APPUNTI DI ALGEBRA

Manuel Deodato

Indice

1 | Teoria dei gruppi

§1.1 Il gruppo degli automorfismi

Lemma 1.0.1. Siano H, G due gruppi ciclici; un omomorfismo $\varphi : G \to H$ è univocamente determinato da come agisce su un generatore di G.

Dimostrazione. Sia $g_0 \in G$ tale che $\langle g_0 \rangle = G$ e sia $\varphi(g_0) = \overline{h} \in H$. Per $g \in G$ generico, per cui $g_0^k = g$ per qualche intero k, si ha:

$$\varphi(g) = \varphi(g_0^k) = \varphi(g_0)^k = \overline{h}^k$$

Cioè tutti gli elementi di $\operatorname{Im}\varphi$ sono esprimibili come potenze di $\overline{h}$. □

Osservazione 1.1. Non ogni scelta di $\overline{h} \in H$ è ammissibile, ma bisogna rispettare l'ordine di g_0. Se $g_0^n = e_G$, allora $e_H = \varphi(g_0^n) = \varphi(g_0)^n = \overline{h}^n$. Questa condizione, impone che $\operatorname{ord}(\overline{h}) \mid \operatorname{ord}(g_0)$.

Definizione 1.1 (Gruppo degli automorfismi). Sia G un gruppo; si definisce il gruppo dei suoi automorfismi come

$$\operatorname{Aut}(G) = \{f : G \to G \mid f \text{ è un isomorfismo di gruppi}\}$$

Esempio 1.1. Si calcola $\operatorname{Aut}(\mathbb{Z})$.

Svolgimento. Il gruppo $(\mathbb{Z}, +)$ è ciclico, quindi un omomorfismo è determinato in base a come agisce su un generatore. Prendendo, per esempio 1, si definisce $q_a : \mathbb{Z} \to \mathbb{Z}$ tale che $q_a(1) = a$; perché $\langle q_a(1) \rangle = \mathbb{Z}$[a], è necessario che a sia un generatore di $\mathbb{Z}$, perciò sono ammessi $a = \pm 1$. In questo caso, $\operatorname{Aut}(\mathbb{Z}) = \{\pm \operatorname{Id}_{\mathbb{Z}}\} \cong (\mathbb{Z}/2\mathbb{Z}, +)$. ■

[a] Richiesto dal fatto che q_a sia suriettivo.

Teorema 1.1. $\operatorname{Aut}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^*$.

Dimostrazione. $(\mathbb{Z}/m\mathbb{Z}, +)$ è ciclico, quindi si stabilisce l'azione di $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ su un generatore. Preso, allora, $\overline{k} \in \mathbb{Z}/m\mathbb{Z}$ tale che $\gcd(k, m) = 1$ e scelto $f(\overline{k}) = \overline{a}$, si ha che $\langle f(\overline{k}) \rangle = \langle \overline{a} \rangle = \mathbb{Z}/m\mathbb{Z} \iff \gcd(a, m) = 1 \iff \overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$. □

Definizione 1.2 (Automorfismo interno). Sia G un gruppo; si definisce $\phi_g : G \to G$, $\forall g \in G$, come $\phi_g(x) = gxg^{-1}$ ed è detto *automorfismo interno*. L'insieme di questi automorfismi, al variare di $g \in G$, forma il gruppo

$$\mathrm{Int}(G) = \{\phi_g : G \to G \mid g \in G \text{ e } \phi_g \text{ automorfismo interno}\}$$

Proposizione 1.1. Sia G un gruppo; allora $\mathrm{Int}(G) \lhd \mathrm{Aut}(G)$ e $\mathrm{Int}(G) \cong G/Z(G)$.

Dimostrazione. $\mathrm{Int}(G)$ è un sottogruppo di $\mathrm{Aut}(G)$ perché $\mathrm{Id}(x) = exe^{-1} = x \Rightarrow \mathrm{Id} \in \mathrm{Int}(G)$. Inoltre, $\phi_g \circ \phi_h(x) = ghxh^{-1}g^{-1} = \phi_{gh}(x) \in \mathrm{Int}(G)$ e $\phi_{g^{-1}} \circ \phi_g(x) = x \Rightarrow \phi_g^{-1} = \phi_{g^{-1}} \in \mathrm{Int}(G)$.

È un sottogruppo normale perché $\forall f \in \mathrm{Aut}(G)$, si ha

$$f \circ \phi_g \circ f^{-1}(x) = f\left(gf^{-1}(x)g^{-1}\right) = f(g)xf(g)^{-1} \in \mathrm{Int}(G)$$

Per finire, si definisce $\Phi : G \to \mathrm{Int}(G)$. Questo è un omomorfismo perché $\Phi(gh) = \phi_{gh} = \phi_g \circ \phi_h = \Phi(g)\Phi(h)$. È, inoltre, suriettivo perché ogni automorfismo interno è associato ad un elemento di G, cioè $\forall \phi_g \in \mathrm{Int}(G),\ \exists g \in G : \Phi(g) = \phi_g$. Allora, la tesi deriva dal I teorema di omomorfismo, visto che $\mathrm{Ker}\,\Phi = Z(G)$. □

Osservazione 1.2. $H \lhd G \iff \phi_g(H) = H,\ \forall \phi_g \in \mathrm{Int}(G)$.

Dimostrazione. Per ogni elemento di $\mathrm{Int}(G)$, si ha $\phi_g(H) = H \iff gHg^{-1} = H \iff H \lhd G$. □

Definizione 1.3 (Sottogruppo caratteristico). Sia G un gruppo e $H < G$. Si dice che H è *caratteristico* se è invariante per automorfismo, cioè $\forall f \in \mathrm{Aut}(G),\ f(H) = H$.

Corollario 1.1.1. Sia G un gruppo; per la proposizione 1.1 e l'osservazione 1.2 se H è caratteristico, allora $H \lhd G$.

Il viceversa è falso, cioè normale $\not\Rightarrow$ caratteristico; infatti, in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, il sottogruppo $\langle(1,0)\rangle$ è normale, ma non caratteristico perché l'automorfismo che scambia le coordinate è tale per cui $\langle(1,0)\rangle \mapsto \langle(0,1)\rangle \neq \langle(1,0)\rangle$.

§1.2 Azioni di gruppo

Definizione 1.4 (Azione). Sia G un gruppo; un'azione di G su un insieme X è un omomorfismo

$$\gamma : \begin{array}{ccc} G & \longrightarrow & S(X) = \{f : X \to X \mid f \text{ biettiva}\} \\ g & \longmapsto & \psi_g : \psi_g(x) = g \cdot x \end{array}$$

Più concretamente, si definisce *azione* la mappa $\gamma : G \times X \to X$ tale che

(a). $e \cdot x = x$, per $e \in G$ e $x \in X$;

(b). $h \cdot (g \cdot x) = (hg) \cdot x$, per $g, h \in G$ e $x \in X$.

Si verifica che una mappa $\gamma : G \times X \to X$, con G gruppo e X insieme generico, che soddisfi le proprietà (a) e (b), è tale che $\gamma(g)(x) = \psi_g(x)$ (cioè a g fissato) è biettiva.

Dimostrazione. Per l'iniettività, si ha $\psi_g(x) = \psi_g(y) \iff g \cdot x = g \cdot y \iff x = y$, visto che si può applicare l'azione inversa $\gamma(g^{-1})$ ad entrambi i lati. Per la suriettività, invece, si nota che $\forall x \in X$, si trova anche una $y \in X : y = g^{-1} \cdot x$ dovuta all'azione di $\gamma(g^{-1})$, per cui $\psi_g(y) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = x$. □

Esempio 1.2. Sia $G = \{z \in \mathbb{C}^* \mid |z| = 1\} \cong S^1$ la circonferenza unitaria e $X = \mathbb{R}^2$. Un'azione di G su X è una rotazione definita da $\gamma(z) = R(\arg z)$. Questa è un omomorfismo perché $\gamma(zw) = R(\arg zw) = R(\arg z + \arg w) = R(\arg z)R(\arg w) = \gamma(z)\gamma(w)$.

Un'azione γ di G su X definisce, proprio su X, una relazione di equivalenza definita da

$$x \sim_\gamma y \iff x = \psi_g(y) = g \cdot y, \text{ con } x, y \in X \tag{1.2.1}$$

La relazione di equivalenza è ben definita perché le ψ_g sono mappe biettive.

Definizione 1.5 (Orbita). Sia $\gamma : G \to S(X)$ un'azione di G gruppo su X. Dato $x \in X$, la sua classe di equivalenza rispetto alla relazione $\sim_\gamma$ è detta *orbita* ed è indicata con $\mathrm{Orb}(x) = \{g \cdot x \mid g \in G\}$.

Ricordando che una relazione di equivalenza fornisce una partizione dell'insieme su cui è definita, si ha:

$$X = \bigsqcup_{x \in R} \mathrm{Orb}(x) \tag{1.2.2}$$

con R insieme dei rappresentati di tutte le orbite. Se, poi, X ha cardinalità finita, allora:

$$|X| = \sum_{x \in R} |\mathrm{Orb}(x)| \tag{1.2.3}$$

Definizione 1.6 (Stabilizzatore). Sia $\gamma : G \to S(X)$ un'azione di G su X; allora per ogni $x \in X$, si definisce l'insieme

$$\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\} < G$$

Lemma 1.1.1. Sia G un gruppo che agisce su un insieme X e sia $x \in X$ un suo elemento. Dati anche $g \cdot x, h \cdot x \in \mathrm{Orb}(x)$ tali che $g \cdot x = h \cdot x$, allora g e h appartengono alla stessa classe di $G/\mathrm{Stab}(x)$.

Dimostrazione. Se $g \cdot x,\ h \cdot x \in \mathrm{Orb}(x)$ sono uguali, allora $x = h^{-1}g \cdot x$, cioè $h^{-1}g \in G$ lascia invariato x, quindi è in $\mathrm{Stab}(x)$. Da questo segue che $h\,\mathrm{Stab}(x) = hh^{-1}g\,\mathrm{Stab}(x) = g\,\mathrm{Stab}(x)$. □

Teorema 1.2 (Teorema di orbita-stabilizzatore). Esiste una mappa biettiva $\Gamma : \mathrm{Orb}(x) \to G/\mathrm{Stab}(x)$ tale che $\Gamma(g \cdot x) = g\,\mathrm{Stab}(x)$.

Dimostrazione. Γ è iniettiva come diretta conseguenza del lemma 1.1.1 ed è suriettiva perché $\forall g\,\mathrm{Stab}(x) \in G/\mathrm{Stab}(x), \exists g \cdot x \in \mathrm{Orb}(x)$ tale che $\Gamma(g \cdot x) = g\,\mathrm{Stab}(x)$. Segue che $|\mathrm{Orb}(x)| = |G|/|\mathrm{Stab}(x)|$. □

Osservazione 1.3. Si osserva che, per il teorema di orbita-stabilizzatore, la cardinalità di un'orbita indica il numero di classi laterali dello stabilizzatore nel gruppo che compie l'azione, cioè il teorema di orbita-stabilizzatore si può riscrivere come $|\mathrm{Orb}(x)| = [G : \mathrm{Stab}(x)] = |G/\mathrm{Stab}(x)| = |G|/|\mathrm{Stab}(x)|$.

§1.2.1 Azione di coniugio

Un caso notevole di azione è il coniugio: per $X = G$, si definisce $\gamma : G \to \mathrm{Int}(G) \subset S(G)$. Le orbite indotte da questa azione sono dette *classi di coniugio* e si indicano con $\mathrm{Cl}(x)$, mentre lo stabilizzatore è detto *centralizzatore* e si indica con:

$$Z(x) = \left\{g \in G \mid g \cdot x = gxg^{-1} = x\right\} \tag{1.2.4}$$

Come conseguenza del teorema di orbita-stabilizzatore (1.2), si ha:

$$|G| = |\mathrm{Cl}(x)||Z(x)|,\ \forall x \in G \tag{1.2.5}$$

Proposizione 1.2. Sia G un gruppo e γ l'azione di coniugio su di esso; allora

$$\bigcap_{x \in G} Z(x) = Z(G)$$

Dimostrazione. Si ha $g \in Z(x),\ \forall x \iff gxg^{-1} = x,\ \forall x \in G \iff g \in Z(G)$. □

Osservazione 1.4 (Centro di un sottogruppo). Sia G un gruppo e $H < G$; allora il centro di H è definito come

$$\bigcap_{x \in H} Z(x) = Z(H)$$

Si considera, ora, l'azione di coniugio di un gruppo G su $X = \{H \subseteq G \mid H < G\}$ e $\gamma(g) = \psi_g$ tale che $\psi_g(H) = gHg^{-1}$. Questa è un'azione ed è ben definita.

Dimostrazione. Per dimostrare che è un'azione, si deve mostrare che la mappa $g \overset{\gamma}{\mapsto} \psi_g$ è un omomorfismo e che $\psi_g : X \to X$ sia biettiva.

Si nota che $g \overset{\gamma}{\mapsto} \psi_g$ è un omomorfismo perché $\psi_{g_1g_2}(H) = g_1g_2Hg_2^{-1}g_1^{-1} = \psi_{g_1} \circ \psi_{g_2}(H)$, cioè $g_1g_2 \mapsto \psi_{g_1}\psi_{g_2}$. Inoltre, $\psi_g : X \to X$ è biettiva perché $\exists \psi_g^{-1} = \psi_{g^{-1}} : \psi_{g^{-1}} \circ \psi_g(H) = H$.

Per mostrare che è ben definita, si fa vedere che effettivamente $\forall g, \psi_g$ mappa un sottogruppo di G in un altro sottogruppo, cioè che $gHg^{-1} < G$. Intanto, $e \in gHg^{-1}$ perché $H < G \Rightarrow e \in H \Rightarrow geg^{-1} = e$; poi, $(ghg^{-1})(gh'g^{-1}) = ghh'g^{-1} \in gHg^{-1}$ e $h^{-1} \in H \Rightarrow \exists (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$ elemento inverso. □

Lo stabilizzatore di questa azione è detto *normalizzatore*, in quanto è definito come tutti elementi di G rispetto a cui H è normale:

$$N_G(H) = \mathrm{Stab}(H) = \left\{g \in G \mid gHg^{-1} = H\right\} \tag{1.2.6}$$

Infine, l'orbita è l'insieme (classe di equivalenza) di tutti i coniugati di un sottogruppo di G:

$$\mathrm{Orb}(H) = \left\{gHg^{-1} \mid g \in G\right\} \tag{1.2.7}$$

Per il teorema di orbita-stabilizzatore (1.2), si ha:

$$|G| = |N_G(H)||\mathrm{Orb}(H)| \tag{1.2.8}$$

da cui si ricava anche che $H \lhd G \iff N_G(H) = G \iff \mathrm{Orb}(H) = \{H\}$.

§1.2.2 Formula delle classi

Si ricorda che le orbite definite da un'azione di un gruppo G su un insieme X formano una partizione di X stesso, in quanto sono delle classi di equivalenza. Se $|X| < \infty$, si ha:

$$|X| = \sum_{x\in R} |\mathrm{Orb}(x)| = \sum_{x\in R} \frac{|G|}{|\mathrm{Stab}(x)|} = \sum_{x\in R'} 1 + \sum_{x\in R\setminus R'} \frac{|G|}{|\mathrm{Stab}(x)|} \tag{1.2.9}$$

con R insieme dei rappresentanti delle orbite e R' insieme dei rappresentati delle orbite tali che $\mathrm{Orb}(x) = \{x\}$, cioè degli elementi invarianti sotto l'azione di G.

Teorema 1.3 (Formula delle classi). Sia $\gamma : G \to S(G)$ l'azione di coniugio di un gruppo G su un insieme X; allora:

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

Dimostrazione. Segue per quanto appena detto e dall'osservazione che

$$R' = \{x \in R \mid \mathrm{Orb}(x) = x\} = \left\{x \in R \mid gxg^{-1} = x\right\} = Z(G)$$

Visto che ogni orbita del genere contiene un solo elemento, i rappresentanti delle orbite sono esattamente tutti gli elementi di $Z(G)$, cioè un elemento $x \in Z(G)$ non può essere contenuto in nessun'altra orbita, se non nel singoletto $\{x\}$. Perciò, la relazione in eq. 1.2.9, avendo $X = G$, conferma la tesi. $\square$

§1.3 I p-gruppi

Definizione 1.7 (p-gruppo). Sia $p \in \mathbb{Z}$ un numero primo; allora si dice che G è p-gruppo se $|G| = p^n$, per qualche $n \in \mathbb{N}$.

Proposizione 1.3. Il centro di un p-gruppo è non-banale.

Dimostrazione. Per la formula delle classi, si ha:

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

Se $|Z(G)| = p^n$, la tesi è verificata, altrimenti $\exists x \in R\setminus Z(G)$, quindi tale che $Z(x) \subsetneq G$; allora, per $k_x \in \mathbb{N}$, si ha $|G|/|Z(x)| = p^{k_x}$, con almeno un $k_x > 0$, da cui:

$$|Z(G)| = p^n - \sum_{x\in R\setminus Z(G)} p^{k_x} \implies p \mid |Z(G)|$$

Visto che $e \in Z(G)$, deve risultare $|Z(G)| \geq 1$, pertanto $|Z(G)| = p^s$, per qualche intero $s > 1$. □

Lemma 1.3.1. Vale $G/Z(G)$ ciclico $\iff$ G è abeliano.

Dimostrazione. Sia $G/Z(G)$ ciclico e sia $x_0 Z(G)$ il suo generatore. Date due classi laterali distinte $xZ(G), yZ(G) \in G/Z(G)$ e visto che $x_0 Z(G)$ genera, si avrà $x_0^m Z(G) = xZ(G)$ e $x_0^n Z(G) = yZ(G)$, ossia, per $z, w \in Z(G)$, $x = x_0^m z$, $y = x_0^n w$. Allora:

$$xy = x_0^m z x_0^n w = x_0^m x_0^n z w = x_0^n w x_0^m z = yx$$

Essendo questo valido per $x, y \in G$ generiche, si è dimostrata l'implicazione verso destra.

Per l'implicazione inversa, sia G abeliano; allora $Z(G) = G$ e $G/Z(G) = \{e\}$, che è ovviamente ciclico. □

Proposizione 1.4. Un gruppo di ordine p^2 è abeliano.

Dimostrazione. Sia G un p-gruppo tale che $|G| = p^2$. Per mostrare che è abeliano, si fa vedere che $Z(G) = G$, ossia $|Z(G)| = p^2$. Per la proposizione 1.3, si può avere solamente $|Z(G)| = p$, oppure $|Z(G)| = p^2$. Se, per assurdo, fosse $|Z(G)| = p$, allora $|G|/|Z(G)| = p$, quindi $G/Z(G)$ avrebbe ordine primo e, quindi, sarebbe ciclico; per il lemma precedente (1.3.1), però, questo è assurdo perché risulterebbe anche abeliano al contempo, ma senza avere $|Z(G)| = |G|$. Quindi deve essere $|Z(G)| = p^2 = |G| \Rightarrow Z(G) = G$, da cui G è abeliano. □

§1.4 Teoremi di Cauchy e Cayley

Lemma 1.3.2 (Teorema di Cauchy abeliano). Sia p un primo e G un gruppo abeliano finito; se $p \mid |G|$, allora $\exists x \in G : \operatorname{ord}(x) = p$.

Dimostrazione. Sia $|G| = pn$; si procede per induzione su n. Il passo base è ovvio: se $|G| = p$, allora è ciclico e, quindi, contiene un elemento di ordine p.

Per il passo induttivo, si suppone che la tesi sia vera per ogni $m < n$ e si dimostra per n.

Sia, allora $|G| = pn$; sia, poi $y \in G$, $y \neq e$ tale che $\langle y \rangle = H < G$: per Lagrange, $|G| = |G/H||H|$. Allora, se $p \mid |G| \Rightarrow p \mid |H|$, oppure $p \mid |G/H|$.

- Se $p \mid |H|$, allora può essere $|G| = |H|$, caso in cui $G = \langle y \rangle$ sarebbe ciclico e, quindi, avrebbe un elemento di ordine p[a], oppure può essere $|H| = pm < pn$, caso in cui l'elemento di ordine p è presente per ipotesi induttiva.

- Se $p \mid |G/H|$, invece, allora $|G/H| = pm' < pn$ perché H contiene almeno due elementi, cioè y ed e; per ipotesi induttiva, allora, esiste $zH \in G/H$ il cui ordine è p. Considerando la proiezione $\pi_H : G \to G/H$ tale che $x \mapsto xH$ e ricordando che è un omomorfismo, si ha che, per questo motivo, $\text{ord}(zH) \mid \text{ord}(z) \Rightarrow \text{ord}(z) = pk$; se $k = n$, allora G è ciclico e z^n ha ordine p, altrimenti, se $k < n$, si ha la tesi per induzione.

□

[a] In questo caso, l'elemento di ordine p sarebbe proprio $y^{p^{n-1}} \in G$; infatti, $(y^{p^{n-1}})^p = y^{p^n} = e$, visto che $|G| = p^n$.

Teorema 1.4 (Teorema di Cauchy). Sia p un numero primo e G un gruppo finito; se $p \mid |G|$, allora esiste $x \in G : \text{ord}(x) = p$.

Dimostrazione. Sia $|G| = pn$, con p primo e $n \in \mathbb{N}$; si procede per induzione su n. Se $n = 1$, $|G| = p \Rightarrow G$ è ciclico, quindi $\exists x \in G : \langle x \rangle = G$ e $\text{ord}(x) = p$.

Per il passo induttivo, si assume che la tesi sia valida per ogni $m < n$ e si dimostra per n.

Si nota che se $\exists H < G$ tale che $p \mid |H|$, allora $|H| = pm$, $m < n \Rightarrow \exists x \in H$ tale che $\text{ord}(x) = p$ per ipotesi induttiva. Si assume, dunque, che non esista alcun sottogruppo di G il cui ordine sia divisibile per p. Per la formula delle classi

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

Ora, visto che $Z(x) < G \Rightarrow p$ non divide $|Z(x)|$, quindi si ha la certezza che, essendo $p \mid |G| = |Z(x)||G|/|Z(x)|$, p divide $|G|/|Z(x)|$. Allora $p \mid |Z(G)|$, per cui $Z(G) = G$; infatti, se così non fosse, sarebbe un sottogruppo proprio di G e p non lo potrebbe dividere, il che è assurdo.

Da questo, segue che G è abeliano, quindi la tesi segue dal teorema di Cauchy per gruppi abeliani (lemma 1.3.2). □

Proposizione 1.5. Siano $H, K < G$; allora $HK < G \iff HK = KH$ e $|HK| = |H||K|/|H \cap K|$.

Dimostrazione. Per la prima parte, è sufficiente osservare che per $hk \in HK$, l'elemento neutro $(hk)^{-1} = k^{-1}h^{-1}$ sta in HK se e solo se $HK = KH$, e, allo stesso modo, il prodotto è chiuso cioè $hkh'k' = hh''k''k' \in HK$ solamente se $HK = KH$ così da poter trovare un elemento di HK che sia uguale a $kh' \in KH$ che compare in tale prodotto.

La seconda parte, invece, si verifica considerando l'applicazione $\gamma : H \times K \to HK$ tale che $\gamma((h,k)) = hk$, che è evidentemente suriettiva; inoltre, se $s \in H \cap K$, allora $(hs, s^{-1}k) \in H \times K \Rightarrow \gamma((hs, s^{-1}k)) = hk$, il che vuol dire che $\forall hk \in HK$, si trovano $|H \cap K|$ coppie in $H \times K$ che hanno immagine hk, da cui la tesi. □

Esempio 1.3 (Classificazione dei gruppi di ordine 6). Sia G un gruppo di ordine 6; per Cauchy, allora, esistono $x, y \in G$ tali che $\mathrm{ord}(x) = 2$ e $\mathrm{ord}(y) = 3$. Se G è abeliano, poi, si ha $\mathrm{ord}(xy) = 6$[a], quindi $G = \langle xy \rangle \cong \mathbb{Z}/6\mathbb{Z}$.

Se, invece, G non è abeliano, si considera il sottogruppo $\langle x, y \rangle$ e si considera anche l'insieme $\langle x \rangle \langle y \rangle$ che, in generale, non è un sottogruppo.

Applicando la proposizione precedente (1.5), si ha che $|\langle x, y \rangle| = (3 \cdot 2)/1 = 6$[b], da cui $G = \langle x \rangle \langle y \rangle$, con $\langle x \rangle = \{e, x\}$ e $\langle y \rangle = \{e, y, y^2\}$, quindi $G = \{e, x, y, xy, y^2, xy^2\}$.

Per finire, si mostra che $G \cong S_3$. Per farlo, si definisce $\phi : G \to S_3 = \{e, \tau, \rho, \tau\rho, \tau^2, \rho\tau^2\}$ tale che $\phi(x) = \rho$ e $\phi(y) = \tau$, con $\tau = (1,2,3)$ e $\rho = (1,2)$. Questa mappa è suriettiva per costruzione, quindi è biettiva per questioni di cardinalità; inoltre, è un omomorfismo, da cui segue la tesi.

[a] $\langle x \rangle \cap \langle y \rangle e$ perché sono generati da elementi diversi, altrimenti avrebbero stesso ordine.

[b] Come già accennato, l'intersezione è solo l'unità perché i due elementi hanno ordini diversi, quindi generano gruppi disgiunti.

Teorema 1.5 (Teorema di Cayley). Sia G un gruppo; allora G è isomorfo a un sottogruppo di $S(G)$. In particolare, se $|G| = n$, allora G è isomorfo a un sottogruppo di S_n.

Dimostrazione. Si definisce l'azione

$$\phi : \begin{array}{ccc} G & \longrightarrow & S(G) \\ g & \longmapsto & \gamma_g \end{array}, \quad \text{tale che } \gamma_g(x) = g \cdot x = gx$$

Questa è ben definita perché $\gamma : G \to G$ è biettiva, infatti $\gamma_g(x) = \gamma_g(y) \iff gx = gy \iff x = y$ e $\forall y \in G$, $\exists \gamma_g(g^{-1}y) = y$, il che mostra che è rispettivamente iniettiva e suriettiva. Inoltre, ϕ è un omomorfismo (ovvio) ed è anche iniettiva perché $\mathrm{Ker}\,\phi = \{g \in G \mid \phi_g = \phi_e\} = \{g \in G \mid gx = x\} = \{e\}$. Da questo, segue che $S(G)$ contiene una copia isomorfa a G. □

§1.5 Commutatore e gruppo derivato

Definizione 1.8. Sia G un gruppo e $S \subset G$ un suo sottoinsieme; allora $\langle S \rangle$ è il più piccolo sottogruppo di G contenente anche S.

Proposizione 1.6. Dato G un gruppo e $S \subset G$ un suo sottoinsieme, vale la relazione

$$\langle S \rangle = \left\{ s_1 s_2 \dots s_k \mid k \in \mathbb{N},\ s_i \in S \cup S^{-1} \right\} = X$$

con $S^{-1} = \{s^{-1} \mid s \in S\}$.

Dimostrazione. Per definizione

$$\langle S \rangle = \bigcap_{\substack{H<G \\ S \subset H}} H$$

Questa scrittura è ben definita perché l'intersezione di gruppi è ancora un gruppo e, in questo modo, si ha il gruppo più piccolo contenente S; se così non fosse, ne esisterebbe uno più piccolo ancora, che, però, farebbe parte dell'intersezione e sarebbe assurdo.

Ora, per quanto detto sopra, S è contenuto in tutti i gruppi la cui intersezione genera $\langle S \rangle$, quindi anche S^{-1} deve essere contenuto in tali sottogruppi di G. Segue che $S, S^{-1} \subset H \Rightarrow X \subset H,\ \forall H < G$ e $S \subset H$, quindi $X \subset \bigcap H = \langle S \rangle$.

Allo stesso tempo, X è evidentemente un sottogruppo di G e contiene S per costruzione, quindi $X \supset \langle S \rangle$, da cui la tesi. □

Definizione 1.9 (Commutatore). Sia G un gruppo; dati $g, h \in G$, il loro *commutatore* è definito come

$$[g, h] = ghg^{-1}h^{-1}$$

Definizione 1.10 (Gruppo derivato). Dato un gruppo G, si definisce *gruppo dei commutatori*, o *derivato* di G, il gruppo

$$G' = \langle [g, h] \mid g, h \in G \rangle = [G : G]$$

Ora si caratterizza il gruppo derivato. Intanto, si ricorda che $\langle S \rangle$ è abeliano $\iff \forall s_1, s_2 \in S,\ s_1 s_2 = s_2 s_1$, $\langle S \rangle$ è normale $\iff \forall g \in G, \forall s \in S,\ gsg^{-1} \in \langle S \rangle$ e, infine, $\langle S \rangle$ è caratteristico $\iff \forall f \in \mathrm{Aut}(G),\ \forall s \in S$ si ha $f(s) \in S$. Applicando queste alla definizione di commutatore, si ottiene la seguente.

Proposizione 1.7 (Proprietà del derivato). Sia G un gruppo e G' il suo derivato; allora:

(a). $G' = \{e\} \iff G$ è abeliano;

(b). $G' \lhd G$;

(c). G' è caratteristico in G;

(d). dato $H \lhd G$, se G/H è abeliano, allora $G' \subset H$.

Dimostrazione. La (a) è immediata perché $G' = \{e\} \iff \forall g_1, g_2 \in G,\ [g_1, g_2] = e$, cioè g_1 e g_2 commutano, da cui G abeliano.

Per la (b), $\forall x \in G,\ \forall g, h \in G$, si ha

$$\begin{aligned} x[g,h]x^{-1} &= xghg^{-1}h^{-1}x^{-1} = xgx^{-1}xhx^{-1}xg^{-1}x^{-1}xh^{-1}x^{-1} \\ &= [xgx^{-1}, xhx^{-1}] \in G' \end{aligned}$$

Per la (c), si nota che $\forall f \in \mathrm{Aut}(G),\ \forall g, h \in G$, si ha:

$$f([g,h]) = f(ghg^{-1}h^{-1}) = f(g)f(h)f(g)^{-1}f(h)^{-1} = [f(g), f(h)] \in G'$$

Infine, per la (d), se $H \lhd G$ e G/H è abeliano, si ha $\forall x, y \in G$

$$xHyH = yHxH \Rightarrow xyH = yxH \implies x^{-1}y^{-1}xy \in H \Rightarrow [x,y] \in H$$

da cui $H \supset G'$. □

Corollario 1.5.1. Sia G un gruppo e G' il suo derivato; allora G/G' è sempre abeliano ed è chiamato *abelianizzazione* di G, nel senso che è il più grande quoziente abeliano di G.

Dimostrazione. Si mostra che G/G' è sempre abeliano. Siano, quindi $gG', hG' \in G/G'$ due classi laterali; allora si osserva che

$$(gG')(hG') = ghG' = hg[g^{-1}, h^{-1}]G' = hgG'$$

visto che $g^{-1}h^{-1}gh = [g^{-1}, h^{-1}] \in G'$. Allora, dalla proprietà (d) della precedente proposizione (1.7), si ha $G' \subset H = G'$, cioè in questo caso si ha l'inclusione nell'insieme più piccolo, ovvero proprio G'. Questo vuol dire che G/G' è il quoziente con più elementi che sia abeliano perché ottenuto tramite quoziente con G', che è l'insieme più piccolo che soddisfa la proprietà[a]. □

[a]Per controposizione, se $G' \not\subset H \implies G/H$ non abeliano.

§1.6 Gruppi liberi

Si definisce l'insieme $S = \{x_1, x_2, x_3, \dots\}$ di simboli arbitrari, che può essere finito o infinito, e si definisce *parola* una qualunque loro concatenazione, in cui sono ammesse ripetizioni. L'insieme delle parole ottenibili a partire dagli elementi di S si indica con W. Le concatenazioni dello stesso simbolo si possono esprimere in notazione esponenziale: $x_1 x_1 \dots x_1 = x_1^n$.

Per arrivare alla costruzione di un gruppo, servono degli inversi ed un elemento neutro; l'elemento neutro si indica con 1 ed è tale per cui

$$1 \cdot \prod_i x_i^{a_i} = \prod_i x_i^{a_i} \cdot 1 = \prod_i x_i^{a_i}$$

L'insieme degli elementi inversi, invece, si indica con S^{-1} e si definisce $S' = S \cup S^{-1}$. Indicando, ora, con W' l'insieme delle parole che si possono costruire in S', si nota la possibilità di trovare una sequenza della forma $\dots xx^{-1} \dots$, oppure $\dots x^{-1}x \dots$; questo indica che la parola può essere opportunamente ridotta cancellando tali simboli, cioè usando la definizione $x^{-1}x = xx^{-1} = 1$.

Definizione 1.11 (Parola ridotta). Una parola di W' si dice *ridotta* se non è possibile operare ulteriori cancellazioni.

A partire da una stessa parola, o dalle sue cancellazioni, è possibile operare la riduzione cancellando i termini in ordine diverso, ma giungendo sempre allo stesso risultato. Alla luce di questo, si ha la seguente definizione.

Definizione 1.12 (Parole equivalenti). Due parole $w, w' \in W'$ si dicono *equivalenti*, e si scrive $w \sim w'$, se hanno la stessa forma ridotta w_0.

Osservazione 1.5. Si può dimostrare che $\sim$ è una relazione di equivalenza.

Proposizione 1.8. Sia F l'insieme delle classi di equivalenza di parole in W'; allora F è un gruppo rispetto alla legge di composizione indotta W'.

Dimostrazione. La concatenazione di parole di W' è associativa e la legge di composizione indotta da questa tra le parole che rappresentano una classe di equivalenza sarà altrettanto associativa. Inoltre, la classe dell'elemento neutro 1 è l'identità e la classe della parola inversa di w è l'inversa della classe di w. $\square$

Definizione 1.13 (Gruppo libero). Si definisce *gruppo libero sull'insieme* S il gruppo F con la composizione indotta da W'.

Si indica con F_1 il gruppo libero su $S = \{x\}$, cioè è il gruppo generato da un singolo simbolo e da tutte le sue concatenazioni, quindi da tutte le sue potenze. Questo si sa caratterizzare bene perché, evidentemente, $F_1 \cong \mathbb{Z}$; infatti basta definire $\phi : \mathbb{Z} \to F_1$, con $\phi(k) = x^k$.

Proposizione 1.9 (Proprietà universale). Sia F_S il gruppo libero su un insieme S e sia G un gruppo; ogni applicazione tra insiemi $f : S \to G$ si estende in modo unico ad un omomorfismo di gruppi $\varphi : F_S \to G$.

Dimostrazione. Indicando con $\widetilde{x} = f(x)$, per $x \in S$, allora φ mappa una parola di S' nel corrispondente prodotto in G.

