Algebra

Luca De Paulis

30 aprile 2021

Indice

1

Gruppi

1.1 INTRODUZIONE AI GRUPPI

Definizione 1.1.1 – Gruppo

Sia $G \neq \emptyset$ un insieme e sia $*$ un'operazione su G, ovvero

$$\begin{aligned} * : G \times G &\to G \\ (a, b) &\mapsto a * b. \end{aligned} \tag{1.1}$$

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 $*$, ovvero per ogni $a \in G$ vale che

$$a * e_G = e_G * a = a.$$

(G3) Ogni elemento di G è *invertibile* rispetto all'operazione $*$, ovvero 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

(G1) l'operazione $*$ è commutativa, ovvero per ogni $a, b \in G$ vale che

$$a * b = b * a.$$

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 per ogni $a, b, c \in G$ si ha 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 un $-a \in G$ tale che

$$a + (-a) = (-a) + a = e_G.$$

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

(G4) l'operazione $+$ è commutativa, ovvero per ogni $a, b \in G$ vale che

$$a + b = b + a.$$

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. La struttura $(\mu_n, \cdot)$ dove

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

è un gruppo, detto **gruppo delle radici n-esime dell'unità**.

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 $xy \in \mu_n$;

(G0) $\cdot$ è associativa in $\mathbb{C}$, dunque lo è in $\mu_n \subseteq \mathbb{C}$;

(G0) $1 \in \mathbb{C}$ è l'elemento neutro di $\cdot$ e $1 \in \mu_n$ in quanto $1^n = 1$;

(G0) 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 $x^{-1} \in \mu_n$;

(G0) inoltre $\cdot$ è commutativa in $\mathbb{C}$, dunque lo è anche in μ_n.

Da ciò segue che μ_n è un gruppo abeliano. □

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

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

è un gruppo abeliano.

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

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

è un gruppo abeliano.

Dimostrazione. Infatti

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

(G0) $\cdot$ è associativa in $\mathbb{Z}/n\mathbb{Z}$, dunque lo è in $\mathbb{Z}/n\mathbb{Z}^\times \subseteq \mathbb{Z}/n\mathbb{Z}$;

(G0) $1 \in \mathbb{Z}/n\mathbb{Z}$ è l'elemento neutro di $\cdot$ e $1 \in \mathbb{Z}/n\mathbb{Z}^\times$ in quanto 1 è invertibile e il suo inverso è 1;

(G0) ogni elemento di $\mathbb{Z}/n\mathbb{Z}^\times$ ammette inverso per definizione;

(G0) inoltre $\cdot$ è commutativa in $\mathbb{Z}/n\mathbb{Z}$, dunque lo è in $\mathbb{Z}/n\mathbb{Z}^\times \subseteq \mathbb{Z}/n\mathbb{Z}$.

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

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

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

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

Dimostrazione. Infatti

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

(G0) l'operazione di composizione di funzioni è associativa;

(G0) la funzione

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

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

(G0) 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. Valgono le seguenti affermazioni.

(i) L'elemento neutro di G è unico.

(ii) Per ogni $g \in G$, l'inverso di g è unico.

(iii) Per ogni $g \in G$ vale che $\left(g^{-1}\right)^{-1} = g$.

(iv) Per ogni $h, g \in G$ vale che $(hg^{-1})^{-1} = g^{-1}h^{-1}$.

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

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

Dimostrazione. Dimostriamo le varie affermazioni separatamente.

(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 il punto precedente l'inverso è unico e quindi $(g^{-1})^{-1} = g$.

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

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

(v) Legge di cancellazione sinistra:

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

Legge di cancellazione destra:

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

1.2 SOTTOGRUPPI

Definizione 1.2.1 – Sottogruppo

Sia $(G, *)$ un gruppo e sia $H \neq \varnothing$. Allora H insieme ad un'operazione $*_H$ si dice *sottogruppo* di $(G, *)$ se $(H, *_H)$ è un gruppo.

Si scrive $H \leq G$ se l'operazione $*_H$ è l'operazione $*$, ovvero l'operazione del sottogruppo è indotta da 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 $H \leq G$ se e solo se

(i) $*$ è un'operazione su H, ovvero per ogni $a, b \in H$ vale che $a * b \in H$;

(ii) ogni elemento di H è invertibile (in H), ovvero per ogni $h \in H$ vale che $h^{-1} \in H$.

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

$\boxed{\implies}$ Ovvio in quanto se $H \leq G$ allora H è un gruppo.

$\boxed{\impliedby}$ 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 $h \in H$. Siccome H è chiuso per inversi (ipotesi (ii)) dovrà esistere anche $h^{-1} \in H$, mentre dal fatto che H è chiuso per prodotti (ipotesi (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. $\square$

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) $Z(G) \leq G$;

(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 $Z(G) \neq \emptyset$ 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 $g * (x * y) = (x * y) * g$.

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

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

Per ipotesi

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

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

Per la Proposizione 1.2.2 segue che $Z(G) \leq G$.

$Z(G) = G$ se e solo se G abeliano

Dimostriamo entrambi i versi dell'implicazione.

$\boxed{\implies}$ Ovvia: $Z(G)$ è un gruppo abeliano, dunque se $G = Z(G)$ allora G è abeliano.

$\boxed{\impliedby}$ 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 $\mathbb{Z}$

Per ogni $n \in \mathbb{Z}$ vale che $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

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

(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 $n\mathbb{Z} \leq \mathbb{Z}$, ovvero la tesi. □

Corollario 1.2.7

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

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

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

Dimostrazione. Dimostriamo le due affermazioni separatamente.

(1) Dimostriamo entrambi i versi dell'implicazione.

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

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

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

$$\implies m \mid n.$$

$\boxed{\Longleftarrow}$ 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.

(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 il punto precedente $m \mid n$ e $n \mid m$, ovvero n e m sono uguali a meno del segno. □

Proposizione 1.2.8 – Intersezione di sottogruppi è un sottogruppo

Sia $(G, \cdot)$ un gruppo e siano $H, K \leq G$. Allora $H \cap K \leq G$.

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 $H \cap K \leq G$. □

1.3 GENERATORI E GRUPPI CICLICI

Innanzitutto diamo una definizione generale di potenze:

Definizione 1.3.1 – Potenze intere

Sia $(G, \cdot)$ un gruppo e sia $g \in G$ qualsiasi.
Allora definiamo g^k per $k \in \mathbb{Z}$ nel seguente modo:

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

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

Più 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 $g \in G$. Si dice *sottogruppo generato da* g l'insieme

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

Proposizione 1.3.3 – Il sottogruppo generato è un sottogruppo abeliano

Sia $(G, \cdot)$ un gruppo e sia $g \in G$ qualsiasi. Allora $< g > \leq G$. Inoltre $< g >$ è abeliano.

Dimostrazione. Innanzitutto notiamo che $< g > \neq \emptyset$ 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 $< g > \leq G$.
Inoltre notiamo che dati $g^n, g^m \in < g >$ qualsiasi si ha

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

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

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

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

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

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 $\mathrm{ord}_G(x) = d < +\infty$. Valgono i seguenti due fatti:

(i) Il sottogruppo generato $< x >$ è

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

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

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

Dimostrazione. Dimostriamo le due affermazioni separatamente.

▸ PARTE 1 Sicuramente vale che

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

Dimostriamo che vale l'uguaglianza.

Sia $k \in \mathbb{Z}$ qualsiasi. Allora $x^k \in < x >$.

Dimostriamo che necessariamente $x^k \in \{e, x, \dots, x^{d-1}\}$.

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

$$k = qd + r$$

con $0 \leq r < d$. 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 $0 \leq r < d$, dunque $x^r \in \{e, x, \dots, x^{d-1}\}$. Dato che $x^r = x^k$ concludiamo che

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

e quindi

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

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 $0 \leq a < b < d$ (senza perdita di generalità) tali che $x^a = x^b$.

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

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

▸ PARTE 2. Dimostriamo entrambi i versi dell'implicazione.

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

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

$$n = qd + r$$

con $0 \leq r < d$.

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 $d \mid n$.

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

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

□

Definizione 1.3.6 – Gruppo ciclico

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

$$G = < g >.$$

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 $g \in G$ e sia $H \leq G$ un suo sottogruppo. Allora H è ciclico, ovvero esiste $h \in \mathbb{Z}$ tale che $H = \left\langle g^h \right\rangle$.

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 se $g^k \in H$ allora $g^{-k} \in H$ possiamo supporre senza perdita di generalità $k > 0$.

Consideriamo l'insieme S tale che

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

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

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

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

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

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

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

$$n = q h_0 + r$$

con $0 \leq r < h_0$. Dunque dovrà valere che

$$\begin{aligned} g^n &= g^{q h_0 + r} \\ &= g^{q h_0} g^r. \end{aligned}$$

Moltiplicando entrambi i membri per $g^{-q h_0}$ otteniamo

$$\iff g^n g^{-q h_0} = g^r.$$

Ma $g^n \in H$ e $g^{-q h_0} \in H$ (in quanto è una potenza intera di g^{h_0}), dunque anche il loro prodotto $g^n g^{-q h_0} = g^r$ dovrà essere un elemento di 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 $n = q h_0$, ovvero che $g^n \in \left\langle g^{h_0} \right\rangle$, ovvero $H \subseteq \left\langle g^{h_0} \right\rangle$.

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

Consideriamo i sottogruppi di $\mathbb{Z}$. Tramite la Proposizione 1.2.6 abbiamo dimostrato che per ogni $n \in \mathbb{Z}$ segue che $n\mathbb{Z} \leq \mathbb{Z}$. 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 $n\mathbb{Z} \leq \mathbb{Z}$ 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 $<n> = n\mathbb{Z}$ per qualche $n \in \mathbb{Z}$.

Per la Voce (2) sappiamo che $n\mathbb{Z} = (-n)\mathbb{Z}$, dunque possiamo considerare (senza perdita di generalità) n positivo o nullo, ovvero $n \in \mathbb{N}$.

Segue quindi che 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 dato da da

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

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

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

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

$$\left|\mathbb{Z}/n\mathbb{Z}\right| = \left|\overline{1}\right| = \operatorname{ord}(\overline{1}) = n. \tag{1.2}$$

Proposizione 1.3.9 – Ordine degli elementi di $\mathbb{Z}/n\mathbb{Z}$

Sia $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ qualsiasi. Allora vale che

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

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

Dimostrazione. Per definizione di ordine

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

Si tratta quindi di trovare la minima soluzione positiva di $ax \equiv 0 \ (n)$. Dividendo 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 $t \in \mathbb{Z}$.

La minima soluzione positiva è ottenuta per $t = 1$, da cui segue che

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

□

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 $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ vale che $\operatorname{ord}(\overline{a}) \mid n$.

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

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

Dimostrazione. Dimostriamo separatamente le tre affermazioni.

(i) Ovvia in quanto (per la Proposizione 1.3.9)

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

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

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

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

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

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

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

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

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

Sia $b \in \mathbb{Z}$ tale che $a = n/d\, b$. Dato che $(n, a) = n/d$ 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 $\phi(d)$ scelte per b, ovvero esistono $\phi(d)$ elementi di ordine d.

□

Questo corollario ci consente di enunciare una proprietà della funzione ϕ.

Corollario 1.3.11 – Espressione per n in termini della funzione di Eulero

Sia $n \in \mathbb{Z}$. Allora vale che

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

Dimostrazione. Sia X_d l'insieme

$$X_d := \left\{ \overline{a} \in \mathbb{Z}/n\mathbb{Z} \ : \ \mathrm{ord}(\overline{a}) = d \right\}.$$

Se $d \nmid n$ per il Corollario 1.3.10 (in particolare per il primo punto) segue che $X_d = \varnothing$.
Si ha quindi che

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

Per il Corollario 1.3.10 (in particolare per il terzo punto) sappiamo che $|X_d| = \phi(d)$, dunque passando alle cardinalità segue che

$$\left|\mathbb{Z}/n\mathbb{Z}\right| = n = \sum_{d \mid n} X_d. \qquad \square$$

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 $H \leq \mathbb{Z}/n\mathbb{Z}$. Allora H è ciclico e $|H| = d$ per qualche $d \mid n$.

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

Dimostrazione. Dimostriamo separatamente le due affermazioni.

(i) Sia $H \leq \mathbb{Z}/n\mathbb{Z}$; per il Teorema 1.3.7 sappiamo che H deve essere ciclico, ovvero $H = \left\langle \overline{h} \right\rangle$ per qualche $\overline{h} \in \mathbb{Z}/n\mathbb{Z}$.

Sia $d = \mathrm{ord}(\overline{h})$. Allora per il Corollario 1.3.10 (in particolare per il primo punto) segue che

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

(ii) Sia H_d l'insieme

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

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

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

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

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 $H \leq \mathbb{Z}/n\mathbb{Z}$ tale che $|H| = d$. Per il Teorema 1.3.7 segue che $H = \langle \overline{x} \rangle$ per qualche $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ tale che $\text{ord}(\overline{x}) = d$.

Seguendo la dimostrazione del terzo punto del Corollario 1.3.10 possiamo scrivere $\overline{x} = \overline{\frac{n}{d}b}$ con $b \in z\mathbb{Z}$ tale che $(b, d) = 1$.

Ma $H_d = \left\langle \overline{\frac{n}{d}} \right\rangle$ contiene tutti i multipli di $\overline{\frac{n}{d}}$, dunque deve contenere anche $\overline{x}$.

Dunque dato che $\overline{x} \in H_d$ segue che $H = \langle \overline{x} \rangle \subseteq H_d$. Ma gli insiemi H e H_d hanno la stessa cardinalità, dunque $H = H_d$, ovvero vi è un solo sottogruppo di ordine d. □

1.4 OMOMORFISMI DI GRUPPI

Definizione 1.4.1 – Omomorfismo tra gruppi

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

$$f : G_1 \to G_2$$

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

$$f(x * y) = f(x) \star f(y). \tag{1.3}$$

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

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 $H \leq G_1$, $K \leq G_2$. 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 $H \leq G_1$ vale che $f(H) \leq G_2$;

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

(v) $f(G_1) \leq G_2$ e $\ker f \leq G_1$;

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

Dimostrazione. Dimostriamo le varie proprietà separatamente.

(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 (v) otteniamo

$$e_2 = f(e_1).$$

(ii) Sfruttando il punto Voce (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 $H \leq G_1$. Dato che $H \neq \emptyset$ 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

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

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

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

Dunque $f(H) \leq G_2$.

(iv) Sia $K \leq G_2$. Dato che $e_2 \in K$, sicuramente $f^{-1}(K) \neq \emptyset$, in quanto $e_1 = f^{-1}(e_2) \in f^{-1}(K)$.
Dunque per la proposizione 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

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

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

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

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

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

(vi) Dimostriamo entrambi i versi dell'implicazione.

$\boxed{\implies}$ 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 $\ker f = \{e_1\}$.

$\boxed{\impliedby}$ 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

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

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

□

Proposizione 1.4.8 – Omomorfismi e ordine

Siano $(G_1, *)$, $(G_2, \star)$ due gruppi e sia $f : G_1 \to G_2$ omomorfismo.
Allora valgono le seguenti due affermazioni

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

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

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

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

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

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

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

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

(ii) Dimostriamo entrambi i versi dell'implicazione.

$\boxed{\Longrightarrow}$ Supponiamo f iniettiva.

- Se $\operatorname{ord}(f(x)) = +\infty$ allora per il punto (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 (vi) $\ker f = \{ e_1 \}$, da cui segue che $x^m = e_1$.
Dunque per la Voce (ii) segue che

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

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

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

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

Ma $\operatorname{ord}(x) = 1$ se e solo se $x = e_1$, ovvero $\ker f = \{ e_1 \}$, dunque per la Voce (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 $(G_1, *)$, $(G_2, *)$ due gruppi e sia $\varphi : G_1 \to G_2$ un isomorfismo.

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

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

Allora la funzione

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

è bigettiva.

Dimostrazione. Siccome $H \leq G_1$ e φ è un omomorfismo, allora $f(H) = \varphi(H) \leq G_2$ (ovvero $f(H) \in \mathcal{K}$) per la Voce (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 Voce (iv).

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

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

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

Teorema 1.4.12 – Isomorfismi di gruppi ciclici

Sia $(G, \cdot)$ un gruppo ciclico. Allora

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

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

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

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

$g^k \neq g^h$. Sia allora

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

Per definizione di $G = < g >$ 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 $\text{ord}(g) = n$, 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.
  $$\text{Im}\,\varphi = \varphi(\mathbb{Z}/n\mathbb{Z}) = \{ g^0, g^1, \dots, g^n \} = < g > = G.$$

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

□

Corollario 1.4.13 – Sottogruppi del gruppo ciclico

Sia $(G, \cdot)$ un gruppo ciclico.

(i) Se G è infinito e $H \leq G$ 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 $H \leq G$ 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 Voce (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 Voce (ii).

3. per la Proposizione 1.4.11 sappiamo che se $f : G_1 \to G_2$ è un isomorfismo, allora

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

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

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

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

Allora per il Teorema 1.4.12 esiste un isomorfismo

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

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

$$\{ K : K \leq G \} = \left\{ \psi(\langle [d] \rangle) = \left\langle g^d \right\rangle : d \,\middle|\, n \right\}. \qquad \square$$

Definizione 1.4.14 – Automorfismo

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

Proposizione 1.4.15 – Gruppo degli automorfismi

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

Dimostrazione. Mostriamo che valgono gli assiomi di gruppo.

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

▸ **ASSOCIATIVITÀ** La composizione di funzioni è associativa.

▸ **ELEMENTO NEUTRO** L'elemento neutro di 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 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 $n \geq 0$. 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

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

Parte I

ALGEBRA I

2

Teoria dei Gruppi

2.1 GRUPPI E GENERATORI

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

Definizione 2.1.1 – Gruppo generato da un suo sottoinsieme

Sia G un gruppo e sia $S \subseteq G$ un suo sottoinsieme.

G si dice **generato da** S, oppure si dice che S è un **insieme di generatori per** G (e si indica con $G = \langle S \rangle$), se

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

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

Parleremo più nel dettaglio di generatori quando introdurremo il gruppo libero su un insieme.

Osservazione 2.1.1. $s_1 \dots s_n$ 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 2.1.2. 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 2.1.3. 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 $< s > \leq G$ è un sottogruppo finito, e sarà della forma

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

dove $m := \mathrm{ord}_G(s)$. Siccome $< s >$ è un sottogruppo di G segue che $s^{-1} \in < s >$, dunque $s^{-1} = s^k$ per qualche $0 \leq k < m$. Dunque ogni occorrenza di s^{-1} in una parola può essere sostituita con s^k che è ottenibile dai soli elementi di S. □

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

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

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

Al contrario degli spazi vettoriali non è detto che esista una *dimensione* del gruppo: due insiemi di generatori minimali possono avere cardinalità diverse.

Esempio 2.1.3. 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.

Un tipo particolare di gruppi sono i **gruppi finitamente generati**.

Definizione 2.1.4 – Finitamente generato

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

Proposizione 2.1.5

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

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

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

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

$$S = \{ x_{11} \dots xk_{11}, \dots, x_{1n} \dots xk_{nn} \}.$$

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

2.2 GRUPPO DIEDRALE

Uno degi gruppi più importanti in algebra è il gruppo delle isometrie dell'n-agono regolare (ovvero delle trasformazioni che mandano l'n-agono regolare in sé), detto **gruppo diedrale**.

Definizione 2.2.1 – Gruppo diedrale

Se $n \geq 3$, si dice **gruppo diedrale** D_n l'insieme delle isometrie del piano che mandano in sé l'n-agono regolare insieme all'operazione di composizione.

Per mostrare che il gruppo diedrale è effettivamente un gruppo dobbiamo mostrare che la composizione di isometrie è un'isometria (il che è ovvio) e che ogni isometria ammette un'inversa. Ma l'inversa di una trasformazione σ è semplicemente l'isometria che *annulla* l'effetto di σ, dunque D_n è un gruppo.

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

Proposizione 2.2.2 – Cardinalità del gruppo diedrale

La cardinalità di D_n è $2n$ per ogni $n \geq 3$.

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

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 distinte, 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 $\#D_n = 2n$. □

Abbiamo quindi visto che vi sono due tipi distinti di elementi: le **rotazioni** e le **simmetrie**. 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 $s_i r, s_i r^2, \dots, s_i r^{n-1}$ sono anch'essi tutti elementi di D_n per qualsiasi i: dobbiamo capire quali di questi siano uguali.

Proposizione 2.2.3

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

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

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

Mostriamo che sr^i è una simmetria, ovvero non è una rotazione. Se per assurdo lo fosse, allora sarebbe uguale a r^j per qualche $j \in \mathbb{Z}$, $0 \leq j < n$. 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 tramite una *presentazione di gruppo*:

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

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.

2.2.1 Sottogruppi del gruppo diedrale

Studiamo ora 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 **??** segue che $< r > \triangleleft D_n$.

Tuttavia possiamo anche mostrare che per ogni $j = 0, \dots, n-1$ il gruppo $\left\langle r^j \right\rangle$ 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 2.2.4

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

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

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

Inoltre esso contiene tutti gli elementi di ordine d poiché è l'unico sottogruppo ciclico di $< r >$ 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 2.2.5

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 2.2.6

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 $\left\langle r^{\frac{n}{d}} \right\rangle$ è normale in D_n.

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

Proposizione 2.2.7 – Centro di D_n

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

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 $\mathrm{id}, r^{n/2}$, da cui segue che
$$Z(D_n) = \left\langle r^{\frac{n}{2}} \right\rangle. \qquad \square$$

Siccome il centro di un gruppo è sempre un sottogruppo normale di quel gruppo (per la **??**) segue che $\left\langle r^{n/2} \right\rangle$ è un sottogruppo normale di D_n.
Vale quindi il seguente Teorema.

Teorema 2.2.8 – Sottogruppi generati dalle rotazioni sono normali

Ogni sottogruppo di D_n della forma $< r^i >$ è normale in D_n.

2.3 AUTOMORFISMI DI UN GRUPPO

Studiamo in questa sezione un tipo fondamentale di gruppo di funzioni, ovvero il gruppo degli **automorfismi** di un gruppo G.

Definizione 2.3.1 – Automorfismo

Sia G un gruppo. Si dice **automorfismo di** G un isomorfismo da G in G. Inoltre si indica con Aut(G) l'insieme di tutti gli automorfismi di G.

Proposizione 2.3.2 – Gli automorfismi formano un gruppo

Sia G un gruppo. Allora Aut(G) con l'operazione di composizione è un gruppo, ed in particolare $\mathrm{Aut}(G) \leq \mathcal{S}(G)$.

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

L'automorfismo più importante è l'automorfismo per *coniugio*.

Definizione 2.3.3 – Coniugio e automorfismi interni

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

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

Questa mappa viene chiamata **coniugio di x per g**. Inoltre si dice **insieme degli automorfismi interni** l'insieme

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

Proposizione 2.3.4

Sia G un gruppo, $g \in G$. Allora il coniugio per g è un automorfismo di G. In particolare vale che

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

Prima di mostrare la Proposizione 2.3.4 dimostriamo un semplice Lemma che semplificherà i calcoli da fare.

Lemma 2.3.5 – Proprietà degli automorfismi interni

Siano $g, h \in G$ e sia $e \in G$ l'identità. Allora valgono le seguenti affermazioni:

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

(2) $\varphi_g \circ \varphi_h = \varphi_{gh}$.

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

Come vedremo più avanti, questo significa dire che il coniugio è un'**azione** di G su se stesso. Per ora limitiamoci a dimostrare il Lemma.

Dimostrazione. Dimostriamo separatamente le tre affermazioni.

▸ CONIUGIO PER L'IDENTITÀ Sia $g \in G$ qualunque. Allora

$$\varphi_e(g) = ege^{-1} = g = \mathrm{id}(g).$$

Dato che questo vale per ogni $g \in G$ segue che $\varphi_e = \mathrm{id}$.

▸ COMPOSIZIONE DI CONIUGI Sia $x \in G$ qualunque. Allora

$$(\varphi_g \circ \varphi_h)(x) = \varphi_g(\varphi_h(x)) = \varphi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \varphi_{gh}(x),$$

da cui $\varphi_g \circ \varphi_h = \varphi_{gh}$.

▸ INVERSO DI UN CONIUGIO Mostriamo che $\varphi_g \circ \varphi_{g^{-1}} = \varphi_{g^{-1}} \circ \varphi_g = \mathrm{id}$. Sia quindi $x \in G$ qualunque.

$$(\varphi_g \circ \varphi_{g^{-1}})(x) = \varphi_g(\varphi_{g^{-1}}(x)) = g(g^{-1}xg)g^{-1} = x,$$
$$(\varphi_{g^{-1}} \circ \varphi_g)(x) = \varphi_{g^{-1}}(\varphi_g(x)) = g^{-1}(gxg^{-1})g = x,$$

da cui la tesi. □

Dimostrazione della Proposizione 2.3.4. Sicuramente φ_g è ben definita: per ogni $x \in G$ segue che $\varphi_g(x) = gxg^{-1}$ che è ancora un elemento di 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 $\mathrm{Aut}(G)$, 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 per il Lemma 2.3.5 $\varphi_g \circ \varphi_h = \varphi_{gh}$ che ovviamente appartiene a $\mathrm{Inn}(G)$.
- Se $\varphi_g \in \mathrm{Inn}(G)$ allora per il Lemma 2.3.5 $\varphi_g^{-1} = \varphi_{g^{-1}}$ che è ancora elemento di $\mathrm{Inn}(G)$, dunque $\mathrm{Inn}(G)$ è chiuso per inversi.

Infine mostriamo che $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$, ovvero che data che $\sigma \in \mathrm{Aut}(G)$ qualunque si ha $\sigma\,\mathrm{Inn}(G)\sigma^{-1} \subseteq \mathrm{Inn}(G)$, ovvero che per ogni $g \in G$ vale che

$$\sigma\varphi_g\sigma^{-1} \in \mathrm{Inn}(G).$$

Sia quindi $x \in G$ qualsiasi. Allora

$$\begin{aligned}(\sigma\varphi_g\sigma^{-1})(x) &= \sigma\Big(\varphi_g\big(\sigma^{-1}(x)\big)\Big)\\ &= \sigma\Big(g\big(\sigma^{-1}(x)\big)g^{-1}\Big)\\ &= \sigma(g)\cdot\sigma(\sigma^{-1}(x))\cdot\sigma(g^{-1})\\ &= \sigma(g)x\sigma(g)^{-1},\end{aligned}$$

dunque $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)} \in \mathrm{Inn}(G)$, ovvero $\mathrm{Inn}(G)$ è un sottogruppo normale di $\mathrm{Aut}(G)$. □

Osserviamo che se G è un gruppo abeliano allora $\mathrm{Inn}(G) = \{\mathrm{id}\}$: infatti per ogni $g, x \in G$ si ha che $\varphi_g(x) = gxg^{-1} = x$.

Proposizione 2.3.6

$$\mathrm{Inn}(G) \simeq G/Z(G).$$

Dimostrazione. Consideriamo la mappa

$$\begin{aligned}\Phi : G &\to \mathrm{Inn}(G)\\ g &\mapsto \varphi_g,\end{aligned}$$

chiaramente ben definita e surgettiva.

▸ OMOMORFISMO Mostriamo che Φ è un omomorfismo di gruppi:

$$\Phi(g_1g_2) = \varphi_{g_1g_2} \overset{(1)}{=} \varphi_{g_1} \circ \varphi_{g_2} = \Phi(g_1) \circ \Phi(g_2),$$

dove in (1) abbiamo usato il Lemma 2.3.5.

▸ NUCLEO Il nucleo di Φ è

$$\ker\Phi = \{g \in G : \varphi_g = \mathrm{id}\} = \{g \in G : gxg^{-1} = x \forall x \in G\} = Z(G).$$

La tesi segue per il Teorema 3.2.2. □

Osservazione 2.3.1. Abbiamo osservato che se $G/Z(G)$ è ciclico allora G è abeliano, dunque $\mathrm{Inn}(G)$ è ciclico solo se G è abeliano, dunque per qunaot osservato sopra $\mathrm{Inn}(G)$ è ciclico solo se è banale.

Un modo molto comodo per caratterizzare i sottogruppi normali è analizzare la loro relazione con gli automorfismi interni. In effetti, per definizione $N \triangleleft G$ se e solo se $gNg^{-1} \subseteq N$ per ogni $g \in G$, ovvero se e solo se

$$\varphi_g(N) \subseteq N.$$

Proposizione 2.3.7 – Invarianza dei sottogruppi normali per automorfismi interni

I sottogruppi normali N di un gruppo G sono **invarianti per automorfismi interni**, ovvero si ha che $\varphi_g(N) \subseteq N$ (e dunque $\varphi_g(N) = N$, poiché l'altra inclusione è banale e sempre vera).

Inoltre ogni automorfismo interno di G definisce un automorfismo di N tramite la restrizione:

$$\begin{aligned} \mathrm{Inn}(G) &\to \mathrm{Aut}(N) \\ \varphi_g &\mapsto \varphi_g|_N. \end{aligned}$$

Dimostrazione. La prima parte è ovvia per definizione di sottogruppo normale: per ogni $g \in G$ vale che

$$\varphi_g(N) = gNg^{-1} = N.$$

Mostriamo ora che $\varphi_g|_N$ è un automorfismo di N.

In effetti $\varphi_g|_N$ può essere considerato come una funzione da N in sé, in quanto come abbiamo mostrato sopra la sua immagine è $\varphi_g|_N(N) = N$.

Inoltre siccome è una restrizione di un isomorfismo esso è ancora un isomorfismo, da cui segue che è un automorfismo di N. □

Definizione 2.3.8 – Sottogruppo caratteristico

$H \leq G$ si dice **caratteristico** se è invariante per automorfismi, ovvero se per ogni $\varphi \in \mathrm{Aut}(G)$ si ha che

$$\varphi(H) = H.$$

Anche in questo caso per mostrare che H è caratteristico è sufficiente vedere che $\varphi(H) \subseteq H$ per ogni automorfismo φ: infatti φ^{-1} è ancora un automorfismo di G, dunque abbiamo anche verificato che $\varphi^{-1}(H) \subseteq H$, che è equivalente a $H \subseteq \varphi(H)$, che è ciò che volevamo.

Proposizione 2.3.9

Se H è caratteristico in G, allora $H \triangleleft G$.

Dimostrazione. Ovvia: se H è caratteristico è invariante per automorfismi, dunque è invariante per *automorfismi interni*, dunque è normale. □

Osservazione 2.3.2. Il viceversa è falso! Infatti consideriamo $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e siano

$$H_1 := \langle (1,0) \rangle, \qquad H_2 := \langle (0,1) \rangle, \qquad H_3 := \langle (1,1) \rangle.$$

Siccome G è abeliano tutti i suoi sottogruppi sono normali. Mostriamo che H_1 non è caratteristico.

Sia $\varphi : G \to G$ tale che

- $\varphi((1,0)) = (1,1)$
- $\varphi((0,1)) = (0,1)$
- $\varphi((a,b)) = a\varphi((1,0)) + b\varphi((0,1)) = (a,a) + (0,b) = (a, a+b)$.

▸ OMOMORFISMO φ è un omomorfismo in quanto

$$\begin{aligned}\varphi((a,b)+(c,d)) &= \varphi((a+c,b+d))\\ &= (a+c, a+c+b+d)\\ &= (a, a+b)+(c, c+d)\\ &= \varphi((a,b))+\varphi((c,d)).\end{aligned}$$

▸ INIETTIVITÀ φ è iniettiva in quanto

$$\begin{aligned}\ker\varphi &= \{(a,b)\in G \,:\, \varphi((a,b)) = (a, a+b) = 0\}\\ &= \{(a,b)\in G \,:\, a=0, b=0\}\\ &= \{(0,0)\}.\end{aligned}$$

Dunque φ è un automorfismo di G (in quanto è un endomorfismo iniettivo di G e G è un gruppo finito). Ma

$$\varphi(H_1) = \varphi\Big(\big\langle (1,0)\big\rangle\Big) = \big\langle \varphi((1,0))\big\rangle = <(1,1)> = H_3 \neq H_1,$$

dunque H_1 è normale in G ma non è caratteristico.

