H \,\}.$$

Osservazione. Siccome le classi laterali sinistre (o destre) rappresentano le classi di equivalenza rispetto alla relazione $\sim_L$ (risp. $\sim_R$) possiamo definire un insieme di rappresentanti R per cui

$$G = \bigsqcup_{a \in R} aH. \quad (\text{risp. } Ha) \tag{8}$$

Teorema 1.5.4 **Teorema di Lagrange.** *Sia* $(G, \cdot)$ *un gruppo finito e sia* $H \leqslant G$ *qualsiasi. Allora vale che*

$$|H| \mid |G|.$$

In breve, il Teorema di Lagrange afferma che per ogni gruppo finito l'ordine di un suo qualsiasi sottogruppo divide l'ordine del gruppo. Prima di dimostrarlo, dimostriamo un lemma che ci tornerà utile.

Lemma 1.5.5 *Sia* $(G, \cdot)$ *un gruppo e sia* H *un suo sottogruppo. Allora per qualsiasi* $g \in G$ *vale che*

$$|gH| = |H| = |Hg|.$$

Dimostrazione. Per dimostrare che $|gH| = |H|$ consideriamo la mappa

$$\begin{aligned} \varphi : H &\to gH \\ h &\mapsto gh \end{aligned}$$

e facciamo vedere che è bigettiva.

INIETTIVITÀ Supponiamo che per qualche $h, k \in H$ valga che $\varphi(h) = \varphi(k)$, ovvero $gh = gk$. Siccome $gh, gk \in G$ vale la legge di cancellazione sinistra, dunque segue che $h = k$, ovvero φ è iniettiva.

SURGETTIVITÀ Segue naturalmente dalla definizione di gH.

Dunque φ è bigettiva e quindi gli insiemi gH e H hanno la stessa cardinalità. Analogamente si mostra che la funzione

$$\begin{aligned} \psi : H &\to Hh \\ h &\mapsto hg \end{aligned}$$

è bigettiva, dunque segue la tesi. □

Dimostriamo ora il Teorema di Lagrange

Dimostrazione del Teorema 1.5.4. Per l'osservazione precendente sappiamo che se R è un insieme di rappresentanti della relazione di equivalenza $\sim_L$ allora

$$G = \bigsqcup_{a \in R} aH,$$

dunque passando alle cardinalità

$$|G| = \sum_{a \in R} |aH|.$$

Per il Lemma 1.5.5 segue quindi che

$$\begin{aligned} &= \sum_{a \in R} |H| \\ &= |R| \cdot |H|. \end{aligned}$$

Dunque $|H| \mid |G|$, dunque la tesi. □

Osservazione. Osserviamo che in generale le classi laterali di un sottogruppo del gruppo G non sono sottogruppi di G: dato che partizionano il gruppo una sola di esse contiene l'elemento neutro del gruppo.

Proposizione 1.5.6 *Sia* $(G, \cdot)$ *un gruppo, sia* $H \leqslant G$ *e sia* $g \in G$ *qualsiasi. Allora i seguenti fatti sono equivalenti:*

(i) $gH \leqslant G$,

(ii) $g \in H$,

(iii) $H = gH$.

Dimostrazione. Dimostriamo la catena di implicazioni $(i) \implies (ii) \implies (iii) \implies (i)$.

($(i) \implies (ii)$) Supponiamo che $gH \leqslant G$. Allora $e_G \in gH$, ovvero esiste $h \in H$ tale che $gh = e_G$. Ma tale h è g^{-1}, dunque se $g^{-1} \in H$ segue che $g \in H$.

($(ii) \implies (iii)$) Supponiamo che $g \in H$.

($gH \subseteq H$) Supponiamo $gh \in gH$ per qualche $h \in H$. Ma essendo $g \in H$ per ipotesi il prodotto gh sarà un elemento di H, dunque $gH \subseteq H$.

($H \subseteq gH$) Sia $h \in H$. Siccome $g \in H$ e H è un gruppo segue che $g^{-1} \in H$, dunque $g^{-1}h \in H$. Ma questo significa che $g \cdot (g^{-1}h) = h \in gH$, dunque $H \subseteq gH$.

Concludiamo che $gH = H$.

($(iii) \implies (i)$) Siccome $gH = H$ e $H \leqslant G$ allora $gH \leqslant G$. □

Siccome ogni elemento di una classe è un possibile rappresentante della classe stessa, la proposizione precedente ci dice che l'unica classe laterale (sinisra) di H che è un sottogruppo di G è quella che contiene l'identità, ovvero la classe $e_G H = H$.

Corollario 1.5.7 **Corollario al Teorema di Lagrange.** *Sia* $(G, \cdot)$ *un gruppo finito. Allora valgono i seguenti fatti:*

(i) per ogni $g \in G$ *vale che* $\operatorname{ord}_G(g) \mid |G|$,

(ii) per ogni $x \in G$ *vale che* $x^{|G|} = e_G$.

Dimostrazione. (i) Siccome $\langle g \rangle \leqslant G$, per il Teorema di Lagrange vale che

$$\operatorname{ord}_G(g) = |\langle g \rangle| \mid |G|.$$

(ii) Sia $n := |G|$ e $k := \operatorname{ord}_G(g)$. Per il punto precedente vale che $k \mid n$, ovvero che esiste $m \in \mathbb{Z}$ tale che

$$n = km.$$

Dunque segue che

$$\begin{aligned} g^{|G|} &= g^n \\ &= (g^k)^m && \text{(per def. di ordine)} \\ &= e^m \\ &= e. \end{aligned}$$ □

Corollario 1.5.8 **I gruppi di ordine primo sono ciclici.** *Sia* $(G, \cdot)$ *un gruppo tale che* $|G| = p$ *per qualche* $p \in \mathbb{Z}$, p *primo. Allora* G *è ciclico ed in particolare*

$$G \simeq \mathbb{Z}/_{p\mathbb{Z}}.$$

Dimostrazione. Sia $x \in G$, $x \neq e_G$. Allora $\langle x \rangle \neq \{ e_G \}$, da cui segue che

$$1 \neq \mathrm{ord}_G(x) \mid p = |G|.$$

Dunque per definizione di numero primo $\mathrm{ord}_G(x) = p$, ma siccome l'ordine del sottogruppo $\langle x \rangle$ è uguale all'ordine di G segue che $G = \langle x \rangle$.

Dunque G è ciclico e per il Teorema 1.4.12 è isomorfo a $\mathbb{Z}/_{p\mathbb{Z}}$. □

Il teorema di Lagrange ci consente inoltre di dimostrare molto semplicemente il Teorema di Eulero-Fermat.

