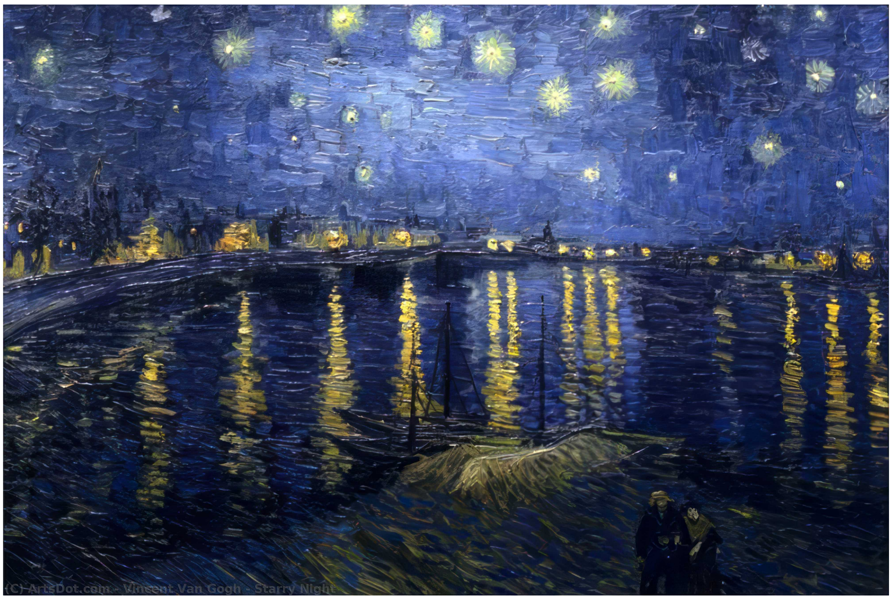
APPUNTI DI ALGEBRA

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 $\langle q_a(1) \rangle = \mathbb{Z}$[1], è necessario che a sia un generatore di $\mathbb{Z}$, perciò sono ammessi $a = \pm 1$. In questo caso, $\operatorname{Aut}(\mathbb{Z}) = \{\pm \operatorname{Id}_{\mathbb{Z}}\} \cong (\mathbb{Z}/2\mathbb{Z}, +)$. ■

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

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

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

[1] Richiesto dal fatto che q_a sia suriettivo.

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 $\psi_g(y) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = x$. $\square$

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 $h\,\mathrm{Stab}(x) = hh^{-1}g\,\mathrm{Stab}(x) = g\,\mathrm{Stab}(x)$. $\square$

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 $|\mathrm{Orb}(x)| = |G|/|\mathrm{Stab}(x)|$. $\square$

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 $\psi_{g_1 g_2}(H) = g_1 g_2 H g_2^{-1} g_1^{-1} = \psi_{g_1} \circ \psi_{g_2}(H)$, cioè $g_1 g_2 \mapsto \psi_{g_1}\psi_{g_2}$. 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. □

§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 $|Z(G)| \geqslant 1$, 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 $\exists x \in G : \mathrm{ord}(x) = p$.

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[1], 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, $\mathrm{ord}(zH) \mid \mathrm{ord}(z) \Rightarrow \mathrm{ord}(z) = pk$; se $k = n$, allora G è ciclico e z^n ha ordine p, altrimenti, se $k < n$, si ha la tesi per induzione.

□

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

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 $\mathrm{ord}(x) = p$.

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 $\mathrm{ord}(x) = p$ 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,

[1] 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 $|G| = p^n$.

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). $\square$

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. $\square$

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 $\operatorname{ord}(x) = 2$ e $\operatorname{ord}(y) = 3$. Se G è abeliano, poi, si ha $\operatorname{ord}(xy) = 6$[1], 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 $|\langle x, y \rangle| = (3 \cdot 2)/1 = 6$[2], 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.

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 $\operatorname{Ker} \phi =$

[1] $\langle x \rangle \cap \langle y \rangle$e perché sono generati da elementi diversi, altrimenti avrebbero stesso ordine.
[2] Come già accennato, l'intersezione è solo l'unità perché i due elementi hanno ordini diversi, quindi generano gruppi disgiunti.