Si nota che f associa un simbolo ad un elemento di G; allora la mappa φ associa, a ciascuna parola composta dai simboli di S', la loro immagine tramite f: se $w = x_1 \cdots x_n$, allora $\varphi(w) = f(x_1) \dots f(x_n) = \widetilde{x}_1 \cdots \widetilde{x}_n$, con $\varphi(x^{-1}) = f(x)^{-1} = \widetilde{x}^{-1}$.

Due parole equivalenti di S', allora, vengono mappate nell'analogo prodotto in G, per cui risulteranno avere stessa immagine attraverso φ; questo perché se w e w' si riducono a w_0, allora la loro immagine tramite φ andrà in due elementi il cui prodotto si ridurrà al prodotto degli elementi immagine di w_0.

Infine:

$$ww' = x_1 \cdots x_n x'_1 \cdots x'_n \longmapsto \widetilde{x}_1 \cdots \widetilde{x}_n \widetilde{x}'_1 \cdots \widetilde{x}'_n = \varphi(w)\varphi(w')$$

il che prova che φ è un omomorfismo. L'unicità deriva dal fatto che φ è univocamente determinato da come f mappa gli elementi di S in quelli di G; se, infatti, si avesse $\varphi(w) = \varphi(w')$, allora si avrebbe $f(x_i) = f(x'_i)$, $\forall i$. □

Proposizione 1.10 (Presentazione di un gruppo). Sia G un gruppo generato da n elementi $g_1, \dots, g_n$ e sia F_n il gruppo libero su un insieme di n elementi; allora $F_n / \operatorname{Ker} \varphi \cong G$, con $F_n \xrightarrow{\varphi} G$.

Dimostrazione. Per la precedente proposizione, esiste un omomorfismo $\varphi : F_n \to G$ tale che a ciascun $x_i \in F_n$ è associato il relativo generatore $g_i \in G$; visto che $\{g_1, \dots, g_n\} \subset \operatorname{Im} \varphi < G$, allora $\operatorname{Im} \varphi = G$, essendo che $\operatorname{Im} \varphi$ contiene tutti i generatori di G ed ogni loro potenza. Per il I teorema di omomorfismo, allora, $F_n / \operatorname{Ker} \varphi \cong G$. □

Osservazione 1.6. Il nucleo dell'omomorfismo φ definito sopra è composto da tutte quelle relazioni che mappano i generatori nell'elemento neutro.

In realtà, il nucleo è il più piccolo sottogruppo normale ottenuto a partire dall'insieme delle relazioni, indicato con $\langle R \rangle_N$. Questo significa che se una relazione del tipo $r = 1$ vale in G, allora vale anche $xrx^{-1} = 1$, visto che $\langle R \rangle_N$ è normale per definizione e, quindi, contiene tutti i suoi coniugati.

Esempio 1.4. Si ha $\mathbb{Z}/n\mathbb{Z} = \langle x \mid (x,n) = 1 \text{ e } x^n = 0\rangle \cong F_1/\langle x^n \rangle$.

Proposizione 1.11 (Presentazione dei gruppi quoziente). Sia G un gruppo e sia $N \lhd G$. Si considera G/N, ottenuto tramite la proiezione $\pi : G \to G/N$, con $\pi(x) = \overline{x} = xN$, e si considera, dato un altro gruppo G', $\varphi : G \to G'$ un omomorfismo tale che con $N < \operatorname{Ker}\varphi$; allora $\exists! \overline{\varphi} : G/N \to G'$ tale che $\overline{\varphi} \circ \pi = \varphi$.

Dimostrazione. Si dimostra che è soddisfatto il seguente diagramma:

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & G' \\
G/N \arrow[ur, "\overline{\varphi}"'] &
\end{tikzcd}$$

con $\overline{\varphi}(\overline{a}) = \varphi(a)$.

Per poter definire $\overline{\varphi} : G/N \to G$, bisogna definire $\overline{\varphi}(\alpha)$, $\forall \alpha \in G/N$; per farlo, si sceglie $a \in G : \pi(a) = \alpha$, per cui $\alpha = \overline{a}$. Volendo che $\overline{\varphi}(\pi(a)) = \varphi(a)$, si deve definire $\overline{\varphi}$ tramite la relazione $\overline{\varphi}(\alpha) = \varphi(a)$.

Ora si fa vedere che, in questo modo, $\overline{\varphi}$ è ben definito, cioè si mostra che il valore $\overline{\varphi}(\alpha)$, cioè $\varphi(a)$, non dipende dalla scelta del rappresentante della classe di equivalenza. Siano, allora, $a, a' \in G : \overline{a} = \overline{a}' = \alpha$; l'uguaglianza $\overline{a} = \overline{a}'$ implica che $a' = an$, per qualche $n \in N$ e, visto che $N \subset \operatorname{Ker}\varphi$, si ha $\varphi(a') = \varphi(a)\varphi(n) = \varphi(a)$.

Per finire, si ha che $\overline{\varphi}$ è un omomorfismo perché $\overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b}) = \varphi(a)\varphi(b) = \varphi(ab) = \overline{\varphi}(\overline{ab})$, mentre l'unicità deriva dal fatto che, se $\exists \overline{\psi}$ tale che $\varphi = \overline{\psi} \circ \pi$, allora $\overline{\psi}(\alpha) = \overline{\psi}(\pi(a)) = \varphi(a) = \overline{\varphi}(\pi(a)) = \overline{\varphi}(\alpha)$, $\forall \alpha$. □

Teorema 1.6. Siano H, K due gruppi, con $H = \langle x_1, \dots, x_n \mid R \rangle$, cioè è generato dagli x_i, i quali soddisfano anche le relazioni $R = \{w_1, \dots, w_m\}$; allora:

$$\operatorname{Hom}(H,K) \longleftrightarrow \left\{ \{x_1, \dots, x_n\} \xrightarrow{f} K \;\middle|\; f(x_1), \dots, f(x_n) \text{ soddisfano le relazioni di } R \right\}$$

dove la doppia freccia indica una biezione.

Dimostrazione. Sia $F = \langle x_1, \dots, x_n \rangle$ il gruppo libero sui generatori $x_1, \dots, x_n$ e sia N la chiusura normale di R in F; allora, per la presentazione dei gruppi quoziente, si ha $F/N \cong H$. Sia, ora:

$$\Phi : \mathrm{Hom}(H, K) \longrightarrow \{(k_1, \dots, k_n) \in K^n : \ k_i = f(x_i) \text{ soddisfano } R\}$$

che mappa ciascun omomorfismo $f \in \mathrm{Hom}(H, K)$ nella n-upla $(f(x_1), \dots, f(x_n)) \in K^n$.

(a). Φ è ben definita.

Se $f \in \mathrm{Hom}(H, K)$, allora ogni parola $w \in R$ rappresenta l'identità in H, quindi la sua immagine tramite f è l'identità in K. Pertanto le componenti $f(x_i)$ soddisfano le relazioni di R.

(b). Φ è iniettiva.

Siano $f, g \in \mathrm{Hom}(H, K)$ tali che $\Phi(f) = \Phi(g)$; allora $\forall i, f(x_i) = g(x_i)$. Visto che gli x_i generano H, allora ogni elemento di H è una parola nei generatori; dato che f e g coincidono sui generatori, ne segue che coincidono su tutto H, quindi $f = g$.

(c). Φ è suriettiva.

Sia $(k_1, \dots, k_n) \in K^n$ una n-upla che soddisfa le relazioni di R; allora esiste un unico omomorfismo $f : F \to K$ che manda $x_i \longmapsto k_i$. Le ipotesi sulle relazioni implicano che ogni $w \in R$ viene mandata nell'identità di K, cioè $N < \mathrm{Ker}\, f$; per la presentazione dei gruppi quoziente, allora, si ha $\overline{f} : F/N \cong H \longrightarrow K$ che mappa la classe di x_i in k_i. Quindi la n-upla data è l'immagine di $\overline{f}$ tramite Φ.

Se ne conclude che Φ è una biezione, quindi esiste una corrispondenza biunivoca tra gli omomorfismi $H \to K$ e le n-uple di elementi di K che soddisfano le relazioni R. □

Osservazione 1.7. Si nota che nella formulazione del teorema si può usare indifferentemente l'insieme delle funzioni $f : \{x_1, \dots, x_n\} \longrightarrow K$, che mappano x_i in elementi di K che soddisfano R, oppure l'insieme delle n-uple $\{(k_1, \dots, k_n) \in K^n : k_i \text{ soddisfano } R\}$. Questo perché, fissato l'ordinamento dei generatori $x_1, \dots, x_n$, esiste una biezione

$$\{f : \{x_1, \dots, x_n\} \longrightarrow K\} \xrightarrow{\cong} K^n, \qquad f \longmapsto \big(f(x_1), \dots, f(x_n)\big)$$

§1.7 Gruppi diedrali

Definizione 1.14 (Gruppo diedrale). Per $n \in \mathbb{N}$, si considera un n-agono regolare nel piano; l'insieme di tutte le isometrie del piano che mandano l'n-agono in se stesso è indicato con D_n ed è noto col nome di *gruppo diedrale*.

Proposizione 1.12. Per $n \in \mathbb{N}$, il gruppo diedrale D_n ha cardinalità $|D_n| = 2n$.

Dimostrazione. Un'isometria è univocamente determinata dall'immagine di un vertice e di un lato adiacente al vertice stesso; allora, l'immagine può essere pari a n possibili vertici, con due, conseguenti, possibilità per il lato, da cui $2n$ possibili isometrie. □

Proposizione 1.13. Sia ρ una rotazione che sottende un lato[a] e σ una simmetria (riflessione) dell'n-agono regolare; allora $\rho^n = e$, $\sigma^2 = e$ e $\sigma\rho\sigma = \rho^{-1}$.

Dimostrazione. Visto che ρ manda un lato dell'n-agono regolare nella posizione del successivo, impiegherà n iterazioni a far tornare il lato di partenza nella posizione originale; similmente, se σ è una riflessione, sarà sufficiente riapplicarla per far tornare l'n-agono nella posizione originale.

Per l'ultima, si nota che, componendo una rotazione e una riflessione, si ottiene una riflessione; applicando la seconda proprietà, si ottiene $\sigma\rho\sigma\rho = e \Rightarrow \sigma\rho\sigma = \rho^{-1}$. □

[a]Cioè che manda un lato nel successivo.

Osservazione 1.8. Ponendo l'n-agono regolare nel piano $\mathbb{R}^2$, gli elementi di D_n si possono mettere in relazione con $\mathrm{GL}_2(\mathbb{R})$, visto che si possono vedere come applicazioni lineari da $\mathbb{R}^2$ in se stesso, cioè possono essere rappresentate tramite matrici[a]:

$$\rho \xmapsto{\gamma} \begin{pmatrix} \cos(2k\pi/n) & \sin(2k\pi/n) \\ -\sin(2k\pi/n) & \cos(2k\pi/n) \end{pmatrix} = M_\rho \qquad \sigma \xmapsto{\gamma} \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} = M_\sigma$$

Si nota, inoltre, che indicando con $\mathbb{D}_n$ il gruppo generato da queste matrici, allora la mappa $\gamma : \langle \rho, \sigma \rangle \to \mathbb{D}_n$ è un omomorfismo di gruppi; infatti, dati due elementi $s_1, s_2 \in \langle \rho, \sigma \rangle$:

$$\gamma(s_1 s_2)v = M_{s_1 s_2}v = (s_1 s_2)(v) = s_1(s_2(v)) = M_{s_1}M_{s_2}v = \gamma(s_1)\gamma(s_2)v$$

con $v \in \mathbb{R}^2$ e $s(v)$ è l'applicazione della rotazione o riflessione $s \in \langle \rho, \sigma \rangle$ a tale vettore di $\mathbb{R}^2$. Conseguentemente, si ha $M_\rho^n = \mathrm{Id} = M_\sigma^2$ e $M_\sigma M_\rho M_\sigma = M_\rho^{-1}$.

Essendo γ un omomorfismo, si vede anche che ρ e σ, come elementi di D_n, non sono legati da alcuna relazione perché, altrimenti, lo sarebbero anche le loro matrici associate, cosa che sarebbe assurda.

[a] Le riflessioni così definite devono essere rispetto ad un asse opportuno, cioè che sia un asse di simmetria per l'n-agono in questione. Nella matrice delle riflessioni, l'angolo θ è l'angolo dell'asse rispetto a cui si riflette ed è preso con riferimento all'asse x.

Proposizione 1.14. Tutti gli elementi di D_n si scrivono come $\sigma\rho^i$, oppure ρ^i, con $i \in \{0, \dots, n-1\}$.

Dimostrazione. Sia $g \in D_n$; allora g sarà una generica composizione di riflessioni e rotazioni del tipo $g = \rho^{a_1}\sigma^{b_1} \dots \rho^{a_k}\sigma^{b_k}$, dove $a_i \in \mathbb{Z}$ e $b_j \in \{0,1\}$. Usando le relazioni $\sigma^2 = \rho^n = e$, si riscalano gli esponenti per scrivere $g = \rho^{c_1}\sigma \dots \rho^{c_m}\sigma$, dove si sono anche, eventualmente, uniti esponenti di rotazioni consecutive (quindi $m \leq k$). Ora, utilizzando la relazione $\rho\sigma = \sigma\rho^{-1}$, è possibile spostare tutte le σ verso l'estrema sinistra, cioè come primo termine della parola; così facendo, si vede che tale parola diventa o una potenza di ρ, oppure un termine del tipo $\sigma\rho^d$, che è esattamente quello che si voleva dimostrare. $\square$

Grazie alla precedente proposizione, è possibile definire $\rho^{[i]} = \rho^i$, con $[i] \in \mathbb{Z}/n\mathbb{Z}$, visto che $\rho^n = e$.

Inoltre, se $\rho, \sigma \in D_n$, allora $\langle \rho, \sigma \rangle < D_n$; però, per quanto detto finora, si ha $|\langle \rho, \sigma \rangle| = 2n$ perché $\rho^n = e = \sigma^2$, quindi, per ragioni di cardinalità, segue che $D_n = \langle \rho, \sigma \rangle$.

§1.7.1 Sottogruppi di D_n

Numero di elementi di ordine k. Sia ρ una rotazione in D_n; si considera $\langle \rho \rangle \cong C_n < D_n$[1].

Essendo C_n ciclico, vi sono $\phi(k)$ elementi di ordine k, se $k \mid n$. Oltre alle n rotazioni ρ^i, in D_n sono presenti anche le n riflessioni $\sigma\rho^i$; osservando che $\sigma\rho^i\sigma\rho^i = \rho^{-i}\rho^i = e$, si conclude che se n è pari, vi sono $n+1$ elementi di ordine 2 (cioè le n riflessioni e $\rho^{n/2}$), mentre se n è dispari, vi sono n elementi di ordine 2. Ricapitolando:

$$\#\{\text{elementi di ordine } k\} = \begin{cases} n+1 & , \text{ se } k = 2 \text{ e } n \text{ pari} \\ n & , \text{ se } k = 2 \text{ e } n \text{ dispari} \\ \phi(k) & , \text{ se } k \mid n \\ 0 & , \text{ altrimenti} \end{cases} \tag{1.7.1}$$

[1] Qui, con C_n si indica un generico gruppo ciclico di ordine n.

visto che le n riflessioni sono tutte di ordine 2 e l'esistenza di $\rho^{n/2}$ dipende dalla parità di n.

I sottogruppi. Nel punto precedente, si è notato che C_n è uno dei sottogruppi. Inoltre, i sottogruppi di C_n sono noti: ne esiste uno per ogni divisore dell'ordine del gruppo, cioè n in questo caso, per cui se $H < D_n$ e $H < C_n$, allora H è l'unico sottogruppo di ordine $|H|$. Se, invece $H < D_n$ e $H \not< C_n$, allora H contiene almeno una riflessione τ.

Proposizione 1.15. Per $H < D_n$ e $H \cap C_n \neq H$ (cioè H contiene almeno una riflessione), si ha $H = (H \cap C_n) \bigsqcup (\tau H \cap C_n)$ ed esiste una mappa biettiva tra $(H \cap C_n)$ e $(\tau H \cap C_n)$[a].

Dimostrazione. Si considera

$$\begin{tikzcd} H \arrow[r, "\gamma"] \arrow[rr, bend right, "\varphi"'] & \mathrm{GL}_2(\mathbb{R}) \arrow[r, "\det"] & \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z} \end{tikzcd}$$

dove γ è l'omomorfismo che a ρ e σ associa le relative matrici, mentre le matrici di $\mathrm{GL}_2(\mathbb{R})$ sono mappate a $\{\pm 1\}$ tramite il determinante: $\det M_\rho = 1$ e $\det M_\sigma = -1$. La mappa $\varphi = \gamma \circ \det$ è un omomorfismo suriettivo, infatti γ è un omomorfismo e per il teorema di Binet per cui $\det(M_\rho^i M_\sigma^j) = \det(M_\rho)^i \det(M_\sigma)^j = 1^i(-1)^j = 1 \iff j = 0$. La suriettività è assicurata dal fatto che almeno una riflessione stia in H.

Considerando, quindi, $\varphi : H \to \mathbb{Z}/2\mathbb{Z}$, il suo kernel è $H \cap C_n$; per il I teorema di omomorfismo, allora, $H/(H \cap C_n) \cong \mathbb{Z}/2\mathbb{Z}$, da cui $|H|/|H \cap C_n| = |\mathbb{Z}/2\mathbb{Z}| = 2$.

Poi, $\tau H \cap C_n$ e $H \cap C_n$ sono disgiunti perché se $h \in H \cap C_n$ non potrebbe stare anche in $\tau H \cap C_n$, altrimenti sarebbe una rotazione e una riflessione allo stesso tempo.

Rimane da mostrare solo che i due insiemi hanno stessa cardinalità, quindi l'esistenza di una mappa biettiva che li colleghi. Sia, allora

$$\psi : \begin{array}{ccc} H \cap C_n & \longrightarrow & \tau H \cap C_n \\ h & \longmapsto & \tau h \end{array}$$

questa è biettiva perché $\tau h_1 = \tau h_2 \iff h_1 = h_2$ e $\forall \tau h \in \tau H \cap C_n$, si ha $\psi(h) = \tau h$. □

[a] Per $\tau H \cap C_n$, si intende $\tau(H \cap C_n)$.

Si osserva che, per qualche m, $H \cap C_n = \langle \rho^m \rangle = \{e, \rho^m, \rho^{2m}, \dots, \rho^{n-m}\}$, con $m \mid n$; se $\tau = \sigma\rho^i$, allora $\tau H \cap C_n = \{\sigma\rho^i, \sigma\rho^{i+m}, \dots, \sigma\rho^{i+n-m}\}$ e si sa che l'unione dei due restituisce tutto H. Allora H è composto da m rotazioni e m simmetrie; in particolare $H = \langle \rho^m, \tau \rangle \cong D_m$, quindi, se $m \mid n$, si hanno dei sottogruppi della forma $\mathbb{Z}/m\mathbb{Z}$ e D_m.

Sottogruppi normali. Per lo studio dei sottogruppi normali, si considerano le due seguenti proposizioni.

Proposizione 1.16. Sia $H < G$ un sottogruppo tale che $[G : H] = 2$; allora $H \lhd G$.

Dimostrazione. Si considerano gli insiemi $\{H, gH\}$ e $\{H, Hg\}$ delle classi laterali, rispettivamente, sinistre e destre di H in G, con $g \notin H$. Ora, $\forall x \in H$, si ha direttamente $xH = H = Hx$; si mostra che lo stesso vale anche per elementi non in H. Se $y \in G \setminus H$, allora $yH \neq H \neq Hy$; visto che entrambe le classi laterali formano una partizione di G, allora deve valere $yH = G \setminus H = Hy$, pertanto $yH = Hy$, $\forall y \in G \setminus H$. Si conclude che $gH = Hg$, $\forall g \in G$, quindi $H \lhd G$. □

Proposizione 1.17. Siano $H \lhd G$ e $K < H$, con K caratteristico in H; allora $K \lhd G$.

Dimostrazione. Si considera, per $g \in G$, $\phi_g : G \to G$ con $\phi_g(x) = gxg^{-1}$; per definizione, si ha $\phi_g(H) = H$, quindi $\phi_g|_H$ è un automorfismo e, allora, $\phi_g|_H(K) = K$, $\forall g \in G \Rightarrow gKg^{-1} = K$, pertanto $K \lhd G$. □

L'indice di C_n in D_n è 2, quindi $C_n \lhd D_n$ per la prima proposizione. Per G ciclico di ordine n, esiste un unico H, con $|H| = m \mid n$; visto che ogni sottogruppo di un gruppo ciclico è caratteristico, allora, nel caso di D_n, ogni sottogruppo di $\langle \rho \rangle \cong C_n$ è caratteristico, quindi normale.

Se n è pari, allora $\langle \rho^2 \rangle < C_n$ ha $n/2$ elementi; considerando $H < D_n$ e $H \not\subset C_n$, con $H \cap C_n = \langle \rho^2 \rangle$, si ha

$$H = \langle \rho^2 \rangle \sqcup \tau \langle \rho^2 \rangle$$

quindi $[D_n : H] = 2$, per cui $H \lhd D_n$. Di sottogruppi di questa forma, se ne trovano due: $\langle \rho^2, \sigma \rangle$ e $\langle \rho^2, \sigma\rho \rangle$; tuttavia non si sa se siano tutti i sottogruppi normali, quindi si cerca di caratterizzarli meglio.

Si sa che $H \lhd G \iff gHg^{-1} = H$, $\forall g \in G$, quindi per ogni elemento di un sottogruppo normale, devono figurare anche tutti i suoi coniugati. Per la proposizione 1.14, per capire come sono fatti i coniugati di D_n, è sufficiente studiare quali siano quelli di ρ^i e $\sigma\rho^i$. Si nota che:

$$\rho^j \rho^i \rho^{-j} = \rho^i \qquad \sigma\rho^j \rho^i \rho^{-j} \sigma = \sigma \rho^i \sigma = \rho^{-i}$$

quindi l'insieme dei coniugati di ρ^i è $\{\rho^i, \rho^{-i}\}$; in particolare, se $i \in \{0, n/2\}$, tale insieme diventa $\{e\}$, oppure $\left\{\rho^{n/2}\right\}$ rispettivamente. Poi, si nota che:

$$\rho^i \sigma \rho^j \rho^{-i} = \sigma \rho^{-i} \rho^j \rho^{-i} = \sigma \rho^{j-2i} \qquad \sigma \rho^i \sigma \rho^j \rho^{-i} \sigma = \rho^{-i} \rho^j \rho^{-i} \sigma = \sigma \rho^{2i-j}$$

quindi se n è pari, allora $\sigma\rho^s \sim \sigma\rho^t \iff s \equiv t \pmod 2$, quindi le riflessioni di spezzano in due classi di coniugio; se n è dispari, invece, le riflessioni sono tutte coniugate[1].

Ricapitolando:

- se n è dispari e se un sottogruppo contiene una riflessione, allora, per essere normale, le deve contenere tutte e tutte le riflessioni generano D_n, infatti σ e $\sigma\rho$ sono dati, dai quali si ottiene $\rho = (\sigma)(\sigma\rho)$, quindi $H \lhd D_n \Rightarrow H = D_n$, mentre se non contiene alcuna riflessione, allora è un sottogruppo di C_n;

- se n è pari, oltre ai sottogruppi di C_n, si considerano gli $H \lhd D_n$ che sono tali che $\sigma\rho^i \in H$, per cui $\sigma\rho^{i+2} \in H$ e $\rho^2 \in H$, pertanto, se $H \neq D_n$, devono essere della forma $\langle \rho^2, \sigma \rangle$, o $\langle \rho^2, \sigma\rho \rangle$.

Sottogruppi caratteristici. Usando quanto visto per i sottogruppi normali, si conclude che i possibili sottogruppi caratteristici sono i sottogruppi di C_n e $\langle \rho^2, \sigma \rangle$ e $\langle \rho^2, \sigma\rho \rangle$. Mentre si sa già che i sottogruppi di C_n sono caratteristici, si osserva che, per gli altri due, la mappa $\tau : D_n \to D_n$ tale che $\tau(\rho) = \rho$ e $\tau(\sigma) = \sigma\rho$ è un automorfismo che scambia $\langle \rho^2, \sigma \rangle$ con $\langle \rho^2, \sigma\rho \rangle$ e viceversa, quindi non sono caratteristici.

§1.7.2 Centro, quozienti e automorfismi di D_n

Il centro. Si cercano tutti gli elementi $\tau \in D_n$ tale che $\forall \rho \in D_n,\ \rho\tau\rho^{-1} = \tau$. Dal precedente studio dei coniugi nei sottogruppi normali, si conclude che $Z(D_n) = \{e\}$ se n è dispari e $Z(D_n) = \left\{e, \rho^{n/2}\right\} \cong \mathbb{Z}/2\mathbb{Z}$ se n è pari.

Quozienti. Si sa che i quozienti sono in corrispondenza biunivoca con i sottogruppi normali, il che vuol dire che esiste un quoziente per ciascun $H \lhd G$. A meno di un automorfismo, i quozienti si ottengono come segue. Per quanto visto precedentemente, i sottogruppi normali sono i sottogruppi di C_n e, se n è pari, anche quelli della forma $\langle \rho^2, \sigma \rangle$ e $\langle \rho^2, \sigma\rho \rangle$. Sia, $\langle \rho^m \rangle < C_n$, con $m \mid n$, per cui $|D_n/\langle \rho^m \rangle| = 2n/(n/m) = 2m$.

[1] Questo è dato dal fatto che, visto che i compare con un 2 davanti all'esponente, se n è pari, allora, variando i, si ottengono solo permutazioni pari perché l'esponente fa salti di due andando di pari in pari; se n è dispari, l'esponente non può fare salti di due in due: arrivato ad un certo punto, aumentando di 2, si finisce in un numero dispari e si raggiungono tutte le riflessioni. Questo permette di concludere che, quando n è pari, le riflessioni si dividono in due classi diverse, mentre quando n è dispari, sono tutte coniugate fra loro.

Proposizione 1.18. Si ha $D_n/\langle \rho^m \rangle \cong D_m$.

Dimostrazione. Si considera

$$\begin{array}{rccc} & D_n & \longrightarrow & D_{n/m} \\ \gamma: & \sigma & \longmapsto & \tau \\ & \rho & \longmapsto & \epsilon \end{array}$$

dove $D_n = \langle \sigma, \rho \mid \rho^n = \sigma^2 = e, \sigma\rho\sigma = \rho^{-1} \rangle$ e $D_m = \langle \tau, \epsilon \mid \epsilon^m = \tau^2 = e,\ \tau\epsilon\tau = \epsilon^{-1} \rangle$. Per verificare che si tratta di un omomorfismo ben definito, è sufficiente far vedere che rispetta le relazioni di D_n (th. 1.6):

$$\begin{aligned} &\gamma(\rho)^n = \epsilon^n = (\epsilon^m)^k = e && \text{(visto che } m \mid n) \\ &\gamma(\sigma)^2 = \tau^2 = e \\ &\gamma(\sigma)\gamma(\rho)\gamma(\sigma) = \tau\epsilon\tau = \epsilon^{-1} = \gamma(\rho)^{-1} \end{aligned}$$

quindi è effettivamente un omomorfismo. Si nota che questo è suriettivo e il suo nucleo è $\langle \rho^m \rangle$, quindi si ha la tesi per il I teorema di omomorfismo. □

Nel caso di n pari, poi, vi sono gli altri due sottogruppi citati sopra, che hanno indice 2 e, quindi, i cui quozienti sono isomorfi a $\mathbb{Z}/2\mathbb{Z}$.

Gli automorfismi. Si studia $\mathrm{Aut}(D_n)$. Per farlo, si cerca di calcolarne la cardinalità. Per definire un automorfismo in D_n, lo si definisce sui generatori, che si sanno essere ρ e σ. L'immagine di questi generatori deve essere un altro generatore: ad esempio, l'immagine di ρ, che ha ordine n, deve avere come immagine un elemento di ordine n; questi sono della forma ρ^i, con $\gcd(i, n) = 1$, quindi ci sono $\phi(n)$ possibili scelte. Poi, σ ha ordine 2 e deve avere, come immagine, un altro elemento di ordine 2 che, insieme al ρ^i scelto prima, generi D_n; ci sono n riflessioni della forma $\sigma\rho^j$, quindi un totale di n scelte possibili. Si nota che se n è pari, anche $\rho^{n/2}$ ha ordine 2, ma la coppia $\rho^i, \rho^{n/2}$ non genera D_n. Sia, allora

$$\begin{array}{rccc} & D_n & \longrightarrow & D_n \\ \gamma: & \rho & \longmapsto & \rho^i \\ & \sigma & \longmapsto & \sigma\rho^j \end{array}$$

con $\gcd(i, n) = 1$ e j qualsiasi; γ è ben definita (si può verificare che è un omomorfismo vedendo che soddisfa le relazioni del gruppo) e si nota che:

$$\gamma\left((\rho^s)(\sigma\rho^t)\right) = \gamma(\sigma\rho^{t-s}) = \sigma\rho^j\rho^{i(t-s)} = \sigma\rho^{-is}\rho^j\rho^{it} = \rho^{is}\sigma\rho^j\rho^{it} = \gamma(\rho^s)\gamma(\sigma\rho^t)$$

Inoltre, è biettiva per costruzione, quindi si ha $|\mathrm{Aut}(D_n)| = n\phi(n)$; da un punto di vista insiemistico, esiste una biezione tra $\mathrm{Aut}(D_n)$ e $\mathbb{Z}/n\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^*$.

Esercizio 1.1. Studiare D_4 (risultati a pagina 19) e D_6.

§1.8 Permutazioni

Definizione 1.15 (Permutazione). Sia X un insieme; una mappa $f : X \to X$ è detta *permutazione* se è biettiva. Le permutazioni formano un gruppo rispetto alla composizione tra funzioni ed è indicato con

$$S(X) = \{f : X \to X \mid f \text{ è biettiva}\}$$

Se $X = \{1, \dots, n\}$, allora il gruppo delle permutazioni si indica con S_n e $|S_n| = n!$.

Una permutazione di S_n può essere rappresentata tramite cicli, i quali sono disgiunti e, quindi, commutano fra loro.

Ogni k-ciclo (ciclo di lunghezza k) ha k scritture diverse, tutte equivalenti fra loro, dovute alla possibilità di scegliere uno fra i k elementi del ciclo come primo elemento; dopo questa scelta, tutti gli altri sono univocamente determinati.

Proposizione 1.19. I cicli di una permutazione di S_n sono orbite degli elementi di $X = \{1, \dots, n\}$ formate dall'azione indotta da tale permutazione.

Dimostrazione. Sia $\sigma \in S_n$ e sia $\langle\sigma\rangle$ il sottogruppo ciclico generato da σ. Si considera l'azione di $\langle\sigma\rangle$ su X secondo la legge $\sigma^k \cdot x = \sigma^k(x)$; l'orbita di ciascun elemento di X è della forma

$$\mathrm{Orb}(x) = \left\{\sigma^k(x) \mid k \in \mathbb{Z}\right\}$$

Si nota che $|X| < \infty \Rightarrow |\mathrm{Orb}(x)| < \infty,\ \forall x$. Sia, poi, $m \geq 1$ il più piccolo intero tale che $\sigma^m(x) = x$[a]; allora gli elementi

$$x,\ \sigma(x),\ \sigma^2(x), \dots,\ \sigma^{m-1}(x)$$

sono tutti distinti (per definizione di m) e formano $\mathrm{Orb}(x)$. Facendo agire σ su $\mathrm{Orb}(x) \subset X$, si nota che

$$x \mapsto \sigma(x),\ \sigma(x) \mapsto \sigma^2(x), \dots,\ \sigma^{m-1}(x) \mapsto \sigma^m(x) = x$$

L'azione di σ ristretta a $\mathrm{Orb}(x)$, allora, si può vedere come la permutazione

$$\begin{pmatrix} x & \sigma(x) & \sigma^2(x) & \cdots & \sigma^{m-1}(x) \end{pmatrix}$$

che è un m-ciclo. Se $O_1, \ldots, O_r$ sono le orbite non banali (cioè di lunghezza > 1), σ agisce su ciascuna O_i come un m_i-ciclo, chiamato c_i per ogni orbita, con $|O_i| = m_i$, mentre su quelle banali agisce come l'identità. Visto che le orbite partizionano X, ciascun ciclo c_i è disgiunto dagli altri e la loro composizione restituisce proprio σ, visto che per definizione sono la restrizione di σ a partizioni di X. □

[a]Questo esiste per forza, altrimenti si avrebbero orbite di infiniti elementi a partire da un insieme finito.

Corollario 1.6.1. Il gruppo S_n è generato dai cicli.

Dimostrazione. Il teorema precedente mostra come ciascuna permutazione $\sigma \in S_n$ si possa scrivere come composizione di un numero finito di cicli disgiunti, pertanto combinando l'insieme di tutti i possibili cicli, si ottiene S_n. □

Numero di k-cicli di $\mathbf{S_n}$. Si cerca quanti k-cicli, con $k \leq n$, sono contenuti in S_n. Visto che un ciclo è una sequenza di k numeri, il problema si riduce a trovare quanti k numeri possono essere estratti da un insieme di n numeri, che si sa essere dato da $\binom{n}{k}$. Queste, però, non sono tutte perché i k numeri si possono scambiare in $k!$ modi diversi; allo stesso tempo, è possibile costruire k k-cicli equivalenti, quindi il numero totale ammonta a $\binom{n}{k}\frac{k!}{k} = \binom{n}{k}(k-1)!$.

Numero di permutazioni di $\mathbf{S_{12}}$ sono composizione di 2 3-cicli e 3 2-cicli disgiunti. Dal punto precedente, si sa che in S_{12} si trovano $\binom{12}{3}\frac{3!}{3}$; fissato il primo 3-ciclo, restano $12-3$ elementi liberi per gli altri cicli[1], quindi, per il secondo 3-ciclo, si hanno $\binom{9}{3}\frac{3!}{3}$ scelte possibili. Continuando così per tutti i cicli rimanenti, si ottengono

$$\binom{12}{3}\frac{3!}{3}\binom{9}{3}\frac{3!}{3}\binom{6}{3}\frac{2!}{2}\binom{4}{3}\frac{2!}{2}\binom{2}{3}\frac{2!}{2}$$

possibili permutazioni, dove si è modificata la formula per scegliere due 3-cicli e tre 2-cicli. Però se ne sono contati troppi: prendendo d'esempio i due 3-cicli, essendo disgiunti, questi possono commutare senza alterare la permutazione, però col conto precedente si sono considerati distinti. Per risolvere, si deve dividere per tutti i possibili modi di commutare i 3-cicli, cioè 2! in questo caso. Lo stesso si deve fare per i tre 2-cicli, i cui

[1]I tre scelti vanno rimossi affinché gli altri cicli siano disgiunti.

modi di permutarle sono 3!. Complessivamente, si hanno un totale di

$$\binom{12}{3}\frac{3!}{3}\binom{9}{3}\frac{3!}{3}\binom{6}{3}\frac{2!}{2}\binom{4}{3}\frac{2!}{2}\binom{2}{3}\frac{2!}{2}\frac{1}{3!2!}$$

possibili permutazioni.

