Algebra 2 — Teoria dei Gruppi

Alberto Canonaco (alberto.canonaco@unipv.it)
Università di Pavia — Corso di Laurea in Matematica

Ultima revisione: 11 luglio 2024

Sommario

Queste pagine derivano dalle slides del corso di Algebra 2 tenuto negli anni 2020/2021, che si possono ancora reperire all'indirizzo https://www-dimat.unipv.it/canonaco/2020-2021/alg2.html.

- Integrazioni con note di studenti e con corsi degli anni successivi. Per questo motivo, la presentazione del materiale ha subito qualche cambiamento e delle dimostrazioni sono state cambiate.
- Inseriti alcuni richiami più o meno estesi ad argomenti di Algebra 1.
- Bibliografia estesa. Segnaliamo in particolare [Tsu], una risorsa preziosa di esercizi di varia difficoltà.

Testi di riferimento

[Alu] P. Aluffi. *Algebra: Notes from the Underground*. In particolare i capitoli 11 e 12. Cambridge University Press.

[Her] I.N. Herstein. *Algebra*. In particolare le sezioni 2.9, 2.11, 2.12 e 5.7. Editori Riuniti University Press.

[Mil] James S. Milne. *Group Theory*. In particolare i capitoli 3, 4, 5 e 6. URL: https://www.jmilne.org/math/CourseNotes/GT.pdf.

[Tsu] Yu Tsumura. *Problems in Mathematics – Group Theory*. URL: https://yutsumura.com/category/group-theory/.

Indice

1 Azioni di gruppi

Definizione 1.1. Un'*azione* di un gruppo G su un insieme X è una funzione

$$\phi : G \times X \to X$$

tale che:

1. $\phi(gh, x) = \phi(g, \phi(h, x))$ per ogni $g, h \in G$ e $x \in X$
2. $\phi(1, x) = x$ per ogni $x \in X$.

Un G-*insieme* è il dato di un insieme X e di un'azione $\phi : G \times X \to X$, e viene indicato come una coppia (X, ϕ). Spesso si usa la notazione moltiplicativa: spesso, al posto di $\phi(g, x)$, si usa scrivere $g \cdot x$ o addirittura gx indicare l'azione di un elemento g del gruppo su un elemento sull'elemento x dell'insieme. A livello teorico, si riducono il numero di parentesi e possono risultare più agevoli comunque: possiamo dire "sia X un G-insieme ..." nominando solo l'insieme e senza destinare un nome specifico all'azione $G \times X \to X$ perché stiamo assumendo che lavoreremo con queste ultime notazioni.

Proposizione 1.2 (Azioni come omomorfismi)**.** Sia X un G-insieme. Allora per ogni $g \in G$ la funzione

$$\phi(g) : X \to X\,,\ x \mapsto gx$$

è biunivoca. In tal caso, si ha l'omomorfismo di gruppi $\phi : G \to S(X)$ tale che $\phi(g)$ manda x in gx. Viceversa, dato un omomorfismo di gruppi $\phi : G \to S(X)$, la funzione

$$G \times X \to X\,,\ (g, x) \mapsto \phi(g)(x)$$

definisce un'azione del gruppo G sull'insieme X.

Quindi un'azione è una funzione $G \times X \to X$ con le proprietà della Definizione 1.1 oppure un omomorfismo di gruppi $G \to S(X)$ come nella Proposizione 1.2. Questa proposizione mostra come si può passare da una impostazione all'altra.

Dimostrazione. A causa di (1 in Definizione 1.1), per ogni $g, h \in G$ e per ogni $x \in X$ si ha

$$\phi(gh)(x) = (gh)x = g(hx) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x)$$

quindi $\phi(gh) = \phi(g) \circ \phi(h)$. Inoltre, per (2 in Definizione 1.1), abbiamo che

$$\phi(1)(x) = 1x = x = \mathrm{id}_X(x)$$

per cui $\phi(1) = \mathrm{id}_X$. Così stando le cose, abbiamo

$$\phi(g) \circ \phi\left(g^{-1}\right) = \phi\left(g^{-1}\right) \circ \phi(g) = \mathrm{id}_X$$

e questo basta per dimostrare che $\phi(g)$ è biunivoca, con inversa $\phi\left(g^{-1}\right)$. Riassumendo, $\phi(g) : X \to X$ è biunivoca e $\phi(gh) = \phi(g) \circ \phi(h)$ per ogni $g, h \in G$, e tanto basto per poter introdurre un omomorfismo di gruppi

$$\phi : G \to S(X)\,,\ g \mapsto \phi(g).$$

Viceversa, se $\phi : G \to S(X)$ è un omomorfismo di gruppi, allora per ogni $g, h \in G$ e per ogni $x \in X$

$$(gh)x = \phi(gh)(x) = (\phi(g) \circ \phi(h))(x) = \phi(g)(\phi(h)(x)) = g(hx),$$

vale a dire (1 in Definizione 1.1). Inoltre $\phi(1) = \mathrm{id}_X$ poiché ϕ è omomorfismo, per cui $1x = \phi(1)(x) = \mathrm{id}_X(x) = x$, cioè (2 in Definizione 1.1). □

Ecco una lista di semplici esempi. Sottolineiamo che in questi esempi si presentano le cose in entrambe le formulazioni della definizione di azione. In ogni caso, è bene averli a mente, visto alcuni verranno riciclati per ottenere risultati raffinati come i Teoremi di Sylow.

