Algebra

Luca De Paulis

18 ottobre 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

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

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. $\square$

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

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

è un gruppo abeliano;

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

$$\mathbb{Z}/^\times_{n\mathbb{Z}} \coloneqq \{ [n] \in \mathbb{Z}/_{n\mathbb{Z}} : [n] \text{ è invertibile rispetto a } \cdot \}$$

è un gruppo abeliano.

Dimostrazione. Infatti

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

(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. $\square$

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*

$$ab = ac \iff b = c \tag{sx}$$
$$ba = ca \iff b = c \tag{dx}$$

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:

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

□

1.2 SOTTOGRUPPI

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

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

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

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

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

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

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

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

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

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

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

Da ciò viene la tesi. □

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

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

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

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

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

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

Allora vale che

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

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

Dimostrazione. Mostriamo le due affermazioni separatamente

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

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

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

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

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

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.

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

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

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

$$\Longrightarrow m \mid n.$$

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

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

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

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

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 $H \cap K \leqslant G$. $\square$

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

$$< g > := \left\{ g^k \ : \ k \in \mathbb{Z} \right\}.$$

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

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

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

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

Dunque per la proposizione 1.2.2 segue che $< g > \leqslant G$.
Inoltre notiamo che

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

dunque $< g >$ 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

$$\mathrm{ord}_G(x) := \min\Big\{ k > 0 \ : \ x^k =_G e \Big\}.$$

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

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

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

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

(i) Il sottogruppo generato $<x>$ *è*

$$<x> = \Big\{ e, x, x^2, \ldots, x^{d-1} \Big\}.$$

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

(ii) $x^n = e$ *se e solo se* $d \mid n$.

Dimostrazione. Dimostriamo le due affermazioni separatamente.

PARTE 1. Sicuramente vale che

$$\Big\{ e, x, \ldots, x^{d-1} \Big\} \subseteq <x>.$$

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

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

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 $x^r \in \{ e, x, \ldots, x^{d-1} \}$. Dato che $x^r = x^k$ concludiamo che

$$x^k \in \Big\{ e, x, \ldots, x^{d-1} \Big\}$$

e quindi

$$<x> = \Big\{ e, x, \ldots, x^{d-1} \Big\}.$$

Ci rimane da mostrare che $|\langle x \rangle| = d$, ovvero che tutti gli elementi di $<x>$ 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 $<x>$ 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

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

$\square$

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

$$G = <g>.$$

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

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

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

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

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

Se $H = \{e_G\}$ allora H è ciclico, e $H = <e_G>$.

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

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

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

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

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

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

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

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

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

Dunque

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

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

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

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

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

Consideriamo i sottogruppi di $\mathbb{Z}$. Tramite la proposizione 1.2.6 abbiamo dimostrato che per ogni $n \in \mathbb{Z}$ allora $n\mathbb{Z} \leqslant \mathbb{Z}$. La prossima proposizione mostra che i sottogruppi della forma $n\mathbb{Z} = <n>$ 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 $\mathbb{Z} = <1>$) per il teorema 1.3.7 ogni suo sottogruppo dovrà essere ciclico, ovvero dovrà essere della forma $<n>$ 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 $<n> = n\mathbb{Z}$, 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

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

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

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

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

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

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

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

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

Dimostrazione. Per definizione di ordine

$$\operatorname{ord}([a]) = \min\{\, k > 0 \; : \; k[a] = [0] \,\}.$$

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

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

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

(i) Per ogni $[a] \in \mathbb{Z}/_{n\mathbb{Z}}$ *vale che* $\operatorname{ord}([a]) \mid n$.

(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. Dimostriamo separatamente le tre affermazioni.

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

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

$$\langle [x] \rangle = \mathbb{Z}/_{n\mathbb{Z}}$$

ovvero se la cardinalità di $\langle [x] \rangle$ è n.

Per la proposizione 1.3.9 $\operatorname{ord}([x]) = \dfrac{n}{(n,x)}$, dunque $[x]$ 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 $[a] \in \mathbb{Z}/_{n\mathbb{Z}}$ tale che

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

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 ci sono $\varphi(d)$ scelte per b, ovvero esistono $\varphi(d)$ elementi di ordine d.

$\square$

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

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

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

Dimostrazione. Sia X_d l'insieme

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

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

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

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

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

□

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

Proposizione 1.3.12 **Caratterizzazione dei sottogruppi di $\mathbb{Z}/_{n\mathbb{Z}}$.** *Valgono i seguenti due 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. Dimostriamo separatamente le due affermazioni.

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

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

(ii) Sia H_d l'insieme

$$H_d = \left\{ [0],\ [\frac{n}{d}],\ 2[\frac{n}{d}], \dots,\ (d-1)[\frac{n}{d}] \right\}.$$

Mostriamo innanzitutto che $H_d = \left\langle \dfrac{[n]}{d} \right\rangle$.

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

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

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 $H = \langle [x] \rangle$ per qualche $[x] \in \mathbb{Z}/_{n\mathbb{Z}}$ tale che $\mathrm{ord}([x]) = d$.
Seguendo la dimostrazione di 1.3.10: (iii) possiamo scrivere $[x] = [\frac{n}{d}]b$ con $b \in Z$ tale che $(b, d) = 1$.
Ma $H_d = \left\langle [\frac{n}{d}] \right\rangle$ contiene tutti i multipli di $[\frac{n}{d}]$, dunque deve contenere anche $[x]$.
Dunque dato che $[x] \in H_d$ segue che $H = \langle [x] \rangle \subseteq H_d$. 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

$$\pi_n(a + b) = [a + b] = [a] + [b] = \pi_n(a) + \pi_n(b).$$

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. $\square$

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 $\text{ord}(f(x)) \mid \text{ord}(x)$, dunque $\text{ord}(f(x)) = \text{ord}(x)$.

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

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

Ma $\text{ord}(x) = 1$ 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

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

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 $G = <g>$ 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

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

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

- Mostriamo che φ è ben definita. Siano $a, b \in [a]$ e mostriamo che $\varphi([a]) = \varphi([b])$, 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.

  $$\varphi([a] + [b]) = g^{a+b} = g^a g^b = \varphi([a])\varphi([b]).$$

- Mostriamo che φ è surgettiva.

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

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 $|G| = \operatorname{ord}(g) = n$ per qualche n finito.
Allora per il Teorema 1.4.12 esiste un isomorfismo
$$\begin{aligned} \psi : \mathbb{Z}/_{n\mathbb{Z}} &\to G \\ [a] &\mapsto g^a. \end{aligned}$$
Per l'osservazione 2) sopra i sottogruppi di $\mathbb{Z}/_{n\mathbb{Z}}$ sono tutti e solo della forma $\langle [d] \rangle$, dunque per l'osservazione 3) segue che
$$\{ K : K \leqslant G \} = \left\{ \psi(\langle [d] \rangle) = \left\langle g^d \right\rangle : d \mid n \right\}. \qquad \square$$

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 $\operatorname{Aut}(G)$.

Proposizione 1.4.15 **Gruppo degli automorfismi.** *Sia* $(G, \cdot)$ *un gruppo. Allora la struttura* $(\operatorname{Aut}(G), \circ)$ *(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

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

1.5 PRODOTTO DIRETTO DI GRUPPI

Definizione 1.5.1 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 1.5.2 **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 1.5.3 **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 1.5.4 **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*

$$\mathrm{ord}_{G_1 \times G_2}((x, y)) = \big(\mathrm{ord}_{G_1}(x), \mathrm{ord}_{G_2}(y)\big).$$

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

($d \mid (n, m)$) Vale che

$$(x, y)^{(n,m)} = \left(x^{(n,m)}, y^{(n,m)}\right).$$

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

$$\left(x^{(n,m)}, y^{(n,m)}\right) = (e_1, e_2)$$

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 1.5.5 **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 $\mathrm{ord}(g) = |G|$: 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 1.5.4 vale che

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

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

$$\operatorname{ord}(g) \leqslant [n,m] = \frac{mn}{d} < mn$$

da cui segue che G non può essere ciclico;

2. se $(n,m) = 1$ allora per ogni $g \in G$ vale che

$$\operatorname{ord}(g) \leqslant [n,m] = mn.$$

In particolare se consideriamo $g = (\overline{1}, \overline{1})$ si ha che

$$\operatorname{ord}(\overline{1},\overline{1}) = \left[\frac{n}{(n,1)}, \frac{m}{(m,1)}\right] = [m,n] = mn$$

, dunque $G = \left\langle (\overline{1},\overline{1}) \right\rangle$, 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

$$\begin{aligned} \varphi : \mathbb{Z}/_{nm\mathbb{Z}} &\to \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}} \\ [a]_{mn} &\mapsto ([a]_n, [a]_m) \end{aligned} \tag{4}$$

è bigettiva. Inoltre

$$\begin{aligned} \varphi([a]_{mn} + [b]_{mn}) &= \varphi([a+b]_{mn}) \\ &= ([a+b]_n, [a+b]_m) \\ &= ([a]_n + [b]_n, [a]_m + [b]_m) \\ &= ([a]_n, [a]_m) + ([b]_n, [b]_m) \\ &= \varphi([a]_{mn}) + \varphi([b]_{mn}), \end{aligned}$$

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 1.5.6 **Isomorfismo tra i gruppi degli invertibili.** *Siano $n, m \in \mathbb{Z}$ entrambi non nulli. Allora se $(n,m) = 1$ segue che*

$$\mathbb{Z}/_{nm\mathbb{Z}}^{\times} \simeq \mathbb{Z}/_{n\mathbb{Z}}^{\times} \times \mathbb{Z}/_{m\mathbb{Z}}^{\times}. \tag{5}$$

Dimostrazione. Consideriamo la funzione

$$\begin{aligned} \varphi^* : \mathbb{Z}/_{nm\mathbb{Z}}^{\times} &\to \mathbb{Z}/_{n\mathbb{Z}}^{\times} \times \mathbb{Z}/_{m\mathbb{Z}}^{\times} \\ [a]_{mn} &\mapsto [a]_n \times [a]_m. \end{aligned}$$

Essa è ben definita: infatti se $[a]_{mn} \in \mathbb{Z}/_{nm\mathbb{Z}}^{\times}$ segue che $(a, mn) = 1$. Siccome per ipotesi $(m,n) = 1$ per la PROPOSIZIONE NON

SCRITTA segue che $(m, n) = (a, m) = 1$, ovvero $[a]_n \in \mathbb{Z}/_{n\mathbb{Z}}^{\times}$ e $[a]_m \in \mathbb{Z}/_{m\mathbb{Z}}^{\times}$.

Inoltre questa funzione è una restrizione della φ definita in (4), dunque è iniettiva. Infine

$$|\mathbb{Z}/_{nm\mathbb{Z}}| = \phi(nm) = \phi(n)\phi(m) = |\mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}|$$

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. □

1.5.1 Prodotto interno di sottogruppi

Definizione 1.5.7 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 1.5.8 **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 il loro prodotto $(h_1k_1) \cdot (h_2k_2)$ sia ancora una volta un elemento di 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 $HK = KH$. □

1.6 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

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

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 1.6.1 **Classe laterale sinistra.** Sia $(G, \cdot)$ un gruppo, $H \leqslant G$ un suo sottogruppo e $x \in G$ un elemento del gruppo 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 1.6.2. 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

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

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

Definizione 1.6.3 **Classe laterale destra.** Sia $(G, \cdot)$ un gruppo, $H \leqslant G$ un suo sottogruppo e $x \in G$ un elemento del gruppo 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 1.6.4 **Teorema di Lagrange.** *Sia* $(G, \cdot)$ *un gruppo finito e sia* $H \leqslant G$ *qualsiasi. Allora vale che*

$$|H| \bigm| |G|.$$

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 1.6.5 *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 1.6.4. 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 1.6.5 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 1.6.6 *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 1.6.7 **Corollario al Teorema di Lagrange.** *Sia* $(G, \cdot)$ *un gruppo finito. Allora valgono i seguenti fatti:*

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

(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

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

(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 1.6.8 **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

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

Dunque per definizione di numero primo $\operatorname{ord}_G(x) = p$, 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 1.6.7 (in particolare dal punto (ii)) considerando come gruppo $(\mathbb{Z}/_{n\mathbb{Z}}^{\times}, \cdot)$: infatti per definizione $\varphi(n) = |\mathbb{Z}/_{n\mathbb{Z}}^{\times}|$, da cui la tesi. □

1.6.1 Sottogruppi normali e gruppo quoziente

Definizione 1.6.9 **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 1.6.10 *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.

$(\implies)$ 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 $gHg^{-1} \subseteq H$.

