Complementi di Algebra 1

APPUNTI DEL CORSO DI ALGEBRA 1 TENUTO
DALLA PROF. DEL CORSO E DAL PROF. LOMBARDO

Leonardo Migliorini
l.migliorini@studenti.unipi.it

Anno Accademico 2022-23

Indice

1 Insiemi di generatori **3**

2 Automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$ **4**

3 Gruppo diedrale **5**
3.1 Elementi del gruppo 5
3.2 Sottogruppi 6
3.3 Classi di coniugio 9
3.4 Legge di gruppo e omomorfismi 10
3.5 Automorfismi 11

4 Automorfismi di un prodotto diretto **13**

5 Gruppo derivato **16**

6 Azioni di gruppo **18**
6.1 Azioni transitive 18

§1 Insiemi di generatori

Definizione 1.1. Dati un gruppo G e $x_1, \dots, x_n$ elementi di G, chiamiamo **sottogruppo generato** da $x_1, \dots, x_n$ il più piccolo sottogruppo $\langle x_1, \dots x_n \rangle$ di G contenente $x_1, \dots, x_n$, cioè

$$\langle x_1, \dots, x_n \rangle = \bigcap_{\substack{H \leqslant G \\ \{x_1, \dots, x_n\} \subseteq H}} H$$

Osservazione 1.2 — La definizione è ben posta, infatti l'intersezione avviene su una famiglia non vuota di insiemi dal momento che G è un sottogruppo di se stesso contenente $x_1, \dots, x_n$. Inoltre l'intersezione non è vuota in quanto contiene almeno l'identità e gli elementi $x_1, \dots, x_n$.

La definizione data non dà informazioni su come sono fatti gli elementi di $\langle x_1, \dots, x_n \rangle$, cerchiamo quindi di caratterizzare in modo diverso tale sottogruppo. Poiché chiuso per l'operazione indotta da G, $\langle x_1, \dots, x_n \rangle$ deve contenere tutti i prodotti finiti, in qualsiasi ordine, delle potenze di $x_1, \dots, x_n$, cioè deve contenere l'insieme

$$\{g_1^{\pm 1}, \dots, g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \dots, x_n\} \ \forall i \in \{1, \dots, r\}\}$$

Proposizione 1.3

Dati un gruppo G e $x_1, \dots, x_n$ elementi di G, allora

$$\langle x_1, \dots, x_n \rangle = \{g_1^{\pm 1}, \dots, g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \dots, x_n\} \ \forall i \in \{1, \dots, r\}\}$$

Dimostrazione. Poniamo $S = \{g_1^{\pm 1}, \dots, g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \dots, x_n\} \ \forall i \in \{1, \dots, r\}\}$, mostriamo che S è un sottogruppo di G. Effettivamente $e \in S$ in quanto è prodotto nessuna potenza di $x_1, \dots, x_n$, il prodotto di due elementi di S è ancora un elemento di S in quanto prodotto finito di potenze di $x_1, \dots, x_n$ e l'inverso di un elemento $g_1^{\pm 1} \dots g_r^{\pm 1} \in S$ è $(g_1^{\pm 1} \dots g_r^{\pm 1})^{-1} = g_r^{\mp 1} \dots g_1^{\mp 1}$, che è un elemento di S. Abbiamo quindi che S è un sottogruppo di G contenente $x_1, \dots, x_n$, pertanto $\langle x_1, \dots, x_n \rangle \subseteq S$ per minimalità di $\langle x_1, \dots, x_n \rangle$. D'altra parte, per quanto osservato sopra abbiamo che tutti gli elementi della forma $g_1^{\pm 1} \dots g_r^{\pm 1}$ con $r \in \mathbb{N}$, $g_i \in \{x_1, \dots, x_n\}$ per ogni $i \in \{1, \dots, r\}$ devono essere contenuti in $\langle x_1, \dots, x_n \rangle$, pertanto i due sottogruppi coincidono. □

Osservazione 1.4 — Se G è un gruppo ciclico abbiamo che esiste $x \in G$ tale che $\langle x \rangle = G$, cioè tutti gli elementi di G sono potenze di x.

Diciamo che $x_1, \dots, x_n \in G$ sono **generatori** per G, o che l'insieme $\{x_1, \dots, x_n\}$ **genera** G se $\langle x_1, \dots, x_n \rangle = G$.

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

Dato p un primo, vogliamo determinare quanti sono gli automorfismi di $(\mathbb{Z}/p\mathbb{Z})^n$, per fare ciò è conveniente definire una struttura di spazio vettoriale, quindi un prodotto per scalari

$$\cdot : \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n : (\overline{\lambda}, v) \longmapsto \overline{\lambda}v$$

con $\overline{\lambda}v = \underbrace{v + \ldots + v}_{\tilde{\lambda} \text{ volte}}$ e $\tilde{\lambda}$ un qualsiasi rappresentante di $\overline{\lambda}$. Tale prodotto è ben definito, infatti se $\lambda, \lambda' \in \mathbb{Z}$ sono tali che $\overline{\lambda} = \overline{\lambda'}$, cioè esiste $k \in \mathbb{Z}$ tale che $\lambda = \lambda' + kp$, allora

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

in quanto $\underbrace{v + \ldots + v}_{kp \text{ volte}} = 0$. Si verifica che $((\mathbb{Z}/p\mathbb{Z})^n, +, \cdot)$ è effettivamente uno spazio vettoriale sul campo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (dove $\cdot$ è il prodotto per scalari appena definito). Per come abbiamo definito il prodotto per scalari, abbiamo che per ogni $\varphi \in \mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ vale $\varphi(\lambda v) = \lambda\varphi(v)$ per ogni $\lambda \in \mathbb{F}_p$, pertanto

$$\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) = GL((\mathbb{F}_p)^n) = \{\varphi : (\mathbb{F}_p)^n \longrightarrow (\mathbb{F}_p)^n \mid \varphi \text{ isomorfismo di spazi vettoriali}\}.$$

Poiché $GL((\mathbb{F}_p)^n) \cong GL_n(\mathbb{F}_p) = \{M \in M_{n\times n}(\mathbb{F}_p) \mid \det M \neq 0\}$ possiamo rappresentare ogni automorfismo di $(\mathbb{Z}/p\mathbb{Z})^n$ con una matrice invertibile di taglia $n \times n$ a coefficienti in $\mathbb{F}_p$.

Proposizione 2.1

Dato p un primo, allora

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

Dimostrazione. Osserviamo che un elemento di $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ deve necessariamente mandare una base di $(\mathbb{Z}/p\mathbb{Z})^n$ in un'altra base, e si dermina univocamente in questo modo. Sia $\{v_1, \ldots, v_n\}$ una base di $(\mathbb{Z}/p\mathbb{Z})^n$ e $\varphi \in \mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$, consideriamo $\varphi(v_1)$: $\varphi(1)$ può assumere qualsiasi valore non nullo, pertanto abbiamo $(p^n - 1)$ possibilità per l'immagine del primo vettore. Per quanto riguarda v_2, $\varphi(v_2)$ può assumere qualsiasi valore non nullo che non sia multiplo di $\varphi(v_1)$, che sono $p^n - p$, analogamente $\varphi(v_3)$ può assumere qualsiasi valore non nullo che non sia combinazione lineare di v_1 e v_2, che sono $p^n - p^2$, e così via. Reiteriamo questo ragionamento fino a $\varphi(v_n)$, che può essere scelto in $p^n - p^{n-1}$ modi, da cui

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

□

§3 Gruppo diedrale

§3.1 Elementi del gruppo

Definizione 3.1. Dato $n \geqslant 2$ un naturale, consideriamo un poligono regolare di n vertici, definiamo il **gruppo diedrale** su n vertici D_n come l'insieme delle isometrie del piano che mandano i vertici in se stessi, cioè che fissano il poligono (per $n = 2$ consideriamo le isometrie che mandano un segmento in se stesso).