2.4 AZIONI DI GRUPPO

Definizione 2.4.1 – 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 2.4.2. 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 2.4.3. Sia V un $\mathbb{K}$-spazio vettoriale. Allora l'applicazione

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

è un'azione del gruppo moltiplicativo degli scalari $\mathbb{K}^\times$ 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.

2.4.1 Orbite e stabilizzatori

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

$$x\sim y \iff \exists g\in G \text{ tale che } \varphi_g(x) = y. \tag{2.1}$$

Proposizione 2.4.4

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 (2.1) 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 2.4.1. 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 $\varphi_{g^{-1}}$:
$$\begin{aligned}\varphi_{g^{-1}} \circ \varphi_g &= \varphi(g^{-1}) \circ \varphi(g) = \varphi(g)^{-1} \circ \varphi(g) = \mathrm{id}\,.\\ \varphi_g \circ \varphi_{g^{-1}} &= \varphi(g) \circ \varphi(g^{-1}) = \varphi(g) \circ \varphi(g)^{-1} = \mathrm{id}\,.\end{aligned}$$

Introduciamo ora i concetti fondamentali di **orbita** e **stabilizzatore**.

Definizione 2.4.5 – Orbita

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

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

Osservazione 2.4.2. L'orbita di x è esattamente la classe di equivalenza data dalla relazione di equivalenza definita in (2.1). In particolare se R è un insieme di rappresentanti vale che

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

Definizione 2.4.6 – Stabilizzatore

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

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

Proposizione 2.4.7 – Lo stabilizzatore è un sottogruppo

Sia G un gruppo che agisce sull'insieme X; sia inoltre $x \in X$. Allora vale che

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

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

- CHIUSURA PER INVERSI 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 $g^{-1} \in \mathrm{Stab}_G(x)$.

- CHIUSURA PER PRODOTTI 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. □

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

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

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

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

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 2.4.8 – 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

$$|G| = |\mathrm{orb}(x)| \cdot |\mathrm{Stab}_G(x)|. \tag{2.2}$$

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. □

2.4.2 Azione di coniugio

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

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

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

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

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

Invece lo stabilizzatore di x in G è:

$$\mathrm{Stab}_G(x) = \{\, g \in G \,:\, \varphi_g(x) = x \,\} = \{\, g \in G \,:\, gxg^{-1} = x \,\} = g \in G gx = xg = Z_G(x),$$

ovvero il centralizzatore di x in G.

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

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

ovvero $|\mathrm{Cl}(x)| \mid |G|$.

Da questo segue un'altra importante proprietà dei gruppi normali.

Proposizione 2.4.9 – I gruppi normali sono unione di classi di coniugio

Sia G un gruppo, $H \leq G$. Allora $H \triangleleft G$ se e solo se H è unione di intere classi di coniugio.

Dimostrazione. Mostriamo entrambi i versi dell'implicazione.

$\boxed{\Longrightarrow}$ Se $H \triangleleft G$ 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 $\{ ghg^{-1} : g \in G \} = \mathrm{Cl}(h) \subseteq H$, ovvero H è unione di intere classi di coniugio.

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

2.4.3 Coniugio di sottogruppi

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

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

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

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

Segue quindi che φ è un'azione di G sui suoi sottogruppi.

Sia $H \leq G$. L'orbita di H rispetto a questa azione è

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

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

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

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

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

Proposizione 2.4.10 – Sottogruppi normali e azione di coniugio per sottogruppi

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

(i) $H \triangleleft G$.

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

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

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 $\mathrm{orb}(H) = \{ H \}$.

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

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

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

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

□

2.4.4 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

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

Sicuramente $x \in \mathrm{orb}(x)$ in quanto $x = \varphi_{e_G}(x)$; inoltre possiamo notare che $\mathrm{Cl}(x) = \{ x \}$ 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 $|G| = |\mathrm{Cl}(x)| \cdot |Z_G(x)|$. Allora vale che $\mathrm{Cl}(x) = \{ x \}$ se e solo se $|\mathrm{Cl}(x)| = 1$, 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

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

Se G è finito, passando alle cardinalità si ottiene

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

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 2.4.11 – Formula delle classi

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

$$|G| = |Z(G)| + \sum_{x\in R\setminus Z(G)}\frac{|G|}{|Z_G(x)|}. \tag{2.3}$$

Osserviamo che la formula delle classi non vale solo per G, ma anche per tutti i sottogruppi normali di G. Infatti per la Proposizione 2.4.9 segue che

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

dunque se H è finito si ha

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

2.5 ALCUNI RISULTATI CHE DERIVANO DA AZIONI DI GRUPPO

Elenchiamo in questa sezione alcuni risultati importanti che possono essere dimostrati considerando particolari azioni di gruppo.

2.5.1 p-Gruppi

Definizione 2.5.1 – p-gruppo

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

Come vedremo in seguito, i p-gruppi sono fondamentali nello studio di gruppi più complicati. Vediamo alcune loro proprietà di base.

Proposizione 2.5.2 – 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 $Cl(x) = \frac{|G|}{|Z_G(x)|} > 1$, 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. □

Proposizione 2.5.3

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 2.5.2 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 **??**) 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. □

2.5.2 Teorema di Cauchy (caso non abeliano)

Teorema 2.5.4 – Teorema di Cauchy

Sia $p \in \mathbb{Z}$ primo e G un gruppo finito. Se $p \mid |G|$ allora esiste $g \in G$ tale che

$$\mathrm{ord}_G(g) = p.$$

Dimostrazione. Sia $|G| = p^n$. Dimostriamo il Teorema per induzione su n.

- CASO BASE Supponiamo $n = 1$: allora $p^n = p$, dunque $G \simeq \mathbb{Z}/p\mathbb{Z}$ e un qualsiasi generatore di $\mathbb{Z}/p\mathbb{Z}$ ha ordine 1.

- PASSO INDUTTIVO Supponiamo che la tesi sia vera per tutti i gruppi di ordine p^m con $1 \leq m < n$ e mostriamola per un gruppo G di cardinalità p^n. Dividiamo la dimostrazione in due casi.

  - Supponiamo che esista un $H \leq G$, $H \neq G$ di ordine multiplo di p. Allora $|H| = p^k$ per qualche $k < n$, dunque per ipotesi induttiva esiste $g \in H$ tale che $\mathrm{ord}_H(g) = p$, da cui $\mathrm{ord}_G(g) = p$.

- Se invece non esiste alcun sottogruppo di ordine multiplo di p per la Formula delle classi si ha che

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

Siccome $Z_G(x) \leq G$ segue che $p \nmid |Z_G(x)|$; inoltre $p \mid G$, dunque segue necessariamente che p divide ogni termine della sommatoria, da cui

$$p \mid \sum_{x \in R \setminus Z(G)} \frac{|G|}{|Z_G(x)|}.$$

Ma allora per differenza $Z(G)$ ha cardinalità multipla di p, da cui segue che non può essere un sottogruppo proprio di G.

Segue quindi che G è abeliano, e la tesi segue dal Teorema di Cauchy per gruppi abeliani. □

2.5.3 Teorema di Cayley

Teorema 2.5.5 – Teorema di Cayley

Sia G un gruppo. Allora G è isomorfo ad un sottogruppo di un gruppo di permutazioni.
In particolare se G è un gruppo finito di ordine n, G è isomorfo ad un sottogruppo di $\mathcal{S}_n$.

Dimostrazione. Per mostrare che G è isomorfo ad un sottogruppo di un gruppo di permutazioni è sufficiente mostrare che esiste un omomorfismo iniettivo (ovvero un'*immersione*) di G in tale gruppo $\mathcal{S}$: infatti se $\lambda : G \hookrightarrow \mathcal{S}$ è un'immersione, per il Primo Teorema degli Omomorfismi si ha che

$$G/\{e_G\} \simeq G \simeq \operatorname{Im}\lambda \leq \mathcal{S}.$$

Poniamo dunque $\mathcal{S} := \mathcal{S}(G)$ e consideriamo l'azione di G su se stesso per *moltiplicazione a sinistra*: allora

$$\begin{aligned} \lambda : G &\to \mathcal{S}(G) \\ g &\mapsto (x \mapsto gx) \end{aligned}$$

è effettivamente un omomorfismo di gruppi iniettivo.

▸ BUONA DEFINIZIONE La funzione $\lambda_g = x \mapsto gx$ è una bigezione (e quindi appartiene a $\mathcal{S}(G)$) poiché è iniettiva (per la legge di cancellazione sinistra se $gx = gy$ allora $x = y$) ed è surgettiva (basta osservare che $\lambda_g(g^{-1}y) = gg^{-1}y = y$ per ogni $y \in G$).

▸ OMOMORFISMO Infatti per ogni $x \in G$

$$\lambda(g_1g_2)(x) = g_1g_2x = \lambda(g_1)\big(\lambda(g_2)(x)\big) = \big(\lambda(g_1) \circ \lambda(g_2)\big)(x),$$

ovvero $\lambda(g_1g_2) = \lambda(g_1) \circ \lambda(g_2)$, come volevamo.

▸ INIETTIVITÀ Si ha che

$$\ker\lambda = \{\, g \in G \,:\, \lambda(g) = \mathrm{id} \,\} = \{\, g \in G \,:\, \lambda(g)(x) = gx = x,\ \forall x \in G \,\} = \{\, e_G \,\},$$

da cui λ è iniettiva.

Si ha quindi che $G \hookrightarrow \mathcal{S}(G)$, come volevamo. In particolare se $|G| = n$ avremo che $\mathcal{S}(G) \simeq \mathcal{S}_n$, da cui il secondo punto. □

2.6 SOTTOGRUPPO DERIVATO

Definizione 2.6.1 – Commutatore

Sia G un gruppo, $x, y \in G$. Si dice **commutatore** di x, y la quantità

$$[x, y] := xyx^{-1}y^{-1}.$$

Il commutatore di due elementi ci dice *quanto commutano*: infatti se $xy = yx$ allora $[x, y] = xyx^{-1}y^{-1} = e_G$.

Definizione 2.6.2 – Sottogruppo derivato

Sia G un gruppo. Si dice **sottogruppo dei commutatori di** G, oppure **sottogruppo derivato** di G il gruppo

$$G' = [G, G] := \langle [x, y] \mid x, y \in G \rangle.$$

Sicuramente $G' \leq G$ in quanto è generato da elementi di G. In particolare vale la seguente proposizione.

Proposizione 2.6.3

Sia G un gruppo.

(1) G' è caratteristico in G.

(2) Sia $H \triangleleft G$. Allora G/H è abeliano se e solo se $G' \subseteq H$.

(3) G' è banale se e solo se G è abeliano.

Dimostrazione. Dimostiamo le tre affermazioni.

(1) Sia $\varphi \in \mathrm{Aut}(G)$ qualunque e mostriamo che $\varphi(G') \subseteq G'$. Sia $S := \{ [x, y] : x, y \in G \}$: dato che $G' = <S>$ si ha

$$\varphi(G') = \varphi(<S>) = \langle \varphi(S) \rangle,$$

dove l'ultima uguaglianza viene dal fatto che φ è un omomorfismo di gruppi. Basta allora mostrare che per ogni commutatore $[x, y] \in S$ vale che $\varphi([x, y]) \in G'$. In effetti

$$\varphi([x, y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = [\varphi(x), \varphi(y)] \in G',$$

dunque $\varphi(G') \subseteq G'$, ovvero G è caratteristico in G.

(2) G/H è abeliano se e solo se per ogni $xH, yH \in G/H$ si ha

$$xHyH = yHxH.$$

Siccome per ipotesi $H \triangleleft G$ questo è equivalente a $xyH = yxH$, ovvero

$$(yx)^{-1}xy = x^{-1}y^{-1}xy = [x^{-1}, y^{-1}] \in H.$$

Dunque l'insieme S di generatori deve essere un sottoinsieme di H, dunque essendo H un gruppo segue che $< S > = G' \leq H$.

(3) Segue dal punto precedente: G è abeliano se e solo se G/H è abeliano per qualsiasi $H \triangleleft G$, ovvero se $G' \subseteq H$ per ogni $H \triangleleft G$. Ma l'unico gruppo contenuto in ogni sottogruppo normale è $\{ e_G \}$ (poiché anch'esso è normale), dunque G è abeliano se e solo se $G' = \{ e_G \}$. □

Segue quindi che G' è il più piccolo sottogruppo normale di G che renda il quoziente abeliano (poiché ogni tale sottogruppo deve contenere G'): il quoziente G/G' è dunque il più *grande* quoziente abeliano di G, e si chiama per questo **abelianizzato** di G.

2.7 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 2.7.1 – Gruppo libero su un insieme

Sia $X = \{ x_1, x_2, \dots \}$ un insieme di simboli e poniamo $X^{-1} := \{ x_1^{-1}, x_2^{-1}, \dots \}$ l'insieme dei loro inversi formali.

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

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

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 2.7.1. 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

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

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

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

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 $X \to H$. Nel caso il generatore sia uno solo (ovvero nel caso di $\mathbb{Z}$) esiste una sola funzione dal generatore in un dato elemento del gruppo H, dunque la bigezione è con gli elementi di H.

Costruzione della presentazione di un gruppo

Consideriamo ora un gruppo H generato da $g_1, \ldots, g_n$ (non libero). Per l'osservazione precedente deve esistere un omomorfismo dal gruppo libero su n elementi (chiamiamolo $F(n)$) verso H:

$$F(n) \xrightarrow{\varphi} H \tag{2.4}$$

tale che $x_i \mapsto g_i$ per ogni $i = 1, \ldots, n$.

Notiamo che φ è un omomorfismo surgettivo: l'immagine di φ contiene i generatori di H, dunque deve essere tutto H. Per il **??** vale quindi che

$$H = \mathrm{Im}\,\varphi \simeq {}^{F(n)}\!/_{\ker \varphi}\,. \tag{2.5}$$

Una *presentazione* di H è quindi un'espressione del tipo

$$H = < x_1, \ldots, x_n \mid w_1, \ldots, w_m > \tag{2.6}$$

dove $x_1, \ldots, x_n$ sono i generatori e $w_1, \ldots, w_m$ sono delle parole contenenti gli x_i e i loro inversi che generano $\ker \varphi$.

Corollario 2.7.2

Sia $H = < x_1, \ldots, x_n \mid w_1, \ldots, w_m >$ e sia K un gruppo qualsiasi. Allora esiste una bigezione tra $\mathrm{Hom}(H, K)$ e l'insieme delle funzioni

$$f : \{ x_1, \ldots, x_n \} \to K$$

tali che le immagini di $x_1, \ldots, x_n$ rispettano le condizioni $w_1, \ldots, w_m$.

Dimostrazione. Abbiamo già mostrato che ${}^{F(n)}\!/_{< w_1, \ldots, w_m >} \simeq H$; inoltre, siccome esiste sempre un omomorfismo dal gruppo libero su n elementi ad un gruppo generato da n elementi, dovrà esistere un omomorfismo

$$g : F(n) \to \langle f(x_1), \ldots, f(x_n) \rangle.$$

Dall'ipotesi che $f(x_i)$ rispetta le condizioni date da $w_1, \ldots, w_m$ segue che $w_1, \ldots, w_m \in \ker g$, ovvero

$$< w_1, \ldots, w_m > \subseteq \ker g.$$

Per il Primo Teorema degli Omomorfismi esisterà allora un unico omomorfismo φ tale

che il seguente diagramma commuti:

$$\begin{array}{ccc} F(n) & \xrightarrow{g} & \left\langle f(x_1), \dots, f(x_n) \right\rangle \subseteq K \\ {\scriptstyle\pi}\downarrow & \nearrow_{\varphi} & \\ H \simeq \frac{F(n)}{< w_1, \dots, w_m >} & & \end{array} \tag{2.7}$$

In particolare quindi per ogni scelta di f esiste un unico omomorfismo da H in $\left\langle f(x_1), \dots, f(x_n) \right\rangle \subseteq K$, da cui la tesi. □

Questo corollario ci consente di trovare gli omomorfismi tra gruppi molto semplicemente, a patto di conoscere una presentazione del gruppo di partenza. Infatti per descrivere un omomorfismo da H in K è sufficiente trovare una funzione f dai generatori di H in K tale che le immagini dei generatori rispettino le condizioni date dalla presentazione di H.

2.7.3 Esercizio Descrivere tutti gli omomorfismi di S_3 in sè.

Soluzione Una presentazione di S_3 è data da

$$S_3 = \left\langle \sigma, \tau \;\middle|\; \sigma^3 = 1, \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \right\rangle.$$

Per il corollario precedente $\mathrm{Hom}(()S_3, S_3)$ è in bigezione con le funzioni $f : \{\sigma, \tau\} \to S_3$ tali che

- $f(\sigma)^3 = 1$,
- $f(\tau)^2 = 1$,
- $f(\tau\sigma\tau) = f(\sigma^{-1})$.

Per la prima condizione segue che $f(\sigma) \in \{\mathrm{id}, \sigma, \sigma^2\}$.

(i) Se $f(\sigma) = \mathrm{id}$ la terza relazione è banale: per ogni scelta di $f(\tau)$ che rispetta la seconda relazione si ha

$$f(\tau\sigma\tau) = f(\tau)f(\sigma)f(\tau) = f(\tau)f(\tau) = f(\tau)^2 = \mathrm{id} = f(\sigma)^{-1}.$$

Le scelte di $f(\tau)$ sono 4: id, τ, $\tau\sigma$ e $\tau\sigma^2$.

(ii) Se $f(\sigma) = \sigma$, la terza relazione è verificata per ogni scelta di $f(\tau)$ che rispetti la seconda condizione, tranne la scelta $f(\tau) = \mathrm{id}$. Ho quindi 3 scelte per $f(\tau)$.

(iii) Se $f(\sigma) = \sigma^2$ ho le stesse 3 scelte per $f(\tau)$ del punto precedente.

Vi sono quindi 10 omomorfismi da S_3 in sé, tutti univocamente determinati dalle immagini di σ e τ. In particolare vi sono 6 automorfismi, che corrispondono agli omomorfismi del secondo e terzo punto. ⌟

2.8 GRUPPI DI PERMUTAZIONI

Usando la teoria sulle azioni di gruppo viste finora possiamo finalmente studiare bene i *gruppi di permutazione*. Un gruppo di permutazioni è il gruppo

$$\mathcal{S}_n := \left\{ f : \{1, \dots, n\} \to \{1, \dots, n\} \;:\; f \text{ bigettiva} \right\}$$

insieme all'operazione di composizione tra funzioni.

Ogni elemento di $\mathcal{S}_n$ può essere rappresentato nei seguenti modi:

$$\mathcal{S}_3 \ni \begin{Bmatrix} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \end{Bmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3),$$

dove il primo semplicemente mi dà l'immagine di ogni elemento di $\{1,\dots,n\}$, il secondo fa la stessa cosa ma sotto forma di matrice e il terzo va letto come "1 viene portato in 2 che viene portato in 3 che viene riportato in 1".

Useremo nella maggior parte dei casi il terzo metodo, poiché è quello più veloce e fa trasparire tante proprietà delle permutazioni.

Per studiare il comportamento di una permutazione $\sigma \in \mathcal{S}_n$ dobbiamo *dare la sua azione* sull'insieme $\{1,\dots,n\}$, che corrisponde all'inclusione del sottogruppo generato da σ:

$$\begin{aligned} \langle \sigma \rangle &\hookrightarrow \mathcal{S}_n \\ \sigma^k \mapsto \sigma^k : \{1,\dots,n\} &\to \{1,\dots,n\} \\ i &\mapsto \sigma^k(i). \end{aligned}$$

Sia $x \in \{1,\dots,n\}$ qualsiasi e consideriamo la sua orbita:

$$\mathrm{orb}(x) = \left\{ \sigma^k(x) \,:\, k \geq 0 \right\} = \left\{ x, \sigma(x), \dots, \sigma^{m_x - 1}(x) \right\}.$$

Osserviamo che ovviamente $<\sigma>$ agisce ciclicamente su ogni orbita: se $y \in \mathrm{orb}(x)$ allora $\sigma^k(y) \in \mathrm{orb}(x)$, dunque $\sigma^k(\mathrm{orb}(x)) = \mathrm{orb}(x)$ poiché $\mathrm{orb}(x)$ è già l'insieme di tutte le possibili immagini.

▸ CLAIM: $m_x := \min\{ k > 0 \,:\, \sigma^k(x) = x \}$.

> **Dimostrazione.** Sia k il minimo intero positivo tale che $\sigma^k(x)$ appartenga all'insieme $\{x, \dots, \sigma^{k-1}(x)\}$: dovrà quindi esistere un $0 \leq h < k$ tale che $\sigma^k(x) = \sigma^h(x)$, il che equivale a dire che
>
> $$\sigma^{k-h}(x) = \mathrm{id}(x) = x.$$
>
> Dunque σ^{k-h} appartiene a $\{x, \dots, \sigma^{k-1}(x)\}$ e inoltre $0 < k - h \leq k$ poiché $h < k$. Per minimalità di k segue quindi che $h = 0$, cioè $\sigma^k(x) = x$, come volevamo. □

L'orbita di σ (o più precisamente del sottogruppo di $\mathcal{S}_n$ generato da σ) è quindi il sottoinsieme di $\{1,\dots,n\}$ che viene *permutato ciclicamente* da σ.

Definizione 2.8.1 – Ciclo

Sia $\sigma \in \mathcal{S}_n$, $x \in \{1,\dots,n\}$. Si dice **ciclo** l'orbita di x rispetto all'azione di $<\sigma>$ vista come insieme ordinato.

Esempio 2.8.2. Consideriamo la permutazione $\tau \in \mathcal{S}_5$ data da

$$\begin{Bmatrix} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 4 \\ 4 \mapsto 5 \\ 5 \mapsto 3 \end{Bmatrix}$$

L'orbita di 1 è $\mathrm{orb}(1) = 1,2$ e l'orbita di 3 è $\mathrm{orb}(3) = 3,4,5$: queste due orbite formano i cicli della permutazione.

Osservazione 2.8.1. Un ciclo di lunghezza k (chiamato anche k-ciclo) ha k scritture diverse.

Dimostrazione. Infatti possiamo scegliere il primo elemento arbitrariamente, mentre gli altri seguono dall'ordine. □

Esempio 2.8.3. Nell'esempio precedente, il ciclo $\mathrm{orb}(3) = (3,4,5)$ può anche essere scritto come $(4,5,3)$ oppure $(5,3,4)$ ma non $(5,4,3)$.

Inoltre ogni permutazione di $\mathcal{S}_n$ è determinata in modo univoco dai propri cicli. Ad esempio la permutazione

$$\sigma = (1,2,3)(4,5)(6,7,8,9)(10) \in \mathcal{S}_{10}$$

ha 4 orbite disgiunte, che corrispondono ai suoi 4 cicli disgiunti:

$$\sigma_1 = (1,2,3) \quad \sigma_4 = (4,5) \quad \sigma_6 = (6,7,8,9) \quad \sigma_{10} = (10).$$

Siccome ogni orbita è necessariamente disgiunta (poiché lo sono le orbite di ogni azione) ogni elemento di $\{1,\dots,n\}$ è *mosso* da uno solo dei cicli:

$$\sigma = \sigma_1 \circ \sigma_4 \circ \sigma_6 \circ \sigma_{10}.$$

I cicli $\sigma_1, \sigma_4, \sigma_6$ e σ_{10} vengono detti **disgiunti** in quanto nessuno di essi permuta un elemento mosso dagli altri cicli.

Definizione 2.8.4 – Permutazione ciclica

Una permutazione di $\mathcal{S}_n$ si dice ciclica se è composta da un singolo ciclo non banale.

Ad esempio $\sigma_1, \sigma_4, \sigma_6$ e σ_{10} sono permutazioni cicliche (che chiameremo per brevità, anche se con un po' di abuso di notazione, **cicli**), mentre σ non lo è.

Osservazione 2.8.2. Cicli disgiunti commutano; inoltre l'ordine di una permutazione ciclica come elemento di $\mathcal{S}_n$ è la lunghezza del suo unico ciclo non banale.

Dimostrazione. Il fatto che cicli disgiunti commutino è banale: ognuno di essi agisce su un sottoinsieme di $\{1,\dots,n\}$ e questi sottoinsiemi sono disgiunti, quindi l'ordine in cui avvengono le permutazioni non ha importanza.

Sia ora $\sigma = (x_1,\dots,x_k)$ una permutazione ciclica di lunghezza k: osserviamo che

$$\sigma^k(x_i) = \sigma^{k-1}(x_{i+1}) = \cdots = x_{i+k}.$$

Tuttavia il ciclo ha lunghezza k, dunque $x_{i+k} = x_i$. Segue quindi che $\sigma^k = \mathrm{id}$. Inoltre questo è il minimo numero di volte che dobbiamo applicare σ ad x_i per ottenere nuovamente x_i, dunque $\mathrm{ord}_{\mathcal{S}_n}(\sigma) = k$. □

Proposizione 2.8.5 – Scrittura di una permutazione in cicli disgiunti

Ogni permutazione si scrive in modo "unico" in cicli disgiunti, dove l'unicità è a meno dell'ordine e della scrittura dei singoli cicli.

Dimostrazione. Abbiamo già osservato che ogni permutazione è determinata univocamente dai suoi cicli, ovvero dalle orbite della sua azione su $\{1,\dots,n\}$, ed essi

sono naturalmente disgiunti, in quanto orbite di un'azione. Inoltre essendo disgiunte commutano, quindi l'unicità è a meno dell'ordine. □

Vale quindi il seguente corollario.

Corollario 2.8.6

$\mathcal{S}_n$ è generato dalle permutazioni cicliche.

Numero degli elementi di un determinato tipo

Definizione 2.8.7 – Tipo di una permutazione

Una permutazione $\sigma \in \mathcal{S}_n$ si dice di **tipo** "$k_1 + k_2 + \cdots + k_q$" se si decompone in un prodotto di q cicli disgiunti, il cui i-esimo ciclo è un k_i-ciclo.

Ad esempio la permutazione di prima

$$\sigma = (1,2,3)(4,5)(6,7,8,9)(10) \in \mathcal{S}_n$$

è di tipo $3+2+4+1$.

Vogliamo quindi studiare il numero di k-cicli presenti in $\mathcal{S}_n$.

Proposizione 2.8.8

$$\#\{\,\sigma \in \mathcal{S}_n \;:\; \sigma \text{ è un } k\text{-ciclo}\,\} = \binom{n}{k} \cdot \frac{k!}{k} = \binom{n}{k}(k-1)!$$

Dimostrazione. Bisogna innanzitutto scegliere i k elementi di $\{1,\dots,n\}$ su cui σ agisce in modo non banale, e questo può esser fatto in $\binom{n}{k}$ modi. Le permutazioni di questi elementi sono $k!$, tuttavia ogni ciclo può essere espresso in k modi (perché possiamo scegliere arbitrariamente il suo primo elemento), dunque in totale abbiamo $\binom{n}{k}(k-1)!$ modi, come volevamo. □

Esempio 2.8.9. Calcoliamo il numero di permutazioni di $\mathcal{S}_{20}$ di tipo $2+2+2+4+5+5$, ovvero che sono della forma

$$\sigma = \tau_1\tau_2\tau_3\rho\eta_1\eta_2,$$

con i τ_i di ordine 2, ρ di ordine 4 e gli η_j di ordine 5.

Studiamo il numero di 2-cicli: per la Proposizione 2.8.8 ho

- $\binom{20}{2} \cdot 1! = \binom{20}{2}$ possibilità per τ_1,
- $\binom{18}{2}$ possibilità per τ_2 (devo escludere gli elementi già scelti per τ_1),
- $\binom{16}{2}$ possibilità per τ_3.

Osserviamo inoltre che queste trasposizioni possono essere in qualunque ordine, dunque dobbiamo dividere per $3!$, ottenendo che il numero di scelte per i τ_i sono

$$\frac{1}{3!} \cdot \binom{20}{2} \cdot \binom{18}{2} \cdot \binom{16}{2}.$$

Per il singolo 4-ciclo possiamo usare direttamente la formula: abbiamo

$$\binom{14}{4} \cdot 3!$$

scelte.

Infine per i 5-cicli, ripetendo il ragionamento fatto per i 2-cicli, abbiamo

$$\frac{1}{2!}\cdot\binom{10}{5}4!\cdot\binom{5}{5}4!$$

scelte.

In totale il numero di permutazioni di tipo $2+2+2+4+5+5$ in $\mathcal{S}_20$ è

$$\frac{1}{3!}\cdot\binom{20}{2}\cdot\binom{18}{2}\cdot\binom{16}{2}\cdot\binom{14}{4}\cdot 3!\cdot\frac{1}{2!}\cdot\binom{10}{5}4!\cdot\binom{5}{5}4!.$$

▸ Ordine di una permutazione

Possiamo ora studiare l'ordine in $\mathcal{S}_n$ di una permutazione qualunque.

Proposizione 2.8.10 – Ordine di una permutazione

Sia $\sigma\in\mathcal{S}_n$ della forma $\sigma=\sigma_1\cdots\sigma_k$, dove i σ_i sono cicli disgiunti. Allora vale che

$$\operatorname{ord}_{\mathcal{S}_n}(\sigma)=\operatorname{lcm}\Big(\operatorname{ord}_{\mathcal{S}_n}(\sigma_i)\Big)_{i=1,\dots,k}.$$

Osservazione 2.8.3. Ricordiamo che l'ordine di una permutazione ciclica è la lunghezza del suo ciclo non banale: l'ordine di una permutazione qualunque è quindi il minimo comune multiplo delle lunghezze dei suoi cicli.

Dimostrazione. Sia $l_i:=\operatorname{ord}(\sigma_i)$ la lunghezza (ovvero l'ordine) dell'i-esimo ciclo, e sia $d=\operatorname{lcm}(l_1,\dots,l_n)$. Mostriamo che $\operatorname{ord}(\sigma)$ è un divisore di d e viceversa.

($\operatorname{ord}(\sigma)\mid d$) Mostriamo che $\sigma^d=\mathrm{id}$. In effetti

$$\sigma^d=(\sigma_1\cdots\sigma_k)^d=\sigma_1^d\cdots\sigma_k^d=\mathrm{id},$$

dove la seconda uguaglianza viene dal fatto che cicli disgiunti commutano, mentre l'ultima viene dal fatto che $l_i\mid d$ per ogni i, poiché d è il loro minimo comune multiplo.

($d\mid\operatorname{ord}(\sigma)$) Sia $m:=\operatorname{ord}(\sigma)$. Allora

$$\mathrm{id}=\sigma^m=(\sigma_1\cdots\sigma_k)^m=\sigma_1^m\cdots\sigma_k^m,$$

dove ancora una volta l'ultima uguaglianza segue dal fatto che cicli disgiunti commutano.

Siccome i cicli sono tutti disgiunti, ognuno di essi agirà in modo non banale su elementi diversi di $\{1,\dots,n\}$, dunque se la loro composizione fa l'identità (ovvero la permutazione che manda ogni elemento in sé) ogni σ_i^m deve essere l'identità. Segue quindi che $l_i\mid m$ per ogni i, dunque il loro minimo comune multiplo d divide $m=\operatorname{ord}(\sigma)$.

Segue quindi che $\operatorname{ord}(\sigma)=\operatorname{lcm}(l_1,\dots,l_n)$. □

Chiameremo **trasposizione** una permutazione ciclica il cui ciclo non banale abbia lunghezza 2, ovvero un 2-ciclo. Vale il seguente risultato.

Proposizione 2.8.11

$\mathcal{S}_n$ è generato dalle sue trasposizioni.