Dimostrazione. Segue dal Corollario 1.5.7 (in particolare dal punto (ii)) considerando come gruppo $(\mathbb{Z}/^{\times}_{n\mathbb{Z}}, \cdot)$: infatti per definizione $\varphi(n) = \left|\mathbb{Z}/^{\times}_{n\mathbb{Z}}\right|$, da cui la tesi. □

1.5.1 Sottogruppi normali e gruppo quoziente

Definizione 1.5.9 **Sottogruppo normale.** Sia $(G, \cdot)$ un gruppo e sia $H \leqslant G$. Allora si dice che H è un *sottogruppo normale* di G se per ogni $g \in G$ vale che

$$gH = Hg. \tag{9}$$

Se H è normale si scrive $H \triangleleft G$.

Osservazione. Se G è abeliano allora tutti i suoi sottogruppi sono normali.

Osservazione. Se un sottogruppo H è normale non significa che per ogni $h \in H$ vale che $gh = hg$, ma soltanto che per ogni $h \in H$ esiste un $h' \in H$ tale che

$$gh = h'g.$$

Proposizione 1.5.10 *Sia $(G, \cdot)$ un gruppo e $H \leqslant G$. Allora H è normale se e solo se è chiuso per coniugio, ovvero se e solo se per ogni $g \in G$ vale che*

$$gHg^{-1} \subseteq H.$$

Dimostrazione. Mostriamo entrambi i versi dell'implicazione.

($\Longrightarrow$) Supponiamo che $H \triangleleft G$, ovvero che per ogni $g \in G$ vale che

$$gH = Hg,$$

ovvero per ogni $h \in H$ esiste un $h' \in H$ tale che

$$gh = h'g.$$

Moltiplicando a destra per g^{-1} si ottiene che

$$ghg^{-1} = h' \in H,$$

da cui $gHg^{-1} \subseteq H$.

□

Proposizione 1.5.11 **Il centro è un sottogruppo normale.** *Sia $(G, \cdot)$ un gruppo. Allora vale che*

$$Z(G) \triangleleft G.$$

Definizione 1.5.12 **Indice di un sottogruppo.** Sia $(G, \cdot)$ un gruppo e sia $H \leqslant G$. Allora si dice *indice di H in G* il numero di classi laterali sinistre di H, e si indica con

$$[G : H]. \tag{10}$$

Proposizione 1.5.13 *Sia* $(G, \cdot)$ *un gruppo,* $H \leqslant G$*. Allora se* $[G : H] = 2$ *segue che* $H \triangleleft G$.

Proposizione 1.5.14 **Nucleo di omomorfismi e normalità.** *Siano* $(G, \cdot)$, $(G', *)$ *due gruppi e sia* $f : G \to G'$ *un omomorfismo.*
Valgono le seguenti affermazioni.

(i) $\ker f \triangleleft G$,

(ii) per ogni $x, y \in G$ *vale che* $f(x) = f(y)$ *se e solo se* $x \ker f = y \ker f$, *ovvero se* x, y *appartengono alla stessa classe laterale del nucleo,*

(iii) se $z \in \operatorname{Im} f$ *(ovvero* $f(x) = z$ *per qualche* $x \in G$*) allora* $f^{-1}(\{ z \}) = x \ker f$.

Dimostrazione. (i) Per la Proposizione 1.5.10 la tesi è equivalente a dimostrare che

$$g(\ker f)g^{-1} \subseteq \ker f$$

per ogni $g \in G$.
Sia $x \in \ker f$ qualsiasi: mostriamo che $gxg^{-1} \in \ker f$. Per definizione di kernel, questo significa mostrare che $f(gxg^{-1}) = e_G$, ovvero (siccome f è un omomorfismo)

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

Per ipotesi $x \in \ker f$, dunque $f(x) = e_G$; inoltre per la Proposizione 1.4.7: (ii) sappiamo che $f(g^{-1}) = f(g)^{-1}$.
Dunque segue che

$$\begin{aligned} f(g) * f(x) * f(g^{-1}) &= f(g) * e_G * f(g)^{-1} \\ &= f(g) * f(g)^{-1} \\ &= e_G \end{aligned}$$

che è la tesi.

(ii) Supponiamo $f(x) = f(y)$. Moltiplicando a destra per $f(y)^{-1}$ segue che

$$\begin{aligned} & f(x) * f(y)^{-1} = e_G \\ \iff & f(x) * f(y^{-1}) = e_G \\ \iff & f(xy^{-1}) = e_g \\ \iff & xy^{-1} \in \ker f \\ \iff & x \sim_L y. \end{aligned}$$

Dunque le classi di equivalenza di x e y sono uguali, ovvero

$$x \ker f = y \ker f.$$

(iii) Per definizione di controimmagine:

$$\begin{aligned} f^{-1}(z) &= \{ g \in G : f(g) = z \} && \text{(hp: } f(x) = z\text{)} \\ &= \{ g \in G : f(g) = f(x) \} && \text{(per il punto (ii))} \\ &= x \ker f. \end{aligned}$$

□

Consideriamo ora l'insieme di tutte le possibili classi laterali sinistre di un sottogruppo $H \leqslant G$ e chiamiamo questo insieme $G/_H$:

$$G/_H := \{ gH : g \in G \}. \tag{11}$$

Se $H \triangleleft G$ possiamo definire un'operazione su $G/_H$:

$$\begin{aligned} \cdot : G/_H \times G/_H &\to G/_H \\ (aH, bH) &\mapsto abH. \end{aligned} \tag{12}$$

La struttura $(G/_H, \cdot)$ si definisce *gruppo quoziente*.

Proposizione 1.5.15 *Sia $(G, \cdot)$ un gruppo e sia $N \triangleleft G$. Allora la struttura $(G/_N, \star)$ (dove l'operazione è definita come in (12)) è un gruppo.*

Dimostrazione. Mostriamo innanzitutto che l'operazione $*$ è ben definita. Supponiamo che $xN = x'N$ e $yN = y'N$ e mostriamo che $xyN = x'y'N$.

Siano n_1, n_2 tali che

$$x' = xn_1, \quad y' = yn_2.$$

Allora vale che

$$x'y' = xn_1yn_2.$$

Siccome $N \triangleleft G$ segue che $Ny = yN$, ovvero che esiste un $n_3 \in N$ tale che $n_1y = yn_3$. Dunque

$$\begin{aligned} &= xyn_3n_2 && (N \text{ è chiuso rispetto a } \cdot) \\ &\in xyN. \end{aligned}$$

Per simmetria dunque $xyN = x'y'N$.