Osservazione 3.2 — D_n è un gruppo, in quanto l'applicazione identità che fissa tutti i vertici è un'isometria dal poligono in se stesso, la composizione di isometrie è un'isometria e un'isometria ammette sempre un'inversa, che è anch'essa un'isometria.

Osservazione 3.3 — Una rotazione di angolo $\dfrac{2\pi}{n}$ è un elemento di D_n, così come una simmetria rispetto a un asse.

Proseguendo con questa intuizione geometrica, indicheremo con r una rotazione di angolo $\dfrac{2\pi}{n}$ e con s una simmetria rispetto a un qualsiasi asse. Notiamo che $\operatorname{ord}(r) = n$ e $\operatorname{ord}(s) = 2$ (per convenzione, indichiamo con un angolo positivo una rotazione in senso antiorario e con un angolo negativo una rotazione in senso orario).

Definizione 3.4. Data $r \in D_n$ una rotazione di ordine n, indichiamo con $\mathcal{R}$ il **sottogruppo delle rotazioni** $\langle r \rangle$.

Osservazione 3.5 — Il sottogruppo $\mathcal{R}$ contiene tutte le rotazioni di D_n, infatti se r' è una rotazione di angolo $\dfrac{2k\pi}{n}$, $k \in \mathbb{Z}$, allora $r^k = r'$ in quanto anche r^k è una rotazione di angolo $\dfrac{2k\pi}{n}$.

Per determinare come sono fatti gli elementi di D_n, studiamo il sottogruppo $\langle r, s \rangle$. Sicuramente $\langle r, s \rangle$ contiene il sottogruppo $\mathcal{R}$ e tutti gli elementi della forma sr^k, $sr^k s$, $sr^k sr^h$ e così via, vogliamo mostrare che in effetti D_n è generato da r e s.

Osservazione 3.6 — Gli elementi della forma r^k e sr^h sono distinti per ogni $h, k \in \mathbb{Z}$. Infatti sappiamo dall'algebra lineare che il determinante di una simmetria è -1 e che il determinante di una rotazione è 1, per la moltiplicatività del determinante quindi $\det(r^k) = (\det r)^k = 1$ e $\det(sr^h) = (\det s)(\det r)^h = -1$, da cui $r^k \neq sr^h$.

Lemma 3.7

Per ogni rotazione $r \in D_n$ e per ogni simmetria $s \in D_n$ vale

$$srs^{-1} = r^{-1}$$

Dimostrazione.

$$srs^{-1} = r^{-1} \iff sr = r^{-1}s = (s^{-1}r)^{-1}$$

si conclude osservando che $s^2 = 1$, pertanto $s^{-1} = s$ e

$$(s^{-1}r)^{-1} = (sr)^{-1} = r^{-1}s^{-1} = r^{-1}s$$

□

Proposizione 3.8
Se $n \geqslant 3$ allora $|D_n| = 2n$.

Dimostrazione. Indicando con $1, \dots, n$ gli n vertici di un poligono regolare di n lati, notiamo che un elemento $g \in D_n$ è univocamente determinato da $g(1), \dots, g(n)$. In particolare, fissato $g(1)$, per il quale abbiamo n possibili scelte, abbiamo al massimo due valori per $g(2)$, cioè $g(2) \in \{g(1)+1, g(1)-1\}$ (a meno di sommare n se uno dei due elementi è negativo). Poiché $g(1)$ e $g(2)$ individuano due vettori nel piano non allineati, cioè linearmente indipendenti, ne costituiscono una base: fissati i valori di $g(1)$ e $g(2)$ abbiamo quindi determinato ogni elemento di D_n in modo unico e, poiché possiamo farlo in al più $2n$ modi, $|D_n| \leqslant 2n$. Ricordiamo adesso che D_n contiene gli elementi della forma r^k, sr^h al variare di $h, k \in \mathbb{Z}$, mostriamo che questi sono infatti $2n$. Gli elementi r^k appartengono al gruppo ciclico $\mathcal{R}$ di ordine n, pertanto sono n elementi distinti, inoltre

$$sr^i = sr^j \iff r^i = r^j \iff i \equiv j \mod n$$

pertanto anche questi sono n elementi distinti. Allora $|D_n| = 2n$. □

Osservazione 3.9 — Abbiamo mostrato che effettivamente $D_n = \langle r, s \rangle$, quindi i suoi elementi sono tutti della forma r^k, sr^h al variare di $h, k \in \mathbb{Z}$.

Osservazione 3.10 — Il risultato è valido anche per D_2, ma con motivazioni diverse. Se consideriamo un segmento nel piano $\mathbb{R}^2$ giacente sulla retta $y = 0$, le isometrie che possiamo applicare sono l'identità, la rotazione di angolo π, la simmetria lungo la retta $y = 0$ e la simmetria lungo l'asse passante per il suo punto medio. D_2 contiene quindi quattro elementi, l'identità e tre elementi di ordine 2, pertanto è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

§3.2 Sottogruppi

Consideriamo un sottogruppo $H \leqslant D_n$, distinguiamo due possibilità: $H \subseteq \mathcal{R}$ oppure $H \nsubseteq \mathcal{R}$. Nel primo caso abbiamo che $|H| \mid n$, ed è l'unico sottogruppo di $\mathcal{R}$ con questa proprietà in quanto $\mathcal{R}$ è ciclico, in particolare H è ciclico della forma $\left\langle \frac{n}{d} \right\rangle$, con $d \mid n$. Studiamo quindi il caso $H \nsubseteq \mathcal{R}$: notiamo che $\mathcal{R} \trianglelefteq D_n$ in quanto $[D_n : \mathcal{R}] = 2$, pertanto $D_n/\mathcal{R}$ è un gruppo con l'operazione indotta da D_n e risulta essere isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Consideriamo la proiezione al quoziente

$$\pi_{\mathcal{R}} : D_n \longrightarrow D_n/\mathcal{R} : g \mapsto [g]$$

poiché $H \nsubseteq \mathcal{R}$ abbiamo che esiste $h \in H$ tale che $h \notin \mathcal{R}$, pertanto $\pi_{\mathcal{R}}(h) \notin [\mathcal{R}]$ e in particolare $\pi_{\mathcal{R}}(H) \nsubseteq [\mathcal{R}]$. Dato che i sottogruppi di $D_n/\mathcal{R}$ sono solo $\{[\mathcal{R}]\}$ e $D_n/\mathcal{R}$

abbiamo $\pi_{\mathcal{R}}(H) = {}^{D_n}\!/_{\mathcal{R}}$. Osserviamo inoltre che $\ker \pi_{|H} = \ker \pi \cap H = \mathcal{R} \cap H$, per il Primo Teorema di Omomorfismo allora ${}^{H}\!/_{H \cap \mathcal{R}} \cong \mathbb{Z}/2\mathbb{Z}$, quindi $|H \cap \mathcal{R}| = \dfrac{1}{2}|H|$. Dato che $R \cap H \subseteq \mathcal{R}$, esiste $k \in \mathbb{Z}$ tale che $H \cap \mathcal{R} = \langle r^k \rangle$ in particolare $\langle r^k \rangle$ e $\langle sr^h \rangle$, $h \in \mathbb{Z}$, sono contenuti in H.