Ordine di una permutazione di $\mathbf{S_n}$. Un k-ciclo ha ordine k; infatti per $\sigma = (a_1 \ \cdots \ a_k)$, si ha

$$\sigma^s(a_i) = a_j \quad \text{con } j \equiv s + i \pmod k \text{ e } j < k$$

quindi $\sigma^s(a_i) = a_{i+s} = a_i \iff s + i \equiv i \pmod k \iff s \equiv 0 \pmod k$.

Se la permutazione è formata da ℓ cicli disgiunti σ_i, invece, il suo ordine è

$$\mathrm{ord}(\sigma) = \mathrm{mcm}(\mathrm{ord}(\sigma_1), \ldots, \mathrm{ord}(\sigma_\ell))$$

perché è il più piccolo numero tale che ogni ciclo torni al punto di partenza. Si nota, infatti, che se m è tale che $\sigma^m = e$, allora

$$e = \sigma^m = \sigma_1^m \cdots \sigma_\ell^m \implies \sigma_i^m = e, \ \forall i = 1, \ldots, \ell$$

quindi $\mathrm{ord}(\sigma_i) \mid m$, $\forall i$ e, quindi, $m = \mathrm{mcm}(\mathrm{ord}(\sigma_1), \ldots, \mathrm{ord}(\sigma_\ell))$.

Definizione 1.16 (Trasposizione). Sia $\tau \in S_n$; se τ è della forma (a_i, a_j), cioè è un 2-ciclo, allora si dice *trasposizione*.

Proposizione 1.20. Tutte le permutazioni di S_n si scrivono come composizione di trasposizioni.

Dimostrazione. Per il corollario 1.6.1, è sufficiente mostrare che vale per un k-ciclo generico. A questo proposito, si osserva che:

$$(1, \ldots, k) = (1, k)(1, k-1) \cdots (1, 2)$$

□

Osservazione 1.9. La decomposizione in trasposizioni non è unica: per esempio:

$$(12) = (12)(34)(34) = (12)(34)(35)(67)(34)(35)(67)$$

Proposizione 1.21. L'applicazione

$$\operatorname{sgn}: \begin{array}{ccc} S_n & \longrightarrow & \{\pm 1\} = \mathbb{Z}^* \\ \sigma & \longmapsto & \operatorname{sgn}\sigma = \displaystyle\prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{array}$$

è un omomorfismo di gruppi. Inoltre, se σ è una trasposizione, si ha $\operatorname{sgn}\sigma = -1$.

Dimostrazione. È un omomorfismo perché:

$$\begin{aligned} \operatorname{sgn}(\sigma\tau) &= \prod_{1 \le i < j \le n} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} \\ &= \prod_{1 \le i < j \le n} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \prod_{1 \le i < j \le n} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) \end{aligned}$$

dove si è moltiplicato sopra e sotto per $\tau(i) - \tau(j)$ e si sono separate le produttorie[a].

Sia $\sigma = (a, b)$ una trasposizione; allora

$$\operatorname{sgn}\sigma = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Se uno solo tra i e j è uguale a a oppure b, allora

$$\frac{\sigma(i) - \sigma(j)}{i - j} = \frac{i - j}{i - j} = 1$$

mentre se $\{i, j\} \cap \{a, b\} = \{i, a\}$, si trova

$$\begin{cases} \dfrac{\sigma(i) - \sigma(a)}{i - a} = \dfrac{i - b}{i - a} & , \quad \text{se } i < a \\[2ex] \dfrac{\sigma(a) - \sigma(i)}{a - i} = \dfrac{b - i}{a - i} = \dfrac{i - b}{i - a} & , \quad \text{se } a < i \end{cases}$$

Lo stesso vale per l'intersezione $\{i, j\} \cap \{a, b\} = \{i, b\}$:

$$\frac{\sigma(i) - \sigma(b)}{i - b} = \frac{\sigma(b) - \sigma(i)}{b - i} = \frac{i - a}{i - b}$$

I fattori del caso precedente si semplificano a 1, quindi rimane unicamente il caso in cui $\{i, j\} \cap \{a, b\} = \{a, b\}$; assumendo senza perdita di generalità che $a < b$, si trova:

$$\frac{\sigma(a) - \sigma(b)}{a - b} = \frac{b - a}{a - b} = -1$$

pertanto, nella produttoria, si ha un unico fattore pari a -1, il che implica che $\operatorname{sgn} \sigma = -1$. □

[a] La prima produttoria restituisce il $\operatorname{sgn} \sigma$ perché al massimo applicare prima τ altera l'ordine dell'insieme, quindi non è garantito che $\tau(i) < \tau(j)$ se $i < j$; questo, però, non importa perché se $\tau(i) > \tau(j)$, allora l'espressione si può riscrivere come $\frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)}$. Prendendo $a = \tau(i)$ e $b = \tau(j)$, si potrebbe anche riscrivere la produttoria come $\prod_{1 \leq a < b \leq n} \frac{\sigma(a) - \sigma(b)}{a - b}$.

Corollario 1.6.2. La mappa $\operatorname{sgn} \sigma$ restituisce la parità di trasposizioni presenti in σ, quando decomposta in prodotto di trasposizioni.

Nucleo del segno. Si nota che

$$\operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n \mid \operatorname{sgn} \sigma = 1\} = A_n \tag{1.8.1}$$

ed è noto come *gruppo alterno*. Si nota, intanto, che $S_n / A_n \cong \{\pm\} \cong \mathbb{Z}^*$ per il I teorema di omomorfismo; poi si nota che, essendo, $S_n / A_n \cong \{\pm 1\}$, si ha:

$$2 = |S_n / A_n| = \frac{S_n}{A_n} \implies |A_n| = \frac{|S_n|}{|S_n / A_n|} = \frac{n!}{2}$$

Infine, visto che A_n ha indice 2 in S_n, se ne conclude che $A_n \lhd S_n$.

Teorema 1.7. Due permutazioni di S_n sono coniugate se e solo se hanno lo stesso tipo di decomposizione in cicli disgiunti.

Dimostrazione. Si divide la dimostrazione nelle due implicazioni.

- ($\Rightarrow$) Siano $\sigma, \tau \in S_n$; si considerano $\sigma = (a_1, \ldots, a_k)$ e $\tau\sigma\tau^{-1}$. Si nota che, se $\tau(a_i) = b_i \Rightarrow \tau\sigma\tau^{-1}(b_i) = \tau\sigma(a_i) = \tau(a_{i+1}) = b_{i+1}$; inoltre, se $x \neq b_i$ per ogni i:

$$\tau^{-1}(x) \neq a_i \implies \tau\sigma\tau^{-1}(x) = \tau\sigma\left(\tau^{-1}(x)\right) = \tau\tau^{-1}(x) = x$$

  pertanto il coniugato di un k-ciclo è ancora un k-ciclo. Se la permutazione è composizione di cicli disgiunti, invece, si può scrivere

$$\sigma = \sigma_1 \ldots \sigma_k \implies \tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1} \ldots \tau\sigma_k\tau^{-1}$$

  quindi ci si può ricondurre al caso precedente.

- ($\Leftarrow$) Siano $\sigma = (a_1, \dots, a_k)$ e $\rho = (b_1, \dots, b_k)$ due k-cicli; si può prendere, allora, τ tale che $\tau(a_i) = b_i$, da cui $\tau\sigma\tau^{-1} = \rho$. Nel caso di più cicli disgiunti, si mappa ciclo con ciclo:
$$\begin{array}{rccc} \sigma = & (x_{11} \dots x_{1k_1}) & \cdots & (x_{r1} \dots x_{rk_r}) \\ & \downarrow & & \downarrow \\ \rho = & (y_{11} \dots y_{1k_1}) & \cdots & (y_{r1} \dots y_{rk_r}) \end{array}$$
con $\tau(x_{ij}) = y_{ij}$, quindi vale $\tau\sigma\tau^{-1} = \rho$.

□

Centralizzatore di una permutazione. Quanto al centralizzatore di $\sigma \in S_n$, si sa, dal teorema orbita-stabilizzatore, che:

$$|Z(\sigma)||\mathrm{Cl}(\sigma)| = n! \tag{1.8.2}$$

Per il teorema precedente, si sa calcolare $|\mathrm{Cl}(\sigma)|$, quindi è possibile ottenere $|Z(\sigma)|$.

Esempio 1.5. Sia $\sigma = (1234)(56) \in S_{10}$; il numero possibile di permutazioni coniugate sono tutte quelle che si scrivono come un 4-ciclo e un 2-ciclo in S_{10}, numero ottenuto come

$$|\mathrm{Cl}(\sigma)| = \binom{10}{4}\frac{4!}{4}\binom{6}{2} = \frac{10!}{192} \implies |Z(\sigma)| = 192 = 4!8$$

Sia
$$H = \mathrm{Sym}\,(7,8,9,10) = \{h \in S_{10} \mid h(i) = i,\ \forall i \notin \{7,8,9,10\}\} \cong S_4$$
e sia $K = \langle (1234), (56) \rangle$; allora $H, K \lhd Z(\sigma)$, $H \cap K = \{e\}$ e $HK = Z(\sigma)$, per cui

$$Z(\sigma) \cong H \times K \cong S_4 \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

Dimostrazione. Si ha $H < Z(\sigma)$ perché ogni permutazione di H modifica solo l'insieme $\{7,8,9,10\}$, quindi commuta con σ. Inoltre, $H \cong S_4 \Rightarrow |H| = 4!$. Si ha $K < Z(\sigma)$ perché ogni elemento di K è della forma $(1234)^j(56)^k$, quindi commuta sempre con σ. Visto che (1234) ha ordine 4 e (56) ha ordine 2 e i due cicli sono disgiunti, si ha $|K| = 4 \cdot 2 = 8$. Si nota, in particolare, che $\langle (1234) \rangle \cong C_4 \cong \mathbb{Z}/4\mathbb{Z}$, cioè è isomorfo a un gruppo ciclico di ordine 4; analogamente $\langle (56) \rangle \cong C_2 \cong \mathbb{Z}/2\mathbb{Z}$. Infine, questi due sono sottogruppi normali perché le permutazioni di $Z(\sigma)$ sono quelle che hanno cicli disgiunti con quelli di σ, quindi sono quelle di H, oppure sono quelle che commutano con i cicli di σ, cioè proprio quelle di H. Questo significa che ciascuna permutazione di $Z(\sigma)$ commuta sia con gli elementi di H, che con quelli di K, rendendoli entrambi sottogruppi normali di $Z(\sigma)$.

Evidentemente la loro intersezione è banale perché le permutazioni di H agiscono esclusivamente su $\{7, 8, 9, 10\}$, mentre quelle di K su $\{1, 2, 3, 4, 5, 6\}$, quindi deve essere $H \cap K = \{e\}$.

Visto che $H, K < Z(\sigma)$ e $|HK| = |H||K| = 192$ (essendo $|H \cap K| = 1$), si ha $HK = Z(\sigma)$. Sempre perché $H \cap K$ è banale, si ha $HK \cong H \times K$, da cui

$$Z(\sigma) \cong H \times K \cong S_4 \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

□

§1.9 Gruppi di Sylow e prodotti diretti

Definizione 1.17 (Gruppo di Sylow). Sia G un gruppo finito con $|G| = p^m n$, con p primo e $\gcd(p, n) = 1$; se $H < G$ e $|H| = p^m$, allora H è detto p-Sylow di G.

Esempio 1.6. Si considera il gruppo diedrale D_7; si ha $|D_7| = 14 = 7 \cdot 2$, con $|\langle\rho\rangle| = 7$; allora $\langle\rho\rangle$ è un 7-Sylow di D_7 ed è unico. Tuttavia, i p-Sylow non sono unici; per esempio, i $\langle\rho^i\sigma\rangle \subset D_7$ sono sette 2-Sylow.

Lemma 1.7.1. Siano $H, K \lhd G$, con $H \cap K = \{e\}$; allora $hk = kh$, $\forall h \in H$, $\forall k \in K$.

Dimostrazione. Si ha $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$; visto che K è normale, allora $hkh^{-1} \in K$, quindi $hkh^{-1}k^{-1} \in K$. Allo stesso tempo, $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1})$ e, siccome anche H è normale, si ha $kh^{-1}k^{-1} \Rightarrow hkh^{-1}k^{-1} \in H$. Allora, visto che $hkh^{-1}k^{-1} \in H \cap K$ e visto che $H \cap K = \{e\}$ per assunzione, si ha $hkh^{-1}k^{-1} = e \Rightarrow hk = kh$. □

Teorema 1.8 (Teorema di decomposizione diretta). Sia G un gruppo e siano $H, K \lhd G$; se $HK = G$ e $H \cap K = \{e\}$, allora $G \cong H \times K$.

Dimostrazione. Sia $\phi : H \times K \to G$ tale che $\phi((h, k)) = hk$; allora ϕ è un omomorfismo per il lemma precedente (1.7.1), è iniettiva per la seconda ipotesi ed è suriettiva per la prima. □

Corollario 1.8.1. In un prodotto diretto, i fattori commutano fra loro.

Osservazione 1.10. Sia $G = H \times K$; per il teorema precedente (1.8), $Z(H \times K) \cong Z(H) \times Z(K)$, visto che $Z(H) \times \{e_K\}$ e $\{e_h\} \times Z_K$ sono sottogruppi normali di $Z(H \times K)$. Conseguentemente, ricordando la proposizione 1.1, si trova:

$$\mathrm{Int}(H \times K) \cong (H \times K)/Z(H \times K) \cong H/Z(H) \times K/Z(K) \cong \mathrm{Int}(H) \times \mathrm{Int}(K)$$

dove il penultimo isomorfismo è ottenuto definendo

$$\gamma : \begin{array}{ccc} H \times K & \longrightarrow & H/Z(H) \times K/Z(K) \\ (h,k) & \longmapsto & (h+Z(H), k+Z(K)) \end{array}$$

e dal I teorema di omomorfismo.

Teorema 1.9. Sia

$$\phi : \begin{array}{ccc} \mathrm{Aut}(H) \times \mathrm{Aut}(K) & \longrightarrow & \mathrm{Aut}(H \times K) \\ (f,g) & \longmapsto & \gamma = (f,g) \end{array}$$

Allora ϕ è un omomorfismo iniettivo, mentre è suriettivo se e solo se $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici in $H \times K$.

Dimostrazione. Intanto, γ è ben definita perché $\forall (f,g) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, si ha $f(h) \in H,\ \forall h \in H$ e $g(k) \in K,\ \forall k \in K$, quindi $\gamma((h,k)) = (f(h), g(k)) \in H \times K$.

Poi, ϕ è ben definita perché γ è un automorfismo; infatti è un omomorfismo:

$$\gamma((h,k)(h',k')) = \big(f(hh'), g(kk')\big) = \big(f(h)f(h'), g(k)g(k')\big) = \gamma((h,k))\gamma(h',k')$$

È anche iniettiva perché

$$\begin{aligned} \mathrm{Ker}\,\gamma &= \{(h,k) \in H \times K \mid \gamma((h,k)) = (e_H, e_K)\} = \{(h,k) \in \mathrm{Ker}\, f \times \mathrm{Ker}\, g\} \\ &= \{(e_H, e_K)\} \end{aligned}$$

ed è suriettiva perché $\forall (h,k) \in H \times K,\ \exists! (h_0,k_0) \in H \times K : ((f(h_0), g(k_0)) = (h,k)$, dove si è usato, in tutte le dimostrazioni, che sia f che g sono automorfismi. Segue che γ è effettivamente un automorfismo di $H \times K$.

Ora si verifica che ϕ è un omomorfismo ed è sempre iniettivo; la prima vale perché

$$\phi((f,g)(\varphi,\psi)) = \phi(f \circ \varphi, g \circ \psi) = (f \circ \varphi, g \circ \psi) = (f,g) \circ (\varphi,\psi) = \phi((f,g)) \circ \phi((\varphi,\psi))$$

mentre è iniettivo perché $\phi((f,g)) = \mathrm{Id}_{H \times K} \iff f = \mathrm{Id}_H$ e $g = \mathrm{Id}_K$.

Ora si dimostra che ϕ è suriettivo se e solo se $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici in $H \times K$.

- ($\Leftarrow$) Si assume che $H \times \{e_K\}$ e $\{e_H\} \times K$ siano caratteristici in $H \times K$ e si mostra che ϕ è suriettivo. Per farlo, si considerano, $\forall \gamma \in \mathrm{Aut}(H \times K)$, le mappe

$f : H \to H$ e $g : K \to K$ tali che

$$f(h) = \pi_H \gamma(h, e_K) \qquad g(k) = \pi_K \gamma(e_H, k)$$

e si dimostra che $f \in \mathrm{Aut}(H),\ g \in \mathrm{Aut}(K)$ e $\gamma = \phi(f, g)$. Si nota che, sia f che g sono composizioni di due omomorfismi, quindi sono, a loro volta, omomorfismi; inoltre

$$\begin{aligned}\mathrm{Ker}\, f &= \{h \in H \mid \pi_H \gamma(h, e_K) = e_H\} = \{h \in H \mid \pi_H(h', e_K) = e_H\} \\ &= \{h \in H \mid e_H = h' = \gamma(h)\} = \{e_H\}\end{aligned}$$

Lo stesso vale per g, quindi entrambe le mappe sono omomorfismi iniettivi. Usando il fato che γ è suriettiva, si ha che $\forall h' \in H,\ \exists h \in H : \gamma(h, e_K) = (h', e_K)$, quindi $f(h) = \pi_H \gamma(h, e_K) = \pi_H(h', e_K) = h'$ e lo stesso si può ripetere per g quindi f e g sono automorfismi. Per concludere, si nota che

$$\phi(f, g)((h, k)) = \big(\pi_H \gamma((h, e_K)), \pi_K \gamma((e_H, k))\big) = (h', k') = \gamma(h, k)$$

- ($\Rightarrow$) Sia ϕ anche suriettivo, quindi è un isomorfismo; si mostra che $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici in $H \times K$.

  Se ϕ è suriettivo, significa che ogni automorfismo di $\mathrm{Aut}(H \times K)$ è della forma $(f, g) : f \in \mathrm{Aut}(H),\ g \in \mathrm{Aut}(K)$, ma allora, per $\psi \in \mathrm{Aut}(H \times K)$, si ha:

$$\psi(H \times \{e_K\}) = f(H) \times \{e_K\} = H \times \{e_K\}$$

  perché f è un automorfismo di H e $\{e_K\} \xmapsto{g} \{e_K\}$ perché g è un automorfismo di K.

$\square$

Proposizione 1.22. Sia $G = H \times K$, con $|H| = n$ e $|K| = m$; se $\gcd(n, m) = 1$, allora H e K sono caratteristici in G.

Dimostrazione. Sia $f \in \mathrm{Aut}(H \times K)$, con $f(h, e_K) = (h', k')$; visto che $\mathrm{ord}((h, e_K)) = \mathrm{ord}(h) \mid n$, deve essere $\mathrm{ord}((h', k')) = \mathrm{mcm}(\mathrm{ord}(h'), \mathrm{ord}(k')) \mid n$, visto che f è automorfismo e, in particolare $\mathrm{ord}(k') \mid n$. Per ipotesi, deve essere $\mathrm{ord}(k') \mid m$, ma, visto che $\gcd(n, m) = 1$, deve essere $k' = e_K$, da cui $f(H \times \{e_K\}) \subset H \times \{e_K\}$. Lo stesso procedimento si può applicare a $f(e_H, k)$. $\square$

§1.10 Prodotto semidiretto

Definizione 1.18 (Prodotto semidiretto). Siano H, K dei gruppi e $\gamma : K \to \mathrm{Aut}(H)$ un omomorfismo tale che $\gamma(k) = \gamma_k \in \mathrm{Aut}(H)$, dove $\gamma_k : H \to H$ mappa $h \mapsto h' \in H$; si chiama *prodotto semidiretto* di H e K via γ il prodotto cartesiano $H \times K$ con l'operazione definita da

$$(h, k) * (h', k') = (h\gamma_k(h'), kk')$$

e si indica con $(H \times K, *) = H \rtimes_\gamma K$.

Proposizione 1.23. Dati due gruppi H, K; il loro prodotto semidiretto $H \rtimes_\gamma K$ è un gruppo.

Dimostrazione. La chiusura dell'operazione deriva direttamente dal fatto che sono due gruppi. Tale operazione è associativa:

$$\begin{aligned}(a, b)\,[(c, d)(e, f)] &= (a, b)(c\gamma_d(e), df) = \big(a\gamma_b(c\gamma_d(e)), bdf\big) = \big(a\gamma_b(c)\gamma_b(\gamma_d(e)), bdf\big)\\ &= \big(a\gamma_b(c)\gamma_{bd}(e), bdf\big) = (a\gamma_b(c), bd)(e, f) = [(a, b)(c, d)]\,(e, f)\end{aligned}$$

L'elemento neutro è (e_H, e_K):

$$(a, b)(e_H, e_K) = (a\gamma_b(e_H), be_K) = (a, b)$$

perché γ_b è un automorfismo. Infine, l'elemento inverso è dato da[a]:

$$(a, b)\big(\gamma_{b^{-1}}(a^{-1}), b^{-1}\big) = \big(a\gamma_b \circ \gamma_{b^{-1}}(a^{-1}), e_K\big) = (aa^{-1}, e_K) = (e_H, e_K)$$

□

[a] Questo si può ottenere imponendo che $(a, b)(x, y) = (e_H, e_K)$, risolvendo per x e y.

Osservazione 1.11. Il prodotto semidiretto è un caso particolare di prodotto diretto: scegliendo $\gamma(K) = \mathrm{Id}_H \in \mathrm{Aut}(H)$, si ha, infatti, $(h, k)(h', k') = (h\,\mathrm{Id}_H(h'), kk') = (hh', kk'),\ \forall k \in K$.

Esempio 1.7. Si studia $\mathbb{Z}/7\mathbb{Z} \rtimes_\gamma \mathbb{Z}/7\mathbb{Z}$, con $\gamma : \mathbb{Z}/7\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^* \cong \mathbb{Z}/6\mathbb{Z}$. Per questione di ordine, si ha $\gamma([1]_7) = [0]_6$, visto che $\gamma([1]_7)$, in quanto elemento di $\mathbb{Z}/6\mathbb{Z}$, deve avere $\mathrm{ord}(\gamma([1]_7)) \mid 6$ e, come immagine di $[1]_7$, che ha $\mathrm{ord}([1]_7) = 7$, deve essere tale che $\mathrm{ord}(\gamma([1]_7)) \mid 7$; l'unico elemento che divide sia 6, che 7 è 1, per cui γ deve mappare $[1]_7$ in $[0]_6$. Visto che $[1]_7$ genera $\mathbb{Z}/7\mathbb{Z}$, significa che $\gamma(\mathbb{Z}/7\mathbb{Z}) = \{[0]_6\}$, cioè è l'omomorfismo banale. In sostanza, $\mathbb{Z}/7\mathbb{Z} \rtimes_\gamma \mathbb{Z}/7\mathbb{Z} = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

Proposizione 1.24. Siano H, K due gruppi; si considera il loro prodotto semidiretto $H \rtimes_\gamma K$. Dati $\overline{H} = H \times \{e_K\}$ e $\overline{K} = \{e_H\} \times K$, per i quali si sa che $\overline{K}, \overline{H} \lhd H \times K$, vale $\overline{H} \lhd H \rtimes_\gamma K$ sempre e $\overline{K} \lhd H \rtimes_\gamma K \iff$ il prodotto è diretto.

Dimostrazione. Si ha sempre $\overline{H} \lhd H \rtimes_\gamma K$ perché $\pi_K : H \rtimes_\gamma K \to K$ tale che $\pi_K((h,k)) = k$ è un omomorfismo e $\overline{H} = \operatorname{Ker} \pi_K$.

Per $\overline{K}$, si assume prima che sia normale e si mostra che γ deve essere per forza banale. A questo scopo, si osserva che $\forall (e_H, k) \in \overline{K}$ ed un elemento generico $(h, e_K) \in \overline{H} \lhd H \rtimes_\gamma K$:

$$(h, e_K)(e_H, k)(h, e_K)^{-1} = (h\gamma_{e_K}(e_H), e_K k)(h, e_K)^{-1} = (h\gamma_k(h^{-1}), k)$$

Il fatto che $\overline{K}$ sia normale, implica che $\forall k,\ (h\gamma_k(h^{-1}), k) = (e_H, k)$, cioè $\forall k,\ \gamma_k(h^{-1}) = h^{-1}$, pertanto γ deve essere l'omomorfismo banale e, quindi, il prodotto è diretto.

Per l'implicazione inversa, cioè assumendo che il prodotto sia diretto, è possibile seguire la stessa dimostrazione fatta per $\overline{H}$. □

Osservazione 1.12. Sia G un gruppo e $H, K < G$, con $H \lhd G$; allora $HK < G$.

Teorema 1.10 (Teorema di decomposizione semidiretta). Sia G un gruppo e siano $H \lhd G$ e $K < G$ due sottogruppi; se $HK = G$ e $H \cap K = \{e_G\}$, allora $G \cong H \rtimes_\gamma K$, con $\gamma : K \to \operatorname{Aut}(H)$ e $\gamma(k) = khk^{-1}$.

Dimostrazione. Prima si dimostra la buona definizione del prodotto semidiretto definito nella tesi.

- $\gamma(k) = \gamma_k$ è un automorfismo di H.

  La mappa $\gamma(k) : H \to H$ è ben definita, visto che $H \lhd G$; infatti, $\forall k \in K,\ \forall h \in H$, si ha $khk^{-1} \in H$. Poi, γ_k è un omomorfismo perché

  $$\gamma_k(h_1h_2) = k(h_1h_2)k^{-1} = (kh_1k^{-1})(kh_2k^{-1}) = \gamma_k(h_1)\gamma_k(h_2)$$

  Infine, è biettiva perché ha inversa $\gamma(k)^{-1} = \gamma(k^{-1}) = \gamma_{k^{-1}}$; infatti $\gamma_{k^{-1}} \circ \gamma_k = \gamma_{e_K} = \operatorname{Id}_H$.

- $\gamma : K \to \operatorname{Aut}(H)$ è un omomorfismo.

  Dati $k_1, k_2 \in K$ e $h \in H$:

  $$\gamma(k_1k_2)(h) = (k_1k_2)h(k_1k_2)^{-1} = k_1(k_2hk_2^{-1})k_1^{-1} = (\gamma_{k_1} \circ \gamma_{k_2})(h)$$

Ora si introduce il prodotto semidiretto dei gruppi $H \rtimes_\gamma K$ con la legge $(h,k)(h',k') = (hkh'k^{-1}, kk')$. Si dimostra che $G \cong H \rtimes_\gamma K$. Per farlo, si introduce $F : H \rtimes_\gamma K \to G$ tale che $F(h,k) = hk \in G$ e si mostra che è un isomorfismo di gruppi.

- F è un omomorfismo.

  Siano $(h,k),(h',k') \in H \times K$; si osserva che:

$$\begin{aligned} F\big((h,k)(h',k')\big) &= F\big((hkh'k^{-1}, kk')\big) = hkh'k^{-1}kk' = (hk)(h'k') \\ &= F(h,k)F(h',k') \end{aligned}$$

- F è biettivo.

  Per la suriettività, si nota che, essendo $HK = G$ per ipotesi, allora ogni $g \in G$ si scrive come $g = hk$, con $h \in H$ e $k \in K$. Ne consegue che $F(h,k) = hk$ è suriettivo.

  Per l'iniettività, sia $(h,k) \in \operatorname{Ker} F$; allora $F(h,k) = hk = e_G \iff hk = e_G \iff h = k^{-1}$, ma visto che $H \cap K = \{e_G\}$, deve essere $h = k = e_H$, quindi $\operatorname{Ker} F = \{(e_G, e_G)\}$.

Allora $F : H \rtimes_\gamma K \to G$ è un isomorfismo di gruppi, per cui $G \cong H \rtimes_\gamma K$. □

Esercizio 1.2. Dimostrare che $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.

Svolgimento. Sia $D_n = \langle \rho, \sigma \mid \rho^n = \sigma^2 = e,\ \sigma\rho\sigma = \rho^{-1} \rangle$. Notando che $\langle\rho\rangle \cong \mathbb{Z}/n\mathbb{Z}$ e che $\langle\sigma\rangle \cong \mathbb{Z}/2\mathbb{Z}$, si mostra sostanzialmente che $D_n \cong \langle\rho\rangle \rtimes_\varphi \langle\sigma\rangle$. Per poter applicare il teorema di decomposizione, si nota che $\langle\rho\rangle \lhd D_n$ perché ha indice 2, poi $\langle\rho\rangle \cap \langle\sigma\rangle = \{e\}$ e, infine, $|\langle\rho\rangle\langle\sigma\rangle| = |D_n|$ perché

$$|\langle\rho\rangle\langle\sigma\rangle| = \frac{|\langle\rho\rangle||\langle\sigma\rangle|}{|\langle\rho\rangle \cap \langle\sigma\rangle|} = 2n$$

Allora $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.

Il prodotto semidiretto, in questo caso, è definito da $\varphi : \langle\sigma\rangle \to \operatorname{Aut}(\langle\rho\rangle)$ tale che $\sigma \longmapsto \varphi_\sigma$ e $\varphi_\sigma(\rho) = \sigma\rho\sigma = \rho^{-1}$. Visto che φ è un omomorfismo, deve valere $\operatorname{ord}(\varphi_\sigma) \mid \operatorname{ord}(\sigma) = 2$, quindi ci sono due possibilità: o $\varphi_\sigma = \operatorname{Id}$, oppure è tale che $\rho \longmapsto \rho^{-1}$; nel primo caso, si ha il prodotto diretto, mentre nel secondo caso si ha il prodotto semidiretto che definisce D_n.

Se, poi, in $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$ sono presenti altri elementi di ordine 2, come nel caso di $\operatorname{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong (\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, si possono definire altri prodotti semidiretti, che potrebbero risultare isomorfi al caso dell'identità o a $\rho \longmapsto \rho^{-1}$. ■

Esempio 1.8 (Classificazione dei gruppi di ordine pq.). Si considera prima il caso $p = q$, da cui $|G| = p^2$, per il quale si sa che le uniche possibilità sono $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, oppure $G \cong \mathbb{Z}/p^2\mathbb{Z}$.

Si assume, ora, $q > p$ e $|G| = pq$; per Cauchy, esistono due sottogruppi $H, K < G$ di ordine q e p rispettivamente; usando la proposizione 1.31, si sa anche che $H \triangleleft G$[a]

Inoltre, si sa anche che H è caratteristico perché è l'unico sottogruppo di ordine q. Infatti, se esistesse $H' < G$ tale che $|H'| = q$, si avrebbe $|HH'| = |H||H'|/|H \cap H'| = q^2/|H \cap H'|$. Visto che $|H \cap H'|$ può essere 1, oppure q, quindi $|HH'|$ è q, o q^2, ma non può essere q^2 perché sarebbe maggiore di $|G|$, quindi $|H \cap H'| = q \Rightarrow H = H'$.

Usando il teorema di scomposizione (1.10), si conclude che $G = H \rtimes_\gamma K$ perché, per una questione di ordine, $H \cap K = \{e_G\}$ e $|HK| = |H||K|/|H \cap K| = |H||K| = pq$, quindi $G = HK$[b].

Prendendo $H = \langle x \rangle$ e $K = \langle y \rangle$, si ha

$$\gamma : \langle y \rangle \longrightarrow \mathrm{Aut}(\langle x \rangle),\ \gamma(y)(x) = \gamma_y(x) = yxy^{-1} = x^\ell$$

Visto che γ è un omomorfismo, deve valere $\mathrm{ord}(\gamma_y) \mid \mathrm{ord}(y)$, cioè $\mathrm{ord}(\gamma_y) \in \{1, p\}$ (visto che p è primo), quindi se $p \nmid (q-1)$[c], allora $\mathrm{ord}(\gamma_y) = 1$ e $\gamma_y = \mathrm{Id}_H$, quindi $G \cong \mathbb{Z}/(pq)\mathbb{Z}$. Se, invece, $p \mid (q-1)$, allora esiste un sottogruppo di ordine p in $\mathbb{Z}/(q-1)\mathbb{Z}$, il quale ha $p-1$ elementi di ordine p (sempre perché p è primo), quindi ci sono $p-1$ possibili omomorfismi γ che generano gruppi $H \rtimes_\gamma K$ diversi a seconda di dove mandano y; l'idea è di dimostrare che questi sono tutti isomorfi tra loro.

Siano, allora γ, γ' due omomorfismi tali che $\gamma_y(x) = x^\ell$ e $\gamma'_y(x) = x^{\ell'}$, con ℓ, ℓ' coprimi con q[d]; si ha:

$$(\gamma_y)^p = \mathrm{Id} \implies x^{\ell^p} = x \implies \ell^p = 1$$

quindi $\mathrm{ord}(\ell) = \mathrm{ord}(\ell') = p$, per cui $\exists r \in \mathbb{N}$ tale che $\ell' = \ell^r$, con $0 < r < p-1$. Questo significa che $\gamma'_y = \gamma_{y^r}$, infatti $\gamma_{y^r}(x) = (\gamma_y(x))^r = x^{\ell^r} = x^{\ell'}$. Per conclude, si nota che $\psi : H \rtimes_\gamma K \longrightarrow H \rtimes_{\gamma'} K$ tale che $\psi((x, y)) = (x, y^r)$ è un isomorfismo (facile verifica), quindi ogni prodotto semidiretto genera gruppi isomorfi.

Se ne conclude che, nel caso $p \mid q-1$, ci sono solo due possibili gruppi distinti di ordine pq, a meno di isomorfismi.

[a]Perché $[G : H] = |G/H| = |G|/|H| = qp/q = p$.
[b]Si ricorda che $H \triangleleft G$ implica che HK è un gruppo.
[c]La richiesta deriva dal fatto che $|\mathrm{Aut}(\langle x \rangle)| = |\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})| = |(\mathbb{Z}/q\mathbb{Z})^*| = q-1$. La richiesta $p \mid q-1$, invece, è legata alla necessità che $\mathrm{ord}(\gamma_y) \mid \mathrm{ord}(y) = p$, cioè che in $(\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$

esista un sottogruppo di ordine esattamente p (visto che p è primo), cosa che è verificata se e solo se $p \mid q-1$.