Dimostrazione. Devo mostrare che ogni permutazione è prodotto di trasposizioni (non necessariamente disgiunte). Siccome ogni permutazione è prodotto di cicli disgiunti, basta mostrare che le trasposizioni generano i cicli.

Sia allora $(a_1, \dots, a_k)$ un ciclo qualsiasi e mostriamo che

$$(a_1, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2).$$

Dato che le permutazioni sono semplicemente bigezioni di $\{1, \dots, n\}$ in sé, basta mostrare che hanno la stessa immagine mediante ogni elemento di $\{1, \dots, n\}$. Distinguiamo due casi.

- Se $j \in \{1, \dots, n\}$ è diverso da tutti gli a_i, allora entrambe le funzioni mandano j in sé.
- Se $j = a_i$ per qualche indice $1 \leq i \leq k$, allora il ciclo a sinistra manda $j = a_i$ in a_{i+1}. Il prodotto di trasposizioni a destra invece

$$j = a_i \xmapsto{(a_1,a_2)} a_i \mapsto \cdots \mapsto a_i \xmapsto{(a_1,a_i)} a_1 \xmapsto{(a_1,a_{i+1})} a_{i+1} \mapsto \cdots \mapsto a_{i+1}.$$

Dunque le due funzioni concordano su ogni elemento del dominio, dunque sono uguali. □

Osserviamo che la scrittura di una permutazione come prodotto di trasposizioni non è unica: infatti ad esempio

$$(1,2)(2,4) = (1,2)(3,4)(3,4)(2,4)$$

poiché $(3,4)^2 = \mathrm{id}$.

Tuttavia mostreremo che se una permutazione si scrive come prodotto di un numero pari di trasposizioni, ogni altra decomposizione avrà un numero pari di trasposizioni, e analogamente se il numero è dispari.

Per far ciò definiamo la funzione **segno**.

Definizione 2.8.12 – Segno di una permutazione

Si dice segno di una permutazione la mappa

$$\begin{aligned} \operatorname{sgn} : \mathcal{S}_n &\to \{\pm 1\} \\ \sigma &\mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}. \end{aligned}$$

Proposizione 2.8.13

La funzione segno è un omomorfismo di gruppi. Inoltre se τ è una trasposizione si ha che $\operatorname{sgn}(\tau) = -1$.

Dimostrazione. ▸ BUONA DEFINIZIONE Mostriamo innanzitutto che per ogni $\sigma \in \mathcal{S}_n$ si ha che $\operatorname{sgn}(\sigma) \in \pm 1$.

Siccome σ è una bigezione, a numeratore e a denominatore troveremo tutti i numeri

della forma $i - j$ o al più $j - i$: il risultato è quindi 1 oppure -1.

▸ OMOMORFISMO Siano $\sigma, \rho \in \mathcal{S}_n$. Allora

$$\begin{aligned}\operatorname{sgn}(\sigma\rho) &= \prod_{i<j} \frac{\sigma\rho(i) - \sigma\rho(j)}{i - j} \\ &= \prod_{i<j} \frac{\sigma\rho(i) - \sigma\rho(j)}{\rho(i) - \rho(j)} \cdot \frac{\rho(i) - \rho(j)}{i - j} \\ &= \left(\prod_{i<j} \frac{\sigma\rho(i) - \sigma\rho(j)}{\rho(i) - \rho(j)}\right) \cdot \left(\prod_{i<j} \frac{\rho(i) - \rho(j)}{i - j}\right) \\ &= \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\rho),\end{aligned}$$

dove l'ultimo passaggio viene dal fatto che applicando ρ a tutti gli elementi di $\{1, \dots, n\}$ ottengo ancora una volta tutti gli elementi di $\{1, \dots, n\}$ (ρ è bigettiva).

▸ SEGNO DELLE TRASPOSIZIONI Sia $\tau = (a, b)$ una trasposizione e studiamo il segno dei vari fattori di

$$\prod_{i<j} \frac{\tau(i) - \tau(j)}{i - j}.$$

- Se $\{i, j\} \cap \{a, b\} = \varnothing$ (ovvero i e j sono distinti da a, b) si ha che $\tau(i) = i$, $\tau(j) = j$ e quindi
$$\frac{\tau(i) - \tau(j)}{i - j} = \frac{i - j}{i - j} = 1.$$
- Per ogni coppia della forma $\{i, a\}$, $i \neq b$, il cui "segno" è
$$\frac{\tau(i) - \tau(a)}{i - a} = \frac{i - b}{i - a},$$
esiste la coppia complementare $\{i, b\}$ il cui segno è
$$\frac{\tau(i) - \tau(b)}{i - b} = \frac{i - a}{i - b}.$$
Il prodotto di queste due è 1, dunque tutte le coppie di questo tipo contribuiscono con un segno positivo.
- La coppia $\{a, b\}$ ha segno
$$\frac{\tau(a) - \tau(b)}{a - b} = \frac{b - a}{a - b} = -1.$$

Il segno della trasposizione τ è quindi -1. □

Definizione 2.8.14 – Parità di una permutazione

Una permutazione $\sigma \in \mathcal{S}_n$ si dice **pari** se $\operatorname{sgn}(\sigma) = 1$, dispari se $\operatorname{sgn}(\sigma) = -1$.

Definizione 2.8.15 – Gruppo alterno

Si dice **gruppo alterno** su n elementi il sottogruppo

$$\mathcal{A}_n := \ker \operatorname{sgn} = \{\, \sigma \in \mathcal{S}_n \;:\; \operatorname{sgn}(\sigma) = 1 \,\}.$$

Il gruppo $\mathcal{A}_n$ è quindi il gruppo di tutte le permutazioni pari. Osserviamo che, essendo il nucleo di un omomorfismo, esso è normale in $\mathcal{S}_n$: inoltre per il Primo Teorema di Omomorfismo si ha che

$$\mathcal{S}_n / \mathcal{A}_n \simeq \{\pm 1\},$$

da cui segue che $\#\mathcal{A}_n = \frac{n!}{2}$.

Proposizione 2.8.16

Un k-ciclo è pari se e solo se k è dispari.

Dimostrazione. Un k-ciclo $\sigma = (a_1, \dots, a_k)$ è il prodotto di $k-1$ trasposizioni τ_i della forma

$$\sigma = (a_1, a_k) \cdots (a_1, a_2).$$

Allora

$$\operatorname{sgn}(\sigma) = \prod_{i=1}^{k} \operatorname{sgn}(\tau_i) = (-1)^{k-1},$$

che è uguale ad 1 se e solo se $k-1$ è pari, ovvero k è dispari. □

2.8.1 Classi di coniugio in $\mathcal{S}_n$

Il coniugio in $\mathcal{S}_n$ è un'operazione molto più semplice da realizzare di quanto possa sembrare inizialmente. Vale infatti il seguente risultato.

Lemma 2.8.17 – Coniugio in $\mathcal{S}_n$

Siano $\sigma, \tau \in \mathcal{S}_n$ qualsiasi, con σ della forma

$$\sigma = (c_{11}, \dots, c_{1,l_1})(\dots)(c_{k1}, \dots, c_{k,l_k}).$$

Allora

$$\tau\sigma\tau^{-1} = (\tau(c_{11}), \dots, \tau(c_{1,l_1}))(\dots)(\tau(c_{k1}), \dots, \tau(c_{k,l_k})),$$

ovvero $\tau\sigma\tau^{-1}$ si ottiene applicando τ ad ogni elemento dei cicli di σ.

Dimostrazione. Innanzitutto considero il caso in cui σ sia composta da un unico ciclo, ovvero $k = 1$. La tesi è che se $\sigma = (c_1, \dots, c_l)$ allora

$$\tau\sigma\tau^{-1} = (\tau(c_1), \dots, \tau(c_l)).$$

Per dimostrare la tesi basta far vedere che le due funzioni concordano per ogni elemento del dominio $\{1, \dots, n\}$: consideriamo quindi due casi.

- Se $j \in \{1, \dots, n\}$ è diverso da $\tau(c_i)$ per ogni $i = 1, \dots, l$, dobbiamo mostrare che entrambe le funzioni lo mandano in sé. Sicuramente quella del secondo membro manda j in sé.

Per quanto riguarda $\tau\sigma\tau^{-1}$, osserviamo che siccome $j \neq \tau(c_i)$ segue che $\tau^{-1}(j) \neq c_i$ per ogni i, ovvero j non compare nel ciclo non banale di σ, da cui

$$\sigma\tau^{-1}(j) = \tau^{-1}(j).$$

Segue quindi che $\tau\sigma\tau^{-1}(j) = \tau\tau^{-1}(j) = j$, come volevamo.

- Sia invece $j \in \{1, \dots, n\}$ tale che $j = \tau(c_i)$ per qualche $i = 1, \dots, k$ e mostriamo che l'immagine di j mediante le due funzioni è la stessa.

  L'immagine mediante la seconda funzione è

  $$\tau(c_i) \xmapsto{(\tau(c_1),\dots,\tau(c_i),\tau(c_{i+1}),\dots,\tau(c_k))} \tau(c_{i+1}).$$

  Invece l'immagine mediante la prima funzione è

  $$\tau(c_i) \overset{\tau^{-1}}{\longmapsto} c_i \overset{\sigma}{\mapsto} c_{i+1} \overset{\tau}{\mapsto} \tau(c_{i+1}),$$

  e dunque le due immagini sono uguali.

Segue quindi che le due funzioni sono uguali.
Se invece $\sigma = \sigma_1 \cdots \sigma_k$, basta osservare che

$$\begin{aligned}\tau\sigma\tau^{-1} &= \tau \cdot (\sigma_1 \cdots \sigma_k) \cdot \tau^{-1} \\ &= \tau \cdot \left(\sigma_1(\tau^{-1}\tau)\sigma_2(\tau^{-1}\tau)\cdots(\tau^{-1}\tau)\sigma_k\right) \cdot \tau^{-1} \\ &= (\tau\sigma_1\tau^{-1}) \cdot (\tau\sigma_2\tau^{-1}) \cdots (\tau\sigma_k\tau^{-1}).\end{aligned}$$

Ma i σ_i sono formati da un singolo ciclo, dunque per quanto dimostrato prima segue la tesi. □

Teorema 2.8.18 – Classi di coniugio in $\mathcal{S}_n$

Due permutazioni di $\mathcal{S}_n$ sono coniugate se e solo se hanno lo stesso tipo.

Dimostrazione. Dimostriamo entrambi i versi dell'implicazione.

$\boxed{\Longrightarrow}$ Per il Lemma 2.8.17 se $\rho = \tau\sigma\tau^{-1}$, allora ρ si ottiene da σ facendo agire τ su ogni elemento che compone i cicli di σ, dunque ρ ha lo stesso tipo di σ.

$\boxed{\Longleftarrow}$ Siano

$$\begin{aligned}\sigma &:= (a_{11}, \dots, a_{1,l_1})(\dots)(a_{k1}, \dots, a_{k,l_k}) \\ \rho &:= (b_{11}, \dots, b_{1,l_1})(\dots)(b_{k1}, \dots, b_{k,l_k})\end{aligned}$$

e mostriamo che σ e ρ sono coniugate.

Definiamo allora $\tau \in \mathcal{S}_n$ come la permutazione tale che $\tau(a_{ij}) = b_{ij}$ per ogni $i = 1, \dots, k$, $j = 1, \dots, l_i$. Tale funzione è ben definita ed è una bigezione di $\{1, \dots, n\}$ in sé, in quanto nella scrittura di σ dovranno comparire tutti gli elementi di $\{1, \dots, n\}$ una e una sola volta, e stessa cosa per gli elemnti di ρ.

Per il Lemma 2.8.17 segue quindi che $\tau\sigma\tau^{-1} = \rho$. □

Corollario 2.8.19

Valgono le seguenti affermazioni.

(1) Il numero di classi di coniugio di $\mathcal{S}_n$ è uguale al numero di partizioni di $n \in \mathbb{N}$ come somma di numeri interi positivi.

(2) Sia $H \leq \mathcal{S}_n$. Allora $H \triangleleft \mathcal{S}_n$ se e solo se per ogni $\sigma \in H$, H contiene tutte le partizioni con lo stesso tipo di σ.

Dimostrazione. (1) Una classe di coniugio in $\mathcal{S}_n$ è rappresentata da tutte le permutazioni con un determinato tipo, e un tipo è una partizione di n come somma di interi positivi.

(2) $H \triangleleft \mathcal{S}_n$ se e solo se è unione di intere classi di coniugio, ovvero se e solo se è unione di interi tipi di permutazioni.

□

2.9 DECOMPOSIZIONE IN PRODOTTI DIRETTI E SEMIDIRETTI

Abbiamo studiato in passato cosa sia il prodotto diretto di due gruppi G e H e quali proprietà ha. Vogliamo ora trovare delle condizioni per cui un gruppo possa essere decomposto nel prodotto diretto di suoi sottogruppi.

Iniziamo con due semplici lemmi.

Lemma 2.9.1

Se $H \triangleleft G$, $K \leq G$ allora $HK = KH$ e dunque segue che $HK \leq G$.

Dimostrazione. Siccome $H \triangleleft G$ si ha che $gH = Hg$ per ogni $g \in G$, dunque $kH = Hk$ per ogni $k \in K \leq G$, ovvero $KH = HK$. Per il **??** segue quindi che $HK = KH \leq G$. □

Lemma 2.9.2

Siano $H, K \triangleleft G$ tali che $H \cap K = \{ e_G \}$. Allora gli elementi di H e K commutano, ovvero

$$HK = KH.$$

Dimostrazione. È sufficiente mostrare che per ogni $h \in H, k \in K$ vale $hk = kh$, ovvero $[h, k] = hkh^{-1}k^{-1} = e_G$. Osserviamo che per associatività

$$[h, k] = h(kh^{-1}k^{-1}) = (hkh^{-1})k^{-1}.$$

Il primo è un elemento di H, in quanto è il prodotto di $h \in H$ e $kh^{-1}k^{-1} \in kHk^{-1}$, che è uguale ad H poiché H è normale in G.

Analogamente si mostra che $(hkh^{-1})k^{-1}$ è un elemento di K.

Dunque, essendo entrambi uguali al commutatore $[h, k]$, segue che $[h, k] \in H \cap K = \{ e_G \}$, ovvero $hk = kh$, come volevamo. □

Possiamo quindi enunciare e dimostrare il Teorema di Decomposizione nel Prodotto Diretto.

Teorema 2.9.3 – Decomposizione nel prodotto diretto

Sia G un gruppo, $H, K \leq G$ tali che

(1) $H, K \triangleleft G$,

(2) $HK = G$,

(3) $H \cap K = \{ e_G \}$.

Allora $G \simeq H \times K$.

Dimostrazione. Consideriamo la mappa

$$\begin{aligned} \varphi : H \times K &\longrightarrow G \\ (h, k) &\mapsto hk. \end{aligned}$$

Ovviamente la mappa è ben definita (poiché $H, K \leq G$ e G è chiuso per prodotto). Mostriamo quindi che è un isomorfismo di gruppi.

▸ OMOMORFISMO Siano $(h_1, k_1), (h_2, k_2) \in H \times K$. Allora

$$\begin{aligned} \varphi((h_1, k_1)(h_2, k_2)) &= \varphi((h_1 h_2, k_1 k_2)) \\ &= h_1 h_2 k_1 k_2. \end{aligned}$$

Dato che $H \cap K = \{ e_G \}$ si applica il **??**, da cui segue che

$$\begin{aligned} &= (h_1 k_1) \cdot (h_2 k_2) \\ &= \varphi((h_1, k_1)) \cdot \varphi((h_2, k_2)). \end{aligned}$$

▸ SURGETTIVITÀ Segue banalmente dall'ipotesi che $G = HK$.

▸ INIETTIVITÀ Si ha che

$$\ker \varphi = \{ (h, k) \in H \times K \ : \ \varphi((h, k)) = hk = e_G \}.$$

Tuttavia essendo $h, k \in G$ si ha che il loro prodotto è l'identità se e solo se $h = k^{-1}$, da cui (siccome $h \in H$, $k^{-1} \in K$) segue che $h, k \in H \cap K = \{ e_G \}$. Segue quindi che $\ker \varphi = \{ (e_G, e_G) \}$, ovvero φ è iniettivo.

Segue quindi che φ è un isomorfismo di gruppi, come volevamo. □

Una possibile applicazione è la seguente proposizione.

Proposizione 2.9.4

Gli unici gruppi di ordine p^2 (a meno di isomorfismo) sono

$$\mathbb{Z}/p^2\mathbb{Z}, \qquad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Dimostrazione. Sia G di ordine p^2. Abbiamo già dimostrato che ogni p-gruppo di ordine p^2 è abeliano. Inoltre G è ciclico allora $G \simeq \mathbb{Z}/p^2\mathbb{Z}$: supponiamo dunque che G non sia ciclico e mostriamo che $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Siccome G ha ordine p^2, i suoi elementi hanno ordine 1, p oppure p^2. L'unico elemento

di ordine 1 è l'identità, non esistono elementi di ordine p^2 poiché altrimenti G sarebbe ciclico, dunque segue che ogni elemento di G diverso dall'identità deve avere ordine p.
Sia quindi $x \in G$ di ordine p e sia $H := <x>$; sia inoltre $y \in G \setminus <x>$ e sia $K := <y>$. Facciamo alcune osservazioni.

- H e K sono normali in G poiché G è abeliano;
- $H \cap K$ è il gruppo banale: infatti $H \cap K$ è un sottogruppo di H e di K, dunque l'ordine di $H \cap K$ deve dividere $|H| = |K| = p$. Dunque deve valere che $H = K = H \cap K$ oppure $H \cap K = \{ e_G \}$, tuttavia la prima opzione è impossibile in quanto $H = <x>$, $K = <y>$ e $y \notin <x>$.
- Vale che
$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K| = p^2 = |G|,$$
dunque $G = HK$.

Per il Teorema 2.9.3 segue quindi che $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

Abbiamo quindi un modo per decomporre un gruppo nel prodotto diretto di due gruppi. Notiamo che a partire da gruppi abeliani, il prodotto diretto genera sempre gruppi abeliani: è impossibile decomporre gruppi non abeliani sottoforma di prodotto diretto di gruppi abeliani. Abbiamo quindi bisogno di un altro modo per costruire nuovi gruppi.

Definizione 2.9.5 – Prodotto semidiretto

Siano H, K due gruppi e sia
$$\begin{aligned} \varphi : K &\longrightarrow \mathrm{Aut}(H) \\ k &\longmapsto \varphi(k) = \varphi_k \end{aligned}$$
un'azione di K su H. Si dice **prodotto semidiretto** di H e K via φ (e lo si indica $H \rtimes_\varphi K$) il gruppo avente

- come insieme sottostante il prodotto cartesiano $H \times K$,
- come legge di composizione la legge
$$(h, k)(h', k') := (h\varphi_k(h'), kk').$$

Mostriamo che $H \rtimes_\varphi K$ è effettivamente un gruppo.

▸ BUONA DEFINIZIONE Osserviamo che se $(h, k), (h', k') \in H \rtimes_\varphi K$ allora
$$(h, k)(h', k') = (h\varphi_k(h'), kk') \in H \rtimes_\varphi K$$
poiché $\varphi_k \in \mathrm{Aut}(H)$, dunque $h\varphi_k(h') \in H$.

▸ **ASSOCIATIVITÀ** Siano $(x,y),(z,t),(h,k) \in H \rtimes_\varphi K$. Allora

$$\begin{aligned}\big((x,y)(z,t)\big)(h,k) &= \big(x \cdot \varphi(y)(z), yt\big)(h,k)\\ &= \big(x \cdot \varphi(y)(z) \cdot \varphi(yt)(h), ytk\big)\\ &= \Big(x \cdot \varphi(y)(z) \cdot \varphi(y)\big(\varphi(t)(h)\big), ytk\Big)\\ &= \Big(x \cdot \varphi(y)\big(z \cdot \varphi(t)(h)\big), ytk\Big)\\ &= (x,y)\big(z \cdot \varphi(t)(h), tk\big)\\ &= (x,y)\big((z,t)(h,k)\big),\end{aligned}$$

dunque l'operazione è associativa.

▸ **ELEMENTO NEUTRO** L'elemento neutro per $H \rtimes_\varphi K$ è (e_H, e_K). Infatti per ogni $(h,k) \in H \rtimes_\varphi K$ si ha che

$$(h,k)(e_H,e_K) = (h \cdot \varphi(k)(e_H), k \cdot e_K) = (h \cdot e_H, k \cdot e_K) = (h,k).$$
$$(e_H,e_K)(h,k) = (e_H \cdot \varphi(e_K)(h), e_K \cdot k) = (e_H \cdot h, e_K \cdot k) = (h,k).$$

Nel primo caso abbiamo usato il fatto che $\varphi(k) = \varphi_k$ è un omomorfismo, dunque l'immagine di e_H deve essere l'identità, mentre nel secondo caso abbiamo sfruttato il fatto che, essendo φ un omomorfismo, $\varphi(e_K)$ è l'identità di $\mathrm{Aut}(H)$, ovvero $\varphi(e_K) = \mathrm{id}$.

▸ **INVERSI** Sia $(h,k) \in H \rtimes_\varphi K$: mostriamo che $\Big(\varphi_{k^{-1}}(h^{-1}), k^{-1}\Big)$ è l'inverso di (h,k). In effetti

$$\begin{aligned}(h,k)\Big(\varphi_{k^{-1}}(h^{-1}), k^{-1}\Big) &= \Big(h \cdot \varphi_k\big(\varphi_{k^{-1}}(h^{-1})\big), kk^{-1}\Big)\\ &= \big(h \cdot \varphi_{kk^{-1}}(h^{-1}), e_K\big)\\ &= (hh^{-1}, e_K)\\ &= (e_H, e_K).\\ \Big(\varphi_{k^{-1}}(h^{-1}), k^{-1}\Big)(h,k) &= \Big(\varphi_{k^{-1}}(h^{-1}) \cdot \varphi_{k^{-1}}(h), k^{-1}k\Big)\\ &= \Big(\varphi_{k^{-1}}(h^{-1}h), e_K\Big)\\ &= (e_H, e_K).\end{aligned}$$

Osservazione 2.9.1. Il prodotto diretto è un caso particolare del prodotto semidiretto. Infatti un prodotto semidiretto $H \rtimes_\varphi K$ è diretto se e solo se

$$(hh', kk') = (h,k)(h',k') = (h\varphi_k(h'), kk'),$$

ovvero se e solo se $h' = \varphi_k(h')$ per ogni $h' \in H$, $k \in K$. Ma questo significa che φ_k è l'identità per ogni $k \in K$, ovvero che l'azione di K su H è l'azione banale

$$\begin{aligned}\varphi : K &\to \mathrm{Aut}(H)\\ k &\mapsto \mathrm{id}_H .\end{aligned}$$

Analogamente al prodotto diretto, sotto alcune condizioni possiamo scomporre un gruppo nel prodotto semidiretto di alcuni suoi sottogurppi.

Teorema 2.9.6 – Decomposizione nel prodotto semidiretto

Sia G un gruppo, $H, K \leq G$ tali che

(1) $H \triangleleft G$,

(2) $G = HK$,

(3) $H \cap K = \{ e_G \}$.

Allora

$$G \simeq H \rtimes_\varphi K,$$

dove φ è l'azione di K su H per coniugio, ovvero

$$\begin{aligned} \varphi : K &\longrightarrow \mathrm{Aut}(H) \\ k &\mapsto \varphi_k = (h \mapsto khk^{-1}). \end{aligned}$$

3

Teoria degli Anelli

3.1 ANELLI ED IDEALI

Riprendiamo la nostra trattazione degli anelli ricordandone la definizione: un insieme A insieme a due operazioni $+$ e $\cdot$ si dice *anello* se

- $(A, +)$ è un gruppo abeliano;
- l'operazione di prodotto è associativa;
- vale la proprietà distributiva del prodotto sulla somma.

Un anello si dice *commutativo* se anche l'operazione di prodotto è commutativa; inoltre si dice che l'anello è *con identità* se esiste un elemento $1_A \in A$ che fa da elemento neutro per il prodotto.

Vogliamo ora studiare più approfonditamente le sottostrutture di un anello.

Definizione 3.1.1 – Sottoanello

Sia A un anello. $B \subseteq A$ si dice *sottoanello* di A se B è chiuso rispetto alle operazioni $+$ e $\cdot$.

Notiamo che non viene richiesto che l'anello sia commutativo o con identità: se fosse commutativo allora necessariamente anche il sottoanello sarebbe commutativo, mentre se A fosse con identità non è detto che B contiene l'identità.

Dato un anello A, un elemento $a \in A$ e un sottoinsieme $X \subseteq A$, indicheremo con aX e con Xa rispettivamente gli insiemi

$$aX := \{ ax : x \in X \} \subseteq A,$$
$$Xa := \{ xa : x \in X \} \subseteq A.$$

Questa operazione è fondamentale per descrivere la sottostruttura più importante degli anelli, cioè gli ideali.

Definizione 3.1.2 – Ideale

Sia A un anello, $I \subseteq A$. Si dice che I è un *ideale sinistro* di A se

- $(I, +)$ è un sottogruppo di $(A, +)$;
- per ogni $a \in A$ vale che $aI \subseteq I$.

Si dice che I è un *ideale destro* di A se

- $(I, +)$ è un sottogruppo di $(A, +)$;
- per ogni $a \in A$ vale che $Ia \subseteq I$.

Infine si dice che I è un *ideale bilatero* di A se I è sia ideale sinistro che ideale destro.

La proprietà $aI \subseteq I$, che può anche essere riscritta come

$$\text{per ogni } a \in A, x \in I \text{ vale che } ax \in I,$$

viene detta *proprietà di assorbimento*.

Osserviamo che nel caso di un anello commutativo ogni ideale è bilatero.

Esempio 3.1.3. $n\mathbb{Z}$ è un ideale di $\mathbb{Z}$ per ogni $n \in \mathbb{N}$.

Esempio 3.1.4. Dato un qualsiasi anello A, gli insiemi $\{0\}$ e A sono ideali di A, e vengono chiamati rispettivamente *ideale banale* e *ideale improprio*.

Osserviamo anche che, se l'anello ha identità, per mostrare che $I \subseteq A$ è un ideale basta mostrare che è chiuso per somma e che vale la proprietà di assorbimento. Infatti se vale la proprietà di assorbimento allora $-1I \subseteq I$, dunque gli inversi di tutti gli elementi sono contenuti nell'ideale.

Mostriamo alcune proprietà degli ideali.

Proposizione 3.1.5

Sia A un anello commutativo con identità e sia I un suo ideale. Valgono i seguenti fatti.

(i) I è un ideale proprio se e solo se $I \cap A^\times = \varnothing$. In particolare un ideale che contiene l'identità è sempre tutto l'anello.

(ii) A è un campo se e solo se non ha ideali propri non banali.

Dimostrazione. Mostriamo entrambe le affermazioni.

(i) Supponiamo che esista $x \in I \cap A^\times$. Siccome x è invertibile esisterà $y \in A$ tale che $xy = 1$. Quindi $1 = xy \in I$; da questo segue che per ogni $a \in A$ l'elemento

$$a = a \cdot 1 = a(xy) \in I,$$

da cui $A \subseteq I$. Ma I è un sottoinsieme di A, da cui necessariamente $I = A$.

(ii) Siccome per definizione A un campo se e solo se $A^\times = A \setminus \{0\}$, per il punto precedente l'unico ideale proprio è $\{0\}$, da cui la tesi. □

3.1.1 Operazioni sugli ideali

Sia A un anello (per semplicità commutativo e con identità): cerchiamo di capire quali operazioni possiamo compiere sui suoi sottoinsiemi e sui suoi ideali per ottenere altri ideali.

Ideale generato da un sottoinsieme

Definizione 3.1.6 – Ideale generato

Sia $S \subseteq A$ non vuoto. Si dice *ideale generato da* S l'insieme

$$(S) := \left\{ \sum_{i=1}^{n} a_i s_i \ : \ n \in \mathbb{N}, a_i \in A, s_i \in S \right\}.$$

Verifichiamo che questa costruzione è effettivamente un ideale.

Sottogruppo Siano $x, y \in (S)$, ovvero

$$x = \sum_{i=1}^{n} a_i s_i, \qquad y = \sum_{j=1}^{m} \alpha_j \sigma_j$$

con $a_i, \alpha_j \in A$, e $s_i, \sigma_j \in S$. Allora evidentemente $x + y$ è una somma di termini della forma as con $a \in A$, $s \in S$, da cui segue che $x + y \in (S)$.

Assorbimento Sia $x \in (S)$ e $a \in A$. Allora

$$ax = a \sum_{i=1}^{n} a_i s_i = \sum_{i=1}^{n} (a a_i) s_i \in (S)$$

poiché $a a_i \in A$.

Esempio 3.1.7. Se $S = \{x\}$, allora $(x) = \{ax : a \in A\} = Ax$.

Esempio 3.1.8. L'insieme dei multipli di n, cioè $n\mathbb{Z}$, è un ideale generato da un singolo elemento (in particolare $n\mathbb{Z} = (n)$).

In particolare un ideale generato da un solo elemento si dice **ideale principale**.

Enunciamo ora una proposizione che caratterizza gli ideali generati da un sottoinsieme come *il più piccolo ideale* che contiene quel sottoinsieme; la dimostreremo poco avanti.

Proposizione 3.1.9

Sia A un anello, $S \subseteq A$ un suo sottoinsieme qualunque. Allora (S) è il più piccolo ideale che contiene S, ovvero

$$(S) = \bigcup_{\substack{I \text{ ideale di } A \\ S \subseteq I \subseteq A}} I.$$

Intersezione di due ideali

Siano $I, J \subseteq A$ due ideali di A. Mostriamo che $I \cap J$ è ancora un ideale di A.

Sottogruppo Siccome $I, J \leq (A, +)$ segue che $I \cap J \leq (A, +)$.

Assorbimento Sia $a \in A$. Allora per ogni $x \in I \cap J$ vale che $ax \in I$ e $ax \in J$ poiché I e J sono ideali. Da questo segue dunque che $ax \in I \cap J$.

Esempio 3.1.10. $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$: infatti l'intersezione tra i multipli di n e di m è l'insieme dei multipli del loro minimo comune multiplo.

Possiamo ora dimostrare la Proposizione 3.1.9.

Dimostrazione della Proposizione 3.1.9. Innanzitutto siccome (S) è un ideale che contiene S segue che

$$(S) \supseteq \bigcup_{\substack{I \text{ ideale di } A \\ S \subseteq I \subseteq A}} I.$$

Mostriamo ora il contenimento contrario: sia $x \in (S)$ qualunque. Allora per ogni I ideale di A che contiene S vale che

$$x = \sum_{i=1}^{n} a_i s_i \in I,$$

poiché

- gli s_i appartengono ad S che è contenuto in I;
- $a_i s_i \in I$ per ogni $a_i \in A$ per la proprietà di assorbimento;
- la somma di termini in I è ancora un elemento di I in quanto è un gruppo con la somma.

Segue quindi che $x \in I$ per qualsiasi ideale I contenente S, dunque x dovrà appartenere alla loro intersezione, da cui

$$(S) \subseteq \bigcup_{\substack{I \text{ ideale di } A \\ S \subseteq I \subseteq A}} I.$$

Segue quindi che i due insiemi sono uguali, ovvero la tesi. □

Somma di ideali

Definiamo la somma tra due sottoinsiemi di A come

$$I + J := \{ x + y \ : \ x \in I, y \in J \}.$$

Proposizione 3.1.11 – Somma di ideali

Siano I, J due ideali di A. Allora $I + J$ è ancora un ideale di A ed in particolare vale che

$$I + J = (I, J).$$

Dimostrazione. Basta mostrare il secondo punto: da esso discende direttamente il primo.

Innanzitutto $I + J \subseteq (I, J)$ in quanto nel secondo vi sono tutte le possibili somme tra elementi di I e di J.