Esempio 1.3. L'*azione banale* non muove gli elementi dell'insieme, cioè quella definita da

$$gx = x \quad \text{per ogni } g \in G, x \in X.$$

Nella riformulazione della Proposizione 1.2, questa azione è l'omomorfismo $G \to S(X)$ che manda tutti di elementi di G in id_X.

Esempio 1.4. Se G è un sottogruppo di $S(X)$, allora X è un G-insieme con l'omomorfismo di inclusione $G \hookrightarrow S(X)$. Qui abbiamo dato l'azione come nella Proposizione 1.2. Se vogliamo l'azione così come è stata espressa nella Definizione 1.1, allora possiamo scriverla come

$$\begin{aligned} G \times X &\to X \\ (f, x) &\mapsto f(x). \end{aligned}$$

Quando un gruppo G agisce su un insieme X e G è un sottogruppo di $S(X)$, allora quando diciamo che "X è un G-insieme" intendiamo X è munito dell'azione vista nel precedente esempio. Salvo avviso contrario, ovviamente.

Esempio 1.5. Se H è un sottogruppo di G, allora un G-insieme X con un omomorfismo $\phi : G \to S(X)$ è anche un H-insieme con $\phi|_H : H \to S(X)$. Più in generale, dato un omomorfismo di gruppi $f : G' \to G$, X è anche un G'-insieme con $\phi \circ f : G' \to S(X)$. Vediamo come si scrive $\phi \circ f$ nell'altra veste, usando la Proposizione 1.2:

$$\begin{aligned} \widehat{\phi \circ f} : G' \times X &\to X \\ (g', x) &\mapsto \phi(f(g'))(x) \end{aligned}$$

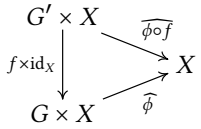
Se facciamo lo stesso con l'omomorfismo ϕ, abbiamo

$$\begin{aligned} \widehat{\phi} : G \times X &\to X \\ (g, x) &\mapsto \phi(g)(x) \end{aligned}$$

Da questo deduciamo che

$$\widehat{\phi \circ f}\,(g', x) = \widehat{\phi}\,(f\,(g'), x) \quad \text{per ogni } g' \in G', x \in X.$$

In diagrammi succede questo: commuta



I gruppi possono anche agire su se stessi, o più precisamente sull'insieme dei propri elementi.

Esempio 1.6 (Azione di coniugio)**.** Un'azione che è bene ricordare anche per il seguito è l'*azione di coniugio* di un gruppo G su di sé, definita da

$$\begin{aligned} G \times G &\to G \\ (g, a) &\mapsto gag^{-1}. \end{aligned}$$

Infatti vale (1 in Definizione 1.1) perché $(gh)a(gh)^{-1} = g(hah^{-1})g^{-1}$ per ogni $g, h, a \in G$ e (2 in Definizione 1.1) perché $1a1^{-1} = a$. L'immagine dell'azione espressa come omomorfismo di gruppi $G \to S(G)$ è il sottogruppo degli *automorfismi interni* e si indica con $\mathrm{Int}(G)$. Come suggerisce il nome, c'è questa relazione di inclusione tra sottogruppi:

$$\mathrm{Int}(G) < \mathrm{Aut}(G) < S(G)$$

dove $\mathrm{Aut}(G)$ è il gruppo degli *automorfismi* di G.

Esempio 1.7 (Azione di traslazione)**.** L'*azione per traslazione a sinistra* di G su G è definita da

$$G \times G \to G$$
$$(g, a) \mapsto ga.$$

Vale (1 in Definizione 1.1) perché il prodotto di G è associativo e (2 in Definizione 1.1) perché 1 è elemento neutro. Il corrispondente omomorfismo di gruppi $L : G \to S(G)$ è iniettivo, e questo fatto è noto come Teorema di Cayley. Per quanto banale possa sembrare, dice che in $S(G)$ si può trovare una copia di G.

Esempio 1.8 (Traslazione di classi laterali)**.** Sia H un sottogruppo di un qualunque gruppo G, e consideriamo la famiglia delle classi laterali sinistre G/H.[1] Abbiamo l'azione

$$G \times G/H \to G/H$$
$$(g, hH) \mapsto g(hH) = (gh)H$$

La verifica che questa è un'azione è lasciata per esercizio. Indicheremo ancora con $L : G \to S(G/H)$ il corrispondente omomorfismo di gruppi, che in generale non è iniettivo.

Esempio 1.9. Un'azione di G su X ne induce sempre di G su $\mathcal{P}(X)$:

$$G \times \mathcal{P}(X) \to \mathcal{P}(X)$$
$$(g, A) \mapsto gA := \{gx : x \in A\}$$

La verifica che questa è davvero un'azione è lasciata per esercizio.

Definizione 1.10. Un sottoinsieme A di un G-insieme X è *G-stabile* o *G-invariante* se $gA = A$ per ogni $g \in G$.

Osservazione 1.11. Un sottoinsieme G-stabile di un G-insieme è in modo naturale un G-insieme per restrizione dell'azione a $G \times A$.