Proposizione 3.11
Dati $H \leqslant D_n$ un sottogruppo tale che $H \not\subseteq \mathcal{R}$, se r è un generatore di $\mathcal{R}$ tale che $H \cap \mathcal{R} = \langle r^k \rangle$ e s è una simmetria allora

$$H = \langle r^k \rangle \cdot \langle sr^h \rangle = \{xy \mid x \in \langle r^k \rangle, y \in \langle sr^h \rangle\}, h, k \in \mathbb{Z}$$

Dimostrazione. Per quanto visto sopra abbiamo che $|\langle r^k \rangle| = \dfrac{1}{2}|H|$, inoltre osserviamo che $\mathrm{ord}(sr^h) = 2$ in quanto

$$(sr^h)^2 = sr^h sr^h = (srs)^h r^h = (srs^{-1})^h r^h = r^{-h} r^h = e$$

pertanto $\langle sr^h \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Da questo ricaviamo $\langle sr^h \rangle \subseteq N_{D_n}(\langle r^k \rangle)$, infatti per ogni $m \in \mathbb{Z}$ abbiamo

$$(sr^h) r^{mk} (sr^h)^{-1} = sr^{h+mk} sr^h = r^{-h-mk} r^h = r^{-mk} \in \langle r^k \rangle$$

cioè $\langle sr^h \rangle \subseteq N_{D_n}(\langle r^k \rangle)$ e quindi $\langle r^k \rangle \cdot \langle sr^h \rangle$ è un sottogruppo di D_n[1]. Poiché $\langle r^k \rangle$ e $\langle sr^h \rangle$ sono contenuti in H abbiamo che $\langle r^k \rangle \cdot \langle sr^h \rangle \subseteq H$, inoltre

$$|\langle r^k \rangle \cdot \langle sr^h \rangle| = \frac{1}{2}|H| \cdot 2 = |H|$$

in quanto $\langle r^k \rangle \cap \langle sr^h \rangle = \{e\}$[2], pertanto i due sottogruppi coincidono. □

Osservazione 3.12 — Per $k \mid n$ e $0 \leqslant h < k$, i sottogruppi $H_{k,h} = \langle r^k, sr^h \rangle$ e $H = \langle r^k \rangle \cdot \langle sr^h \rangle$ coincidono. Infatti $H_{k,h} \subseteq H$ in quanto r^k, sr^h sono elementi di H, d'altra parte $H \subseteq H_{k,h}$ in quanto $H_{h,k}$ contiene tutti i prodotti finiti delle potenze di r^k e sr^h, in particolare gli elementi di H.

Osservazione 3.13 — Per $k \mid n$ e $0 \leqslant h < k$, $\langle r^k, sr^h \rangle = \langle r^k, sr^{h+k} \rangle$. Infatti $\langle r^k, sr^h \rangle \subseteq \langle r^k, sr^{h+k} \rangle$ in quanto $sr^h = (sr^{h+k})r^{-k}$ è un elemento del secondo gruppo, simmetricamente $\langle r^k, sr^{h+k} \rangle \subseteq \langle r^k, sr^h \rangle$ in quanto $sr^{h+k} = (sr^h)r^k$ è un elemento del primo gruppo.

Teorema 3.14 (Classificazione dei sottogruppi di D_n)
I sottogruppi di D_n sono della forma

(1) $\langle r^k \rangle$ con $k \mid n$;

(2) $\langle r^k, sr^h \rangle$ con $k \mid n$, $0 \leqslant h < k$,

con $r \in \mathcal{R}$ e s una simmetria. Inoltre tali sottogruppi sono tutti distinti.

[1] Dati K, N sottogruppi di un gruppo G, se vale almeno una delle inclusioni $K \subseteq N_G(N)$, $N \subseteq N_G(K)$ allora $HK = KH$, quindi HK è un sottogruppo di G.

[2] Se H, K sono sottogruppi finiti di un gruppo G e $HK \leqslant G$ allora vale $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.

Dimostrazione. Abbiamo già visto che i sottogruppi di D_n sono di questo tipo, mostriamo quindi che sono tutti distinti. A meno di cambiare k, possiamo supporre $\mathcal{R} = \langle r \rangle$, cioè $\operatorname{ord}(r) = n$. Consideriamo $H, K \leqslant D_n$ due sottogruppi, abbiamo tre casi:

- se $H = \langle r^k \rangle$ e $K = \langle r^m \rangle$, $m \in \mathbb{Z}$, allora $H = K \iff k = m$ in quanto entrambi sottogruppi di $\mathcal{R}$, pertanto esiste un unico sottogruppo della forma $\langle r^k \rangle$ per $k \mid n$;
- se $H = \langle r^k \rangle$ e $K = \langle r^m, sr^h \rangle$, $m \mid n$, allora $H \neq K$ in quanto H è ciclico e K no;
- se $H = \langle r^k, sr^h \rangle$ e $K = \langle r^m, sr^l \rangle$, con $m \mid n$ e $0 \leqslant l < m$, considerando le intersezioni $H \cap \mathcal{R} = \langle r^k \rangle$ e $K \cap \mathcal{R} = \langle r^m \rangle$ abbiamo

$$H \cap \mathcal{R} = K \cap \mathcal{R} \iff \langle r^k \rangle = \langle r^m \rangle \iff k = m$$

Inoltre, se $sr^h \in \langle r^m, sr^l \rangle = \langle r^m \rangle \cdot \langle sr^l \rangle$, allora esiste $t \in \mathbb{Z}$ tale che

$$sr^h = (r^m)^t sr^l \iff sr^h = s^2 r^{mt} sr^l \iff r^h = r^{-mt+l} \iff h \equiv l - mt \mod n$$

da cui ricaviamo $h \equiv l \mod m$ in quanto $m \mid n$. Ma allora $h = l$ dato che $0 \leqslant h < k$ e $0 \leqslant l < m$.

□

Lemma 3.15

Dati un gruppo G e A, B due sottogruppi tali che $A \leqslant B \leqslant G$, se $B \trianglelefteq G$ e A è caratteristico in B allora $A \trianglelefteq G$.

Dimostrazione. Fissato $g \in G$, consideriamo l'omomorfismo di coniugio

$$\varphi_g : G \longrightarrow G : x \longmapsto gxg^{-1}$$

poiché $B \trianglelefteq G$ è ben definita la restrizione $\varphi_{g|B} \in \operatorname{Aut}(B)$. Dal momento che A è un sottogruppo caratteristico di B abbiamo che $\varphi_{g|B}(A) = \varphi_g(A) = A$, pertanto $A \trianglelefteq G$. □

Corollario 3.16

Ogni sottogruppo di $\mathcal{R}$ è normale in D_n.