Inoltre possiamo notare che $I \subseteq I + J$ e $J \subseteq I + J$ (basta sceglere come elemento rispettivamente di J e di I lo zero), dunque $I + J$ contiene necessariamente il più piccolo ideale che contiene sia I che J, ovvero (per la Proposizione 3.1.9) $I + J \supseteq (I, J)$, da cui la tesi. □

Esempio 3.1.12. $m\mathbb{Z} + n\mathbb{Z} = (m\mathbb{Z}, n\mathbb{Z}) = (m, n)\mathbb{Z}$. Mostriamo infatti che gli elementi di $m\mathbb{Z} + n\mathbb{Z}$ sono tutti e soli i multipli del massimo comun divisore tra m e n.

Se $x \in m\mathbb{Z} + n\mathbb{Z}$ allora $x = mk + nh$ per qualche $k, h \in \mathbb{Z}$. Sia $d := (m, n)$: allora

$$x = m'dk + n'dh = (m'k + n'h)d \in d\mathbb{Z}.$$

Mostriamo ora l'inclusione contraria: supponiamo $x = dz$ per qualche $z \in \mathbb{Z}$. Per Bézout esistono x_0 e y_0 tali che $d = x_0 m + y_0 n$. Moltiplicando entrambi i membri per z otteniamo

$$x = dx = (x_0 z)m + (y_0 z)n \in m\mathbb{Z} + n\mathbb{Z},$$

che è la tesi.

Ideale generato dai prodotti

Se I e J sono ideali di A, si definisce l'ideale prodotto IJ come l'ideale generato da tutti i prodotti di elementi di I per elementi di J, ovvero

$$IJ := (\{ xy \ : \ x \in I, y \in J \}).$$

Per definizione IJ è un ideale.

Esempio 3.1.13. $m\mathbb{Z} \cdot n\mathbb{Z} = (mn)\mathbb{Z}$.

Radicale di un ideale

Sia I un ideale di A. Si dice *radicale di* I l'insieme

$$\sqrt{I} := \{ x \in A : x^n \in I \text{ per qualche } n \in \mathbb{N} \}.$$

Mostriamo che il radicale di un ideale è sempre un ideale.

Sottogruppo Siano $x, y \in \sqrt{I}$, ovvero esistono $n, m \in \mathbb{N}$ tali che $x^n, y^m \in I$. Per mostrare che $x + y \in \sqrt{I}$ è sufficiente mostrare che esiste un $d \in \mathbb{N}$ tale che $(x + y)^d \in I$.

Prendiamo $d := n + m$. Allora per il Binomio di Newton (che vale poiché l'anello è commutativo)

$$(x + y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^i y^{n+m-i}.$$

Osserviamo che per ogni i compreso tra 0 e $n + m$ si ha necessariamente una delle seguenti:

- $i \geq n$, da cui $x^i \in I$ e dunque (per la proprietà di assorbimento di I) anche $x_i \cdot y^{n+m-i} \in I$;
- $n + m - i \geq m$, da cui $y^{n+m-i} \in I$ e dunque (per la proprietà di assorbimento di I) anche $x_i \cdot y^{n+m-i} \in I$.

Assorbimento Sia $a \in A$ e sia $x \in \sqrt{I}$ qualunque (cioè $x^n \in I$ per qualche $n \in \mathbb{N}$). Allora vale che $(ax)^n = a^n x^n \in I$, ovvero $ax \in \sqrt{I}$.

Divisione tra ideali

Siano I, J ideali di A. Si dice *divisione tra* I *e* J l'operazione tra ideali data da

$$(I : J) := \{ x \in A : xJ \subseteq X \}.$$

Mostriamo che $(I : J)$ è ancora un ideale di A.

Sottogruppo Siano $x, y \in (I : J)$. Allora

$$(x + y)J \subseteq xJ + yJ \subseteq I$$

dove l'ultima inclusione viene dal fatto che I è chiuso per somma.

Assorbimento Sia $a \in A$, $x \in (I : J)$. Allora

$$axJ = a(xJ) \subseteq aI \subseteq I,$$

da cui $ax \in (I : J)$.

3.2 OMOMORFISMI DI ANELLO

Ricordiamo che se A, B sono anelli (commutativi con identità), allora $f : A \to B$ si dice **omomorfismo di anelli** se

(1) $f(1_A) = 1_B$.

(2) Per ogni $a, b \in A$ vale che $f(a + b) = f(a) + f(b)$.

(3) Per ogni $a, b \in A$ vale che $f(ab) = f(a)f(b)$.

Osserviamo che la prima condizione non è automatica dalle altre due, a meno che B non sia un dominio di integrità.

Come nel caso degli omomorfismi di gruppi possiamo considerare il nucleo e l'immagine di un omomorfismo di anelli; possiamo quindi chiederci se si può generalizzare l'idea dei gruppi quoziente e del Primo Teorema degli Omomorfismi agli anelli.

Anelli quoziente

Sia A un anello, $I \subseteq A$ un ideale. Sicuramente A/I è un gruppo, in quanto I è un sottogruppo di $(A,+)$ ed essendo l'operazione di somma commutativa I è necessariamente normale. Osserviamo che possiamo anche dare naturalmente un'operazione di prodotto all'insieme quoziente: date due classi laterali $a+I$ e $b+I$ si definisce

$$(a+I)(b+I) \coloneqq ab+I.$$

Possiamo verificare che questa operazione è ben definita e valgono gli assiomi degli anelli, da cui $(A/I,+,\cdot)$ è ancora un anello, detto **anello quoziente**.

Come nel caso dei gruppi esiste un omomorfismo

$$\begin{aligned}\pi_I : A &\to A/I \\ a &\mapsto a+I\end{aligned}$$

detto **proiezione al quoziente**. Come nel caso dei gruppi, la sua immagine è $\operatorname{Im}\pi_n = A/I$ (ovvero π_I è surgettivo) mentre il suo nucleo è $\ker\pi_I = I$. Vale quindi un analogo della **??**.

Proposizione 3.2.1

Sia A un anello. Allora $I \subseteq A$ è un ideale se e solo se è il nucleo di un omomorfismo definito su A.

Dimostrazione. Per il "solo se" basta notare che ogni ideale è il nucleo della proiezione al quoziente π_I. Per l'altra implicazione basta mostrare che se f è un omomorfismo di anelli con dominio A allora $\ker f$ è un ideale di A.

Sottogruppo Il nucleo di un omomorfismo è sempre un sottogruppo del gruppo additivo di un anello.

Assorbimento Sia $a \in A$ qualunque, $x \in \ker f$. Allora

$$f(ax) = f(a)f(x) = f(a)\cdot 0 = 0,$$

ovvero $ax \in \ker f$. □

3.2.1 Teoremi di omomorfismo

Valgono quindi delle versioni analoghe dei teoremi di omomorfismo per i gruppi.

Teorema 3.2.2 – Primo Teorema degli Omomorfismi

Siano A, B due anelli e sia $f : A \to B$ un omomorfismo di anelli. Sia inoltre I un ideale di A contenuto in $\ker f$.

Allora esiste un unico omomorfismo $\varphi : A/I \to B$ per cui il seguente diagramma commuta:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \pi_I}\downarrow & \nearrow_{\varphi} & \\ A/I & & \end{array} \tag{3.1}$$

Inoltre vale che

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

In particolare se $I = \ker f$ allora φ è iniettiva.

Dimostrazione. Siccome A, B e I sono in particolare gruppi, per il Primo Teorema di Omomorfismo (per gruppi) sappiamo che esiste un unico omomorfismo di gruppi φ con le proprietà sopra elencate. Mostriamo che φ è un omomorfismo di anelli.

Siano $a + I, b + I \in A/I$ qualunque. Allora

$$\begin{aligned}\varphi\big((a+I)(b+I)\big) &= \varphi\big(ab+I\big)\\ &= \varphi\big(\pi_I(ab)\big)\\ &= f(ab)\\ &= f(a)f(b)\\ &= \varphi\big(\pi_I(a)\big)\varphi\big(\pi_I(b)\big)\\ &= \varphi\big(a+I\big)\varphi\big(b+I\big).\end{aligned}$$

□

Da questo teorema deriva immediatamente anche il Secondo Teorema di Omomorfismo.

Teorema 3.2.3 – Secondo Teorema degli Omomorfismi

Sia A un anello e siano I, J due ideali di A, con $I \subseteq J$. Allora

$$\frac{A/I}{J/I} \simeq A/J. \tag{3.2}$$

Osservazione 3.2.1. Gli anelli $\frac{A/I}{J/I}$ e A/J sono isomorfi come gruppi (dal Secondo Teorema di Omomorfismo (per gruppi)), ma per quest'ultimo risultato sono isomorfi anche come anelli.

Prima di dimostrare il Teorema di Corrispondenza tra Ideali dimostriamo un lemma importante.

Lemma 3.2.4

Siano A, B due anelli e $f : A \to B$ un omomorfismo.

(1) Per ogni $J \subseteq B$ ideale di B vale che $f^{-1}(J)$ è un ideale di A.

(2) Se f è surgettiva, allora per ogni $I \subseteq A$ ideale di A vale che $f(A)$ è un ideale di B.

Dimostrazione. Mostriamo entrambe le affermazioni.

(1) Sappiamo già che $f^{-1}(J)$ è un sottogruppo di A, quindi basta mostrare che vale la proprietà di assorbimento. Sia $a \in A$. Allora

$$x \in f^{-1}(J) \iff f(x) \in J \implies f(a)f(x) = f(ax) \in J \iff ax \in f^{-1}(J),$$

dove l'implicazione deriva dal fatto che J è un ideale di B e $f(a) \in B$.

(2) Sappiamo già che $f(I)$ è un sottogruppo di B. Sia quindi $b \in B$; poiché f è surgettiva dovrà esistere $a \in A$ tale che $f(a) = b$. Allora per ogni $x \in I$ (cioè $f(x) \in f(I)$) vale che

$$bf(x) = f(a)f(x) = f(ax) \in f(I).$$

□

Definizione 3.2.5 – Estensione e contrazione di un ideale

iano A, B due anelli e $f : A \to B$ un omomorfismo di anelli. Se $J \subseteq B$ è un ideale di B allora l'ideale $f^{-1}(A)$ si dice **contrazione di** J **ad** A **via** f.

Se $I \subseteq A$ è un ideale di A allora si dice **estensione di** I **a** B **via** f l'ideale

$$IB := \big(f(I)\big) = f(I)B.$$

Possiamo quindi enunciare e dimostrare una prima parte del Teorema di Corrispondenza tra Ideali.

Teorema 3.2.6 – Teorema di Corrispondenza tra Ideali

Sia A un anello, $I \subseteq A$ un suo ideale. Allora la proiezione canonica π_I induce una corrispondenza biunivoca tra gli ideali di A/I e gli ideali di A contenenti I. Questa corrispondenza conserva le inclusioni e gli indici di sottogruppo.

Dimostrazione. Per il **??** esiste una corrispondenza tra i sottogruppi di A e di A/I. Bisogna mostrare che se questa corrispondenza viene ristretta agli ideali essa continua ad associare ad un ideale di A un ideale di A/I (e viceversa).

Sia quindi $\mathcal{A}$ l'insieme degli ideali di A contenenti I e sia $\mathcal{B}$ l'insieme degli ideali di A/I. Per il Lemma 3.2.4 vale che

- per ogni ideale $\mathfrak{b} \in \mathcal{B}$ la sua controimmagine $\pi_I^{-1}(\mathfrak{b})$ è un ideale di A (e contiene I per il **??**);
- per ogni ideale $\mathfrak{a} \in \mathcal{A}$ la sua immagine $\pi_I(\mathfrak{a})$ è un ideale di B poiché π_I è surgettiva. □

3.3 IDEALI PRIMI E MASSIMALI

Per poter studiare i concetti di ideali primi e massimali abbiamo bisogno di alcuni concetti di Teoria degli Insiemi, ed in particolare del Lemma di Zorn.

Definizione 3.3.1 – Maggioranti, massimi e massimali

Sia $(\mathcal{F}, \preceq)$ un insieme con una relazione di ordine parziale.

Maggiorante Un elemento $M \in \mathcal{F}$ si dice **maggiorante** per un sottoinsieme $X \subseteq \mathcal{F}$ se per ogni $A \in X$ vale che $A \preceq M$.

Massimo Si dice che un elemento $A \in \mathcal{F}$ è un **massimo** per $\mathcal{F}$ se per ogni $B \in \mathcal{F}$ vale che $A \preceq B$.

Massimale Si dice che un elemento $A \in \mathcal{F}$ è **massimale** se per ogni $B \in \mathcal{F}$ tale che $A \preceq B$ vale che $A = B$.

Osservazione 3.3.1. La differenza tra i massimi e gli elementi massimale è che un elemento è massimo quando è maggiore o uguale (nel senso della relazione $\preceq$) di tutti gli elementi dell'insieme, mentre un elemento è massimale se, quando è confrontabile con un altro elemento e risulta minore o uguale di esso, allora è necessariamente uguale ad esso.

Esempio 3.3.2. Consideriamo l'insieme dei sottoinsiemi propri di $\{1,2,3\}$, ovvero

$$(\mathcal{F},\preceq) \coloneqq \big(\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\}\},\subseteq\big).$$

Gli elementi $\{1,2\}$, $\{1,3\}$ e $\{2,3\}$ sono massimali, in quanto ognuno di essi non è contenuto in un altro elemento al di fuori di se stesso. Tuttavia nessuno di essi è un massimo, poiché tra di loro non sono confrontabili.

Definizione 3.3.3 – Catena

Sia $(\mathcal{F},\preceq)$ un insieme parzialmente ordinato. Si dice **catena** di $\mathcal{F}$ un sottoinsieme di $\mathcal{F}$ totalmente ordinato (rispetto alla relazione $\preceq$).

Definizione 3.3.4 – Struttura induttiva

Sia $(\mathcal{F},\preceq)$ un insieme parzialmente ordinato: esso si dice **induttivo** se ogni catena di $\mathcal{F}$ ammette un maggiorante in $\mathcal{F}$.

Possiamo finalmente enunciare il Lemma di Zorn.

Lemma 3.3.5 – Lemma di Zorn

Sia $(\mathcal{F},\preceq)$ un insieme parzialmente ordinato, $\mathcal{F}\neq\varnothing$, $\mathcal{F}$ induttivo. Allora $\mathcal{F}$ ammette elementi massimali.

Useremo il Lemma di Zorn sull'insieme degli ideali propri di un anello, dove la relazione d'ordine è data dall'inclusione.

Definizione 3.3.6 – Ideale primo e massimale

Sia A un anello, $I\subsetneq A$ un ideale proprio di A.

Primo Si dice che I è un **ideale primo** di A se per ogni $x,y\in A$ tali che $xy\in I$ vale che $x\in I$ oppure $y\in I$.

Massimale Si dice che I è un **ideale massimale** se è massimale nell'insieme degli ideali propri di A, ovvero se J è un ideale proprio di A tale che $I\subseteq J$, allora $J=I$.

3.3.7 Esercizio Gli ideali primi di $\mathbb{Z}$ sono tutti e soli della forma $(p)=p\mathbb{Z}$ al variare p primo.

Soluzione Mostriamo entrambi i versi dell'equivalenza.

$\boxed{\Longrightarrow}$ Siano $x,y\in\mathbb{Z}$ tali che $xy\in p\mathbb{Z}$, ovvero $p\mid xy$. Allora $p\mid x$ oppure $p\mid y$, ovvero $x\in p\mathbb{Z}$ oppure $y\in p\mathbb{Z}$.

$\boxed{\Longleftarrow}$ Mostriamo la contronominale: sia $m\in\mathbb{Z}$ non primo. Allora m è riducibile (poiché in $\mathbb{Z}$ i primi sono tutti e soli gli irriducibili), ovvero esistono $a,b\in\mathbb{Z}$ tali che $ab=m$. Allora $ab\in m\mathbb{Z}$ ma $a,b\notin m\mathbb{Z}$, da cui $m\mathbb{Z}$ non è un ideale primo. ⌟

Proposizione 3.3.8

Sia A un anello, $I\subsetneq A$ un ideale proprio di A. Valgono le seguenti affermazioni:

(1) I è contenuto in un ideale massimale di A;

(2) ogni elemento non invertibile di A appartiene ad un ideale massimale di A.

Dimostrazione. Chiaramente la seconda affermazione deriva direttamente dalla prima. Infatti se $x \in A \setminus A^\times$ segue che l'ideale generato da x è un ideale proprio di A. Dunque per la prima affermazione $(x) \subseteq \mathfrak{m}$ (dove $\mathfrak{m}$ è un ideale massimale di A), da cui

$$x \in (x) \subseteq \mathfrak{m}.$$

Mostriamo ora la prima affermazione: consideriamo l'insieme

$$\mathcal{F} := \{ J \subsetneq A \ : \ J \text{ ideale}, I \subseteq J \}.$$

Siccome I è un elemento di $\mathcal{F}$ segue che $\mathcal{F}$ non è vuoto: mostriamo che è induttivo.

Sia $\mathcal{C} := (J_n)$ con $J_i \subseteq J_{i+1}$ una catena di $\mathcal{F}$. Dimostriamo che $\mathcal{J} := \bigcup J_n$ è un maggiorante per $\mathcal{C}$.

- Ovviamente $J_n \subseteq \mathcal{J}$ per ogni n.
- Certamente $I \subseteq J_n \subseteq \mathcal{J}$; inoltre $\mathcal{J} \subsetneq A$ poiché se per assurdo J fosse A allora $1 \in \mathcal{J} = \bigcup J_n$, da cui esisterebbe un indice i tale che $1 \in J_i$. Ma un ideale che contiene l'unità è necessariamente improprio, da cui segue l'assurdo.
- Infine $\mathcal{J}$ è un ideale poiché unione in catena di ideali.

Segue quindi che $\mathcal{J} \in \mathcal{F}$ è un maggiorante della catena $\mathcal{C}$. Per il Lemma di Zorn dunque $\mathcal{F}$ ammette almeno un elemento massimale.

Chiamiamo $\mathfrak{m}$ l'elemento massimale di $\mathcal{F}$: siccome contiene I per definizione di $\mathcal{F}$, rimane solamente da mostrare che $\mathfrak{m}$ è un ideale massimale di A, ovvero che è massimale nella famiglia degli ideali propri di A.

Sia $L \subsetneq A$ un ideale tale che $\mathfrak{m} \subseteq L$. Allora $I \subseteq \mathfrak{m} \subseteq L$, da cui L è un elemento della famiglia $\mathcal{F}$. Tuttavia $\mathfrak{m}$ è massimale in $\mathcal{F}$, da cui L è necessariamente uguale ad $\mathfrak{m}$, ovvero $\mathfrak{m}$ è un ideale massimale contenente I. □

Proposizione 3.3.9

Sia A un anello, $I \subsetneq A$ un ideale proprio di A.

(1) I è un ideale primo se e solo se A/I è un dominio.

(2) I è un ideale massimale se e solo se A/I è un campo.

Dimostrazione. Mostriamo separatamente le due affermazioni.

(1) Sappiamo che A/I è un dominio se e solo se non esistono divisori dello zero, ovvero se e solo se per ogni $x, y \in A$ vale che

$$\begin{aligned} &(x + I)(y + I) = I \\ \implies &x + I = I \text{ oppure } y + I = I \\ \iff &x \in I \text{ oppure } y \in I. \end{aligned}$$

Tuttavia

$$(x + I)(y + I) = I \iff xy + I = I \iff xy \in I,$$

da cui A/I è un dominio se e solo se per ogni $x, y \in A$ tali che $xy \in I$ vale che $x \in I$ oppure $y \in I$, ovvero se e solo se I è un ideale primo.

(2) Per il Teorema di Corrispondenza tra Ideali I è un ideale massimale se e solo se A/I ha come unici ideali l'ideale banale e quello improprio, ovvero se e solo se A/I è un campo. □

Corollario 3.3.10

Sia A un anello.

1. A è un dominio se e solo se l'ideale banale è primo.
2. A è un campo se e solo se l'ideale banale è massimale.
3. Se un ideale proprio $I \subsetneq A$ è massimale, allora è necessariamente primo.

Dimostrazione. I primi due punti vengono direttamente dalla proposizione precedente (poiché $A/(0)$ è isomorfo ad A); per quanto riguarda il terzo I è massimale se e solo se A/I è un campo, quindi a maggior ragione un dominio, ovvero I è anche primo. □

Corollario 3.3.11

Sia A un anello e I un suo ideale. La corrispondenza biunivoca tra gli ideali di A contenenti I e gli ideali di A/I conserva la primalità e la massimalità.

Dimostrazione. Sia J un ideale di A contenente I e consideriamo la proiezione canonica $\pi : A \to A/I$.

Per la Proposizione 3.3.9 J è primo in A se e solo se A/J è un dominio, mentre J/I è primo in A/I se e solo $\frac{A/I}{J/I}$ è un dominio. Tuttavia per il Secondo Teorema degli Omomorfismi segue che

$$\frac{A/I}{J/I} \simeq A/J,$$

da cui segue che π conserva la primalità. Con una dimostrazione analoga (sostituendo "primo" con "massimale" e "dominio" con "campo") si dimostra che π conserva la massimalità, da cui la tesi. □

3.4 ANELLO DELLE FRAZIONI

In questa sezione A sarà un dominio di integrità.

Definizione 3.4.1 – Parte moltiplicativa

Sia $S \subseteq A$ un sottoinsieme di A tale che

- $0 \notin S$,
- $1 \in S$,
- se $a, b \in S$ allora $ab \in S$.

S si dice **parte moltiplicativa** di A.

Consideriamo l'insieme $S^{-1}A$ dato da

$$S^{-1}A := A \times S/\sim,$$

dove la relazione $\sim$ è definita da $(a, s) \sim (b, t)$ se e solo se $at = bs$.

Mostriamo che $\sim$ è una relazione di equivalenza.

Riflessività Ovviamente $(a, s) \sim (a, s)$.

Simmetria Se $(a,s) \sim (b,t)$ allora $at = bs$, ovvero $bs = at$, cioè $(b,t) \sim (a,s)$.

Transitività Supponiamo che $(a,s) \sim (b,t)$ e $(b,t) \sim (c,u)$: mostriamo che $(a,s) \sim (c,u)$.

Le due ipotesi ci dicono che $at = bs$ e $bu = tc$; per verificare che $au = cs$ moltiplichiamo entrambi i membri della prima relazione per u, ottenendo

$$aut = bus = cts,$$

dove la seconda uguaglianza viene dalla seconda relazione. A questo punto raccogliendo t si ottiene che

$$t(au - cs) = 0,$$

dunque siccome A è un dominio dovrà valere che $t = 0$ oppure $au = cs$. Tuttavia $t \in S$, dunque per definizione di parte moltiplicativa $t \neq 0$, da cui la tesi.

Indicheremo $\frac{a}{s}$ la classe di equivalenza della coppia (a,s). Vale il seguente risultato.

Proposizione 3.4.2

$S^{-1}A$ con le operazioni definite da

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st},$$

è un anello commutativo con identità.

Dimostrazione. Mostriamo innanzitutto che le operazioni sono ben definite. Siano $\frac{a}{s} = \frac{a'}{s'}$ e $\frac{b}{t} = \frac{b'}{t'}$ elementi di $S^{-1}A$ e mostriamo che

$$\frac{a}{s} + \frac{b}{t} = \frac{a'}{s'} + \frac{b'}{t'}, \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{a'}{s'} \cdot \frac{b'}{t'}.$$

Per definizione di somma vale che

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \qquad \frac{a'}{s'} + \frac{b'}{t'} = \frac{a't' + b's'}{s't'};$$

queste due frazioni sono uguali se e solo se

$$\begin{aligned} &(at + bs)s't' = (a't' + b's')st \\ \iff &att's' + bss't' = a't'ts + b's'st \end{aligned}$$

e quest'uguaglianza è verificata poiché $as' = a's$ e $bt' = b't$.

Analoga dimostrazione per la buona definizione del prodotto. Il resto delle verifiche è standard. □

L'anello $S^{-1}A$ viene chiamato **anello delle frazioni** oppure **localizzato di** A **ad** S.

Proposizione 3.4.3

L'anello A si immerge naturalmente in $S^{-1}A$ tramite l'omomorfismo iniettivo

$$\begin{aligned} \iota : A &\hookrightarrow S^{-1}A \\ a &\mapsto \frac{a}{1}. \end{aligned}$$

Dimostrazione. Mostriamo prima che ι è un omomorfismo e poi che è iniettivo. Infatti:

$$\iota(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \iota(a) + \iota(b),$$
$$\iota(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = \iota(a) \cdot \iota(b).$$

Inoltre siccome A è un dominio vale automaticamente che $\iota(1) = 1/1$.

Inoltre il nucleo di ι è

$$\ker \iota = \left\{ a \in A \,:\, \frac{a}{1} = \frac{0}{1} \right\} = \{ a \in A \,:\, a = 0 \} = \{0\},$$

da cui ι è iniettivo. □

Osserviamo che se A è un dominio l'insieme $S := A \setminus \{0\}$ è una parte moltiplicativa di A:

- $0 \notin A \setminus \{0\}$,
- $1 \in A \setminus \{0\}$,
- siccome A è un dominio, se $x, y \in A \setminus \{0\}$ allora anche $xy \in A \setminus \{0\}$.

In questo caso chiamiamo **campo dei quozienti** di A il localizzato di A ad S e lo indichiamo con $Q(A)$. Vale la seguente proposizione.

Proposizione 3.4.4

Il campo dei quozienti $Q(A)$ di un dominio A è un campo ed in particolare è il più piccolo campo che contiene A.

3.4.1 Ideali di $S^{-1}A$

Sia $I \subseteq A$ un ideale di A. Definiamo

$$S^{-1}I := \left\{ \frac{x}{s} \in S^{-1}A \,:\, x \in I, s \in S \right\}.$$

Proposizione 3.4.5

Sia A un dominio, $I \subseteq A$ un suo ideale e S una parte moltiplicativa di A. Valgono le seguenti affermazioni.

1. $S^{-1}I$ è un ideale di $S^{-1}A$.
2. Per ogni $J \subseteq S^{-1}A$ ideale di $S^{-1}A$ esiste un ideale I di A tale che $J = S^{-1}I$.
3. $S^{-1}I$ è un ideale proprio di $S^{-1}A$ se e solo se $S \cap I = \varnothing$.
4. Sia $P \subseteq A$ un ideale primo di A, $S \cap P = \varnothing$. Allora $S^{-1}P$ è un ideale primo di $S^{-1}A$.

Osserivamo che i primi due punti ci dicono che gli ideali di $S^{-1}A$ sono tutti e soli della forma $S^{-1}I$ al variare di I tra gli ideali di A.

3.5 DIVISIBILITÀ NEI DOMINI

Considereremo A dominio di integrità per il resto della sezione.

Definizione 3.5.1 – Divisione esatta

Siano $a, b \in A$ con $a \neq 0$. Si dice che a **divide** b (e lo si indica con $a \mid b$) se esiste $c \in A$ tale che $b = ac$.

Questa definizione può anche essere data in termini di ideali: $a \mid b$ è equivalente a $(b) \subseteq (a)$. Infatti $a \mid b$ significa che $b = ac$ per qualche $c \in A$, da cui $b \in (a)$. Ma allora per ogni $x \in A$ vale che $xb \in (a)$ (per la proprietà di assorbimento di (a)) e quindi tutto l'ideale generato da b deve essere incluso nell'ideale generato da a.

Definizione 3.5.2 – Elementi associati

Due elementi non nulli $a, b \in A$ si dicono **associati** (e si scrive $a \sim b$) se esiste un elemento $u \in A^\times$ tale che $a = ub$.

Osserviamo che la relazione di associazione tra elementi di un dominio è una relazione di equivalenza: infatti

- $a = 1 \cdot a$, da cui $a \sim a$;
- se $a = ub$ con $u \in A^\times$ allora $b = u^{-1}a$, ovvero $b \sim a$;
- se $a \sim b$ e $b \sim c$ (ovvero se esistono $x, y \in A^\times$ tali che $a = xb$ e $b = yc$) allora $a = xyc$ e $xy \in A^\times$, da cui $a \sim c$.

Proposizione 3.5.3 – Caratterizzazione degli elementi associati

Siano $a, b \in A \setminus \{0\}$. Le seguenti affermazioni sono equivalenti.

(i) a, b sono associati.

(ii) $a \mid b$ e $b \mid a$.

(iii) $(a) = (b)$.

Dimostrazione. Mostriamo la catena di implicazioni

$$\text{(i)} \implies \text{(ii)} \implies \text{(iii)} \implies \text{(i)}.$$

(i) $\implies$ (ii) Sicuramente $b \mid a$ in quanto $a = ub$. Inoltre moltiplicando entrambi i membri per l'inverso di u (che esiste poiché $u \in A^\times$) segue che $b = u^{-1}a$, ovvero $a \mid b$.

(ii) $\implies$ (iii) Abbiamo mostrato sopra che la divisibilità equivale all'inclusione tra ideali, ovvero

$$a \mid b \implies (a) \subseteq (b), \qquad b \mid a \implies (b) \mid (a),$$

da cui $(a) = (b)$.

(iii) $\implies$ (i) Siccome $(a) = (b)$ segue che $a \in (b)$ e $b \in (a)$. Dalla prima uguaglianza otteniamo che esiste $x \in A$ tale che $a = xb$, mentre dalla seconda otteniamo che esiste $y \in A$ tale che $b = ya$. Sostituendo questa uguaglianza nella prima si ottiene che

$$a = xya \implies xy = 1,$$

da cui in particolare $x \in A^\times$ e quindi $a \sim b$.

□

Possiamo quindi estendere il concetto di massimo comun divisore a domini generici.

Definizione 3.5.4 – Massimo comun divisore

Siano $a, b \in A$ non entrambi nulli. Si dice che $d \in A$ è un **massimo comun divisore** per a e b se

(i) $d \mid a$ e $d \mid b$,

(ii) per ogni $x \in A$, se $x \mid a$ e $x \mid b$ allora $x \mid d$.

Notiamo che in genere il massimo comun divisore non è unico, tuttavia se d e d' sono due massimi comuni divisori di a e b, allora $d \sim d'$.

Definizione 3.5.5 – Elementi primi ed irriducibili

Sia $x \in A$, x non invertibile e non nullo.

- x si dice **primo** se per ogni $a, b \in A$ vale che
$$x \mid ab \implies x \mid a \text{ oppure } x \mid b.$$
- x si dice **irriducibile** se per ogni $a, b \in A$ vale che
$$x = ab \implies a \in A^\times \text{ oppure } b \in A^\times.$$

Come nel caso dei numeri interi vale che ogni elemento primo è irriducibile, tuttavia non vale necessariamente il viceversa.

Proposizione 3.5.6 – Relazione tra elementi e ideali

Sia $x \in A$ non invertibile e non nullo. Valgono le seguenti affermazioni.

(i) x è primo se e solo se (x) è un ideale primo (non nullo).

(ii) x è irriducibile se e solo se (x) è massimale nell'insieme degli ideali principali.

Dimostrazione. La prima proposizione è ovvia, dunque dimostriamo entrambi i versi dell'implicazione.

$\boxed{\implies}$ Supponiamo che x sia irriducibile e sia $y \in A$ tale che $(x) \subseteq (y) \subsetneq A$. Allora esiste $z \in A$ tale che $x = yz$; inoltre necessariamente $y \notin A^\times$, altrimenti l'ideale generato da y sarebbe tutto l'anello A.

Tuttavia x è irriducibile, dunque uno tra z e y deve essere invertibile, ma per l'osservazione appena sopra sappiamo che $y \notin A^\times$, dunque z è invertibile. Da questo segue che $x \sim y$, da cui per la Proposizione 3.5.3 $(x) = (y)$, ovvero (x) è massimale tra gli ideali principali.