($\Longleftarrow$) Supponiamo che $gHg^{-1} \subseteq H$, ovvero che per ogni $h \in H$ valga che $ghg^{-1} \in H$. Questo significa che per qualchea $h' \in H$ vale che $ghg^{-1} = h'$, il che è equivalente ad affermare $gh = h'g \in Hg$, da cui segue che $gH \subseteq Hg$.

Mostriamo ora che vale anche l'inclusione contraria. Dato che la relazione deve valere per quasliasi g, dovrà valere anche per $g^{-1} \in G$: dunque $g^{-1}Hg \subseteq H$. Moltiplicando a sinistra per g^{-1} e a destra per g si ottiene $H \subseteq gHg^{-1}$.

Dunque $gHg^{-1} = H$, da cui $gH = Hg$, ovvero la tesi. □

Proposizione 1.6.11 **Il centro è un sottogruppo normale.** *Sia $(G, \cdot)$ un gruppo. Allora vale che*

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

Dimostrazione. Per mostrare che il centro di G è normale in G, è sufficiente mostrare che $gZ(G)g^{-1} \in Z(G)$. Sia quindi $g \in G$, $x \in \mathbb{Z}(G)$ qualunque. Allora

$$gxg^{-1} = gg^{-1}x = x \in Z(G),$$

da cui segue che $gZ(G)g^{-1} \subseteq Z(G)$, ovvero $Z(G) \triangleleft G$. □

Definizione 1.6.12 **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

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

Tornando alla dimostrazione del Teorema di Lagrange, notiamo che la classe di rappresentanti R dovrà contenere esattamente un elemento per ogni classe laterale di H. Dunque vale il seguente risultato:

$$|G| = [G : H] \cdot |H|, \tag{11}$$

o equivalentemente, l'indice di un sottogruppo H in un gruppo G è dato dal rapporto tra la cardinalità di G e quella di H.

Proposizione 1.6.13 *Sia $(G, \cdot)$ un gruppo, $H \leqslant G$. Allora se $[G : H] = 2$ segue che $H \triangleleft G$.*

Dimostrazione. Osserviamo che la classe $eH = H$ è sempre una classe laterale di H. Siccome le classi laterali formano una partizione dell'insieme G e l'indice di H in G è 2, segue che esiste una singola altra classe laterale data da $gH = G \setminus H$, per qualche $g \notin H$. Questo implica che $Hg \neq H$, in quanto altrimenti avremmo $g \in G$: dunque $gH = Hg$ poiché gH è l'unica classe laterale diversa da H, da cui $H \triangleleft G$. □

Proposizione 1.6.14 **Nucleo di omomorfismi e normalità.** *Siano $(G, \cdot)$, $(G', *)$ due gruppi e sia $f : G \to G'$ un omomorfismo.*

Valgono le seguenti affermazioni.

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

(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 1.6.10 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:

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

□

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

$$G/_H := \{ gH : g \in G \}. \tag{12}$$

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

$$\begin{aligned} \cdot : G/_H \times G/_H &\to G/_H \\ (aH, bH) &\mapsto abH. \end{aligned} \tag{13}$$

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

Proposizione 1.6.15 *Sia* $(G, \cdot)$ *un gruppo e sia* $N \triangleleft G$*. Allora la struttura* $(G/_N, \star)$ *(dove l'operazione è definita come in (13)) 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

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

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 $xN \in G/_N$

$$e_GN \star xN = e_GxN = xN.$$
$$xN \star e_GN = xe_GN = xN.$$

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

$$xN \star x^{-1}N = xx^{-1}N = e_GN.$$
$$x^{-1}N \star xN = x^{-1}xN = e_GN.$$

Dunque $(G/_N, \star)$ è un gruppo. □

ESEMPIO 1.6.16. 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 1.6.17 *Sia* $(G, \cdot)$ *un gruppo e sia* $N \triangleleft G$*. Allora la mappa*

$$\begin{aligned} \pi_N : G &\to G/_N \\ x &\mapsto xN \end{aligned} \tag{14}$$

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 1.6.6 (in particolare per l'equivalenza tra i punti (ii) e (iii)). □

L'omomorfismo π_N viene chiamato *proiezione canonica al quoziente*.

Corollario 1.6.18 *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 1.6.17 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 1.6.14. □

Altri risultati derivanti dai gruppi quozienti

In questa sezione esporremo alcuni importanti risultati che possono essere ottenuto sfruttando particolari quozienti.

Teorema 1.6.19 **Teorema di Cauchy per gruppi abeliani.** *Sia* $(G, \cdot)$ *un gruppo abeliano finito e sia* $p \in \mathbb{Z}$ *un primo tale che* $p \mid |G|$. *Allora esiste* $g \in G$ *tale che* $\mathrm{ord}_G(g) = p$.

Dimostrazione. Ragioniamo per induzione forte su $n := |G|$.

CASO BASE Se G ha ordine p, allora per il Corollario 1.6.8 segue che $G \simeq \mathbb{Z}/_{p\mathbb{Z}}$, dunque ogni elemento invertibile ha ordine p.

PASSO INDUTTIVO Supponiamo $n > p$, $p \mid n$.

Se G è ciclico, allora $G \simeq \mathbb{Z}/_{n\mathbb{Z}}$. Per il Corollario 1.3.10 sappiamo che ci sono $\varphi(p) = p - 1$ elementi di ordine p in $\mathbb{Z}/_{n\mathbb{Z}}$, dunque in particolare vi è almeno un elemento di ordine p.

Sia ora G un gruppo generico, $g \in G \setminus \{ e_G \}$ un elemento diverso dall'identità. Se l'ordine di g è multiplo di p, allora $\#< g >$ è un multiplo di p, da cui segue che c'è almeno un elemento di ordine p in $\langle g \rangle$ (poiché $\langle g \rangle$ è ciclico continua a valere la proposizione Corollario 1.3.10) e quindi in G.

Se l'ordine di g non è multiplo di p considero il gruppo $H := G/_{< g >}$: H è un gruppo in quanto G è abeliano e tutti i sottogruppi di un gruppo abeliano sono normali. Per la (11) segue che

$$|H| = \frac{|G|}{|< g >|} < n;$$

inoltre siccome $p \mid |G|$ e $p \nmid |< g >|$ segue che $p \mid \frac{|G|}{|< g >|}$. Per ipotesi induttiva segue quindi che H contiene un elemento di ordine p: chiamiamolo h.

Sia $\pi_H : G \to H$ la proiezione canonica al quoziente; scelgo $t \in G$ tale che $\pi_H(t) = h$. Essendo π_H surgettiva, tale elemento sicuramente esiste (anche se non è detto che sia unico). Per la Proposizione 1.4.8 segue che

$$p = \mathrm{ord}_H(h) = \mathrm{ord}_H(\pi_H(t)) \mid \mathrm{ord}_G(t),$$

da cui $\langle t \rangle \leqslant G$ è un sottogruppo di ordine multiplo di p, da cui si procede come prima. $\square$

Proposizione 1.6.20 *Sia $(G, \cdot)$ un gruppo tale che $G/_{Z(G)}$ è ciclico. Allora G è abeliano.*

Dimostrazione. Siccome $G/_{Z(G)}$ è ciclico, deve esistere $a \in G$ tale che $G/_{Z(G)} = \langle aZ(G) \rangle$. Sia $H = G/_{Z(G)}$.

Se $a \in Z(G)$ allora $aZ(G) = Z(G)$, da cui $G/_{Z(G)} = \langle e_H \rangle = \{ e_H \}$. Questo implica che $Z(G) = G$, ovvero G è abeliano.

Supponiamo quindi che $a \notin Z(G)$: questo significa che esiste un $b \in G$ tale che $ab \neq ba$. Sia $\pi_H : G \to H$ la proiezione canonica sul quoziente. Allora vale che

$$\pi_H(b) = bZ(G) = a^k Z(G),$$

dove l'ultima uguaglianza è data dal fatto che $aZ(G)$ è un generatore di H. Questo significa in particolare che $a^k b^{-1} \in Z(G)$, ovvero esiste $z \in Z$ tale che $z = a^k b^{-1}$ (ovvero $b = a^k z^{-1}$, $a^k = zb$).

$$\begin{aligned} ab &= aa^k z^{-1} = a^{k+1} z^{-1} \\ ba &= a^k z^{-1} a = a^{k+1} z^{-1} \end{aligned}$$

dove l'ultima uguaglianza segue dal fatto che $z^{-1} \in Z(G)$. Dunque $ab = ba$, il che è assurdo, dunque segue che $a \in Z(G)$ e quindi G è abeliano.

$\square$

1.7 TEOREMI DI OMOMORFISMO

1.7.1 Primo Teorema degli Omomorfismi

Teorema 1.7.1 **Primo Teorema degli Omomorfismi.** *Siano $(G, \cdot)$, $(G', *)$ due gruppi e sia $f : G \to G'$ un omomorfismo di gruppi. Sia inoltre $N \lhd G$, $N \subseteq \ker f$.*

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

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_N"'] & G' \\ G/_N \arrow[ur, "\varphi"'] & \end{tikzcd} \tag{15}$$

Inoltre vale che

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

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

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

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

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

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 1.7.2 *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:*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_{\ker f}"'] & G' \\ G/_{\ker f} \arrow[ur, hook, "\varphi"'] & \end{tikzcd} \tag{16}$$

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 $\ker f \triangleleft G$ 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:

$$\begin{tikzcd} G \arrow[r, two heads, "\pi_{\ker f}"'] \arrow[rrr, bend left, "f"] & G/_{\ker f} \arrow[r, hook, two heads, "\varphi"'] & \operatorname{Im} f \arrow[r, hook, "\iota"'] & G' \end{tikzcd} \tag{17}$$

Vale dunque il seguente corollario.

Corollario 1.7.3 *Siano $(G, \cdot)$, $(G', *)$ due gruppi e sia $f : G \to G'$ un omomorfismo di gruppi. Allora*

$$G/_{\ker f} \simeq \operatorname{Im} f. \tag{18}$$

1.7.2 Secondo Teorema degli Omomorfismi

Teorema 1.7.4 **Secondo Teorema degli Omomorfismi.** *Sia $(G, \cdot)$ un gruppo e siano $H, K \triangleleft G$, con $H \subseteq K$. Allora*

$$\frac{G/_H}{K/_H} \simeq G/_K. \tag{19}$$

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 $H \triangleleft G$ (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:

$$\begin{tikzcd} G \arrow[r, "\pi_K"] \arrow[d, "\pi_H"'] & G/_K \\ G/_H \arrow[ur, two heads, "\varphi"'] & \end{tikzcd}$$

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:

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

$\tilde{\varphi}$ 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

$${}^{G/_H}/_{K/_H} \simeq G/_K. \qquad \square$$

1.7.3 Terzo Teorema degli Omomorfismi

Teorema 1.7.5 **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*

$$\frac{H}{H \cap N} \simeq \frac{HN}{N}. \tag{20}$$

Dimostrazione. Dimostriamo innanzitutto le due condizioni di normalità.

$(N \triangleleft HN)$ Mostriamo innanzitutto che HN è un sottogruppo di G. Per la Proposizione 1.5.8, 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

$$\operatorname{Im} f = HN/_N$$

il che equivale a

$$\{hN \in HN/_N \,:\, h \in H\} = \{yN \in HN/_N \,:\, y \in HN\}.$$

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

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

Prima di studiare il Teorema di Corrispondenza, introduciamo un lemma che ci sarà utile:

Lemma 1.7.6 *Siano $(G, \cdot)$, $(G', \cdot)$ due gruppi e sia $f : G \to G'$ un omomorfismo. Se $K \triangleleft G'$, allora $f^{-1}(K) \triangleleft G$.*

Inoltre se f è surgettivo e $H \triangleleft G$ segue che

$$f(H) \triangleleft G' = f(G).$$

Teorema 1.7.7 **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* $A/_N \triangleleft G/_N$.

Prima di iniziare la dimostrazione, osserviamo che siccome la proiezione canonica è un omomorfismo, vale che

$$\pi(H) \leqslant G/_N, \qquad \pi^{-1}(K) \leqslant G$$

per ogni $H \leqslant G$, $K \leqslant G/_N$.

Dimostrazione. Siano α e β le mappe date da:

$$\begin{aligned} X &\leftrightarrow Y \\ H &\overset{\alpha}{\mapsto} H/_N = \pi_N(H) \\ \pi_N^{-1}(K) &\overset{\beta}{\leftarrow\!\shortmid} K. \end{aligned}$$

BUONA DEFINIZIONE α è ben definita poiché l'immagine di un sottogruppo attraverso la proiezione canonica è un sottogruppo:

$$\alpha(H) = \pi_N(H) = H/_N \leqslant G/_N.$$

Mostriamo quindi che β è ben definita: sia $K \leqslant G/_N$ e mostriamo che $\beta(K) = \pi_N^{-1}(K)$ è un sottogruppo di G che contiene N. Siccome $G/_N$ è il quoziente modulo N la sua identità è $N = eN$; per definizione di sottogruppo ogni elemento di $\mathcal{N}$ dovrà contenere l'identità del gruppo, ovvero N. Segue quindi che

$$N = \pi_N^{-1}(N) \subseteq \pi_N^{-1}(K),$$

da cui $\pi_N^{-1}(K) \in \mathcal{G}$.