Mostriamo ora che valgono gli assiomi di gruppo.

ASSOCIATIVITÀ Siano $xN, yN, zN \in G/_N$. Mostriamo che vale la proprietà associativa.

$$\begin{aligned} xN \star (yN \star zN) &= xN \star yzN \\ &= x(yz)N && (\text{ass. in } G) \\ &= (xy)zN \\ &= xyN \star zN \\ &= (xN \star yN) \star zN. \end{aligned}$$

ELEMENTO NEUTRO L'elemento neutro del gruppo è e_GN. Infatti per qualsiasi $xN \in G/_N$

$$\begin{aligned} e_GN \star xN &= e_GxN = xN. \\ xN \star e_GN &= xe_GN = xN. \end{aligned}$$

INVERTIBILITÀ Sia $xN \in G/_N$. Mostriamo che il suo inverso rispetto a $\star$ è $x^{-1}N$.

$$\begin{aligned} xN \star x^{-1}N &= xx^{-1}N = e_GN. \\ x^{-1}N \star xN &= x^{-1}xN = e_GN. \end{aligned}$$

Dunque $(G/_N, \star)$ è un gruppo. □

ESEMPIO 1.5.16. Se consideriamo il gruppo $\mathbb{Z}$ e il suo sottogruppo normale $n\mathbb{Z}$ il gruppo quoziente $\mathbb{Z}/_{n\mathbb{Z}}$ è esattamente il gruppo delle classi resto modulo n.

Proposizione 1.5.17 *Sia* $(G, \cdot)$ *un gruppo e sia* $N \triangleleft G$. *Allora la mappa*

$$\begin{aligned} \pi_N : G &\to G/_N \\ x &\mapsto xN \end{aligned} \tag{13}$$

è un omomorfismo di gruppi e $\ker \pi_N = N$.

Dimostrazione. Mostriamo innanzitutto che π_N è un omomorfismo.

$$\begin{aligned} \pi_N(xy) &= xyN \\ &= xN \cdot yN \\ &= \pi_N(x) \cdot \pi_N(y). \end{aligned}$$

Inoltre per definizione

$$\begin{aligned} \ker \pi_N &= \{ x \in G : \pi_N(x) = xN = N \} \\ &= \{ x \in G : x \in N \} \\ &= N, \end{aligned}$$

dove il secondo segno di uguaglianza viene dalla Proposizione 1.5.6 (in particolare per l'equivalenza tra i punti (ii) e (iii)). □

Corollario 1.5.18 *I sottogruppi normali di* G *sono tutti e solo i nuclei degli omomorfismi definiti su* G.

Dimostrazione. Infatti se $N \triangleleft G$ allora per la Proposizione 1.5.17 segue che $N = \ker \pi_N$; invece dato un omomorfismo di gruppi $\varphi : G \to G'$ vale che $\ker \varphi$ è normale per la Proposizione 1.5.14. □

1.6 TEOREMI DI OMOMORFISMO

Teorema 1.6.1 **Primo Teorema degli Omomorfismi.** *Siano* $(G, \cdot)$, $(G', *)$ *due gruppi e sia* $f : G \to G'$ *un omomorfismo di gruppi. Sia inoltre* $N \triangleleft G$, $N \subseteq \ker f$.

Allora esiste un unico omomorfismo $\varphi : G/_N \to G'$ *per cui il seguente diagramma commuta:*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_N"'] & G' \\ G/_N \arrow[ur, "\varphi"'] & \end{tikzcd} \tag{14}$$

Inoltre vale che

$$\operatorname{Im} f = \operatorname{Im} \varphi, \quad \ker \varphi = \ker f/_N.$$

Dimostrazione. Notiamo che se φ esiste allora è necessariamente unica. Infatti se φ rende il diagramma commutativo significa che $f = \varphi \circ \pi_N$, da cui segue che per ogni $x \in G$

$$\begin{aligned} f(x) &= (\varphi \circ \pi_N)(x) \\ &= \varphi(\pi_N(x)) \\ &= \varphi(xN). \end{aligned}$$

Questa equazione assegna a φ un valore per ogni elemento del dominio $G/_N$, da cui segue l'unicità.

Mostriamo dunque che la funzione

$$\begin{aligned} \varphi : G/_N &\to G' \\ gH &\mapsto f(g) \end{aligned}$$

è ben definita ed è un omomorfismo di gruppi. Inoltre verifichiamo le due proprietà dell'immagine e del nucleo.

BUONA DEFINIZIONE Siano x, y tali che $xN = yN$. Dato che esse rappresentano classi di equivalenza, ciò significa che $x \in yN$. Sia dunque $n \in N$ tale che $x = yn$. Allora vale che

$$\begin{aligned} f(x) &= f(yn) && \text{(f è omo.)} \\ &= f(y) * f(n) && (N \subseteq \ker f) \\ &= f(y) * e' \\ &= f(y). \end{aligned}$$

Dunque segue che

$$\varphi(xN) = f(x) = f(y) = \varphi(yN),$$

ovvero φ è ben definita.

OMOMORFISMO Siano $xN, yN \in G/_N$ e mostriamo che

$$\varphi(xN \cdot yN) = \varphi(xN) * \varphi(yN).$$

Infatti vale che

$$\begin{aligned} \varphi(xN \cdot yN) &= \varphi(xyN) \\ &= f(xy) && \text{(f è omo.)} \\ &= f(x) * f(y) \\ &= \varphi(xN) * \varphi(yN). \end{aligned}$$

PROPRIETÀ DELLE IMMAGINI Per definizione

$$\begin{aligned} \operatorname{Im} \varphi &= \{ \varphi(xN) : xN \in G/_N \} \\ &= \{ f(x) : xN \in G/_N \}. \end{aligned}$$

Tuttavia, come abbiamo verificato nella parte relativa alla buona definizione di φ, se $xN = yN$ allora $f(x) = f(y)$, dunque vale che

$$\begin{aligned} \operatorname{Im} \varphi &= \{ f(x) : x \in G \} \\ &= \operatorname{Im} f. \end{aligned}$$

PROPRIETÀ DEI NUCLEI Per definizione

$$\begin{aligned} \ker \varphi &= \left\{ xN \in G/_N : \varphi(xN) = e' \right\} \\ &= \left\{ xN \in G/_N : f(x) = e' \right\} \\ &= \{ xN \in G/_N : x \in \ker f \} \\ &= \ker f/_N. \end{aligned}$$

□

Nel caso particolare in cui $N = \ker f$ abbiamo che φ è iniettiva, come ci assicura il seguente corollario.