[d]Perché le mappe γ_y e γ'_y sono automorfismi di $\mathbb{Z}/q\mathbb{Z}$, quindi devono mappare un generatore (x in questo caso) in un altro generatore.

Osservazione 1.13. Si riassume e si dà un'idea qualitativa dei risultati sulla classificazione dei gruppi di ordine pq. Nel caso in cui $p \nmid q-1$, l'unico gruppo possibile di ordine pq a meno di isomorfismi è $G \cong \mathbb{Z}/pq\mathbb{Z}$ perché non esistono automorfismi di ordine p in $\mathrm{Aut}(H) \cong \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Se, invece, $p \mid q-1$, si hanno due possibilità: $G \cong \mathbb{Z}/pq\mathbb{Z}$, oppure G è isomorfo a un gruppo non-abeliano relativo ad un prodotto semidiretto non banale. Tale gruppo non-abeliano è unico a meno di isomorfismo perché $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ è ciclico, quindi tutti gli elementi di ordine p generano lo stesso sottogruppo, pertanto inducono lo stesso prodotto semidiretto.

§1.11 Ancora sulle permutazioni

Per il teorema delle classi, si sa che $|Z_{S_n}(\sigma)||\,\mathrm{Cl}_{S_n}(\sigma)| = n!$; analogamente, se $\sigma \in A_n$, allora $|Z_{A_n}(\sigma)||\,\mathrm{Cl}_{A_n}(\sigma)| = n!/2$, con

$$Z_{A_n}(\sigma) = \left\{\rho \in A_n \mid \rho\sigma\rho^{-1} = \sigma\right\} = Z_{S_n}(\sigma) \cap A_n$$

Osservazione 1.14. Dalla formula delle classi, appare che, passando da S_n ad A_n, una classe di coniugio può rimanere uguale, oppure scindersi in due di uguale grandezza. La seconda eventualità è relativa a quando il centralizzatore di S_n del rappresentante è interamente contenuto in A_n; in questo caso, infatti, il centralizzatore di A_n coincide con quello di A_n, quindi, per la formula delle classi:

$$|\mathrm{Cl}_{A_n}(\sigma)||Z_{A_n}(\sigma)| = |\mathrm{Cl}_{A_n}(\sigma)||Z_{S_n}(\sigma)| = |\mathrm{Cl}_{A_n}(\sigma)|\frac{n!}{|\mathrm{Cl}_{S_n}(\sigma)|} = \frac{n!}{2}$$
$$\implies |\mathrm{Cl}_{A_n}(\sigma)| = \frac{|\mathrm{Cl}_{S_n}(\sigma)|}{2}$$

Nella prima eventualità, invece, è l'ordine della classe a rimanere invariato nel passaggio da S_n ad A_n.

Lemma 1.10.1. Sia $H < S_n$; allora $|H \cap A_n| = |H|$, se $H \subset A_n$, altrimenti $|H \cap A_n| = H/2$.

Dimostrazione. Si considera il seguente diagramma:

$$\begin{tikzcd} H \arrow[r, "\phi"] \arrow[rr, bend right, "\gamma"'] & S_n(\mathbb{R}) \arrow[r, "\psi"] & S_n/A_n \cong \{\pm 1\} \end{tikzcd}$$

con ψ omomorfismo suriettivo e $S_n/A_n \cong \{\pm 1\}$ per il I teorema di omomorfismo applicato all'omomorfismo suriettivo $S_n \xrightarrow{\text{sgn}} \{\pm 1\}$, dove $\operatorname{Ker} \operatorname{sgn} = A_n$.

Ora, considerando la mappa $\gamma : H \to S_n/A_n \cong \{\pm 1\}$, si nota che se $H \cap A_n = H$, allora H contiene unicamente permutazioni pari e γ è l'applicazione banale perché $\operatorname{Ker} \gamma = H$. Se, invece, $H \not\subset A_n$, significa che H contiene almeno una permutazione dispari, per cui il quoziente H/A_n ha indice 2 e γ è un omomorfismo suriettivo, pertanto $H/\operatorname{Ker} \gamma \cong \{\pm 1\}$. Si osserva che $\operatorname{Ker} \gamma = H \cap A_n$, quindi: nel primo caso, si ottiene $H \cap A_n = H$, quindi $|H \cap A_n| = |H|$; nel secondo caso, si ha $H/H \cap A_n \cong \{\pm 1\}$, quindi $|H| = 2|H \cap A_n|$. □

Esercizio 1.3. I 3-cicli sono tutti coniugati in A_n, con $n \geq 5$.

Svolgimento. Dato $\sigma = (a, b, c) \in S_5$ un 3-ciclo, per $n \geq 5$ si ha $(d, e) \in Z_{S_n}(\sigma)/Z_{A_n}(\sigma)$, con $d, e \notin \{a, b, c\}$; per il lemma precedente, quindi, $|\mathrm{Cl}_{A_n}(\sigma)| = |\mathrm{Cl}_{S_n}(\sigma)|$.

Se, al contrario, si considera $n = 3$, per esempio, $A_3 = \langle(1, 2, 3)\rangle = \{\mathrm{Id}, (1, 2, 3), (1, 3, 2)\}$; se, per assurdo, $\mathrm{Cl}_{A_n}(1, 2, 3) = \{(1, 2, 3), (1, 3, 2)\}$, si avrebbe $|\mathrm{Cl}_{A_n}(1, 2, 3)| = 2 \nmid 3 = |A_3|$[a], quindi $\mathrm{Cl}_{A_n}(1, 2, 3) = \{(1, 2, 3)\}$.

Infine, per $n = 4$, si ha $|A_4| = 12$ e $|\mathrm{Cl}_{S_4}(a, b, c)| = \binom{4}{3} 2! = 8 \nmid 12$. ■

[a] Il fatto che l'ordine della classe di coniugio debba dividere l'ordine del gruppo è diretta conseguenza della formula delle classi.

Esercizio 1.4. I 5-cicli non sono tutti coniugati in A_5.

Svolgimento. Le classi di coniugio di un 5-ciclo di S_5 sono 4!; se $\mathrm{Cl}_{A_5}(\sigma)$ avesse stessa cardinalità, con σ un 5-ciclo, allora, per la formula delle classi:

$$|Z_{A_5}(\sigma)| = \frac{|A_5|}{|\mathrm{Cl}_{A_5}(\sigma)|} = \frac{5!/2}{4!} = \frac{5}{2}$$

che è assurdo, quindi tale classe di equivalenza si scinde in due. ■

Esercizio 1.5. A_4 non contiene sottogruppi di ordine 6.

Svolgimento. Poniamo caso che $\exists H < A_4$ con $|H| = 6$, allora $H \lhd A_4$[a] e $\exists \sigma \in H$ con $\operatorname{ord}(\sigma) = 2$ e $\sigma = (a, b)(c, d)$. Si nota che

$\mathrm{Cl}_{S_4}(\sigma) = \{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} = \mathrm{Cl}_{A_4}(\sigma)$; inoltre, $K = \{e,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} \lhd S_4$, ma se H è normale e $\sigma \in H$, allora $\mathrm{Cl}_{A_4}(\sigma) \subset H$, quindi $K \lhd H$, il che è assurdo perché $|K| = 4 \nmid 6 = |H|$. ■

[a]Si avrebbe $[A_4 : H] = 2$, quindi risulterebbe $H \lhd A_4$.

Proposizione 1.25. Per ogni $n \geq 5$, A_n è semplice, cioè non ha sottogruppi normali non-banali.

Dimostrazione. Si procede per induzione su n. Per il passo base, si considera $n = 5$. In questo caso, $|A_5| = 60$; considerando $H \lhd A_5$, se H contiene un 3-ciclo, li contiene tutti, ma visto che questi generano A_n, allora $H = A_n$. Se contiene un 2×2-ciclo, invece, per coniugio, contiene un 3-ciclo[a] e ci si ritrova nel caso precedente. Se H contiene un 5-ciclo, ancora per coniugio, contiene un 3-ciclo[b] e, nuovamente, si è nel primo caso. Allora H è banale.

Ora si assume che la tesi sia vera $\forall m < n$ e si dimostra per n. Si considera, allora, per $n \geq 6$, $A_n \supset G_i = \{\sigma \in A_n \mid \sigma(i) = 1\} \cong A_{n-1}$, dove ogni G_i è coniugato di qualche altro.

Sia, ora, $N \lhd A_n$, per cui $N \cap G_i \lhd G_i$; per induzione, dunque, si ha, per ogni i, $N \cap G_i = G_i$, oppure $N \cap G_i = \{e\}$. Se $\forall i,\ N \cap G_i = G_i$, allora per un certo i, G_i contiene un 3-ciclo, pertanto $N = A_n$.

Se, al contrario, $\forall i,\ N \cap G_i = \{e\}$, allora N è il sottogruppo degli elementi che non fissano alcun elemento. Siano $\sigma, \tau \in N$; se $\sigma(i) = \tau(i) \implies \sigma\tau^{-1}(i) = i \implies \sigma = \tau$. Allora si scrive σ come prodotto di cicli disgiunti di lunghezze $r_1, \ldots, r_k$ decrescenti: $\sigma = C_1 \cdots C_k$. Si assume $r_i \geq 3$ per un certo i, quindi $C_i = (i_1, i_2, i_3, \ldots)$; prendendo $\rho = (i_3, j, k)$ tale che $j, k \notin \{i_1, i_2, i_3\}$, si ha $\rho\sigma\rho^{-1} = \tau$ e $\sigma(i_1) = \tau(i_1) = i_2$, ma $\sigma \neq \tau$ che è assurdo.

Si considera, ora, $\forall i,\ r_i = 2$, quindi $\sigma = (i,j)(k,l)\ldots$ è prodotto di trasposizioni; scegliendo $\rho = (\ell, p, q)$, con $p, q \notin \{i, j, k\}$, si ha che $\tau = \rho\sigma\rho^{-1}$ e σ sono distinti, ma $\sigma(i) = \tau(i) = j$, il che è assurdo.

Si conclude che N è banale, pertanto A_n è semplice. □

[a]Per esempio, $((1,2)(3,4))((1,5)(3,4)) = (1,5,2)$.
[b]Per esempio, $(1,2,3,4,5)(1,5,3,4,2) = (3,4,5)$.

Sottogruppi normali di $\mathbf{S_n}$. Per $n = 4$, si hanno A_4 e $\langle (1,2)(3,4), (1,3)(2,4) \rangle$. Per $n = 5$, S_n ha un solo sottogruppo normale, cioè A_5; infatti, se $H \lhd S_n$ e $|H| \nmid |A_n|$, allora $H \cap A_n \lhd A_n$, però A_n è semplice, quindi $H \cap A_n = \{e\}$. Questo implica che H è generato da una trasposizione, quindi non è normale.

Esercizio 1.6. Dimostrare che $S_n \cong A_n \rtimes_\varphi \langle(1\ 2)\rangle$.

Svolgimento. Visto che $[S_n : A_n] = 2$, allora $A_n \lhd S_n$; inoltre, essendo $|A_n| = n!/2$, per questione di cardinalità, si ha $A_n\langle(1\ 2)\rangle = S_n$[a]. Ora, ricordando che $A_n = \operatorname{Ker}\operatorname{sgn}$ e che $\langle(1\ 2)\rangle$ contiene solo trasposizioni (il cui segno è -1), deve valere $A_n \cap \langle(1\ 2)\rangle = \{e\}$. In questo modo, le ipotesi del teorema di decomposizione semidiretta (th. 1.10) sono soddisfatte, pertanto $S_n \cong A_n \rtimes_\varphi \langle(1\ 2)\rangle$. ■

[a] Si nota che $\langle(1\ 2)\rangle = \{(2\ 1) = e, (1\ 2)\}$, quindi $|\langle(1\ 2)\rangle| = 2$.

§1.12 Teorema di struttura per gruppi abeliani finiti

Definizione 1.19 (p-torsione). Sia G un gruppo abeliano finito; si definisce *p-componente* o *componente di p-torsione* l'insieme $G(p) = \{g \in G \mid \operatorname{ord}(g) = p^k,\ k \in \mathbb{N}\}$.

Proposizione 1.26. Dato G abeliano e finito; allora $G(p) < G$ è un p-sottogruppo e $G(p) \operatorname{char} G$ (cioè è un sottogruppo caratteristico).

Dimostrazione. $G(p) < G$ perché se $x, y \in G : \operatorname{ord}(x) = p^m$, $\operatorname{ord}(y) = p^n$, con $m, n \in \mathbb{N}$, allora $\operatorname{ord}(xy) \mid [\operatorname{ord}(x), \operatorname{ord}(y)]$, il che vuol dire che $\operatorname{ord}(xy) = p^s$, per qualche $s \in \mathbb{N}$. Inoltre, l'ordine del prodotto di qualsiasi coppia di elementi di G è sempre finito, quindi sempre nella forma di potenze di p, perché $|G| < \infty$ per assunzione.

Il fatto che sia un p-gruppo deriva direttamente dal teorema di Cauchy: se fosse $|G(p)| = p^\ell m$, con $m \in \mathbb{N}$ generico, questo si decompone in una serie di numeri primi; il fatto che l'ordine di $G(p)$ possa essere diviso per un numero primo $q \neq p$, implica l'esistenza di un elemento di ordine q in $G(p)$, che è assurdo.

Infine, $G(p)$ è caratteristico perché gli automorfismi conservano l'ordine degli elementi, pertanto $G(p)$ viene mandato in se stesso. □

Teorema 1.11. Sia G un gruppo abeliano con $|G| = n = p_1^{e_1} \cdots p_s^{e_s}$, con p_i tutti primi e $p_i \neq p_j$, $\forall i \neq j$; allora

$$G \cong G(p_1) \times \ldots G(p_s)$$

Inoltre, la decomposizione di G come prodotto di p-gruppi tra loro coprimi è unica.

Dimostrazione. Per l'esistenza, si considera $|G| = n$, con $n = p_1^{e_1} \cdots p_s^{e_s}$; si procede per induzione su s.

Se $s = 1$, allora $|G| = p_1^{e_1} \Rightarrow G = G(p_1)$. Si assume che la tesi sia versa $\forall 2 \leq m < n$ e si verifica per n, che può essere scritto come $n = mm'$, con $(m, m') = 1$ e $m, m' < n$.

Si verifica prima (in notazione additiva) che $G \cong mG \times m'G$. Intanto si osserva che $mG, m'G < G$ e, visto che G è abeliano per assunzione, si ha anche che $mG, m'G \lhd G$. Inoltre, visto che $(m, m') = 1$, allora $\exists h, k \in \mathbb{Z}$ tali che

$$mh + m'k = 1 \implies m(gh) + m'(gk) = g, \ \forall g$$

da cui $G \subseteq mG + m'G$, mentre l'inclusione inversa segue direttamente dalla chiusura di G. Allora $mG + m'G = G$. Sia, ora, $x \in mG \cap m'G$, cioè $x = mg = m'g'$; allora si nota che $m'x = m'mg = ng = 0$ e $mx = mm'g' = ng' = 0$, pertanto $\operatorname{ord}(x) \mid m$ e $\operatorname{ord}(x) \mid m'$, quindi $\operatorname{ord}(x) \mid (m, m') = 1$, da cui $x = 0$. Questo implica che $mG \cap m'G = \{e\}$, il che completa le verifiche per le ipotesi del teorema 1.8 e permette di concludere che $G \cong mG \times m'G$.

Ora si fa vedere che

$$mG = G_{m'} = \{g \in G \mid m'g = 0\} \qquad m'G = G_m = \{g \in G \mid mg = 0\}$$

Si mostra che $m'G = G_m$, cioè che l'insieme dei multipli di m' in G è uguale a quello degli elementi di G il cui ordine divide m, mostrando la doppia inclusione insiemistica. Per $m'G \subseteq G_m$, si prende $m'x \in m'G$; visto che $mm'x = nx = 0$, allora $\operatorname{ord}(x) \mid m$[a], quindi $m'x \in G_m$. Viceversa, dato $x \in G_m$, cioè tale che $mx = 0$, si osserva che

$$\underbrace{mx}_{=0} h + m'kx = x \implies x = m'(kx) \implies x \in m'G$$

quindi $G_m \subseteq m'G$ e, allora, $m'G = G_m$. Questo permette di scrivere che

$$G \cong G_m \times G_{m'}$$

Visto che G_m contiene tutti e soli gli elementi di G il cui ordine divide m (analogo per $G_{m'}$), allora $|G_m|, |G_{m'}| < |G|$; inoltre, $G_m, G_{m'} \neq \{0\}$ per Cauchy, quindi $G_{m'}, G_m \lneq G$. Avendo concluso che i due sottogruppi sono propri, si può applicare l'ipotesi induttiva per scrivere che:

$$G_m = \prod_{i \in I} G(p_i) \qquad G_{m'} = \prod_{j \in J} G(p_j)$$

con $I \cup J = \{1, \ldots, s\}$ e $I \cap J = \varnothing$ (visto che $(m, m') = 1$).

Per l'unicità, la scrittura come prodotto di p-componenti deve essere unica, altrimenti, se G fosse isomorfo ad altri p-gruppi, si avrebbe

$$G \cong H_1 \times \ldots \times H_n$$

con $H_i < G$ p_i-gruppo; allora $H_i \subseteq G(p_i)$, visto che $G(p_i)$ contiene tutti gli elementi il cui ordine è una potenza di p_i, ma essendo che

$$|G| = |H_1| \cdots |H_s| = |G(p_1)| \cdots |G(p_s)| \implies |H_i| = |G(p_i)|, \ \forall i$$

visto che, per coprimalità tra gli altri fattori, $|G(p_i)|$ divide $|H_i|$ e viceversa. Quindi $H_i = G(p_i), \ \forall i = 1, \ldots, s$. □

[a] Non si considera m' perché, per ipotesi, $m'x \neq 0$.

Lemma 1.11.1. Sia G un p-gruppo e sia $x_1 \in G$ un elemento di ordine massimo; preso $\overline{x} \in G/\langle x_1 \rangle$, si trova $y \in \pi^{-1}_{\langle x_1 \rangle}(\overline{x})$ tale che $\mathrm{ord}_G(y) = \mathrm{ord}_{G/\langle x_1 \rangle}(\overline{x})$, cioè preso un elemento nel quoziente, se ne trova sempre un nella sua fibra con lo stesso ordine.

Dimostrazione. Sia, allora, $\overline{x} \in G/\langle x_1 \rangle$, quindi della forma $\overline{x} = x + \langle x_1 \rangle$; si vuole calcolare $\pi^{-1}_{\langle x_1 \rangle}(\overline{x}) = \pi^{-1}_{\langle x_1 \rangle}(x + \langle x_1 \rangle)$, per cui $y \in \pi^{-1}(\overline{x})$ sarà della forma $y = x + ax_1$. Visto che x e y sono nella stessa classe laterale di $G/\langle x_1 \rangle$, allora $\pi_{\langle x_1 \rangle}(y) = \pi_{\langle x_1 \rangle}(x) = \overline{x}$. Inoltre, il quoziente è ancora un p-gruppo, quindi sia

$$p^r = \mathrm{ord}_{\langle x_1 \rangle}(\pi_{\langle x_1 \rangle}(y)) = \mathrm{ord}_{\langle x_1 \rangle}(\overline{x}) \mid \mathrm{ord}_G(y)$$

visto che π è un omomorfismo. Per questo, si può scegliere y (al variare di a in $x + ax_1$ perché x è fissato dalla scelta di $\overline{x}$) in modo che il suo ordine sia esattamente p^r:

$$p^r y = p^r x + p^r a x_1 = 0 \iff p^r x = -p^r a x_1$$

dove, essendo $\mathrm{ord}_{\langle x_1 \rangle}(\overline{x}) = p^r$, allora $p^r x \in \langle x_1 \rangle$, cioè la sua proiezione modulo $\langle x_1 \rangle$ è nella classe laterale banale, quindi $p^r x = b x_1$. Per ipotesi, si era assunto che x_1 ha ordine massimo, sia questo p^{r_1}; allora deve risultare che $r \leq r_1$, ma

$$0 = p^{r_1} x \iff p^{r_1 - r} p^r x = 0 \iff p^{r_1 - r} b x_1 = 0$$

dove si è moltiplicato e diviso per p^r. L'ultima uguaglianza è versa se e solo se $p^{r_1} \mid p^{r_1 - r} b$ (visto che $\mathrm{ord}_G(x_1) = p^{r_1}$), quindi se e solo se $p^r \mid b \implies b = p^r b_1$. Per finire, scegliendo $a = -b_1$ e sostituendo nell'espressione iniziale, si ottiene

$$p^r y = p^r x - p^r b_1 x_1 = bx_1 - \underbrace{p^r b_1}_{=b} x_1 = 0$$

perciò $y = x - b_1 x_1 \in G$ realizza la richiesta. $\square$

Teorema 1.12. Sia G un p-gruppo abeliano; allora esistono e sono univocamente determinati $r_1, \ldots, r_t \in \mathbb{N}$, con $r_1 \geq r_2 \geq \ldots \geq r_t$, tali che:

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{r_t}\mathbb{Z}$$

Dimostrazione. Sia, quindi, $|G| = p^n$; si dimostra per induzione su n. Se $n = 1$, allora $|G| = p$, per cui $G \cong \mathbb{Z}/p\mathbb{Z}$ e la tesi è verificata.

Si assume che la tesi sia vera per $1 \leq m < n$ e si dimostra per n. Sia, allora, $x_1 \in G$ un elemento di ordine massimo, sia questo $\mathrm{ord}(x_1) = p^{r_1}$; si hanno due possibili casi: $r_1 = n$ e $r_1 < n$. Il primo caso è banale: $r_1 = n \Rightarrow G$ ciclico, per cui $G \cong \mathbb{Z}/p^n\mathbb{Z}$.

Si considera, ora, il caso in cui $r_1 < n$. Essendo G abeliano, si ha $\langle x_1 \rangle \triangleleft G$, per cui si può considerare che $G/\langle x_1 \rangle$ ha ordine $p^{n-r_1} < p^n$; allora vale la tesi induttiva e il gruppo quoziente si può fattorizzare come prodotto di gruppi ciclici:

$$G/\langle x_1 \rangle \cong \langle \overline{x}_2 \rangle \times \ldots \times \langle \overline{x}_t \rangle$$

con $\mathrm{ord}(\overline{x}_i) = p^{r_i}$ e, complessivamente, $|\langle \overline{x}_2 \rangle \times \ldots \times \langle \overline{x}_t \rangle| = p^{n-r_1}$. Si assume che tale decomposizione sia già ordinata con $r_2 \geq \ldots \geq r_t$ e si considera la seguente proiezione al quoziente:

$$\pi : G \to G/\langle x_1 \rangle \cong \langle \overline{x}_2 \rangle \times \ldots \times \langle \overline{x}_t \rangle$$

Per il lemma precedente, dunque, si trovano $x_2, \ldots, x_t \in G$ tali che

$$\mathrm{ord}_G(x_i) = \mathrm{ord}_{G/\langle x_1 \rangle}(\overline{x}_i) = p^{r_i}$$

Ora, si vuole mostrare che:

$$H = \langle x_1, \ldots, x_t \rangle \cong \langle x_2 \rangle \times \ldots \times \langle x_t \rangle$$

La proiezione al quoziente ristretta ad H è data da:

$$\pi|_H : \begin{array}{ccc} H & \longrightarrow & G/\langle x_1 \rangle \cong \langle \overline{x}_2 \rangle \times \ldots \times \langle \overline{x}_t \rangle \\ a_2 x_2 + \ldots + a_t x_t & \longmapsto & (a_2 \overline{x}_2, \ldots, a_t \overline{x}_t) \end{array}$$

Questo è un isomorfismo, infatti π è un omomorfismo suriettivo perché i generatori di H si possono mappare nelle tuple di generatori di $G/\langle x_1 \rangle$ e, per l'iniettività, si osserva che:

$$\pi(a_2x_2 + \ldots + a_tx_t) = (a_2\overline{x}_2, \ldots, a_t\overline{x}_t) = (0, \ldots, 0) \iff a_i\overline{x}_i = 0, \ \forall i$$

cioè se e solo se $\mathrm{ord}_{G/\langle x_1 \rangle}(\overline{x}_i) = p^{r_i} \mid a_i$[a]. Però, valendo anche $\mathrm{ord}(x_i) = p^{r_i}$, allora quanto appena detto è equivalente a richiedere che $a_ix_i = 0, \ \forall i$. Allora $\pi|_H$ è un isomorfismo e, quindi, vale che:

$$H \cong \langle \overline{x}_2 \rangle \times \ldots \times \langle \overline{x}_t \rangle \cong \langle x_2 \rangle \times \ldots \times \langle x_t \rangle$$

dove l'ultimo isomorfismo deriva dal fatto che si sono scelti elementi di ordini uguali, che, quindi, generano gli stessi gruppi ciclici a meno di isomorfismo.

Si dimostra, infine, che $G \cong \langle x_1 \rangle \times H$; per farlo, si verificano le ipotesi del teorema 1.8. Si inizia col far vedere che l'intersezione è banale; questo è dato dal fatto che ogni suo elemento si scrive come $a_1x_1 = a_2x_2 + \ldots + a_tx_t$, con a_1 e $a_2, \ldots, a_t$ fissati; applicando $\pi_{\langle x_1 \rangle}$ ad entrambi i membri, si ottiene

$$\overline{0} = a_2\overline{x}_2 + \ldots + a_t\overline{x}_t \iff (a_2\overline{x}_2, \ldots, a_t\overline{x}_t) = (\overline{0}, \ldots, \overline{0})$$

quindi si deve avere $x_i = 0$ nel gruppo di partenza e $a_1x_1 = 0$, da cui $\langle x_1 \rangle \cap H = \{0\}$. Per mostrare che $\langle x_1 \rangle + H = G$, si nota che $\langle x_1 \rangle + H \subseteq G$ e che

$$|\langle x_1 \rangle + H| = \frac{|\langle x_1 \rangle||H|}{|\langle x_1 \rangle \cap H|} = \frac{p^{r_1} \cdot p^{n-r_1}}{1} = p^n$$

quindi le ipotesi sono soddisfatte e $G \cong \langle x_1 \rangle \times H \cong \langle x_1 \rangle \times \ldots \times \langle x_t \rangle$.

Quanto all'unicità, si procede ancora per induzione su n in $|G| = p^n$. Se $n = 1$, la tesi è sempre verificata dal fatto che $G \cong \mathbb{Z}/p\mathbb{Z}$. Si assume, quindi, la tesi vera $\forall m < n$ e si dimostra per n.

Sia

$$G \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{r_t}\mathbb{Z} \cong \mathbb{Z}/p^{k_1}\mathbb{Z} \times \ldots \mathbb{Z}/p^{k_s}\mathbb{Z}$$

dove si assume che siano ordinati in modo tale da avere $r_1 \geq \ldots \geq r_t$ e $k_1 \geq \ldots \geq k_s$. Intanto deve valere $s = t$ perché, considerando $G_p = \{g \in G \mid gp = 0\}$ (sottogruppo degli elementi di G il cui ordine divide p), che è caratteristico (perché gli omomorfismi conservano l'ordine), si nota che gli elementi di G di ordine tale da dividere p stanno tutti in G_p, quindi G_p è isomorfo a un sottogruppo della forma $(\mathbb{Z}/p\mathbb{Z})^{\ell}$, con ℓ numero dei fattori $\mathbb{Z}/p^h\mathbb{Z}$ distinti:

$$G_p \cong (\mathbb{Z}/p\mathbb{Z})^t \cong (\mathbb{Z}/p\mathbb{Z})^s \iff t = s$$

Per concludere, si mostra che sono uguali anche le potenze di ciascun fattore. A questo scopo, si può applicare l'ipotesi induttiva al gruppo pG (con $|pG| = p^{n-t}$):

$$\begin{aligned} pG &\cong \frac{p\mathbb{Z}}{p^{r_1}\mathbb{Z}} \times \ldots \times \frac{p\mathbb{Z}}{p^{r_t}\mathbb{Z}} \cong \mathbb{Z}/p^{r_1-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{r_t-1}\mathbb{Z} \\ &\cong \mathbb{Z}/p^{k_1-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{k_t-1}\mathbb{Z} \cong \frac{p\mathbb{Z}}{p^{k_1}\mathbb{Z}} \times \ldots \times \frac{p\mathbb{Z}}{p^{k_t}\mathbb{Z}} \end{aligned}$$

dove la sequenza di isomorfismi è giustificata dall'assunzione che vi siano più fattorizzazioni per G, quindi anche per pG, ma pG deve avere decomposizione unica per ipotesi induttiva, quindi:

$$r_1 - 1 = k_1 - 1, \ldots, r_t - 1 = k_t - 1 \iff r_1 = k_1, \ldots, r_t = k_t$$

e quindi i singoli fattori hanno stesse potenze. $\square$

[a] L'uguaglianza deriva dal lemma precedente.

Teorema 1.13 (Teorema di struttura). Sia G un gruppo abeliano finito; allora G è prodotto diretto di gruppi ciclici, cioè:

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

Questa scrittura, inoltre, è unica se $n_{i+1} \mid n_i, \ \forall i \in \{1, \ldots, s-1\}$.

Dimostrazione. Si inizia col dimostrare l'esistenza. Facendo uso del teorema 1.11, allora $G \cong G(p_1) \times \ldots \times G(p_s)$. Applicando, poi, il teorema 1.12 a ciascun $G(p_i)$, si ottiene:

$$\begin{aligned} G &\cong G(p_1) \times \ldots \times G(p_s) \\ &\cong \left(\mathbb{Z}/p_1^{r_{11}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_1^{r_{1t_1}}\mathbb{Z}\right) \times \ldots \times \left(\mathbb{Z}/p_s^{r_{s1}}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_s^{r_{st_s}}\mathbb{Z}\right) \end{aligned}$$

con $r_{i1} \geq r_{it_i}$. Per il teorema cinese del resto, si possono ricomporre i termini formati da primi distinti:

$$G \cong \underbrace{\frac{\mathbb{Z}}{\left(p_1^{r_{11}} \cdots p_s^{r_{s1}}\right)\mathbb{Z}}}_{n_1} \times \ldots \times \underbrace{\frac{\mathbb{Z}}{\left(p_1^{r_{1t}} \cdots p_s^{r_{st}}\right)\mathbb{Z}}}_{n_t}$$

dove si è imposto $r_{ih} = 0$ se $h > t_i$ e con $t = \max\{t_1, \ldots, t_s\}$. Per come si è riscritta la fattorizzazione, vale $n_t \mid n_{t-1},\ n_{t-1} \mid n_{t-2}, \ldots, n_2 \mid n_1$.

Infine, l'unicità deriva direttamente dai teoremi 1.11 e 1.12; infatti, se ci fossero due decomposizioni di G diverse con ordini che si dividono a catena, ripercorrendo gli isomorfismi, si ritroverebbero due decomposizioni diverse per $G(p)$ (o per G come prodotto di p-componenti). □

Esempio 1.9. Sia

$$\begin{aligned} G &\cong \mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \\ &\cong \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \end{aligned}$$

Raggruppando ciascun termine in base all'ordine degli elementi, si ottengono i p-sottogruppi:

$$G \cong \underbrace{\left(\mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right)}_{G(2)} \times \underbrace{\left(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\right)}_{G(3)} \times \underbrace{\left(\mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\right)}_{G(5)}$$

Infine, per il teorema di struttura, si può riscrivere il prodotto in ordine decrescente, rimettendo insieme i p-gruppi ciclici di ordine massimo:

$$G \cong \mathbb{Z}/\left(2^3 \cdot 3 \cdot 5^2\right)\mathbb{Z} \times \mathbb{Z}/\left(2^2 \cdot 3 \cdot 5\right) \times \mathbb{Z}/2\mathbb{Z}$$

Esempio 1.10 (Classificazione dei gruppi di ordine 1000). Si classificano i gruppi abeliani di ordine 1000. Per farlo, si inizia col notare che $1000 = 2^3 \cdot 5^3$, quindi $G \cong G(2) \times G(5)$, con $|G(2)| = 2^3$ e $|G(5)| = 5^3$. Ne segue che le p-componenti si possono riscrivere nei seguenti modi:

$$G(2) \cong \begin{cases} \mathbb{Z}/2^3\mathbb{Z} \\ \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases} \qquad G(5) \cong \begin{cases} \mathbb{Z}/5^3\mathbb{Z} \\ \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \end{cases}$$

Ne segue che i gruppi abeliani di ordine 1000, a meno di isomorfismo, sono $3 \cdot 3 = 9$, visto che, per il teorema di struttura, si ha una fattorizzazione unica come prodotto di gruppi ciclici finiti e, per tale fattorizzazione, si hanno tre scelte per la 2-componente e tre scelte per la 5-componente.

§1.13 I teoremi di Sylow

Nel teorema seguente, sono riuniti tutti i teoremi di Sylow; il primo corrisponde al punto (a), il secondo ai punti (b) e (c) e il terzo al punto (d).

Teorema 1.14 (Teorema di Sylow). Sia G un gruppo finito e p un numero primo tale che $|G| = p^n m$, con $\gcd(m, p) = 1$; allora:

(a). *esistenza*: $\forall \alpha \in \mathbb{N} : 0 \leq \alpha \leq n,\ \exists H < G$ con $|H| = p^\alpha$;

(b). *inclusione*: ogni p-gruppo di G è contenuto in un p-Sylow[a];

(c). *coniugio*: due qualsiasi p-Sylow sono coniugati;

(d). *numero*: indicando con n_p il numero di p-Sylow di G, si ha che $n_p \mid |G|$ e $n_p \equiv 1 \pmod{p}$.

Dimostrazione. Si divide la dimostrazione nei vari punti.