Dimostrazione. Siano $\langle r^k \rangle$ un sottogruppo di $\mathcal{R}$ e $\varphi \in \operatorname{Aut}(\mathcal{R})$, allora $\varphi(\langle r^k \rangle) = \langle r^k \rangle$ in quanto φ preserva l'ordine del sottogruppo e $\langle r^k \rangle$ è l'unico sottogruppo di $\mathcal{R}$ di tale ordine ($\mathcal{R}$ è ciclico), pertanto $\langle r^k \rangle$ è caratteristico in $\mathcal{R}$. Poiché $\mathcal{R}$ è un sottogruppo normale di D_n, per il Lemma 2.15 abbiamo $\langle r^k \rangle \trianglelefteq D_n$. □

Osservazione 3.17 — $\mathcal{R}$ è caratteristico in D_n per $n \geqslant 3$. Infatti se $\mathcal{R} = \langle r \rangle$, necessariamente $\operatorname{ord}(r) = \operatorname{ord}(\varphi(r))$, da cui $|\langle \varphi(r) \rangle| = n$. Se fosse $\varphi(r) \notin \mathcal{R}$ avremmo $\operatorname{ord}(\varphi(r)) = 2$, quindi $|\varphi(r)| = n = 2$, che è assurdo in quanto $|D_n| = 2n \geqslant 6$. Questo non è vero per D_2, che contiene una rotazione e due simmetrie. Poiché $\operatorname{Aut}(D_2) \cong S_3$, esiste un automorfismo che manda la rotazione in una riflessione, quindi che non fissa $\mathcal{R}$.

Corollario 3.18

Per $k \mid n$ e $0 \leqslant h < k$, il sottogruppo $H_{k,h} = \langle r^k, sr^h \rangle$ è normale in D_n se e solo se $r, s \in N_{D_n}(H_{k,h})$.

Dimostrazione.

- Se $H_{k,h} \trianglelefteq D_n$ allora $N_{D_n}(H_{k,h}) = D_n$, in particolare $r, s \in N_{D_n}(H_{k,h})$;
- se $r, s \in N_{D_n}(H_{k,h})$, poiché il normalizzatore è un sottogruppo di D_n abbiamo che $D_n = \langle r, s \rangle \subseteq N_{D_n}(H_{k,h})$, pertanto $H_{k,h} \trianglelefteq D_n$.

□

Vediamo effettivamente quali sono i sottogruppi normali della forma $\langle r^k, sr^h \rangle$. Consideriamo gli automorfismi di coniugio

$$\varphi_s : D_n \longrightarrow D_n : x \longmapsto sxs^{-1} \qquad \varphi_r : D_n \longrightarrow D_n : x \longmapsto rxr^{-1}$$

e sia $x_1^{\pm 1} \dots x_m^{\pm 1} \in H_{k,h} = \langle r^k, sr^h \rangle$, allora

$$\varphi_s(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_s(x_1)^{\pm 1} \dots \varphi_s(x_m)^{\pm 1} \in \langle srs, r^h s^{-1} \rangle = \langle sr^k s, r^h s^{-1} \rangle = \langle r^k, sr^{-h} \rangle$$

$$\varphi_r(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_r(x_1)^{\pm 1} \dots \varphi_r(x_m)^{\pm 1} \in \langle r^k, rsr^{h-1} \rangle = \langle r^k, sr^{h-2} \rangle$$

Pertanto $H_{k,h} \trianglelefteq D_n$ se e solo se $\langle r^k, sr^{h-2} \rangle = \langle r^k, sr^{-h} \rangle = \langle r^k, sr^h \rangle$, se e solo se $h \equiv h - 2 \mod k$, cioè $k \in \{1, 2\}$.

- Se $k = 1$ allora $H_{k,h} = \langle r, s \rangle = D_n$;
- se $k = 2$ (e n pari) allora $H_{k,h} = \langle r^2, sr \rangle$ oppure $H_{k,h} = \langle r^2, s \rangle$.

Osservazione 3.19 — Il secondo caso si presenta solo se n è pari, questo corrisponde al fatto che in un poligono con un numero pari di lati gli assi di simmetria sono per metà passanti per i lati e metà passanti per i vertici opposti. In un poligono con un numero dispari di lati gli assi di simmetria sono tutti passanti per i lati.

§3.3 Classi di coniugio

Abbiamo visto che possiamo scrivere ogni elemento di D_n nella forma $s^h r^k$, dove s è una simmetria e r è una rotazione che genera $\mathcal{R}$, con $h \in \{0, 1\}$ e $k \in \{0, \dots, n-1\}$ in quanto $\operatorname{ord}(s) = 2$ e $\operatorname{ord}(r) = n$. Inoltre tutti gli elementi della forma sr^h hanno ordine 2.

Consideriamo la classe di coniugio di r, $C_r = \{grg^{-1} \mid g \in D_n\}$, fissato $g \in D_n$ abbiamo due possibili valori per grg^{-1}:

- se $g \in \mathcal{R}$ allora g è una potenza di r, pertanto i due elementi commutano e si ha $grg^{-1} = r$;
- se $g \notin \mathcal{R}$ allora $g = sr^h$ con $h \in \mathbb{Z}$, quindi

$$(sr^h)r(sr^h)^{-1} = (sr^h)r(sr^h) = sr^{h+1}sr^h = s^2 r^{-1-h} r^h = r^{-1}$$

cioè $C_r = \{r, r^{-1}\}$. In modo analogo si mostra che $C_{r^k} = \{r^k, r^{-k}\}$ per ogni $k \in \mathbb{Z}$.

Osservazione 3.20 — Se n è pari, scriviamo $n = 2m$ e consideriamo la classe di coniugio di r^m. Poiché $r^m \neq e$ e $r^{2m} = (r^m)^2 = e$ abbiamo che $\operatorname{ord}(r^m) = 2$, cioè $(r^m)^{-1} = r^m$. Allora $C_{r^m} = \{r^m\}$, pertanto abbiamo trovato un elemento del centro di D_n (infatti se G è un gruppo e $x \in G$, allora $x \in Z(G)$ se e solo se $C_x = \{x\}$).

Consideriamo adesso la classe di coniugio di sr^h, $C_{sr^h} = \{g(sr^h)g^{-1} \mid g \in D_n\}$, fissato $g \in D_n$ abbiamo due possibili valori per $g(sr^h)g^{-1}$:

- se $g \in \mathcal{R}$ allora $g = r^k$ con $k \in \mathbb{Z}$, pertanto
$$r^k(sr^h)r^{-k} = sr^{-k}r^hr^{-k} = sr^{h-2k}$$
- se $g \notin \mathcal{R}$ allora $g = sr^k$ con $k \in \mathbb{Z}$, pertanto
$$(sr^k)(sr^h)(sr^k)^{-1} = (sr^k)(sr^h)(sr^k) = sr^{2k-h}$$

cioè $C_{sr^k} = \{sr^{h-2k}, sr^{2k-h} \mid k \in \mathbb{Z}\}$.

Osservazione 3.21 — La classe di coniugio di sr^h contiene tutte le simmetrie in cui l'esponente di r ha la stessa parità di h. Se n è dispari tutte le simmetrie appartengono alla stessa classe, mentre se n è pari abbiamo due classi distinte: quella delle simmetrie rispetto agli assi passanti per i vertici opposti e quella delle simmetrie rispetto agli assi passanti per i lati.