Corollario 1.6.2 *Siano $(G, \cdot)$, $(G', *)$ due gruppi e sia $f : G \to G'$ un omomorfismo di gruppi.*

Allora esiste un unico omomorfismo φ tale che il seguente diagramma commuta:

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_{\ker f}"'] & G' \\ G/_{\ker f} \arrow[ur, hook, "\varphi"'] & \end{tikzcd} \tag{15}$$

In particolare φ è iniettivo, dunque ogni omomorfismo è fattorizzabile come composizione di un omomorfismo surgettivo e uno iniettivo.

Dimostrazione. Siccome $\ker f \subseteq \ker f$ e $\ker f \lhd G$ possiamo applicare il Primo Teorema degli Omomorfismi, da cui segue che esiste un unico omomorfismo φ tale che

$$f = \varphi \circ \pi_{\ker f}.$$

INIETTIVITÀ DI φ Per definizione di φ vale che $\varphi(x \ker f) = e_{G'}$ se e solo se $f(x) = e_{G'}$, ovvero se e solo se $x \in \ker f$. Dunque il nucleo di φ è $\ker f$, che è l'elemento neutro del gruppo quoziente $G/_{\ker f}$, da cui segue che φ è iniettiva.

Essendo inoltre $\pi_{\ker f}$ surgettivo segue la tesi. □

La fattorizzazione definita dal precedente corollario può essere resa ancora più precisa specificando un oggetto intermedio, l'immagine di f: l'omomorfismo f viene quindi scomposto nella composizione di un omomorfismo surgettivo (la proiezione canonica modulo il kernel, ovvero $\pi_{\ker f}$), un isomorfismo e infine un omomorfismo iniettivo (l'inclusione canonica $\iota : \operatorname{Im} f \to G'$, $\iota(g) = g$).

L'isomorfismo è proprio l'omomorfismo φ del Primo Teorema degli Omomorfismi: infatti per l'osservazione precedente φ è iniettivo; inoltre restringendo il codominio a $\operatorname{Im} f$ e sapendo che $\operatorname{Im} \varphi = \operatorname{Im} f$ segue che φ è anche surgettivo, rendendolo un isomorfismo.

Il seguente diagramma dunque commuta:

$$\begin{tikzcd} G \arrow[r, two heads, "\pi_{\ker f}"'] \arrow[rrr, bend left, "f"] & G/_{\ker f} \arrow[r, hook, two heads, "\varphi"'] & \operatorname{Im} f \arrow[r, hook, "\iota"'] & G' \end{tikzcd} \tag{16}$$

Vale dunque il seguente corollario.

Corollario 1.6.3 *Siano $(G, \cdot)$, $(G', *)$ due gruppi e sia $f : G \to G'$ un omomorfismo di gruppi. Allora*

$$G/_{\ker f} \simeq \operatorname{Im} f. \tag{17}$$

Teorema 1.6.4 **Secondo Teorema degli Omomorfismi.** *Sia $(G, \cdot)$ un gruppo e siano $H, K \lhd G$, con $H \subseteq K$. Allora*

$$ {}^{G/_H}\!/_{K/_H} \simeq G/_K. \tag{18}$$

Dimostrazione. Consideriamo le proiezioni canoniche π_H e π_K. Siccome $H \subseteq K = \ker \pi_K$ possiamo applicare il Primo Teorema degli Omomorfismi all'omomorfismo π_K e al sottogruppo normale $H \lhd G$ (tramite la proiezione π_H). Dunque esiste un unico omomorfismo

$$\begin{aligned} \varphi : G/_H &\to G/_K \\ gH &\mapsto gK \end{aligned}$$

che fa commutare il seguente diagramma:

$$\begin{tikzcd} G \arrow[r, "\pi_K"] \arrow[d, "\pi_H"'] & G/K \\ G/H \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Tale funzione è anche surgettiva, in quanto per il Primo Teorema degli Omomorfismi sappiamo che $\operatorname{Im}\varphi = \operatorname{Im}\pi_K$, e π_K è surgettiva. Inoltre

$$\ker\varphi = \ker\pi_K/H = K/H.$$

Consideriamo ora i gruppi G/H e G/K e il sottogruppo $G/H/\ker\varphi$, che corrisponde a $G/H/K/H$. Per il Primo Teorema degli Omomorfismi esiste un unico omomorfismo

$$\tilde{\varphi} : G/H/K/H \to G/K$$

che fa commutare il seguente diagramma:

$$\begin{tikzcd} G/H \arrow[r, two heads, "\varphi"] \arrow[d, "\pi_{K/H}"'] & G/K \\ G/H/K/H \arrow[ur, hook, "\tilde{\varphi}"'] & \end{tikzcd}$$

$\tilde{\varphi}$ è un isomorfismo di gruppi: infatti essendo φ surgettivo anche $\tilde{\varphi}$ lo è; inoltre la proiezione $\pi_{K/H}$ porta il gruppo G/H nel quoziente modulo $\ker\varphi = K/H$, dunque l'omomorfismo $\tilde{\varphi}$ è iniettivo ed è dunque un isomorfismo di gruppi.

Segue quindi che

$$G/H/K/H \simeq G/K. \qquad \square$$

Teorema 1.6.5 **Terzo Teorema degli Omomorfismi.** *Sia* $(G,\cdot)$ *un gruppo e siano* $H \leqslant G, N \triangleleft G$. *Valgono le seguenti affermazioni:*

- N *è un sottogruppo normale di* HN,
- $H \cap N$ *è un sottogruppo normale di* H,
- *inoltre*

$$\frac{H}{H \cap N} \simeq \frac{HN}{N}. \tag{19}$$

Dimostrazione. Dimostriamo innanzitutto le due condizioni di normalità.

($N \triangleleft HN$) Mostriamo innanzitutto che HN è un sottogruppo di G. Per la Proposizione 1.4.23, è sufficiente mostrare che $HN = NH$. Siccome N è normale in G segue che $gN = Ng$ per ogni $g \in G$. Dato che $H \subseteq G$ segue che $hN = Nh$ per ogni $h \in H$, ovvero $HN = NH$. Dunque HN è un sottogruppo di G.

Notiamo inoltre che $N \subseteq HN$ (basta scegliere tutti gli elementi della forma $e_G n$ al variare di $n \in N$), dunque essendo N normale in G segue che N è normale in ogni sottogruppo di G che lo contiene; in particolare $N \triangleleft HN$.

($H \cap N \triangleleft H$) Sia $n \in H \cap N$ e sia $g \in H$.