Osservazione 1.12. In realtà per verificare se un insieme è G-stabile è sufficiente verificare una sola inclusione: un sottoinsieme A di un G-insieme X è G-stabile se e solo se $gA \subseteq A$ per ogni $g \in G$. L'inclusione opposta è infatti sempre vera: per ogni $g \in G$ si ha anche (dato che $g^{-1}A \subseteq A$)

$$A = 1A = (gg^{-1})A = g(g^{-1}A) \subseteq gA.$$

Nel seguente esempio facciamo vedere come alcuni concetti della teoria dei gruppi possono essere ridefiniti in termini di stabilità sotto certe azioni.

1. Ricordiamo che in generale c'è una biezione tra la famiglia delle classi laterali sinistre e quella delle classi laterali destre: per questa ragione, quando scriviamo G/H possiamo intendere una qualsiasi di queste due famiglie. Se in più H è normale, allora $gH = Hg$ per goni $g \in G$ e le due famiglie coincidono. In questo esempio, per semplicità, lo usiamo per indicare l'insieme delle classi laterali sinistre.

Esempio 1.13 (Sottogruppi normali e sottogruppi caratteristici)**.** Sia G un gruppo e H un suo sottogruppo.

- Ricordiamo che H è normale in G se e solo se $gHg^{-1} = H$ per ogni $g \in G$. Precedentemente abbiamo incontrato l'azione di coniugio (Esempio 1.6): è immediato quindi constatare che H è un sottogruppo normale di G se e solo se H è un sottogruppo stabile sotto l'azione di coniugio. Abbiamo visto anche nell'Esempio 1.4 che possiamo definire l'azione $\mathrm{Int}(G) \times G \to G$ che manda (f, g) in $f(g)$. Pertanto, H è un sottogruppo normale di G se e solo se è un sottogruppo stabile sotto l'azione appena menzionata.
- Un sottogruppo H di G è detto *caratteristico* qualora $\mathrm{im}\, f = G$ per ogni $f \in \mathrm{Aut}(G)$. Sempre richiamando l'Esempio 1.4, possiamo introdurre l'azione $\mathrm{Aut}(G) \times G \to G$ che manda (f, g) in $f(g)$. In questo caso, H è *caratteristico* in G se e solo se H è stabile sotto questa azione.[2] [3]

Definizione 1.14 (Morfismi di G-insiemi)**.** Se X e Y sono G-insiemi, una funzione $f : X \to Y$ è un *morfismo* di G-insiemi (o di azioni di G) qualora

$$f(gx) = gf(x) \quad \text{per ogni } g \in G, x \in X.$$

f è un *isomorfismo* di G-insiemi se è anche biunivoco.

Osservazione 1.15. id_X è un isomorfismo. Se f è un isomorfismo, anche f^{-1} lo è. La composizione di (iso)morfismi è un (iso)morfismo. Un morfismo $f : X \to Y$ è un isomorfismo se e solo se esiste un morfismo $f' : Y \to X$ tale che $f' \circ f = \mathrm{id}_X$ e $f \circ f' = \mathrm{id}_Y$. La relazione di isomorfismo è di equivalenza.

Esempio 1.16. Se A è un sottoinsieme G-stabile di un G-insieme X, l'inclusione $A \hookrightarrow X$ è un morfismo di G-insiemi.

Esempio 1.17. Sia G un gruppo e H un suo sottogruppo. Supponiamo G munito dell'azione di traslazione, vedi Esempio 1.7). Lo stesso si può fare con la famiglia di classi laterali G/H, ovvero richiama l'Esempio 1.8. La funzione

$$G \to G/H\,,\ a \mapsto aH$$

è un morfismo di G-insiemi, ed è un isomorfismo se e solo se H è banale.

2 Orbite e stabilizzatori

Definizione 2.1 (Orbita di un elemento)**.** Su un G-insieme X si può assegnare la relazione di equivalenza definita da

$$x \sim y \iff \exists g \in G : y = gx.$$

(Verificare che sia effettivamente una relazione di equivalenza!) La classe di equivalenza di $x \in X$ sotto questa relazione è il sottoinsieme

$$Gx := \{gx : g \in G\}$$

di X e si chiama *orbita* di x rispetto all'azione di G.

2. Osserviamo che ogni sottogruppo caratteristico è normale, ma non viceversa. Per esempio, i sottogruppi non banali di C_2^2 sono normali ma non caratteristici.
3. H è caratteristico in G se l'unico sottogruppo di G isomorfo a H è H stesso. Questo succede in particolare se H è l'unico sottogruppo di G del suo ordine. Quindi per esempio ogni sottogruppo di un gruppo ciclico finito è caratteristico.

[Inserire esempi di orbite delle azioni menzionate fino ad ora.]

Esempio 2.2. Ricolleghiamoci all'Esempio 1.7, mantenendone le notazioni. Qual è l'orbita di un elemento $a \in G$ (qui è l'*insieme* G)? L'orbita è semplicemente G: infatti

$$\{ga \mid g \in G\} = Ga = G.$$

Esempio 2.3. Richiama l'Esempio 1.8. L'orbita di $H \in G/H$ è G/H stesso.

Definizione 2.4 (Azioni transitive)**.** Un'azione di G su X è *transitiva* se X è costituito da una sola orbita. Si dice anche che X è un G-insieme *omogeneo*.

Esempio 2.5. Se $H < G$, il G-insieme G/H (vedi l'Esempio 1.8) è omogeneo: infatti gli elementi della famiglia G/H sono della forma gH per $g \in G$.