$\boxed{\impliedby}$ Supponiamo che x sia riducibile, ovvero $x = yz$ per qualche $y, z \in A$ entrambi non invertibili. Allora
$$(x) \subsetneq (y) \subsetneq A,$$
dove il primo $\subsetneq$ viene dal fatto che z non è invertibile (poiché se gli ideali fossero uguali allora $z \in A^\times$), mentre il secondo viene dal fatto che y non è invertibile.

□

3.6 CATEGORIE DI ANELLI

Le proprietà dell'anello $\mathbb{Z}$ non si estendono a tutti i domini di integrità: vogliamo quindi classificare i domini in categorie a seconda di quante proprietà degli interi vengono rispettate.

Anche in questa sezione considereremo quindi A un generico dominio di integrità.

3.6.1 Domini euclidei

Definizione 3.6.1 – Dominio euclideo

Sia A un dominio di integrità. A si dice **dominio euclideo** se esiste una funzione

$$d : A \setminus \{0\} \to \mathbb{N}$$

detta **grado** tale che

(i) per ogni $x, y \in A \setminus \{0\}$ vale che $d(x) \leq d(xy)$;

(ii) per ogni $x \in A$, $y \in A \setminus \{0\}$ esistono $q, r \in A$ tali che

$$x = qy + r$$

e $r = 0$ oppure $d(r) < d(y)$.

La funzione grado ci consente quindi di effettuare una divisione euclidea tra gli elementi del dominio A: possiamo ben approssimare tutti gli elementi con multipli di altri elementi.

Esempio 3.6.2. $\mathbb{Z}$ è un dominio euclideo: la funzione grado è data da $d(x) = |x|$ per ogni $x \neq 0$.

Esempio 3.6.3. Dato un campo $\mathbb{K}$ il dominio dei polinomi $\mathbb{K}[X]$ è un dominio euclideo: infatti la funzione grado data da

$$d(f) = \deg f$$

è definita su ogni polinomio non nullo e ha le proprietà descritte sopra.

Interi di Gauss

Un ultimo esempio è dato dall'insieme

$$\mathbb{Z}[i] = \{ a + ib \ : \ a, b \in \mathbb{Z} \} \subseteq \mathbb{C}.$$

Questo insieme viene detto insieme degli **interi di Gauss**, ed ha molte proprietà aritmeticamente interessanti. Il grado è dato dalla funzione **norma**:

$$d(a + ib) = N(a + ib) := a^2 + b^2.$$

Proprietà dei domini euclidei

Proposizione 3.6.4 – Algoritmo di Euclide nei domini euclidei

Sia A un dominio euclideo, $a, b \in A$ non entrambi nulli. Allora l'algoritmo di Euclide per il massimo comun divisore termina in un numero finito di passi e restituisce come ultimo resto non nullo un massimo comun divisore tra a e b.

La dimostrazione di questa proposizione è essenzialmente identica al caso aritmetico.

Proposizione 3.6.5 – Gli elementi di grado minimo sono invertibili

ia A un dominio euclideo. Gli elementi di grado minimo di A sono tutti e soli gli elementi di $A^\times$.

Dimostrazione. L'immagine della funzione grado è un sottoinsieme di $\mathbb{N}$ non vuoto, pertanto ammette un minimo. Sia d_0 tale minimo e mostriamo che un elemento ha grado d_0 se e solo se è invertibile.

$\boxed{\Longrightarrow}$ Sia $x \in A \setminus \{0\}$ con grado $d(x) = d_0$.

Allora per ogni $y \in A \setminus \{0\}$ vale che esistono $q, r \in A$ tali che $y = qx + r$, con $d(r) < d(x)$ oppure $r = 0$.

Tuttavia se fosse la prima avremmo un elemento di A con grado minore di d_0, il che è assurdo, quindi $r = 0$, ovvero $y = qx$, ovvero $y \in (x)$.

In particolare se $y = 1$ dovrà esistere $q \in A$ tale che $qx = 1$, ovvero x è invertibile.

$\boxed{\Longleftarrow}$ Sia $x \in A^\times$, ovvero $(x) = A$. Allora per ogni $a \in A$ dovrà esistere $q \in A$ tale che $qx = a$. Ma per la prima proprietà del grado segue che $d(x) \leq d(qx) = d(a)$, da cui x ha grado minimo. □

Proposizione 3.6.6 – Ogni ideale di un dominio euclideo è principale

Sia $I \subseteq A$ un ideale di un dominio euclideo. Allora I è principale ed in particolare è generato da un elemento di grado minimo.

Dimostrazione. Siccome $I = (0)$ è automaticamente principale dimostriamo la proposizione per I non banale.

Sia $x \in I$ un elemento di grado minimo tra gli elementi di I. Sicuramente $(x) \subseteq I$; inoltre per ogni $a \in I$ vale che $a = qx + r$ con $r = 0$ oppure $d(r) < d(x)$. Tuttavia $r = a - qx \in I$, dunque se r non fosse nullo il suo grado deve essere necessariamente maggiore o uguale al grado di x, il che è assurdo. Segue quindi che $r = 0$, ovvero $a = qx$, da cui $I \subseteq (x)$.

Segue quindi che $I = (x)$, ovvero la tesi. □

3.6.2 Domini ad ideali principali

Definizione 3.6.7 – Dominio ad ideali principali

ia A un dominio di integrità. A si dice **dominio ad ideali principali** (abbreviato in PID, *Principal Ideal Domain*) se tutti gli ideali di A sono principali.

Osserviamo che la Proposizione 3.6.6 ci dice che un dominio euclideo è sempre un PID, mentre il viceversa non è necessariamente vero.

Proposizione 3.6.8 – Ideali primi in un PID

Sia A un PID. Gli ideali primi di A sono (0) e gli ideali massimali.

Dimostrazione. Innanzitutto (0) è necessariamente primo (per il Corollario 3.3.10), in quanto A è un dominio. Inoltre ogni ideale massimale è primo, dunque questo dimostra un'implicazione della tesi.

Viceversa, sia P è un ideale primo non banale. Dato che A è un PID, $P = (x)$ per qualche $x \in A$. Questo implica che x sia un elemento primo, da cui segue che x è anche un elemento irriducibile. Per la Proposizione 3.5.6 vale che (x) è massimale nell'insieme degli ideali principali; tuttavia siccome A è un PID ogni ideale è principale, dunque (x) è un ideale massimale, che è la tesi. □

Proposizione 3.6.9 – Massimo comun divisore in un PID

ia A un PID, $x, y \in A$ non entrambi nulli. Sia $d \in A$ tale che

$$(d) = (x, y).$$

Allora d è un massimo comun divisore tra x e y.

Dimostrazione. Innanzitutto un tale d esiste poiché A è un PID, dunque l'ideale generato da x e da y deve essere necessariamente uguale ad un ideale principale.

Siccome $x, y \in (d)$ segue che $d \mid x$ e $d \mid y$. Inoltre se $c \in A$ divide sia x che y segue che $x, y \in (c)$, da cui $(d) = (x, y) \subseteq (c)$, ovvero $c \mid d$. □

3.6.3 Domini a fattorizzazione unica

Definizione 3.6.10 – Dominio a fattorizzazione unica

Sia A un dominio di integrità. A si dice **a fattorizzazione unica** (UFD, da *Unique Factorization Domain*) se ogni $a \in A$ non nullo e non invertibile è esprimibile in modo unico come prodotto di irriducibili, dove l'unicità è a meno di una permutazione dei fattori e di moltiplicazione per elementi invertibili.

Proposizione 3.6.11 – Massimo comun divisore negli UFD

Sia A un UFD. Per ogni $a, b \in A$ non nulli esiste un massimo comun divisore, ed è definito dal prodotto di tutti i fattori irriducibili comuni nella fattorizzazione di a e di b, presi con il minimo esponente.

Teorema 3.6.12 – Caratterizzazione degli UFD

Sia A un dominio di integrità. Le seguenti due condizioni sono equivalenti.

1. A è un UFD.
2. Valgono le seguenti due condizioni:
   (i) Ogni elemento irriducibile di A è primo.
   (ii) Ogni catena discendente di divisibilità è stazionaria, ovvero se $(a_n)_n$ è una successione di elementi di a tale che
   $$\cdots \mid a_n \mid a_{n-1} \mid \cdots \mid a_2 \mid a_1,$$
   allora esiste un indice n_0 tale che $a_i \sim a_{n_0}$ per ogni $i \geq n_0$.

Osserviamo che la seconda condizione può essere riformulata in termini di ideali: essa equivale a dire che ogni catena (per l'inclusione) ascendente di ideali principali è stazionaria, ovvero data una successione di ideali principali $\big((a_n)\big)_n$ tali che

$$(a_1) \subseteq (a_2) \subseteq \dots$$

esiste un indice n_0 tale che $(a_i) = (a_{n_0})$ per ogni $i \geq n_0$.

Dal Teorema 3.6.12 segue semplicemente la seguente proposizione.

Proposizione 3.6.13 – Ogni PID è un UFD

Sia A un PID. Allora A è un UFD.

Dimostrazione. Per il Teorema 3.6.12 è sufficiente mostrare le condizioni (i) e (ii).

(i) Sia $x \in A$ un elemento irriducibile: per la Proposizione 3.5.6 (x) è massimale tra gli ideali principali, ma siccome A è un PID tutti i suoi ideali sono principali, da cui (x) è un ideale massimale. In particolare quindi (x) è anche un ideale primo, ovvero x è un elemento primo.

(ii) Mostriamo che ogni catena ascendente di ideali principali è stazionaria. Sia quindi

$$(a_i) \subseteq (a_2) \subseteq \dots$$

la catena di ideali di A, e poniamo $I := \bigcup_{i\geq 0}(a_i)$. Innanzitutto I è un ideale di A (in quanto unione di ideali in catena), dunque $I = (a)$ per qualche $a \in A$ perché A è un PID.

Ma allora esisterà un indice n_0 tale che $a \in (a_{n_0})$: da questo segue che $(a) \subseteq (a_{n_0})$; tuttavia necessariamente $(a_{n_0}) \subseteq I = (a)$, da cui $I = (a_{n_0})$ e quindi la tesi. □

3.7 POLINOMI COME UFD

Lo scopo di questa sezione sarà dimostrare il seguente teorema.

Teorema 3.7.1

Sia A un UFD. Allora $A[X]$ è un UFD.

Da questo teorema segue per induzione anche il prossimo corollario.

Corollario 3.7.2

Sia A un UFD. Allora $A[X_1, \dots, X_n]$ è un UFD.

Dimostriamo innanzitutto che $A[X]$ è un dominio: dati $f, g \in A[X] \setminus \{0\}$ sappiamo che

$$\deg fg = \deg f + \deg g \geq 0,$$

dunque fg non può essere il polinomio nullo in quanto esso non ha grado. Ricordiamo inoltre che

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

Per mostrare che $A[X]$ è un UFD sfrutteremo il Teorema 3.6.12: dimostreremo quindi che

- ogni irriducibile di $A[X]$ è primo;
- ogni catena discendente di divisibilità è stazionaria.

Ogni irriducibile di $A[X]$ è primo

Per dimostrare che gli irriducibili di $A[X]$ sono anche primi dobbiamo espandere alcuni concetti introdotti nella prima parte.

Definizione 3.7.3 – Contenuto di un polinomio

Sia A un UFD, $f \in A[X]$ tale che

$$f(X) = \sum_{i=0}^{n} a_i X^i.$$

Si dice **contenuto** di f la quantità

$$c(f) := \mathrm{mcd}\{ a_0, \dots, a_n \}.$$

Osserviamo che, siccome A è un UFD, $c(f)$ è univocamente definito a meno di moltiplicazione per un'unità.

Definizione 3.7.4 – Polinomio primitivo

Sia A un UFD, $f \in A[X]$. f si dice **primitivo** se $c(f) \sim 1$.

È facile mostrare che ogni polinomio può essere scritto come prodotto del suo contenuto e di un polinomio primitivo.

Infatti sia $f \in A[X]$ e sia $d := c(f)$. Allora il polinomio

$$f'(X) := \sum_{i=0}^{n} \frac{a_i}{d} X^i$$

è un polinomio a coefficienti in A, in quanto $d \mid a_i$ per ogni i. Inoltre essendo d il massimo comun divisore tra tutti gli a_i segue che il contenuto di f' è (associato a) 1, ovvero f' è primitivo.

Teorema 3.7.5 – Lemma di Gauss

Sia A un UFD e siano $f, g \in A[X]$. Vale che

$$c(fg) = c(f)\, c(g).$$

Dimostrazione. Dividiamo la dimostrazione in due casi.

Caso 1 Supponiamo $c(f) = c(g) = 1$ (ovvero entrambi primitivi) e mostriamo che $c(fg) = 1$.

Se per assurdo fg non fosse primitivo allora $c(fg)$ non sarebbe invertibile, da cui (per l'ipotesi che A è un UFD) esisterebbe un elemento primo $p \in A$ tale che $p \mid c(fg)$.

Consideriamo la proiezione canonica

$$\pi : A[X] \to {}^{A}\!/_{(p)}[X].$$

Osserviamo che

- $\pi\big(f(X)\big)$ non è l'elemento nullo di ${}^{A}\!/_{(p)}[X]$ in quanto $p \nmid c(f) = 1$;
- $\pi\big(g(X)\big)$ non è l'elemento nullo di ${}^{A}\!/_{(p)}[X]$ in quanto $p \nmid c(g) = 1$;
- $\pi\big(f(X)\big)$ è l'elemento nullo di ${}^{A}\!/_{(p)}[X]$.

Ma per la Proposizione 3.3.9 siccome (p) è un ideale primo segue che ${}^{A}\!/_{(p)}$ è un dominio, da cui anche ${}^{A}\!/_{(p)}[X]$ è un dominio, dunque abbiamo trovato un assurdo e $c(fg) = 1$.

Caso 2 Scriviamo

$$f(X) = c(f) \cdot f'(X), \qquad g(X) = c(g) \cdot g'(X),$$

dove f', g' sono polinomi primitivi. Allora

$$c(fg)(fg)' = fg = c(f)\,c(g)f'g'.$$

Osserviamo che i polinomi $(fg)'$ e $f'g'$ sono entrambi primitivi: il primo per costruzione, il secondo per il caso precedente. Uguagliamo quindi i contenuti di entrambi i membri:

$$\begin{aligned} & c(fg)\,c\big((fg)'\big) = c(f)\,c(g)\,c(f'g') \\ \iff\ & c(fg)\cdot 1 = c(f)\,c(g)\cdot 1 \\ \iff\ & c(fg) = c(f)\,c(g), \end{aligned}$$

cioè la tesi.

□

Per il resto della sezione considereremo $\mathbb{K} := Q(A)$.

Corollario 3.7.6

Siano $f, g \in A[X]$, f primitivo e tali che $f \mid g$ in $\mathbb{K}[X]$. Allora $f \mid g$ in $A[X]$.

Dimostrazione. $f \mid g$ in $\mathbb{K}[X]$ significa che esiste $h \in \mathbb{K}[X]$ tali che $g = fh$. Sia ora $d \in A$ tale che $h_1(X) := d \cdot h(X)$ sia un polinomio a coefficienti in A (basta prendere il massimo comune divisore dei denominatori). Allora $h_1(X)f(X) = d \cdot g(X)$ è a sua volta un polinomio a coefficienti in A: prendendo i contenuti si ottiene che

$$d\,c(g) = c(h_1 f) = c(h_1)\,c(f) = c(h_1),$$

ovvero $d \mid c(h_1)$. Ma questo significa che il polinomio $\dfrac{h_1(X)}{d} = h(X)$ è ancora a coefficienti in A, che è la tesi. □

Corollario 3.7.7

Sia $f \in A[X]$. Se f è riducibile in $\mathbb{K}[X]$ (ovvero se esistono $g, h \in \mathbb{K}[X]$ di grado maggiore o uguale a 1 tali che $f = gh$) allora esiste un $\delta \in \mathbb{K}^\times$ tale che

- $g_1 := \delta \cdot g \in A[X]$,
- $h_1 := \delta^{-1} \cdot h \in A[X]$,

da cui $f = g_1 h_1$ è riducibile in $A[X]$ e i fattori sono associati ai rispettivi fattori in $\mathbb{K}[X]$.

Dimostrazione. Sia $d \in A$ tale che $g_1 := d \cdot g$ sia un polinomio a coefficienti in A. Sicuramente d ammette inverso in $\mathbb{K}$, dunque

$$f = (d \cdot g)(d^{-1} \cdot h) = g_1(d^{-1} \cdot h) = c(g_1)(g_1)'(d^{-1} \cdot h).$$

Siccome $(g_1)'$ è un polinomio primitivo a coefficienti in A e $(g_1)' \mid f$ in $\mathbb{K}[X]$, per il corollario precedente segue che $(g_1)' \mid f$ in $A[X]$, ovvero $h_1 := c(g_1)d^{-1}h$ è un polinomio in $A[X]$ e $\delta := d^{-1}\,c(g)$. □

Possiamo quindi finalmente caratterizzare gli irriducibili di $A[X]$.

Teorema 3.7.8 – Caratterizzazione degli irriducibili dell'anello dei polinomi

Sia A un UFD. Gli irriducibili di $A[X]$ sono tutti e soli i polinomi $f \in A[X]$ che soddisfano una delle seguenti proprietà:

1. f è una costante irriducibile in A;
2. f ha grado maggiore o uguale di 1, è primitivo ed irriducibile in $\mathbb{K}[X]$.

Dimostrazione. Dimostriamo i due casi separatamente.

Caso 1. Sia $f \in A[X]$ una costante irriducibile in A.

Sia $f = gh$ con $g, h \in A[X]$. Allora

$$0 = \deg f = \deg g + \deg h,$$

da cui segue che $\deg g = \deg h = 0$, ovvero anche g e h sono costanti. Siccome gli invertibili di $A[X]$ sono gli invertibili di A segue che f è riducibile in $A[X]$ se e solo se f è riducibile in A.

Caso 2. Sia $f \in A[X]$ con $\deg f \geq 1$. Mostriamo entrambi i versi dell'implicazione.

$\boxed{\Longrightarrow}$ Supponiamo che f sia irriducibile in $A[X]$. Scriviamo innanzitutto

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

da cui segue che $c(f)$ è un'unità di $A[X]$, ovvero è un'unità di A, da cui f è primitivo.

Scriviamo ora $f = gh$ in $\mathbb{K}[X]$. Per il Corollario 3.7.7 varrà quindi che $f = g_1 h_1$ con $g_1, h_1 \in A[X]$ e $\deg g_1 = \deg g$, $\deg h_1 = \deg h$. Ma f è invertibile in A, dunque uno tra g_1 e h_1 deve essere invertibile. Si ha quindi che

$$\deg g_1 = 0 \text{ oppure } \deg h_1 = 0 \tag{3.3}$$
$$\iff \deg g = 0 \text{ oppure } \deg h = 0 \tag{3.4}$$
$$\iff g \in \mathbb{K}[X]^\times \text{ oppure } h \in \mathbb{K}[X]^\times, \tag{3.5}$$

cioè f è irriducibile in $\mathbb{K}[X]$.

$\boxed{\Longleftarrow}$ Supponiamo f primitivo e irriducibile in $\mathbb{K}[X]$.

Sia $f = gh$ con $g, h \in A[X]$ (e quindi anche in $\mathbb{K}[X]$). Poiché f è irriducibile in $\mathbb{K}[X]$ segue che uno tra g e h è invertibile in $\mathbb{K}[X]$, cioè è una costante. Supponiamo senza perdita di generalità che g sia costante (ovvero $g(X) = g_0$) e consideriamo il contenuto di entrambi i membri:

$$1 = c(f) = c(gh) = c(g)\, c(h) = g_0 \cdot c(h).$$

Segue quindi che g_0 è invertibile in A, ovvero g è invertibile in $A[X]$, da cui f è irriducibile in $A[X]$. □

Proposizione 3.7.9 – Irriducibili e primi negli UFD

Sia A un UFD. Ogni irriducibile di $A[X]$ è anche primo.

Dimostrazione. Sia $f \in A[X]$ irriducibile. Per definizione f è un elemento primo se per ogni $g, h \in A[X]$ vale che

$$f \mid gh \text{ (in } A[X]) \implies f \mid g \text{ oppure } f \mid h \text{ (in } A[X]).$$

Dal Teorema 3.7.8 si ha che f è irriducibile se e solo se è una costante irriducibile oppure è primitivo e irriducibile in $\mathbb{K}[X]$.

Se f è una costante irriducibile, allora f è un elemento primo in A poiché A è un UFD. Allora supponiamo che $f \mid gh$ per qualche $g, h \in A[X]$. Segue quindi che

$$f = c(f) \mid c(gh) = c(g)\, c(h),$$

ma per primalità di $f = c(f)$ in A segue che

$$f \mid c(g) \text{ oppure } f \mid c(h),$$

ovvero

$$f \mid g \text{ oppure } f \mid h,$$

cioè f è primo in $A[X]$.

Supponiamo ora che f sia un polinomio di grado maggiore o uguale ad 1, primitivo e irriducibile in $\mathbb{K}[X]$. Siccome $\mathbb{K}[X]$ è un ED segue che f è primo in $\mathbb{K}[X]$, cioè se $f \mid gh$ in $A[X]$ allora f divide uno tra g ed h in $\mathbb{K}[X]$. Ma essendo f primitivo vale il Corollario 3.7.6, ovvero f divide uno tra g e h in $A[X]$, cioè f è primo in $A[X]$. □

Ogni catena discendente di divisibilità è stazionaria

Teorema 3.7.10

Sia $(f_n)_{n\in\mathbb{N}}$ una successione di elementi di $A[X]$ tali che

$$\cdots \mid f_3 \mid f_2 \mid f_1 \mid f_0.$$

Allora esiste un n_0 tale che $f_i \sim f_{n_0}$ per ogni $i \geq n_0$.

Osserviamo innanzitutto che dal **??** si ha che se $f \mid g$ allora $c(f) \mid c(g)$ e $f' \mid g'$. Infatti se $g = fh$ per qualche $h \in A[X]$ allora $c(g) = c(f)\, c(h)$ (cioè $c(f) \mid c(g)$) ma anche

$$c(g)g' = c(f)\, c(h) f' h'$$

ovvero $f' \mid g'$.

Dimostrazione del Teorema 3.7.10. Associamo alla successione (f_n) le successioni $(c(f_n))$ e (f'_n). Per quanto osservato sopra si ha che queste due successioni rispettano la stessa catena discendente di divisibilità, cioè per ogni $igeq0$ si ha

$$c(f_{i+1}) \mid c(f_i) \text{ e } f'_{i+1} \mid f'_i.$$

Mostriamo che queste due successioni sono stazionarie:

- quella dei contenuti lo è poiché è una catena discendente di divisibilità nell'UFD A, dunque esiste un m_0 tale che $c(f_i) \sim c(f_{m_0})$ per ogni $i \geq m_0$;
- consideriamo ora la successione dei polinomi primitivi. Associamo ad essa la successione dei gradi $(\deg f'_n)$. Siccome per ogni $i \geq 0$ vale che $f'_{i+1} \mid f'_i$ segue che $\deg f'_{i+1} \leq \deg f'_i$. La successione $(\deg f'_n)$ è pertanto una successione debolmente decrescente di numeri naturali, e pertanto deve stabilizzarsi.

Sia quindi d_0 tale che $\deg f'_i = \deg f'_{d_0}$ per ogni $i \geq d_0$. Allora f'_i e f'_{d_0} hanno lo stesso grado e $f'_i \mid f'_{d_0}$, dunque i due polinomi differiscono per una costante. Tuttavia i due polinomi sono primitivi, dunque devono differire per un'unità, ovvero $f'_i \sim f'_{d_0}$ per ogni $i \geq d_0$, cioè la successione è stazionaria.

Sia $n_0 := \max\{ m_0, d_0 \}$. Da quanto detto sopra segue che, per ogni $i \geq n_0$, $c(f_i) \sim c(f_{n_0})$ e $f'_i \sim f'_{n_0}$, ovvero

$$f_i = c(f_i)f'_i \sim c(f_{n_0})f'_{n_0} = f_{n_0},$$

ovvero la successione di polinomi originale è stazionaria. □

Segue quindi che se A è un UFD allora $A[X]$ è un UFD.

4

Teoria dei Campi

4.1 ESTENSIONI DI CAMPI

Spesso, dato un campo $\mathbb{K}$, siamo interessati a risolvere equazioni polinomiali a coefficienti in $\mathbb{K}$: vogliamo quindi trovare tutte le radici di un dato polinomio. Tuttavia ciò non sempre è possibile: i classici esempi sono $x^2 - 2 \in \mathbb{Q}[x]$ e $x^2 + 1 \in \mathbb{R}[x]$. Questi polinomi sono di grado 2, ma sono comunque irriducibili: le loro radici non sono nel campo dato ma in qualche campo *più grande*.

Lo studio della Teoria dei Campi inizia pertanto con lo studio di tutti i modi di poter *estendere* un campo dato, come il campo dei razionali $\mathbb{Q}$ o il campo degli interi modulo p primo $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, aggiungendo nuovi elementi più o meno estranei al campo originale.

Definizione 4.1.1 – Estensione di campi

Siano $\mathbb{K}, \mathbb{L}$ due campi con $\mathbb{K} \subseteq \mathbb{L}$. Allora si dice che $\mathbb{L}$ **estende** $\mathbb{K}$, e si indica l'estensione con $\mathbb{L} / \mathbb{K}$.

Più in generale un'estensione può essere realizzata come un'immersione $\iota : \mathbb{K} \hookrightarrow \mathbb{L}$: in tal caso infatti l'immagine di $\mathbb{K}$ mediante ι sarebbe un campo isomorfo a $\mathbb{K}$ contenuto in $\mathbb{L}$. Le estensioni $\mathbb{L} / \mathbb{K}$ e $\mathbb{L} / \iota(\mathbb{K})$ vengono perciò accomunate e parleremo di inclusione tra campi anche quando in realtà c'è semplicemente un'immersione.

Inoltre le immersioni sono l'unico modo per costruire omomorfismi non banali fra campi.

Lemma 4.1.2

Ogni omomorfismo non banale che ha come dominio un campo è iniettivo ed è quindi un'immersione.

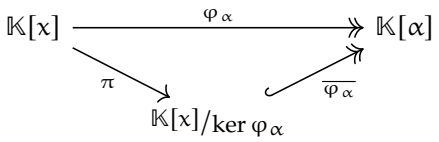
Dimostrazione. Consideriamo l'omomorfismo di anelli $\varphi : \mathbb{K} \to A$, dove $\mathbb{K}$ è un campo mentre A può essere un anello qualsiasi. Sappiamo che $\ker \varphi$ è un ideale di $\mathbb{K}$, ma gli unici ideali di $\mathbb{K}$ sono (0) e $\mathbb{K}$ stesso, dunque o φ è iniettivo oppure è banale. □

Consideriamo quindi un elemento $\alpha \in \mathbb{L}$ e cerchiamo di costruire l'estensione di $\mathbb{K}$ **generata** da α, ovvero la più piccola estensione di $\mathbb{K}$ contenente sia $\mathbb{K}$ che l'elemento α dato. Indicheremo tale estensione con $\mathbb{K}(\alpha)$. Un'estensione generata da un singolo elemento si dirà **semplice**.

Il modo principe per costruire una tale estensione consiste nel considerare un omomorfismo di anelli:

$$\begin{aligned} \varphi_\alpha : \mathbb{K}[x] &\to \mathbb{K}[\alpha] \subseteq \mathbb{L} \\ f(x) &\mapsto f(\alpha), \end{aligned} \tag{4.1}$$

dove $\mathbb{K}[\alpha]$ è l'insieme di tutte le espressioni polinomiali in α. Per il Primo Teorema degli Omomorfismi possiamo disegnare il seguente diagramma commutativo:



da cui segue che

$$\mathbb{K}[x]/\ker\varphi_\alpha \simeq \mathbb{K}[\alpha].$$

Per avanzare nello studio di $\mathbb{K}[\alpha]$ abbiamo però bisogno di più informazioni su $\ker\varphi_\alpha$.

Introduciamo quindi il concetto di elementi algebrici e trascendenti.

Definizione 4.1.3 – Elementi algebrici e trascendenti

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $\alpha \in \mathbb{L}$. α si dice

- **algebrico** se esiste un polinomio $f \in \mathbb{K}[x] \setminus \{0\}$ tale che
$$f(\alpha) = 0,$$
- **trascendente** altrimenti.

In altri termini, $\alpha \in \mathbb{L}$ è algebrico se e solo se esiste un $f \in \mathbb{K}[x]$ non nullo tale che $\varphi_\alpha(f) = f(\alpha) \neq 0$, ovvero se e solo se $\ker\varphi_\alpha \neq 0$.

Osserviamo inoltre che essendo $\mathbb{K}[\alpha] \subseteq \mathbb{L}$ un sottoanello di un campo, esso deve essere necessariamente un dominio di integrità, dunque $\ker\varphi_\alpha$ deve essere un ideale primo in $\mathbb{K}[x]$. Essendo $\mathbb{K}[x]$ un PID (poiché $\mathbb{K}[x]$ è un dominio euclideo) se $\ker\varphi_\alpha \neq (0)$ per la Proposizione 3.6.8 segue quindi che $\ker\varphi_\alpha$ è un ideale massimale e dunque $\mathbb{K}[x]/\ker\varphi_\alpha \simeq \mathbb{K}[\alpha]$ è un campo.

Dato che ogni polinomio in α è *combinazione algebrica* di elementi di $\mathbb{K} \cup \{\alpha\}$, certamente $\mathbb{K}[\alpha] \subseteq \mathbb{K}(\alpha)$. D'altro canto però $\mathbb{K}(\alpha)$ è il più piccolo campo contenente $\mathbb{K}$ e α, dunque necessariamente $\mathbb{K}[\alpha] \supseteq \mathbb{K}(\alpha)$.

Abbiamo quindi dimostrato il seguente teorema.

Teorema 4.1.4

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi, $\alpha \in \mathbb{L}$ algebrico su $\mathbb{K}$. Allora

$$\mathbb{K}(\alpha) = \mathbb{K}[\alpha] \simeq \mathbb{K}[x]/\ker\varphi_\alpha,$$

dove φ_α è l'omomorfismo di valutazione definito in (4.1).

Nel caso φ_α abbia nucleo banale invece otteniamo che

$$\mathbb{K}[\alpha] \simeq \mathbb{K}[x]/\ker\varphi_\alpha = \mathbb{K}[x],$$

quindi $\mathbb{K}[\alpha]$ non è un campo e non può quindi essere il campo $\mathbb{K}(\alpha)$.

Possiamo tuttavia considerare il campo dei quozienti

$$Q(\mathbb{K}[\alpha]) := \left\{ \frac{f(\alpha)}{g(\alpha)} \,:\, f, g \in \mathbb{K}[x] \right\}.$$

Notiamo che non c'è bisogno della richiesta $g(\alpha) \neq 0$ in quanto questo è garantito dal fatto che α è trascendente su $\mathbb{K}$. Per quanto studiato in precedenza, il campo dei quozienti di un anello è il più piccolo campo contenente l'anello di partenza: dunque $Q(\mathbb{K}[\alpha])$ è il più piccolo campo contenente $\mathbb{K}$ e α, dunque per definizione è uguale a $\mathbb{K}(\alpha)$.

Osservazione 4.1.1. Questa caratterizzazione di $Q(\mathbb{K}[\alpha])$ vale anche nel caso in cui α sia algebrico su $\mathbb{K}$.