Ovviamente $gng^{-1} \in H$, in quanto n ed g sono entrambi elementi di H. Inoltre essendo N un sottogruppo normale di G segue che $gng^{-1} \in N$ per ogni $g \in G$, dunque a maggior ragione per ogni $g \in H \subseteq G$.

Dunque $gng^{-1} \in H \cap N$, da cui segue che $H \cap N$ è normale in H.

Consideriamo ora l'applicazione

$$\begin{aligned} f : H &\to {}^{HN}/_{N} \\ h &\mapsto hN. \end{aligned}$$

Quest'applicazione è una restrizione all'insieme $H \subseteq HN$ della proiezione canonica

$$\pi_N : HN \to {}^{HN}/_{N};$$

questo ci garantisce che f è ben definita e che è un omomorfismo di gruppi.

Inoltre f è surgettiva: basta mostrare che

$$\begin{aligned} &\operatorname{Im} f = {}^{HN}/_{N} \\ \iff &\{\, hN \in {}^{HN}/_{N} \;:\; h \in H \,\} = \{\, yN \in {}^{HN}/_{N} \;:\; y \in HN \,\} \end{aligned}$$

L'inclusione $\operatorname{Im} f \subseteq {}^{HN}/_{N}$ è data dalla definizione; l'inclusione contraria viene dal fatto che se $yN \in {}^{HN}/_{N}$, ovvero $y = hn$ per qualche $hn \in HN$, allora $yN = hnN \in \{\, hN : h \in H \,\}$ in quanto $nN = N$.

Inoltre

$$\begin{aligned} \ker f &= \{\, h \in H \;:\; f(h) = N \,\} \\ &= \{\, h \in H \;:\; hN = N \,\} \\ &= \{\, h \in H \;:\; h \in N \,\} \\ &= H \cap N. \end{aligned}$$

Dunque per il Corollario al Primo Teorema degli Omomorfismi segue che

$$\frac{H}{H \cap N} \simeq \operatorname{Im} f = \frac{HN}{N}. \qquad \square$$

Teorema 1.6.6 **Teorema di Corrispondenza tra Sottogruppi.** *Sia* $(G, \cdot)$ *un gruppo e* $N \triangleleft G$. *Sia* $\mathcal{G}$ *l'insieme dei sottogruppi di* G *che contengono* N *e* $\mathcal{N}$ *l'insieme dei sottogruppi di* ${}^{G}/_{N}$.

Allora esiste una corrispondenza biunivoca tra $\mathcal{G}$ *e* $\mathcal{N}$ *che preserva l'indice di sottogruppo e i sottogruppi normali, ovvero esiste una funzione*

$$\begin{aligned} \psi : \mathcal{G} &\to \mathcal{N} \\ A &\mapsto {}^{A}/_{N} \end{aligned}$$

tale che

- $[G \;:\; A] = [{}^{G}/_{N} \;:\; {}^{A}/_{N}]$,
- *se* $A \triangleleft G$ *allora* ${}^{A}/_{N} \triangleleft {}^{G}/_{N}$.

Parte II

ALGEBRA I

2 TEORIA DEI GRUPPI

2.1 GRUPPI E GENERATORI

Nella prima parte abbiamo studiato gruppi generati da un solo elemento (i gruppi *ciclici*). Un gruppo può però essere generato da più di un singolo elemento: in particolare possiamo considerare un gruppo generato da un suo sottoinsieme:

Definizione 2.1.1 **Gruppo generato da un suo sottoinsieme.** Sia $(G, \cdot)$ un gruppo e sia $S \subseteq G$. Allora G si dice *generato da* S, oppure si dice che S è un insieme di generatori per G (e si indica con $G = \langle S \rangle$), se

$$G := \left\{ s_1 \dots s_n \, : \, n \in \mathbb{N}, s_i \in S \cup S^{-1} \right\},$$

dove S^{-1} è l'insieme degli inversi degli elementi di S.

Osservazione. $s_1 \dots s_n$ rappresenta tutte le parole di lunghezza finita formate da elementi di S o dai loro inversi: siccome G è un gruppo (ed è quindi chiuso per prodotto) e $S, S^{-1} \subseteq G$ segue che la parola $s_1 \dots s_n \in G$, dunque $\langle S \rangle \subseteq G$.

Osservazione. Se $S = \{ g \}$ allora

$$G = \{ g^{\varepsilon_1} \dots g^{\varepsilon_n} \, : \, n \in \mathbb{N}, \varepsilon_i = \pm 1 \} = \left\{ g^{\sum \varepsilon_i} \right\} = \langle g \rangle.$$

Osservazione. Se il gruppo G è finito è sufficiente che $s_i \in S$ (non serve considerare S^{-1}).

> **Dimostrazione.** Siccome G è finito ogni suo sottogruppo è finito; in particolare se $s \in S$ allora $\langle s \rangle \leqslant G$ è un sottogruppo finito, e sarà della forma
>
> $$\langle s \rangle = \left\{ e_G, s, s^2, \dots, s^m \right\},$$
>
> dove $m := \operatorname{ord}_G(s)$. Siccome $\langle s \rangle$ è un sottogruppo di G segue che $s^{-1} \in \langle s \rangle$, dunque $s^{-1} = s^k$ per qualche $0 \leqslant k < m$. Dunque ogni occorrenza di s^{-1} in una parola può essere sostituita con s^k che è ottenibile dai soli elementi di S. □

Esempio 2.1.2. Mostriamo che $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} = \langle (1,0), (0,1) \rangle$.

Come abbiamo osservato in precedenza l'inclusione $\supseteq$ è banale, dunque basta far vedere che $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}$ è un sottoinsieme di $\langle (1,0), (0,1) \rangle$.

$$\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} = \left\{ (1,0), (0,1), \overbrace{(1,0) + (0,1)}^{=(1,1)}, \overbrace{(1,0) + (1,0)}^{=(0,0)} \right\} \subseteq \langle (1,0), (0,1) \rangle.$$

Esempio 2.1.3. Sappiamo già che $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Mostriamo che $\mathbb{Z} = \langle 2, 3 \rangle$ e che $\{ 2, 3 \}$ è un insieme minimale di generatori.

È sufficiente mostrare che $\mathbb{Z} \subseteq \langle 2, 3 \rangle$, ovvero che per ogni $n \in \mathbb{Z}$ esistano $a, b \in \mathbb{Z}$ tali che

$$n = a \cdot 2 + b \cdot 3.$$

Per l'identità di Bézout sappiamo che esistono $a_0, b_0 \in \mathbb{Z}$ tali che

$$a_0 \cdot 2 + b_0 \cdot 3 = (2,3) = 1,$$

dunque moltiplicando tutto per n otteniamo la tesi.