Esempio 2.6. Rispetto all'azione per coniugio di G su se stesso, l'orbita di $a \in G$ è la classe di coniugio di $a \in G$ è il sottoinsieme

$$[a]_G := \{gag^{-1} : g \in G\}.$$

Se si può sottintendere G senza creare problemi, scriviamo semplicemente $[a]$. Si ha $[a] = \{a\}$ se e solo se $a \in Z(G)$. Dunque l'azione è transitiva se e solo se G è banale. Avremo presto modo di capire quanto è importante la relazione di coniugio.

Definizione 2.7. Se X è un G-insieme, lo *stabilizzatore* di $x \in X$ è

$$\mathrm{Stab}(x) := \{g \in G : gx = x\}.$$

In altri termini, lo stabilizzatore di x è l'insieme dei $g \in G$ che tengono fisso x.

Proposizione 2.8. Se X è un G-insieme, allora $\mathrm{Stab}(x)$ è sottogruppo di G per ogni $x \in X$.

Dimostrazione. $1 \in \mathrm{Stab}(x)$. Verifichiamo che se $g, h \in \mathrm{Stab}(x)$ allora $gh^{-1} \in \mathrm{Stab}(x)$. Infatti

$$(gh^{-1})x = (gh^{-1})(hx) = g((h^{-1}h)x) = gx = x. \qquad \square$$

Definizione 2.9. Un'azione di G su X è *libera* qualora $\mathrm{Stab}(x) = \{1\}$ per ogni $x \in X$, ovvero se per ogni $x \in X$ si ha

$$gx = x \Rightarrow g = 1.$$

Un'azione di G su X è *fedele* quando $\mathrm{Stab}(x) = \{1\}$ per ogni $x \in X$ si ha

$$\bigcap_{x \in X} \mathrm{Stab}(x) = \{1\}.$$

Ovviamente ogni azione libera è fedele.

Osservazione 2.10. Se l'azione è assegnata come omomorfismo di gruppi $\phi : G \to S(X)$, allora

$$\ker \phi = \bigcap_{x \in X} \mathrm{Stab}(x).$$

In tal caso, l'azione è libera se e solo se l'omomorfismo è iniettivo.

Esempio 2.11 (Centralizzatore di un elemento)**.** Lo stabilizzatore di $a \in G$ rispetto all'azione per coniugio è il sottogruppo

$$C_G(a) := \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\}$$

e viene chiamato *centralizzatore* o (*centralizzante*) di a in G. Anche in questo caso, se non si creano problemi, abbandoniamo il pedice e scriviamo $C(a)$. Poiché $C(1) = G$, l'azione per coniugio è libera se e solo se $G = \{1\}$. D'altra parte l'azione è fedele se e solo se

$$\{1\} = \bigcap_{a \in G} C(a) = Z(G).$$

Dunque l'azione per coniugio è fedele ma non libera se $G \neq \{1\}$ e $Z(G) = \{1\}$ (per esempio, se $G = S_3$).

Esempio 2.12 (Normalizzatore di un sottogruppo)**.** Considerando $\mathcal{P}(G)$ come un G-insieme con l'azione indotta dal coniugio ("indotta" nel senso dell'Esempio 1.9), lo stabilizzatore di un sottogruppo H di G è il sottogruppo

$$N_G(H) := \{g \in G : gHg^{-1} = H\}$$

detto *normalizzatore* o (*normalizzante*) di H in G. Anche qui, se non ci sono problemi, scriviamo $N(G)$. $N(H)$ ha questo proprietà:

- $H \lhd N(H) < G$;
- Se $H \lhd K < G$, allora $K \subseteq N(H)$.

A parole: $N(H)$ è il più grande dei sottogruppi di G che ha come sottogruppo normale H. In particolare $N(H) = G$ se e solo se $H \lhd G$.

Proposizione 2.13. Se X è un G-insieme, per ogni $g \in G$ e per ogni $x \in X$

$$\operatorname{Stab}(gx) = g \operatorname{Stab}(x) g^{-1}.$$

In particolare $\operatorname{Stab}(gx) \cong \operatorname{Stab}(x)$.

Dimostrazione. Mostriamo che $\operatorname{Stab}(gx) \subseteq g \operatorname{Stab}(x) g^{-1}$. Sia $h \in \operatorname{Stab}(gx)$. Allora $gx = hgx$, da cui segue che $x = g^{-1}gx = g^{-1}hgx$, ovvero $h = gh'g^{-1} \in g \operatorname{Stab}(x) g^{-1}$. Proviamo l'inclusione opposta, $g \operatorname{Stab}(x) g^{-1} \subseteq \operatorname{Stab}(gx)$. Sia $h \in g \operatorname{Stab}(x) g^{-1}$, cioè $h = gh'g^{-1}$ per qualche $h' \in \operatorname{Stab}(x)$. Allora $hgx = gh'g^{-1}gx = gh'x = gx$, e quindi $h \in \operatorname{Stab}(gx)$. □

Esempio 2.14. Consideriamo l'azione di traslazione, richiama Esempio 1.8, e calcoliamo lo stabilizzatore di un qualsiasi elemento aH di G/H. Per la proposizione appena dimostrata si ha $\operatorname{Stab}(aH) = a \operatorname{Stab}(H) a^{-1}$. Qui lo stabilizzatore di H è facile da calcolare, cioè $\operatorname{Stab}(H) = \{g \in G : gH = H\} = H$. Quindi

$$\operatorname{Stab}(aH) = aHa^{-1}.$$

Ci servirà per il corollario che segue.