(a). Si fissa $0 \leq \alpha \leq n$. Sia $\mathcal{M} = \{M \subset G \mid |M| = p^\alpha\}$; allora

$$|\mathcal{M}| = \binom{p^n m}{p^\alpha} = \frac{(p^n m)!}{p^\alpha!(p^n m - p^\alpha)!} = \frac{p^n m \displaystyle\prod_{i=1}^{p^\alpha - 1} (p^n m - i)}{p^\alpha \displaystyle\prod_{i=1}^{p^\alpha - 1} (p^\alpha - i)} = p^{n-\alpha} m \prod_{i=1}^{p^\alpha - 1} \frac{p^n m - i}{p^\alpha - i}$$

Da questo, si osserva che $p^{n-\alpha} \mid |\mathcal{M}|$ e, per $i = 1, \ldots, p^\alpha - 1$, definendo $v_p(n) := \max\left\{k \in \mathbb{N} \mid p^k \text{ divide } n\right\}$, si ha che:

$$v_p(p^n m - i) = v_p(p^\alpha - i) = v_p(i) \implies v_p\left(\frac{p^n m - i}{p^\alpha - i}\right) = v_p(p^n m - i) - v_p(p^\alpha - i) = 0$$

essendo $i \leq p^\alpha - 1$ e $\alpha \leq n$. Visto che v_p conta l'esponente massimo per cui è possibile dividere il suo input, si conclude che $p^{n-\alpha}$ divide esattamente $|\mathcal{M}|$ e $n - \alpha$ è il massimo esponente con cui p può divide $|\mathcal{M}|$[b].

Ora si considera l'azione di G su $\mathcal{M}$ data da $\phi : G \to S(\mathcal{M})$, con $\phi(g)(M) = \phi_g(M) = gM$; per il teorema delle classi:

$$|\mathcal{M}| = \sum_{M_i \in R} |\text{Orb}(M_i)| = \sum_{M_i \in R} \frac{|G|}{|\text{Stab}(M_i)|}$$

con R insieme dei rappresentanti delle orbite. Il fatto che $p^{n-\alpha} \mid\mid |\mathcal{M}|$[c] implica che $\exists i$ tale per cui

$$p^{n-\alpha+1} \nmid |\text{Orb}(M_i)| = \frac{|G|}{|\text{Stab}(M_i)|} = \frac{p^n m}{|\text{Stab}(M_i)|}$$

Ne segue che $p^\alpha \mid |\text{Stab}(M_i)|$, perché se ogni potenza di p con esponente maggiore di $n - \alpha$ non deve dividere l'ordine dell'orbita, allora, al denominatore, deve essere presente una potenza di p con esponente $\geq \alpha$.

Quindi, si ha $|\text{Stab}(M_i)| \geq p^\alpha$ e si dimostra che $|\text{Stab}(M_i)| = p^\alpha$. Per farlo, si considera la mappa $\text{Stab}(M_i) \longrightarrow M_i$ tale che $\text{Stab}(M_i) \ni y \longmapsto yx$, per $x \in M_i$, è iniettiva perché $yx = y_1 x \iff y = y_1$, quindi $\text{Stab}(M_i) \leq |M_i| = p^\alpha$, da cui $|\text{Stab}(M_i)| = p^\alpha$. Essendo $\text{Stab}(M_i) < G$, significa che in G esiste un sottogruppo di ordine p^α.

(b). Sia S un p-Sylow di G, con $|S| = p^n$ e sia $H < G$ un sottogruppo con $|H| = p^\alpha$. Si nota che $|G/S| = |G|/|S| = p^n m / p^n = m$.

Si considera l'azione di H su $G/S = X$ definita da

$$\varphi : \begin{array}{ccc} H & \longrightarrow & S(X) \\ h & \longmapsto & \varphi_h \end{array}, \text{ con } \varphi_h(gS) = hgS$$

Per la formula delle classi:

$$m = |X| = \sum_{g \in R} |\text{Orb}(gS)| = \sum_{g \in R} \frac{|H|}{|\text{Stab}(gS)|} = \sum_{g \in R} p^{a_g}$$

dove R è l'insieme dei rappresentanti delle classi di G/S e a_g è un esponente dipendente dal g in R. Visto che $p \nmid m$[d], deve esistere un $g \in R$ tale che $a_g = 0$, per cui $\text{Orb}(gS) = \{gS\} \Rightarrow \text{Stab}(gS) = H$. Questo significa anche che $\forall h \in H,\ hgS = gS \Rightarrow H \subset gSg^{-1}$, ma gSg^{-1} è un p-Sylow perché $|gSg^{-1}| = |S|$, quindi H è contenuto in un p-Sylow.

(c). Quanto riportato in (b) dimostra anche la parte sul congiugio; infatti, se H è un p-Sylow con $|H| = p^n$, allora è un p-gruppo, allora $H \subset gSg^{-1}$ e, visto che hanno stessa cardinalità, segue che $H = gSg^{-1}$.

(d). Sia S un p-Sylow; visto che tutti i p-Sylow sono coniugati, per un certo p fissato, significa che il loro numero è pari all'ordine della classe di coniugio di S, pertanto $n_p = |\text{Cl}(S)| = [G : N_G(S)] \mid |G|$. Si considera, ora, l'azione di S sull'insieme dei coniugati di S in G, Y, definita da $\phi : S \to S(Y)$, con $\phi(g)(xSx^{-1}) = \gamma_g(xSx^{-1}) = gxSx^{-1}g^{-1}$; si vuole dimostrare che $\text{Orb}(S)$ è l'unica orbita banale di questa azione.

Per dimostrarlo, si considera, allora, $H \in Y$ con $\text{Orb}(H) = \{H\}$, per cui $S = \text{Stab}(H) = \{s \in S \mid sHs^{-1} = H\}$; questo, però, è equivalente a richiedere che $S \subset N_G(H) \iff SH = HS < G$. Si ha $|HS| = |H||S|/|H \cap S| = p^n p^n/|H \cap S|$, ma visto che $HS < G$, allora $|HS| \mid |G| = p^n m$, per cui deve essere $|H \cap S| = p^n$, per cui $H = S$.

Per finire, si nota che

$$|Y| = n_p = \sum_{H \in R} |\text{Orb}(H)| = \text{Orb}(S) + \sum_{H \in R \setminus \{S\}} \text{Orb}(H) = 1 + \sum_{H \in R \setminus \{S\}} \frac{|S|}{|\text{Stab}(H)|}$$

da cui $n_p = 1 + \ell p^k$, che implica $n_p \equiv 1 \pmod p$, con R insieme dei rappresentanti delle orbite.

□

[a]Si intende che se $H < G$ con $|H| = p^\alpha$, con $0 \leq \alpha \leq n$, allora H è contenuto in un sottogruppo di G di ordine $p^{\alpha+1}$.

[b]Per vederlo più chiaramente, si assume che qualche potenza di p divida i, altrimenti $p^n m - i$ e $p^\alpha - i$ non sarebbero divisibili per alcuna potenza di i e si avrebbe la tesi. Allora, si può scrivere $i = p^s j$, con $\gcd(p, j) = 1$, da cui $p^n m - i = p^s(p^{n-s} m - j)$ e $p^\alpha - i = p^s(p^{\alpha - s} - j)$. Il loro rapporto semplifica p^s e rimane il rapporto di due termini non divisibili per alcuna potenza di p perché $(j, p) = 1$.

[c]La notazione || si usa per indicare divisione esatta, cioè nessun esponente maggiore è divisore.

[d]Questo è per assunzione, cioè $|G| = p^n m$ con $(p, m) = 1$.

Osservazione 1.15. Sia G un gruppo tale che $|G| = p^n m$, con $(p, m) = 1$ e p primo. L'ultimo teorema di Sylow afferma che $n_p \mid |G|$, oltre che $n_p \equiv 1 \pmod p$. Il fatto che $n_p \mid |G|$, in realtà, si può migliorare notando che $n_p \mid m$ perché se S è un p-Sylow (quindi $|S| = p^n$), allora il $S < N_G(S)$[a] e, quindi, $|S| = p^n \mid |N_G(S)| \implies |N_G(S)| =$

$p^n q$. Ne segue che, per il teorema di orbita-stabilizzatore:

$$|G| = |\mathrm{Cl}_G(S)||N_G(S)| \implies n_p = |\mathrm{Cl}_G(S)| = \frac{p^n m}{p^n q} = \frac{m}{q}$$

cioè $n_p \mid m$.

[a] Questo perché ogni elemento di S è tale da normalizzare S, visto che il gruppo è chiuso sotto relativa operazione.

§1.13.1 Classificazione dei sottogruppi di ordine 12

Sia $|G| = 12 = 2^2 \cdot 3$. Per Sylow, devono esistere un 2-Sylow P_2 e un 3-Sylow P_3, con $|P_2| = 4$ e $|P_3| = 3$; essendo p-gruppi distinti, deve valere anche $P_2 \cap P_3 = \{e\}$. Si nota, inoltre, che:

$$|P_2 P_3| = \frac{|P_2||P_3|}{|P_2 \cap P_3|} = 12$$

quindi $G = P_2 P_3$.

Ora si conta il numero dei sottogruppi di Sylow. Dovendo valere $n_2 \equiv 1 \pmod 2$ e $n_2 \mid |G|/4 = 3$, si ha $n_2 = 1, 3$; analogamente, si può avere $n_3 = 1, 4$. Questo significa anche che almeno uno fra P_2 e P_3 deve essere normale, altrimenti G conterrebbe più elementi di quanti effettivamente ne contiene: se $n_2 = 3$ e $n_3 = 4$, ci sarebbero 12 elementi all'interno dei 2-Sylow e altri 12 all'interno dei 3-Sylow, per un totale di $24 - 7 = 17$ elementi distinti di G (il -7 è relativo all'unità, elemento che è condiviso da tutti).

Avendo almeno uno fra i due sottogruppi che è normale, sono soddisfatte le ipotesi del teorema di decomposizione semidiretta, per cui si può avere

$$G \cong P_2 \rtimes_\varphi P_3 \qquad \text{oppure} \qquad G \cong P_3 \rtimes_\varphi P_2$$

Si studiano separatamente i due casi.

- Caso $G \cong P_2 \rtimes_\varphi P_3$.

  In questo caso, si ha $P_2 \lhd G$, con $|P_2| = 4$, per cui si ha $P_2 \cong \mathbb{Z}/4\mathbb{Z}$, oppure $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

  Il primo caso è relativo al prodotto $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$, con

$$\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

In questo caso, si può solo avere $[1]_3 \mapsto \mathrm{Id}$, quindi il prodotto semidiretto diventa il prodotto diretto $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$.

Nel secondo caso, invece, si ha $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$, con

$$\varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$$

Allora si può mappare $[1]_3 \mapsto \mathrm{Id}$, per avere il prodotto diretto

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

oppure si può mappare $[1]_3$ in qualunque altro elemento, il cui ordine divida 3, cioè uno dei due 3-cicli in questo caso, per cui si hanno altre due possibilità per $\varphi([1]_3)$. In realtà, si vede che queste due possibilità portano a due prodotti semidiretti che originano gruppi isomorfi (come nel caso dei gruppi di ordine pq).

Si nota, infine, che

$$G = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/3\mathbb{Z} \hookrightarrow S_4$$

perché G agisce per coniugio sull'insieme $X = \{P_3, P_3', P_3'', P_3'''\}$ dei suoi quattro 3-Sylow, pertanto si ha l'azione $\phi : G \longrightarrow S(X) \cong S_4$, con $\mathrm{Ker}\, \phi = \{\mathrm{Id}\}$. Allora è possibile dimostrare che $G \cong A_4$, cioè al gruppo alternante di 4 elementi.

- Caso $G \cong P_3 \rtimes_\varphi P_2$.

  In questo caso, si ha $P_3 \lhd G$. Come prima, essendo che $|P_2| = 4$, per il teorema di struttura, si ha:

  $$P_2 \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases} \qquad \text{e} \qquad P_3 \cong \mathbb{Z}/3\mathbb{Z}$$

  Il primo caso possibile è il prodotto $\mathbb{Z}/3\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z}$, con $\varphi : \mathbb{Z}/4\mathbb{Z} \longmapsto \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, per cui $[1]_4 \longmapsto \mathrm{Id}, -\mathrm{Id}$; se $[1]_4 \mapsto \mathrm{Id}$, si ha il prodotto diretto $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$, altrimenti si ha il gruppo risultante da $\mathbb{Z}/3\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z}$.

  Considerando, ora, il caso in cui $P_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, allora si considera il prodotto semidiretto con

  $$\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

Mappando gli elementi di $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nell'identità di $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$, si avrebbe il prodotto diretto $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Per l'altro caso, si nota che in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, si hanno due elementi di ordine 2 che vanno in $-\mathrm{Id}$ e un altro elemento di ordine 2 che va in Id[1]; in questo modo, si costruiscono tre prodotti semidiretti che originano gruppi isomorfi tra loro. Assumendo, senza perdita di generalità, che

$$\varphi_x = \mathrm{Id} \qquad \varphi_y = -\mathrm{Id} \qquad \varphi_{xy} = -\mathrm{Id}$$

con $\langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e $\langle z \rangle \cong \mathbb{Z}/3\mathbb{Z}$, allora:

$$\varphi_x(z) = xzx^{-1} = \mathrm{Id}(z) = z$$

cioè x e z commutano. Similmente

$$\varphi_y(z) = yzy^{-1} = -\mathrm{Id}(z) = -z$$

A questo punto, si può concludere che il sottogruppo generato da y e z soddisfa la seguente presentazione:

$$\langle y, z \mid y^2 = z^3 = 1,\ yzy^{-1} = z^{-1} \rangle$$

cioè è isomorfo a D_3. Infine, visto che x commuta sia con y, che con z, si ha il prodotto diretto tra $\langle x \rangle \cong \mathbb{Z}/2\mathbb{Z}$ e $\langle y, z \rangle \cong D_3$, cioè:

$$\mathbb{Z}/2\mathbb{Z} \times D_3 \cong D_6$$

In questo modo, si sono classificati tutti i gruppi di ordine 12, che sono:

$$\mathbb{Z}/12\mathbb{Z} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \quad A_4 \quad \mathbb{Z}/3\mathbb{Z} \rtimes_\varphi \mathbb{Z}/4\mathbb{Z} \quad D_6$$

[1] Questo è dovuto al fatto che, escludendo di mandare entrambi gli elementi dell'insieme generatore in Id, che corrisponderebbe al caso del prodotto diretto, si trova che quando uno dei due generatori va in $-\mathrm{Id}$ e l'altro va in Id, allora il terzo elemento di ordine 2 va in $-\mathrm{Id}$, mentre se entrambi vanno in $-\mathrm{Id}$, il terzo va in Id.

§1.14 I quaternioni

Definizione 1.20 (Gruppo dei quaternioni). Il gruppo dei quaternioni è definito tramite la seguente presentazione:

$$Q_8 = \langle i, j \mid i^4 = 1,\ i^2 = j^2,\ ij = j^3 i \rangle$$

Osservazione 1.16. Visto che $i^4 = 1$ e che $i^2 = j^2$, allora $j^4 = 1$, per cui $\operatorname{ord}(j) \mid 4$; considerando anche che

$$\operatorname{ord}(j^2) = \frac{\operatorname{ord}(j)}{(2, \operatorname{ord}(j))} = \operatorname{ord}(i^2) = 2 \implies \operatorname{ord}(j) = 4$$

Questo significa che Q_8 contiene due gruppi ciclici di ordine 4, rispettivamente $\langle i \rangle$ e $\langle j \rangle$, con

$$\langle i \rangle \cap \langle j \rangle = \left\{1, i^2 = j^2\right\}$$

Dalle regole di presentazione del gruppo, si vede che $Q_8 = \langle i \rangle \langle j \rangle$, visto che una relazione permette di scambiare i con j; allora:

$$|Q_8| = |\langle i \rangle \langle j \rangle| = \frac{|\langle i \rangle||\langle j \rangle|}{|\langle i \rangle \cap \langle j \rangle|} = \frac{16}{2} = 8$$

In effetti, gli elementi del gruppo sono:

$$Q_8 = \left\{1,\ i,\ i^2 = j^2,\ i^3,\ j,\ j^3,\ ij,\ i^3 j\right\}$$

Dalle relazioni del gruppo, si nota, inoltre, che non è abeliano:

$$ij = j^3 i = j^{-1} i \neq ji$$

§1.14.1 Sottogruppi di Q_8

Si vede che $\langle i \rangle, \langle j \rangle \lhd Q_8$, visto che hanno indice 2.

Proposizione 1.27. Si ha $\langle i^2 \rangle, \langle j^2 \rangle \lhd Q_8$.

Dimostrazione. Dalla presentazione del gruppo, si ha $ij = j^3 i = j^{-1} i$, ossia $j^{-1} ij = j^{-2} i = j^2 i = i^3 = i^{-1}$, quindi $j^{-1} ij = i^{-1}$. Ora si può osservare che:

$$j^{-1} i^2 j = (j^{-1} ij)^2 = i^{-2} = i^2$$

cioè i^2 commuta con i generatori i e j, quindi commuta con tutto Q_8, dunque è normale. Dalla relazione $i^2 = j^2$ segue che $\langle i^2 \rangle = \langle j^2 \rangle$, quindi si ha anche $\langle j^2 \rangle$. $\square$

Lemma 1.14.1. Un sottogruppo $H < G$ di ordine 2 è normale se e solo se è un sottogruppo di $Z(G)$.

Dimostrazione. Dato $H = \{e, h\} \lhd G$, allora $gHg^{-1} = H$, $\forall g \in G$ per assunzione. Questo, però, è vero se e solo se $ghg^{-1} \in H \iff ghg^{-1} = h \iff gh = hg$, $\forall g \in G$, quindi $h \in Z(G)$, pertanto $H \leq Z(G)$. $\square$

Proposizione 1.28. Si ha $\langle i^2 \rangle = Z(Q_8)$.

Dimostrazione. Per quanto detto nel lemma precedente, si deve avere $\langle i^2 \rangle \leq Z(Q_8)$; inoltre, Q_8 è un p-gruppo non abeliano, essendo $|Q_8| = 2^3$, quindi sicuramente non può avere centro banale. Le altre possibilità sono:

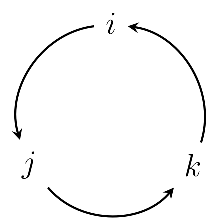
- $|Z(Q_8)| = 2$;
- $|Z(Q_8)| = 4$, ma si avrebbe $Q_8/Z(Q_8) = 2$, che è primo, quindi sarebbe ciclico e, conseguentemente, Q_8 abeliano, che è assurdo;
- $|Z(Q_8)| = 8$, cioè $Z(Q_8) = Q_8$, da cui risulterebbe Q_8 abeliano, che è assurdo.

L'unica possibilità è che $Z(Q_8)$ abbia ordine 2, quindi coincide con $\langle i^2 \rangle = \langle j^2 \rangle$. $\square$

Prodotto in $\mathbf{Q_8}$. Convenzionalmente, si definisce $ij = k$; in questo modo, gli elementi del gruppo si possono riscrivere come:

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

con $i^2 = -1$, $i^3 = -i$, $j^3 = -j$ e $i^3 j = -ij = -k$. In questo modo, si vede che i prodotti tra gli elementi di Q_8 soddisfano il seguente 3-ciclo:



Percorrendo il ciclo in senso antiorario, si ha:

$$ij = k \qquad jk = i \qquad ki = j$$

In senso orario, invece:

$$ji = -k \qquad ik = -j \qquad kj = -i$$

Inoltre, si nota che:

$$k^2 = (ij)^2 = ijij = i^2$$

Ne segue, quindi, che $\text{ord}(1) = 1$ e $\text{ord}(-1) = 2$, mentre l'ordine di $\pm i, \pm j, \pm k$ è 4.

Per motivi di ordine degli elementi, quindi, nonostante Q_8 abbia ordine 8 e non sia abeliano, non si ha un isomorfismo con D_4, visto che quest'ultimo ha un solo elemento di ordine 4.

Sottogruppi di $\mathbf{Q_8}$. Quanto ai sottogruppi di Q_8, si vede, intanto, che $\langle -1 \rangle = Z(Q_8)$ ed è caratteristico, visto che è il centro (oppure si può concludere osservando che è l'unico sottogruppo di ordine 2). Al contrario, $\langle i \rangle$, $\langle j \rangle$ e $\langle k \rangle$ sono sottogruppi di ordine 4 e, come accennato, sono normali. Questo permette di concludere che ogni sottogruppo di Q_8 è normale.

Prodotto semidiretto. Infine, si osserva che Q_8 non può essere ottenuto come prodotto semidiretto di alcun suo sottogruppo; infatti, $\forall H_1, H_2 < Q_8$, si ha $H_1 \cap H_2 \neq \{1\}$ perché l'intersezione contiene sempre anche -1.

§1.14.2 Classificazione dei gruppi di ordine 8

Si considera $|G| = 8 = 2^3$. Si distingue, anzitutto, il caso in cui G risulta abeliano; in questo caso, infatti, si può fare uso del teorema di struttura per concludere le varie possibilità:

$$\mathbb{Z}/8\mathbb{Z} \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Considerando, adesso, il caso in cui G non sia abeliano, si nota che G deve contenere almeno un elemento di ordine 4; infatti, se contenesse solo elementi di ordine 2, sarebbe isomorfo a $(\mathbb{Z}/2\mathbb{Z})^3$, che è abeliano. Sia, dunque, $a \in G$ tale che $\text{ord}(a) = 4$. Visto che $\langle a \rangle$ ha indice 2 in G, si ha $\langle a \rangle \triangleleft G$ e

$$G/\langle a \rangle = \{\langle a \rangle, b\langle a \rangle\}$$

con $b \in G \setminus \langle a \rangle$. Quanto all'elemento $b\langle a \rangle \in G/\langle a \rangle$, si nota che $b^2\langle a \rangle = \langle a \rangle$, altrimenti si avrebbe $b^2\langle a \rangle = b\langle a \rangle \implies b\langle a \rangle = \langle a \rangle$, che è assurdo. Dunque:

$$b^2\langle a \rangle = \langle a \rangle \implies b^2 \in \langle a \rangle = \left\{e, a, a^2, a^3\right\}$$

però non può essere $b^2 = a$, oppure $b = a^3$ perché b avrebbe ordine 8 (quindi $b \in G \Rightarrow G$ abeliano perché generato da b), quindi rimangono solamente $b^2 = 1$, oppure $b^2 = a^2$.

- Caso $b^2 = 1$.

  Ricordando che $a^4 = 1$ perché $\operatorname{ord}(a) = 4$ e avendo $b^2 = 1$ per assunzione, il gruppo G è composto dai seguenti elementi:

  $$G = \left\{1, a, a^2, a^3, b, ba, ba^2, ba^3\right\} = \langle a\rangle\langle b\rangle$$

  da cui si vede che $\langle a\rangle$ e $\langle b\rangle$ soddisfano le condizioni per il teorema di decomposizione semidiretta, quindi

  $$G \cong \langle a\rangle \rtimes_\varphi \langle b\rangle \cong D_4,\ \varphi : \langle b\rangle \longmapsto \operatorname{Aut}(\langle a\rangle) \cong \mathbb{Z}/2\mathbb{Z}$$

  dove $b \mapsto -\operatorname{Id}$, altrimenti si avrebbe uno dei prodotti diretti visti sopra.

- Caso $b^2 = a^2$.

  In questo caso, si ha $a^4 = 1$ e $b^2 = a^2$ Si ha che $bab^{-1} \in \langle a\rangle$, essendo $\langle a\rangle \lhd G$; inoltre, non può valere $bab^{-1} = 1$, altrimenti si avrebbe $a = 1$, ma neanche $bab^{-1} = a^2$ perché il coniugio conserva l'ordine degli elementi e nemmeno $bab^{-1} = a$ perché si assunto che G non sia commutativo. Per esclusione, l'unica possibilità è $baab^{-1} = a^3$, cioè $ba = a^3b$, per cui G soddisfa la presentazione del gruppo dei quaternioni e, dunque:

  $$G \cong Q_8$$

  dove l'isomorfismo mappa $a \mapsto i$ e $b \mapsto j$.

Ricapitolando, un gruppo di ordine 8 può uno fra i seguenti:

$$\mathbb{Z}/8\mathbb{Z} \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad (\mathbb{Z}/2\mathbb{Z})^3 \qquad D_4 \qquad Q_8$$

§1.14.3 Classificazione dei gruppi di ordine 30

Sia $|G| = 30 = 2 \cdot 3 \cdot 5$ e, nuovamente, si distinguono i due casi in cui G è abeliano, oppure non lo è. Nel primo caso, per il teorema di struttura, si ha la seguente, unica, possibilità:

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z}$$

Ora si considera il caso in cui G non sia abeliano. Si nota che G deve contenere un sottogruppo di ordine 15; infatti, dati un suo 3-Sylow P_3 e un suo 5-Sylow P_5, almeno uno fra questi due deve avere $n_p = 1$, quindi essere normale. Prima di dimostrare questo, si osserva che se uno di questi due è normale, sia questo P_5 senza perdita di generalità, si ha $P_3P_5 = P_5P_3$, per cui $P_3P_5 < G$; inoltre, avendo questi due intersezione nulla, visto che i rispettivi ordini sono coprimi, si ha

$$|P_3P_5| = \frac{|P_3||P_5|}{|P_3 \cap P_5|} = |P_3||P_5| = 15$$

Ora si dimostra la proposizione anticipata, che farà riferimento al caso di gruppi non abeliani perché il caso abeliano è ovvio: $\mathbb{Z}/15\mathbb{Z}$ è un sottogruppo di G.

Proposizione 1.29. Sia G un gruppo di ordine 30 non abeliano; allora G contiene un sottogruppo di ordine 15.

Dimostrazione. È sufficiente mostrare che uno fra P_3 o P_5 è normale perché il discorso fatto sopra risulti coerente. Per l'ultimo teorema di Sylow, si sa che $n_3 \equiv 1 \pmod 3$ e $n_3 \mid 10$, quindi $n_3 \in \{1, 10\}$, mentre $n_5 \equiv 1 \pmod 5$ e $n_5 \mid 6$, quindi $n_5 \in \{1, 6\}$.

Ammettendo che entrambi siano maggiori di 1, si avrebbero un totale di dieci 3-Sylow e sei 5-Sylow, per un totale di 45 elementi distinti, un numero ben maggiore dell'ordine di G. Questo significa che almeno uno dei due deve essere normale, da cui deriva la tesi. □

Si nota, inoltre, che questo gruppo di ordine 15 è un gruppo di ordine pq, con $p \nmid q - 1$, pertanto è isomorfo a $\mathbb{Z}/15\mathbb{Z}$ ed è ciclico; per altro, avendo indice 2, è anche normale.

Per Cauchy, G contiene un elemento di ordine 2 che è, dunque, isomorfo a $\mathbb{Z}/2\mathbb{Z}$; questi due sottogruppi soddisfano le ipotesi di decomposizione semidiretta, permettendo di scrivere che:

$$G \cong \mathbb{Z}/15\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$$

con

$$\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/15\mathbb{Z}) \cong (\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Quindi $[1]_2 \mapsto \varphi_y : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z} : x \longmapsto x^l$, in notazione moltiplicativa. Deve risultare $\mathrm{ord}(\varphi_y) \mid 2$, quindi ci sono due possibilità: o $\varphi_y = \mathrm{Id}$ (cioè $l = 1$, oppure $\varphi_y^2 = \mathrm{Id}$, che corrisponde a $\varphi_y^2(x) = (x^l)^l = x^{l^2} \overset{!}{=} x$, da cui, essendo x un generatore di $\mathbb{Z}/15\mathbb{Z}$, deve risultare

$$l^2 \equiv 1 \pmod{15} \implies l \equiv \pm 1,\ \pm 4 \pmod{15}$$

Se $l = 1$, si ha il prodotto diretto già trovato sopra, mentre negli altri tre casi si hanno tre gruppi non isomorfi tra loro.

- Caso $l = -1$.

  In questo caso, si nota che $\varphi_y(x) = x^{-1}$, che è equivalente a richiedere $yxy^{-1} = x^{-1}$, quindi $\mathbb{Z}/15\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} \cong D_{15}$.

- Caso $l = 4$.

  Si trova che l'azione data dal coniugio soddisfa $yxy^{-1} = x^4$. Se x è un elemento di ordine 3, allora si ha $x = x^4$, pertanto si conclude che y commuta con tutti gli elementi di ordine 3, il che significa che l'azione è banale solo sul fattore $\mathbb{Z}/3\mathbb{Z}$, il quale risulta normale di conseguenza e, pertanto, si può portare fuori dal prodotto semidiretto. La parte rimanente soddisfa le stesse condizioni di D_5, pertanto, se $l = 4$, risulta $G \cong D_5 \times \mathbb{Z}/3\mathbb{Z}$.

- Caso $l = -4$.

  In questo caso, si ottiene che y commuta con x se e solo se x ha ordine 5, visto che è soddisfatta la relazione $yxy^{-1} = x^{-4}$. Come nel caso precedente, questo significa che $\mathbb{Z}/5\mathbb{Z}$ è invariante sotto φ_y, quindi è normale e può essere portato fuori dal prodotto semidiretto, lasciando un gruppo che soddisfa le relazioni di D_3. In questo caso, si ha $G \cong D_3 \times \mathbb{Z}/5\mathbb{Z}$.

I gruppi trovati non sono isomorfi anche per via del fatto che hanno centri diversi:

$$Z(D_{15}) = \langle Id \rangle \quad Z(D_5 \times \mathbb{Z}/3\mathbb{Z}) = Z(D_5) \times Z(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \quad Z(D_3 \times \mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$$

Riassumendo, i gruppi di ordine 30 sono i seguenti:

$$\mathbb{Z}/30\mathbb{Z} \qquad D_{15} \qquad D_5 \times \mathbb{Z}/3\mathbb{Z} \qquad D_3 \times \mathbb{Z}/5\mathbb{Z}$$

§1.15 Complementi di teoria

Proposizione 1.30 (Quadrato di permutazioni). Una permutazione è un quadrato se e solo se i cicli di lunghezza pari compaiono a coppie.

Dimostrazione. Si nota che se η è un k-ciclo, con k dispari, allora si può scrivere

$$\eta = \eta^{k+1} = \left(\eta^{\frac{k+1}{2}}\right)^2$$

cioè un k-ciclo con k dispari è il quadrato di un altro k-ciclo. Nel caso in cui k sia pari, invece, allora è verificata la relazione

$$(a_1\ b_1\ \dots\ a_k\ b_k)^2 = (a_1\ \dots\ a_k)(b_1\ \dots\ b_k)$$

cioè il risultato del quadrato di una permutazione restituisce una decomposizione in due cicli di lunghezza pari disgiunti.

A partire da questi risultati, il caso di una permutazione generica $x^2 = (\eta_1\ \dots\ \eta_s)^2 = \eta_1^2 \cdots \eta_s^2$ è dimostrato di conseguenza: la decomposizione di questo quadrato sarà formata da cicli di lunghezza dispari e da coppie di cicli di lunghezza pari per quanto detto sopra. □

Esempio 1.11. Si considera il caso di una coppia di 3-cicli in S_6; questa si può scrivere sia come il quadrato di un ciclo di lunghezza pari, sia come il quadrato di due cicli di lunghezza dispari:

$$(123)(456) = (142536)^2 = ((132)(465))^2$$

dove la prima uguaglianza è dimostrabile per conto diretto: il prodotto di due cicli $(a_1\ \dots\ a_m)(b_1\ \dots\ b_m)$ di lunghezza dispari m si può sempre scrivere come il quadrato di un ciclo di lunghezza $2m$ $(a_1\ b_1\ \dots\ a_m\ b_m)$.

Invece, una coppia di cicli di lunghezza pari di S_4 può essere soltanto il quadrato di un 4-ciclo:

$$(12)(34) = (1423)^2 = (1324)^2$$

Proposizione 1.31. Sia G un gruppo di ordine n e sia p il più piccolo primo che divide n; se $H < G$ e $[G : H] = p$, allora $H \lhd G$.

Dimostrazione. L'insieme delle classi laterali è $G/H = \{g_1H, \dots, g_pH\}$, visto che $[G : H] = p$. Si definisce l'azione $\gamma : G \to S(G/H)$ con $\gamma(g) = \pi_g$ e $\pi_G(g_iH) = gg_iH$, che consiste nella permutazione di tutte le classi di equivalenza. Il nucleo di questo omomorfismo (è facile vedere che è un omomorfismo perché consiste nella moltiplicazione per g) è dato da:

$$\operatorname{Ker}\gamma = \{g \in G \mid \forall i,\ gg_iH = g_iH\} = \left\{ g \in G \mid g \in \bigcap_{x\in G} \operatorname{Stab}(xH) \right\}$$

Si nota che $g \in \operatorname{Stab}(xH) \Rightarrow gxH = xH \Rightarrow x^{-1}gxH = H$, che è vero se e solo se $x^{-1}gx \in H$, ossia $g \in xHx^{-1}$. Pertanto, il nucleo si può scrivere come:

$$\operatorname{Ker}\gamma = \left\{ g \in G \mid g \in \bigcap_{x\in G} xHx^{-1} \right\} \stackrel{\text{def}}{=} H_G$$

L'azione definita sopra consiste nella permutazione delle classi di equivalenza: ogni π_g moltiplica ciascuna classe per g, rimappando ciascuna classe in un'altra (in modo univoco, visto che è un automorfismo). Allora $\gamma : G \to \mathcal{S}_p(G/H) \subset S(G/H)$, con $\mathcal{S}_p(G/H) \cong S_p$; qui $\mathcal{S}_p(G/H)$ è l'insieme degli automorfismi π_g, mentre S_p è l'insieme delle permutazioni su $\{1, \dots, p\}$.

Per il I teorema di omomorfismo, $G/H_G \longrightarrow S_p$ è iniettiva[a], cioè $G/H_G \hookrightarrow S_p$; pertanto $|G/H| \mid p!$ per Lagrange. Allora ci sono due possibilità: o $|G/H| = 1$, oppure $|G/H| = p$, visto che $|G/H|$ deve dividere sia n (che ha come primo più piccolo p), che $p!$ (che ha come primo più grande p).

Per finire, basta osservare che, essendo $H \in G/H$, si ha in particolare $g \in \operatorname{Ker}\gamma \Rightarrow gH = H \iff g \in H \Rightarrow H_G \subset H$, da cui $|G/H_G| \geq p$; questo permette di escludere $|G/H| = 1$ come possibilità e concludere che $|G/H| = p$, con $H = H_G$, il che vuol dire che H è il nucleo di un omomorfismo, quindi è normale. □

[a] Non è detto che sia suriettiva, in generale sarà un isomorfismo se ristretta a un sottoinsieme di S_p.

§1.15.1 Utilizzo delle varie azioni di gruppo

(1). **Azione su classi laterali (traslazione a sinistra/destra)** Definizione: $g \cdot (xH) = (gx)H$.

- Si usa quando compare lindice $[G : H]$.
- Induce un omomorfismo $G \to S_{[G:H]}$.
- Il nucleo è il *core* di H: $\bigcap_{g\in G} gHg^{-1}$.

- Risultati tipici: un sottogruppo di indice primo (o il più piccolo primo che divide $|G|$) è normale.

(2). **Azione per coniugio su elementi del gruppo** Definizione: $g \cdot x = gxg^{-1}$.