LE DUE FUNZIONI SONO UNA L'INVERSA DELL'ALTRA Mostriamo che $\alpha \circ \beta = \mathrm{id}$. Sia $K \in \mathcal{N}$: allora

$$(\alpha \circ \beta)(K) = \alpha\big(\pi^{-1}(K)\big) = \pi\big(\pi^{-1}(K)\big) = K,$$

dove il penultimo passaggio viene dal fatto che π è surgettiva, e quindi invertibile da destra.

Mostriamo ora che $\beta \circ \alpha = \mathrm{id}$. Sia $H \in \mathcal{G}$: allora

$$\begin{aligned} (\beta \circ \alpha)(H) &= \beta(\pi(H)) \\ &= \beta\big(H/_N\big) \\ &= \pi_N^{-1}\big(H/_N\big) \\ &= \{x \in G : \pi_N(x) \in H/_N\} \\ &= \{x \in G : xN \in H/_N\} \\ &= \{x \in G : x \in H\} \\ &= H. \end{aligned}$$

LA BIGEZIONE PRESERVA I SOTTOGRUPPI NORMALI Sia $H \in \mathcal{G}$; mostriamo che

$$H \triangleleft G \iff H/_N \triangleleft G/_N.$$

($\implies$) Segue dal Secondo Teorema degli Omomorfismi. Infatti siccome $N, H \triangleleft G$ e $N \subseteq H$ segue che

$$\frac{G/_N}{H/_N} \simeq G/_H.$$

Ma questo significa che $\dfrac{G/N}{H/N}$ è un gruppo, da cui segue che

$$H/N \lhd G/N.$$

($\Longleftarrow$ **)** Segue dal Lemma 1.7.6.

LA BIGEZIONE CONSERVA L'INDICE DI SOTTOGRUPPO Sia $H \in \mathcal{G}$: mostriamo che

$$[G : H] = [G/N : H/N].$$

Siano $x, y \in G$ qualsiasi. Mostriamo che le classi laterali xH e yH sono uguali se e solo se

$$(xN)H/N = (yN)H/N.$$

Per definizione

$$(xN)H/N = \{xNhN : h \in H\} = \{xhN : h \in H\};$$

allo stesso modo

$$(yN)H/N = \{yhN : h \in H\}.$$

FINIRE $\square$

2 ANELLI E CAMPI

2.1 ANELLI

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

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

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

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

(S1) Vale la *proprietà commutativa della somma*:

per ogni $a, b \in A$ vale che $a + b = b + a$.

(S2) Vale la *proprietà associativa della somma*:

per ogni $a, b, c \in A$ vale che $(a + b) + c = a + (b + c)$.

(S3) Esiste un elemento $0 \in A$ che è *elemento neutro* per la somma:

per ogni $a \in A$ vale che $a + 0 = 0 + a = a$.

Tale elemento si chiama *zero dell'anello*.

(S4) Ogni elemento di A è *invertibile* rispetto alla somma:

per ogni $a \in A$ esiste $(-a) \in A$ (detto *opposto di* a) tale che $a + (-a) = 0$.

(P) Vale il seguente assioma per il prodotto:

(P1) Vale la *proprietà associativa del prodotto*:

per ogni $a, b, c \in A$ vale che $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(D) Vale la *proprietà distributiva del prodotto rispetto alla somma* sia a destra che a sinistra:

per ogni $a, b, c \in A$ vale che $a(b + c) = ab + ac$ e che $(a + b)c = ac + bc$.

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

(P2) Vale la *proprietà commutativa del prodotto*:

per ogni $a, b \in A$ vale che $a \cdot b = b \cdot a$.

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

(P2) Esiste un elemento $1 \in A$ che è *elemento neutro* per il prodotto:

per ogni $a \in A$ vale che $a \cdot 1 = 1 \cdot a = a$.

Tale elemento si dice *unità dell'anello*.

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

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

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

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

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

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

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

$$ab = 0.$$

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

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

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

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

Dimostrazione. Dimostriamo separatamente le varie affermazioni.

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

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

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

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

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

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

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

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

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

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

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

Siccome è invertibile segue che

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

Ma allora

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ora mostro che φ_x è bigettiva.

φ_x **È INIETTIVA** Supponiamo che per qualche $a, b \in A$ valga che $\varphi_x(a) = \varphi_x(b)$ e mostriamo che segue che $a = b$.

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

φ_x **È SURGETTIVA** Poiché la cardinalità del dominio e del codominio di φ_x è la stessa ed è finita segue che φ_x è anche surgettiva.

Dunque φ_x è bigettiva. Dato che $1 \in A = \varphi_x(A)$ segue che esiste un $y \in A$ tale che

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

ovvero x è invertibile e A è un campo. □

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

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

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

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

2.2 ANELLO DEI POLINOMI

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

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

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

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

Gli a_i si dicono *coefficienti del polinomio*.
L'insieme dei polinomi a coefficienti in A si indica con $A[X]$.

Dato che la successione che definisce il polinomio è definitivamente nulla, possiamo scrivere il polinomio come una sequenza finita di termini: basta prendere i termini fino al massimo indice per cui a_i è diverso da 0. Diamo però alcune definizioni preliminari.
Innanzitutto d'ora in avanti $(A, +, \cdot)$ è un anello commutativo con identità a meno di ulteriori specifiche.

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

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

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

Il polinomio $0_{A[X]}$ non ha grado.

Notiamo che i polinomi di grado 0 sono tutti e solo della forma $p(X) = a_0$ per qualche $a_0 \in A$; ovvero sono tutte e sole le costanti dell'anello A. Possiamo quindi considerare l'anello A come un sottoinsieme dell'insieme dei polinomi $A[X]$.

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

Definiamo ora le operazioni di somma e prodotto tra polinomi.

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

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

nel seguente modo:

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

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

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

nel seguente modo:

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

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

Dimostrazione. Basta verificare tutti gli assiomi degli anelli. □

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

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

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

Dimostrazione. Siano i due polinomi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Notiamo che $p, q \neq 0_{A[X]}$. Infatti se uno dei due fosse il polinomio nullo per la punto 2.1.9: (i) il loro prodotto dovrebbe essere il polinomio nullo e non l'unità. Allora esistono $\deg p, \deg q \geqslant 0$ e vale che

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

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

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

Dopo aver caratterizzato gli elementi invertibili in $A[X]$ possiamo definire il concetto di *elementi associati*.

Definizione 2.2.11 **Polinomi associati.** Siano $f, g \in A[X]$. Allora f, g si dicono *associati* se esiste $\alpha \in A[X]^\times$ (ovvero in $A^\times$) tale che

$$f(X) = \alpha g(X).$$

Definizione 2.2.12 **Funzione polinomiale.** Sia $p \in A[X]$, $p(X) = \sum_{i=0}^{\deg p} a_i X^i$. Allora possiamo associare al polinomio p una funzione $A \to A$ tale che

$$A \ni \alpha \mapsto \sum_{i=0}^{\deg p} a_i \alpha^i \in A. \tag{21}$$

Tale funzione si dice *funzione polinomiale associata a* p e si indica solitamente come il polinomio a cui è associata.

2.2.1 Polinomi a coefficienti in un campo

In questa sezione studieremo l'anello $\mathbb{K}[X]$, dove $\mathbb{K}$ è un campo generico. Questo anello ha una relazione molto stretta con l'insieme $\mathbb{Z}$ dei numeri interi, soprattutto per quanto riguarda le proprietà di divisibilità.

Teorema 2.2.13 **Esistenza e unicità della Divisione Euclidea.** *Siano* $f, g \in \mathbb{K}[X]$ *con* $f(X) \neq 0_{\mathbb{K}[X]}$. *Allora esistono e sono unici due polinomi* $q, r \in \mathbb{K}[X]$ *tali che*

$$g(X) = q(X)f(X) + r(X),$$

con $r(X) = 0_{\mathbb{K}[X]}$ *oppure* $0 \leqslant \deg r \leqslant \deg f$.

Dimostrazione dell'esistenza. Se $g(X) = 0_{\mathbb{K}[X]}$ allora posso scegliere $q(X) = 0_{\mathbb{K}[X]}$ e $r(X) = q(X) = 0_{\mathbb{K}[X]}$. Altrimenti procedo per induzione su $n := \deg g$.

CASO BASE Supponiamo $\deg g = 0$, ovvero $g(X) = g_0$. Abbiamo due casi:

- se $\deg f = 0$, ovvero $f(X) = f_0 \in \mathbb{K}$, allora

$$q(X) = g_0 {f_0}^{-1}, \quad r(X) = \mathbf{0};$$

- se $\deg f > \deg g$ allora

$$q(X) = \mathbf{0}, \; r(X) = g(X).$$

PASSO INDUTTIVO Sia $m \coloneqq \deg f$. Come nel caso base, se $\deg f > \deg g$ basta scegliere q uguale al polinomio nullo, $r(X) = g(X)$. Supponiamo invece che $\deg f \leqslant \deg g$. Possiamo scrivere i due polinomi come

$$f(X) = \sum_{i=0}^{m} a_i X^i, \; g(X) = \sum_{i=0}^{n} b_i X^i.$$

Sia $g_1 \in \mathbb{K}[X]$ il seguente polinomio:

$$\begin{aligned} g_1[X] &\coloneqq g(X) - \frac{b_n}{a_m} X^{n-m} f(X) \\ &= g(X) - b_n X^n + \dots \end{aligned}$$

dove i puntini indicano termini di grado inferiore al termine di grado massimo (ovvero n).
Il polinomio g_1 ha sicuramente grado inferiore al polinomio g, in quanto il termine di grado n (ovvero $b_n X^n$) è stato eliso.
Segue quindi per ipotesi induttiva che esistono $q_1, r_1 \in \mathbb{K}[X]$ tali che

$$g_1(X) = q_1(X) f(X) + r_1(X)$$

con $r_1 = 0_{\mathbb{K}[X]}$ oppure $0 \leqslant r_1 \leqslant \deg f$.
Dunque possiamo ricavare un'espressione per g dalla definizione di g_1:

$$\begin{aligned} g(X) &= g_1(X) + \frac{b_n}{a_m} x^{n-m} f(X) \\ &= q_1(X) f(X) + r_1(X) + \frac{b_n}{a_m} x^{n-m} f(X) \\ &= (q_1(X) + \frac{b_n}{a_m} x^{n-m}) f(X) + r_1(X). \end{aligned}$$

Dunque scegliendo $q(X) = q_1(X) + \frac{b_n}{a_m} x^{n-m}$ e $r(X) = r_1(X)$ otteniamo la divisione euclidea tra f e g.

□

Dimostrazione dell'unicità. Siano $q_1, r_1, q_2, r_2 \in \mathbb{K}[X]$ tali che

$$g(X) = q_1(X) f(X) + r_1(X) = q_2(X) f(X) + r_2(X)$$

con $r_1 = 0_{\mathbb{K}[X]}$ oppure $0 \leqslant \deg r_1 \leqslant \deg f$, $r_2 = 0_{\mathbb{K}[X]}$ oppure $0 \leqslant \deg r_2 \leqslant \deg f$.

Riarrangiando i termini otteniamo

$$(q_1(X) - q_2(X)) f(X) = r_2(X) - r_1(X). \tag{22}$$

Se $r_1 = r_2$ segue che $q_1 = q_2$ (per differenza), dunque supponiamo per assurdo $r_1 \neq r_2$.