Proposizione 2.15 (Teorema di Cayley generalizzato)**.** Sia G un gruppo e H un suo sottogruppo. Allora

$$\ker\left(G \xrightarrow{L} S(G/H)\right) = \bigcap_{g \in G} gHg^{-1}$$

è il più grande sottogruppo normale di G contenuto in H.

Dimostrazione. Grazie all'esempio precedente, siamo in grado di scrivere:

$$\ker(L) = \bigcap_{g\in G} \mathrm{Stab}(gH) = \bigcap_{g\in G} g\,\mathrm{Stab}(H)g^{-1} = \bigcap_{g\in G} gHg^{-1}.$$

$\ker(L)$ è normale in G, in quanto nucleo di omomorfismo di gruppi, ed è dentro H. Resta da dimostrare che se $K \lhd G$ è contenuto in H, allora $K \subseteq \ker(L)$:

$$\underbrace{K = \bigcap_{g\in G} gKg^{-1}}_{K\lhd G} \subseteq \bigcap_{g\in G} gHg^{-1} = \ker(L). \qquad \square$$

Vediamo ora un'applicazione. Se $L : G \to S(G/H)$ è iniettivo, allora $G \cong \mathrm{im}(L) < S(G/H)$. Dunque, se $S(G/H)$ non ha sottogruppi isomorfi a G e se H è un sottogruppo *proprio* di G, possiamo concludere che

$$\{1\} \subsetneq \ker(L) \subseteq H \subsetneq G.$$

In particolare, G non è semplice, dato che $\ker(L) \lhd G$.

Corollario 2.16. Sia G un gruppo finito. Se ha un sottogruppo proprio H tale che $|G| \nmid [G : H]!$, allora G non è semplice.

Dimostrazione. Infatti, per il teorema di Lagrange, $S(G/H)$ non può proprio contenere sottogruppi di ordine $|G|$, quindi ricadiamo nelle considerazioni fatte poc'anzi. $\square$

Esempio 2.17. Sia $H < G$. Allora G non è semplice in ciascuno dei seguenti casi.

- $|G| = 36$, $|H| = 9$: $[G : H] = 4$ e $36 \nmid 4! = 24$.
- $|G| = 80$, $|H| = 16$: $[G : H] = 5$ e $80 \nmid 5! = 120$.
- $|G| = 150$, $|H| = 25$: $[G : H] = 6$ e $150 \nmid 6! = 720$.

Avremo modo di applicare ciò in seguito.

Se G è un gruppo che agisce su un insieme X, allora l'azione si può restringere sulle orbite, cioè ad un'azione $G \times Gx \to Gx$ per $x \in X$. In questo senso diciamo che Gx è un G-insieme. Per la proposizione che segue richiama anche l'Esempio 1.8.

Proposizione 2.18. Sia X un G-insieme. Allora per ogni $x \in X$ la funzione

$$f : G/\mathrm{Stab}(x) \to Gx,\ a\,\mathrm{Stab}(x) \mapsto ax$$

è un isomorfismo di G-insiemi. In particolare, se X è finito e $x \in X$, allora

$$|Gx| = [G : \mathrm{Stab}(x)].$$

Quindi le cardinalità dello stabilizzatore e dell'orbita di uno stesso elemento hanno un vincolo che può essere molto forte.

Dimostrazione. Scriviamo $\overline{a}$ al posto di $a\,\mathrm{Stab}(x)$. f è ben definita, poiché se $a' = ab$ per qualche $b \in \mathrm{Stab}(x)$ allora $a'x = (ab)x = a(bx) = ax$. Facciamo vedere che è un morfismo di G-insiemi: per ogni $g, a \in G$ si ha

$$f(g\overline{a}) = f(\overline{ga}) = (ga)x = g(ax) = gf(\overline{a}).$$

f è suriettiva, dato che per ogni $a \in G$ si ha $ax = f(\overline{a})$. f è anche iniettiva: se $a, a' \in G$ sono tali che $f(\overline{a}) = f(\overline{a'})$, cioè $ax = a'x$, allora $a^{-1}a' \in \mathrm{Stab}(x)$ e quindi $\overline{a} = \overline{a'}$. $\square$

Esempio 2.19. Quindi se, per esempio, se G è un gruppo finito, allora

- sotto l'azione di coniugio, si ha $|[a]| = [G : C(a)]$ per $a \in G$
- sotto l'azione di coniugio indotta sulle parti di G, si ha $|[H]| = [G : N(H)]$ per ogni sottogruppo H di G.

Teorema 2.20. Se X è un G-insieme finito e $X = \coprod_{i=1}^{n} Gx_i$ per degli x_1, ..., $x_n \in X$, allora

$$|X| = \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)].$$

Esercizio 2.21. Come diventa la formula se l'azione considerata è quella dell'Esempio 1.8?

Nel caso specifico dell'azione per coniugio la sostanza è la stessa, ma appare anche il centro e ha un nome suo.

Teorema 2.22 (Formula delle classi)**.** Se G è un gruppo finito e $G = \coprod_{i=1}^{n} [a_i]$ per degli a_1, ..., $a_m \in G \setminus Z(G)$ e degli a_{m+1}, ..., $a_n \in Z(G)$, allora

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C(a_i)].$$

Dimostrazione. Gli $a_{m+1}, \dots, a_n \in Z(G)$ hanno orbita banale, così come gli elementi di $Z(G)$: quindi possiamo concludere che $Z(G) = \{a_{m+1}, \dots, a_n\}$. Basta ora usare il corollario precedente. □

Come si può intuire, per cardinalità particolari le cose potrebbero semplificarsi o condurre a risultati particolari.