§3.4 Legge di gruppo e omomorfismi

Se g è un elemento di D_n possiamo scrivere g in modo unico come s^ar^b con $a \in \{0,1\}$ e $b \in \{0,\dots,n-1\}$, utilizziamo questa proprietà per esplicitare la legge di gruppo di D_n. Fissati $g_1, g_2 \in D_n$, scriviamo $g_1 = s^{a_1}r^{b_1}$ e $g_2 = s^{a_2}r^{b_2}$ con $a_1, a_2 \in \{0,1\}$ e $b \in \{0,\dots,n-1\}$,
$$g_1g_2 = (s^{a_1}r^{b_1})(s^{a_2}r^{b_2}) = s^{a_1}s^{a_2}(s^{a_2}r^{b_1}s^{-a_2})r^{b_2} = s^{a_1}s^{a_2}\varphi_{s^{a_2}}(r^{b_1})r^{b_2}$$
dove $\varphi_{s^{a_2}}$ è l'automorfismo di coniugio per s^{a_2} (ricordiamo che $s^{a_2} = s^{-a_2}$). Poiché $\varphi_{s^{a_2}}$ è un omomorfismo e $\varphi_x \circ \varphi_y = \varphi_{xy}$ per ogni $x, y \in G$, abbiamo $(\varphi_{s^{a_2}}(r^{b_1})) = (\varphi_s^{a_2}(r))^{b_1}$, quindi
$$g_1g_2 = s^{a_1}s^{a_2}(\varphi_s^{a_2}(r))^{b_1}r^{b_2} = s^{a_1+a_2}r^{(-1)^{a_2}b_1+b_2}$$
Per l'unicità della scrittura che stiamo usando (scegliendo $a \in \{0,1\}$ e $b \in \{0,\dots,n-1\}$), possiamo identificare ogni elemento $g = s^ar^b \in D_n$ con la coppia (a,b), la legge di gruppo è quindi tale che
$$(a_1,b_1)(a_2,b_2) = (a_1+a_2, (-1)^{a_2}b_1 + b_2)$$

Usiamo il risultato appena ottenuto per descrivere gli omomorfismi da D_n in un qualsiasi gruppo G. Poiché ogni elemento $g \in D_n$ si scrive come s^ar^b, con $a, b \in \mathbb{Z}$, un omomorfismo $\varphi \in \operatorname{Hom}(D_,G)$ è univocamente determinato da $\varphi(r)$ e $\varphi(s)$: infatti
$$\varphi(g) = \varphi(s^ar^b) = \varphi(s)^a\varphi(r)^b$$
Poniamo $x = \varphi(s)$, $y = \varphi(r)$, necessariamente $\operatorname{ord}(x) \mid 2$ e $\operatorname{ord}(y) \mid n$, cioè $x^2 = e_G$ e $y^n = e_G$, inoltre
$$xyx^{-1} = \varphi(s)\varphi(r)\varphi(s)^{-1} = \varphi(srs^{-1}) = \varphi(r^{-1}) = \varphi(r)^{-1} = y^{-1}$$
Mostriamo che effettivamente queste condizioni sono anche sufficienti:

Proposizione 3.22
Dati un gruppo G e un'applicazione

$$\varphi : D_n \longrightarrow G : s^a r^b \longmapsto x^a y^b$$

dove $x = \varphi(s)$ e $y = \varphi(r)$, allora φ è un omomorfismo se e solo se $x^2 = e_G$, $y^n = e_G$ e $xyx^{-1} = y^{-1}$.

Dimostrazione. Mostriamo che tali condizioni sono sufficienti affinché φ sia un omomorfismo. Poiché $x^m = x^{-m}$ per ogni $m \in \mathbb{Z}$, fissati $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ abbiamo

$$\begin{aligned}(x^{a_1}y^{b_1})(x^{a_2}y^{b_2}) &= x^{a_1}x^{a_2}(x^{a_2}y^{b_1}x^{-a_2})y^{b_2} = x^{a_1+a_2}\varphi_{x^{a_2}}(y^{b_1})y^{b_2} = \\ &= x^{a_1+a_2}(\varphi_x^{a_2}(y))^{b_1}y^{b_2} = x^{a_1+a_2}y^{(-1)^{a_2}b_1}y^{b_2} = x^{a_1+a_2}y^{(-1)^{a_2}b_1+b_2}\end{aligned}$$

dove φ_g è l'automorfismo di coniugio per $g \in G$. Allora abbiamo che φ è un omomorfismo, infatti per ogni $h_1, h_2, k_1, k_2 \in \mathbb{Z}$

$$\begin{aligned}\varphi((s^{h_1}r^{k_1})(s^{h_2}r^{k_2})) &= \varphi(s^{h_1+h_2}r^{(-1)^{h_2}k_1+k_2}) = \\ &= x^{h_1+h_2}y^{(-1)^{h_2}k_1+k_2} = (x^{h_1}y^{k_1})(x^{h_2}y^{k_2}) = \varphi(s^{h_1}r^{h_2})\varphi(s^{h_2}r^{h_2})\end{aligned}$$

$\square$

§3.5 Automorfismi

Studiamo separatamente gli automorfismi di D_n per $n \geqslant 3$ e di D_2.
Per $n \geqslant 3$ consideriamo $\varphi \in \mathrm{Aut}(D_n)$, poiché $D_n = \langle r, s\rangle$ è sufficiente studiare le immagini di r, s per determinare φ. Osserviamo che necessariamente $\varphi(r) = r^k$ con $(n, k) = 1$, infatti φ deve preservare l'ordine di r e la sua immagine deve essere un generatore di $\mathcal{R}$, in quanto $\mathcal{R}$ è caratteristico in D_n è isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Per quanto riguarda $\varphi(s)$, se n è dispari allora le simmetrie sono gli unici elementi di ordine 2, pertanto $\varphi(s) = sr^h$ con $0 \leqslant h < n$. Se n è pari abbiamo apparentemente due possibilità:

(1) $\varphi(s) = sr^h$, con $0 \leqslant h < n$;

(2) $\varphi(s) = r^{\frac{n}{2}}$, se n è pari.

D'altra parte, se fosse $\varphi(s) = r^{\frac{n}{2}}$ allora φ non sarebbe né iniettiva né surgettiva, pertanto $\varphi(s) = sr^h$ con $0 \leqslant h \leq n$. Verifichiamo che φ è un omomorfismo, per la caratterizzazione che abbiamo dato sopra è sufficiente verificare che $\varphi(s)\varphi(r)\varphi(s)^{-1} = \varphi(r)^{-1}$:

$$\varphi(s)\varphi(r)\varphi(s)^{-1} = (sr^h)r^k(sr^h)^{-1} = sr^{h+k}r^{-h}s = sr^k s^{-1} = r^{-k} = \varphi(r)^{-1}$$

Inoltre φ è surgettiva, infatti $r^k, sr^h \in \mathrm{Im}\varphi$, cioè

$$\langle r^k, sr^h\rangle = \langle r, sr^h\rangle = \langle s, r\rangle = D_n \subseteq \mathrm{Im}\varphi$$

da cui $\mathrm{Im}\varphi = D_n$. Poiché D_n è finito abbiamo che φ è un automorfismo. Gli automorfismi di $D_n = \langle r, s\rangle$ quindi sono tutti e soli gli omomorfismi da D_n in D_n che mandano r in un generatore di $\mathcal{R}$, che sono $\phi(n)$, e s in un'altra simmetria, che sono n, pertanto $|\mathrm{Aut}(D_n)| = n\phi(n)$.