Consideriamo i gradi dei polinomi contenuti nell'equazione (22):

$$\deg(r_2 - r_1) = \deg f + \deg(q_1 - q_2) \geqslant \deg f.$$

Ma il grado della differenza $r_2 - r_1$ è minore o uguale al grado dei polinomi r_1 e r_2, dunque non può essere maggiore del grado di f. Abbiamo quindi trovato un assurdo, da cui segue che $r_1 = r_2$. □

Teorema 2.2.14 **Teorema di Ruffini.** *Sia* $f \in \mathbb{K}[X]$ *un polinomio e sia* $\alpha \in \mathbb{K}$. *Allora*

$$f(\alpha) = 0 \iff (X - \alpha) \mid f(X). \tag{23}$$

Dimostrazione. Per il Teorema di Divisione Euclidea esisteranno $q, r \in \mathbb{K}[X]$ tali che

$$f(X) = (X - \alpha)q(X) + r(X),$$

con $r = 0_{\mathbb{K}[X]}$ oppure $0 \leqslant \deg r < \deg(X - \alpha)$.Siccome $\deg(X - \alpha) = 1$ segue che $\deg r = 0$, ovvero $r(X) = r_0$ per qualche $r_0 \in \mathbb{K}$. Valutando f in α otteniamo quindi

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r_0.$$

Allora $f(\alpha) = 0$ se e solo se $r_0 = 0$, ovvero se e solo se $(X - \alpha) \mid f$, cioè la tesi. □

Definizione 2.2.15 **Massimo comun divisore tra polinomi.** Siano $f, g \in \mathbb{K}[X]$ non entrambi nulli. Allora $d \in \mathbb{K}[X]$ è un *massimo comun divisore* di f e g se

(i) $d \mid f$, $d \mid g$;

(ii) se $h \mid f$, $h \mid g$ allora $h \mid d$.

Teorema 2.2.16 **Esistenza ed unicità del massimo comun divisore.** *Siano* $f, g \in \mathbb{K}[X]$ *non entrambi nulli. Allora*

- *esiste* $d \in \mathbb{K}[X]$ *tale che* d *è un massimo comun divisore di* f *e* g;
- *esistono* $a, b \in \mathbb{K}[X]$ *tali che* $d(X) = a(X)f(X) + b(X)g(X)$;
- *se* $d' \in \mathbb{K}[X]$ *è un altro massimo comun divisore di* f *e* g, *allora* d *e* d' *sono polinomi associati, ovvero esiste un* $\gamma \in A^{\times}$ *tale che* $d(X) = \gamma d'(X)$.

Anche nell'anello dei polinomi possiamo definire il concetto di *elemento primo* e *elemento irriducibile*.

Definizione 2.2.17 **Polinomio irriducibile.** Sia $f \in \mathbb{K}[X]$, $\deg f > 1$. Allora f si dice *irriducibile* in $\mathbb{K}[X]$ se

$$f(X) = g(X)h(X) \implies g \in \mathbb{K}[X]^{\times} \text{ oppure } h \in \mathbb{K}^{\times}.$$

Definizione 2.2.18 **Polinomio primo.** Sia $f \in \mathbb{K}[X]$, $\deg f > 1$. Allora f si dice *primo* in $\mathbb{K}[X]$ se

$$f(X) = g(X)h(X) \implies f \mid g \text{ oppure } f \mid h.$$

Nel caso particolare in cui il polinomio sia a coefficienti in un campo vale la stessa uguaglianza tra elementi primi e elementi irriducibili che sussiste in $\mathbb{Z}$:

Proposizione 2.2.19 **Un polinomio è primo se e solo se è irriducibile.** *Sia* $f \in \mathbb{K}[X]$, $\deg f > 1$. *Allora* f *è irriducibile se e solo se è primo.*

Dimostrazione. La dimostrazione è uguale alla dimostrazione della **??**. □

Teorema 2.2.20 **Teorema di fattorizzazione unica.** *Sia* $f \in \mathbb{K}[X]$, $\deg f > 1$. *Allora* f *si fattorizza in modo unico come prodotto di polinomi irriducibili, a meno di fattori invertibili e dell'ordine dei fattori.*

Corollario 2.2.21 *Sia* $f \in \mathbb{K}[X]$, $f \neq 0_{\mathbb{K}[X]}$. *Allora* f *ha al massimo* $\deg f$ *radici in* $\mathbb{K}$ *(contate con la loro molteplicità).*

2.3 FATTORIZZAZIONE DI POLINOMI

2.3.1 Fattorizzazione sui complessi

Teorema 2.3.1 **Teorema Fondamentale dell'Algebra.** *Sia* $f \in \mathbb{C}[X]$ *con* $\deg f \geqslant 1$. *Allora* f *ha almeno una radice in* $\mathbb{C}$.

Corollario 2.3.2 **Gli irriducibili sui complessi sono lineari.** *Sia* $f \in \mathbb{C}[X]$. *Allora* f *è irriducibile se e solo* $\deg f = 1$.

Dimostrazione. L'implicazione da destra verso sinistra è valida in ogni campo, dunque dimostriamo l'altra: sia $f \in \mathbb{C}[X]$ con $\deg f = n > 1$. Allora per il Teorema Fondamentale dell'Algebra esiste $\alpha \in \mathbb{C}$ tale che $f(\alpha) = 0$. Per il Teorema di Ruffini allora $X - \alpha \mid f(X)$, dunque $f(X) = (X - \alpha)g(X)$ per qualche $g \in \mathbb{C}[X]$. Da questa equazione segue che $\deg g = \deg f - 1 > 0$, dunque f è riducibile, da cui segue la tesi. □

Corollario 2.3.3 *Sia* $f(X) \in \mathbb{C}[X]$ *di grado* $\deg f \geqslant 1$. *Allora vale che* f *ha esattamente* $\deg f$ *radici complesse, ovvero* f *è fattorizzabile in esattamente* n *fattori lineari, contati con la loro molteplicità.*

Dimostrazione. In $\mathbb{C}[X]$ vale il Teorema di fattorizzazione unica; inoltre gli irriducibili di $\mathbb{C}[X]$ sono tutti e soli i polinomi di primo grado (per il corollario precedente): da ciò segue la tesi. □

2.3.2 Fattorizzazione sugli interi e sui razionali

Definizione 2.3.4 **Contenuto di un polinomio.** Sia $f \in \mathbb{Z}[X]$ tale che $f(X) \coloneqq \sum_{i=0}^{n} a_0 X^i$. Si dice *contenuto di* f il valore

$$c(f) \coloneqq \operatorname{mcd}(a_0, a_1, \dots, a_n).$$

Definizione 2.3.5 **Polinomio primitivo.** Sia $f \in \mathbb{Z}[X]$. Allora f si dice *primitivo* se $c(f) = 1$, ovvero se i suoi coefficienti non hanno fattori in comune.

Osservazione. Ogni polinomio a coefficienti interi può essere scritto come il prodotto del suo contenuto e di polinomio primitivo:

$$f(X) = c(f) \cdot f_1(X),$$

dove $f_1 \in \mathbb{Z}[X]$ è primitivo.

Il seguente Lemma ci permette di studiare la fattorizzazione su $\mathbb{Q}$ e su $\mathbb{Z}$ allo stesso modo.

Teorema 2.3.6 **Lemma di Gauss.** *Sia* $f \in \mathbb{Z}[X]$ *primitivo. Allora* f *è irriducibile in* $\mathbb{Z}[X]$ *se e solo se è irriducibile in* $\mathbb{Q}[X]$.

Proposizione 2.3.7 **Radici razionali di un polinomio a coefficienti interi.** *Sia* $f(X) \in \mathbb{Z}[X]$ *un polinomio a coefficienti interi tale che*

$$f(X) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

Sia $\frac{c}{d} \in \mathbb{Q}$ *ridotta ai minimi termini (ovvero* $(c, d) = 1$*).*
Allora se $\frac{c}{d}$ *è una radice di* f *segue che* $c \mid a_0$ *e* $d \mid a_n$*.*

Dimostrazione. Per definizione di radice di un polinomio

$$f\left(\frac{c}{d}\right) = a_0 + a_1\frac{c}{d} + \cdots + a_{n-1}\left(\frac{c}{d}\right)^{n-1} + a_n\left(\frac{c}{d}\right)^n = 0.$$

Moltiplicando entrambi i membri per d^n otteniamo

$$\iff a_0 d^n + a_1 c d^{n-1} + \cdots + a_{n-1} c^{n-1} d + a_n c^n = 0.$$

Se vale l'uguaglianza, allora i due membri saranno anche congrui modulo d:

$$a_0 d^n + a_1 c d^{n-1} + \cdots + a_{n-1} c^{n-1} d + a_n c^n \equiv 0 \pmod{d}.$$

$$\iff a_n c^n \equiv 0 \pmod{d}$$

Dato che $(c, d) = 1$, allora c^n è invertibile modulo d)

$$\begin{aligned} &\iff a_n \equiv 0 \pmod{d} \\ &\iff d \mid a_n. \end{aligned}$$

Consideriamo ora la congruenza modulo c:

$$a_0 d^n + a_1 c d^{n-1} + \cdots + a_{n-1} c^{n-1} d + a_n c^n \equiv 0 \pmod{c}.$$

$$\begin{aligned} &\iff a_0 d^n \equiv 0 \pmod{c} \\ &\iff a_0 \equiv 0 \pmod{c} \\ &\iff c \mid a_0. \end{aligned}$$

□

Un altro metodo per scomporre i polinomi a coefficienti interi è quello di sfruttare le congruenze. Sia $p \in \mathbb{Z}$ primo; chiamiamo *riduzione modulo* p la seguente funzione:

$$\begin{aligned} \pi_p : \mathbb{Z}[X] &\to \mathbb{Z}/_{p\mathbb{Z}}[X] \\ \sum_{i=0}^{n} a_i X^i &\mapsto \sum_{i=0}^{n} \overline{a_i} X^i. \end{aligned}$$

Si può verificare molto semplicemente che questa funzione è un omomorfismo di anelli; inoltre se $p \nmid a_n$ segue che $\deg f = \deg \pi_p f$.

Proposizione 2.3.8 **Criterio di riduzione.** *Sia* $p \in \mathbb{Z}$ *primo,* $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ *primitivo. Se*

- $p \nmid a_n$;
- $\pi_p f$ *è irriducibile in* $\mathbb{Z}/_{p\mathbb{Z}}$

allora f *è irriducibile in* $\mathbb{Z}[X]$ *e dunque in* $\mathbb{Q}[X]$.

Dimostrazione. Per dimostrare la proposizione è sufficiente mostrare la contronominale: se f è riducibile in $\mathbb{Z}[X]$ allora deve esserlo anche in $\mathbb{Z}/_{p\mathbb{Z}}[X]$ per qualunque p primo.

Siano $a, b \in \mathbb{Z}[X]$ di grado positivo tali che $f(X) = a(X)b(X)$: allora

$$\pi_p(f(X)) = \pi_p(a(X)b(X)) = \pi_p(a(X))\pi_p(b(X)),$$

dunque la riduzione modulo p del polinomio f è riducibile se e solo se $\pi_p(a(X))$ e $\pi_p(b(X))$ sono entrambi di grado positivo.

Per la Proposizione 2.2.8 sappiamo che $\deg f = \deg a + \deg b$. Inoltre siccome $p \nmid a_n$ segue che $\deg f = \deg \pi_p(f)$. Combinando i due risultati e sapendo che il grado della riduzione modulo p è minore o uguale al grado del polinomio originale:

$$\begin{aligned}\deg a + \deg b &= \deg f \\ &= \deg \pi_p(f) \\ &= \deg \pi_p(a) + \deg \pi_p(b) \\ &\leqslant \deg a + \deg \pi_p(b) \\ &\leqslant \deg a + \deg b.\end{aligned}$$

Dunque tutte le disuguaglianze sono uguaglianze e $\deg a = \deg \pi_p(a)$, $\deg b = \deg \pi_p(b)$. In particolare i grado delle riduzioni di a e di b sono positivi, da cui segue che $\pi_p(f)$ è riducibile. □

Proposizione 2.3.9 **Criterio di Eisenstein.** *Sia* $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$*. Se esiste un primo* $p \in \mathbb{Z}$ *tale che*

- $p \mid a_i$ *per ogni* $i = 0, \ldots, n-1$*;*
- $p \nmid a_n$*;*
- $p^2 \nmid a_0$

allora f *è irriducibile in* $\mathbb{Z}[x]$*.*

Dimostrazione. Supponiamo per assurdo che f sia riducibile in $\mathbb{Z}[X]$, ovvero che esistano due polinomi $g, h \in \mathbb{Z}[X]$ di grado positivo e tali che $f(X) = g(X)h(X)$. Sia $n := \deg f$, $m := \deg g \geqslant 1$; da ciò segue che $\deg h = n - m \leqslant 1$.

Siccome f è primitivo e $p \nmid a_n$ segue che

$$\pi_p(f(X)) = \pi_p(g(X))\pi_p(h(X))$$

e i gradi di $\pi_p(g)$, $\pi_p(h)$ sono uguali ai gradi di g e di h, rispettivamente.

Dal fatto che p divide tutti i coefficienti di f tranne a_n segue che

$$\pi_p(f(X)) = \overline{a_n}X^n.$$

Siccome in $\mathbb{Z}/_{p\mathbb{Z}}$ vale il Teorema di fattorizzazione unica (poiché $\mathbb{Z}/_{p\mathbb{Z}}$ è un campo) gli unici fattori di $\overline{a_n}X^n$ sono della forma X^k per qualche costante.