Definizione 2.23. Sia p un numero primo. Un *p-gruppo* è un gruppo di ordine una potenza di p.

Proposizione 2.24. I p-gruppi non banali hanno centro non banale.

Dimostrazione. Sia G un gruppo di cardinalità p^n con $n > 0$. Per l'equazione delle classi

$$|Z(G)| = |G| - \sum_{i=1}^{m} [G : C(a_i)]$$

per degli $a_1, \dots, a_m \in G$ che non stanno nel centro. Qui necessariamente per ogni i si ha $[G : C(a_i)] = p^{n_i}$ con $0 < n_i \leq n$. In particolare p divide $|G|$ e p divide tutti i termini $[G : C(a_i)]$. Allora $p \mid |Z(G)|$, e quindi $Z(G) \neq \{1\}$. □

Corollario 2.25. Sia G un gruppo di ordine p^2, con p primo. Allora G è abeliano. Quindi (a meno di isomorfismo) i gruppi di ordine p^2 sono due: C_{p^2} e $C_p \times C_p$.

Dimostrazione. Qui $|Z(G)|$ è > 1 e divide p^2. Per il teorema di Lagrange, sono due le possibilità: $Z(G)$ ha cardinalità p oppure p^2. Nel primo caso $|(G/Z(G))| = p$ e quindi il quoziente è ciclico: allora G è abeliano. (Ricorda che un gruppo G è abeliano se e solo se $G/Z(G)$ è ciclico.) Nel secondo caso, $G = Z(G)$ perché hanno la stessa cardinalità e sono finiti. □

3 I teoremi di Sylow

Teorema 3.1 (Teorema di Sylow I)**.** Siano G un gruppo finito, p primo e $l > 0$ tali che p^l divide $|G|$. Allora esiste un sottogruppo H di G di cardinalità p^l.

Per la dimostrazione del teorema abbiamo bisogno di un lemma.

Lemma 3.2 (Teorema di Cauchy per gruppi abeliani)**.** Siano G un gruppo *abeliano* finito e p primo tali p divide $|G|$. Allora G ha qualche sottogruppo H di cardinalità p. In particolare questo sottogruppo è ciclico, e quindi G ha qualche elemento di ordine p.

È bene richiamare in questa sede che in ogni gruppo *ciclico*, per ogni divisore d dell'ordine si può trovare un qualche elemento di ordine d.

Dimostrazione Lemma 3.2. Procediamo per induzione su $n := |G|$. Il caso $n = p$ è banalmente vero. Sia quindi $n > p$. Possiamo scegliere così un $b \in G$ diverso dall'identità. I casi ora sono due:

- p divide $\operatorname{ord} b$. In questo caso, nel sottogruppo *ciclico* $\langle b \rangle$ si può sempre trovare un sottogruppo di ordine p.
- Altrimenti, abbiamo il gruppo quoziente $G/\langle b \rangle$ che sicuramente ha ordine multiplo di p e $< n$. Per induzione, $G/\langle b \rangle$ ha un sottogruppo di cardinalità p: questo sottogruppo sarà ciclico, ovvero generato da un qualche $a\langle b \rangle \in G/\langle b \rangle$ di ordine p. L'ordine di questo elemento divide $\operatorname{ord} a$. Possiamo concludere perché nel sottogruppo *ciclico* $\langle a \rangle$ si può trovare un qualche elemento di ordine p. □

Proposizione 3.3 (Sottogruppi normali di un p-gruppo)**.** Sia G un gruppo di ordine p^n con p primo e $n \in \mathbb{N}$. Allora per ogni $m \in \mathbb{N}$ tale che $0 \le m \le n$ esiste un sottogruppo normale di G di ordine p^m. In particolare G è semplice se e solo se $n = 1$ [nel qual caso, G è ciclico].

Dimostrazione. Andiamo per induzione su n. Il caso $n = 0$ è immediatamente vero. Quindi assumiamo che $n > 0$; possiamo supporre anche $m > 0$. Abbiamo visto poco fa che $|Z(G)| = p^{n'}$ con $0 < n' \le n$. Esiste $K < Z(G)$ di ordine p, perché $p \mid |Z(G)|$ e $Z(G)$ è abeliano. Poiché $K \lhd G$, G/K è un gruppo di ordine p^{n-1}. Per l'ipotesi induttiva, G/K ha un sottogruppo normale di ordine p^{m-1}: Questo gruppo è della forma H/K per qualche H sottogruppo normale di G. La cardinalità di H è p^m. □

Possiamo ora puntare a dimostrare il Teorema di Sylow I. Anche qui verrà impiegato il Teorema 2.22.

Dimostrazione Teorema 3.1. Ragioniamo per induzione sulla cardinalità n di G. Il caso $n = p^l$ è ovvio, in quanto basta prendere il gruppo stesso. Supponiamo quindi che $n > p^l$. Per l'equazione delle classi si ha

$$|Z(G)| = |G| - \sum_{i=1}^{m} [G : C(a_i)]$$

per opportuni $a_1, \dots, a_m \in G$. Abbiamo quindi che $1 < [G : C(a_i)] \mid n$ per ogni $i = 1, \dots, m$, e in particolare quindi i centralizzatori $C(a_i)$ sono sottogruppi propri di G. Sono due i casi ora.