- Si usa per studiare centro, classi di coniugio, centralizzatori e normalizzatori.
- Porta alla *class equation*: $|G| = |Z(G)| + \sum[G : C_G(x)]$.
- Risultato tipico: il centro di un p-gruppo è non banale.

(3). **Azione per coniugio su sottogruppi** Definizione: $g \cdot H = gHg^{-1}$.

- Si usa per studiare la normalità di H.
- Lorbita di H è linsieme delle sue coniugate.
- Il numero di coniugate divide $[G : H]$.
- Lintersezione delle coniugate è un sottogruppo normale (il *core*).

(4). **Azione regolare (su se stesso per moltiplicazione)** Definizione: $g \cdot x = gx$.

- Ogni gruppo si immerge in $S_{|G|}$ (Lemma di Cayley).
- Risultato tipico: ogni gruppo è isomorfo a un sottogruppo di un simmetrico.

(5). **Azione su insiemi di sottogruppi o sottostrutture** Esempi: su sottogruppi di ordine fissato, su p-sottogruppi, su insiemi di generatori.

- Utile per applicare orbit-stabilizer e contare.
- Risultati tipici: teoremi di Sylow (numero di p-sottogruppi congruo a 1 $\pmod p$).

(6). **Azione su strutture esterne** (spazi, radici di polinomi, grafi, ecc.)

- Contesto più avanzato (es. teoria di Galois).
- Esempio tipico: gruppo di Galois che agisce sulle radici di un polinomio.

§1.15.2 Automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$

Si vuole caratterizzare $\mathrm{Aut}\left((\mathbb{Z}/p\mathbb{Z})^n\right)$, con p primo. Per farlo, si inizia col notare che $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ è un campo e che, conseguentemente, $(\mathbb{Z}/p\mathbb{Z})^n$ è uno spazio vettoriale su $\mathbb{F}_p$, dove il prodotto per scalari è tale che

$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^n & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^n \\ (\overline{\lambda}, v) & \longmapsto & \overline{\lambda}v = \underbrace{v + v + \ldots + v}_{\widetilde{\lambda}} \end{array}$$

con $\widetilde{\lambda}$ un qualsiasi elemento della classe di equivalenza di $\overline{\lambda}$. Questo prodotto è ben definito perché se $\lambda, \lambda' \in \mathbb{Z}$ sono tali che $\overline{\lambda} = \overline{\lambda'}$, ossia $\exists k \in \mathbb{Z} : \lambda = \lambda' + kp$, allora

$$\overline{\lambda'}v = \underbrace{v + v + \ldots + v}_{\lambda'} = \underbrace{v + v + \ldots + v}_{\lambda+kp} = \underbrace{v + v + \ldots + v}_{\lambda}$$

Allora, per come si è definito il prodotto per scalare, è facile convincersi che $\forall \lambda \in \mathbb{Z}/p\mathbb{Z}$, $\forall \varphi \in \operatorname{Aut}\big((\mathbb{Z}/p\mathbb{Z})^n\big)$ vale $\varphi(\lambda v) = \lambda\varphi(v)$, essendo φ un omomorfismo rispetto alla somma definita in $(\mathbb{Z}/p\mathbb{Z})^n$. Da questo, si conclude che richiedere che una mappa $(\mathbb{Z}/p\mathbb{Z})^n \to (\mathbb{Z}/p\mathbb{Z})^n$ sia un automorfismo è equivalente a richiedere che sia un isomorfismo di spazi vettoriali, quindi $\operatorname{Aut}\big((\mathbb{Z}/p\mathbb{Z})^n\big) \cong \mathrm{GL}\big((\mathbb{Z}/p\mathbb{Z})^n\big) \cong \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

Proposizione 1.32. Sia p un primo; allora

$$\left|\operatorname{Aut}\big((\mathbb{Z}/p\mathbb{Z})^n\big)\right| = \prod_{i=0}^{n-1}(p^n - p^i)$$

Dimostrazione. Sia φ un automorfismo di $(\mathbb{Z}/p\mathbb{Z})^n$; allora questo è univocamente determinato da come agisce su una base di tale spazio vettoriale. Data $\{v_1, \ldots, v_n\}$ una base, allora $\varphi(v_1)$ può essere un qualunque vettore non-nullo di $(\mathbb{Z}/p\mathbb{Z})^n$, quindi si hanno $p^n - 1$ possibilità; analogamente, v_2 potrà essere mappato in qualunque elemento, eccetto l'elemento neutro e un multiplo $\varphi(v_1)$, quindi si hanno $p^n - p$ elementi. Continuando col ragionamento, si conclude che v_k potrà essere mappato in un qualsiasi elemento eccetto l'elemento neutro e un multiplo degli elementi già assegnati, per un totale di $p^n - p^{k-1}$ possibilità. □

§1.16 Esercizi

Esercizio 1.7. Studiare il gruppo $\operatorname{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$.

Svolgimento. Il sottogruppo $\{0\} \times \mathbb{Z}/n\mathbb{Z}$ è caratteristico perché un automorfismo deve conservare gli ordini degli elementi e se la prima coordinata non fosse nulla, l'elemento avrebbe ordine infinito.

Ora si considera l'immagine (a, b) dell'elemento $(1, 0)$ attraverso un automorfismo φ. ■

Esercizio 1.8. Studiare $\mathrm{Aut}(\mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

Svolgimento. Si nota che $\mathbb{Z}/20\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, quindi:

$$\begin{aligned}\mathrm{Aut}(\mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) &\cong \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \\ &\cong \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z}\end{aligned}$$

dove si è usato che $(\mathbb{Z}/5\mathbb{Z})^*$ è ciclico di ordine 4, quindi isomorfo a $\mathbb{Z}/4\mathbb{Z}$. Rimane da studiare $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

Il gruppo $G_2 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ha, come generatori, $\langle (a, 0), (0, b) \rangle$, con $\mathrm{ord}((a, 0)) = 4$ e $\mathrm{ord}((0, b)) = 2$; per studiare gli automorfismi di G_2, è necessario e sufficiente stabilire come si comportano su questi elementi, cioè imporre che vengano mandati in altri elementi di ordine 4 e 2 rispettivamente.

Concretamente, siano $(1, 0)$ e $(0, 1)$ i generatori di ordine 4 e 2 rispettivamente; il primo, allora, può essere mandato in un elemento di $\{(1, 0), (3, 0), (1, 1), (3, 1)\}$, mentre il secondo in un elemento di $\{(0, 1), (2, 0), (2, 1)\}$.

Ora, considerando $u \in \{(1, 0), (3, 0), (1, 1), (3, 1)\}$, $\langle u \rangle$ è un gruppo ciclico di ordine 4, pertanto contiene un elemento di ordine 2, che è proprio u^2; evidentemente, il gruppo $\langle u, u^2 \rangle \neq G_2$ perché ha ordine 4, quindi, fissato u, si deve rimuovere dalla lista degli elementi di ordine 2 quello corrispondente a u^2.

A questo punto, le possibili scelte sono 4 dall'insieme degli elementi di ordine 4 e 2 da quelli di ordine 2, per un totale di 8 automorfismi.

Si è dimostrato che $|\mathrm{Aut}(G_2)| = 8$; ora si mostra che $\mathrm{Aut}(G_2) \cong D_4$. Per farlo, si cercano due elementi $\alpha, \Gamma \in \mathrm{Aut}(G_2)$ tali che $\mathrm{ord}(\Gamma) = 4$, $\mathrm{ord}(\alpha) = 2$ e $\alpha\Gamma\alpha = \Gamma^{-1}$. Si prendono $\alpha((1, 0)) = (1, 0)$, $\alpha(0, 1) = (2, 1)$ e $\Gamma((0, 1)) = (2, 1)$ e $\Gamma((1, 0)) = (1, 1)$; si osserva che:

$$\begin{aligned}\alpha((x, y)) &= \alpha(x(1, 0) + y(0, 1)) = x(1, 0) + y(2, 1) = (2y + x, y) \\ \Gamma((x, y)) &= \Gamma(x(1, 0) + y(0, 1)) = x(1, 1) + y(2, 1) = (2y + x, x + y)\end{aligned}$$

da cui si può verificare l'ordine di ciascun automorfismo e, conseguentemente, che $\alpha\Gamma\alpha = \Gamma^{-1}$. ■

Esercizio 1.9. Sia $\rho = (1234)(56) \in S_{10}$; calcolare $Z(\rho)$ e

$$N(\langle \rho \rangle) = \left\{ \tau \in S_{10} \mid \tau\rho\tau^{-1} \in \langle \rho \rangle \right\}$$

Svolgimento. Si nota, intanto, che $|Z(\rho)| = |S_{10}|/|\mathrm{Cl}(\rho)| = 8 \cdot 4!$. Si considerano, poi, $H = \langle (1234), (56) \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ e $K = S_{\{7,8,9,10\}} \cong S_4$; per il teorema 1.8, visto che questi due sottogruppi sono normali, con $HK = Z(\rho)$ e hanno intersezione banale, si ha $Z(\rho) \cong \mathbb{Z}/4\mathbb{Z} \times Z/2\mathbb{Z} \times S_4$.

Per $N(\langle \rho \rangle)$, visto che $\langle \rho \rangle = \{\mathrm{Id}, \rho, \rho^2, \rho^{-1}\}$, si ha

$$\begin{aligned} N(\langle \rho \rangle) &= \left\{ \tau \in S_{10} \mid \tau\rho\tau^{-1} = \rho \text{ o } \tau\rho\tau^{-1} = \rho^{-1} \right\} \\ &= Z(\rho) \cup \left\{ \tau \in S_{10} \mid \tau\rho\tau^{-1} = \rho^{-1} \right\} = Z(\rho) \times G_{-1} \end{aligned}$$

cioè è necessario che l'immagine sotto coniugio di un generatore, in questo caso ρ, sia ancora un generatore. Allora è sufficiente caratterizzare G_{-1}. Si nota che $\rho^{-1} = \rho^3 = (56)(2341)$, quindi una possibilità è $\tau_0 = (24)$, oppure $\tau_1 = (1,4)(2,3)(5,6)$; per trovarle tutte, si osserva che

$$\tau_1^{-1}\tau_0\rho\tau_0^{-1}\tau_1 = \tau_1^{-1}\rho^{-1}\tau_1 = \rho \implies \tau_1^{-1}\tau_0 \in Z(\rho) \iff \tau_0 \in \tau_1 Z(\rho)$$

perciò $\tau \in G_{-1} \iff \tau \in \tau_0 Z(\rho)$. Ne consegue che $|N(\langle \rho \rangle)| = 2|Z(\rho)|$; in generale:

$$\begin{aligned} &N_{S_n}(\langle \rho \rangle) = \left\{ \tau \in S_n \mid \tau\rho\tau^{-1} = \rho^k,\ \gcd(\mathrm{ord}(\rho), k) = 1 \right\} \\ &\Rightarrow |N_{S_n}(\langle \rho \rangle)| = |\{k \in \mathbb{Z} \mid \gcd(k, \mathrm{ord}(\rho)) = 1\}||Z_{S_n}(\rho)| = \phi(\mathrm{ord}(\rho))|Z_{S_n}(\rho)| \end{aligned} \tag{1.16.1}$$

cioè è il centralizzatore per il numero di equazioni della forma $\tau\rho\tau^{-1} = \rho^k$. ∎

Osservazione 1.17. Si nota che il coniugio non cambia la forma della permutazione, quindi l'equazione $\tau\rho\tau^{-1} = \rho^k$ ha soluzione se e solo se k è coprimo con $\mathrm{ord}(\rho)$.

Esercizio 1.10. Determinare il minimo n tale che $Q_8 \hookrightarrow S_n$.

Svolgimento. Per il teorema di Cayley, si conclude immediatamente che $n \leq 8$; inoltre, per il teorema di Lagrange, si deve avere $n \geq 4$ perché $|S_n| = n!$ e l'immagine di Q_8 attraverso l'immersione deve avere ancora ordine 8, per cui Lagrange implica che $8 \mid n!$, cosa che si verifica unicamente da $n = 4$. In questo modo, si è ridotto il problema a considerare le seguenti cinque possibilità: S_4, S_5, S_6, S_7, S_8.

- Caso S_4.

  Se Q_8 si immergesse in S_4, con $|S_4| = 2^3 \cdot 3$, sarebbe un suo 2-Sylow, però si sa che $D_n \hookrightarrow S_n$, $\forall n$, quindi D_4 sarebbe un 2-Sylow di S_4. Per i teoremi di Sylow, si sa che ciascuna coppia di gruppi di Sylow deve essere coniugata, ma Q_8 e D_4 non lo sono, perciò Q_8 non si può immergere in S_4.

- Caso S_5.

Si procede analogamente al caso precedente. Anche nel caso di S_5, Q_8 sarebbe un suo 2-Sylow, ma visto che $D_4 \subset S_4 \subset S_5$, significa che i 2-Sylow di S_4 sono anche i 2-Sylow di S_5 (cioè sono collegati tramite isomorfismo), quindi, per le stesse ragioni di prima, Q_8 non si può immergere in S_5.

- Caso S_6.

  In questo caso, $|S_6| = 2^4 \cdot 3^2 \cdot 5$. Se fosse $Q_8 \hookrightarrow S_6$, si dovrebbe avere

  $$i \longmapsto \sigma \qquad j \longmapsto \rho \qquad k \longmapsto \sigma\rho = \eta$$

  con $\mathrm{ord}(\sigma) = \mathrm{ord}(\rho) = 4$ e $\sigma^2 = \rho^2 = \eta^2$, dove $\mathrm{ord}(\sigma^2) = \mathrm{ord}(\rho^2) = \mathrm{ord}(\eta^2) = 2$. Si nota che le permutazioni di ordine 4 in S_6 possono soltanto essere 4-cicli, oppure 4-cicli uniti a 2-cicli, mentre le permutazioni di ordine 2 sono prodotto di trasposizioni (al massimo tre, essendo in S_6).

  Usando la proposizione 1.30, il fatto che $\sigma^2 = \rho^2 = \eta^2$ abbiano ordine 2, cioè sono composte solo da trasposizioni, e che sono quadrati permette di concludere che si scrivono come il prodotto di trasposizioni; essendo in S_6, l'unica possibilità è che

  $$\sigma^2 = \rho^2 = \eta^2 = (a\ b)(c\ d)$$

  perché, in S_6, non esistono due coppie di trasposizioni tutte disgiunte. Ora si risolve $x^2 = (12)(34)$, che restituisce le seguenti possibilità:

  $$x_1 = (1324) \qquad x_2 = (1423) \qquad x_3 = (1324)(56) \qquad x_4 = (1423)(56)$$

  visto che la trasposizione (56) scompare se elevata al quadrato. In questo modo, si vede che le soluzioni possibili sono 4 in S_6, mentre in Q_8 se ne avevano 6 di elementi di ordine 4 con uguale quadrato.

- Caso S_7.

  Come nel caso di S_5, i 2-Sylow di S_7 sono isomorfi a quelli di S_6, pertanto anche S_7 non va bene.

- Caso S_8.

  Questo deve essere il caso corretto. Per Cayley, l'immersione $Q_8 \hookrightarrow S(Q_8)$ è realizzata dall'azione di moltiplicazione a sinistra:

  $$i \longmapsto \varphi_i \qquad \text{con} \qquad \varphi_i : Q_8 \longrightarrow Q_8 : x \longmapsto ix$$

e lo stesso vale per gli altri elementi di Q_8. In particolare, usando la notazione dei cicli, si ha che l'immagine di φ_i in Q_8 è data da:

$$\underbrace{(1\ i\ -1\ -i)}_{\text{4-ciclo}}(j\ k\ -j\ -k)$$

Infatti, attraverso φ_i, $1 \mapsto i \mapsto -1 \mapsto -i \mapsto 1$ e l'analogo avviene sull'insieme $\{\pm j, \pm k\}$, i quali formano due cicli disgiunti.

In maniera del tutto analoga, $\varphi_j(Q_8)$ è data da

$$(1\ j\ -1\ -j)(k\ i\ -k\ -i)$$

In questo modo, si sono costruiti i cicli di S_8 in cui vengono mappati i generatori di Q_8; assegnando dei numeri a ciascun elemento di Q_8, si possono riscrivere i cicli esposti sopra in una forma più convenzionale: per l'azione di φ_i su Q_8, ad esempio, si potrebbe avere

$$(1234)(5678)$$

mentre per l'azione di φ_j, si avrebbe, di conseguenza:

$$(1537)(2846)$$

■

2 Teoria degli anelli

§2.1 Introduzione

Definizione 2.1 (Anello). Un insieme A non vuoto si dice *anello* se sono definite due operazioni, una somma $+$ e un prodotto $\cdot$, tali che:

(a). $(A, +)$ è un gruppo abeliano;

(b). la moltiplicazione è associativa;

(c). le due sono distributive a destra e a sinistra.

Definizione 2.2 (Anello con identità). Un anello A è detto *con identità* quando è definito anche l'elemento neutro rispetto al prodotto.

Definizione 2.3 (Anello commutativo). Un anello A è detto *commutativo* quando anche il prodotto è commutativo.

Definizione 2.4 (Divisore dello zero). Sia A un anello; un suo *divisore dello zero* è un elemento $a \in A$ tale che $\exists b \in A,\ b \neq 0$ per cui $ab = 0$. L'insieme dei divisori dello zero è indicato con $D(A)$.

Definizione 2.5 (Dominio). Un anello A in cui l'unico divisore dello zero è 0 è detto *dominio*.

Definizione 2.6 (Campo). Un anello A in cui ciascun elemento eccetto 0 ha un inverso è detto *corpo*; si parla di *campo*, invece, quando A è anche commutativo.

Definizione 2.7 (Elemento nilpotente). Sia A un anello e sia $x \in A$; allora x è detto *nilpotente* se $\exists n \in \mathbb{N} : x^n = 0$. L'insieme degli elementi nilpotenti si indica con $\mathcal{N}(A)$.

Proposizione 2.1. Sia A un anello commutativo con identità; allora:

(a). $(A^*, \cdot)$ è un gruppo abeliano;

(b). $A^* \cap D(A) = \varnothing$;

(c). se A è finito, allora $A = D(A) \cup A^*$[a].

Dimostrazione. Si divide la dimostrazione nei vari punti.

(a). È chiuso rispetto al prodotto perché se $x, y \in A^*$, allora $(xy)^{-1} = y^{-1}x^{-1}$ è il suo inverso, è presente l'elemento neutro perché 1 è invertibile, il prodotto è associativo per definizione, ogni elemento ha un inverso perché l'inverso di ogni elemento è, a sua volta, invertibile ed è commutativo perché l'intero anello lo è.

(b). Se, per assurdo, $x \in A^* \cap D(A)$, allora, in A, si ha sia il suo inverso x^{-1}, sia un elemento $y \neq 0$ tale che $xy = 0$; ma allora $y = yxx^{-1} = 0$, che è assurdo.

(c). Evidentemente $D(A) \cup A^* \subseteq A$, visto che $D(A)$ e A^* sono sottoinsiemi di A. Per l'inclusione inversa, invece, se $x \in A$ e $x \in D(A)$, allora la tesi è dimostrata, altrimenti (cioè $x \in A \setminus D(A)$, si definisce l'omomorfismo di gruppi $\varphi_x : A \to A$ tale $a \longmapsto xa$; il suo nucleo è $\operatorname{Ker} \varphi_x = \{y \in A \mid \varphi_x(y) = xy = 0\} = \{0\}$, visto che x non è un divisore dello zero. Essendo $|A| < +\infty$, l'omomorfismo è anche suriettivo, quindi è un isomorfismo, quindi $1 \in \operatorname{Im} \varphi_x$ e, perciò, $\exists a \in A$ tale che $\varphi_x(a) = xa = 1 \implies x \in A^*$.

□

[a] Si nota che, quindi, un dominio finito è un campo.

Definizione 2.8 (Sottoanello). Sia A un anello e $B \subseteq A$; si dice che B è un *sottoanello* di A se è chiuso rispetto a somma e prodotto.

§2.2 Ideali

Definizione 2.9 (Ideale). Sia A un anello e sia $I \subseteq A$ un suo sottoinsieme; si dice che I è un ideale di A se:

(a). $(I, +) < (A, +)$;

(b). è soddisfatta la proprietà di assorbimento $aI \subset I$ e $Ia \subset I$, $\forall a \in A$[a].

[a] Un ideale che le soddisfa entrambe è detto *bilatero*, altrimenti è detto *ideale destro*, o *sinistro* a seconda di quella che soddisfa.

In generale, si assumerà che gli anelli siano con identità e commutativi.

Osservazione 2.1. Per verificare che un sottoinsieme di un anello commutativo con identità è un ideale, è sufficiente mostrare che $(I, +)$ è chiuso e che valga la proprietà di assorbimento perché, da queste, segue che $(-1)a \in I$, visto che -1 deve appartenere ad $(A, +)$.

Definizione 2.10 (Ideale generato). Sia A un anello e $S = \{s_1, \dots, s_n\} \subset A$ un sottoinsieme non vuoto; si definisce l'*ideale generato* da S come:

$$\langle S \rangle = \left\{ \sum_{i=1}^{n} a_i s_i \;\middle|\; a_i \in A,\ s_i \in S \right\}$$

Ora si giustifica la precedente definizione, mostrando che è effettivamente un ideale.

Dimostrazione. $\langle S \rangle$ è chiuso rispetto alla somma; infatti, dati due suoi elementi $x = \sum_{i=1}^{n} a_i s_i$ e $y = \sum_{i=1}^{n} a_i' s_i$, si ha:

$$x + y = \sum_{i=1}^{n} a_i s_i + \sum_{i=1}^{n} a_i' s_i = \sum_{i=1}^{n} (a_i + a_i') s_i \in \langle S \rangle$$

Inoltre, $\forall a \in A$, si ha:

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

quindi vale anche la proprietà di assorbimento e la tesi è dimostrata. □

Proposizione 2.2 (Operazioni tra ideali). Sia A un anello e siano $I, J \subset A$ due ideali; allora i seguenti insiemi sono ideali:

(a). $I \cap J$;

(b). $I + J = \langle I, J \rangle = \{i + j \mid i \in I,\ j \in J\}$;

(c). $IJ = \left\{ \sum_{k=1}^{n} i_k j_k \;\middle|\; n \geq 1,\ i_k \in I,\ j_k \in J \right\}$;

(d). $\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N} : x^n \in I\}$;

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

Dimostrazione. Si divide la dimostrazione nei vari punti.

(a). Si sa già che l'intersezione di sottogruppi è un sottogruppo, quindi rimane da mostrare l'assorbimento. Dato $a \in A$ e $x \in I \cap J$, allora $ax \in I$ perché I è un ideale, ma $ax \in J$ perché anche J lo è, quindi $ax \in I \cap J$.

(b). Visto che vale la proprietà commutativa (per definizione, gli ideali sono gruppi commutativi rispetto alla somma), allora dati $x, y \in I + J$ tali che $x = i_1 + j_1$ e $y = i_2 + j_2$, allora

$$x + y = (i_1 + i_2) + (j_1 + j_2) \in I + J$$

Per l'assorbimento, si nota che $ax = ai_1 + aj_1 = i'_1 + j'_1$, visto che I e J sono ideali.

(c). La chiusura è data dal fatto che la somma di due elementi è ancora una somma della stessa forma, mentre l'assorbimento a destra e sinistra è ovvio.

(d). Si nota che questo caso è valido esclusivamente per A commutativo con identità. Siano $x, y \in \sqrt{I}$, ossia $x^n, y^m \in I$, per qualche $n, m \in \mathbb{N}$; si nota che:

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

dove, per ogni $i = 0, \ldots, m+n$, si ha o che $i \geq n$, quindi $x^i \in I$, oppure che $n + m - i \geq m$, quindi $y^{n+m-i} \in I$. Ne segue che tutti i termini di $(x+y)^{n+m}$ stanno in I e, quindi, $x + y \in \sqrt{I}$. Infine, $\forall a \in A$, $(ax)^n = a^n x^n \in I$ perché $x^n \in I$ e vale la proprietà di assorbimento, quindi $ax \in \sqrt{I}$.

(e). Siano $x, y \in (I : J)$; allora $(x+y)J = xJ + yJ \implies x + y \in (I : J)$ visto che $xJ \subseteq I$ e $yJ \subseteq I$ per assunzione. Infine, $\forall \in A$, si ha $axJ = a(xJ) \subseteq aI \subseteq I \implies ax \in (I : J)$.

□

Proposizione 2.3. Sia A un anello e siano I, J due suoi ideali; in generale, $IJ \subseteq I \cap J$ e vale l'uguaglianza quando $I + J = A$.

Dimostrazione. Siano $x \in I$ e $y \in J$; per assorbimento, visto che x, y appartengono anche ad A, si ha $xy \in I$ (considerando $y \in A$) e $xy \in J$ (considerando $x \in A$), quindi $xy \in I \cap J$.

Infine, assumendo che $I + J = A$, allora vale che $i + j = 1$, per qualche $i \in I$ e $j \in J$; ne segue che $I \cap J \subseteq IJ$ perché, dato un generico $x \in I \cap J$, si ha:

$$x \cdot 1 = x(i+j) = xi + xj \in IJ$$

visto che è somma di due elementi di IJ, il quale è un gruppo additivo. Evidentemente, si è usata la commutatività del prodotto per scrivere $xi = ix$ in modo da avere un elemento di I per un elemento di J. □

Definizione 2.11 (Ideale proprio). Sia A un anello; un suo ideale I è detto *proprio* se $I \subsetneq A$.

Proposizione 2.4. Sia A un ideale; allora un suo ideale $I \subset A$ è proprio se e solo se $I \cap A^* = \varnothing$.

Dimostrazione. Se $I \cap A^* = \varnothing$, allora I è proprio perché non possiede gli elementi invertibili di A.

L'implicazione verso destra si dimostra per controposizione: sia $x \in I \cap A^*$; allora $\exists x^{-1} \in A$ tale per cui $1 = x^{-1}x \in I$ per assorbimento, ma $\forall a \in A,\ \ a = a \cdot 1 \in I$ per assorbimento, quindi $I = A$. □

Corollario 2.0.1. Sia A un anello; allora A è un campo se e solo se i suoi unici ideali sono $\{0\}$ e A.

Dimostrazione. Visto che A è un campo se e solo se $A^* = A \setminus \{0\}$, ne segue che l'unico elemento fuori A è 0, quindi, per la proposizione precedente (2.4), si conclude che gli unici ideali ammissibili sono $I = \{0\}$ e $I = A$. □

§2.3 Omomorfismi di anelli e anelli quoziente

Definizione 2.12 (Omomorfismo di anelli). Siano A, B due anelli[a]; si dice che $f : A \to B$ è un omomorfismo di anelli se, per ogni $a, a' \in A$:

(a). $f(aa') = f(a)f(a')$;

(b). $f(a + a') = f(a) + f(a')$.

Se gli anelli sono commutativi e con identità, generalmente, si assume anche che $f(1_A) = 1_B$.

[a]Non necessariamente commutativi e con unità.

Osservazione 2.2. In generale, $f(1_A) = 1_B$ non è assicurata; infatti:

$$f(a) = f(1_A a) = f(1_A a) \implies f(a) - f(1_A)f(a) = (1_B - f(1_A))f(a) = 0$$

ma la legge di cancellazione non è garantita in quanto non è detto che A sia un dominio. Se B è un dominio e $f(a) \neq 0$, allora segue $f(1_A) = 1_B$, ma se $f(A) \subset D(B)$, allora non è assicurato.

Definizione 2.13 (Anello quoziente). Sia A un anello e $I \subseteq A$ un suo ideale; si definisce *anello quoziente* la struttura $(A/I, +, \cdot)$, dove la moltiplicazione è definita da

$$(a + I) \cdot (b + I) = ab + I$$

Il quoziente è inteso rispetto alla somma, visto che I è un gruppo additivo.

Si verifica che l'operazione è ben definita: dati $a+I = a'+I$ e $b+I = b'+I$, allora

$$(a'+I)(b'+I) = a'b'+I = (a+I)(b+I) = ab+I$$

Da questo si può, poi, verificare che questo prodotto sul gruppo quoziente $(A/I, +)$ definisca, effettivamente, una struttura di anello.

Analogamente al caso dei gruppi, si definisce la proiezione al quoziente come l'omomorfismo di anelli

$$\pi_I : \begin{array}{ccc} A & \longrightarrow & A/I \\ a & \longmapsto & a+I \end{array} \tag{2.3.1}$$

Essendo un caso particolare di omomorfismo di gruppi, segue direttamente che è anche suriettivo, con $\operatorname{Ker}\pi_I = I$.

Proposizione 2.5. Sia A un anello; i suoi ideali sono tutti e soli i nuclei degli omomorfismi di anello definiti su A.

Dimostrazione. Si dimostra l'implicazione verso sinistra; sia, quindi, $\varphi : A \to B$ un omomorfismo di anelli. Si ha che $\operatorname{Ker}\varphi$ è un ideale di A perché $\operatorname{Ker}\varphi < A$, visto che φ è anche un omomorfismo di gruppi, e $\forall a \in A$, si ha $ax \in \operatorname{Ker}\varphi$, essendo che $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)\cdot 0 = 0$. Quindi i nuclei degli omomorfismi sono ideali.

Viceversa, tutti gli ideali sono i nuclei degli omomorfismi di proiezione al relativo quoziente, come visto poco sopra. □

Teorema 2.1 (I teorema di omomorfismo di anelli). Siano A, B due anelli e sia $f : A \to B$ un omomorfismo di anelli; allora esiste un unico omomorfismo di anelli φ che rispetta il diagramma[a]:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, two heads, "\pi"'] & B \\ A/\operatorname{Ker} f \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

cioè tale che $f = \varphi \circ \pi$, con φ iniettivo e $\operatorname{Im}\varphi = \operatorname{Im} f$.

Dimostrazione. Per il I teorema di omomorfismo di gruppi, visto che f è, in particolare, un omomorfismo di gruppi, si ha l'esistenza e l'unicità di

$$\varphi : {}^{A}\!/_{I} \longrightarrow B$$

con $I = \operatorname{Ker} f$. Inoltre, sempre per lo stesso motivo, si sa che tale mappa soddisfa $f = \varphi \circ \pi$ ed è iniettiva, con $\operatorname{Im} \varphi = \operatorname{Im} f$.

Rimane da verificare che φ è anche un omomorfismo di anelli; a questo proposito, si nota che:

$$\varphi\big((a+I)(b+I)\big) = \varphi(ab+I) = f(ab) = f(a)f(b) = \varphi(a+I)\varphi(b+I)$$

per ogni $a, b \in A$. □

[a] La freccia con due teste indica una suriezione, mentre la freccia tratteggiata indica che tale mappa deve esistere. In questo caso, le mappe in gioco si sottintendono essere omomorfismi di anelli.

Di seguito si riportano il II e il III teorema di omomorfismo, i quali sono diretta conseguenza del primo e si dimostrano a partire da un'opportuna scelta di un omomorfismo suriettivo. La dimostrazione e l'enunciato sono validi in maniera analoga per i gruppi, con le dovute precisazioni, cioè sostituendo gli ideali con i sottogruppi normali e i sottoanelli con i sottogruppi.

Teorema 2.2 (II teorema di omomorfismo). Siano A un anello, $I \subseteq A$ un suo ideale e sia R un suo sottoanello; allora

$$\frac{R}{R \cap I} \cong \frac{R+I}{I}$$

Dimostrazione. Si considera la proiezione $\pi : A \to A/I$, con $\pi(a) = a + I$; la sua restrizione ad R è data da $\pi|_R : R \to A/I$. Si nota che la sua immagine e il suo nucleo sono:

$$\begin{aligned} \operatorname{Im} \pi|_R &= \{r + I \mid r \in R\} = {}^{R+I}\!/_{I} \\ \operatorname{Ker} \pi|_R &= \{r \in R \mid r \in I\} = R \cap I \end{aligned}$$

da cui, per il I teorema di omomorfismo, si ha la tesi. Si nota che l'immagine della restrizione è $R + I$, che è il più piccolo sottoanello generato da R e da I, perché il quoziente R/I non è, in generale, ben definito; infatti, sarebbe necessario che I fosse un ideale di R, ma visto che si sta considerando un sottoanello generico, non è detto che $I \subseteq R$. Se così fosse, si avrebbe $R + I = R$. □

Teorema 2.3 (III teorema di omomorfismo). Sia A un anello e I, J due suoi ideali, con $I \subseteq J$; allora:

$$\frac{A/I}{J/I} \cong {}^{A}\!/_{J}$$

Dimostrazione. Si considera la proiezione $\pi : A/I \to A/J$, con $\pi(a+I) = a+J$. Intanto si nota che tale mappa è ben definita perché se $a+I = a'+I$, allora $a-a' \in I \subseteq J$, da cui $a+J = a'+J$. Inoltre, è suriettiva: $\forall a+J \in A/J$, si trova $a+I \in A/I$ tale che $\pi(a+I) = a+J$. Infine, il suo nucleo è

$$\operatorname{Ker}\pi = \{a+I \in A/I \mid a \in J\} = J/I$$

da cui, per il I teorema di omomorfismo, si ottiene la tesi. □

Lemma 2.3.1. Sia $f : A \to B$ un omomorfismo di anelli; allora valgono le due seguenti affermazioni:

(a). $\forall J \subset B$ ideale, si ha che $f^{-1}(J)$ è un ideale di A;

(b). se f è suriettiva, allora $\forall I \subset A$ ideale, si ha che $f(I)$ è un ideale di B.

Dimostrazione. Si divide la dimostrazione nei due punti.

(a). Visto che J è un ideale di B, è anche un sottogruppo di B, quindi l'immagine attraverso l'omomorfismo[a] f^{-1} sarà un sottogruppo di A. Inoltre, vale la proprietà di assorbimento perché se $x \in f^{-1}(J)$, allora $f(x) \in J$, quindi:

$$\underbrace{f(a)}_{\in B}\underbrace{f(x)}_{\in J} = f(ax) \in J, \ \forall x \in f^{-1}(J)$$

da cui $ax \in f^{-1}(J)$.

(b). Si sa che $f(I)$ è un sottogruppo di B; si verifica, allora, l'assorbimento. Per farlo, sia $b \in B$; visto che f è suriettiva, allora esiste $a \in A$ tale che $b = f(a)$ e, quindi:

$$bf(x) = f(a)f(x) = f(\underbrace{ax}_{\in I}) \in f(I)$$

□

[a] L'inversa di un omomorfismo è un omomorfismo perché se $f(ab) = f(a)f(b)$, allora $f^{-1}(f(a))f^{-1}(f(b)) = ab = f^{-1}(f(ab))$.