Da ciò segue che $\pi_p(g(X)) = \overline{b_n}X^m$, $\pi_p(h(X)) = \overline{c_n}X^m$, dove $\overline{b}\overline{c} = \overline{a_n}$. In particolare questo significa che i termini noti di g e di h (rispettivamente b_0 e c_0) devono essere divisibili per p, il che implica

$$p^2 \mid b_0 c_0 = a_0;$$

ma ciò è assurdo, dunque f è irriducibile. □

2.4 QUOZIENTI DI ANELLI POLINOMIALI

In questa sezione studieremo i quozienti di anelli polinomiali. Innanzitutto abbiamo bisogno di una nozione equivalente a quella di gruppo normale.

Definizione 2.4.1 **Ideale.** Sia A un anello commutativo. Allora $I \subseteq A$ si dice *ideale* se

1. $(I, +)$ è un sottogruppo di $(A, +)$;
2. vale la *proprietà di assorbimento*: per ogni $a \in A$, $x \in I$ vale che $ax \in I$.

Definizione 2.4.2 **Ideale generato da un elemento.** Sia A un anello commutativo e sia $r \in A$. Allora si dice *ideale generato da* r l'ideale

$$(a) \coloneqq \{ ra \ : \ a \in A \}.$$

Nel caso degli anelli polinomiali, come $\mathbb{K}[X]$, gli ideali generati da un polinomio f assumono la forma

$$\big(f(X)\big) = \{ f(X) \cdot a(X) \ : \ a \in \mathbb{K}[X] \}.$$

Siccome $\mathbb{K}[X]$ forma un gruppo abeliano con l'operazione di somma abbiamo automaticamente che $\big(f(X)\big) \lhd \mathbb{K}[X]$, dunque possiamo definire il gruppo quoziente

$$\mathbb{K}[X]/_{\big(f(X)\big)} \coloneqq \big\{ p(X) + \big(f(X)\big) \ : \ p(X) \in \mathbb{K}[X] \big\}.$$

Su questo gruppo è automaticamente definita un'operazione di somma

$$p(X) + \big(f(X)\big) + q(X) + \big(f(X)\big) = p(X) + q(X) + \big(f(X)\big);$$

tuttavia, possiamo anche definire un'operazione di prodotto tra classi laterali:

$$\Big(p(X) + \big(f(X)\big)\Big) \Big(q(X) + \big(f(X)\big)\Big) = p(X)q(X) + \big(f(X)\big).$$

Teorema 2.4.3 *La struttura* $\left(\mathbb{K}[X]/_{\big(f(X)\big)}, +, \cdot\right)$ *è un anello commutativo con identità.*

Dimostrazione. Basta verificare gli assiomi degli anelli. Lo zero dell'anello è dato da $\big(f(X)\big)$, mentre l'identità è data da $1 + \big(f(X)\big)$. □

Per semplicità definiamo $\overline{a(X)} \coloneqq a(X) + \big(f(X)\big)$, esattamente allo stesso modo come abbiamo fatto nel caso degli interi e le classi resto. Prima di dimostrare alcune proprietà importanti di questo anello, mostriamo il seguente lemma:

Lemma 2.4.4 *Siano* $f, r \in \mathbb{K}[X]$ *con* $r = 0_{\mathbb{K}[X]}$ *oppure* $\deg r < \deg f$. *Allora* $r \in \big(f(X)\big)$ *se e solo se* $r = 0_{\mathbb{K}[X]}$.

Dimostrazione. I polinomi di $\big(f(X)\big)$ sono tutti e solo i multipli di $f(X)$, dunque se non sono nulli hanno grado maggiore o uguale al grado di f, da cui segue che r deve essere il polinomio nullo. □

Teorema 2.4.5 *Sia* $f \in \mathbb{K}[X]$ *e sia* $n \coloneqq \deg f$. *Allora*

(i) un insieme minimale di rappresentanti dell'anello quoziente $\mathbb{K}[X]/_{\big(f(X)\big)}$ *è dato dall'insieme di tutti i possibili resti delle divisioni per* f, *ovvero da tutti e soli i polinomi* $r \in \mathbb{K}[X]$ *tali che* $r = 0_{\mathbb{K}[X]}$ *oppure* $0 \leqslant \deg r < n$;

(ii) l'anello quoziente è un $\mathbb{K}$*-spazio vettoriale di dimensione* n *e in particolare una sua base è data da*
$$\left(\overline{1}, \dots, \overline{X^{n-1}}\right).$$

Dimostrazione. Mostriamo innanzitutto che l'insieme dei possibili resti è un insieme di rappresentanti. Sia $a \in \mathbb{K}[X]$ un polinomio qualunque. Per il Teorema di Divisione Euclidea esisteranno due polinomi $q, r \in \mathbb{K}[X]$, con $r = 0_{\mathbb{K}[X]}$ oppure $0 \leqslant \deg r < n$ tali che

$$a(X) = q(X)f(X) + r(X).$$

Ma allora vale che

$$a(X) + \big(f(X)\big) = r(X) + \overbrace{q(X)f(X)}^{\in (f(X))} + \big(f(X)\big) = a(X) + \big(f(X)\big),$$

ovvero $\overline{a} = \overline{r}$.

Mostriamo inoltre che l'insieme dei resti è un insieme di rappresentanti minimale, ovvero che se due resti $r_1, r_2 \in \mathbb{K}[X]$ (con $\deg r_1 < n, \deg r_2 < n$) rappresentano la stessa classe di equivalenza, allora devono essere uguali.

$$\begin{aligned} & r_1(X) + \big(f(X)\big) = r_2 + \big(f(X)\big) \\ \iff & r_1(X) - r_2(X) \in \big(f(X)\big) && \text{(per il Lemma 2.4.4)} \\ \iff & r_1(X) - r_2(X) = 0_{\mathbb{K}[X]} \\ \iff & r_1(X) = r_2(X). \end{aligned}$$

Da questo segue direttamente che $\left(\overline{1}, \dots, \overline{X^{n-1}}\right)$ sono un insieme di generatori per $\mathbb{K}[X]/_{\left(f(X)\right)}$: infatti per ogni $\overline{a} \in \mathbb{K}[X]/_{\left(f(X)\right)}$ segue che esiste un polinomio r di grado minore di n tale che $\overline{a} = \overline{r}$. Siccome $\deg r < n$ esso può essere espresso come combinazione lineare di $\left(\overline{1}, \dots, \overline{X^{n-1}}\right)$, da cui segue che

$$\overline{a} = \overline{r} \in \operatorname{span}\left(\overline{1}, \dots, \overline{X^{n-1}}\right).$$

Inoltre questi vettori sono linearmente indipendenti. Per mostrarlo consideriamo una loro combinazione lineare e poniamola uguale a $\overline{0}$:

$$\sum_{i=0}^{n-1} a_i \overline{X^i} = \overline{0}.$$

Sia $\overline{r(X)} = \sum_{i=0}^{n-1} a_i \overline{X^i}$. Sicuramente $r = 0_{\mathbb{K}[X]}$ oppure $\deg r < n$, dunque per il Lemma 2.4.4 segue che $r = 0_{\mathbb{K}[X]}$, ovvero $a_1 = \dots = a_{n-1} = 0$, il che significa che i vettori $\overline{X^i}$ sono indipendenti e dunque formano una base dello spazio vettoriale. $\square$

Proposizione 2.4.6 **Divisori di zero e invertibili in** $\mathbb{K}[X]/_{\left(f(X)\right)}$. *Siano* $f \in \mathbb{K}[X]$, $\overline{a(X)} \in \mathbb{K}[X]/_{\left(f(X)\right)}$. *Allora*

(i) $\overline{a}$ *è invertibile se e solo se* $(a(x))f(x) = 1$;

(ii) $\overline{a}$ *è divisore di zero se e solo se* $(a(x))f(x) \neq 1$.

In particolare ogni elemento di $\mathbb{K}[X]/_{\left(f(X)\right)}$ *è invertibile oppure divisore di zero.*

Dimostrazione. Dimostriamo separatamente le due affermazioni.

(i) Il massimo comun divisore tra a e f è 1 se e solo se esistono due polinomi $h, k \in \mathbb{K}[X]$ tali che

$$a(X)h(X) + f(X)k(X) = 1.$$

Riducendo tutto modulo $\big(f(X)\big)$ otteniamo

$$\overline{a(X)h(X)} + \overline{f(X)k(X)} = \overline{1},$$

ma siccome $\overline{f(X)k(X)} = \overline{0}$ poiché $f(X)k(X) \in \big(f(X)\big)$

$$\begin{aligned} &\iff \overline{a(X)h(X)} = \overline{1} \\ &\iff \overline{a(X)} \cdot \overline{h(X)} = \overline{1}, \end{aligned}$$

ovvero se e solo se $\overline{a}$ è invertibile.

(ii) Supponiamo $(a(X))f(X) = d(X)$ con $\deg d \geqslant 1$. Sia $b(X) \coloneqq \frac{f(X)}{d(X)} \in \mathbb{K}[X]$ con $\deg b < \deg f$.
Sicuramente $\overline{b} \neq 0_{\mathbb{K}[X]}$, tuttavia $\overline{a(X)b(X)} = \overline{0}$ poiché

$$f(X) \mid a(X)b(X) = \frac{a(X)}{d(X)} f(X)$$

e $\frac{a(X)}{d(X)} \in \mathbb{K}[X]$ poiché d è un divisore di a.
Viceversa se $\overline{a}$ è divisore di zero allora dovrà esistere $\overline{b} \in \mathbb{K}[X]/_{\big(f(X)\big)}$, con $\overline{b} \neq \overline{0}$, tale che

$$\overline{a(X)b(X)} = \overline{0}.$$

Questo implica che $f(X) \mid a(X)b(X)$, ma siccome $f(X) \nmid b(X)$ (altrimenti b sarebbe nella classe di $0_{\mathbb{K}[X]}$) segue che $f(X) \mid a(X)$, ovvero $\overline{a} = \overline{0}$.

□

Corollario 2.4.7 *Sia $f \in \mathbb{K}[X]$. Allora vale che $\mathbb{K}[X]/_{\big(f(X)\big)}$ è un campo se e solo se f è irriducibile in $\mathbb{K}[X]$.*

Dimostrazione. Il quoziente $\mathbb{K}[X]/_{\big(f(X)\big)}$ è un campo se e solo se tutti i suoi elementi non nulli sono invertibili, ovvero (per la Proposizione 2.4.6) se e solo se per ogni polinomio $a \in \mathbb{K}[X]$ vale che $(a(X))f(X) = 1$, ovvero se e solo se f è irriducibile. □

2.5 ESTENSIONI DI CAMPI

Definizione 2.5.1 **Estensione di campi.** Siano K, F campi con $K \subseteq F$. Allora F si dice *estensione* di K e l'estensione si indica con F / K.

Definizione 2.5.2 **Elementi algebrici e trascendenti.** Sia F / K un'estensione di campi. $\alpha \in F$ si dice *algebrico su* K se esiste un polinomio $f \in \mathbb{K}[X] \setminus \left\{ 0_{\mathbb{K}[X]} \right\}$ tale che $f(\alpha) = 0$. Se α non è algebrico si dice *trascendente*.

Definizione 2.5.3 **Estensioni algebriche.** Sia F / K un'estensione di campi. F / K si dice *algebrica* se ogni $\alpha \in F$ è algebrico su K.

Dato un valore $\alpha \in F$ possiamo valutare tutti i polinomi di $K[X]$ in α per verificare il loro valore: l'immagine di questa funzione è l'insieme

$$K[\alpha] := \{ f(\alpha) \ : \ f \in K[X] \}.$$

Siccome $f(\alpha) \in F$ questo insieme è un sottoinsieme di F. In particolare essendo un sottoinsieme di un campo possiamo indurre due operazioni sugli elementi di $K[\alpha]$ (una somma e un prodotto) che si comportano esattamente come si comportano in F. Vale quindi la seguente proposizione.

Proposizione 2.5.4 *Sia F / K un'estensione di campi, $\alpha \in F$. Allora $(K[\alpha], +, \cdot)$ è un anello.*

La funzione che porta ogni elemento di $K[X]$ nella sua valutazione in α si dice *omomorfismo di valutazione*, ed è definito da

$$\begin{aligned} \varphi_\alpha : K[X] &\to K[\alpha] \subseteq F \\ f(X) &\mapsto f(\alpha). \end{aligned}$$

Esso è un omomorfismo tra l'anello dei polinomi $K[X]$ e l'anello $K[\alpha]$. Osserviamo inoltre che è un omomorfismo surgettivo, in quanto $K[\alpha] = \operatorname{Im} \varphi_\alpha$.