- p^l divide $|C(a_i)|$ per un certo $i \in \{1, \dots, m\}$. Quindi, per induzione, $C(a_i)$ ha un sottogruppo H di ordine p^l, che è anche sottogruppo di G.
- p^l non divide nessuno dei $|C(a_i)|$, vale a dire p divide tutti i $[G : C(a_i)]$. Ne deriva che p divide $|Z(G)|$. Per il Teorema 3.2, $Z(G)$ ha un sottogruppo K di ordine p. Questo sottogruppo è normale in G perché è abeliano. Ora il gruppo G/K ha ordine multiplo di p^{l-1} e $< n$: pertanto, per induzione, G/K ha un sottogruppo di ordine p^{l-1}; questo sottogruppo è della forma H/K con H sottogruppo di G. Abbiamo terminato, perché H ha ordine p^l. □

Una conseguenza immediata è la generalizzazione del Lemma 3.2 a tutta la classe dei gruppi finiti.

Corollario 3.4 (Teorema di Cauchy)**.** Siano G un gruppo finito e p primo tali p divide $|G|$. Allora G ha qualche sottogruppo H di cardinalità p.

Esiste un criterio che può essere comodo per verificare se un gruppo è un p-gruppo.

Corollario 3.5. Sia p un primo. Un gruppo finito è un p-gruppo se e solo se tutti i suoi elementi hanno ordine una potenza di p.

Dimostrazione. Un'implicazione è ovvia per il Teorema di Lagrange. Assumiamo ora che gli elementi di un gruppo finito G abbiano tutti ordine una potenza di p. A causa sempre del Teorema di Lagrange, $|G|$ è multiplo di p. Possiamo quindi scrivere $|G| = p^r k$ con $r, k \in \mathbb{N}$ tali che p che non divide k. Se $k \neq 1$, allora a causa del Corllario 3.4 per ogni primo q che divide k il gruppo ha un elemento di ordine q. Ma p e q sono coprimi. □

Definizione 3.6. Sia G un gruppo finito, p numero primo e $r, m > 0$ tali che $|G| = p^r m$ e p non divide m. Un *p-sottogruppo di Sylow*, o semplicemente un *p-Sylow*, di G è un qualsiasi sottogruppo di G di ordine p^r. Si usa indicare con s_p il numero di p-Sylow di G.

Osservazione 3.7. $s_p \geq 1$ per il Teorema 3.1.

Teorema 3.8 (Teorema di Sylow II)**.** Sia G un gruppo finito, p primo, e $r, m > 0$ interi positivi tali che $|G| = p^r m$ e p non divide m. Allora:

1. Due qualunque p-Sylow di G sono coniugati. In particolare, $s_p = [G : N_G(H)]$ dove H è un qualunque p-Sylow di G.
2. $s_p \equiv 1 \mod p$ e s_p divide m.
3. Ogni p-sottogruppo di G è contenuto in qualche p-Sylow di G.

[Esistono dimostrazioni più *simpatiche* di questo teorema: vada per quelle.]

Prima di procedere alla dimostrazione di questo risultato, richiamiamo/introduciamo qualche strumento che ci servirà poi per un Lemma.

Osservazione 3.9 (Richiami sul prodotto di sottogruppi)**.** Sia G un gruppo e H e K sue suoi sottogruppi. Possiamo introdurre l'insieme

$$HK := \{ab : a \in H, b \in K\}$$

che in generale non è un sottogruppo di G. Elenchiamo alcune proprietà notevoli.

1. HK è sottogruppo di G se e solo se $HK = KH$.

2. Se H oppure K è normale, allora HK è un sottogruppo. Se entrambi sono normali, allora HK è pure normale.
3. La funzione
$$f : H \times K \to G, \ f(a,b) := ab$$
è un omomorfismo di gruppi se e solo se $ab = ba$ per ogni $a \in H, b \in K$. In tal caso il suo nucleo è $H \cap K$.
4. Se H e K sono sottogruppi normali di G e $H \cap K = \{1\}$, allora $HK \cong H \times K$.[4]
5. Se H e K sono finiti, allora
$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Le prime tre proprietà sono facili da verificare. Osserviamo soltanto che l'ultima segue facilmente dal Primo Teorema di Isomorfismo nel caso in cui f è un isomorfismo. Tuttavia questo è un fatto molto più generale. Ne diamo una dimostrazione che usa quanto trattato fino ad ora delle azioni di gruppi. (Non ce n'è il bisogno, si può fare anche senza, ma è istruttivo per chi legge.)

Dimostrazione di 5. Consideriamo questa azione di $H \times K$ su HK
$$\begin{aligned}(H \times K) \times HK &\to HK \\ ((h,k),x) &\mapsto hxk^{-1}.\end{aligned}$$
Calcoliamo adesso lo stabilizzatore e l'orbita di $1 \in HK$. Lo stabilizzatore è
$$\{(h,k) \in H \times K : h1k^{-1} = 1\} = \{(h,k) \in H \times K : h = k\}$$
mentre l'orbita è
$$\{h1k^{-1} : (h,k) \in H \times K\} = HK.$$
Per la Proposizione 2.18, abbiamo finito. □

Con il lemma che segue cerchiamo di capire come sono fatte le orbite di un sottogruppo sotto l'azione di coniugio indotta sulle parti di un gruppo G.