Inoltre $\langle 2 \rangle = 2\mathbb{Z}$, $\langle 3 \rangle = 3\mathbb{Z}$, dunque $\{ 2, 3 \}$ è un insieme minimale di generatori.

Definizione 2.1.4 **Finitamente generato.** Sia $(G, \cdot)$ un gruppo. G si dice *finitamente generato* se G ammette un insieme finito di generatori.

Proposizione 2.1.5 *Se G è finitamente generato, allora ogni suo insieme minimale di generatori ha cardinalità finita.*

Dimostrazione. Siccome G è finitamente generato esisterà un insieme di generatori

$$S = \{ s_1, \ldots, s_n \}$$

tale che $G = \langle S \rangle$.

Sia X un insieme di generatori per G di cardinalità infinita. Dato che $S \subseteq G$ ogni elemento di S è esprimibile come una parola finita formata da elementi di X o da loro inversi: per ogni $s_i \in S$ esisteranno quindi k_i elementi di $X \cup X^{-1}$ tali che

$$s_i = x_{1i} \ldots xk_i i.$$

Segue quindi che

$$S = \{ x_{11} \ldots xk_1 1, \ldots, x_{1n} \ldots xk_n n \}.$$

Dato che S è un insieme di generatori per G segue che gli elementi x_{ij} generano il gruppo G, in quanto sono sufficienti per generare i generatori di G. Siccome essi sono in numero finito segue che X non è minimale, da cui la tesi. □

2.2 GRUPPO DIEDRALE

Definizione 2.2.1 **Gruppo diedrale.** Si dice D_n l'insieme delle isometrie del piano che mandano in sé l'n-agono regolare, con $n \geqslant 3$.

Osservazione. Se compongo due isometrie che mandano l'n-agono regolare in sé ho ancora un'isometria che manda l'n-agono regolare in sé. Inoltre ogni isometria ammette un'inversa, che è semplicemente l'isometria che porta l'n-agono nella posizione precedente. Da ciò possiamo dedurre che D_n è un gruppo.

Per studiare la struttura del gruppo diedrale, numeriamo i vertici dell'n-agono regolare da 1 a n.

Proposizione 2.2.2 **Cardinalità del gruppo diedrale.** *La cardinalità di* D_n *è* $2n$ *per ogni* $n \geqslant 3$.

Dimostrazione. Mostriamo inizialmente che $\#D_n \leqslant 2n$.

Sia $x \in D_n$. Questa isometria manderà ogni vertice dell'n-agono in un altro vertice, ed ogni lato in un altro lato.

Sia quindi $i := x(1)$, ovvero i è il vertice in cui viene mandato il vertice 1. A questo punto il lato $(1, 2)$ dovrà essere mandato in un altro lato, dunque segue che $x(2) = i + 1$ oppure $i - 1$.

Dopo aver fatto queste due scelte, l'isometria x è fissata: se $x(2) = i + 1$ allora $x(3) = i + 2$, $x(4) = i + 3$ eccetera; se $x(2) = i - 1$

allora $x(3) = i - 2$ eccetera. Abbiamo quindi n possibili scelte per $x(1)$ e 2 possibili scelte per $x(2)$, dunque il numero di isometrie distinte è al più $2n$.

Mostriamo ora che queste scelte sono tutte distine, ovvero che $\#D_n = 2n$. Innanzitutto l'n-agono ammette n rotazioni distinte, di cui una è la rotazione banale id; inoltre vi sono n assi di simmetria:

- se n è pari essi congiungono i vertici con i vertici opposti e le metà dei lati con le metà dei lati opposti;
- se n è dispari, essi congiungono i vertici con le metà dei lati opposti ai vertici.

Inoltre ogni simmetria non è una rotazione, in quanto le simmetrie invertono l'orientazione dei vertici mentre le rotazioni la mantengono. Dunque vi sono almeno $2n$ elementi in D_n, da cui segue che $\#D_n = 2n$. □

Chiamiamo r la rotazione attorno al centro di $\frac{2\pi}{n}$: le altre rotazioni saranno date da

$$\mathrm{id} = r^0, r, r^2, \dots, r^{n-1}.$$

Le simmetrie saranno invece $s_1, s_2, \dots, s_n$. Tuttavia essendo D_n un gruppo segue che $sr, sr^2, \dots, sr^{n-1}$ sono tutti elementi di D_n.

Proposizione 2.2.3 *Sia r la rotazione di $\frac{2\pi}{n}$ radianti attorno all'origine e sia s una simmetria qualunque dell'n-agono regolare. Allora*

$$D_n = \left\{ \mathrm{id}, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1} \right\}..$$

Dimostrazione. Sappiamo già che le rotazioni sono distinte tra loro e che le simmetrie non sono rotazioni.

Mostriamo che sr^i è una simmetria, ovvero non è una rotazione. Se per assurdo lo fosse, allora sarebbe uguale a r^j per qualche $j \in \mathbb{Z}$, $0 \leqslant j < n$. Allora abbiamo tre possibilità:

1. se $i = j$ allora $s = \mathrm{id}$, da cui s è una rotazione, il che è assurdo;
2. se $i > j$ allora $sr^{i-j} = \mathrm{id}$, da cui s è l'inversa di una rotazione e quindi è una rotazione, il che è assurdo;
3. se $i < j$ allora $s = r^{j-1}$, da cui s è una rotazione, il che è assurdo.

Dunque sr^i è una simmetria.

Mostriamo che le simmetrie sono distinte fra loro: siano sr^i, sr^j due simmetrie con $i \neq j$ e mostriamo che $sr^i \neq sr^j$. Per la legge di cancellazione da ciò segue che $r^i = r^j$; tuttavia questo è assurdo in quanto le rotazioni sono distinte tra loro. □

Possiamo quindi esprimere D_n come una *presentazione di gruppo*:

$$D_n := \langle r, s \,:\, r^n = \mathrm{id}, s^2 = \mathrm{id}, sr = r^{-1}s \rangle.$$

Questo modo di scrivere il gruppo mette in evidenza:

- i generatori del gruppo, ovvero r e s;
- gli ordini dei generatori: $\mathrm{ord}(r) = n$ e $\mathrm{ord}(s) = 2$;
- le relazioni tra i generatori: come mostreremo tra poco vale che $sr = r^{-1}s$.