Proposizione 2.5.5 *Sia F / K un'estensione di campi, $\alpha \in F$. Allora vale che*

$$K[X]/_{\ker \varphi_\alpha} \simeq K[\alpha].$$

Dimostrazione. Consideriamo i gruppi additivi $K[X]$ e $K[\alpha]$ insieme all'omomorfismo φ_α e alla proiezione canonica sul quoziente. Per il Primo Teorema degli Omomorfismi vale che

$$\begin{tikzcd} K[X] \arrow[r, two heads, "\varphi_\alpha"] \arrow[d, hook, "\pi_{\ker \varphi_\alpha}"'] & K[\alpha] \\ K[X]/_{\ker \varphi_\alpha} \arrow[ur, hook, two heads, "\bar{\varphi}"'] & \end{tikzcd}$$

Innanzitutto osservo che

$$\varphi_\alpha(f(X)) = \left(\bar{\varphi} \circ \pi_{\ker \varphi_\alpha}\right)(f(X)) = \bar{\varphi}(f(X) + \ker \varphi_\alpha) = \bar{\varphi}([f(X)]).$$

Da questo possiamo verificare immediatamente che $\bar{\varphi}$ è un omomorfismo di anelli:

- $\bar{\varphi}([1]) = \varphi_\alpha(1) = 1$ poiché φ_α è un omomorfismo di anelli;
- $\bar{\varphi}([a(X)] \cdot [b(X)]) = \bar{\varphi}([a(X)]) \cdot \bar{\varphi}([b(X)])$ poiché:

$$\begin{aligned} \bar{\varphi}([a(X)] \cdot [b(X)]) &= \bar{\varphi}([a(X) \cdot b(X)]) \\ &= \varphi_\alpha(a(X) \cdot b(X)) \\ &= \varphi_\alpha(a(X)) \cdot \varphi_\alpha(b(X)) \\ &= \bar{\varphi}([a(X)]) \cdot \bar{\varphi}([b(X)]). \end{aligned}$$

Notiamo che non c'è bisogno di verificare che $\bar{\varphi}$ rispetti la struttura di gruppo additivo poiché sappiamo già che è un omomorfismo di gruppi.

Siccome il quoziente è sul nucleo di φ_α e φ_α è surgettiva segue che $\bar{\varphi}$ è bigettiva, dunque è un isomorfismo di anelli, da cui segue che la tesi. □

Osservazione. L'omomorfismo di valutazione ci consente di descrivere gli elementi algebrici e quelli trascendenti sfruttando le proprietà degli omomorfismi. Infatti

$$\ker \varphi_\alpha = \{ f(X) \in K[X] \,:\, \varphi_\alpha(f(X)) = f(\alpha) = 0 \}.$$

Dunque un elemento $\alpha \in F$ è algebrico su K se e solo se $\ker \varphi_\alpha \neq \{0\}$, ovvero se e solo se φ_α non è iniettivo.

In particolare se α è trascendente vale che $K[X]/_{\ker \varphi_\alpha} = K[X]$, dunque $K[\alpha] \simeq K[X]$.

2.5.1 Polinomio minimo di un elemento algebrico

Sia F/K un'estensione di campi e sia $\alpha \in F$ un elemento algebrico su K, ovvero $\ker \varphi_\alpha \neq \{0\}$. Notiamo che siccome $\ker \varphi_\alpha$ non è banale, esso contiene almeno un polinomio diverso dal polinomio nullo, dunque l'insieme dei gradi dei polinomi non nulli nel nucleo di φ_α è un sottoinsieme di $\mathbb{N}$ non vuoto, perciò ha minimo.

Proposizione 2.5.6 *Sia $\mu_\alpha \in \ker \varphi_\alpha$ un polinomio monico e di grado minimo tra i polinomi di $\ker \varphi_\alpha$. Allora valgono le seguenti affermazioni:*

(i) *μ_α è irriducibile in $K[X]$;*

(ii) *$\ker \varphi_\alpha = \big(\mu_\alpha(X)\big)$;*

(iii) *μ_α è l'unico polinomio monico irriducibile di $K[X]$ che si annulla in α.*

Dimostrazione. Dimostriamo le tre affermazioni separensatamente.

(i) Per ipotesi $\mu_\alpha(\alpha) = 0$. Supponiamo per assurdo che μ_α sia riducibile in $K[X]$, ovvero che esistano $a,\ b \in K[X]$ con $\deg a,\ \deg b < \deg \mu_\alpha$ tali che $\mu_\alpha(X) = a(X)b(X)$. Questo significa che

$$\mu_\alpha(\alpha) = a(\alpha)b(\alpha) = 0 \in F.$$

Siccome F è un campo vale la legge di annullamento del prodotto, dunque $a(\alpha) = 0$ oppure $b(\alpha) = 0$. Ma ciò è assurdo in quanto μ_α è di grado minimo tra i polinomi che si annullano in α, mentre a e b hanno grado minore. Dunque μ_α è irriducibile.

(ii) Per definizione l'ideale generato da μ_α è

$$\big(\mu_\alpha(X)\big) = \{ a(X)\mu_\alpha(X) \,:\, a(X) \in K[X].\}$$

Siccome $\mu_\alpha \in \ker \varphi_\alpha$ segue che $\big(\mu_\alpha(X)\big) \subseteq \ker \varphi_\alpha$: infatti per ogni $a(X) \in K[X]$ vale che

$$\begin{aligned} \varphi_\alpha(a(X)\mu_\alpha(X)) &= \varphi_\alpha(a(X))\varphi_\alpha(\mu_\alpha(X)) \\ &= a(\alpha)\mu_\alpha(\alpha) \\ &= 0. \end{aligned}$$

Sia ora $f \in \ker \varphi_\alpha$: dimostriamo che $f \in \big(\mu_\alpha\big)$. Per il Teorema di Divisione Euclidea esistono $q, r \in K[X]$ tali che

$$f(X) = q(X)\mu_\alpha(X) + r(X),$$

con $r = 0_{K[X]}$ oppure $\deg r < \deg f$.

Applicando l'omomorfismo di valutazione ad entrambi i membri otteniamo che

$$0 = f(\alpha) = q(\alpha)\mu_\alpha(\alpha) + r(\alpha) = r(\alpha),$$

dove la prima uguaglianza viene dal fatto che $f \in \ker \varphi_\alpha$, mentre l'ultima viene dal fatto che μ_α si annulla in α.
Da questo segue che r si annulla in α, ma ciò è possibile se e solo se $r = 0_{K[X]}$, in quanto altrimenti sarebbe un polinomio che si annulla in α di grado minore di μ_α. Dunque

$$f(X) = q(X)\mu_\alpha(X) \in (\mu_\alpha),$$

da cui segue che $\ker \varphi_\alpha = \mu_\alpha$.

(iii) Sia $f \in K[X]$ un polinomio che si annulla in α, monico e irriducibile: dimostriamo che $f = \mu_\alpha$.
Siccome per il punto precedente tutti i polinomi che si annullano in α sono nell'ideale generato da μ_α, segue che $f(X) = g(X)\mu_\alpha(X)$ per qualche $g \in K[X]$. Tuttavia se $\deg g \geqslant 1$ allora f sarebbe riducibile, dunque $\deg g = 0$, ovvero $g(X) = k_0$ per qualche $k_0 \in K^\times$. Ma f deve essere monico, e siccome μ_α è monico segue che $k_0 = 1$, da cui $f = \mu_\alpha$. □

Definizione 2.5.7 **Polinomio minimo.** Sia F / K un'estensione di campi, $\alpha \in F$ algebrico su K. L'unico polinomio monico e irriducibile di $K[X]$ che si annulla in α viene detto *polinomio minimo* di α su K.

Esempio 2.5.8. Data l'estensione $\mathbb{R} / \mathbb{Q}$, $\alpha = \sqrt[3]{2} \in \mathbb{R}$, vogliamo trovare il polinomio minimo $\mu_\alpha \in \mathbb{Q}[X]$.

Sicuramente $X^3 - 2 \in (\mu_\alpha(X))$ in quanto $\left(\sqrt[3]{2}\right)^3 - 2 = 0$, dunque $\mu_\alpha(X) \mid X^3 - 2$. Inoltre $X^3 - 2$ è monico ed irriducibile in $\mathbb{Q}[X]$, in quanto per il Criterio di Eisenstein (con $p = 2$) è irriducibile su $\mathbb{Z}$ e dunque per il Lemma di Gauss lo è su $\mathbb{Q}$. Da ciò segue che $\mu_\alpha(X) = X^3 - 2$.

Proposizione 2.5.9 *Sia F / K un'estensione di campi, $\alpha \in F$ algebrico su K e $\mu_\alpha \in \mathbb{K}[X]$ il polinomio minimo di α su K. Allora vale che*

$$K[\alpha] \simeq K[X]/_{(\mu_\alpha)}$$

e $K[\alpha]$ è un campo.

Dimostrazione. Siccome μ_α è irriducibile segue direttamente che il quoziente è un campo. Inoltre $K[\alpha]$ è isomorfo al quoziente per la Proposizione 2.5.5 e per il secondo punto della Proposizione 2.5.6. □

Osservazione. Sia $K(\alpha)$ l'insieme

$$K(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} \ : \ f,\ g \in K[X],\ g(\alpha) \neq 0 \right\}.$$

Se α è algebrico su K possiamo mostrare che $K[\alpha] = K(\alpha)$.
Infatti innanzitutto esiste un'inclusione canonica

$$\begin{aligned} K[\alpha] &\to K(\alpha) \\ f(\alpha) &\mapsto \frac{f(\alpha)}{1}. \end{aligned}$$

Inoltre per la proposizione precedente $K[\alpha]$ è un campo, dunque per ogni $g \in K[X]$ vale che $\frac{1}{g(\alpha)} \in K[\alpha]$, dunque per ogni $f \in K[X]$ vale che

$$f(\alpha) \cdot \frac{1}{g(\alpha)} \in K[\alpha],$$

da cui $K[\alpha] = K(\alpha)$.

Definizione 2.5.10 **Grado dell'estensione.** Sia F / K un'estensione di campi. Si dice *grado di* F / K il numero naturale

$$[F : K] \coloneqq \dim_K F.$$

Proposizione 2.5.11 *Sia* F / K *un'estensione di campi,* $\alpha \in F$. *Allora vale che*

$$\dim_K K[\alpha] = \begin{cases} +\infty, & \textit{se } \alpha \textit{ è trascendente su } K \\ \deg \mu_\alpha, & \textit{se } \alpha \textit{ è algebrico su } K. \end{cases}$$

Dimostrazione. Se α è trascendente allora $K[\alpha] \simeq K[X]$, dunque

$$[K[\alpha] : K] = [K[X] : K] = \dim_K K[X] = +\infty.$$

Invece se α è algebrico su K vale che $K[\alpha] \simeq K[X]/_{\left(\mu_\alpha(X)\right)}$, da cui segue che

$$[K[\alpha] : K] = [K[X]/_{\left(\mu_\alpha(X)\right)} : K] = \deg \mu_\alpha$$

per il secondo punto della Teorema 2.4.5. In particolare una K-base di $K[\alpha]$ può essere ottenuta sfruttando una K-base del quoziente e l'isomorfismo:

$$\left([1],\ [x], \ldots,\ [x^{n-1}]\right) \overset{\bar{\varphi}}{\longmapsto} \left(1,\ \alpha, \ldots,\ \alpha^{n-1}\right).$$

$\square$

Parte II

ALGEBRA I

3 | TEORIA DEI GRUPPI

3.1 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 3.1.1 **Gruppo generato da un suo sottoinsieme.** Sia G 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

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

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 $<S> \subseteq G$.

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

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

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 $<s> \leqslant G$ è un sottogruppo finito, e sarà della forma

$$<s> = \left\{ e_G, s, s^2, \dots, s^m \right\},$$

dove $m \coloneqq \mathrm{ord}_G(s)$. Siccome $<s>$ è un sottogruppo di G segue che $s^{-1} \in <s>$, 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 3.1.2. Mostriamo che $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} = <(1,0),(0,1)>$.

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 $<(1,0),(0,1)>$.

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

Esempio 3.1.3. Sappiamo già che $\mathbb{Z} = <1> = <-1>$. Mostriamo che $\mathbb{Z} = <2,3>$ e che $\{2,3\}$ è un insieme minimale di generatori.

È sufficiente mostrare che $\mathbb{Z} \subseteq <2,3>$, 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 $<2> = 2\mathbb{Z}$, $<3> = 3\mathbb{Z}$, dunque $\{2, 3\}$ è un insieme minimale di generatori.

Definizione 3.1.4 **Finitamente generato.** Sia G un gruppo. G si dice *finitamente generato* se G ammette un insieme finito di generatori.