$\{g \in G \mid \phi_g = \phi_e\} = \{g \in G \mid gx = x\} = \{e\}$. 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 $S^{-1} = \left\{ s^{-1} \mid s \in S \right\}$.

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[1]. □

§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.

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

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. □

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 $f(x_i) = f(x_i')$, $\forall i$. $\square$

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, $F_n / \operatorname{Ker} \varphi \cong G$. $\square$

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 $\overline{\psi}(\alpha) = \overline{\psi}(\pi(a)) = \varphi(a) = \overline{\varphi}(\pi(a)) = \overline{\varphi}(\alpha)$, $\forall \alpha$. $\square$

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:

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

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

(a). Φ è ben definita.

Se $f \in \operatorname{Hom}(H, K)$, 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 $(k_1, \ldots, k_n) \in K^n$ 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 $\bar{f} : F/N \cong H \longrightarrow K$ che mappa la classe di x_i in k_i. Quindi la n-upla data è l'immagine di $\bar{f}$ 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 $f : \{x_1, \ldots, x_n\} \longrightarrow K$, che mappano x_i in elementi di K che soddisfano R, oppure l'insieme delle n-uple $\{(k_1, \ldots, k_n) \in K^n : k_i \text{ soddisfano } R\}$. Questo perché, fissato l'ordinamento dei generatori $x_1, \ldots, x_n$, esiste una biezione

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

§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[1] 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 $\sigma\rho\sigma\rho = e \Rightarrow \sigma\rho\sigma = \rho^{-1}$. □

[1] 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 $GL_2(\mathbb{R})$, visto che si possono vedere come applicazioni lineari da $\mathbb{R}^2$ in se stesso, cioè possono essere rappresentate tramite matrici[1]:

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

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.

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 $m \leqslant k$). 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 $\langle \rho \rangle \cong C_n <$

[1] 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.

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:

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

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 $(\tau H \cap C_n)$[2].

Dimostrazione. Si considera

$$\begin{tikzcd} H \arrow[r, "\gamma"] \arrow[rr, bend right, "\varphi"'] & GL_2(\mathbb{R}) \arrow[r, "\det"] & \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z} \end{tikzcd}$$

dove γ è l'omomorfismo che a ρ e σ associa le relative matrici, mentre le matrici di $GL_2(\mathbb{R})$ 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.

[1] Qui, con C_n si indica un generico gruppo ciclico di ordine n.
[2] Per $\tau H \cap C_n$, si intende $\tau(H \cap C_n)$.

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 $\psi(h) = \tau h$. $\square$

Si osserva che, per qualche m, $H \cap C_n = \langle \rho^m \rangle = \left\{e, \rho^m, \rho^{2m}, \dots, \rho^{n-m}\right\}$, con $m \mid n$; se $\tau = \sigma\rho^i$, allora $\tau H \cap C_n = \left\{\sigma\rho^i, \sigma\rho^{i+m}, \dots, \sigma\rho^{i+n-m}\right\}$ 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 $H \lhd G$. $\square$

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 $K \lhd G$. $\square$

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 $\{\rho^{n/2}\}$ 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 $Z(D_n) = \{e, \rho^{n/2}\} \cong \mathbb{Z}/2\mathbb{Z}$ 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,

[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.

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 $|D_n/\langle \rho^m \rangle| = 2n/(n/m) = 2m$.

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):

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

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 $X = \{1, \ldots, n\}$, 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 $X = \{1, \ldots, n\}$ 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

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

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

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

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

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

L'azione di σ ristretta a $\operatorname{Orb}(x)$, 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. $\square$

[1] 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 S_n. Si cerca quanti k-cicli, con $k \leqslant n$, 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 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 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 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

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

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

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

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

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

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:

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

□

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

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

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

Dimostrazione. È un omomorfismo perché:

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

dove si è moltiplicato sopra e sotto per $\tau(i) - \tau(j)$ e si sono separate le produttorie[1].

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

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

[1] 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 $\prod_{1 \leqslant a < b \leqslant n} \frac{\sigma(a) - \sigma(b)}{a - b}$.

