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

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

[1] Richiesto dal fatto che q_a sia suriettivo.

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

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

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

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

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

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

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

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

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

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

1.2 Azioni di gruppo

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

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

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. Se due elementi di un'orbita sono uguali, allora appartengono alla stessa classe di equivalenza di $G/\mathrm{Stab}(x)$.

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

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

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

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

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

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

1.2.1 Azione di coniugio

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 qualche intero $k > 0$, si ha $|G|/|Z(x)| = p^k$, da cui

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

Visto che $e \in Z(G)$, deve risultare $|Z(G)| \geq 1$, da cui $|Z(G)| = p^s$, 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 $x_0Z(G)$ il suo generatore. Date due classi laterali distinte $xZ(G), yZ(G) \in G/Z(G)$ e visto che $x_0Z(G)$ 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, $\text{ord}(zH) \mid \text{ord}(z) \Rightarrow \text{ord}(z) = pk$; se $k = n$, allora G è ciclico e z^n ha ordine p, altrimenti, se $k < n$, si ha la tesi per induzione.

□

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

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

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

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

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

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

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

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

[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 $|G| = p^n$.

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 $\gamma : H \times K \longrightarrow HK$ 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. $\square$

Classificazione dei gruppi di ordine 6

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

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

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

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

[a] Si dimostra per calcolo diretto; per esempio: $(xy)^3 = xyxyxy = xxxyyy = x$.

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

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

Dimostrazione. Si definisce l'azione

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

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

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). $G' \triangleleft G$;

(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 diedrali

Definizione 1.11 (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 1.8. Per $n \in \mathbb{N}$, il gruppo diedrale D_n ha cardinalità $|D_n| = 2n$.

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

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 1.9. 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 $\sigma\rho\sigma\rho = e \Rightarrow \sigma\rho\sigma = \rho^{-1}$. □

OSSERVAZIONE 1.5. Le isometrie del piano che agiscono su un n-agono, quindi gli elementi di D_n, si possono mettere in relazione con $\mathrm{GL}_2(\mathbb{R})$, cioè possono essere rappresentate tramite matrici:

$$\rho \overset{\gamma}{\longmapsto} \begin{pmatrix} \cos(2\pi/n) & \sin(2\pi/n) \\ -\sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} = M_\rho \qquad \sigma \overset{\gamma}{\longmapsto} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = M_\sigma \tag{1.6.1}$$

Si nota, inoltre, che indicando con $\mathbb{D}_n$ il gruppo generato da queste matrici, allora la mappa $\gamma : \langle \rho, \sigma \rangle \to \mathbb{D}_n$ e notare che questo è un omomorfismo di gruppi; infatti, la composizione di isometrie che fissano un punto, sono ancora isometrie che fissano lo stesso punto (in questo caso, l'n-agono). Questo per dire che la mappa $\rho^i\sigma^j \mapsto M_\rho^i M_\sigma^j$ è ben definita.

Si può, inoltre, verificare che $M_\rho^n = \mathrm{Id}$, $M_\sigma^2 = \mathrm{Id}$ e $M_\sigma M_\rho M_\sigma = M_\rho^{-1}$, per cui si conclude che γ è un omomorfismo.

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 1.10. 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 $m \le k$).

Usando $\sigma^2 = e$ e assumendo $c_1 \neq 0$, si può scrivere

$$g = \rho^{c_1}\sigma \dots \rho^{c_m}\sigma = \sigma\sigma\rho^{c_1}\sigma\sigma\sigma\rho^{c_2} \dots \sigma\rho^{c_m}\sigma = \sigma\rho^{-c_1}\rho^{-c_2} \dots \rho^{-c_m} = \sigma\rho^{-d}$$

[1] Cioè che manda un lato nel successivo.

dove si è fatto uso della relazione $\sigma\rho\sigma = \rho^{-1}$ e con $d \equiv -\sum_{i=1}^{m} c_i \pmod{n}$.

Se, invece, $c_1 = 0$ (cioè la *parola* inizia con σ), allora $g = \rho^{-c_2} \dots \rho^{-c_m} = \rho^{d'}$, con $d' \equiv -\sum_{i=2}^{m} c_i \pmod{n}$. $\square$

Da questa proposizione, segue direttamente che se $\rho, \sigma \in D_n$, allora $\langle \rho, \sigma \rangle < D_n$

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