Proposizione 3.1.5 *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

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

tale che $G = <S>$.

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

$$s_i = x_{1i} \dots x k_i i.$$

Segue quindi che

$$S = \{x_{11} \dots x k_1 1, \dots, x_{1n} \dots x k_n n\}.$$

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. □

3.2 GRUPPO DIEDRALE

Definizione 3.2.1 **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 3.2.2 **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 3.2.3 *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*:

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

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.

3.2.1 Sottogruppi del gruppo diedrale

Studiamo i sottogruppi del gruppo diedrale D_n.

Iniziamo studiando $< r >$: siccome $\mathrm{ord}(r) = n$ segue che $[D_n : < r >] = 2$, da cui per la Proposizione 1.6.13 segue che $< r > \triangleleft D_n$.

Tuttavia possiamo anche mostrare che per ogni $j = 0, \dots, n-1$ il gruppo $< r^j >$ è normale in D_n. Osserviamo inizialmente che $< r >$ 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 3.2.4 *$< r^{\frac{n}{d}} >$ è l'unico sottogruppo ciclico di D_n di ordine d per ogni $d > 2$.*

Dimostrazione. Innanzitutto $\mathrm{ord}(r^{\frac{n}{d}}) = d$ 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 $< r >$ di ordine d e gli elementi che non appartengono a $< r >$ hanno ordine 2 (sono simmetrie); da questo segue che è l'unico sottogruppo ciclico di ordine d di D_n. □

Proposizione 3.2.5 *Sia G 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 3.2.6 *Sia G un gruppo. Se H è l'unico sottogruppo ciclico di ordine d di G, allora $H \triangleleft G$.*

Dimostrazione. Se $H = < h >$ 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 $< r^{\frac{n}{d}} >$ è normale in D_n.

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

Proposizione 3.2.7

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

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
$$D_n = < r^{\frac{n}{2}} >. \qquad \square$$

Siccome il centro di un gruppo è sempre un sottogruppo normale di quel gruppo (per la Proposizione 1.6.11) segue che $< r^{n/2} >$ è un sottogruppo normale di D_n.

3.3 AUTOMORFISMI DI UN GRUPPO

Definizione 3.3.1 **Automorfismo.** Sia G un gruppo. Si dice *automorfismo di* G un isomorfismo da G in G. Inoltre si indica con $\mathrm{Aut}(G)$ l'insieme di tutti gli automorfismi di G.

Proposizione 3.3.2 **Gli automorfismi formano un gruppo.** *Sia* G *un gruppo. Allora* $(\mathrm{Aut}(G), \circ)$ *è un gruppo; in particolare* $\mathrm{Aut}(G) \leqslant \mathcal{S}(G)$.

Dimostrazione. Innanzitutto l'identità $\mathrm{id} : G \to G$ è un automorfismo di G, dunque $\mathrm{id} \in \mathrm{Aut}(G)$.

Sia φ un automorfismo di G: essendo un isomorfismo, esso ammette un inverso φ^{-1}. Siccome φ^{-1} è ancora un isomorfismo da G in G segue che φ^{-1} è un automorfismo di G.

Infine siano φ, ψ due automorfismi di G : allora la composizione $\varphi \circ \psi$ è ancora un automorfismo di G. Infatti la composizione è ancora un isomorfismo da G in G, dunque è un automorfismo.

Il fatto che Aut(G) è un sottogruppo di $\mathcal{S}(G)$ segue banalmente dal fatto che Aut(G) è contenuto nell'insieme delle bigezioni da G in G insieme con il fatto che Aut(G) è un gruppo con la stessa operazione di $\mathcal{S}G$. □

Definizione 3.3.3 Sia G un gruppo. Per ogni $g \in G$ definiamo

$$\begin{aligned} \varphi_g &: G \to G \\ g &\mapsto gxg^{-1}. \end{aligned}$$

Questa mappa viene chiamata *coniugio di* x *per* g.

Definizione 3.3.4 **Insieme degli automorfismi interni.** Sia G un gruppo. Si dice *insieme degli automorfismi interni* l'insieme

$$\mathrm{Inn}(G) := \{\, \varphi_g \;:\; g \in G \,\}.$$

Lemma 3.3.5 **Proprietà degli automorfismi interni.** *Siano* $g, h \in G$. *Allora valgono le seguenti due affermazioni:*

$$\varphi_g \circ \varphi_h = \varphi_{gh}. \tag{24}$$

$$(\varphi_g)^{-1} = \varphi_{g^{-1}}. \tag{25}$$

Proposizione 3.3.6 *Sia* G *un gruppo,* $g \in G$. *Allora il coniugio per* g *è un automorfismo di* G. *Inoltre vale che*

$$\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)..$$

Dimostrazione. Mostriamo innanzitutto che φ_g è ben definita: per ogni $x \in G$ segue che $\varphi_g(x) = gxg^{-1} \in G$.

OMOMORFISMO Dati $x, y \in G$ mostriamo che $\varphi_g(xy) = \varphi_g(x)\varphi_g(y)$.

$$\begin{aligned} \varphi_g(xy) = &= g(xy)g^{-1} \\ &= gx(gg^{-1})y \\ &= (gxg^{-1})(gyg^{-1}) \\ &= \varphi_g(x)\varphi_g(y). \end{aligned}$$

INIETTIVITÀ Siano $x, y \in G$: mostriamo che se $\varphi_g(x) = \varphi_g(y)$ allora $x = y$.

$$\begin{aligned} &\varphi_g(x) = \varphi_g(y) \\ \iff &gxg^{-1} = gyg^{-1} \\ \iff &x = y, \end{aligned}$$

dove l'ultimo passaggio è giustificato moltiplicando a sinistra per g^{-1} e a destra per g.

SURGETTIVITÀ Sia $y \in G$ qualunque; siccome $g^{-1}yg \in G$ e $\varphi_g(g^{-1}yg) = gg^{-1}ygg^{-1} = y$, segue che φ_g è surgettiva.

Segue quindi che φ_g è un isomorfismo, dunque un automorfismo di G.

Mostriamo ora che $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.

Innanzitutto l'insieme dei coniugi è un sottogruppo di Aut(G), in quanto

- $\mathrm{id} = \varphi_e \in \mathrm{Inn}(G)$;
- Per ogni coppia di automorfismi interni $\varphi_g, \varphi_h \in \mathrm{Inn}(g)$ segue che $\varphi_g \circ \varphi_h \in \mathrm{Inn}(G)$. Infatti

□

3.4 AZIONI DI GRUPPO

Definizione 3.4.1 **Azione di un gruppo su un insieme.** Sia G 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 $g \cdot x$ e x^g.

Esempio 3.4.2. 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 3.4.3. 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 $\varphi_\lambda(\boldsymbol{v}) = \lambda \cdot \boldsymbol{v}$ 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:

$$x \sim y \iff \exists g \in G \text{ tale che } \varphi_g(x) = y. \tag{26}$$

Proposizione 3.4.4 *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 (26) 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 3.4.5 **Orbita.** Sia G un gruppo che agisce sull'insieme X. Dato $x \in X$ si dice *orbita di* x l'insieme

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

OSSERVAZIONE. L'orbita di x è esattamente la classe di equivalenza data dalla relazione di equivalenza definita in (26). In particolare se R è un insieme di rappresentanti vale che

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

Definizione 3.4.6 **Stabilizzatore.** Sia G un gruppo che agisce sull'insieme X. Dato $x \in X$ si dice *stabilizzatore di* x l'insieme

$$\mathrm{Stab}_G(x) \coloneqq \{\, g \in G \;:\; \varphi_g(x) = x \,\} \subseteq G.$$

Proposizione 3.4.7 **Lo stabilizzatore è un sottogruppo.** *Sia* G *un gruppo che agisce sull'insieme* X*; sia inoltre* $x \in X$*. Allora vale che*

$$\mathrm{Stab}_G(x) \leqslant G.$$

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

Supponiamo che $g \in \mathrm{Stab}_G(x)$, ovvero $\varphi_g(x) = x$: mostriamo che anche $g^{-1} \in \mathrm{Stab}_G(x)$, ovvero $\varphi_{g^{-1}} \in \mathrm{Stab}_G(x)$. 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 $g^{-1} \in \mathrm{Stab}_G(x)$.

Supponiamo infine che $g, h \in \mathrm{Stab}_G(x)$ e mostriamo che $hg \in \mathrm{Stab}_G(x)$. 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 $\mathrm{Stab}_G(x)$ è un sottogruppo di G. □

Osservazione. Consideriamo un'azione generica φ di un gruppo G su un insieme X: sia $x \in X$ e siano $g, h \in G$ tali che $\varphi_g(x) = \varphi_h(x)$. Allora

$$\begin{aligned}&\varphi_g(x) = \varphi_h(x)\\ \iff &(\varphi_{h^{-1}} \circ \varphi_g)(x) = x\\ \iff &\varphi_{h^{-1}g}(x) = x\\ \iff &h^{-1}g = \mathrm{Stab}_G(x) \iff \qquad g\,\mathrm{Stab}_G(x) = h\,\mathrm{Stab}_G(x).\end{aligned}$$

Esiste dunque una bigezione tra l'orbita di un elemento $x \in X$ e le classi laterali di x in G:

$$\begin{aligned}\mathrm{orb}(x) &\leftrightarrow G/_{\mathrm{Stab}_G(x)}\\ \varphi_g(x) &\mapsto g\,\mathrm{Stab}_G(x).\end{aligned}$$

Questa corrispondenza è

BEN DEFINITA: se $\varphi_g(x) = \varphi_h(x)$ allora $g\,\mathrm{Stab}_G(x) = h\,\mathrm{Stab}_G(x)$;

INIETTIVA: se $g\,\mathrm{Stab}_G(x) = h\,\mathrm{Stab}_G(x)$ sicuramente $\varphi_g(x) = \varphi_h(x)$;

SURGETTIVA: le classi laterali di $\mathrm{Stab}_G(x)$ sono tutte e solo della forma $g\,\mathrm{Stab}_G(x)$ al variare di $g \in G$, e per ogni $g \in G$ segue che $\varphi_g(x) \in \mathrm{orb}(x)$.

Segue quindi la seguente proposizione.

Proposizione 3.4.8 **Lemma Orbita-Stabilizzatore.** *Sia* G *un gruppo che agisce su un insieme* X. *Se* G *è finito, allora per ogni* $x \in X$ *vale che*

$$|G| = |\mathrm{orb}(x)| \cdot |\mathrm{Stab}_G(x)|. \tag{27}$$

In particolare quindi $|\mathrm{orb}(x)|$ *divide* $|G|$.

Dimostrazione. Per la bigezione mostrata sopra, la cardinalità dell'orbita di x è uguale al numero di classi laterali di $\mathrm{Stab}_G(x)$ in G, ovvero

$$|\mathrm{orb}(x)| = [G : \mathrm{Stab}_G(x)] = \frac{|G|}{|\mathrm{Stab}_G(x)|},$$

da cui segue la tesi. □

Azione di coniugio

Sia G un gruppo che agisce su se stesso tramite l'azione di coniugio: ovvero

$$\begin{aligned}\varphi : G &\to \mathcal{S}(G)\\ g &\mapsto \varphi_g : G \to G\\ &\qquad\qquad x \mapsto gxg^{-1}.\end{aligned}$$

Abbiamo già osservato che questa è un'azione. Sia ora $x \in G$ qualunque. Allora l'orbita di x è data da

$$\begin{aligned} \operatorname{orb}(x) &= \{ \varphi_g(x) \ : \ g \in G \} \\ &= \{ gxg^{-1} \ : \ g \in G \} \\ &= \operatorname{Cl}(x), \end{aligned}$$

dove $\operatorname{Cl}(x)$ rappresenta la classe di coniugio di x.

Invece lo stabilizzatore di x in G è:

$$\begin{aligned} \operatorname{Stab}_G(x) &= \{ g \in G \ : \ \varphi_g(x) = x \} \\ &= \{ g \in G \ : \ gxg^{-1} = x \} \\ &= g \in Ggx = xg \\ &= Z_G(x), \end{aligned}$$

ovvero il centralizzatore di x in G.

Per il Lemma Orbita-Stabilizzatore, segue che, se G è finito:

$$|G| = |\operatorname{Cl}(x)| \cdot |Z_G(x)|,$$

ovvero $|\operatorname{Cl}(x)| \bigm| |G|$.

Osserviamo un'altra importante proprietà dei gruppi normali.

Proposizione 3.4.9 **I gruppi normali sono unione di classi di coniugio.** *Sia* G *un gruppo,* $H \leqslant G$. *Allora* $H \lhd G$ *se e solo se* H *è unione di intere classi di coniugio.*

Dimostrazione. Mostriamo entrambi i versi dell'implicazione.