Per $n = 2$, sappiamo che $D_2 \cong (\mathbb{Z}/2\mathbb{Z})^2$, pertanto

$$\mathrm{Aut}(D_2) \cong \mathrm{Aut}((\mathbb{Z}/2\mathbb{Z})^2) \cong S_3$$

Alternativamente possiamo considerare $(\mathbb{Z}/2\mathbb{Z})^2$ come spazio vettoriale su $\mathbb{F}_2$, pertanto abbiamo

$$\mathrm{Aut}(D_2) \cong GL_2(\mathbb{F}_2)$$

Per quanto visto nella sezione (2), $GL_2(\mathbb{F}_2)$ contiene $(4-1)(4-2) = 6$ elementi, inoltre GL_2 non è un gruppo commutativo (con l'operazione di prodotto tra matrici), pertanto $GL_2(\mathbb{F}_2) \cong S_3$. In particolare, gli elementi di $GL_2(\mathbb{F}_2)$ sono:

- $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, che è l'identità del gruppo;
- $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, che sono gli elementi di ordine 2 corrispondenti alle trasposizioni;
- $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ che sono gli elementi di ordine 3 corrispondenti ai 3-cicli.

§4 Automorfismi di un prodotto diretto

Consideriamo due gruppi finiti H, K, studiamo il gruppo degli automorfismi di $H \times K$. Chiaramente esiste un'inclusione di $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ in $\mathrm{Aut}(H \times K)$ data dall'omomorfismo

$$\iota : \mathrm{Aut}(H) \times \mathrm{Aut}(K) \longrightarrow \mathrm{Aut}(H \times K) : (\varphi_1, \varphi_2) \longmapsto \varphi_1 \times \varphi_2$$

con

$$\varphi_1 \times \varphi_2 : H \times K \longrightarrow H \times K : (g_1, g_2) \longmapsto (\varphi_1(g_1), \varphi_2(g_2))$$

Mostriamo che ι è ben definita e che è un omomorfismo iniettivo:

- per ogni $(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, per ogni $(g_1, g_2), (h_1, h_2) \in H \times K$ abbiamo

$$\begin{aligned}(\varphi_1 \times \varphi_2)((g_1, g_2)(h_1, h_2)) = (\varphi_1(g_1 h_1), \varphi(g_2 h_2)) = (\varphi_1(g_1)\varphi_1(h_2), \varphi_2(g_2)\varphi_2(h_2)) = \\ = (\varphi_1(g_1), \varphi_2(g_2))(\varphi_1(h_1), \varphi_2(h_2)) = ((\varphi_1 \times \varphi_2)(g_1, g_2))((\varphi_1 \times \varphi_2)(h_1, h_2))\end{aligned}$$

  cioè $\varphi_1 \times \varphi_2$ è un omomorfismo. Inoltre

$$\ker(\varphi_1 \times \varphi_2) = \{(g_1, g_2) \in H \times K \mid (\varphi_1(g_1), \varphi_2(g_2)) = (e_H, e_K)\} = \{(0, 0)\}$$

  quindi $\varphi_1 \times \varphi_2 \in \mathrm{Aut}(H \times K)$ in quanto $H \times K$ è finito, pertanto ι è ben definita;

- per ogni $(\varphi_1, \varphi_2), (\psi_1, \psi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$, per ogni $(g_1, g_2) \in H \times K$ abbiamo

$$\begin{aligned}\iota((\varphi_1, \varphi_2)(\psi_1, \psi_2))(g_1, g_2) = \iota(\varphi_1\psi_1, \varphi_2\psi_2)(g_1, g_2) = (\varphi_1\psi_1 \times \varphi_2\psi_2)(g_1, g_2) = \\ = (\varphi_1(\psi_1(g_1)), \varphi_2(\psi_2(g_2))) = (\varphi_1 \times \varphi_2)(\psi_1(g_1), \psi_2(g_2)) = \\ = ((\varphi_1 \times \varphi_2)(\psi_1 \times \psi_2))(g_1, g_2) = (\iota(\varphi_1, \varphi_2)\iota(\psi_1\psi_2))(g_1, g_2)\end{aligned}$$

  cioè $\iota((\varphi_1, \varphi_2)(\psi_1, \psi_2)) = \iota(\varphi_1, \varphi_2)\iota(\psi_1, \psi_2)$, quindi ι è un omomorfismo;

- ι è iniettiva, infatti

$$\begin{aligned}\ker \iota = \{(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K) \mid \iota(\varphi_1, \varphi_2) = e_{\mathrm{Aut}(H \times K)}\} = \\ = \{(\varphi_1, \varphi_2) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K) \mid (\varphi_1(g_1), \varphi_2(g_2)) = (e_H, e_K)\ \forall (g_1, g_2) \in H \times K\}\end{aligned}$$

  Poiché gli unici elementi $\varphi_1 \in \mathrm{Aut}(H)$, $\varphi_2 \in \mathrm{Aut}(K)$ tali che $\varphi_1(H) = \{e_H\}$ e $\varphi_2(K) = \{e_K\}$ sono rispettivamente $e_{\mathrm{Aut}(H)}$, $e_{\mathrm{Aut}(K)}$ abbiamo

$$\ker \iota = \{(e_{\mathrm{Aut}(H)}, e_{\mathrm{Aut}(K)})\} = \{e_{\mathrm{Aut}(H \times K)}\}$$

Proposizione 4.1

Dati due gruppi finiti H, K, $\mathrm{Aut}(H) \times \mathrm{Aut}(K) \cong \mathrm{Aut}(H \times K)$ se e solo se $H \times \{e_K\}$ e $\{e_H\} \times K$ sono sottogruppi caratteristici di $H \times K$.

Dimostrazione. Sia ι l'immersione da $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ in $\mathrm{Aut}(H \times K)$ definita come sopra, se ι è surgettiva allora ogni elemento di
$Aut(H \times K)$ può essere scritto come $\varphi_1 \times \varphi_2$ con $\varphi_1 \in \mathrm{Aut}(H)$ e $\varphi_2 \in \mathrm{Aut}(K)$. Allora abbiamo

$$(\varphi_1 \times \varphi_2)(H \times \{e_K\}) = (\varphi_1(H), \varphi_2(\{e_K\})) = H \times \{e_K\}$$

$$(\varphi_1 \times \varphi_2)(\{e_K\} \times K) = (\varphi_1(\{e_H\}), \varphi_2(K)) = \{e_H\} \times K$$

cioè $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici in $H \times K$. Viceversa, se i due sottogruppi sono caratteristici, dato $\varphi \in \mathrm{Aut}(H \times K)$ poniamo $\varphi_1 \in \mathrm{Aut}(H)$ tale che $\varphi(g_1, e_K) = (\varphi_1(g_1), e_K)$ e $\varphi_2 \in \mathrm{Aut}(K)$ tale che $\varphi(e_H, g_2) = (e_H, \varphi_2(g_2))$ per ogni $g_1 \in H$, per ogni $g_2 \in K$ (questo possiamo farlo in quanto $H \times \{e_K\}$ e $\{e_H\} \times K$ sono caratteristici). Allora abbiamo

$$\varphi(g_1, g_2) = \varphi((g_1, e_K)(e_H, g_2)) = \varphi(g_1, e_K)\varphi(e_H, g_2) = \\ = (\varphi_1(g_1), e_K)(e_H, \varphi_2(g_2)) = (\varphi_1(g_1), \varphi_2(g_2)) = (\varphi_1 \times \varphi_2)(g_1, g_2)$$

cioè ι è surgettiva e quindi un isomorfismo tra $\mathrm{Aut}(H) \times \mathrm{Aut}(K)$ e $\mathrm{Aut}(H \times K)$. □