Proposizione 4.1.5

Sia $\mathbb{L} / \mathbb{K}$ un'estensione di campi, $\alpha \in \mathbb{L}$ trascendente su $\mathbb{K}$. Allora

$$\mathbb{K}(\alpha) \simeq \mathbb{K}(x),$$

dove $\mathbb{K}(x)$ è il campo delle funzioni razionali a coefficienti in $\mathbb{K}$, ovvero

$$\mathbb{K}(x) := \left\{ \frac{f(x)}{g(x)} \ : \ f, g \in \mathbb{K}[x] \right\} = Q(\mathbb{K}[x]).$$

Dimostrazione. Consideriamo la mappa

$$\begin{aligned} \psi : \mathbb{K}(x) &\longrightarrow \mathbb{K}(\alpha) \\ \frac{f(x)}{g(x)} &\longmapsto \frac{f(\alpha)}{g(\alpha)}. \end{aligned}$$

Innanzitutto tale mappa è sempre ben definita, in quanto per ogni polinomio $p \in \mathbb{K}[x]$ si ha che $p(\alpha) \neq 0$ (in quanto α è trascendente su $\mathbb{K}$). Inoltre è certamente un omomorfismo di campi (poiché è semplicemente una valutazione di una funzione polinomiale) ed è ovviamente surgettiva per come abbiamo caratterizzato $\mathbb{K}(\alpha)$.

Resta da mostrare l'iniettività, ma questo è ovvio poiché ψ è un omomorfismo di campi non banale (ad esempio possiamo notare che $\psi(1) = 1$), dunque deve essere iniettivo. □

Torniamo ora a considerare il caso in cui $\alpha \in \mathbb{L}$ sia un elemento algebrico su $\mathbb{K}$. L'isomorfismo $\mathbb{K}(\alpha) \simeq \mathbb{K}[x]/\ker \varphi_\alpha$ si basa sul quoziente per il nucleo dell'omomorfismo di valutazione φ_α, quindi possiamo studiare un po' più precisamente come è fatto questo nucleo.

Dato che siamo in un PID certamente $\ker \varphi_\alpha = (\mu_\alpha)$ per qualche $\mu_\alpha \in \mathbb{K}[x]$. Siccome $\ker \varphi_\alpha$ è un ideale massimale, certamente f deve essere un polinomio irriducibile in $\mathbb{K}[x]$, inoltre per la Proposizione 3.6.6 essendo $\mathbb{K}[x]$ anche un ED segue che μ_α è un elemento di grado minimo tra tutti gli elementi di (μ_α). Infine dato che gli elementi di grado minimo differiscono per una costante, posso scegliere μ_α in modo che sia monico.

Proposizione 4.1.6 – Polinomio minimo di un elemento algebrico

Sia $\mathbb{L} / \mathbb{K}$ un'estensione di campi, $\alpha \in \mathbb{L}$ algebrico su $\mathbb{K}$. Allora esiste un unico polinomio monico, irriducibile in $\mathbb{K}[x]$, di grado minimo tra i polinomi appartenenti a $\ker \varphi_\alpha$ e quindi tale che

$$\ker \varphi_\alpha = (\mu_\alpha).$$

Tale polinomio si dice **polinomio minimo** di α su $\mathbb{K}$.

Dimostrazione alternativa. Ne abbiamo dato una dimostrazione sopra sfruttando le proprietà dei domini euclidei. Se volessimo limitarci a considerazioni più elementari, possiamo innanzitutto considerare che sicuramente

$$S := \{ \deg f \in \mathbb{N} \ : \ f \in \ker \varphi_\alpha \} \subseteq \mathbb{N}$$

è un sottoinsieme non vuoto di $\mathbb{N}$ (poiché α è algebrico), dunque ammette un minimo.

Possiamo sceglierlo certamente monico, poiché se f è di grado minimo ma non monico basta dividere f per il suo coefficiente di testa.

▸ μ_α È IRRIDUCIBILE Supponiamo per assurdo $\mu_\alpha = pq$ dove $p, q \in \mathbb{K}[x]$ di grado minore di μ_α. Dato che $\mu_\alpha \in \ker \varphi_\alpha$ segue che $0 = \mu_\alpha(\alpha) = p(\alpha)q(\alpha)$ in $\mathbb{L}$. Ma allora per la proprietà di annullamento del prodotto segue che $p(\alpha) = 0$ oppure $q(\alpha) = 0$, e ciò è assurdo in quanto μ_α è il polinomio di grado minimo che si annulla in α.

▸ μ_α GENERA $\ker \varphi_\alpha$ Siccome $\mu_\alpha \in \ker \varphi_\alpha$ certamente

$$(\mu_\alpha) = \{\, \mu_\alpha \cdot p \,:\, p \in \mathbb{K}[x] \,\} \subseteq \ker \varphi_\alpha.$$

Sia quindi $f \in \ker \varphi_\alpha$. Per divisione euclidea $f = q\mu_\alpha + r$, dove $r = 0$ oppure $0 \leq \deg r < \deg \mu_\alpha$. Valutando l'espressione in α otteniamo $f(\alpha) = q(\alpha)\mu_\alpha(\alpha) + r(\alpha)$. Siccome $f, \mu_\alpha \in \ker \varphi_\alpha$ questo implica che $0 = r(\alpha)$, ma se r non fosse identicamente nullo ciò sarebbe assurdo, in quanto sarebbe un polinomio in $\ker \varphi_\alpha$ con grado minore di μ_α. Segue quindi che $r = 0$, ovvero

$$\ker \varphi_\alpha \subseteq (\mu_\alpha).$$

▸ μ_α È UNICO Vogliamo infine mostrare che μ_α è l'unico polinomio monico di grado minimo che si annulla in α. Per il punto precedente ogni polinomio f che si annulla in α (ovvero che appartiene a $\ker \varphi_\alpha$) è della forma $f = q\mu_\alpha$. Abbiamo due casi.

- Se $\deg q > 0$ allora $\deg f = \deg q + \deg \mu_\alpha$ quindi f non ha grado minimo.
- Se $\deg q = 0$ allora $q = k \in \mathbb{K}^\times$. Se $f = k\mu_\alpha$ e f e μ_α sono entrambi monici allora $k = 1$, ovvero $f = \mu_\alpha$.

Segue dunque l'unicità di μ_α. □

Prima di passare al grado di un'estensione generalizziamo il concetto di estensione semplice ad un'estensione *finitamente generata*.

Definizione 4.1.7 – S

a $\mathbb{L}/\mathbb{K}$ un'estensione di campi e siano $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$. Chiameremo

$$\mathbb{K}(\alpha_1, \ldots, \alpha_n)$$

il più piccolo sottocampo di $\mathbb{L}$ contenente $\mathbb{K}$ e tutti gli α_i.

Nel caso in cui gli α_i siano tutti algebrici su $\mathbb{K}$, esattamente come prima questo campo è isomorfo all'anello $\mathbb{K}[\alpha_1, \ldots, \alpha_n]$.

Proposizione 4.1.8

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e siano $\alpha_1, \ldots, \alpha_n \in \mathbb{L}$ algebrici su $\mathbb{K}$. Allora $\mathbb{K}[\alpha_1, \ldots, \alpha_n]$ è un campo ed in particolare

$$\mathbb{K}[\alpha_1, \ldots, \alpha_n] = \mathbb{K}(\alpha_1, \ldots, \alpha_n).$$

Dimostrazione. Dimostriamo che $\mathbb{K}[\alpha_1, \dots, \alpha_n]$ è un campo per induzione.

▸ CASO BASE Se $n = 1$ allora $\mathbb{K}[\alpha] \simeq \mathbb{K}(\alpha)$ come abbiamo già dimostrato.

▸ PASSO INDUTTIVO Supponiamo che la tesi sia vera per $m < n$ e dimostriamola per n. Allora

$$\mathbb{K}[\alpha_1, \dots, \alpha_n] = \mathbb{K}[\alpha_1, \dots, \alpha_{n-1}][\alpha_n] = \mathbb{F}[\alpha_n],$$

dove $\mathbb{F} \coloneqq \mathbb{K}[\alpha_1, \dots, \alpha_{n-1}]$ è un campo per l'ipotesi induttiva. Ma allora α_n è algebrico su $\mathbb{F}$ poiché $\mathbb{K} \hookrightarrow \mathbb{F}$ e α_n è un elemento algebrico su $\mathbb{K}$, dunque per il caso base $\mathbb{F}[\alpha_n]$ è un campo.

Mostriamo ora che $\mathbb{K}[\alpha_1, \dots, \alpha_n]$ è *il più piccolo campo* contenente $\mathbb{K}$ e gli α_i, ovvero $\mathbb{K}[\alpha_1, \dots, \alpha_n]$ è l'intersezione di tutti i sottocampi di $\mathbb{L}$ contenenti $\mathbb{K}$ e gli α_i, che abbiamo denotato con $\mathbb{K}(\alpha_1, \dots, \alpha_n)$.

Sicuramente $\mathbb{K}[\alpha_1, \dots, \alpha_n]$ è un campo contenente gli elementi richiesti, dunque è uno degli elementi dell'intersezione, e quindi contiene $\mathbb{K}(\alpha_1, \dots, \alpha_n)$. D'altro canto ogni campo contenente $\mathbb{K}$ e gli α_i dovrà contenere tutte le espressioni polinomiali negli α_i, dunque $\mathbb{K}[\alpha_1, \dots, \alpha_n]$ è contenuto in $\mathbb{K}(\alpha_1, \dots, \alpha_n)$, da cui la tesi. □

▸ GRADO DI UN'ESTENSIONE

Vogliamo ora misurare quanto sia *grande* un'estensione di campi. Per farlo torna comodo osservare che se $\mathbb{L} / \mathbb{K}$ è un'estensione, allora $\mathbb{L}$ può essere pensato come uno spazio vettoriale su $\mathbb{K}$ dove le operazioni sono

$$\alpha + \beta \in \mathbb{L} \qquad \text{con } \alpha, \beta \in \mathbb{L}$$
$$k\alpha \in \mathbb{L} \qquad \text{con } k \in \mathbb{K}, \alpha \in \mathbb{L}.$$

Definizione 4.1.9 – Grado di un'estensione

Sia $\mathbb{L} / \mathbb{K}$ un'estensione di campi. Si dice **grado** dell'estensione la quantità

$$[\mathbb{L} : \mathbb{K}] \coloneqq \deg_{\mathbb{K}} \mathbb{L},$$

ovvero la dimensione di $\mathbb{L}$ come $\mathbb{K}$-spazio.

Nel caso in cui l'estensione sia semplice possiamo sfruttare il polinomio minimo per ricavare informazioni sul grado.

Proposizione 4.1.10

Sia $\mathbb{L} / \mathbb{K}$ un'estensione di campi e sia $\alpha \in \mathbb{L}$. Vale che

$$[\mathbb{K}(\alpha) : \mathbb{K}] = \begin{cases} +\infty, & \text{se } \alpha \text{ è trascendente su } \mathbb{K} \\ \deg \mu_\alpha, & \text{se } \alpha \text{ è algebrico su } \mathbb{K}. \end{cases}$$

Dimostrazione. Se α è trascendente si ha che $\mathbb{K}(\alpha) \simeq \mathbb{K}(x)$, e $\mathbb{K}(x)$ ha dimensione infinita su $\mathbb{K}$ poiché $1, x, x^2, \dots$ sono tutti linearmente indipendenti su $\mathbb{K}$.

Invece consideriamo $\alpha \in \mathbb{L}$ algebrico su $\mathbb{K}$. Per quanto mostrato in precedenza

$$\mathbb{K}(\alpha) = \mathbb{K}[\alpha] \simeq \mathbb{K}[x] \Big/ (\mu_\alpha).$$

L'anello quoziente $\mathbb{K}[x] \Big/ (\mu_\alpha)$ ha come elementi tutte e sole le classi di equivalenza dei

resti delle divisioni per μ_α, dunque i suoi elementi sono

$$\mathbb{K}[x]\Big/(\mu_\alpha) = \{[f] : \deg f < \deg \mu_\alpha\}.$$

Segue quindi che una base di $\mathbb{K}[x]\Big/(\mu_\alpha)$ come $\mathbb{K}$-spazio è data da $[1], [x], \dots, [x^{n-1}]$, dove $n := \deg \mu_\alpha$. Siccome due spazi vettoriali di dimensione finita sono isomorfi se e solo se hanno la stessa dimensione, segue che $\mathbb{K}(\alpha)$ ha dimensione n su $\mathbb{K}$, come volevamo. □

Osservazione 4.1.2. In particolare una possibile scelta dell'isomorfismo

$$\mathbb{K}[x]\Big/(\mu_\alpha) \simeq \mathbb{K}(\alpha)$$

è data dalla funzione $[x] \mapsto \alpha$, da cui

$$\left(1, \alpha, \dots, \alpha^{n-1}\right)$$

è una $\mathbb{K}$-base di $\mathbb{K}(\alpha)$.

Estensioni algebriche

Oltre a studiare estensioni semplici della forma $\mathbb{K}(\alpha)/\mathbb{K}$ con α algebrico su $\mathbb{K}$ vogliamo studiare anche estensioni generate da più elementi. In particolare siamo interessati alle estensioni per cui *tutti* gli elementi del campo più grande sono algebrici sul sottocampo.

Definizione 4.1.11 – Estensione algebrica

Un'estensione $\mathbb{L}/\mathbb{K}$ si dice **algebrica** se ogni $\alpha \in \mathbb{L}$ è algebrico su $\mathbb{K}$.

Vale in particolare la seguente proposizione.

Proposizione 4.1.12 – Ogni estensione finita è algebrica

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi finita, ovvero tale che $[\mathbb{L} : \mathbb{K}] < +\infty$. Allora $\mathbb{L}/\mathbb{K}$ è un'estensione algebrica.

Dimostrazione. Sia $n := [\mathbb{L} : \mathbb{K}]$ e sia $\alpha \in \mathbb{L}$. Per definizione α è algebrico su $\mathbb{K}$ se e solo se esiste un polinomio $f \in \mathbb{K}[x] \setminus \{0\}$ tale che $f(\alpha) = 0$, ovvero se e solo se esistono $k_0, \dots, k_{m-1} \in \mathbb{K}$ tali che

$$k_0 + k_1\alpha + k_2\alpha^2 + \dots k_{m-1}\alpha^{m-1} = 0,$$

ovvero se e solo se le potenze di α non sono tutte linearmente indipendenti.

Consideriamo allora $\{1, \alpha, \dots, \alpha^n\} \subseteq \mathbb{L}$: questo è un insieme di $n+1$ elementi in uno spazio vettoriale di dimensione n: queste potenze non sono linearmente indipendenti e dunque α è algebrico. Infatti essendo linearmente dipendenti dovranno esistere $k_0, \dots, k_n \in \mathbb{K}$ non tutti nulli tali che

$$k_0 + k_1\alpha + k_2\alpha^2 + \dots k_n\alpha^n = 0,$$

dunque il polinomio

$$f(x) := k_0 + k_1x + \dots + k_nx^n$$

è un polinomio non identicamente nullo che si annulla in α.
Per generalità di α segue quindi che l'estensione $\mathbb{L} / \mathbb{K}$ è algebrica. □

Il viceversa tuttavia è falso: come vedremo successivamente esistono estensioni algebriche infinite.

4.1.1 Proprietà delle torri e del composto

Vogliamo ora studiare come si comportano le estensioni quando vengono *eseguite in sequenza* oppure composte tra loro.

Teorema 4.1.13 – Torri di Estensioni

Siano $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}$ campi. Allora $\mathbb{L} / \mathbb{K}$ è finita se e solo se $\mathbb{L} / \mathbb{F}$ e $\mathbb{F} / \mathbb{K}$ sono finite, e in tal caso

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{K}].$$

Dimostrazione. Sia $\beta_1, \dots, \beta_n$ una K-base di F e $\alpha_1, \dots, \alpha_m$ una F-base di L. Mostriamo che

$$\left\{ \alpha_i \beta_j \right\}_{j=1,\dots,n}^{i=1,\dots,m}$$

è una K-base di L.

▸ GENERATORI Siccome $\{ \alpha_1, \dots, \alpha_n \}$ è una F-base di L vale che per ogni $\alpha \in L$ esistono $\lambda_1, \dots, \lambda_n \in F$ tali che

$$\alpha = \sum_{i=1}^{n} \lambda_i \alpha_i.$$

Inoltre, siccome $\{ \beta_1, \dots, \beta_n \}$ è una K-base di F, per ogni λ_i esisteranno $a_{i1}, \dots, a_{im} \in K$ tali che

$$\lambda_i = \sum_{j=1}^{m} a_{ij} \beta_j.$$

Possiamo quindi scrivere

$$\begin{aligned} \alpha &= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} \beta_j \right) \alpha_i \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} \beta_j \alpha_i, \end{aligned}$$

da cui l'insieme dato è un insieme di generatori di L.

▸ INDIPENDENZA LINEARE Mostriamo che se esistono $a_{ij} \in K$ tali che

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} \beta_j \alpha_i = 0$$

allora essi sono tutti uguali a 0. Osserviamo che

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} \beta_j \alpha_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} \beta_j \right) \alpha_i,$$

dove il vettore interno è un elemento di F. Siccome i α_i formano una F-base di L segue quindi che per ogni i

$$\sum_{j=1}^{m} a_{ij}\beta_j = 0.$$

Ma i β_j formano una K-base di F, dunque $a_{ij} = 0$ per ogni i, j, da cui i vettori sono indipendenti.

Segue quindi infine che i vettori $\alpha_i\beta_j$ formano una K-base di L, da cui la tesi. □

La proprietà delle torri di estensioni ci consente di dimostrare che un'estensione è finita se e solo se è generata da un numero finito di elementi algebrici.

Proposizione 4.1.14

Sia $\mathbb{L} / \mathbb{K}$ un'estensione di campi. Allora $\mathbb{L} / \mathbb{K}$ è finita se e solo se è finitamente generata da elementi algebrici su $\mathbb{K}$, ovvero se e solo se esistono $\alpha_1, \dots, \alpha_n \in \mathbb{L}$ algebrici su $\mathbb{K}$ tali che

$$\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n).$$

Dimostrazione. Il fatto che se un'estensione finita essa è finitamente generata da elementi algebrici è ovvio: infatti per la Proposizione 4.1.12 l'estensione è algebrica, dunque ogni elemento di $\mathbb{L}$ è algebrico su $\mathbb{K}$.

Se $n := [\mathbb{L} : \mathbb{K}]$ allora esisterà una $\mathbb{K}$-base di $\mathbb{L}$: chiamiamo i suoi elementi $\alpha_1, \dots, \alpha_n$. Segue quindi che ogni elemento di $\mathbb{L}$ è esprimibile come $\mathbb{K}$-combinazione lineare di $\alpha_1, \dots, \alpha_n$ e dunque

$$\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n).$$

Infine questi elementi sono tutti algebrici su $\mathbb{K}$ poiché l'estensione $\mathbb{L} / \mathbb{K}$ è algebrica.

Mostriamo ora l'altra implicazione: sia

$$\mathbb{L} := \mathbb{K}(\alpha_1, \dots, \alpha_n)$$

con $\alpha_1, \dots, \alpha_n$ algebrici su $\mathbb{K}$ e mostriamo che questa estensione è finita. Procediamo per induzione sul numero dei generatori:

- CASO BASE Se $\mathbb{L} = \mathbb{K}(\alpha)$ e α è algebrico allora il grado dell'estensione è uguale al grado del polinomio minimo di α su $\mathbb{K}$ per la Proposizione 4.1.10.

- PASSO INDUTTIVO Supponiamo che la tesi sia vera per ogni $m < n$ e dimostriamola per n. Possiamo allora costuire la torre di estensioni

$$\mathbb{K} \text{ —— } \mathbb{F} := \mathbb{K}(\alpha_1, \dots, \alpha_{n-1}) \text{ —— } \mathbb{F}(\alpha_n) = \mathbb{L}.$$

Per ipotesi induttiva l'estensione $\mathbb{F} / \mathbb{K}$ è finita; inoltre $\mathbb{L} / \mathbb{F}(\alpha_n)$ è finita in quanto è semplice ed è generata da un elemento algebrico (se α_n è algebrico su $\mathbb{K}$ lo è anche su ogni sua estensione $\mathbb{F}$, in quanto il polinomio che α annulla appartiene sia a $\mathbb{K}[x]$ che ad ogni $\mathbb{F}[x]$).

Per il Teorema 4.1.13 segue quindi che $\mathbb{L} / \mathbb{K}$ è finita, ovvero la tesi. □

Possiamo inoltre studiare l'insieme formato da tutti gli elementi algebrici di un'estensione.

Proposizione 4.1.15 – Campo degli elementi algebrici

Sia $\mathbb{L} / \mathbb{K}$ un'estensione di campi e sia

$$\mathbb{A}_{\mathbb{L}/\mathbb{K}} := \{ \alpha \in \mathbb{L} \ : \ \alpha \text{ algebrico su } \mathbb{K} \}. \tag{4.2}$$

Allora $\mathbb{A}_{\mathbb{L}/\mathbb{K}}$ è un campo ed in particolare l'estensione $\mathbb{A}_{\mathbb{L}/\mathbb{K}} / \mathbb{K}$ è algebrica.

Dimostrazione. Per alleggerire la notazione definiamo $\mathbb{A} := \mathbb{A}_{\mathbb{L}/\mathbb{K}}$.

Ovviamente se $\mathbb{A}$ è un campo allora conterrà $\mathbb{K}$ (in quanto ogni elemento $a \in K$ annulla almeno un polinomio in $\mathbb{K}[x]$, come ad esempio $(x - a)$), e dato che $\mathbb{A}$ è formato solo da elementi algebrici su $\mathbb{K}$ necessariamente l'estensione $\mathbb{A} / \mathbb{K}$ sarà algebrica.

Per mostrare che $\mathbb{A}$ è un campo basta dimostrare che per ogni $\alpha, \beta \in \mathbb{A}$ gli elementi $\alpha + \beta$, $\alpha\beta$ e $1/\alpha$ sono ancora elementi di $\mathbb{A}$.

Per definizione $\alpha, \beta \in \mathbb{A}$ significa che l'estensione $\mathbb{K}(\alpha, \beta) / \mathbb{K}$ è generata da un numero finito di elementi algebrici su $\mathbb{K}$ e dunque per la Proposizione 4.1.14 è finita.

Per la Proposizione 4.1.12 segue che $\mathbb{K}(\alpha, \beta) / \mathbb{K}$ è algebrica, ogni elemento che appartiene a $\mathbb{K}(\alpha, \beta)$ è algebrico su $\mathbb{K}$. In particolare essendo $\mathbb{K}(\alpha, \beta)$ un campo necessariamente $\alpha + \beta$, $\alpha\beta$ e $1/\alpha$ appartengono a $\mathbb{K}(\alpha, \beta)$, dunque sono algebrici su $\mathbb{K}$, dunque appartengono ad $\mathbb{A}$. Segue quindi la tesi. □

Usando l'idea della proposizione precedente possiamo far vedere che esistono estensioni algebriche infinite, e quindi che l'implicazione contraria della Proposizione 4.1.12 non vale.

Consideriamo $\mathbb{Q} \hookrightarrow \mathbb{C}$ e l'insieme

$$\mathbb{A}_{\mathbb{C}/\mathbb{Q}} := \overline{\mathbb{Q}} = \{ \alpha \in \mathbb{C} \ : \ \alpha \text{ algebrico su } \mathbb{K} \}.$$

Per la Proposizione 4.1.15 $\overline{\mathbb{Q}}$ è un campo e $\overline{\mathbb{Q}} / \mathbb{Q}$ è un'estensione algebrica.

Fissato $n \geq 2$ consideriamo ora la torre di estensioni

$$\mathbb{Q} \text{ —— } \mathbb{Q}\left(\sqrt[n]{2}\right) \text{ —— } \overline{\mathbb{Q}}.$$

La prima estensione ha grado n: infatti il polinomio minimo di $\sqrt[n]{2}$ su $\mathbb{Q}$ è

$$\mu_{\sqrt[n]{2}}(x) = x^n - 2.$$

In effetti questo polinomio è monico, si annulla in $\sqrt[n]{2}$ ed è irriducibile per il criterio di Eisenstein applicato con $p = 2$.

In particolare segue quindi (per il Teorema 4.1.13) che $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$ per ogni $n \geq 2$, dunque $\overline{\mathbb{Q}}$ deve avere grado infinito su $\mathbb{Q}$.

4.1.2 Composto di due estensioni

Definiamo ora il composto di due estensioni di $\mathbb{K}$.

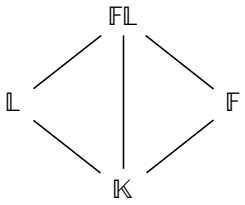
Definizione 4.1.16 – Composto di estensioni

Consideriamo un campo Ω tale che $\mathbb{F}, \mathbb{L} \subseteq \Omega$ siano due suoi sottocampi. Si dice **composto** di $\mathbb{F}$ e $\mathbb{L}$ il campo

$$\mathbb{F}\mathbb{L} := \mathbb{F}(\mathbb{L}) = \mathbb{L}(\mathbb{F})$$

ovvero il sottocampo di Ω che ha come generatori tutti gli elementi di $\mathbb{F}$ e di $\mathbb{L}$, ovvero il più piccolo sottocampo di Ω contenente $\mathbb{F} \cup \mathbb{L}$.

Quando studiamo delle estensioni composte è comodo disegnare il *diagramma* delle estensioni: se $\mathbb{F}, \mathbb{L} \subseteq \Omega$ sono due sottocampi di Ω e $\mathbb{K}$ è un sottocampo di $\mathbb{F}$ e di $\mathbb{L}$ possiamo considerare il diagramma

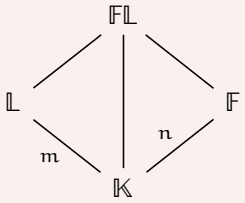


(4.3)

Aggiungendo delle condizioni ai gradi delle sottoestensioni possiamo ricavare informazioni sui gradi delle sovraestensioni tramite le prossime proposizioni.

Proposizione 4.1.17 – Proprietà del composto

Siano $\mathbb{F}, \mathbb{L} \subseteq \Omega$ dei campi e sia $\mathbb{K}$ un sottocampo comune a $\mathbb{F}$ e $\mathbb{L}$ tale che le estensioni $\mathbb{F} / \mathbb{K}$, $\mathbb{L} / \mathbb{K}$ siano finite. Consideriamo il diagramma di estensioni



(4.4)

dove $m := [\mathbb{L} : \mathbb{K}]$, $n := [\mathbb{F} : \mathbb{K}]$.

Allora $\mathbb{FL} / \mathbb{K}$ è un'estensione finita e

$$[m, n] \mid [\mathbb{FL} : \mathbb{K}], \tag{4.5}$$

$$[\mathbb{FL} : \mathbb{K}] \leq [\mathbb{F} : \mathbb{K}][\mathbb{L} : \mathbb{K}] = mn. \tag{4.6}$$

Dimostrazione. Siccome le estensioni $\mathbb{L} / \mathbb{K}$ e $\mathbb{F} / \mathbb{K}$ hanno rispettivamente grado m e n esisteranno degli elementi $\alpha_1, \dots, \alpha_m \in \mathbb{L}$ e $\beta_1, \dots, \beta_n \in \mathbb{F}$ che formano rispettivamente una $\mathbb{K}$-base di $\mathbb{L}$ e di $\mathbb{F}$.

Dato che queste due estensioni sono finite possiamo osservare che

$$\mathbb{FL} = \mathbb{F}(\mathbb{L}) = \mathbb{F}(\mathbb{K}, \alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n).$$

Notiamo ora che ogni elemento di $\mathbb{FL}$ è una combinazione algebrica degli elementi di $\mathbb{F}$ e di $\mathbb{L}$. Sappiamo che ogni elemento di $\mathbb{L}$ può essere espresso come $\mathbb{K}$-combinazione lineare degli α_i e ogni elementi di $\mathbb{F}$ può essere espresso come $\mathbb{K}$-combinazione lineare dei β_j: segue quindi che gli elementi di $\mathbb{FL}$ possono essere espressi come prodotti di $\mathbb{K}$-combinazioni lineari degli α_i e dei β_j, che diventano quindi combinazioni lineari di $\alpha_i \beta_j$ al variare di $i = 1, \dots, m$, $j = 1, \dots, n$.

Segue in particolare che $\{ \alpha_i \beta_j : i = 1, \dots, m,\ j = 1, \dots, n \}$ è un insieme di generatori per $\mathbb{FL}$, dunque la dimensione di $\mathbb{FL}$ come $\mathbb{K}$-spazio è certamente minore o uguale di mn, ovvero

$$[\mathbb{FL} : \mathbb{K}] \leq [\mathbb{F} : \mathbb{K}][\mathbb{L} : \mathbb{K}].$$

Dato che $[\mathbb{FL} : \mathbb{K}]$ è finito per il Teorema 4.1.13 segue che

$$[\mathbb{FL} : \mathbb{K}] \leq [\mathbb{FL} : \mathbb{L}][\mathbb{L} : \mathbb{K}], \qquad [\mathbb{FL} : \mathbb{K}] \leq [\mathbb{FL} : \mathbb{F}][\mathbb{F} : \mathbb{K}].$$

Dalla prima segue che $m \mid [\mathbb{FL} : \mathbb{K}]$, mentre dalla seconda segue che $n \mid [\mathbb{FL} : \mathbb{K}]$, dunque

$$[m, n] \mid [\mathbb{FL} : \mathbb{K}],$$

come volevamo. □

Dalla Proposizione 4.1.17 seguono due semplici corollari.

Corollario 4.1.18

Considerando il diagramma di estensioni come in (4.4), si ha che

$$[\mathbb{FL} : \mathbb{F}] \leq [\mathbb{L} : \mathbb{K}] = m, \qquad [\mathbb{FL} : \mathbb{L}] \leq [\mathbb{F} : \mathbb{K}] = n. \tag{4.7}$$

Dimostrazione. Per la Proposizione 4.1.17 si ha che

$$[\mathbb{FL} : \mathbb{K}] \leq [\mathbb{F} : \mathbb{K}][\mathbb{L} : \mathbb{K}] = mn.$$

Per il Teorema 4.1.13 segue quindi che

(1) $[\mathbb{FL} : \mathbb{K}] = [\mathbb{FL} : \mathbb{F}][\mathbb{F} : \mathbb{K}] = [\mathbb{FL} : \mathbb{F}] \cdot n \leq mn$, dunque deve essere

$$[\mathbb{FL} : \mathbb{F}] \leq m.$$

(2) $[\mathbb{FL} : \mathbb{K}] = [\mathbb{FL} : \mathbb{L}][\mathbb{L} : \mathbb{K}] = [\mathbb{FL} : \mathbb{L}] \cdot m \leq mn$, dunque

$$[\mathbb{FL} : \mathbb{L}] \leq n.$$ □

Corollario 4.1.19

Considerando il diagramma di estensioni come in (4.4), se $(m, n) = 1$ si ha che

$$[\mathbb{FL} : \mathbb{K}] = mn \tag{4.8}$$

e dunque

$$[\mathbb{FL} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] = m, \qquad [\mathbb{FL} : \mathbb{L}] = [\mathbb{F} : \mathbb{K}] = n. \tag{4.9}$$

Dimostrazione. Per il Proposizione 4.1.17 si ha che

$$[m, n] \mid [\mathbb{FL} : \mathbb{K}] \leq mn.$$

Tuttavia siccome $(m, n) = 1$ segue che $[m, n] = mn$, dunque $[\mathbb{FL} : \mathbb{K}] = mn$.
A questo punto per il Teorema 4.1.13 si ha che

$$[\mathbb{FL} : \mathbb{F}] = \frac{[\mathbb{FL} : \mathbb{K}]}{[\mathbb{F} : \mathbb{K}]} = \frac{mn}{n} = m,$$
$$[\mathbb{FL} : \mathbb{L}] = \frac{[\mathbb{FL} : \mathbb{K}]}{[\mathbb{L} : \mathbb{K}]} = \frac{mn}{m} = n,$$

come volevamo. □

Le torri di estensioni e il composto preservano le estensioni algebriche, come dimostrato dalle prossime due proposizioni.