La rotazione r ha ovviamente ordine n: siccome è una rotazione di $\frac{2\pi}{n}$ radianti, ripetendola n volte otteniamo l'n-agono originale. Per lo stesso motivo la simmetria s ha ordine 2.

Per mostrare che $sr = r^{-1}s$ basta mostrare che l'immagine di tutti i vertici mediante le due isometrie è la stessa.

2.2.1 Sottogruppi del gruppo diedrale

Studiamo i sottogruppi del gruppo diedrale D_n.

Iniziamo studiando $\langle r \rangle$: siccome $\mathrm{ord}(r) = n$ segue che $[D_n : \langle r \rangle] = 2$, da cui per la Proposizione 1.5.13 segue che $\langle r \rangle \triangleleft D_n$.

Tuttavia possiamo anche mostrare che per ogni $j = 0, \dots, n-1$ il gruppo $\langle r^j \rangle$ è normale in D_n. Osserviamo inizialmente che $\langle r \rangle$ è l'unico sottogruppo di D_n di ordine n: esso infatti contiene tutte le rotazioni e, siccome tutte le simmetrie hanno ordine 2, non possono esserci altri sottogruppi ciclici di ordine n. Inoltre, essendo un gruppo ciclico, per la Corollario 1.4.13 esso ha uno e un solo sottogruppo di ordine d per ogni d che divide n.

Mostriamo alcuni risultati intermedi.

Proposizione 2.2.4 *$\langle r^{\frac{n}{d}} \rangle$ è l'unico sottogruppo ciclico di D_n di ordine d per ogni $d > 2$.*

Dimostrazione. Innanzitutto $\mathrm{ord}_{D_n}\left(r^{\frac{n}{d}}\right) = d$ in quanto

$$\left(r^{\frac{n}{d}}\right)^d = r^n = \mathrm{id}\,.$$

Inoltre esso contiene tutti gli elementi di ordine d poiché è l'unico sottogruppo ciclico di $\langle r \rangle$ di ordine d e gli elementi che non appartengono a $\langle r \rangle$ hanno ordine 2 (sono simmetrie); da questo segue che è l'unico sottogruppo ciclico di ordine d di D_n. □

Proposizione 2.2.5 *Sia $(G, \cdot)$ un gruppo. Se H è l'unico sottogruppo di ordine d di G, allora $H \triangleleft G$.*

Dimostrazione. Per ogni $g \in G$ vale che gHg^{-1} è un sottogruppo di G di ordine d, dunque siccome H è l'unico sottogruppo con queste proprietà segue che $gHg^{-1} = H$, da cui la tesi. □

Corollario 2.2.6 *Sia $(G, \cdot)$ un gruppo. Se H è l'unico sottogruppo ciclico di ordine d di G, allora $H \triangleleft G$.*

Dimostrazione. Se $H = \langle h \rangle$ per qualche $h \in G$ allora segue che il coniugato gHg^{-1} è generato dall'elemento ghg^{-1}, dunque anche esso è ciclico. Tuttavia l'unico sottogruppo di G di ordine d e ciclico è H, da cui segue che $gHg^{-1} = H$, ovvero H è normale in G. □

Sfruttando le due proposizioni precedenti segue che per ogni d che divide n ($d > 2$) il sottogruppo $\langle r^{\frac{n}{d}} \rangle$ è normale in D_n.

Questo ragionamento non ci permette di mostrare che $\langle r^{\frac{n}{2}} \rangle$ è normale in D_n; tuttavia possiamo dimostrarlo studiando il centro di D_n.

Proposizione 2.2.7

$$Z(D_n) = \begin{cases} \{\, \mathrm{id} \,\}, & \textit{se } n \textit{ è dispari} \\ \langle r^{\frac{n}{2}} \rangle, & \textit{se } n \textit{ è pari.} \end{cases}$$

Dimostrazione. Per definizione di centro di un gruppo, un elemento è nel centro se e solo se commuta con tutti gli elementi del gruppo; è dunque sufficiente mostrare che un elemento commuta con i generatori del gruppo. Segue quindi che

$$Z(D_n) = \left\{ s^\varepsilon r^j \in D_n \ : \ s^\varepsilon r^j \cdot r = r \cdot s^\varepsilon r^j, s^\varepsilon r^j \cdot s = s \cdot s^\varepsilon r^j \right\}.$$

Se $s^\varepsilon r^j$ soddisfa la seconda condizione, allora

$$\begin{aligned} & s^\varepsilon r^j \cdot s = s \cdot s^\varepsilon r^j \\ \iff & s^\varepsilon s r^{-j} = s \cdot s^\varepsilon r^j \\ \iff & s^{\varepsilon+1} r^{-j} = s^{\varepsilon+1} r^j \\ \iff & r^{-j} = r^j. \end{aligned}$$

Dunque segue che $j \equiv -j \mod n$, ovvero $2j \equiv 0 \mod n$. Abbiamo quindi due casi:

- Se n è dispari questo significa che $j \equiv 0 \mod n$, ovvero $j = 0$. Le possibili scelte sono quindi id ed s; tuttavia s non commuta con r, dunque l'unico elemento che rispetta entrambe le condizioni è id e quindi
$$Z(D_n) = \{ \mathrm{id} \}.$$
- Se n è pari questo implica $j \equiv 0 \mod n/2$, da cui segue che $j = 0, n/2$. I quattro elementi che possono essere nel centro di D_n sono quindi
$$\mathrm{id}, r^{\frac{n}{2}}, s, sr^{\frac{n}{2}}.$$
Tuttavia s e $sr^{n/2}$ non commutano con r, in quanto
$$sr = r^{-1}s, \quad sr^{n/2} \cdot r = sr^{\frac{n}{2}+1} \neq sr^{\frac{n}{2}-1} = r \cdot sr^{\frac{n}{2}}.$$
Dunque gli unici elementi nel centro sono id, $r^{n/2}$, da cui segue che
$$D_n = \langle r^{\frac{n}{2}} \rangle. \qquad \square$$

Siccome il centro di un gruppo è sempre un sottogruppo normale di quel gruppo (per la Proposizione 1.5.11) segue che $\langle r^{n/2} \rangle$ è un sottogruppo normale di D_n.

2.3 AZIONI DI GRUPPO

Definizione 2.3.1 **Azione di un gruppo su un insieme.** Sia $(G, \cdot)$ un gruppo e X un insieme qualunque. Si dice *azione di G su X* un omomorfismo di gruppi

$$\begin{aligned} \varphi : G &\to \mathcal{S}(X) \\ g &\mapsto \varphi_g. \end{aligned}$$

Altre notazioni che useremo per la permutazione degli elementi di X definita da g sono gx e x^g.