Esempio 4.2

Consideriamo il gruppo $G = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, osserviamo che il sottogruppo $\{0\} \times \mathbb{Z}/n\mathbb{Z}$ è caratteristico in quanto un automorfismo φ di G deve preservare gli ordini degli elementi, in particolare quello di un generatore, quindi l'immagine di un generatore è un altro generatore del sottogruppo. Poiché gli elementi di G di ordine finito sono tutti della forma $(0, d)$ abbiamo che $\varphi(\{0\} \times \mathbb{Z}/n\mathbb{Z}) = \{0\} \times \mathbb{Z}/n\mathbb{Z}$. Viceversa, l'immagine di φ su un generatore di $\mathbb{Z} \times \{0\}$, ad esempio $\varphi(1, 0)$, è della forma (a, b), e questo implica che $\mathbb{Z} \times \{0\}$ non è caratteristico. Se φ è surgettivo, necessariamente esiste $(x, y) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ tale che $\varphi(x, y) = (\pm 1, 0)$, da cui, posti $\varphi(1, 0) = (a, b)$ e $\varphi(0, 1) = (0, d)$ con n e d coprimi, abbiamo

$$\varphi(x, y) = \varphi(x(1, 0) + y(0, 1)) = x\varphi(1, 0) + y\varphi(0, 1) = \\ = x(a, b) + y(0, d) = (xa, xb + yd) = (\pm 1, 0) \iff a = \pm 1$$

Viceversa, se $a = \pm 1$ allora φ è surgettiva, infatti per ogni $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, scegliendo $x = x_0 a$ e $y \equiv d^{-1}(y_0 - x_0 ab) \mod n$ abbiamo

$$\varphi(x, y) = (x_0 a^2, x_0 ab + dd^{-1}(y_0 - x_0 ab)) = (x_0, y_0)$$

e questo ci permette di concludere che $\mathbb{Z} \times \{0\}$ non è un sottogruppo caratteristico. In questo caso abbiamo solo un'immersione del gruppo $\mathrm{Aut}(\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ dentro a $\mathrm{Aut}(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$, in quanto gli automorfismi che mandano $(\pm 1, 0)$ in (a, b) con $a = \pm 1$ e $b \neq 0$ non possono essere ristretti ad automorfismi di $\mathbb{Z} \times \{0\}$.

È utile riuscire a determinare se i sottogruppi $H \times \{e_K\}$, $\{e_H\} \times K$ sono caratteristici in $H \times K$, da cui il seguente risultato:

Proposizione 4.3

Dati due gruppi finiti H, K, se $(|H|, |K|) = 1$ allora $H \times \{e_K\}$ e $\{e_H\} \times K$ sono sottogruppi caratteristici di $H \times K$.

Dimostrazione. Poniamo $m = |H|$, $n = |K|$, $S = \{(g_1, g_2) \in H \times K \mid (g_1, g_2)^n = (e_H, e_K)\}$, osserviamo che $H \times \{e_K\} = S$, infatti $H \times \{e_K\} \subseteq S$ in quanto tutti gli elementi di $H \times e_K$ hanno ordine che divide n. D'altra parte dato $(g_1, g_2) \in S$, se $\mathrm{ord}(g_1, g_2) \mid n$ allora $\mathrm{ord}(g_1) \mid n$ e $\mathrm{ord}(g_2) \mid n$, ma $\mathrm{ord}(g_2) \mid m$ per il Teorema di Lagrange, quindi $\mathrm{ord}(g_2) = 1$ e $S \subseteq H \times \{e_K\}$, da cui l'uguaglianza. Con un ragionamento analogo possiamo caratterizzare $\{e_H\} \times K$ come

$$\{e_H\} \times K = \{(g_1, g_2) \in H \times K \mid (g_1, g_2)^m = (e_H, e_K)\}$$

Poiché un automorfismo di $H \times K$ deve preservare gli ordini degli elementi, per la caratterizzazione data abbiamo che i due sottogruppi sono caratteristici. □

Corollario 4.4

Se $m, n \geqslant 2$ sono interi coprimi allora

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$$

§5 Gruppo derivato

Definizione 5.1. Dati un gruppo G e x, y elementi di G, chiamiamo **commutatore** di x e y l'elemento $[x, y] = xyx^{-1}y^{-1}$. Chiamiamo **sottogruppo derivato** di G, oppure **sottogruppo dei commutatori** di G il sottogruppo

$$G' = \langle \{[x, y] \mid x, y \in G\} \rangle$$

Osservazione 5.2 — $[x, y] = e$ se e solo se x e y commutano.

Proposizione 5.3
Dato un gruppo G, valgono i seguenti fatti:

(1) G' è un sottogruppo caratteristico di G;

(2) ${}^{G}\!/_{G'}$ è un gruppo abeliano;

(3) dato A un gruppo abeliano e $\varphi \in \text{Hom}(G, A)$, allora $G' \subseteq \ker \varphi$.

Dimostrazione. Mostriamo le affermazioni singolarmente:

(1) consideriamo $\varphi \in \text{Aut}(G)$, poiché φ preserva la struttura di gruppo è sufficiente descrivere come φ agisce sui generatori di G' per determinare $\varphi(G')$. Fissati $x, y \in G$, abbiamo

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

pertanto $\varphi(G') \subseteq G'$, da cui l'uguaglianza in quanto φ è bigettiva;

(2) dati $x, y \in G$, $xG' \cdot yG' = yG' \cdot xG'$ se e solo se $xyG' = yxG'$, che è equivalente a richiedere $xyx^{-1}y^{-1}$. Dato che effettivamente $xyx^{-1}y^{-1} = [x, y]$ è un elemento di G' abbiamo che ${}^{G}\!/_{G'}$ è abeliano;

(3) dati $x, y \in G$, abbiamo

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

e questo coincide con l'identità di A in quanto A è abeliano. Poiché l'immagine di φ è un sottogruppo di A allora $G' \subseteq \ker \varphi$, in quanto il commutatore di ogni coppia di elementi di G è contenuto in $\ker \varphi$.

□

Osservazione 5.4 — Come conseguenza del Primo Teorema di Omomorfismo abbiamo che ${}^{G}\!/_{G'}$ è isomorfo al "più grande" sottogruppo abeliano di G, o analogamente che G' è il "più piccolo" sottogruppo di G che produce un quoziente abeliano. In questo senso, G' misura quanto è abeliano il gruppo G.

Osservazione 5.5 — Dato A un gruppo abeliano, il Primo Teorema di Omomorfismo produce una bigezione naturale tra $\mathrm{Hom}(G, A)$ e $\mathrm{Hom}\left({}^{G}\!/_{G'}, A\right)$. Consideriamo infatti $\varphi \in \mathrm{Hom}(G, A)$, $\pi_{G'} : G \longrightarrow {}^{G}\!/_{G'}$ la proiezione al quoziente e $\overline{\varphi} : {}^{G}\!/_{G'} \longrightarrow A$, il Teorema fornisce un'unico omomorfismo $\overline{\varphi} : {}^{G}\!/_{G'} \longrightarrow A$ che rende commutativo il diagramma

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, two heads, "\pi_{G'}"'] \arrow[dr, phantom, "\circlearrowleft"] & A \\
{}^{G}\!/_{G'} \arrow[ur, hook, "\overline{\varphi}"'] &
\end{tikzcd}$$

Viceversa, dato un omomorfismo $\overline{\varphi} : {}^{G}\!/_{G'} \longrightarrow A$ otteniamo un'unico omomorfismo $\varphi : G \longrightarrow A$ con la composizione $\pi_{G'} \circ \overline{\varphi}$.