Proposizione 4.1.20

Siano $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}$ campi. Allora $\mathbb{L} / \mathbb{K}$ è algebrica se e solo se $\mathbb{L} / \mathbb{F}$ e $\mathbb{F} / \mathbb{K}$ sono algebriche.

Dimostrazione. Dimostriamo entrambe le implicazioni.

$\boxed{\Longrightarrow}$ Questa implicazione è ovvia. Essendo $\mathbb{F} \subseteq \mathbb{L}$ ogni elemento di $\mathbb{F}$ deve essere algebrico su $\mathbb{K}$ (poiché ogni elemento di $\mathbb{F}$ è anche un elemento di $\mathbb{L}$). Invece se $\alpha \in \mathbb{L} \setminus \mathbb{F}$ siccome è algebrico su $\mathbb{K}$ allora esiste un polinomio non nullo in $\mathbb{K}[x]$ che si annulla in α: questo polinomio può anche essere interpretato come polinomio in $\mathbb{F}[x]$ e dunque α è algebrico su $\mathbb{F}$.

$\boxed{\Longleftarrow}$ Sia $\alpha \in \mathbb{L}$ qualsiasi: vogliamo mostrare che se $\mathbb{L} / \mathbb{F}$ e $\mathbb{F} / \mathbb{K}$ sono algebriche allora α è algebrico su $\mathbb{K}$.

Dato che $\mathbb{L} / \mathbb{F}$ è algebrica sicuramente esiste un polinomio $f \in \mathbb{F}[x] \setminus \{0\}$ che si annulla in α, ovvero esiste

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

tale che $f(\alpha) = 0$. Consideriamo allora l'estensione

$$\mathbb{L}_0 := \mathbb{K}(a_1, \ldots, a_n).$$

Dato che $\mathbb{F} / \mathbb{K}$ è algebrica necessariamente $a_1, \ldots, a_n$ sono algebrici su $\mathbb{K}$, dunque per la Proposizione 4.1.14 segue che l'estensione $\mathbb{L}_0 / \mathbb{K}$ è finita. Inoltre il polinomio f appartiene a $\mathbb{L}_0[x]$, dunque α è algebrico su $\mathbb{L}_0$.

Consideriamo allora la torre di estensioni

$$\mathbb{K} \text{ —— } \mathbb{L}_0 \text{ —— } \mathbb{L}(\alpha).$$

Come abbiamo appena mostrato $\mathbb{L}_0 / \mathbb{K}$ è finita; d'altro canto essendo α algebrico su $\mathbb{L}_0$ l'estensione $\mathbb{L}(\alpha) / \mathbb{L}$ è finita e quindi per il Teorema 4.1.13 segue che $\mathbb{L}_0(\alpha) / \mathbb{K}$ è finita.

Per la Proposizione 4.1.12 segue quindi che $\mathbb{L}_0(\alpha) / \mathbb{K}$ è algebrica. In particolare dunque α è algebrico su $\mathbb{K}$.

Per generalità di α segue quindi che ogni elemento di $\mathbb{L}$ è algebrico su $\mathbb{K}$ e quindi l'estensione $\mathbb{L} / \mathbb{K}$ è algebrica. □

Proposizione 4.1.21

Siano $\mathbb{L}, \mathbb{F} \subseteq \Omega$ campi tali che $\mathbb{K} \subseteq \mathbb{L}, \mathbb{F}$. Allora $\mathbb{F}\mathbb{L} / \mathbb{K}$ è algebrica se e solo se $\mathbb{F} / \mathbb{K}$ e $\mathbb{L} / \mathbb{K}$ sono algebriche.

Dimostrazione. Dimostriamo separatamente le due implicazioni.

$\boxed{\Longrightarrow}$ Quest'implicazione è ovvia: siccome $\mathbb{F}$ (rispettivamente $\mathbb{L}$) è un sottocampo di $\mathbb{F}\mathbb{L}$ ogni elemento di $\mathbb{F}$ (risp. $\mathbb{L}$) è un elemento di $\mathbb{F}\mathbb{L}$ e dunque per ipotesi è algebrico su $\mathbb{K}$, da cui l'estensione $\mathbb{F} / \mathbb{K}$ (risp. $\mathbb{L} / \mathbb{K}$) è algebrica.

$\boxed{\Longleftarrow}$ Sia $\alpha \in \mathbb{F}\mathbb{L}$. Per definizione di composto ogni elemento di $\mathbb{F}\mathbb{L}$ è una somma o un prodotto di elementi di $\mathbb{F}$ e di $\mathbb{L}$, tuttavia essendo entrambi i campi immersi in Ω, essendo le operazioni di Ω commutative e dato che la somma/prodotto di elementi di $\mathbb{F}$ (risp. $\mathbb{L}$) sono ancora elementi di $\mathbb{F}$ (risp. $\mathbb{L}$) un elemento di $\mathbb{F}\mathbb{L}$ sarà della forma

$$\alpha = \sum_{i=1}^{n} \alpha_i \beta_i$$

con gli $\alpha_i \in \mathbb{F}$ e i $\beta_i \in \mathbb{L}$.

Allora

$$\alpha \in \mathbb{M} := \mathbb{K}(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n).$$

Inoltre siccome gli α_i e i β_i sono algebrici su $\mathbb{K}$ (poiché sono elementi di $\mathbb{F}$ e di $\mathbb{L}$ e le estensioni $\mathbb{F} / \mathbb{K}$ e $\mathbb{L} / \mathbb{K}$ sono algebriche su $\mathbb{K}$) segue che $\mathbb{M}$ è un'estensione di $\mathbb{K}$ finitamente generata da elementi algebrici su $\mathbb{K}$.

Per la Proposizione 4.1.14 segue che $\mathbb{M}$ è un'estensione finita di $\mathbb{K}$ e dunque (per la Proposizione 4.1.12) è un'estensione algebrica di $\mathbb{K}$. In particolare quindi α è algebrico su $\mathbb{K}$.

Per generalità di α segue quindi che ogni elemento di $\mathbb{FL}$ è algebrico su $\mathbb{K}$, ovvero la tesi.

□

4.2 CHIUSURA ALGEBRICA E CAMPI DI SPEZZAMENTO

In molte costruzioni viste nella sezione precedente abbiamo avuto bisogno di creare un campo *universo* che contenesse i campi di nostro interesse. Vogliamo ora rendere più concreta questa costruzione, mostrando che possiamo sempre considerare un campo dato come sottocampo di un campo più grande.

Definizione 4.2.1 – Campo algebricamente chiuso

Sia $\mathbb{K}$ un campo. $\mathbb{K}$ si dice **algebricamente chiuso** se ogni polinomio non costante $f \in \mathbb{K}[x]$ ammette almeno una radice in $\mathbb{K}$.

Osserviamo che per il Teorema Fondamentale dell'Algebra il campo $\mathbb{C}$ è un campo algebricamente chiuso, mentre ad esempio $\mathbb{R}$ e $\mathbb{Q}$ non lo sono: il polinomio $x^2 + 1$ è un polinomio di $\mathbb{Q}[x]$ (e quindi di $\mathbb{R}[x]$) ma non ammette radici in nessuno dei due campi.

Inoltre dire che $\mathbb{K}$ è algebricamente chiuso equivale a dire che ogni polinomio non costante si fattorizza su $\mathbb{K}$ in un prodotto di polinomi irriducibili di grado 1, ovvero che gli unici irriducibili di $\mathbb{K}[x]$ sono i polinomi di grado 1.

Infine, se $\mathbb{K}$ è algebricamente chiuso non può esistere un'estensione di $\mathbb{K}$ che sia contemporaneamente algebrica e non banale: se $\mathbb{L} / \mathbb{K}$ è un'estensione algebrica e $\alpha \in \mathbb{L}$ allora α annulla un polinomio di $\mathbb{K}[x]$. Tuttavia un tale polinomio si fattorizza come prodotto di polinomi di primo grado in $\mathbb{K}[x]$, dunque α deve annullare almeno uno dei fattori (perché $\mathbb{K}[x]$ è un dominio di integrità), dunque deve essere un elemento di $\mathbb{K}$. Segue quindi che $\mathbb{L} = \mathbb{K}$ e l'estensione è banale.

Un campo algebricamente chiuso è quindi un ottimo candidato per fare da *campo universo*, in quanto non c'è alcun modo per uscirne al di fuori senza sfruttare elementi trascendenti.

Definizione 4.2.2 – Chiusura algebrica di un campo

Sia $\mathbb{K}$ un campo. Si dice **chiusura algebrica** di $\mathbb{K}$ un campo $\overline{\mathbb{K}}$ tale che

(1) $\overline{\mathbb{K}}$ è algebricamente chiuso,

(2) $\mathbb{K} \hookrightarrow \overline{\mathbb{K}}$, ovvero $\mathbb{K}$ può essere considerato un sottocampo di $\overline{\mathbb{K}}$,

(3) $\overline{\mathbb{K}} / \mathbb{K}$ è un'estensione algebrica.

Ad esempio $\mathbb{C}$ è la chiusura algebrica di $\mathbb{R}$, in quanto

$$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i] \simeq \mathbb{R}[x] \Big/ (x^2 + 1).$$

Invece $\mathbb{C}$ non è la chiusura algebrica di $\mathbb{Q}$ in quanto esistono elementi di $\mathbb{C}$ che non sono algebrici su $\mathbb{Q}$ (ad esempio π).

Il seguente teorema ci garantisce che possiamo sempre considerare la chiusura algebrica di un campo dato.

Teorema 4.2.3 – Esistenza ed unicità della chiusura algebrica

Sia $\mathbb{K}$ un campo. Allora esiste una chiusura algebrica $\overline{\mathbb{K}}$ di $\mathbb{K}$ ed essa è unica a meno di isomorfismo, ovvero se $\overline{\mathbb{K}}$ e $\overline{\mathbb{K}}'$ sono due chiusure algebriche di $\mathbb{K}$ allora esiste

$$\varphi : \overline{\mathbb{K}} \xrightarrow{\sim} \overline{\mathbb{K}}'$$

tale che $\varphi|_{\mathbb{K}} = \mathrm{id}$.

Mostriamo che una chiusura algebrica di $\mathbb{Q}$ è

$$\mathbb{A}_{\mathbb{C}/\mathbb{Q}} := \overline{\mathbb{Q}} = \{ \alpha \in \mathbb{C} \ : \ \alpha \text{ algebrico su } \mathbb{Q} \}.$$

Abbiamo già mostrato nella Proposizione 4.1.15 che un tale $\overline{\mathbb{Q}}$ è un campo e che l'estensione $\overline{\mathbb{Q}} / \mathbb{Q}$ è algebrica: rimane quindi solo da mostrare che $\overline{\mathbb{Q}}$ è un campo algebricamente chiuso.

Sia $f \in \mathbb{Q}[x]$ un polinomio non costante. Dato che $\mathbb{C}$ è algebricamente chiuso e $\mathbb{Q} \hookrightarrow \mathbb{C}$ esiste una radice $\alpha \in \mathbb{C}$ del polinomio f. Dobbiamo far vedere che $\alpha \in \overline{\mathbb{Q}}$: costruiamo la torre di estensioni

$$\mathbb{Q} \text{ —— } \overline{\mathbb{Q}} \text{ —— } \overline{\mathbb{Q}}(\alpha).$$

Dato che $\overline{\mathbb{Q}} / \mathbb{Q}$ è algebrica e $\overline{\mathbb{Q}}(\alpha) / \overline{\mathbb{Q}}$ è algebrica in quanto semplice e generata da un elemento algebrico su $\mathbb{Q}$ (e quindi su $\overline{\mathbb{Q}}$), per la Proposizione 4.1.20 l'estensione $\overline{\mathbb{Q}}(\alpha) / \mathbb{Q}$ è algebrica, e quindi $\alpha \in \overline{\mathbb{Q}}$ per definizione.

Osservazione 4.2.1. La stessa argomentazione può essere usata ogni volta che ho un campo $\mathbb{K}$ immerso in un campo Ω algebricamente chiuso: la chiusura algebrica di $\mathbb{K}$ *in* Ω è l'insieme

$$\overline{\mathbb{K}} = \{ \alpha \in \Omega \ : \ \alpha \text{ algebrico su } \mathbb{K} \}.$$

4.2.1 Campo di spezzamento

Partendo da un campo e costruendo la sua chiusura algebrica otteniamo un campo in cui ogni polinomio ha una radice. Tuttavia questa costruzione è *esagerata* nel caso in cui vogliamo estendere un campo solo con le radici di un gruppo di 1 o pochi polinomi.

Definizione 4.2.4 – Campo di spezzamento

Sia $\mathbb{K}$ un campo e sia $f \in \mathbb{K}[x]$ con $\deg f \geq 1$. Siano inoltre $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{K}}$ le radici di f. Si dice allora **campo di spezzamento** di f su $\mathbb{K}$ il campo generato su $\mathbb{K}$ dalle radici di f:

$$\mathbb{K}(\alpha_1, \ldots, \alpha_n).$$

Più in generale se $f_i \subseteq \mathbb{K}[x]$ è una famiglia di polinomi indicizzata da $i \in I$, dove I è un insieme potenzialmente infinito di indici, e se

$$\alpha_{i1}, \ldots, \alpha_{i,n_i}$$

sono le radici di f_i, allora il campo di spezzamento della famiglia $\mathcal{F} \coloneqq \{ f_i : i \in I \}$ è il campo generato su $\mathbb{K}$ da tutte le radici degli f_i, ovvero

$$\mathbb{K}\left(\alpha_{ij} \,\middle|\, i \in I, j = 1, \dots, n_i \right).$$

Tuttavia questa costruzione non è necessaria nel caso finito, in quanto dato $\mathcal{F} = \{ f_1, \dots, f_m \}$ possiamo considerare il polinomio

$$f \coloneqq f_1 \cdots f_n.$$

A questo punto α è radice di un f_i se e solo se è radice di f e quindi il campo di spezzamento della famiglia $\mathcal{F}$ è uguale al campo di spezzamento del singolo polinomio f.

▸ Grado del campo di spezzamento

Sia $\mathbb{K}$ un campo e sia $\mathbb{F}$ il campo di spezzamento di $f \in \mathbb{K}[x]$ su $\mathbb{K}$. Sia $n \coloneqq \deg f$: dato che f si scompone in n fattori lineari su $\overline{\mathbb{K}}$ esisteranno n radici di f. Chiamiamole

$$\alpha_1, \dots, \alpha_n \in \overline{\mathbb{K}}$$

e consideriamo quindi il campo di spezzamento $\mathbb{F} \coloneqq \mathbb{K}(\alpha_1, \dots, \alpha_n)$. Per definizione questo è equivalente ad aggiungere una radice alla volta:

$$\mathbb{F} = \mathbb{K}(\alpha_1) \dots (\alpha_n).$$

Per calcolare il grado dell'estensione possiamo quindi considerare tutti i campi intermedi

$$\mathbb{F}_i \coloneqq \begin{cases} \mathbb{K} & \text{se } i = 0, \\ \mathbb{F}_{i-1}(\alpha_i) & \text{se } 0 < 1 \leq n. \end{cases}$$

In particolare il campo $\mathbb{F}_0$ è il campo base $\mathbb{K}$, mentre $\mathbb{F}_n = \mathbb{F}$.

Consideriamo allora la torre di estensioni

$$\mathbb{K} = \mathbb{F}_0 \text{ —— } \mathbb{F}_1 \text{ —— } \dots \text{ —— } \mathbb{F}_{n-1} \text{ —— } \mathbb{F}_n = \mathbb{F}$$

e mostriamo che l'estensione

$$\mathbb{F}_{i+1} / \mathbb{F}_i = \mathbb{F}_i(\alpha_{i+1}) / \mathbb{F}_i$$

ha grado minore o uguale ad $n - i$.

Consideriamo la scomposizione di f in fattori lineari:

$$f(x) = c \underbrace{(x - \alpha_1) \cdots (x - \alpha_i)}_{\in \mathbb{F}_i} \underbrace{(x - \alpha_{i+1}) \cdots (x - \alpha_n)}_{= g_i(x) \in \mathbb{F}_i[x]}.$$

In effetti ognuno dei primi i fattori appartiene separatamente ad $\mathbb{F}_i$, dunque il polinomio $g_i(x) = (x - \alpha_{i+1}) \cdots (x - \alpha_n)$ deve essere ancora un polinomio di $\mathbb{F}_i[x]$.

Tale polinomio ha grado $n - i$ ed è un polinomio che si annulla in α_{i+1}: segue quindi che il polinomio minimo di α_{i+1} su $\mathbb{F}_i$ divide g_i e dunque ha grado minore o uguale a $n - i$, ovvero l'estensione ha grado minore o uguale ad $n - i$.

Allora per il Teorema 4.1.13 si ha che

$$\left[\mathbb{F} : \mathbb{K} \right] = \prod_{i=0}^{n-1} \left[\mathbb{F}_{i+1} : \mathbb{F}_i \right] \leq \prod_{i=0}^{n-1} n - i = \prod_{k=1}^{n} k = n!$$

Vale quindi il seguente risultato.

Teorema 4.2.5 – Grado del campo di spezzamento

Sia $\mathbb{K}$ un campo e $f \in \mathbb{K}[x]$ un polinomio di grado n. Se $\mathbb{F}$ è il campo di spezzamento di f su $\mathbb{K}$, allora

$$[\mathbb{F} : \mathbb{K}] \leq n!$$

4.3 CAMPI FINITI

Finora abbiamo genericamente studiato estensioni di campi qualsiasi, pensando a $\mathbb{Q}$ nella maggior parte dei casi. Tuttavia, non tutti i campi sono infiniti perché esistono i campi $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ al variare di p primo. Mostreremo in questa sezione che questi campi non sono gli unici campi finiti e determineremo univocamente (a meno di isomorfismo) tutti i campi finiti esistenti.

4.3.1 Caratteristica di un anello

Sia R un anello commutativo con identità qualsiasi e consideriamo la mappa

$$\begin{aligned} \eta : \mathbb{Z} &\to R \\ n &\mapsto n \cdot 1_R := \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ volte}}. \end{aligned}$$

Tale mappa è ovviamente un omomorfismo di anelli, dunque possiamo considerare il suo nucleo

$$\ker \eta = \{ n \in \mathbb{Z} \,:\, n \cdot 1_R = 0 \}.$$

Osservazione 4.3.1. η è in realtà l'unico omomorfismo di anelli $\mathbb{Z} \to R$.

Definizione 4.3.1 – Caratteristica di un anello

Sia R un anello commutativo con identità e sia $\eta : \mathbb{Z} \to R$ l'unico omomorfismo di anelli da $\mathbb{Z}$ in R. Si dice **caratteristica** di R la quantità

$$\operatorname{char} R := \begin{cases} 0 & \text{se } \ker \eta = (0) \\ n & \text{se } \ker \eta = (n) = n\mathbb{Z}. \end{cases}$$

Un anello qualsiasi può avere una caratteristica uguale ad un qualunque intero positivo; nel caso dei campi però vi sono delle limitazioni.

Proposizione 4.3.2 – Caratteristica di un campo

Sia $\mathbb{K}$ un campo. Allora $\operatorname{char} \mathbb{K} = 0$ oppure $\operatorname{char} \mathbb{K} = p$ con $p \in \mathbb{Z}$ primo.

Dimostrazione. Supponiamo per assurdo che $\mathbb{K}$ abbia caratteristica n con n non primo e $n \neq 0$.

Se $\operatorname{char} \mathbb{K} = 1$ allora $\eta(1) = 1_{\mathbb{K}} = 0_{\mathbb{K}}$, ma ciò è assurdo in quanto $0_{\mathbb{K}} \neq 1_{\mathbb{K}}$.

Segue quindi che $n > 1$. Essendo $\mathbb{Z}$ un UFD, dato che n è non-primo n è anche riducibile, ovvero esistono $1 < a, b < n$ tali che $n = ab$. Ma allora

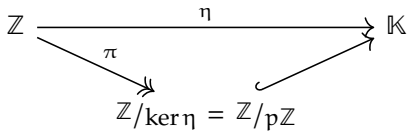
$$\begin{aligned} & \eta(n) = \eta(a)\eta(b) = 0_{\mathbb{K}} \\ \iff\ & \eta(a) = 0_{\mathbb{K}} \text{ oppure } \eta(b) = 0_{\mathbb{K}} \\ \iff\ & a \in \ker \eta \text{ oppure } b \in \ker \eta. \end{aligned}$$

Tuttavia ciò è assurdo poiché $a, b < n$ e dunque $a, b \notin \ker \eta$.
Segue quindi che $\operatorname{char} \mathbb{K}$ è 0 oppure un primo. □

Nel caso $\operatorname{char} \mathbb{K} = 0$ allora il nucleo di $\mathbb{Z} \xrightarrow{\eta} \mathbb{K}$ è banale, da cui $\mathbb{Z} \hookrightarrow \mathbb{K}$. Segue quindi che il campo delle frazioni di $\mathbb{Z}$ è contenuto in $\mathbb{K}$ (poiché il campo delle frazioni di un anello è per definizione il più piccolo campo contenente tale anello), ovvero

$$\mathbb{Q} \hookrightarrow \mathbb{K}.$$

Nel caso invece in cui $\operatorname{char} \mathbb{K} = p$ possiamo considerare il diagramma dato dal Teorema 3.2.2:



Segue quindi che

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \hookrightarrow \mathbb{K}.$$

Vale quindi il seguente risultato.

Teorema 4.3.3 – Esistenza del campo base

Sia $\mathbb{K}$ un campo qualunque.

(1) Se $\operatorname{char} \mathbb{K} = 0$ allora $\mathbb{Q} \hookrightarrow \mathbb{K}$.

(2) Se $\operatorname{char} \mathbb{K} = p$ allora $\mathbb{F}_p \hookrightarrow \mathbb{K}$.

4.3.2 Campi finiti

Vogliamo ora dimostrare che esistono campi finiti che non siano isomorfi ad $\mathbb{F}_p$ e studiare la loro forma.

Sia quindi $f \in \mathbb{F}_p[x]$ un polinomio irriducibile e consideriamo il campo

$$\mathbb{F} := \mathbb{F}_p[x] \Big/ (f).$$

Dato che $\mathbb{F}$ è ottenuto quozientando $\mathbb{F}_p[x]$ per un polinomio di grado $n := \deg f$, una sua $\mathbb{F}_p$-base sarà data dalle classi di resto delle potenze di x, ovvero da $\left([1], [x], \dots, \left[x^{n-1}\right]\right)$.

Ogni elemento di $\mathbb{F}$ può quindi essere espresso come $\mathbb{F}_p$-combinazione lineare di questi elementi, ovvero

$$\mathbb{F} = \left\{ \sum_{i=0}^{n-1} a_i [x^i] \,:\, a_i \in \mathbb{F}_p \right\}.$$

Dato che ogni a_i può essere scelto in p modi (in quanto $\mathbb{F}_p$ ha p elementi) segue che $\mathbb{F}$ ha p^n elementi, e dunque è anch'esso un campo finito.

Dobbiamo ora risolvere tre problemi.

(1) Posso costruire campi finiti con un numero di elementi che non sia una potenza di un primo?

(2) Dato p primo e $n > 1$, esiste sempre un campo con p^n elementi?

(3) Esiste sempre un polinomio $f \in \mathbb{F}_p[x]$ irriducibile e di grado n?

(4) Se esistono due polinomi diversi $f, g \in \mathbb{F}_p[x]$, in che relazione sono i campi ottenuti quozientando $\mathbb{F}_p[x]$ per l'ideale generato da f e da g?

La prossima proposizione risponde alla prima domanda.

Proposizione 4.3.4

Se $\mathbb{F}$ è un campo finito, allora $|\mathbb{F}| = p^n$ per qualche primo p e qualche $n \in \mathbb{N}$.

Dimostrazione. Osserviamo che $\operatorname{char}\mathbb{F}$ non può essere 0, poiché in quel caso $\mathbb{Q} \hookrightarrow \mathbb{F}$ e dunque $\mathbb{F}$ sarebbe infinito.

Sia quindi $p := \operatorname{char}\mathbb{F}$ primo: per quanto studiato in precedenza $\mathbb{F}_p \hookrightarrow \mathbb{F}$, e quindi il grado dell'estensione $\mathbb{F} / \mathbb{F}_p$ deve essere finito in quanto $\mathbb{F}$ è finito.

Sia dunque $n := [\mathbb{F} : \mathbb{F}_p]$. Allora se $(v_1, \dots, v_n)$ è una $\mathbb{F}_p$-base di $\mathbb{F}$ si ha che

$$\mathbb{F} = \left\{ \sum_{i=1}^{n} a_i v_i \ : \ a_i \in \mathbb{F}_p \right\}$$

e dunque, dato che abbiamo p possibili scelte per ognuno degli a_i e queste sono tutte distinte poiché (v_i) è una $\mathbb{F}_p$-base di $\mathbb{F}$, $\mathbb{F}$ ha p^n elementi. □

In realtà vale una condizione molto più forte, che risponde alle domande (2) e (4).

Teorema 4.3.5

Per ogni p primo, $n \in \mathbb{N}$ esiste un unico campo con p^n elementi in una fissata chiusura algebrica di $\mathbb{F}_p$.

Per dimostrare questo teorema abbiamo bisogno del concetto di derivata formale di un polinomio e del cosiddetto **criterio della derivata**.

Definizione 4.3.6 – Derivata formale di un polinomio

Sia R un anello e $f \in R[x]$. Se

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

si dice **derivata formale** di f il polinomio

$$Df(x) = f'(x) := \sum_{k=1}^{n} k a_k x^{k-1}.$$

La derivata formale è esattamente la derivata nel senso analitico e pertanto rispetta tutte le proprietà solite, soltanto che nel contesto di anelli e campi non sempre è possibile definire un concetto di limite e quindi non possiamo usare la *derivata analitica*.

Proposizione 4.3.7 – Criterio della derivata

Sia $\mathbb{K}$ un campo qualsiasi. Allora $f \in \mathbb{K}[x]$ ha radici multiple in $\overline{\mathbb{K}}$ se e solo se $(f, f') \neq 1$, ovvero se e solo se f ha radici in comune con la sua derivata.

Dimostrazione. Sia $\alpha \in \overline{\mathbb{K}}$ una radice di f, ovvero

$$f(x) = (x - \alpha)g(x) \qquad \text{in } \overline{\mathbb{K}}[x].$$

Allora

$$f'(x) = g(x) + (x - \alpha)g'(x),$$

da cui, valutando i polinomi in α, segue che

$$f'(\alpha) = g(\alpha) + (\alpha - \alpha)g'(\alpha) = g(\alpha).$$

Segue quindi che α è una radice in comune tra f e f', ovvero $f'(\alpha) = 0$, se e solo se $g(\alpha) = 0$, ovvero $g(x) = (x - \alpha)h(x)$, ovvero

$$f(x) = (x - \alpha)^2 h(x). \qquad \square$$

Corollario 4.3.8

Sia $f \in \mathbb{K}[x]$ irriducibile. Allora f ha radici multiple in $\overline{\mathbb{K}}$ se e solo se $f' = 0$.

Dimostrazione. Per il Criterio della derivata f ha radici multiple se e solo se $(f, f') \neq 1$. Siccome f è irriducibile però segue che $(f, f') \in \{1, f\}$, dunque si hanno radici multiple se e solo se $(f, f') = f$, ovvero se e solo se f divide f'. Ma f' ha grado minore di f, dunque ciò è possibile se e solo se $f' = 0$. $\square$

Possiamo quindi dimostrare il Teorema 4.3.5.

Dimostrazione del Teorema 4.3.5. Innanzitutto sicuramente se $|\mathbb{F}| = p^n$ allora $\mathbb{F}_p \hookrightarrow \mathbb{F}$. Inoltre $\mathbb{F} / \mathbb{F}_p$ è sicuramente un'estensione finita (poiché $\mathbb{F}$ è finito) e dunque per la Proposizione 4.1.12 si ha che $\mathbb{F} / \mathbb{F}_p$ è algebrica.

Sia allora $\overline{\mathbb{F}_p}$ una chiusura algebrica di $\mathbb{F}_p$: vogliamo mostrare che esiste un $\mathbb{F}$ tale che

$$\mathbb{F}_p \hookrightarrow \mathbb{F} \hookrightarrow \overline{\mathbb{F}}.$$

Se tale $\mathbb{F}$ esiste, il suo gruppo moltiplicativo $\mathbb{F}^\times$ ha ordine $p^n - 1$. Questo significa che per ogni $\alpha \in \mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ si ha che

$$\alpha^{p^n - 1} = 1,$$

ovvero che α è radice del polinomio $x^{p^n - 1} - 1$.

Segue quindi che ogni elemento di $\mathbb{F}$ è radice del polinomio

$$\Psi(x) := x\left(x^{p^n - 1} - 1\right) = x^{p^n} - x,$$

in quanto 0 è radice poiché annulla il fattore x, mentre gli altri elementi sono invertibili e come abbiamo mostrato annullano $x^{p^n - 1} - 1$.

Vale quindi che

$$\mathbb{F} \subseteq \left\{ \alpha \in \overline{\mathbb{F}_p} \,:\, \alpha^{p^n} - \alpha = 0 \right\}.$$

Osservo ora che il polinomio Ψ ha esattamente p^n radici distinte in $\overline{\mathbb{F}_p}$. In effetti

- ne ha al più p^n poiché ha grado p^n;
- per il Criterio della derivata, dato che $\mathbb{F}$ ha caratteristica p si ha che

  $$D\Psi(x) = px^{p^n - 1} - 1 = -1$$

  e quindi $(\Psi, \Psi') = 1$ e quindi tutte le radici di Ψ sono distinte.

Segue quindi che se $\mathbb{F}$ è un campo, allora è l'unico possibile campo contenuto in $\overline{\mathbb{F}_p}$ di cardinalità p^n.

Basta ora mostrare che $\mathbb{F}$ è effettivamente un campo. Sicuramente 0 e 1 sono elementi di $\mathbb{F}$ in quanto sono radici di Ψ. Mostriamo allora che se α, β sono radici di Ψ segue che $\alpha \pm \beta$, $\alpha\beta$ e $1/\alpha$ sono ancora radici di Ψ.

Osserviamo che λ è radice di Ψ se e solo se $\lambda^{p^n} = \lambda$. Allora

$$\begin{aligned} &\alpha \pm \beta \in \mathbb{F}: && (\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta, \\ &\alpha\beta \in \mathbb{F}: && (\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta \\ &\frac{1}{\alpha} \in \mathbb{F}: && \left(\frac{1}{\alpha}\right)^{p^n} = \frac{1}{\alpha^{p^n}} = \frac{1}{\alpha}. \end{aligned}$$

$\mathbb{F}$ è quindi un campo, da cui la tesi. □

Definizione 4.3.9

Fissata una chiusura algebrica $\overline{\mathbb{F}_p}$ di $\mathbb{F}_p$, denotiamo con $\mathbb{F}_{p^n}$ l'unico sottocampo di $\overline{\mathbb{F}_p}$ con p^n elementi.

Osservazione 4.3.2. Non abbiamo ancora dimostrato che per ogni p primo, $n \in \mathbb{N}$ esiste un polinomio irriducibile di grado n in $\mathbb{F}_p[x]$!

4.4 ESTENSIONI QUADRATICHE

Facciamo una breve parentesi sulle estensioni quadratiche di campi, ovvero sulle estensioni di grado 2. Per dimostrare i risultati di questa sezione avremo bisogno di escludere il caso in cui la caratteristica dei campi è 2.

Proposizione 4.4.1 – Ogni estensione quadratica è generata da una radice quadrata

Sia $\mathbb{F}/\mathbb{K}$ un'estensione quadratica, con $\operatorname{char}\mathbb{K} \neq 2$. Allora esiste $\beta \in \mathbb{F}$ tale che $\beta^2 \in \mathbb{K}$ e

$$\mathbb{F} = \mathbb{K}(\beta).$$

Osservazione 4.4.1. $\mathbb{F}$ è *generata da una radice* nel senso che se $\beta^2 = k \in \mathbb{K}$ allora $\mathbb{F} = \mathbb{K}\left(\sqrt{k}\right)$.