Se $\{i, j\} \cap \{a, b\} = \varnothing$, 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

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

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 delle due intersezioni non vuote 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 $\operatorname{sgn} \sigma = -1$. □

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*. Alcune sue caratteristiche sono:

(a). $A_n \lhd S_n$;

(b). $S_n/A_n \cong \{\pm 1\}$.

Visto che $S_n/A_n \cong \{\pm 1\}$, per il teorema di Lagrange, si ha:

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

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 $\sigma = (a_1, \dots, a_k)$ 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

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

  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:

$$\begin{array}{cccc} \sigma = & (x_{11} \dots x_{1k_1}) & \cdots & (x_{r1} \dots x_{rk_r}) \\ & \downarrow & & \downarrow \\ \rho = & (y_{11} \dots y_{1k_1}) & \cdots & (y_{r1} \dots y_{rk_r}) \end{array}$$

  con $\tau(x_{ij}) = y_{ij}$, quindi vale $\tau\sigma\tau^{-1} = \rho$.

$\square$

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 $H, K < Z(\sigma)$, $H \cap K = \{e\}$ 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 $\langle(56)\rangle \cong C_2 \cong \mathbb{Z}/2\mathbb{Z}$.

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

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

$\square$

§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 $H, K \triangleleft G$, 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 $hkh^{-1}k^{-1} = e \Rightarrow hk = kh$. $\square$

Teorema 1.8. Sia G un gruppo e siano $H, K \triangleleft G$; 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. $\square$

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

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

Lo stesso vale per g, quindi entrambe le mappe sono omomorfismi iniettivi. Usando il fatto 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

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

- ($\Rightarrow$) 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 $\operatorname{Aut}(H \times K)$ è della forma $(f, g) : f \in \operatorname{Aut}(H),\ g \in \operatorname{Aut}(K)$, ma allora, per $\psi \in \operatorname{Aut}(H \times K)$, 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 $f \in \operatorname{Aut}(H \times K)$, con $f(h, e_K) = (h', k')$; visto che $\operatorname{ord}((h, e_K)) = \operatorname{ord}(h) \mid n$, deve essere $\operatorname{ord}((h', k')) = \operatorname{mcm}(\operatorname{ord}(h'), \operatorname{ord}(k')) \mid n$, visto che f è automorfismo e, in particolare $\operatorname{ord}(k') \mid n$. Per ipotesi, deve essere $\operatorname{ord}(k') \mid m$, 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 $\gamma : K \to \operatorname{Aut}(H)$ un omomorfismo tale che $\gamma(k) = \gamma_k \in \operatorname{Aut}(H)$, 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:

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

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[1]:

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

□

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 $H = \mathrm{Ker}\,\pi_K$.

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.

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

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 $\gamma : K \to \mathrm{Aut}(H)$ 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

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

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

- $\gamma : K \to \mathrm{Aut}(H)$ 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 $(h, k) \in \mathrm{Ker}\, F$; 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 $\mathrm{Ker}\, F = \{(e_G, e_G)\}$.

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 $\varphi : \langle\sigma\rangle \to \mathrm{Aut}(\langle\rho\rangle)$ tale che $\sigma \longmapsto \varphi_\sigma$ e $\varphi_\sigma(\rho) = \sigma\rho\sigma = \rho^{-1}$. Visto che φ è un omomorfismo, deve valere $\mathrm{ord}(\varphi_\sigma) \mid \mathrm{ord}(\sigma) = 2$, quindi ci sono due possibilità: o $\varphi_\sigma = \mathrm{Id}$, 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 $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ sono presenti altri elementi di ordine 2, come nel caso di $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong (\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 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 1.27, si sa anche che $H \lhd G$[1]

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 $G = HK$[2].

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 $p \nmid (q-1)$[3], 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] Perché $[G : H] = |G/H| = |G|/|H| = qp/q = p$.

[2] Si ricorda che $H \lhd G$ implica che HK è un gruppo).

[3] 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 almeno p, cosa che è verificata se e solo se $p \mid q - 1$.