Esempio 5.6

Consideriamo il gruppo S_3, chiaramente $(S_3)' \neq \{id\}$ in quanto ${}^{S_3}\!/_{\langle id \rangle} \cong S_3$ che non è abeliano, pertanto abbiamo due possibilità: $(S_3)' = S_3$ oppure $(S_3)' = \langle (1\ 2\ 3) \rangle$[a]. D'altra parte ${}^{S_3}\!/_{\langle (1\ 2\ 3) \rangle}$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$, che è abeliano, pertanto $(S_3)'$ è contenuto in $\langle (1\ 2\ 3) \rangle$, da cui necessariamente $(S_3)' = \langle (1\ 2\ 3) \rangle$. Più in generale vedremo che $(S_n)' = \mathcal{A}_n$, dove $\mathcal{A}_n$ è il sottogruppo di S_n delle permutazioni pari (sappiamo già che $(S_n)' \subseteq \mathcal{A}_n$ in quanto ${}^{S_n}\!/_{\mathcal{A}_n} \cong \mathbb{Z}/2\mathbb{Z}$).

[a] Gli unici sottogruppi normali di S_3 sono $\{id\}$, $\langle (1\ 2\ 3) \rangle$, S_3.

§6 Azioni di gruppo

§6.1 Azioni transitive

Definizione 6.1. Siano G un gruppo e X un insieme, un'azione

$$\varphi : G \longrightarrow S(X) : g \longmapsto \varphi_g$$

si dice **transitiva** se per ogni $x, y \in X$ esiste $g \in G$ tale che $\varphi_g(x) = y$, equivalentemente se $\operatorname{Orb}(x) = G$ per ogni $x \in X$. Diciamo anche che G **agisce transitivamente** su X tramite φ.

Lemma 6.2

Dato G un gruppo finito e $H \lneq G$ un suo sottogruppo proprio, allora

$$G \neq \bigcup_{g \in G} gHg^{-1}$$

Dimostrazione. Poniamo $K = \bigcup_{g \in G} gHg^{-1}$, osserviamo che gli elementi della forma xHx^{-1} con $x \in N_G(H)$ contribuiscono una sola volta all'unione, in quanto $xHx^{-1} = H$, pertanto K è unione di $[G : N_G(H)] = \dfrac{|G|}{|N_G(H)|}$ elementi distinti[3]. Poiché $H \subseteq N_G(H)$ e $|gHg^{-1}| = |H|$ per ogni $g \in G$, possiamo stimare la cardinalità di K nel seguente modo

$$|K| \leq \frac{|G|}{|N_G(H)|}|H| \leq \frac{|G|}{|H|}|H| = |G|.$$

D'altra parte, per il Principio di Inclusione-Esclusione abbiamo che $|K|$ è somma delle cardinalità dei singoli termini dell'unione se e solo se l'unione è disgiunta, ma questo è falso in quanto ogni classe di coniugio di H contiene l'identità del gruppo, quindi $|K| < |G|$, cioè $G \neq K$. □

Proposizione 6.3

Dati un gruppo G e un insieme G, se

$$\varphi : G \longrightarrow S(X) : g \longmapsto \varphi_g$$

è un'azione transitiva valgono i seguenti fatti:

(1) per ogni $x, y \in X$ esiste $g \in G$ tale che $g \operatorname{St}(x) g^{-1} = \operatorname{St}(y)$;

(2) se $|X| \geqslant 2$ allora esiste $g \in G$ che agisce su X senza punti fissi, cioè tale che $\varphi_g(x) \neq x$ per ogni $x \in X$.

Dimostrazione. Mostriamo i due fatti singolarmente:

[3] Infatti, se $X = \{N \mid N \leqslant G\}$ e φ è l'azione di coniugio su X, per ogni $N \in X$ abbiamo $\operatorname{St}(N) = N_G(N)$ e $\operatorname{Orb}(N) = C_N = \{gNg^{-1} \mid g \in G\}$. Vale quindi la relazione $|G| = |C_N| \cdot |N_G(N)|$.

(1) sia $g \in G$ tale che $\varphi_g(x) = y$, dato $h \in g\,\mathrm{St}(x)g^{-1}$ esiste $w \in \mathrm{St}(x)$ tale che $h = gwg^{-1}$. Allora

$$\varphi_h(y) = \varphi_{gwg^{-1}}(y) = \varphi_g(\varphi_w(\varphi_h^{-1}(y))) = \varphi_g(\varphi_w(x)) = \varphi_g(x) = y$$

pertanto $g\,\mathrm{St}(x)g^{-1} \subseteq \mathrm{St}(y)$. Osservando che $\varphi_{g^{-1}}(y) = x$ e ragionando in modo simmetrico otteniamo l'inclusione $g^{-1}\,\mathrm{St}(y)g \subseteq \mathrm{St}(x)$, da cui $g\,\mathrm{St}(x)g^{-1} = \mathrm{St}(y)$;

(2) un elemento $g \in G$ con tali proprietà non può essere contenuto nello stabilizzatore di nessun elemento di X, cioè cerchiamo $g \in G$ tale che

$$g \in \bigcap_{x \in X} \mathrm{St}(x)^{\mathcal{C}}$$

che è equivalente a

$$g \notin \bigcup_{x \in X} \mathrm{St}(x) = \bigcup_{h \in G} h\,\mathrm{St}(x_0)h^{-1}$$

per il fatto precedente, fissato $x_0 \in G$. Osserviamo che $\mathrm{St}(x_0) \neq G$, infatti se fosse $\mathrm{St}(x_0) = G$ avremmo

$$|\operatorname{Orb}(x_0)| = \frac{|G|}{|\operatorname{St}(x_0)|} = 1$$

ma questo è assurdo in quanto $\operatorname{Orb}(x_0) = X$ per la transitività di φ e $|X| \geqslant 2$. Allora per il Lemma 5.2 abbiamo

$$G \neq \bigcap_{h \in G} h\,\mathrm{St}(x_0)h^{-1}$$

pertanto esiste almeno un elemento $g \in G$ con la proprietà voluta.

□

Proposizione 6.4

Dato G un gruppo finito e $H \lneq G$ un sottogruppo proprio, se $[G : H] = p$ con p il più piccolo primo che divide l'ordine di G allora H è normale in G.

Dimostrazione. Consideriamo l'azione di G sull'insieme quoziente ${}^{G}\!/\!_{H}$

$$\psi : G \longrightarrow S\left({}^{G}\!/\!_{H}\right) : g \longmapsto \psi_g$$

con

$$\psi_g : {}^{G}\!/\!_{H} \longrightarrow {}^{G}\!/\!_{H} : g'H \longmapsto gg'H$$

Poiché l'immagine di ψ è un sottogruppo di $S\left({}^{G}\!/\!_{H}\right)$, che è isomorfo a S_p, abbiamo che $|\mathrm{Im}\psi| \mid p!$, inoltre $|\mathrm{Im}\psi| = \dfrac{|G|}{|\ker\psi|}$ come conseguenza del Primo Teorema di Omomorfismo. Pertanto $|\mathrm{Im}\psi| \mid (p!, |G|) = p$, in quanto p è il più piccolo primo che divide $|G|$, quindi $|\mathrm{Im}\psi| \in \{1, p\}$. □