Dimostrazione. Consideriamo $\gamma \in \mathbb{F} \setminus \mathbb{K}$. Questa scelta genera una torre di estensioni

$$\mathbb{K} \xrightarrow{\quad} \mathbb{K}(\gamma) \xrightarrow{\quad 2 \quad} \mathbb{F}.$$

Siccome $\gamma \notin \mathbb{K}$ si ha che $[\mathbb{K}(\gamma) : \mathbb{K}] \geq 2$, ma il fatto che $[\mathbb{F} : \mathbb{K}] = 2$ forza $[\mathbb{K}(\gamma) : \mathbb{K}] = 2$. Allora per il Teorema 4.1.13 si ha che

$$[\mathbb{F} : \mathbb{K}(\gamma)] = \frac{[\mathbb{F} : \mathbb{K}]}{[\mathbb{K}(\gamma) : \mathbb{K}]} = \frac{2}{2} = 1,$$

ovvero $\mathbb{F} = \mathbb{K}(\gamma)$.

A questo punto consideriamo $\mu_\gamma \in \mathbb{K}[x]$. Siccome l'estensione è di grado 2 si avrà

$$\mu_\gamma(x) = x^2 + b_1 x + b_0.$$

Valutandolo in γ otteniamo

$$\begin{aligned} &\gamma^2 + b_1\gamma + b_0 = 0 \\ &\iff \left(\gamma + \frac{1}{2}b_1\right)^2 + b_0 - \frac{b_1^2}{4} = 0 \\ &\iff \left(\gamma + \frac{1}{2}b_1\right)^2 = \frac{b_1^2}{4} - b_0 \in \mathbb{K}. \end{aligned}$$

Segue dunque che $\beta := \gamma + \frac{1}{2}b_1$ è un elemento di $\mathbb{F}$ tale che $\beta^2 \in \mathbb{K}$. Inoltre

$$\mathbb{K}(\beta) = \mathbb{K}\left(\gamma + \frac{1}{2}b_1\right) = \mathbb{K}(\gamma) = \mathbb{F},$$

cioè la tesi. □

Osservazione 4.4.2. Notiamo che nella dimostrazione della Proposizione 4.4.1 abbiamo scelto

$$\beta^2 = \frac{b_1^2}{4} - b_0 = \frac{b_1^2 - 4b_0}{4}$$

che è il discriminante dell'equazione $x^2 + b_1 x + b_0$ diviso per 4. Segue quindi che

$$\mathbb{F} = \mathbb{K}(\beta) = \mathbb{K}\left(\frac{\sqrt{\Delta}}{2}\right) = \mathbb{K}\left(\sqrt{\Delta}\right)$$

posto che $\mathbb{K}$ abbia caratteristica diversa da 2.

4.5 ESTENSIONE DI OMOMORFISMI

Abbiamo studiato nelle sezioni precedenti come estendere un campo $\mathbb{K}$ quozientando per un polinomio irriducibile, oppure aggiungendo le radici di un polinomio e ottenendo quindi il campo di spezzamento di tale polinomio su $\mathbb{K}$.

Vogliamo ora estendere le *immersioni*: data un'immersione $\varphi\mathbb{K} \hookrightarrow \overline{\mathbb{K}}$ e un'estensione di campi $\mathbb{L} / \mathbb{K}$ vogliamo scoprire in quali condizioni si può costruire un omomorfismo di campi (e quindi un'immersione)

$$\bar{\varphi} : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$$

tale che $\bar{\varphi}|_{\mathbb{K}} = \varphi$.

Seguiamo la stessa strategia che abbiamo utilizzato per costruire le estensioni di campi: passiamo prima per i polinomi, poi per le estensioni semplici ed infine per le estensioni qualunque (finite).

Teorema 4.5.1 – Estensione di un omomorfismo ai polinomi

Siano R, S anelli commutativi con identità e sia $\varphi : R \to S$ un omomorfismo di anelli.

Per ogni $s \in S$ esiste un unico modo per estendere φ ad un omomorfismo

$$\varphi_* : R[x] \to S$$

tale che $\varphi_*|_R = \varphi$ e $x \mapsto s$.

Dimostrazione. Sia $\sum_{i=0}^{n} a_i x^i \in R[x]$ un polinomio. Allora siccome φ_* deve essere un omomorfismo di anelli segue che

$$\begin{aligned}\varphi_*\left(\sum_{i=1}^{n} a_i x^i\right) &= \sum_{i=0}^{n} \varphi_*\left(a_i x^i\right) \\ &= \sum_{i=0}^{n} \varphi_*(a_i)\varphi_*(x^i) \\ &= \sum_{i=0}^{n} \varphi(a_i) s^i\end{aligned}$$

dove l'ultimo passaggio viene dal fatto che gli a_i sono elementi di R e quindi $\varphi_*(a_i) = \varphi(a_i)$.

Dunque se φ_* esiste è univocamente determinato. Tuttavia la funzione

$$\begin{aligned}R[x] &\to S \\ \sum_{i=0}^{n} a_i x^i &\mapsto \sum_{i=0}^{n} \varphi(a_i) s^i\end{aligned}$$

è certamente un omomorfismo di anelli ben definito, e quindi la tesi. □

Un caso particolare di tale omomorfismo esteso è quello in cui anche il codominio è un anello di polinomi: in tal caso scriveremo φ sia per indicare l'omomorfismo $R \to S$ che per l'omomorfismo

$$\begin{aligned}\varphi : R[x] &\to S[x] \\ p = \sum_{i=1}^{n} a_i x^i &\mapsto \varphi p := \sum_{i=1}^{n} \varphi(a_i) x^i.\end{aligned}$$

L'omomorfismo φ_* che manda x in $s \in S$ può dunque essere denotato anche

$$p \mapsto (\varphi p)(s).$$

In particolare questo Teorema può essere usato nel caso in cui il dominio e codominio siano campi: possiamo estendere $\varphi : \mathbb{K} \hookrightarrow \overline{\mathbb{K}}$ ad un omomorfismo

$$\varphi_* : \mathbb{K}[x] \to \overline{\mathbb{K}}$$

scegliendo un elemento $\beta \in \overline{\mathbb{K}}$ come immagine di x (ovvero $\varphi_*(x) = \beta$).

▸ ESTENSIONE DI id A $\mathbb{K}(\alpha)$

Vogliamo ora estendere

$$\begin{aligned}\mathrm{id}_* : \mathbb{K}[x] &\to \overline{\mathbb{K}} \\ p(x) &\mapsto p(\beta)\end{aligned}$$

ad un omomorfismo

$$\tilde{\varphi} : \mathbb{K}(\alpha) \hookrightarrow \overline{\mathbb{K}}$$

che quindi rispetti $\tilde{\varphi}|_{\mathbb{K}} = \mathrm{id}$.

Ricordiamo che $\mathbb{K}(\alpha) \simeq \mathbb{K}[x]/\ker \varphi_\alpha = \mathbb{K}[x]\Big/(\mu_\alpha)$: per fare in modo che id_* induca per passaggio al quoziente un omomorfismo $\mathbb{K}(\alpha) \hookrightarrow \overline{\mathbb{K}}$ dobbiamo verificare le condizioni del Teorema 3.2.2, ovvero che

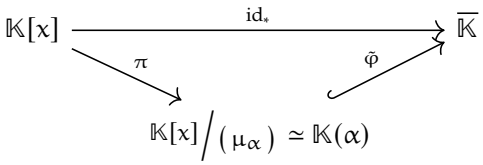
$$(\mu_\alpha) \subseteq \ker \mathrm{id}_* \iff \mu_\alpha \in \ker \mathrm{id}_* \iff \mathrm{id}_*(\mu_\alpha(x)) = \mu_\alpha(\beta) = 0.$$

Dobbiamo quindi scegliere β in modo che β sia radice del polinomio minimo di α.

Definizione 4.5.2 – Coniugato di un elemento algebrico

Sia $\mathbb{K}$ un campo, $\alpha \in \overline{\mathbb{K}}$. Si dice che $\beta \in \overline{\mathbb{K}}$ è un **coniugato** di α se β è radice del polinomio minimo di α su $\mathbb{K}$.

A questo punto possiamo costruire il diagramma



da cui segue che $\tilde{\varphi}$ è un'immersione di $\mathbb{K}(\alpha)$ in $\overline{\mathbb{K}}$. Per commutatività del diagramma segue inoltre che per ogni $k \in \mathbb{K}$

$$k = \mathrm{id}_*(k) = (\tilde{\varphi} \circ \pi)(k) = \tilde{\varphi}\left(\overline{k}\right),$$

ovvero che $\tilde{\varphi}|_{\mathbb{K}} = \mathrm{id}$.

Abbiamo quindi dimostrato che se k è il numero di coniugati distinti di α in $\overline{\mathbb{K}}$ e $\alpha_1, \ldots, \alpha_k \in \overline{\mathbb{K}}$ sono tali coniugati, esistono k omomorfismi

$$\varphi_1, \ldots, \varphi_k : \mathbb{K}(\alpha) \hookrightarrow \overline{\mathbb{K}}$$

tali che $\varphi_i|_{\mathbb{K}} = \mathrm{id}$ e $\varphi_i(\alpha) = \alpha_i$.

▸ RADICI DISTINTE DI μ_α Dobbiamo ora scoprire quanti sono i coniugati distinti di α, ovvero quante sono le radici distinte di μ_α.

Sappiamo che, essendo $\overline{\mathbb{K}}$ algebricamente chiuso, il numero di radici con molteplicità è esattamente uguale al grado di μ_α. Vogliamo ora capire in quali casi tutte le radici di μ_α sono distinte.

Ricordiamo che per il Criterio della derivata un polinomio $f \in \mathbb{K}[x]$ ha radici multiple in $\overline{\mathbb{K}}$ se e solo se $(f, f') \neq 1$. Nel caso particolare in cui f sia irriducibile, per il Corollario 4.3.8 basta controllare che f' non sia il polinomio nullo.

Definizione 4.5.3 – Campo perfetto

Un campo $\mathbb{K}$ si dice **perfetto** se ogni polinomio irriducibile $f \in \mathbb{K}[x]$ non ammette radici multiple in $\overline{\mathbb{K}}$, ovvero se f' non è il polinomio nullo.

Se $\mathbb{K}$ è perfetto segue quindi che ogni polinomio $f \in \mathbb{K}[x]$ irriducibile (e quindi anche μ_α) ha esattamente $\deg f$ radici distinte.

Si può dimostrare che ogni campo di caratteristica 0 e ogni campo finito è perfetto.

Proposizione 4.5.4

Se $\operatorname{char}\mathbb{K} = 0$ allora $\mathbb{K}$ è perfetto.

Dimostrazione. Sia $f \in \mathbb{K}[x]$ irriducibile e quindi di grado maggiore o uguale a 1.

$$f(x) \coloneqq \sum_{i=0}^{n} a_i x^i \quad \Longrightarrow \quad f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$$

e dunque $f' \neq 0$. □

Proposizione 4.5.5

Se $\mathbb{F}$ è un campo finito allora $\mathbb{F}$ è perfetto.

▸ ESISTENZA DI CAMPI NON PERFETTI Tuttavia, esistono anche campi non perfetti: per quanto detto sopra un tale campo deve essere necessariamente un campo infinito di caratteristica non 0.

Prendiamo ad esempio il campo $\mathbb{F}_p(t)$ delle funzioni razionali in $\mathbb{F}_p$. Consideriamo il polinomio $f(x) = x^p - t \in \mathbb{F}_p(t)[x]$: la derivata di tale polinomio è $f'(x) = px^{p-1} = 0$.

Ci rimane quindi da dimostrare che f sia irriducibile in $\mathbb{F}_p(t)[x]$.

Osserviamo che $A = \mathbb{F}_p[t]$ è l'anello il cui campo delle frazioni è $\mathbb{F}_p(t)$ e A è un UFD (poiché è un dominio euclideo). Per una delle conseguenze del Lemma di Gauss (in particolare per il Corollario 3.7.6) è dunque sufficiente mostrare che f sia irriducibile in $A[x]$ (in quanto $f \in A[x]$).

Ma f è irriducibile in $A[x]$ poiché è di Eisenstein rispetto all'ideale primo $\mathfrak{p} \coloneqq (t) \subseteq A$: $\mathfrak{p}$ è primo poiché

$$A/\mathfrak{p} = \mathbb{F}_p[t]/(t) \simeq \mathbb{F}_p$$

è un dominio.

Abbiamo quindi dimostrato che f è un polinomio irriducibile di $\mathbb{F}_p(t)[x]$ che ha radici multiple. In effetti se $\alpha \in \overline{\mathbb{K}}$ è una radice di f, allora

$$f(\alpha) = \alpha^p - t = 0,$$

da cui segue che $t = \alpha^p$. Ma allora

$$f(x) = x^p - \alpha^p = (x - \alpha)^p \qquad \text{in } \overline{\mathbb{K}}[x]$$

dunque f ha una sola radice.

Nel nostro studio delle estensioni di campi considereremo solamente campi perfetti. In particolare parleremo assumeremo che le nostre estensioni siano **separabili**.

Definizione 4.5.6 – Estensione separabile

Un'estensione algebrica di campi $\mathbb{L} / \mathbb{K}$ si dice **separabile** se per ogni $\alpha \in \mathbb{L}$ il polinomio minimo μ_α di α su $\mathbb{K}$ ha $\deg \mu_\alpha$ radici distinte in una chiusura algebrica di $\mathbb{K}$.

Siccome i campi che considereremo saranno sempre perfetti, ogni loro estensione finita (e quindi algebrica) sarà separabile.

Possiamo finalmente enunciare la condizione per estendere l'identità ad un'immersione $\mathbb{K}(\alpha) \hookrightarrow \overline{\mathbb{K}}$.

Teorema 4.5.7 – Estensione dell'identità ad un'estensione semplice

Sia $\mathbb{K}$ un campo (perfetto), $\alpha \in \overline{\mathbb{K}}$. Siano inoltre $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{K}}$ i coniugati di α.
Allora esistono n immersioni

$$\varphi_1, \dots, \varphi_n : \mathbb{K}(\alpha) \hookrightarrow \overline{\mathbb{K}}$$

tali che $\varphi_i|_{\mathbb{K}} = \mathrm{id}$ e $\varphi_i(\alpha) = \alpha_i$.

Estensione di immersioni qualunque a $\mathbb{K}(\alpha)$

Consideriamo ora un'immersione $\varphi : \mathbb{K} \hookrightarrow \overline{\mathbb{K}}$ qualsiasi, con $\mathbb{K}$ perfetto. Come abbiamo visto in precedenza, essa si estende ad un omomorfismo di anelli

$$\begin{aligned} \varphi_* : \mathbb{K}[x] &\to \overline{\mathbb{K}} \\ p(x) &\mapsto (\varphi p)(\beta) \end{aligned}$$

per ogni scelta di $\beta \in \overline{\mathbb{K}}$. Per fare in modo che questo omomorfismo passi al quoziente $\mathbb{K}(\alpha) \simeq \mathbb{K}[x]\Big/(\mu_\alpha)$ dobbiamo ancora una volta imporre che

$$(\mu_\alpha) \subseteq \ker \varphi_* \iff \mu_\alpha \in \ker \varphi_* \iff \varphi_*(\mu_\alpha(x)) = \varphi\mu_\alpha(\beta) = 0,$$

ovvero che β sia radice di $\varphi\mu_\alpha$.

Dunque esistono tante immersioni distinte che estendono φ_* (e quindi φ) quante sono le radici di $\varphi\mu_\alpha$. Osserviamo però che

$$\deg \varphi\mu_\alpha = \deg \mu_\alpha$$

in quanto φ è iniettivo e quindi non può annullare il termine di testa.

Inoltre essendo μ_α irriducibile segue anche che $\varphi\mu_\alpha$ è irriducibile.

Siccome $\mathbb{K}$ è perfetto, $\varphi\mu_\alpha$ ha esattamente $n := \deg \varphi\mu_\alpha = \deg \mu_\alpha$ radici, da cui segue che possiamo estendere φ in n modi diversi.

Teorema 4.5.8 – Estensione di un'immersione ad un'estensione semplice

Sia $\mathbb{K}$ un campo (perfetto), $\varphi : \mathbb{K} \hookrightarrow \overline{\mathbb{K}}$ e $\alpha \in \overline{\mathbb{K}}$.
Allora esistono n immersioni

$$\varphi_1, \dots, \varphi_n : \mathbb{K}(\alpha) \hookrightarrow \overline{\mathbb{K}}$$

tali che $\varphi_i|_{\mathbb{K}} = \varphi$.

Estensioni di immersioni qualunque ad un sovracampo qualsiasi

Dimostriamo ora il caso più generale possibile, ovvero quello in cui l'estensione di campi considerata non sia $\mathbb{K}(\alpha) / \mathbb{K}$ ma una generica estensione finita $\mathbb{L} / \mathbb{K}$.

Teorema 4.5.9 – Estensione di immersioni ad estensioni finite

Sia $\mathbb{L} / \mathbb{K}$ un'estensione finita (e separabile)di grado n. Allora per ogni $\varphi : \mathbb{K} \hookrightarrow \overline{\mathbb{K}}$ esistono n estensioni

$$\varphi_1, \dots, \varphi_n : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$$

tali che $\varphi_i|_{\mathbb{K}} = \varphi$.

Dimostrazione. Lo dimostriamo per induzione su $n := [\mathbb{L} : \mathbb{K}]$.

▸ CASO BASE Se $n = 1$ segue che $bL \simeq \mathbb{K}$ e quindi la tesi è ovvia.

▸ PASSO INDUTTIVO Supponiamo che la tesi sia vera per ogni $m < n$ e dimostriamolo per n.

Sia $\alpha \in \mathbb{L} \setminus \mathbb{K}$. Possiamo costruire la torre di estensioni

$$\mathbb{K} \xrightarrow{m} \mathbb{K}(\alpha) \xrightarrow{d} \mathbb{L}, \qquad \mathbb{K} \xrightarrow{n} \mathbb{L}.$$

Se $m = n$ allora $\mathbb{L} = \mathbb{K}(\alpha)$ e quindi vale il Teorema 4.5.8. Altrimenti deve essere $1 < m < n$: segue quindi che $d := [\mathbb{L} : \mathbb{K}(\alpha)] < n$.

Allora per il Teorema 4.5.8 vale che φ si estende a m immersioni

$$\varphi_1, \dots, \varphi_m : \mathbb{K}(\alpha) \hookrightarrow \overline{\mathbb{K}}.$$

Per ipotesi induttiva dunque ogni $\varphi_i : \mathbb{K}(\alpha) \hookrightarrow \overline{\mathbb{K}}$ si estenderà a d immersioni

$$\varphi_{i1}, \dots, \varphi_{id} : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}.$$

Abbiamo trovato $m \cdot d = n$ immersioni. Osserviamo inoltre che $\varphi_{ij}|_{\mathbb{K}(\alpha)} = \varphi_i$ e $\varphi_i|_{\mathbb{K}} = \varphi$, da cui ogni immersione φ_{ij} estende φ, come volevamo. □

Definizione 4.5.10 – Immersione di un'estensione di campi

Sia $\mathbb{L}/\mathbb{K}$ un'estensione algebrica di campi. Allora si dice **immersione di** $\mathbb{L}/\mathbb{K}$ un'immersione

$$\varphi : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$$

tale che $\varphi|_{\mathbb{K}} = \mathrm{id}$.

4.6 ESTENSIONI NORMALI

Iniziamo questa sezione con un paio di esempi.

Esempio 4.6.1. Consideriamo il polinomio $x^3 - 2$ in $\mathbb{Q}[x]$. Questo polinomio è monico e irriducibile su $\mathbb{Q}$ (poiché di Eisenstein) e pertanto

$$\mu_{\sqrt[3]{2}} = x^3 - 2.$$

Per comodità scriviamo $\alpha := \sqrt[3]{2}$. Costruiamo allora tutte le possibili estensioni $\varphi : \mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}}$ tali che $\varphi|_{\mathbb{Q}} = \mathrm{id}$.

Per quanto visto in precedenza ne esistono tante quante i coniugati di α, che sono

$$\alpha,\ \alpha\zeta_3,\ \alpha\zeta_3^2$$

dove ζ_3 è ovviamente una radice primitiva terza dell'unità.

Segue quindi che

$$\varphi\big(\mathbb{Q}(\alpha)\big) = \mathbb{Q}\big(\varphi(\alpha)\big) = \begin{cases} \mathbb{Q}(\alpha) \\ \mathbb{Q}(\alpha\zeta_3) \\ \mathbb{Q}\left(\alpha\zeta_3^2\right). \end{cases}$$

Tali estensioni sono distinte tra loro: ad esempio $\mathbb{Q}(\alpha)$ è un sottocampo di $\mathbb{R}$ mentre le altre due contengono anche numeri complessi immaginari.

Esempio 4.6.2. Sia p un primo e consideriamo il campo $\mathbb{Q}(\zeta_p)$ ottenuto aggiungendo a $\mathbb{Q}$ una radice primitiva p-esima dell'unità.

Il polinomio minimo di ζ_p su $\mathbb{Q}$ è

$$\mu_{\zeta_p}(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1.$$

In effetti questo polinomio è irriducibile poiché è traslato di un polinomio di Eisenstein ed è monico, quindi deve essere il polinomio minimo di ζ_p.

I coniugati di ζ_p sono quindi

$$\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}.$$

Le estensioni dell'identità a $\mathbb{Q}(\zeta_p)$ dovranno dunue essere della forma

$$\begin{aligned} \varphi_i : \mathbb{Q}(\zeta_p) &\hookrightarrow \overline{\mathbb{Q}} \\ \mathbb{Q} &\mapsto \mathbb{Q} \\ \zeta_p &\mapsto \zeta_p^i \end{aligned}$$

con $i = 1, \ldots, p-1$. Osserviamo ora che per ogni i

$$\varphi_i\big(\mathbb{Q}(\zeta_p)\big) = \mathbb{Q}\big(\varphi_i(\zeta_p)\big) = \mathbb{Q}(\zeta_p^i) = \mathbb{Q}(\zeta).$$

In effetti l'inclusione $\mathbb{Q}(\zeta_p) \supseteq \mathbb{Q}(\zeta_p^i)$ è ovvia in quanto in $\mathbb{Q}(\zeta_p)$ c'è l'elemento ζ_p^i e dunque deve esserci tutto il campo da essa generato. Ma a questo punto possiamo costruire la torre di estensioni

$$\mathbb{Q} \overset{p-1}{\underset{p-1}{\frown}} \mathbb{Q}(\zeta_p^i) = \mathbb{Q}(\zeta_p)$$

da cui segue che il grado dell'estensione $\mathbb{Q}(\zeta_p) / \mathbb{Q}(\zeta_p^i)$ è 1, dunque i due campi devono essere lo stesso campo.

Definizione 4.6.3 – Estensione normale di campi

Sia $\mathbb{F} / \mathbb{K}$ un'estensione algebrica di campi. $\mathbb{F} / \mathbb{K}$ si dice **normale** se per ogni immersione $\varphi : \mathbb{F} \hookrightarrow \overline{\mathbb{K}}$ tale che $\varphi|_{\mathbb{K}} = \mathrm{id}$ si ha

$$\varphi(\mathbb{F}) = \mathbb{F}.$$

Ad esempio per quanto visto sopra $\mathbb{Q}(\zeta_p) / \mathbb{Q}$ è normale, mentre $\mathbb{Q}\left(!\sqrt[3]{2}\right) / \mathbb{Q}$ non lo è.

Proposizione 4.6.4 – Caratterizzazione delle estensioni normali

Sia $\mathbb{F} / \mathbb{K}$ un'estensione algebrica (e finita). I seguenti fatti sono equivalenti.

1. $\mathbb{F} / \mathbb{K}$ è normale.
2. Ogni polinomio $f \in \mathbb{K}[x]$ che ha una radice in $\mathbb{F}$ ha tutte le sue radici in $\mathbb{F}$.
3. $\mathbb{F}$ è il campo di spezzamento di una famiglia di polinomi di $\mathbb{K}[x]$.

Osservazione 4.6.1. I primi due punti della Proposizione 4.6.4 valgono anche per le estensioni algebriche infinite, ma noi la useremo e dimostreremo solo nel caso finito.

Dimostrazione. Dimostriamo la catena di implicazioni

$$(1) \implies (2) \implies (3) \implies (1).$$

(1) $\implies$ (2) Sia $f \in \mathbb{K}[x]$ e siano $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{K}}$ le radici di f. Supponiamo senza

perdita di generalità che α_1 appartenga ad $\mathbb{F}$ e dimostriamo che da ciò segue che $\alpha_2, \dots, \alpha_n \in \mathbb{F}$.

Siccome $\alpha_1 \in \mathbb{F}$ certamente $\mathbb{K}(\alpha_1) \subseteq \mathbb{F}$. Allora per ogni $i = 1, \dots, n$ definiamo

$$\begin{aligned} \varphi_i : \mathbb{K}(\alpha_1) &\hookrightarrow \mathbb{K}(\alpha_i) \subseteq \overline{\mathbb{K}} \\ \alpha_1 &\mapsto \alpha_i \end{aligned}$$

tale che $\varphi_i|_{\mathbb{K}} = \mathrm{id}$.

Dato che $\mathbb{F} / \mathbb{K}$ è finita a maggior ragione lo sarà $\mathbb{F} / \mathbb{K}(\alpha_1)$. Per la **??** possiamo allora estendere ogni φ_i ad un'immersione definita su $\mathbb{F}$:

$$\tilde{\varphi}_i : \mathbb{F} \hookrightarrow \overline{\mathbb{K}}$$

tale che $\tilde{\varphi}_i|_{\mathbb{K}(\alpha_1)} = \varphi_i$, dunque in particolare $\tilde{\varphi}_i|_{\mathbb{K}} = \mathrm{id}$.

Possiamo quindi applicare l'ipotesi che l'estensione $\mathbb{F} / \mathbb{K}$ è normale: $\tilde{\varphi}_i(\mathbb{F}) = \mathbb{F}$ per ogni i. In particolare dato che $\alpha_1 \in \mathbb{K}(\alpha_1)$ si ha che

$$\tilde{\varphi}_i(\alpha_1) = \varphi_i(\alpha_1) = \alpha_i \in \mathbb{F},$$

e dunque $\mathbb{F}$ contiene tutte le radici di f.

(2) $\implies$ (3) Consideriamo il campo di spezzamento su $\mathbb{K}$ della famiglia

$$\mathcal{F} \coloneqq \{ \mu_\alpha \ : \ \alpha \in \mathbb{F} \},$$

dove μ_α indica il polinomio minimo di α su $\mathbb{K}$. Chiamiamo tale campo $\mathbb{F}_0$.

Certamente $\mathbb{F} \subseteq \mathbb{F}_0$: ogni elemento di $\mathbb{F}$ è radice del proprio polinomio minimo, e tale polinomio minimo fa parte della famiglia $\mathcal{F}$. D'altra parte per definizione

$$\mathbb{F}_0 = \mathbb{K}\big(\beta \,\big|\, \beta \text{ radice di qualche } \mu_\alpha \in \mathcal{F} \big).$$

Allora ogni $\beta \in \mathbb{F}_0$ è radice di un polinomio μ_α che ha almeno una radice in $\mathbb{F}$ (ovvero α stessa, per definizione della famiglia FF), dunque per ipotesi $\beta \in \mathbb{F}_0$ e quindi $\mathbb{F}_0 \subseteq \mathbb{F}$.

Segue quindi che $\mathbb{F} = \mathbb{F}_0$ ed è dunque il campo di spezzamento di una famiglia di polinomi di $\mathbb{K}[x]$.

(3) $\implies$ (1) Sia $\mathbb{F}$ il campo di spezzamento su $\mathbb{K}$ di una famiglia $\mathcal{F}$ di polinomi di $\mathbb{K}[x]$. Siccome l'estensione $\mathbb{F} / \mathbb{K}$ è finita, la famiglia è necessariamente finita:

$$\mathcal{F} = \{ f_1, \dots, f_k \}.$$

Dunque in particolare siano $\{ \alpha_{ij} \ : \ j = 1, \dots, n_i \}$ le radici del polinomio f_i: il campo di spezzamento $\mathbb{F}$ può essere descritto come

$$\mathbb{F} = \mathbb{K}\big(\alpha_{ij} \,\big|\, i = 1, \dots, k,\ j = 1, \dots, n_i \big).$$

Sia allora $\varphi : \mathbb{F} \hookrightarrow \overline{\mathbb{K}}$ tale che $\varphi|_{\mathbb{K}} = \mathrm{id}$ e mostriamo che $\varphi(\mathbb{F}) = \mathbb{F}$.

Osserviamo che per ogni scelta di i, j il polinomio minimo $\mu_{\alpha_{ij}}$ di α_{ij} su $\mathbb{K}$ dovrà dividere f_i, poiché f_i è un polinomio che si annulla in α_{ij}. Essendo φ un'immersione di $\mathbb{F} / \mathbb{K}$, φ dovrà mandare α_{ij} in un'altra radice del suo polinomio minimo, che sarà ancora una volta una radice di f_i (poiché il polinomio minimo di α_{ij} divide f).

Segue quindi che

$$\varphi(\alpha_{ij}) = \alpha_{i,j'} \in \mathbb{F}$$

per un qualche $j' \in \{1, \dots, n_i\}$.

Ma allora φ manda i generatori di $\mathbb{F}$ in elementi di $\mathbb{F}$, dunque

$$\varphi(\mathbb{F}) \subseteq \mathbb{F}.$$

Siccome φ è iniettivo segue che $\varphi(\mathbb{F})$ e $\mathbb{F}$ hanno la stessa dimensione finita su $\mathbb{K}$ come spazi vettoriali, dunque $[\mathbb{F} : \mathbb{K}] = [\varphi(\mathbb{F}) : \mathbb{K}]$, da cui $\varphi(\mathbb{F}) = \mathbb{F}$ e quindi $\mathbb{F} / \mathbb{K}$ è un'estensione normale. □

Proposizione 4.6.5 – Estensione di grado 2 $\implies$ normale

Sia $\mathbb{K}$ un campo con $\operatorname{char} \mathbb{K} \neq 2$ e sia $\mathbb{F} / \mathbb{K}$ di grado 2. Allora $\mathbb{F} / \mathbb{K}$ è normale.

Dimostrazione. Sia $\gamma \in \mathbb{F} \setminus \mathbb{K}$. Per quanto dimostrato dalla Proposizione 4.4.1 si ha che $\mathbb{F} = \mathbb{K}(\gamma)$. Sia allora

$$\mu_\gamma(x) = x^2 + b_1 x + b_0 \in \mathbb{K}[x]$$

il polinomio minimo di γ su $\mathbb{K}$ e siano γ_1, γ_2 le sue radici.

Per l'Osservazione 4.4.2 sappiamo che

$$\mathbb{F} = \mathbb{K}\left(\sqrt{\Delta}\right)$$

dove Δ è il discriminante dell'equazione

$$\mu_\gamma(x) = x^2 + b_1 x + b_0 = 0,$$

ovvero $\Delta := b_1^2 - 4b_0$. Per la formula risolutiva delle equazioni di secondo grado allora

$$\gamma_{1/2} = \frac{-b_1 \pm \sqrt{\Delta}}{2},$$

ovvero $\gamma_{1/2} \in \mathbb{K}\left(\sqrt{\Delta}\right) = \mathbb{F}$.

Segue quindi che $\mathbb{F}$ è il campo di spezzamento di μ_γ, dunque per la Proposizione 4.6.4 $\mathbb{F} / \mathbb{K}$ è normale. □

4.6.1 Proprietà delle estensioni normali

Studiamo ora come si comportano le estensioni normali rispetto alle solite operazioni che compiamo sui campi, ovvero l'intersezione, il composto e le torri di estensioni.

Composto ed intersezione