$1)\mathbb{Z}$, 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[1]; si ha:

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

quindi $\operatorname{ord}(\ell) = \operatorname{ord}(\ell') = p$, 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.

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 $\operatorname{Aut}(H) \cong \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$. 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 $\operatorname{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ 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 $|Z_{S_n}(\sigma)||\operatorname{Cl}_{S_n}(\sigma)| = n!$; analogamente, se $\sigma \in A_n$, allora $|Z_{A_n}(\sigma)||\operatorname{Cl}_{A_n}(\sigma)| = n!/2$, 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:

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

[1]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.

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 $\operatorname{Ker} \text{sgn} = A_n$.

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 $n \geqslant 5$.

Svolgimento. Dato $\sigma = (a, b, c) \in S_5$ un 3-ciclo, per $n \geqslant 5$ 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 $|\mathrm{Cl}_{A_n}(1, 2, 3)| = 2 \nmid 3 = |A_3|$[1], quindi $\mathrm{Cl}_{A_n}(1, 2, 3) = \{(1, 2, 3)\}$.

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

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 $H \triangleleft A_4$[2] e $\exists \sigma \in H$ con $\operatorname{ord}(\sigma) = 2$ e $\sigma = (a, b)(c, d)$. Si nota che $\mathrm{Cl}_{S_4}(\sigma) = \{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} =$

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

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

$\mathrm{Cl}_{A_4}(\sigma)$; 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 $|K| = 4 \nmid 6 = |H|$. ■

Proposizione 1.25. Per ogni $n \geqslant 5$, 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[1] e ci si ritrova nel caso precedente. Se H contiene un 5-ciclo, ancora per coniugio, contiene un 3-ciclo[2] 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 $n \geqslant 6$, $A_n \supset G_i = \{\sigma \in A_n \mid \sigma(i) = 1\} \cong A_{n-1}$, 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 $r_1, \dots, r_k$ decrescenti: $\sigma = C_1 \cdots C_k$. Si assume $r_i \geqslant 3$ per un certo i, quindi $C_i = (i_1, i_2, i_3, \dots)$; 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 $\sigma = (i,j)(k,l)\dots$ 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. □

Sottogruppi normali di 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 $A_n \langle (1\ 2) \rangle = S_n$[3]. 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 $S_n \cong A_n \rtimes_\varphi \langle (1\ 2) \rangle$. ■

[1] Per esempio, $((1,2)(3,4))((1,5)(3,4)) = (1,5,2)$.
[2] Per esempio, $(1,2,3,4,5)(1,5,3,4,2) = (3,4,5)$.
[3] 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 $G(p) = \{g \in G \mid \text{ord}(g) = p^k,\ k \in \mathbb{N}\}$.

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

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

Teorema 1.11 (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 $n_{i+1} \mid n_i,\ \forall i \in \{1, \ldots, s-1\}$.

Teorema 1.12. 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.

§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 1.13 (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*: $\forall \alpha \in \mathbb{N} : 0 \leqslant \alpha \leqslant n,\ \exists H < G$ con $|H| = p^\alpha$;

(b). *inclusione*: ogni p-gruppo di G è contenuto in un p-Sylow[1];

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

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

(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 $0 \leqslant \alpha \leqslant n$. Sia $\mathcal{M} = \{M \subset G \mid |M| = p^\alpha\}$; allora

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

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

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

essendo $i \leqslant p^{\alpha-1}$ e $\alpha \leqslant n$. Visto che ν_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 $|\mathcal{M}|$[1].

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:

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

con R insieme dei rappresentanti delle orbite. Il fatto che $p^{n-\alpha} \parallel |\mathcal{M}|$[2] implica che $\exists i$ tale per cui

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

Ne segue anche che $p^\alpha \mid |\mathrm{Stab}(M_i)|$[3], per cui $|\mathrm{Stab}(M_i)| \geqslant p^\alpha$; si vuole mostrare che $|\mathrm{Stab}(M_i)| = p^\alpha$.