Esempio 2.3.2. Se $X = G$ un possibile esempio è dato dal coniugio per g: l'applicazione $g \mapsto \varphi_g$ dove $\varphi_g(x) = gxg^{-1}$ è un omomorfismo tra il gruppo G e il gruppo delle permutazioni degli elementi di G, dunque è un'azione di G su G.

Esempio 2.3.3. Sia V un $\mathbb{K}$-spazio vettoriale. Allora l'applicazione

$$\begin{aligned} \varphi : \mathbb{K}^\times &\to \mathcal{S}(V) \\ \lambda &\mapsto \varphi_\lambda \end{aligned}$$

e $\varphi_\lambda(\vec{v}) = \lambda \cdot \vec{v}$ è un'azione del gruppo degli scalari sullo spazio vettoriale. Più in generale, potremmo definire uno spazio vettoriale come un gruppo abeliano additivo su cui è definita un'azione di $\mathbb{K}^\times$ su V.

Classe di equivalenza definita da un'azione

Sia $\varphi : G \to \mathcal{S}(V)$ un'azione di gruppo. φ definisce su X la seguente relazione:

$$x \sim y \iff \exists g \in G \text{ tale che } \varphi_g(x) = y. \tag{20}$$

Proposizione 2.3.4 *La relazione definita da un'azione di gruppo è una relazione di equivalenza.*

Dimostrazione. Sia G un gruppo, X l'insieme su cui G agisce. Mostriamo che la relazione $\sim$ definita nella (20) è una relazione di equivalenza.

RIFLESSIVITÀ Sia $x \in X$. Siccome φ è un omomorfismo di gruppi segue che $\varphi(e_G) = \varphi_e = \mathrm{id}$, da cui

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

SIMMETRIA Siano $x, y \in X$ tali che $x \sim y$, ovvero $\varphi_g(x) = y$ per qualche $g \in G$. Mostriamo che $\varphi_{g^{-1}}(y) = x$: applicando $\varphi_{g^{-1}}$ ad entrambi i membri otteniamo

$$\begin{aligned}
\varphi_{g^{-1}}(y) &= \varphi_{g^{-1}}\big(\varphi_g(x)\big) \\
&= (\varphi_{g^{-1}} \circ \varphi_g)(x) \\
&= (\varphi(g^{-1}) \circ \varphi(g))(x) \\
&= (\varphi(g)^{-1} \circ \varphi(g))(x) \\
&= x,
\end{aligned}$$

da cui segue $y \sim x$.

TRANSITIVITÀ Siano $x, y, z \in X$ tali che $x \sim y$ e $y \sim z$, ovvero $\varphi_g(x) = y$ e $\varphi_h(y) = z$ per qualche $g, h \in G$. Allora vale che

$$\begin{aligned}
z &= \varphi_h\big(\varphi_g(x)\big) \\
&= (\varphi_h \circ \varphi_g)(x) \\
&= (\varphi(h) \circ \varphi(g))(x) \\
&= \varphi(hg)(x) \\
&= \varphi_{hg}(x),
\end{aligned}$$

da cui segue che $x \sim z$.

□

Osservazione. Notiamo che siccome φ è un omomorfismo di gruppi, se φ_g e φ_h sono le azioni di g e h sull'insieme X, allora la loro composizione sarà l'azione

$$\varphi_g \circ \varphi_h = \varphi(g) \circ \varphi(h) = \varphi(gh) = \varphi_{gh}.$$

Invece, data l'azione φ_g di g su X, segue che la sua inversa è $\varphi_{g^{-1}}$:

$$\begin{aligned}
\varphi_{g^{-1}} \circ \varphi_g &= \varphi(g^{-1}) \circ \varphi(g) = \varphi(g)^{-1} \circ \varphi(g) = \mathrm{id}\,. \\
\varphi_g \circ \varphi_{g^{-1}} &= \varphi(g) \circ \varphi(g^{-1}) = \varphi(g) \circ \varphi(g)^{-1} = \mathrm{id}\,.
\end{aligned}$$

Definizione 2.3.5 **Orbita.** Sia G un gruppo che agisce sull'insieme X. Dato $x \in X$ si dice *orbita di* x l'insieme

$$\mathrm{orb}(x) := \{\, \varphi_g(x) \;:\; g \in G \,\} \subseteq X.$$

Osservazione. L'orbita di x è esattamente la classe di equivalenza data dalla relazione di equivalenza definita in (20). In particolare se R è un insieme di rappresentanti vale che

$$X = \bigsqcup_{x \in R} \operatorname{orb}(x).$$

Definizione 2.3.6 **Stabilizzatore.** Sia G un gruppo che agisce sull'insieme X. Dato $x \in X$ si dice *stabilizzatore di* x l'insieme

$$\operatorname{St}(x) := \{\, g \in G \,:\, \varphi_g(x) = x \,\} \subseteq G.$$

Proposizione 2.3.7 **Lo stabilizzatore è un sottogruppo.** *Sia* G *un gruppo che agisce sull'insieme* X*; sia inoltre* $x \in X$*. Allora vale che*

$$\operatorname{St}(x) \leqslant G.$$

Dimostrazione. Innanzitutto $e_G \in \operatorname{St}(x)$ in quanto $\varphi_e(x) = x$ (l'azione dell'identità è sempre l'identità).

Supponiamo che $g \in \operatorname{St}(x)$, ovvero $\varphi_g(x) = x$: mostriamo che anche $g^{-1} \in \operatorname{St}(x)$, ovvero $\varphi_{g^{-1}} \in \operatorname{St}(x)$. Applichiamo ad entrambi i membri l'azione $(\varphi_g)^{-1}$, ottenendo

$$(\varphi_g)^{-1}(x) = (\varphi_g)^{-1}\big(\varphi_g(x)\big) = x.$$

Come abbiamo osservato precedentemente, $(\varphi_g)^{-1} = \varphi_{g^{-1}}$, da cui segue che $x = \varphi_{g^{-1}}(x)$ e quindi $g^{-1} \in \operatorname{St}(x)$.

Supponiamo infine che $g, h \in \operatorname{St}(x)$ e mostriamo che $hg \in \operatorname{St}(x)$. Infatti

$$\begin{aligned} \varphi_{hg}(x) &= (\varphi_h \circ \varphi_g)(x) \\ &= \varphi_h\big(\varphi_g(x)\big) \\ &= \varphi_h(x) \\ &= x. \end{aligned}$$

Dunque $\operatorname{St}(()x)$ è un sottogruppo di G. $\square$