Teorema 2.4 (Teorema di corrispondenza tra ideali). Sia $I \subset A$ un ideale di A anello e sia π_I la proiezione al quoziente; allora π_I induce una corrispondenza biunivoca tra gli ideali dell'anello quoziente A/I e gli ideali di A che contengono I.

Dimostrazione. Siano $X = \{J \subseteq A \mid J \text{ ideale e } I \subseteq J\}$ e $Y = \{\mathcal{J} \subseteq A/I \mid \mathcal{J} \text{ ideale}\}$; la corrispondenza biunivoca è data dal teorema di corrispondenza tra gruppi. Rimane da dimostrare che, restringendo tale corrispondenza agli ideali, questa associ un ideale di A ad un ideale di A/I e viceversa.

Per il precedente lemma, si sa che, essendo π_I suriettivo, allora le immagini e le controimmagini via π_I, cioè $J \longmapsto \pi_I(J)$ e $\mathcal{J} \longmapsto \pi_I^{-1}(\mathcal{J})$, sono ideali, il che conclude la dimostrazione. □

Definizione 2.14 (Estensione e contrazione). Sia $f : A \to B$ un omomorfismo di anelli e siano $I \subset A$ e $J \subset B$ un ideale, rispettivamente, di A e di B; allora si dice *estensione* di I a B via f l'ideale generato da $f(I)$, mentre si dice *contrazione* di J ad A via f l'ideale generato da $f^{-1}(J)$.

Osservazione 2.3. Generalmente, per indicare l'estensione, ad esempio, si utilizza il l'abuso di notazione $f(I)B = IB$.

Gli omomorfismi sono *inclusioni a meno di isomrfismo*; infatti se l'omomorfismo $\varphi : R \longrightarrow R'$ non fosse iniettivo, si potrebbe passare al quoziente e trovare che $R/\operatorname{Ker}\varphi \hookrightarrow R'$. Allora si può restringere lo studio degli omomorfismi allo studio di quelli iniettivi.

Conoscendo la corrispondenza tra ideali indotta da π_I, si nota che le mappe $I \longmapsto IB$ e $J \longmapsto J \cap A$ fanno si che

$$\varphi : A \hookrightarrow B \longrightarrow B/J$$

sia tale per cui

$$\operatorname{Ker}\varphi = \{a \in A \mid \varphi(a) = a + J = J\} = \{a \in A \mid a \in J\} = J \cap A = \pi_I^{-1}(J)$$

da cui si ottiene

$$\frac{A}{J \cap A} \hookrightarrow B/J \tag{2.3.2}$$

per il I teorema di omomorfismo.

§2.4 Prodotto diretto di anelli

Definizione 2.15 (Anello prodotto). Siano A, B due anelli; il loro prodotto cartesiano $A \times B$ può essere dotato di una struttura di anello tramite le operazioni

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

con $a_1, a_2 \in A$ e $b_1, b_2 \in B$.

Teorema 2.5 (Teorema cinese del resto per anelli). Sia A un anello commutativo con unità e siano I, J due suoi ideali; allora la mappa di doppia proiezione

$$f: \begin{array}{ccc} A & \longrightarrow & A/_I \times A/_J \\ a & \longmapsto & (a+I, a+J) \end{array}$$

è un omomorfismo di anelli, con $\operatorname{Ker} f = I \cap J$. Inoltre, $I + J = A$ se e solo se f è suriettiva e, in tal caso, si ottiene

$$A/_{IJ} \cong A/_I \times A/_J$$

Dimostrazione. Si verifica intanto che f è un omomorfismo di anelli:

$$f(a+b) = \big((a+b)+I, (a+b)+J\big) = (a+I, a+J) + (b+I, b+J) = f(a) + f(b)$$

dove la terza uguaglianza è assicurata dalla struttura di anello quoziente. Analogamente:

$$f(ab) = (ab+I, ab+J) = (a+I, a+J)(b+I, b+J) = f(a)f(b)$$

Ora si nota che

$$\operatorname{Ker} f = \{a \in A \mid f(a) = (a+I, a+J) = (I, J)\} = \{a \in A \mid a \in I \text{ e } a \in J\} = I \cap J$$

Ora si verifica la doppia implicazione.

- ($\Rightarrow$) Sia $I + J = A$, quindi $\exists i \in I,\ j \in J : i + j = 1$ (visto che l'identità è in $I + J$, essendo $I + J = A$); si vuole mostrare che f è suriettiva, cioè che $\forall a, b \in A,\ \exists x \in A$ tale che $f(x) = (a + I, b + J)$.

  Visto che $x \in A = I + J$, allora si può scrivere come $x = bi + aj$, per qualche $i \in I$ e $j \in J$, quindi:

  $$f(x) = (\underbrace{bi}_{\in I} + aj + I, bi + \underbrace{aj}_{\in J} + j) = (aj + I, bi + J)$$

  Notando, poi, che $1 = i + j \Leftarrow i = 1 - j$ e $j = 1 - i$, si ha:

  $$(aj + I, bi + J) = (a(1-i) + I, b(1-j) + J) = (a + I, b_J)$$

  pertanto f è suriettiva.

- ($\Leftarrow$) Si assume, ora, che f sia suriettiva e si mostra che $I + J = A$. Dalla suriettività, si ricava che $\exists i \in A : f(i) = (I, 1 + J)$; per tale i, allora, deve valere $i \in I$ e $i \equiv 1 \pmod{J}$, perciò $i = 1 + j$, il che implica che $1 \in I + J$ e, quindi, $I + J = A$,

Per il I teorema di omomorfismo, infine, si ha che, se f è suriettiva (ed equivalentemente $I + J = A$), allora:

$$A/_{\operatorname{Ker} f} = A/_{I \cap J} = A/_{IJ} \cong A/_{I} \times A/_{J}$$

dove la seconda uguaglianza è giustificata dal fatto che $I+J = A \implies IJ = I \cap J$. $\square$

Osservazione 2.4. Per il teorema cinese del resto fra gruppi, si sapeva già che

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \iff (m, n) = 1$$

Ora, usando il teorema cinese del resto tra anelli, si sa che, data $f : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, con $\operatorname{Ker} f = m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$, vale

$$\mathbb{Z}/[m, n]\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Si è visto che f è suriettiva se e solo se $(m, n) = 1$; in questo modo, $[m, n] = mn$, quindi $n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z} = \mathbb{Z}$ e, pertanto:

$$\mathbb{Z}/[m, n]\mathbb{Z} = \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Questa versione del teorema cinese del resto, quindi, generalizza la precedente.

§2.5 Ideali primi e massimali

Definizione 2.16 (Maggiorante). Sia $(\mathcal{F}, \leq)$ un insieme parzialmente ordinato e sia $X \subset \mathcal{F}$ un suo sottoinsieme; allora si dice che $M \in \mathcal{F}$ è un *maggiorante* per X se $\forall A \in X,\ A \leq M$.

Definizione 2.17 (Elemento massimale). Sia $(\mathcal{F}, \leq)$ un insieme parzialmente ordinato; si dice che $A \in \mathcal{F}$ è un *elemento massimale* per $\mathcal{F}$ se $\forall B \in \mathcal{F} : A \leq B \implies A = B$.

Definizione 2.18 (Massimo). Sia $(\mathcal{F}, \leq)$ un insieme parzialmente ordinato; si dice che $A \in \mathcal{F}$ è un *massimo* per $\mathcal{F}$ se $\forall B \in \mathcal{F}$, si ha $B \leq A$.

Definizione 2.19 (Catena). Sia $(\mathcal{F}, \leq)$ un insieme parzialmente ordinato; una *catena* di $\mathcal{F}$ è un suo sottoinsieme totalmente ordinato.

Definizione 2.20 (Insieme induttivo). Sia $(\mathcal{F}, \leq)$ un insieme parzialmente ordinato; allora si dice che $\mathcal{F}$ è *induttivo* se ogni sua catena ammette maggiorante al suo interno.

Lemma 2.5.1 (Lemma di Zorn). Sia $(\mathcal{F}, \leq)$ un insieme parzialmente ordinato e induttivo; allora $\mathcal{F}$ contiene elementi massimali.

Spesso, il lemma di Zorn si usa su famiglie $\mathcal{F}$ di ideali ordinati secondo la relazione di inclusione $\subseteq$.

Definizione 2.21 (Ideale primo). Sia $I \subsetneq A$ un ideale di A anello; I si dice *primo* se:

$$xy \in I \implies x \in I \text{ oppure } y \in I, \ \forall x, y \in A$$

cioè se ogni volta che contiene un prodotto, allora contiene uno dei due fattori.

Definizione 2.22 (Ideale massimale). Sia A un anello e I un suo ideale; si dice che I è *massimale* se è un elemento massimale della famiglia $\mathcal{F}$ di tutti gli ideali propri di A, cioè

$$I \text{ massimale} \iff \forall J \subsetneq A : I \subseteq J \implies I = J$$

Proposizione 2.6. Ogni anello unitario ammette ideali massimali.

Dimostrazione. Sia $\mathcal{F} = \{I \subsetneq A \mid I \text{ ideale}\}$; si ha che $(\mathcal{F}, \subseteq)$ è un insieme parzialmente ordinato e induttivo. Sia, poi, $\mathcal{C} = \{I_\lambda, \ \lambda \in \Lambda\}$ una catena di $\mathcal{F}$; si nota che

$$I = \bigcup_{\lambda \in \Lambda} I_\lambda$$

è un maggiorante per $\mathcal{C}$ ed è un ideale di A, visto che gli ideali si contengono e, il fatto che $1 \notin A \Leftarrow I \neq A$, essendo che $1 \notin I_\lambda, \ \forall \lambda \in \Lambda$. Ne segue che $I \in \mathcal{F}$ implica che $\mathcal{F}$ è induttivo e, per il lemma di Zorn, ammette elementi massimali. $\square$

Esempio 2.1. Gli ideali primi di $\mathbb{Z}$ sono quelli della forma $\langle p \rangle$, con p primo; infatti:

$$xy \in \langle p \rangle \iff p \mid xy \iff p \mid x \text{ oppure } p \mid y$$

ossia se $x \in \langle p \rangle$, oppure se $y \in \langle p \rangle$.

Considerando, invece, $\langle m \rangle$ con m non primo, allora si può scrivere $m = ab$, dove $a, b \in \mathbb{Z}$ sono tali che $1 < a, b < m$, e, quindi, $ab \in \langle m \rangle$, ma $a \notin \langle m \rangle$ e $b \notin \langle m \rangle$, per cui $\langle m \rangle$ non è primo.

Proposizione 2.7 (Proprietà degli ideali massimali). Sia A un anello; allora:

(a). ogni ideale proprio di A è contenuto in un ideale massimale;

(b). ogni elemento non invertibile di A è contenuto in un ideale massimale.

Dimostrazione. Si divide la dimostrazione nei due punti.

(a). Sia $I \subsetneq A$ un ideale proprio e sia $\mathcal{F}$ la famiglia di tutti gli ideali propri che lo contengono:

$$\mathcal{F} = \{J \subsetneq A \mid I \subseteq J\}$$

Si nota che, essendo $I \in \mathcal{F}$, implica che $\mathcal{F} \neq \varnothing$; inoltre, $(\mathcal{F}, \subseteq)$ è induttivo, infatti, data $\mathcal{C}$ una catena, questa sarà un sottoinsieme totalmente ordinato di $\mathcal{F}$ della forma $\mathcal{C} = \{J_n\} \subseteq \mathcal{F}$, dove ciascun J_n è contenuto nell'altro a catena. Allora, preso $J = \bigcup J_n \in \mathcal{F}$[a], si verifica che è un maggiorante (in realtà si vedrà che è un massimo). Per farlo, si notano i due seguenti punti.

- $\forall J_n \in \mathcal{C}$ si ha $J_n \subseteq J$ per definizione di J.
- Si ha $J \in \mathcal{F}$ perché $I \subset J_n \subset J$, $\forall J_n \in \mathcal{F}$ e, infine, J è un ideale proprio; infatti, se per assurdo si avesse $1 \in J = \bigcup J_n$, allora esiste un certo n per cui $1 \in J_n \subsetneq A$, che è assurdo.

Quindi $\mathcal{F}$ è induttivo e, per il lemma di Zorn, ammette almeno un elemento massimale M. Rimane da verificare che tale elemento massimale M sia un ideale massimale dell'anello, visto che al momento, si è dimostrato che è massimale per la famiglia degli ideali che ne contengono uno proprio, che non è ovviamente la famiglia di tutti gli ideali propri di A. Questo, però, segue direttamente osservando che, per $L \subsetneq A$ ideale proprio con $M \subseteq L$, si ha $I \subseteq M \subseteq L \implies L \in \mathcal{F}$ e, quindi, per massimalità di M, si ha $L = M$.

(b). Segue direttamente dal punto precedente. Sia, infatti, $x \in A \setminus A^*$; allora l'ideale generato da $\langle x \rangle$ è proprio (prop. 2.4) e, quindi, vale il punto (a): $\langle x \rangle \subseteq M \implies x \in M$, con M ideale massimale di A.

□

[a] In realtà, andrebbe dimostrato che l'unione di ideali a catena, proprio come nel caso dei sottogruppi, è ancora un ideale.

Proposizione 2.8 (Caratterizzazione degli ideali primi e massimali). Sia A un anello e $I \subsetneq A$ un suo ideale proprio; allora valgono i seguenti punti.

(a). I è primo se e solo se A/I è un dominio.

(b). I è massimale se e solo se A/I è un campo.

(c). A è un dominio se e solo se $\langle 0 \rangle$ è un ideale primo.

(d). A è un campo se e solo se $\langle 0 \rangle$ è un ideale massimale.

(e). I massimale $\implies$ I primo.

Dimostrazione. Si divide la dimostrazione nei vari punti.

(a). Siano $x, y \in A$; per definizione, si ha che I è primo se e solo se $xy \in I \Rightarrow x \in I$, oppure $y \in I$. D'altra parte, A/I è un dominio se e solo se

$$(x+I)(y+I) = xy + I = I \iff xy \in I \implies x \in I \text{ oppure } y \in I$$

Questo è equivalente a richiedere che, quando un prodotto di elementi si annulla (cioè appartiene alla classe laterale neutra, in questo caso), allora uno dei due elementi è già nella classe laterale neutra del quoziente, il che equivale a richiedere che I è primo.

(b). Per il secondo punto della prop. 2.4, si ha che A/I è un campo se e solo se i suoi unici ideali sono impropri, cioè $\overline{\langle 0 \rangle}$, oppure A/I; per il teorema di corrispondenza, allora, questo è equivalente a richiedere che gli ideali di A che contengono I sono soltanto A e I stesso, pertanto I è un ideale massimale di A.

(c). Per il punto (a) appena mostrato, si sa che $\langle 0 \rangle$ è primo se e solo se $A/\langle 0 \rangle$ è un dominio, ma $A/\langle 0 \rangle \cong A$, quindi A è un dominio.

(d). Per il punto (b) appena mostrato, si sa che $\langle 0 \rangle$ è massimale se e solo se $A/\langle 0 \rangle$ è un campo, ma $A/\langle 0 \rangle \cong A$, pertanto A è un campo.

(e). Per il punto (b) appena mostrato, I è massimale se e solo se A/I è un campo; in particolare, questo significa che A/I è un dominio, ma per il punto (a) appena mostrato, ciò equivale a dire che I è primo.

□

Esempio 2.2. Si nota che $\langle 0 \rangle$ è un ideale primo in $\mathbb{Z}$, visto che $xy \in \langle 0 \rangle \iff xy = 0 \implies x \in \langle 0 \rangle$, oppure $y \in \langle 0 \rangle$, ma non è massimale perché $\langle 0 \rangle \subset \langle m \rangle,\ \forall m \in \mathbb{Z}$.

Proposizione 2.9. La biezione tra ideali $\pi_I : A \to A/I$ conserva ideali primi e massimali (che contengono I).

Dimostrazione. Si nota, intanto, che $I \subseteq J \subseteq A$ per assunzione, e $J \longmapsto \pi_I(J) = J/I$. Si deve mostrare che J è primo (massimale) in A se e solo se J/I è primo (massimale) in A/I. Per quanto visto nella prop. 2.8, richiederer che J sia primo è equivalente a richiedere che A/J sia un dominio (campo) e, analogamente, deve risultare che $\frac{A/I}{J/I}$ è un dominio (campo). Per il II teorema di omomorfismo, però, si ha che

$$\frac{A/I}{J/I} \cong A\big/_J$$

da cui segue la tesi. □

§2.6 Anello delle frazioni di un dominio

Definizione 2.23 (Parte moltiplicativa). Sia A un anello (commutativo con identità) che sia anche un dominio e sia $S \subset A$ tale che:

(a). $0 \notin S$;

(b). $1 \in S$;

(c). S è chiuso sotto moltiplicazione, cioè $xy \in S,\ \forall x, y \in S$.

Allora il sottoinsieme S si dice *parte moltiplicativa* di A.

Definizione 2.24 (Insieme delle frazioni di un dominio). Sia A un anello[a] e che sia un dominio. Sia S la sua parte moltiplicativa; allora, si definisce il suo *insieme delle frazioni* come

$$S^{-1}A = \left\{ \frac{a}{s} \;\middle|\; a \in A,\ s \in S \right\}\Big/_{\sim} \cong A \times S\big/_{\sim}$$

dove la relazione di equivalenza è data da $a/s \sim b/t \iff at = bs$.

[a] È ancora richiesto, per questa trattazione, che sia commutativo con identità.

Proposizione 2.10. L'insieme delle frazioni di un dominio, munito con le operazioni

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

è un anello commutativo con identità (quest'ultima corrispondente a $1/1$).

Dimostrazione. Si mostra che le operazioni sono ben definite, avendole definite tra classi di equivalenza. Siano, allora $a/s \sim a'/s'$ e $b/t \sim b'/t'$; si mostra che prodotto e somma di queste restituiscano lo stesso.

Per la somma, si ha:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \qquad \frac{a'}{s'} + \frac{b'}{t'} = \frac{a't' + b's'}{s't'}$$

Per ipotesi, si ha $as' = a's$ e $bt' = b't$; allora si vede che l'uguaglianza tra le due somme è vera se e solo se

$$\begin{aligned} &(at + bs)s't' = (a't' + b's')st \\ &\Rightarrow att's' + bss't' = a'stt' + b'tss' = (a't' + b's')st \end{aligned}$$

Quindi la somma è ben definita. In maniera analoga, si verifica il prodotto.

Inoltre, si nota che somma e prodotto di due frazioni restituiscono ancora un elemento della forma a/s, visto che il numeratore è il prodotto o la somma di due elementi di A, mentre il denominatore è sempre il prodotto di elementi di S, il quale è chiuso rispetto alla moltiplicazione.

Rimane da verificare che sono soddisfatti gli assiomi di anello. □

Esempio 2.3 (Anello delle frazioni di $\mathbb{Z}$). Si prende $A = \mathbb{Z}$ e $S = \left\{10^k\right\}_{k\geq 0}$ (si verifica ad occhio che S rispetta le proprietà richieste). L'anello delle frazioni, allora, è dato da:

$$S^{-1}A = \left\{ \frac{z}{10^k} \,\middle|\, z \in \mathbb{Z},\ k \geq 0 \right\}$$

dove, per esempio, $\frac{5}{10} \sim \frac{1}{2} \in S^{-1}A$. Inoltre, si può osservare che $\frac{2}{1} \in S^{-1}$ ed è invertibile:

$$\frac{2}{1} \cdot \frac{5}{10} = \frac{1}{1}$$

Proposizione 2.11. Sia A un dominio e $S^{-1}A$ il suo anello delle frazioni; l'applicazione

$$f : \begin{array}{ccc} A & \longrightarrow & S^{-1}A \\ a & \longmapsto & a/1 \end{array}$$

è un omomorfismo iniettivo di anelli.

Dimostrazione. Si inizia col mostrare che f è un omomorfismo:

$$\begin{matrix} f(a+b) = \dfrac{a+b}{1} = \dfrac{a}{1} + \dfrac{b}{1} = f(a) + f(b) \\ f(ab) = \dfrac{ab}{1} = \dfrac{a}{1} \cdot \dfrac{b}{1} = f(a)f(b) \end{matrix} \quad , \quad \forall a, b \in A$$

Inoltre, è iniettiva perché:

$$\operatorname{Ker} f = \left\{ a \in A \;\middle|\; f(a) = \frac{a}{1} = \frac{0}{1} \right\} = \{a \in A \mid a \cdot 1 = 0 \cdot 1 = 0\} = \{0\}$$

quindi f è iniettiva. □

Osservazione 2.5. Quanto appena dimostrato implica che $A \hookrightarrow S^{-1}A$, cioè $A \subset S^{-1}A$, quindi che l'anello delle frazioni è un'estensione di A.

Osservazione 2.6. Si nota, inoltre, che se A è un dominio, allora $S = A \setminus \{0\}$ è una parte moltiplicativa perché $\forall x, y \in S$, cioè $x, y \neq 0$, si ha ancora $xy \in S$, ovvero $xy \neq 0$.

Proposizione 2.12. Sia A un dominio e $S = A \setminus \{0\}$ la sua parte moltiplicativa; allora l'anello delle frazioni $S^{-1}A = Q(A)$ è il più piccolo campo contenente A.

Dimostrazione. Si verifica intanto che $Q(A)$ è un campo, per cui è sufficiente mostrare che esistono gli inverso moltiplicativi, cosa che segue direttamente dal fatto che, $\forall a \in A \setminus \{0\}$, si ha $1/a \in Q(A)$; in questo modo, ciascun elemento di $A \setminus \{0\}$ si puỳ scrivere come $1/a$ e, quindi:

$$\frac{a}{1} \cdot \frac{1}{a} = \frac{1}{1}$$

Per dimostrare che è il più piccolo campo contenente A, si ricorda la proposizione precedente (2.11); questa permette di concludere già che $A \subset S^{-1}A$ e, dal punto precedente, si sa che $S^{-1}A$ è un campo. Quindi rimane da mostrare solo che è il più piccolo.

Per farlo, sia K un campo tale che $A \subset K$; allora $1/a \in K$, $\forall a \in A \setminus \{0\}$, quindi K contiene tutti gli elementi della forma b/a di $S^{-1}A$, con $b \in A$ e $a \in A \setminus \{0\}$, da cui $S^{-1}A \subset K$. Questo implica la tesi. □

Esempio 2.4. Si considerano alcuni esempio di anelli delle frazioni.

- Se $A = \mathbb{Z}$, $S_1 = \left\{10^k\right\}_{k \geq 0}$ e $S_0 = A \setminus \{0\}$, allora:

$$\mathbb{Z} \subset S_1^{-1}\mathbb{Z} \subset S_0^{-1}\mathbb{Z} = Q(\mathbb{Z}) = \mathbb{Q}$$

- Se $A = K[x]$, allora:

$$Q(A) = K(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ g(x) \neq 0 \right\}$$

Definizione 2.25 (Localizzato). Dato un dominio A e $P \subset A$ un suo ideale primo, si può considerare $S = A \setminus P$, che è una parte moltiplicativa perché $0 \notin S$, $1 \in S$ e $\forall x, y \in S$, vale $x, y \notin P \implies xy \notin P$, visto che P primo implica che se non contiene due elementi, non ne contiene neanche il prodotto (per controposizione), quindi il prodotto è nel complementare: $xy \in A \setminus P = S$. In questo caso, si usa la notazione $S^{-1}A = A_p$ e si dice *localizzato* di A a P.

Osservazione 2.7. Il localizzato A_p è anche un **anello locale**, cioè un anello che ha un unico ideale massimale.

Esempio 2.5. Sia $A = \mathbb{Z}$ e $P = 2\mathbb{Z}$; allora la parte moltiplicativa $S = \mathbb{Z} \setminus 2\mathbb{Z}$ (i numeri dispari) permette di definire

$$S^{-1}\mathbb{Z} = \mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \equiv 1 \pmod 2 \right\}$$

Esercizio 2.1. Dati $A = \mathbb{Z}$ e $P = 2\mathbb{Z}$, con $S = \mathbb{Z} \setminus 2\mathbb{Z}$, verificare che $\langle 2 \rangle \mathbb{Z}_{(2)}$ è l'unico ideale massimale di $\mathbb{Z}_{(2)}$.

Svolgimento. La tesi è equivalente a richiedere che $\mathbb{Z}^*_{(2)} = \mathbb{Z}_{(2)} \setminus \langle 2 \rangle \mathbb{Z}_{(2)}$; infatti, si sa già che $\langle 2 \rangle \mathbb{Z}_{(2)}$ è un ideale, mentre ciascun ideale non in esso contenuto deve contenere un elemento invertibile, quindi è improprio.

Se $a/b \notin \langle 2 \rangle \mathbb{Z}_{(2)}$, allora sia a che b sono dispari, per cui $b/a \in \mathbb{Z}_{(2)}$, che è evidentemente l'inverso di a/b. Viceversa, se a/b è invertibile, allora esiste $\frac{c}{d} \in \mathbb{Z}_(2)$ tale che $ac/(bd) = 1 \Rightarrow ac = bd$; se uno tra a e c fosse pari, allora lo sarebbe anche bd e, visto che 2 è primo, uno tra b e d sarebbe pari, contraddicendo la definizione di $\mathbb{Z}_{(2)}$. Allora, $a/b \in \mathbb{Z}_{(2)} \setminus \langle 2 \rangle \mathbb{Z}_{(2)}$. ■

Elementi invertibili di $\mathbf{S^{-1}A}$. Si nota che gli invertibili di $S^{-1}A$ sono dati da:

$$(S^{-1}A)^* = \left\{ \frac{a}{s} \;\middle|\; \frac{s}{a} \in S^{-1}A \right\}$$

cioè esistono $b \in A$ e $t \in S$ tali che $st = ab \in S$; visto che non è assicurato $a \in S$, cosa che è sempre vera nel campo dei quozienti, si richiede che almeno un suo multiplo stia in S. Ne segue che

$$(S^{-1}A)^* = \left\{ \frac{a}{s} \;\middle|\; \exists b \in A : ab \in S \right\}$$

Esempio 2.6. Se $A = \mathbb{Z}$ e $S = \left\{10^k\right\}_{k \geq 0}$, allora

$$\frac{5}{10} = \frac{1}{2} \in (S^{-1}A)^*$$

ma $2 \notin S$, quindi $2 \in (S^{-1}A)^*$, visto che il suo inverso ha una scrittura che rispetta la proprietà richiesta dall'insieme.

Ideali di $\mathbf{S^{-1}A}$. Sia $I \subset A$ un ideale di A; si può costruire l'insieme

$$S^{-1}I = \left\{ \frac{x}{s} \in S^{-1}A \;\middle|\; x \in I,\ s \in S \right\}\Big/\sim \;\cong I \times S\big/\sim \tag{2.6.1}$$

Per questo oggetto valgono le seguenti proprietà.

Proposizione 2.13. Sia $I \subset A$ un ideale e sia $S^{-1}A$ l'anello delle frazioni di A; allora:

(a). $S^{-1}I$ è un ideale di $S^{-1}A$;

(b). $\forall J \subset S^{-1}A,\ \exists I \subset A$ tale che $J = S^{-1}I$;

(c). $S^{-1}I$ è un ideale proprio di $S^{-1}A$ se e solo se $I \cap S = \varnothing$;

(d). dato P ideale primo di A, con $P \cap S = \varnothing$, allora $S^{-1}P$ è un ideale primo di $S^{-1}A$.

Dimostrazione. Si divide la dimostrazione nei vari punti.

(a). Si dimostra la chiusura rispetto alla somma:

$$\frac{x}{s} + \frac{y}{t} = \frac{\overbrace{xt + ys}^{\in I}}{\underbrace{st}_{\in S}} \in S^{-1}I,\ \forall x, y \in I$$

visto che x, y sono elementi di un ideale. Per l'assorbimento, invece:

$$\frac{a}{s} \cdot \frac{x}{t} = \frac{\overbrace{ax}^{\in I}}{\underbrace{st}_{\in S}} \in S^{-1}I,\ \forall \frac{a}{s} \in S^{-1}A$$

(b). Sia $J \subset S^{-1}A$ un ideale; per quanto affermato dalla prop. 2.11, si sa che $S^{-1}A$ è un'estensione di A. Inoltre, considerando $f^{-1}(J)$, si sa che questo è un ideale e, in particolare, è una contrazione di J ad A; quindi:

$$f^{-1}(J) = J \cap A = I \subset A$$

Ora si vuole mostrare che $J = S^{-1}I$. Si nota che $\forall x \in I$, vale $f(X) = x/1 \in J$, quindi:

$$\underbrace{\frac{1}{s}}_{\in S^{-1}A} \cdot \frac{x}{1} = \frac{x}{s} \in J \implies S^{-1}I \subseteq J$$

per la proprietà di assorbimento di J. Viceversa, si ha, $\forall x/s \in J$:

$$\frac{x}{1} = \frac{x}{s} \cdot \frac{s}{1} \in J \implies x = f^{-1}\left(\frac{x}{1}\right) \in I$$

cioè il numeratore di ogni elemento di J è un elemento di I. Allora, considerando $S^{-1}I$, questo contiene tutte le frazioni di J, per cui $x/s \in S^{-1}J \implies J \subseteq S^{-1}I$.

(c). Si dimostra per controposizione, cioè $S^{-1}I$ non-proprio equivale a $S^{-1}I = S^{-1}A$. Visto che $S^{-1}I$ è un ideale, allora questo è vero se e solo se

$$\frac{1}{1} \in S^{-1}I \iff \exists x \in I,\ \exists s \in S : \frac{1}{1} = \frac{x}{s}$$

che, per la relazione definita sugli anelli di frazioni, equivale a richiedere che $I \supset x = s \in S \iff I \cap S \neq \varnothing$.

(d). Sia P un ideale primo; se fosse $P \cap S \neq \varnothing$, allora, per il punto (c), non sarebbe proprio (quindi neanche primo). Viceversa, se $P \cap S = \varnothing$, si dimostra che $S^{-1}P$ è primo in $S^{-1}A$; a questo proposito, si considera che

$$\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}P$$

che è equivalente a dire che $\exists \sigma \in S,\ \exists p \in P$ tali che:

$$\frac{ab}{st} = \frac{p}{\sigma} \iff ab\sigma = pstt \in P \implies ab\sigma \in P$$

visto che $p \in P$. Visto che, per ipotesi, $\sigma \in S$ e $P \cap S = \varnothing$, allora $ab \in P$. Visto anche che P è primo, si deve avere $a \in P$, o $b \in P$, quindi la frazione di uno dei due deve appartenere a $S^{-1}P$, cioè $a/s \in S^{-1}P$, oppure $b/t \in S^{-1}P$, quindi $S^{-1}P$ è primo.

□

§2.7 Divisibilità nei domini

Definizione 2.26 (Divisibilità). Sia A un dominio e siano $a, b \in A$, con $a \neq 0$; si dice che a *divide* b se $\exists c \in A$ tale che $b = ac$.

Osservazione 2.8. Si nota che $a \mid b \iff \langle b \rangle \subseteq \langle a \rangle$, infatti:

$$a \mid b \iff \exists c \in A : b = ac \iff b \in \langle a \rangle \iff \langle b \rangle \subseteq \langle a \rangle$$

Definizione 2.27 (Elementi associati). Sia A un dominio e siano $a, a' \in A$ due suoi elementi; si dice che a e a' sono *associati*, scrivendo $a \sim a'$, se vale una delle seguenti tre condizioni:

(a). $a \mid a'$ e $a' \mid a$;

(b). $\exists u \in A^*$ tale che $a = ua'$;

(c). $\langle a \rangle = \langle a' \rangle$.

Si dimostra, ora, che le tre proprietà che definisco l'associatività tra elementi di un dominio sono equivalenti.

Dimostrazione. Si divide la dimostrazione nelle tre implicazioni.

- (a⇔c) Si ha:

$$a \mid a' \iff \langle a' \rangle \subseteq \langle a \rangle \quad \text{e} \quad a' \mid a \iff \langle a \rangle \subseteq \langle a' \rangle$$

  Quindi $a \mid a'$ e $a' \mid a$ se e solo se $\langle a \rangle = \langle a' \rangle$.

- (a⇒b) Se $a \mid a'$ e $a' \mid a$ al contempo, allora:

$$a' = xa \quad \text{e} \quad a = ya' \implies a = yxa \implies a(1 - xy) = 0$$

  Visto che A è un dominio e $a \in A$ con $a \neq 0$, allora $xy = 1$, quindi $y \in A^*$, che coincide con il punto (b).

- (b⇒c) Si assume che $\exists u \in A^*$ tale che $a = ua'$, quindi $a \in \langle a' \rangle$ e, allora, $\langle a' \rangle \subseteq \langle a \rangle$. Visto che $u \in A^*$, allora $\exists v \in A^*$ tale che $uv = 1$, per cui $a' = va$ e $\langle a \rangle \subseteq \langle a' \rangle$. Questo permette di concludere che $\langle a \rangle = \langle a' \rangle$.

$\square$

Definizione 2.28 (Massimo comune divisore). Siano $a, b \in A$ dominio non entrambi nulli; si dice che $d \in A$ è un *massimo comune divisore* per a e b se valgono entrambe le seguenti condizioni:

(a). $d \mid a$ e $d \mid b$;

(b). $\forall x \in A$ tale che $x \mid a$ e $x \mid b$, vale $x \mid d$.

Proposizione 2.14. Due elementi $d, d' \in A$ dominio sono due massimi comuni divisori di una stessa coppia di elementi $a, b \in A$ se e solo se sono associati ($d \sim d'$).

Dimostrazione. Se d e d' sono due massimi comuni divisori di a e b, allora:

$$\begin{gathered} d \mid a,\ d \mid b \quad \text{e} \quad x \mid a,\ x \mid b \implies x \mid d \\ d' \mid a,\ d' \mid b \quad \text{e} \quad x \mid a,\ x \mid b \implies x \mid d' \end{gathered}$$

quindi sono associati per definizione. Per il viceversa, basta notare che se $d \sim d'$, allora dividono e sono divisi dagli stessi elementi. □

Definizione 2.29 (Elemento primo). Sia A un dominio e $x \in A$, con $x \notin A^* \cup \{0\}$; allora x è detto *primo* se, $\forall a, b \in A$, vale $x \mid ab \implies x \mid a$ oppure $x \mid b$.

Definizione 2.30 (Elemento irriducibile). Sia A un dominio e $x \in A$, con $x \notin A^* \cup \{0\}$; allora x si dice *irriducibile* se, $\forall a, b \in A$, vale $x = ab \implies a \in A^*$ oppure $b \in A^*$.

Proposizione 2.15. Sia A un dominio; se $x \in A$ è primo, allora è irriducibile.