($\implies$) Se $H \lhd G$ allora per ogni $g \in G$ vale che $gHg^{-1} \subseteq H$, ovvero per ogni $g \in G, h \in H$ vale che $ghg^{-1} \in H$, ovvero per ogni $h \in H$ vale che $\{ ghg^{-1} \ : \ g \in G \} = \operatorname{Cl}(h) \subseteq H$, ovvero H è unione di intere classi di coniugio.

($\impliedby$) Supponiamo H sia un sottogruppo di G dato dall'unione di intere classi di coniugio. Allora per ogni $h \in H$ segue che $\operatorname{Cl}(h) \in H$, ovvero per ogni $g \in G$ vale che $gHg^{-1} \subseteq H$, cioè $H \lhd G$. □

Coniugio di sottogruppi

Sia G un gruppo e X l'insieme di tutti i suoi sottogruppi. Definiamo la seguente azione di G su X:

$$\begin{aligned} \varphi : G &\to \mathcal{S}(X) \\ g &\mapsto \varphi_g : X \to X \\ &\qquad\qquad H \mapsto gHg^{-1}. \end{aligned}$$

Mostriamo innanzitutto che φ rappresenta effettivamente un'azione:

OMOMORFISMO Siano $g, h \in G$. Allora per ogni $H \in X$ vale che

$$\varphi_{gh}(H) = (gh)H(gh)^{-1} = g(hHh^{-1})g^{-1} = (\varphi_g \circ \varphi_h)(H).$$

BIGETTIVITÀ Sia $g \in G$ qualunque. Mostriamo che φ_g è una bigezione e $\varphi_{g^{-1}}$ è la sua inversa: per ogni $H \in X$ vale che

$$(\varphi_{g^{-1}} \circ \varphi_g)(H) = \varphi_{g^{-1}}(gHg^{-1}) = g^{-1}gHg^{-1}g = H.$$
$$(\varphi_g \circ \varphi_{g^{-1}})(H) = \varphi_g(g^{-1}Hg) = gg^{-1}Hgg^{-1} = H.$$

Segue quindi che φ è un'azione di G sui suoi sottogruppi. Sia $H \leqslant G$. L'orbita di H rispetto a questa azione è

$$\operatorname{orb}(H) = \{ \varphi_g(H) \,:\, g \in G \} = \{ gHg^{-1} \,:\, g \in G \},$$

ovvero è l'insieme dei sottogruppi di G coniugati ad H. Invece lo stabilizzatore di H è

$$\operatorname{Stab}_G(H) = \{ g \in G \,:\, \varphi_g(H) = H \} = \{ g \in G \,:\, gHg^{-1} = H \} = N_G(H),$$

ovvero è il normalizzatore del sottogruppo H in G.

Osserviamo che, per il Lemma Orbita-Stabilizzatore, il numero di coniugati di H è dato da

$$|\operatorname{orb}(H)| = \frac{|G|}{|N_G(H)|}$$

Proposizione 3.4.10 *Sia G un gruppo e $H \leqslant G$. Consideriamo l'azione di G sull'insieme dei suoi sottogruppi data dal coniugio. Le seguenti affermazioni sono equivalenti:*

(i) $H \triangleleft G$.

(ii) $\operatorname{orb}(H) = \{ H \}$.

(iii) $\operatorname{Stab}_G(H) = G$.

Dimostrazione. Dimostriamo la catena di implicazioni

$$(i) \implies (ii) \implies (iii) \implies (i).$$

((i) $\implies$ (ii)) Se $H \triangleleft G$ allora $gHg^{-1} = H$ per ogni $g \in G$, da cui $\operatorname{orb}(H) = \{ H \}$.

((ii) $\implies$ (iii)) Supponiamo che

$$\operatorname{orb}(H) = \{ gHg^{-1} \,:\, g \in G \} = \{ H \}.$$

Questo significa che per ogni $g \in G$ vale che $gHg^{-1} = H$, da cui $\operatorname{Stab}_G(H) = G$.

((iii) $\implies$ (i)) Supponiamo $\operatorname{Stab}_G(H) = G$. Allora per ogni $g \in G$ vale che $gHg^{-1} = H$, da cui $H \triangleleft G$.

$\square$

3.4.1 Formula delle classi

Sia G un gruppo; consideriamo l'azione φ di G su se stesso data dal coniugio.

Ricordiamo che, dato $x \in G$, la classe di coniugio di x mediante φ è

$$\operatorname{Cl}(x) := \operatorname{orb}(x) = \{ \varphi_g(x) \,:\, g \in G \} = \{ gxg^{-1} \,:\, g \in G \}.$$

Sicuramente $x \in \operatorname{orb}(x)$ in quanto $x = \varphi_{e_G}(x)$; inoltre possiamo notare che $\operatorname{Cl}(x) = \{ x \}$ se e solo se per ogni $g \in G$ vale che $gxg^{-1} = x$, ovvero x è un elemento del centro di G.

Più in generale se G è finito vale il Lemma Orbita-Stabilizzatore, da cui $|G| = |\operatorname{Cl}(x)| \cdot |Z_G(x)|$. Allora vale che $\operatorname{Cl}(x) = \{ x \}$ se e solo se $|\operatorname{Cl}(x)| = 1$, da cui $|G| = |Z_G(x)|$, ovvero $G = Z_G(x)$ (poiché G è finito), da cui $x \in Z(G)$.

Siccome le classi di coniugio formano le classi di equivalenza della relazione data dall'azione di coniugio, dato un insieme di rappresentanti R segue che

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

Se G è finito, passando alle cardinalità si ottiene

$$|G| = \sum_{x \in R} |*|Cl(x).$$

Siccome abbiamo notato prima che gli elementi del centro formano classi di coniugio con un solo elemento possiamo separarle dalle altre, ottenendo

$$\begin{aligned} |G| &= \sum_{x \in R} |*|Cl(x) \\ &= \sum_{x \in Z(G)} |*|Cl(x) + \sum_{x \in R \setminus Z(G)} |*|Cl(x) \\ &= \sum_{x \in Z(G)} 1 + \sum_{x \in R \setminus Z(G)} \frac{|*|G}{|*|Z_G(x)} \\ &= |*|Z(G) + \sum_{x \in R \setminus Z(G)} \frac{|*|G}{|*|Z_G(x)}. \end{aligned}$$

Vale quindi la seguente formula.

Teorema 3.4.11 **Formula delle classi.** *Sia* G *un gruppo finito e sia* R *un insieme di rappresentanti delle classi di coniugio di* G*. Allora*

$$|*|G = |*|Z(G) + \sum_{x \in R \setminus Z(G)} \frac{|*|G}{|*|Z_G(x)}. \tag{28}$$

Osserviamo che la formula delle classi non vale solo per G, ma anche per tutti i sottogruppi normali di G. Infatti per la Proposizione 3.4.9 segue che

$$H = \bigcup_{x \in R \cap H} Cl(x),$$

dunque se H è finito si ha

$$\begin{aligned} |*|H &= \sum_{x \in R \cap H} Cl(x) \\ &= \sum_{x \in Z(G) \cap H} 1 + \sum_{x \in (R \setminus Z(G)) \cap H} Cl(x) \\ &= |*|Z(G) \cap H + \sum_{x \in (R \setminus Z(G)) \cap H} Cl(x). \end{aligned}$$

3.4.2 p-Gruppi

Definizione 3.4.12 Sia $p \in \mathbb{Z}$ primo. Si dice p-*gruppo* un gruppo finito di ordine p^k per qualche $k \in \mathbb{N}$.

Proposizione 3.4.13 **Il centro di un p-gruppo è non banale.** *Sia* G *un* p*-gruppo di ordine* p^n*. Allora* $Z(G) \neq \{e_G\}$*.*

Dimostrazione. Per la formula delle classi vale che

$$p^n = |*|G = |*|Z(G) + \sum_{x \in R \setminus Z(G)} \frac{|*|G}{|*|Z_G(x)}.$$

Notiamo che se $x \in R \setminus Z(G)$ allora $Cl(x) = \dfrac{|*|G}{|*|Z_G(x)} > 1$, in quanto le uniche classi di coniugio formate da un singolo elemento sono date dagli elementi del centro di G. Segue quindi che per ogni $x \in R \setminus Z(G)$ vale che

$$p \mid \frac{|*|G}{|*|Z_G(x)},$$

da cui p divide la somma di questi rapporti.

Per differenza segue dunque che $p \mid |*|Z(G)$, da cui $Z(G)$ è non banale. $\square$

Proposizione 3.4.14 *Un gruppo di ordine p^2 è necessariamente abeliano.*

Dimostrazione. Sia G un gruppo di ordine p^2: siccome è un p-gruppo per la Proposizione 3.4.13 il centro di G è non banale, da cui $Z(G)$ ha ordine p o p^2.

Se per assurdo $Z(G)$ avesse ordine p allora $G/_{Z(G)}$ ha ordine p, ovvero è ciclico. Tuttavia questo (per la Proposizione 1.6.20) implica che G è abeliano, il che è assurdo in quanto abbiamo assunto che il suo centro fosse diverso dall'intero gruppo.

Segue quindi che $|*|Z(G) = p^2$, ovvero $G = Z(G)$ da cui G è abeliano. $\square$

3.5 PRESENTAZIONI DI GRUPPO

Abbiamo visto studiando il gruppo diedrale D_n che se vogliamo esprimere un gruppo in termini dei suoi generatori è necessario esplicitare anche quali condizioni devono essere rispettate dai generatori: se non lo facessimo, il gruppo non sarebbe necessariamente univoco. Per formalizzare il concetto di *presentazione* abbiamo bisogno di alcune definizioni iniziali.

Definizione 3.5.1 **Gruppo libero su un insieme.** Sia $X = \{x_1, x_2, \dots\}$ un insieme di simboli e poniamo $X^{-1} := \left\{x_1^{-1}, x_2^{-1}, \dots\right\}$ l'insieme dei loro inversi formali.

Poniamo $\mathcal{L} := X \cup X^{-1}$; una *parola* è un elemento di

$$\bigcup_{n \geqslant 0} \mathcal{L}^n;$$

ovvero è sequenza finita (ma arbitrariamente lunga) di elementi di $\mathcal{L}$.

Una parola si dice *ridotta* se non contiene consecutivamente i simboli x_i e x_i^{-1} (o viceversa).

Un gruppo $G \supseteq X$ si dice *libero su* X se G è generato da X e tutte le parole ridotte rappresentano elementi diversi di G.

Osservazione. Se $X = \{x\}$ allora le parole ridotte sono delle seguenti forme:

- la parola è vuota;
- la parola è della forma $xxx\dots x$, che può essere rappresentata con x^n (dove n è la lunghezza della sequenza);
- la parola è della forma $x^{-1}x^{-1}x^{-1}\dots x^{-1}$, che può essere rappresentata con x^{-n} (dove n è la lunghezza della sequenza).

Quindi G è libero su X se e solo se le parole sono tutte delle tre forme precedenti; dunque G deve essere isomorfo a $\mathbb{Z}$: questo ci mostra che $\mathbb{Z}$ è un gruppo libero sull'insieme $X = \{1\}$.

Avevamo già osservato che se H è un gruppo qualsiasi, allora esiste una bigezione tra gli elementi di H e gli omomorfismi $\mathbb{Z} \to H$: questa bigezione è data da

$$\begin{aligned} \mathrm{Hom}(\mathbb{Z}, H) &\leftrightarrow H \\ (n \mapsto h^n) &\leftarrow\!\shortmid h. \end{aligned}$$

Questa osservazione può essere estesa ai gruppi liberi con più generatori: se G è libero su X e H è un gruppo qualunque allora esiste una bigezione tra gli omomorfismi $G \to H$ e le funzioni $X \to H$, dato da

$$\begin{aligned} \mathrm{Hom}(G, H) &\longleftrightarrow \{ f : X \to H \} \\ (x_{i_1}^{\pm 1} \cdots x_{i_k}^{\pm 1} \mapsto h_{i_1}^{\pm 1} \cdots h_{i_k}^{\pm 1}) &\leftarrow\!\shortmid \begin{pmatrix} x_1 \mapsto h_1 \\ x_2 \mapsto h_2 \\ \vdots \end{pmatrix} \end{aligned}$$

Le funzioni $X \to H$ ci dicono dove vengono mappati i generatori (ovvero gli elementi di X): questo determina univocamente un omomorfismo da G in H che mappa ogni parola in modo da rispettare la mappa $X \to H$.

COSTRUZIONE DELLA PRESENTAZIONE DI UN GRUPPO Consideriamo ora un gruppo H generato da $g_1, \dots, g_n$. Per l'osservazione precedente deve esistere un omomorfismo