D'altra parte, la mappa $\mathrm{Stab}(M_i) \longrightarrow M_i$ tale che $\mathrm{Stab}(M_i) \ni y \longmapsto yx$, per $x \in M_i$, è iniettiva perché $yx = y_1 x \iff y = y_1$, quindi $\mathrm{Stab}(M_i) \leqslant |M_i| = p^\alpha$, da cui $|\mathrm{Stab}(M_i)| = p^\alpha$. Essendo $\mathrm{Stab}(M_i) < G$, significa che in G esiste un sottogruppo di ordine p^α.

[1] 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 $(j, p) = 1$.

[2] La notazione $\parallel$ si usa per indicare divisione esatta, cioè nessun esponente maggiore è divisore.

[3] Il fatto che $p^{n-\alpha} \mid p^n m / |\mathrm{Stab}(M_i)|$ implica che $p^\alpha \mid |\mathrm{Stab}(M_i)|$, cosa che si vede scrivendo $p^n m / |\mathrm{Stab}(M_i)| = p^{n-\alpha} k$, per qualche intero k.

(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:

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

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 $p \nmid m$[1], deve esistere un $g \in R$ tale che $a_g = 0$, per cui $\mathrm{Orb}(gS) = \{gS\} \Rightarrow \mathrm{Stab}(gS) = H$. 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 $n_p = |\mathrm{Cl}(S)| = [G : N_G(S)] \mid |G|$. 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 $\mathrm{Orb}(S)$ è l'unica orbita banale di questa azione.

Per dimostrarlo, si considera, allora, $H \in Y$ con $\mathrm{Orb}(H) = \{H\}$, per cui $S = \mathrm{Stab}(H) = \left\{s \in S \mid sHs^{-1} = H\right\}$; 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

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

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

□

Esempio 1.9. Sia $G = S_4$; visto che $|S_4| = 2^3 \cdot 3$, esiste un 2-Sylow, sia questo P, con $|P| = 2^3 = 8$.

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

§1.14 Esercizi e complementi

1.14.1 Complementi di teoria

Di seguito, un criterio importante per stabilire se un sottogruppo è normale.

Proposizione 1.27. 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[1], 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 $|G/H_G| \geqslant p$; 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. $\square$

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

1.14.2 Esercizi

Esercizio 1.7. 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 1.8. 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

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

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:

$$\begin{aligned} &N_{S_n}(\langle\rho\rangle) = \{\tau \in S_n \mid \tau\rho\tau^{-1} = \rho^k,\ \gcd(\mathrm{ord}(\rho), k) = 1\} \\ &\Rightarrow |N_{S_n}(\langle\rho\rangle)| = |\{k \in \mathbb{Z} \mid \gcd(k, \mathrm{ord}(\rho)) = 1\}||Z_{S_n}(\rho)| = \phi(\mathrm{ord}(\rho))|Z_{S_n}(\rho)| \end{aligned} \tag{1.14.1}$$

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

Osservazione 1.15. 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 $\mathrm{ord}(\rho)$.

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 $A = D(A) \cup A^*$[1].

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.

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

(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 $\varphi_x(a) = xa = 1 \implies x \in A^*$.

□

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 $Ia \subset I$, $\forall a \in A$[1].

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.

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

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:

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

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

(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 (si sta sempre assumendo che A sia commutativo con identità), 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). 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 $i = 0, \dots, m + n$, si ha o che $i \geqslant n$, quindi $x^i \in I$, oppure che $n + m - i \geqslant m$, 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, $\forall a \in A$, $(ax^n) = a^n x^n$ appartiene ad I perché $x^n \in I$ e vale la proprietà di assorbimento; allora $ax \in \sqrt{I}$.

(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. □

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. Sia $I \cap A^* = \varnothing$; visto che $1 \in A^*$ sempre, allora $\exists a \in A : a \notin I$, per cui $I \subsetneq A$.

Per l'implicazione inversa, sia $I \subsetneq A$ un ideale proprio e sia, per assurdo, $x \in I \cap A^*$; allora x è invertibile, quindi $\exists x^{-1} \in A$ tale che $xx^{-1} = 1$, quindi $1 = x^{-1}x \in I \Rightarrow 1 \in I \Leftarrow I = A$ per assorbimento, da cui l'assurdo. □

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