Dimostrazione. Si assume che $x = ab$; essendo primo per assunzione, allora $x \mid a$, oppure $x \mid b$. Senza perdita di generalità, si assume che $x \mid a$, perciò:

$$a = xc \implies x = bcx \implies x(1 - bc) = 0$$

Visto che A è un dominio e $x \neq 0$ per ipotesi, allora deve valere $bc = 1$, quindi $b, c \in A^*$. In particolare, questo implica che x è irriducibile perché, scrivendolo come $x = ab$, si è verificato che $b \in A^*$. □

Proposizione 2.16. Sia A un dominio; allora valgono i seguenti punti:

(a). x è primo se e solo se $\langle x \rangle$ è un ideale primo non nullo;

(b). x è irriducibile se e solo se $\langle x \rangle$ è un ideale massimale nell'insieme degli ideali principali.

Dimostrazione. Si divide la dimostrazione nei due punti.

(a). Sia $\langle x \rangle$ un ideale primo, cioè:

$$ab \in \langle x \rangle \iff a \in \langle x \rangle \text{ oppure } b \in \langle x \rangle$$

che equivale a richiedere $x \mid a$, oppure $x \mid b$, cioè x primo in A.

(b). Si dimostrano separatamente le due implicazioni. Per iniziare, si assume che x sia irriducibile e che $\langle x \rangle \subseteq \langle y \rangle \subsetneq A$, quindi $\exists z \in A$ tale che $x = yz$. Inoltre, deve valere $y \notin A^*$, altrimenti si avrebbe $\langle y \rangle = A$ e, visto che x è irriducibile, si deve necessariamente avere $z \in A^*$, quindi $x \sim y$, ossia $\langle x \rangle = \langle y \rangle$. Questo significa che $\langle x \rangle$ è massimale tra gli ideali principali.

Per il viceversa, si dimostra la contropositiva: sia x riducibile, quindi $x = yz$ con $y, z \notin A^*$; per quanto detto, si a $\langle x \rangle \subsetneq \langle y \rangle \subsetneq A$, dove la seconda inclusione non può essere un'uguaglianza per il fatto che $y \notin A^*$, per cui $1 \notin \langle y \rangle$, mentre la prima è data dal fatto che $z \notin A^*$ (quindi x e y non sono associati), da cui $\langle x \rangle$ non è massimale tra gli ideali principali.

□

Esempio 2.7. Se x è primo in nel dominio $A = K[x, y]$, allora $A/\langle x \rangle \cong K[y]$, che si sa essere un dominio; per la prop. 2.8, segue che $\langle x \rangle$ è primo.

Visto che x è primo, allora è anche irriducibile, quindi $\langle x \rangle$ è massimale tra gli ideali principali di A, ma non è un ideale massimale di A perché $K[y]$ non è un campo. Infatti, si verifica che $\langle x \rangle \subsetneq \langle x, y \rangle \subsetneq A$, cioè $\langle x \rangle$ non è massimale, in quanto è contenuto nell'ideale proprio $\langle x, y \rangle$.

§2.8 Domini euclidei e PID

Definizione 2.31 (Dominio euclideo). Un dominio A è detto *dominio euclideo* se esiste una mappa

$$d : A \setminus \{0\} \longrightarrow \mathbb{N}$$

detta *grado*, che soddisfa le seguenti proprietà:

(a). $d(x) \leq d(xy), \ \forall x, y \in A \setminus \{0\}$;

(b). $\forall x \in A, \ \forall y \in A \setminus \{0\}$, si trovano $q, r \in A$ tali che $x = yq + r$, con $d(r) < d(y)$ oppure $r = 0$.

Esempio 2.8. Oltre agli interi con il valore assoluto e ai polinomi su un campo K con il grado, un altro esempio di dominio euclideo sono gli interi di Gauss $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ con la norma data da

$$N : \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ \alpha = a + ib & \longmapsto & N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 \end{array}$$

Proposizione 2.17 (Algoritmo di Euclide). Sia A un dominio; allora $\forall a, b \in A$, non entrambi nulli, esiste il loro massimo comune divisore, ottenuto tramite l'algoritmo di Euclide.

Dimostrazione. Visto che è definita una funzione grado come generalizzazione del modulo per gli interi, l'esistenza dell'algoritmo di Euclide segue la stessa dimostrazione del caso degli interi, visto anche che negli anelli euclidei è, per costruzione, prevista una divisione euclidea.

L'algoritmo di Euclide termina perché la successione dei resti r_n è una successione a indici in $\mathbb{N}$ strettamente decrescente (visto che deve valere $d(r_n) < d(y_n)$ ogni volta che si fa una divisione); questo significa che ci sarà un n per cui $r_n = 0$.

Ora si dimostra l'algoritmo per induzione sul numero degli N passi richiesti a completarlo. Se l'algoritmo termina per $N = 1$ passo, si deve avere $a = qb + 0$, cioè $b \mid a$ e, pertanto, il loro massimo comune divisore è $(a, b) = b$.

Per ipotesi induttiva, si assume che l'algoritmo funzioni per ogni $m < N - 1$ e si mostra che è vero per N. Sia:

$$\begin{cases} a = q_0 b + r_1 = q r_0 + r_1 & , \ 0 \leq r_1 < |b| \\ r_0 = q_1 r_1 + r_2 & , \ 0 \leq r_2 < r_1 \\ \vdots \\ r_{n-2} = q_{n-1} r_{n-1} + r_n & , \ 0 \leq n < r_{n-1} \\ r_{n-1} = q_n r_n + 0 \end{cases}$$

Allora si può applicare l'algoritmo di Euclide per (r_0, r_1) e, in questo modo, si trova una sequenza di $N - 1$ passi, per ottenere $r_n = (b, r_1) = (b, a - q_0 b) = (a, b)$, dove l'ultima uguaglianza è giustificata dalla proprietà del massimo comune divisore. □

Proposizione 2.18. Sia A un dominio euclideo; gli elementi di A che hanno grado minimo sono tutti e soli gli elementi di A^*.

Dimostrazione. Si considera l'immagine della funzione grado dell'intero dominio eccetto lo zero: $d(A \setminus \{0\}) \subset \mathbb{N}$; per il principio del minimo, questo insieme, essendo un sottoinsieme di $\mathbb{N}$, ammette un elemento minimo d_0. Sia, allora, $x \in A \setminus \{0\}$ un elemento tale che $d(x) = d_0$, cioè un elemento di grado minimo. Si vuole dimostrare che questo è invertibile. Per farlo, si osserva che $\forall y \in A \setminus \{0\}$ si può calcolare la divisione euclidea per x:

$$y = qx + r$$

In questo caso, non può essere $d(r) < d(x) = d_0$ perché, per definizione, d_0 è il grado minimo, quindi deve essere $r = 0$ e, allora, $y = qx$. Considerando il caso particolare di $y = 1$, allora $\exists q \in A$ tale che $1 = qx$, per cui $x \in A^*$.

Viceversa, sia $x \in A^*$; allora $\langle x \rangle = A$ e, conseguentemente, $\forall a \in A$, si ha $a = qx$ per qualche $q \in A$. Visto che la funzione grado deve soddisfare $d(x) \leq d(qx)$, $\forall q \in A \setminus \{0\}$, allora x deve avere grado minimo. □

Proposizione 2.19. Sia A un dominio euclideo; allora tutti gli ideali di A sono principali (per cui ogni dominio euclideo è un PID) e sono generati da un elemento di grado minimo.

Dimostrazione. Sia $I \subset A$ un ideale; se $I = \{0\}$, allora è principale, altrimenti si mostra che I è generato da un singolo elemento di grado minimo.

Sia $x \in I$ un elemento di grado minimo (che esiste perché $d(I) \subset \mathbb{N}$), quindi $\langle x \rangle \subseteq I$. Viceversa, $\forall a \in I$, si può calcolare la divisione euclidea per x:

$$a = qx + r, \quad d(r) < d(x) \text{ oppure } r = 0$$

da cui deve valere $r = 0$ perché x è di grado minimo, quindi $a = qx \in \langle x \rangle \implies I \subseteq \langle x \rangle$. □

Definizione 2.32 (PID). Un dominio A si dice *a ideali principali* se ogni suo ideale è principale, cioè $\forall I \subseteq A$, con I ideale, $\exists x \in I$ tale che $I = \langle x \rangle$.

Proposizione 2.20. Sia A un PID; i suoi unici ideali primi sono $\langle 0 \rangle$ e gli ideali massimali.

Dimostrazione. Dal punto (c) della prop. 2.8, si sa che A dominio $\iff$ $\langle 0 \rangle$ è un ideale primo; inoltre, dal punto (e) della stessa proposizione, si sa anche che tutti gli ideali massimali di un anelo sono primi.

Viceversa, si dimostra che gli ideali diversi da $\langle 0 \rangle$ in un PID sono solo quelli massimali. Per farlo, sia P un ideale primo diverso da $\langle 0 \rangle$; essendo in un PID, vale $P = \langle x \rangle$. Per verificare che P è massimale, si nota che, essendo A un dominio, per il punto (a) della prop. 2.16, si ha che P è massimale se e solo se x è primo, quindi x irriducibile (visto che primo $\Rightarrow$ irriducibile in ogni dominio per la prop. 2.15). Ora, visto che x è irriducibile, segue che $\langle x \rangle$ è massimale tra gli ideali principali di A, visto il punto (b) della prop. 2.8. Unitamente al fatto che A è un PID (quindi tutti i suoi ideali sono principali), segue che $\langle x \rangle$ è un ideale massimale per A. $\square$

MCD nei PID. Se A è un PID e $x, y \in A$ non entrambi nulli, si osserva che l'ideale generato da x e y deve essere tale che $\langle x, y \rangle = \langle d \rangle$, dove $d = (x, y)$. Infatti, se $x \in \langle d \rangle$ e $y \in \langle d \rangle$, allora $d \mid x$ e $d \mid y$; inoltre, se $c \mid x$ e $c \mid y$, si ha $x, y \in \langle c \rangle$, quindi $\langle d \rangle = \langle x, y \rangle \subseteq \langle c \rangle$ implica che $d \in \langle c \rangle$ e, quindi, che $c \mid d$. Questo significa che d è un MCD di x e y.

§2.9 Domini a fattorizzazione unica

Definizione 2.33 (UFD). Sia A un dominio; questo si dice essere *a fattorizzazione unica* se ogni $x \in A$ tale che $x \notin A^* \cup \{0\}$ si scrive in modo unico, a meno dell'ordine di fattori e di moltiplicazione per elementi invertibili, come prodotto di elementi irriducibili.

Proposizione 2.21. Se A è un dominio a fattorizzazione unica, allora $\forall a, b \in A$ non entrambi nulli esiste il loro massimo comune divisore.

Dimostrazione. Sia d il prodotto dei fattori irriducibili comuni ad a e b presi con il minimo esponente con cui compaiono; allora, questo è un massimo comune divisore perché è possibile verificare direttamente la sua definizione. $\square$

Nei tre tipi di domini analizzati finora, si trova sempre l'MCD, ma con le opportune differenze.

- Se A è un dominio euclideo, allora si determina $d = (a, b)$ tramite l'algoritmo di Euclide e si ottengono i due coefficienti per cui è soddisfatta l'identtià di Bézout: $d = ax_0 + by_0$.

- Se A è un dominio a ideali principali, si sa che presi due elementi $a, b \in A$, deve valere $\langle a, b \rangle = \langle d \rangle$, con d MCD di a e b, ma non esiste un algoritmo che permetta di poterlo determinare. In ogni caso, esistono ancora $x_0, y_0 \in A$ tali per cui è soddisfatta la relazione $d = ax_0 + by_0$, derivante direttamente dal fatto che $d \in \langle a, b \rangle$.

- Se A è un dominio a fattorizzazione unica, infine, allora si trova $d = \gcd(a, b)$, ma non è assicurato che $\langle d \rangle = \langle a, b \rangle$, quindi non è neanche assicurato trovare $x_0, y_0 \in A$ tali che $d = ax_0 + by_0$. Questo perché mentre è effettivamente verificato che $\langle a, b \rangle \subset \langle d \rangle$, non è detto che valga anche il contenimento opposto.

Considerando, per esempio, l'UFD $\mathbb{Z}[x]$, allora l'ideale $I = \langle 2, x\rangle$ è tale per cui $\gcd(2, x) = 1$, ma $1 \notin \langle 2, x\rangle$, altrimenti si avrebbe $1 = 2a(x) + xb(x)$ che implica $1 = 2a(0) + 0b(0) \Rightarrow 1 = 2a(0)$, cioè $2 \mid 1$, che è assurdo.

Teorema 2.6 (Caratterizzazione degli UFD). Sia A un dominio; allora sono equivalenti le seguenti affermazioni.

(a). A è un UFD.

(b). Valgono le due seguenti condizioni:

- (i). ogni elemento irriducibile è primo;
- (ii). ogni catena discendente di divisibilità è stazionaria, cioè se $\{a_i\}_{i\geq 0} \subset A$, con $a_{i+1} \mid a_i$, $\forall i \geq 0$, allora $\exists n_0 \in \mathbb{N}$ tale che $a_i \sim a_{n_0}$, $\forall i \geq n_0$.

Osservazione 2.9. La condizione (i) permette di dimostrare che la fattorizzazione in primi è unica, mentre la condizione (ii) permette di dimostrare l'esistenza della fattorizzazione.

Il teorema sopra, pertanto, permette di concludere che la condizione di UFD per un dominio consiste nella validità del teorema di fattorizzazione unica.

Osservazione 2.10. La condizione (ii) può essere riformulata nel seguente modo: ogni catena ascendente di ideali principali è stazionaria, ossia considerata $\{\langle a_i\rangle\}_{i\geq 0}$ una catena ascendente di ideali di A tale che $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \ldots$, allora $\exists n_0 \in \mathbb{N}$ tale per cui $\langle a_i\rangle = \langle a_{n_0}\rangle$, $\forall i \geq n_0$.

Corollario 2.6.1. Se A è un PID, allora è anche un UFD.

Dimostrazione. Preso A un PID, si dimostra la validità dei punti (i) e (ii) del teorema precedente. Sia, quindi, $x \in A$ un suo elemento irriducibile; per quanto affermato dalla proposizione 2.20, l'ideale $\langle x\rangle$ è massimale in A, ma, dal punto (e) della prop. 2.8, si sa che $\langle x\rangle$ è primo. Inoltre, essendo in un dominio, vale il punto (a) della prop. 2.16, per cui si conclude che x è primo e, quindi, vale il punto (i).

Si considera, ora, una catena ascendente di ideali principali principali $\langle a_1\rangle \subset \langle a_2\rangle \subset \ldots$ e si prende $I = \bigcup_{i\geq 0}\langle a_i\rangle$; tale unione è ancora un ideale di A, quindi è principale e, allora, $I = \langle a\rangle$. Tale elemento a deve appartenere all'unione, quindi si troverà un a_{n_0} tale che $a \in \langle a_{n_0}\rangle$, quindi $I = \langle a\rangle \subseteq \langle a_{n_0}\rangle$. D'altra parte, I è l'unione di tutti gli ideali principali di A, quindi $\langle a_{n_0}\rangle \subseteq \langle a\rangle = I \implies I = \langle a_{n_0}\rangle$. Per definizione di I, allora, $\langle a_i\rangle \subseteq \langle a_{n_0}\rangle$, $\forall i \geq 0$, mentre il contenimento opposto (e quindi l'uguaglianza) è verificato quando $i \geq n_0$ perché si stanno considerando ideali in catena. Questo implica che $\{\langle a_i\rangle\}_{i\geq 0}$ è stazionaria e, allora, è verificato anche il punto (ii). $\square$

Osservazione 2.11. Questo corollario permette di mettere in relazione i vari tipi di domini:

$$\mathrm{ED} \subset \mathrm{PID} \subset UFD$$

Si possono trovare degli anelli che non soddisfano il punto (i), oppure il punto (ii). Come esempio di anello senza la proprietà (ii), si considera $K[\{x^{1/n}\}_{n\geq 1}]$; questa estensione non è un UFD perché la catena

$$x^{1/2^{n+1}} \mid x^{1/2^n} \mid \ldots \mid x^{1/4} \mid x^{1/2} \mid x$$

non è definitivamente stazionaria, infatti il successivo può sempre dividere il precedente. Ne segue che non esiste la fattorizzazione di x.

Ora, invece, si considera $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{-5}) \subset \mathbb{C}$. In questo anello, la proprietà (i) viene meno perché 2 è irriducibile, ma non primo[1]:

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) \implies N(2) = (a^2 + 5b^2)(c^2 + 5d^2)$$

da cui le uniche possibilità sono $a = \pm 2,\ c = \pm 1,\ b = d = 0$, quindi, effettivamente, 2 è irriducibile, ma non primo, in quanto

$$2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \qquad \text{ma} \qquad 2 \nmid (1 + \sqrt{-5}), (1 - \sqrt{-5})$$

Infatti:

$$\alpha = \frac{1 \pm \sqrt{-5}}{2} = \frac{1}{2} \pm \frac{\sqrt{-5}}{2} \notin \mathbb{Z}[\sqrt{-5}]$$

In $\mathbb{Z}[\sqrt{-5}]$, allora, si hanno due fattorizzazioni distinte per 6:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Questo dimostra che $\mathbb{Z}[\sqrt{-5}]$ non è un UFD; per questo motivo, non è neanche un PID e questo si può dimostrare notando l'ideale $(2, 1 + \sqrt{-5})$ non è principale.

§2.10 Anelli di polinomi

Dato un dominio A, si studiano gli anelli dei polinomi $A[x]$; in particolare, segue una loro caratterizzazione come UFD. Per procedere con tale caratterizzazione, sarà prima necessario introdurre altra teoria.

[1] Qui, N indica la funzione grado.

Definizione 2.34 (Contenuto di un elemento). Sia A un UFD e $f(x) \in A[x]$, con $f(x) = \sum_{i=0}^{n} a_i x^i$; si definisce *contenuto* di $f(x)$ il MCD dei suoi coefficienti:

$$c(f(x)) = \gcd(a_0, \dots, a_n)$$

Definizione 2.35 (Elemento primitivo). Sia A un UFD e $f(x) \in A[x]$; si dice che $f(x)$ è *primitivo* se $c(f(x)) \sim 1$.

Osservazione 2.12. Dato $f(x) \in A[x]$, si ha che:

$$f(x) = c(f(x))f'(x)$$

con $f'(x) \in A[x]$ tale che

$$f'(x) = \sum_{i=0}^{n} \frac{a_i}{d} x^i \qquad \frac{a_i}{d} \in A \text{ con } \gcd\left(\frac{a_0}{d}, \dots, \frac{a_n}{d}\right) = 1$$

cioè $c(f'(x)) = 1$.

Lemma 2.6.1 (Lemma di Gauss). Siano $f(x), g(x) \in A[x]$; allora

$$c\big(f(x)g(x)\big) = c(f(x))c(g(x))$$

Dimostrazione. Per dimostrare questo, si considerano due possibili scenari.

- Si ha $c(f(x)) = c(g(x)) = 1$.

  In questo caso, $f(x)$ e $g(x)$ sono primitivi; si vuole verificare che $c\big(f(x)g(x)\big) = 1$. Se $f(x)g(x)$ non fosse primitivo, allora $c\big(f(x)g(x)\big)$ non sarebbe invertibile, cioè non esisterebbe p primo tale che $p \mid c\big(f(x)g(x)\big)$. Si considera, allora, la proiezione modulo p:

  $$\pi_p : \begin{array}{ccc} A[x] & \longrightarrow & A/\langle p \rangle[x] \\ f(x) & \longmapsto & \overline{f(x)} \end{array}$$

  Visto che $p \nmid c(f(x))$, allora $\overline{f(x)} \neq 0$; analogamente $\overline{g(x)} \neq 0$. Tuttavia, si ha $\pi_p(f(x)g(x)) = \overline{f(x)g(x)} = 0$ perché si era assunto che $p \mid c(f(x)g(x))$, ma questo è assurdo perché $A/\langle p \rangle$ è un dominio (visto che $\langle p \rangle$ è un ideale primo). Allora A dominio $\implies A[x]$ dominio, da cui $A/\langle p \rangle[x]$ dominio, perciò $c(f(x)g(x)) = 1$.

- Caso generale.

Per il caso generale, si prendono $f'(x), g'(x)$ primitivi e si considerano $f(x) = c(f(x))f'(x)$ e $g(x) = c(g(x))g'(x)$. Sia

$$h(x) = f(x)g(x) = c(f(x))c(g(x))g'(x)f'(x) = c(h(x))h'(x)$$

Dalla relazione sopra, si ottiene che

$$c(h(x)) = c\big[c(h(x))h'(x)\big] = c(f(x)g(x)) = c\big[c(f(x))c(g(x))g'(x)f'(x)\big]$$

I contenuti presenti in $c(h(x))$ sono costanti, quindi possono essere portati fuori; inoltre, notando che il prodotto di polinomi primitivi è primitivo (per il punto precedente), si ha:

$$c(h(x)) = c(h(x))\underbrace{c(h'(x))}_{=1} = c(f(x))c(g(x))\underbrace{c(g'(x)f'(x))}_{=1}$$

da cui la tesi:

$$c(f(x)g(x)) = c(h(x)) = c(f(x))c(g(x))$$

□

Corollario 2.6.2. Siano $f(x), g(x) \in A[x]$, con $c(f(x)) = 1$ e $f(x) \mid g(x)$ in $K[x]$, con K campo dei quozienti di A; allora $f(x) \mid g(x)$ in $A[x]$.

Dimostrazione. Per ipotesi, si sa che $f(x) \mid g(x)$ in $K[x]$, cioè che esiste $h(x) \in K[x]$ tale per cui $g(x) = f(x)h(x)$; quindi $\exists d \in A$ tale che:

$$h_1(x) = dh(x) \in A[x]$$

Quello che si sta facendo è cancellare il denominatore per portare la relazione data dalla divisione da $K[x]$ a $A[x]$. Ne segue che:

$$dg(x) = f(x)h_1(x) \in A[x]$$

Applicando il lemma di Gauss, si ha:

$$dc(g(x)) = c(f(x)h_1(x)) = c(f(x))c(h_1(x)) = c(h_1(x)) \implies d \mid c(h_1(x))$$

dove si è usato il fatto che $c(f(x)) = 1$. Per quanto appena visto, si conclude che $h_1(x)/d = h(x) \in A[x]$, quindi la divisibilità assunta inizialmente è valida anche in $A[x]$. □

Corollario 2.6.3. Sia $f(x) \in A[x]$ e $f(x) = g(x)h(x)$ in $K[x]$ (con K campo dei quozienti di A), dove $\deg g(x), \deg h(x) \geq 1$ (cioè f è riducibile in $K[x]$); allora $\exists \delta \in K^*$ tale che $g_1(x) = \delta g(x) \in A[x]$ e $h_1(x) = \delta^{-1}h(x) \in A[x]$, per cui $f(x) = g_1(x)h_1(x)$ in $A[x]$.

Dimostrazione. Analogamente al corollario precedente, si sa che $\exists d \in A$ tale che $g_1(x) = dg(x) \in A[x]$, quindi:

$$f(x) = dg(x)d^{-1}h(x) = d_1(x)\left(d^{-1}h(x)\right) = c(g_1(x))g_1'(x)(d^{-1}h(x))$$

con $g_1'(x) \in A[x]$ primitivo. Inoltre, si ha:

$$f(x) = g_1'(x)\underbrace{\left(c(g_1(x))d^{-1}h(x)\right)}_{\in K[x]}$$

cioè $g_1'(x) \mid g(x)$ in $K[x]$. Per il corollario precedente, allora, si ha che $g_1'(x) \mid f(x)$ anche in $A[x]$, per cui

$$h_1(x) = \underbrace{\frac{c(g_1(x))}{d}}_{=\delta^{-1}} h(x)$$

da cui segue la tesi. □

Teorema 2.7. Sia A un UFD; gli elementi irriducibili di $A[x]$ sono tutti e soli quelli che soddisfano una tra le seguenti condizioni:

(a). $f(x) \in A$ e irriducibile in A;

(b). $f(x) \in A[x]$, con $\deg f(x) \geq 1$, $c(f(x)) = 1$ e $f(x)$ irriducibile in $K[x]$[a].

Dimostrazione. Si distinguono due casi.

- Si ha $f(x) \in A$.

  In questo caso, come già osservato prima, $f(x)$ è costante e

  $$f(x) = g(x)h(x) \implies \deg g(x) + \deg h(x) = \deg f(x) = 0$$

  dove l'implicazione è giustificata dal fatto che si sta operando in un dominio. Pertanto, si ha $\deg g(x) = \deg h(x) = 0$ e, allora, anche $g(x), h(x) \in A$. Questo significa che $f(x)$ è irriducibile in $A[x]$ se e solo se f è irriducibile in A (visto che $(A[x])^* = A^*$ e uno tra g e h deve essere invertibile).

- Si ha $f(x)$ generico.

Sia, allora, $f(x)$ con $\deg f(x) \geq 1$. Si assume che sia irriducibile in $A[x]$, per cui $f(x) = c(f(x))f'(x)$, con $c(f(x))$ invertibile in $A[x]$, il che implica che $c(f(x)) \in (A[x])^* = A^*$, cioè $f(x)$ è primitivo. D'altra parte, si prende $f(x) = g(x)h(x)$ in $K[x]$; per il corollario precedente, si può scrivere come prodotto di polinomi dello stesso grado in $A[x]$:

$$f(x) = g_1(x)h_1(x) \quad \text{con} \quad \deg g_1(x) = \deg g(x),\ \deg h_1(x) = \deg h(x)$$

Essendo $f(x)$ irriducibile in $A[x]$, deve essere $g_1(x)$ invertibile, oppure $h_1(x)$ invertibile; ne segue che $\deg g_1(x) = 0$, oppure $\deg h_1(x) = 0$. Sempre per il corollario precedente, si ha $\deg g(x) = 0$, oppure $\deg h(x) = 0$, il che vuol dire che $g(x) \in (K[x])^*$, oppure $h(x) \in (K[x])^*$. Questo significa che $f(x)$ è irriducibile in $K[x]$.

Ora si mostra il viceversa. Sia f primitivo e irriducibile in $K[x]$ (per cui $c(f(x)) \sim 1$) e sia $f(x) = g(x)h(x)$ in $A[x]$ (e anche in $K[x]$); visto che f è irriducibile in $K[x]$, si ha che $g(x)$, o $h(x)$ sono invertibili in $K[x]$, quindi costanti. Assumendo senza perdita di generalità che $g(x) \in A$, allora

$$1 = c(f(x)) = c(g(x)h(x)) = c(g(x))c(h(x)) = gc(h(x))$$

quindi $g \in A^* = (A[x])^*$, da cui f è irriducibile in $A[x]$.

□

[a] Qui, $K[x]$ è l'anello dei polinomi a coefficienti nel campo dei quozienti di A

Terminati i prerequisiti teorici, è ora possibile caratterizzare gli anelli di polinomi di UFD; la teoria sopra sviluppata servirà per completare gli ultimi due punti della dimostrazione.

Teorema 2.8. Se A è un UFD, allora $A[x]$ è un anello a fattorizzazione unica.

Dimostrazione. La dimostrazione di questo si articola nei seguenti tre punti.

(a). $A[x]$ è un dominio.

Siano $f(x), g(x) \in A[x] \setminus \{0\}$, con $\deg f(x) = n$ e $\deg f(x) = m$. Visto che, per questioni di grado, $a_n, b_m \neq 0$, allora $a_n b_m \neq 0$, essendo A un dominio per ipotesi. Ne segue che $f(x)g(x) \neq 0$ se $f(x), g(x) \neq 0$, per cui $A[x]$ è un dominio.

(b). Ogni irriducibile di $A[x]$ è primo (condizione (i)).

Sia $f(x) \in A[x]$ irriducibile; per dimostrare che è primo, si deve verficiare che $\forall g(x), h(x) \in A[x]$, si ha:

$$f(x) \mid g(x)h(x) \implies f(x) \mid g(x) \quad \text{o} \quad f(x) \mid h(x)$$

in $A[x]$. Si distinguono gli stessi due casi visti nel teorema precedente.

- Se $\deg f(x) = 0$, ovvero $f(x) \in A$ (cioè è costante), con $f(x)$ irriducibile per assunzione, visto che A è un UFD, si ha f primo in A; infatti:

$$f \mid gh \implies f = c(f) \mid c(gh) = c(g)c(h) \implies f \mid c(g) \mid g(x) \quad \text{o} \quad f \mid c(h) \mid h(x)$$

- Se $f(x)$ è primitivo e irriducibile in $K[x]$, con $\deg f(x) \geq 1$, notando che $K[x]$ è un dominio euclideo (essendo K campo), si conclude che $f(x)$ è anche primo in $K[x]$ (essendo ED $\subset$ UFD). Ne segue che se $f(x) \mid g(x)h(x)$ in $A[x]$, allora $f(x) \mid g(x)$, oppure $f(x) \mid h(x)$ in $K[x]$; avendo assunto che $f(x)$ è primitivo, vale il corollario 2.6.2, quindi la divisibilità in $K[x]$ implica quella in $A[x]$, da cui $f(x)$ primo in $A[x]$.

(c). Ogni catena discendente di divisibilità è stazionaria (condizione (ii)).

Si dimostrerà che, data $\{f_n(x)\}$ una successione di elementi di $A[x]$ tale che $f_{i+1}(x) \mid f_i(x)$, allora è stazionaria, cioè $\exists n_0 \in \mathbb{N}$ tale che $f_i(x) \sim f_{n_0}(x),\ \forall i \geq 0$.

Per farlo, si osserva che, per il lemma di Gauss, si ha $f(x) \mid g(x) \implies c(f(x)) \mid c(g(x))$ e $f'(x) \mid g'(x)$; infatti, se $g(x) = f(X)h(x)$, allora

$$c(g(x))g'(x) = c(f(x))f'(x)c(h(x))h'(x)$$

ma, per quanto detto, $c(g(x)) = c(f(x)h(x)) = c(f(x))c(h(x))$, per cui $f'(x) \mid g'(x)$.

Per questo motivo, alla successione $\{f_i(x)\}$ si possono associare le successioni $\{c(f_i(x))\}$ e $\{f_i'(x)\}$ e si ha:

$$c(f_{i+1}(x)) \mid c(f_i(x)) \quad \text{e} \quad f_{i+1}'(x) \mid f_i'(x),\ \forall i \geq 0$$

dove la successione $\{c(f_i(x))\}$ è stazionaria, visto che c'è una catena discendente di divisibilità di A UFD, pertanto $\exists m_0 \in \mathbb{N} : c(f_i(x)) \sim c(f_{m_0}(x)),\ \forall i \geq m_0$.

Ora si considera $\{f_i'(x)\}$ e le si associa la successione $\{\deg f_i'(x)\}$. Dalla condizione $f_{i+1}'(x) \mid f_i'(x)$, si ha $\deg f_{i+1}'(x) \leq \deg f_i'(x)$, per cui $\{\deg f_i'(x)\}$

è una successione di numeri naturali decrescente che, dunque, si stabilizza: $\exists d_0 \in \mathbb{N} : \deg f_i'(x) = \deg f_{d_0}'(x),\ \forall i \geq d_0$. Da questo, si conclude che $\forall i \geq d_0$, i polinomi $f_i'(x)$ e $f_{i+1}'(x)$ hanno stesso grado e $f_i'(x) \mid f_{i+1}'(x)$, cioè differiscono per una costante; essendo entrambi primitivi, però, la costante deve essere un'unità, perciò:

$$f_i'(x) \sim f_{d_0}'(x),\ \forall i \geq d_0$$

Per finire, sia dato $n_0 = \max\{m_0, d_0\}$; allora $\forall i \geq n_0$, vale contemporaneamente che:

$$c(f_i(x)) \sim c(f_{m_0}(x)) \quad \text{e} \quad f_i'(x) \sim f_{d_0}'(x)$$

da cui la tesi:

$$f_i(x) = c(f_i(x))f_i'(x) \sim c(f_{n_0}(x))f_{n_0}'(x),\ \forall i \geq n_0$$

La dimostrazione, allora, segue per il teorema di caratterizzazione degli UFD. □

Osservazione 2.13. Dal punto (a) della dimostrazione del teorema precedente, segue anche che $(A[x])^* = A^*$; infatti, considerando $f(x) \in (A[x])^*$, si ha che $\exists g(x) \in A[x]$ tale che

$$f(x)g(x) = 1 \implies \deg f(x) + \deg g(x) = 0 \implies \deg f(x) = \deg g(x) = 0$$

per cui $f(x), g(x) \in A$ e, in particolare, $f(x) = a$ e $g(x) = b$, da cui $ab = 1 \implies f(x) \in A^*$.

Corollario 2.8.1. Se A è un UFD, allora $A[x_1, \ldots, x_n]$ è un anello a fattorizzazione unica.

Dimostrazione. Dal teorema precedente, la dimostrazione segue per induzione; infatti, tale teorema assicura il caso base per $A[x]$, mentre, assumendo vera la tesi per $A[x_1, \ldots, x_{n-1}] = B$, si arriva alla fine della dimostrazione considerando $B[x_n]$, il quale risulta un UFD per il caso iniziale. □

Osservazione 2.14. Si nota che, in generale, se A è un PID, allora non è sempre vero che $A[x]$ è un PID; per esempio, nel caso di $\mathbb{Z}$ si saa che $\mathbb{Z}[x]$ non è un PID perché l'ideale $I = \langle 2, x\rangle$ non è principale.

Analogamente, se A è un ED, allora non è sempre vero che $A[x]$ è un ED; come esempio, si può sempre considerare il caso di $\mathbb{Z}$ e $\mathbb{Z}[x]$.

Osservazione 2.15. Se K è un campo, allora $K[x]$ è euclideo, mentre $K[x, y]$ è un UFD (visto il corollario 2.8.1), mentre non è un PID perché, per esempio, $I = \langle x, y \rangle$ non è principale.

Esercizio 2.2. Dimostrare che, dato $K[x, y]$ campo, allora l'ideale $I = \langle x, y \rangle$ non è principale.

Svolgimento. Risolto a pagina 100 della teoria. ■

Proposizione 2.22 (Criterio di irriducibilità di Eisenstein). Sia A un UFD e $f(x) \in A[x]$ primitivo, con $f(x) = \sum_{i=0}^{n} a_i x^i$. Sia, poi, $p \in A$ un primo tale che:

(a). $p \nmid a_n$;

(b). $p \mid a_i, \ \forall i \in \{0, \ldots, n-1\}$;

(c). $p^2 \nmid a_0$.

Allora $f(x)$ è irriducibile in $A[x]$ (e in $K[x]$, con K campo dei quozienti di A).