Lemma 3.10. Sia G un gruppo finito e $H, K < G$ con H un p-gruppo e K un p-Sylow. Allora $[K]_H = \{K\}$ se e solo se $H \subseteq K$. Altrimenti p divide $|[K]_H|$.

Dimostrazione. Quindi $|H| = p^l$ per qualche $l \in \mathbb{N}$ tale che p^l divide $|G|$ e $|K| = p^s$ con $s \in \mathbb{N}$ tale che p^s divide $|G|$ e p^{s+1} no.
A causa della Proposizione 2.18 abbiamo
$$|[K]_H| = [H : N_H(K)] = p^{l-s}.$$
Quindi le possibilità per $|[K]_H|$ sono due: essere uguale a 1, vale a dire $[K]_H = \{K\}$, oppure essere multiplo di p.
Vediamo l'altra coimplicazione. La parte immediata è che se $H \subseteq K$, allora l'orbita $[K]_H$ è banale. Proviamo che se $[K]_H = \{K\}$, allora $H \subseteq K$. Osserviamo che $[K]_H = \{K\}$ se e solo se $H \subseteq N_H(K)$. Quindi cerchiamo di mostrare che se $H \subseteq N(K)$, allora $H \subseteq K$. Qui $H < N(K)$ e $K \lhd N(K)$ (da definizione di normalizzatore) e quindi $HK < N(K) < G$, vedi richiamo fatto poco sopra. Il

4. Prova che $ab = ba$ per ogni $a \in H$ e $b \in K$ e quindi ricadi nella proprietà precedente.

sottogruppo $H' := H \cap K$ è tale che $|H \cap K| = p^{l'}$, con $l' \leq l$. Allora, sempre per il richiamo sopra,

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = \frac{p^l p^s}{p^{l'}} = p^{s+l-l'} \mid |G| = p^s m.$$

Poiché HK è un sottogruppo di G e p^s è la massima potenza di p che divide $|G|$, allora $s + l - l' \leq s$, e cioè $l' \leq l$. Dobbiamo quindi concludere che $H \cap K = H$, ovvero l'inclusione $H \subseteq K$. □

Dimostrazione Teorema 3.8. Sia H un p-Sylow di G di ordine p^s. Se $K \in [H]_G$, allora $[K]_H \subseteq [K]_G = [H]_G$. Per il Lemma precedente, $[K]_H = \{K\}$ se e solo se $H \subseteq K$. Ma $H = K$, perché $|H| = |K|$. Altrimenti p divide $|[K]_H|$. Ne segue che

$$|[H]_G| \equiv 1 \mod p.$$

Sia ora $H' < G$ un p-gruppo: analogamente a prima $[K]_{H'} \subseteq [K]_G = [H]_G$ per ogni $K \in [H]_G$, e per il Lemma $p \mid |[K]_{H'}|$ se $H' \nsubseteq K$. Ne segue che $\exists K \in [H]_G$ tale che $H' \subseteq K$ (altrimenti $p \mid |[H]_G| \equiv 1 \mod p$).
Ciò dimostra sia il punto 1 che il punto 3. Si ha inoltre

$$s_p = |[H]_G| = [G : N(H)] \mid [G : H] = m$$

e $s_p \equiv 1 \mod p$, il che dimostra anche il punto 2. □

Osservazione 3.11. Il Teorema di Sylow II esprime anche s_p in funzione del normalizzante $N_G(H)$ di un qualsiasi p-Sylow H di G. Ne segue che H è normale in G se e solo se $s_p = 1$.

Richiamo 3.12 (Prodotto di sottogruppi)**.** Sia G un gruppo e H e K sue suoi sottogruppi. Possiamo introdurre l'insieme

$$HK := \{ab : a \in H, b \in K\}$$

che in generale non è un sottogruppo di G. Elenchiamo alcune proprietà notevoli.

1. HK è sottogruppo di G se e solo se $HK = KH$. Se H oppure K è normale, allora HK è un sottogruppo. Se entrambi sono normali, allora HK è pure normale.
2. La funzione
   $$f : H \times K \to G,\ f(a, b) := ab$$
   è un omomorfismo di gruppi se e solo se $ab = ba$ per ogni $a \in H, b \in K$. In tal caso, $\ker f = H \cap K$.
3. Se H e K sono sottogruppi normali di G e $H \cap K = \{1\}$, allora $HK \cong H \times K$.[5]
4. Se H e K sono finiti, allora
   $$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Le prime tre proprietà sono facili da verificare. Osserviamo soltanto che l'ultima segue facilmente dal Primo Teorema di Isomorfismo nel caso in cui f è un isomorfismo. Tuttavia questo è un fatto molto più generale. Ne diamo una dimostrazione che usa quanto trattato fino ad ora delle azioni di gruppi. (Non ce n'è il bisogno, si può fare anche senza, ma è istruttivo per chi legge.)

5. Prova che $ab = ba$ per ogni $a \in H$ e $b \in K$ e quindi ricadi nella proprietà precedente.

Dimostrazione di 5. Consideriamo questa azione di $H \times K$ su HK

$$(H \times K) \times HK \to HK$$
$$((h,k),x) \mapsto hxk^{-1}.$$

Calcoliamo adesso lo stabilizzatore e l'orbita di $1 \in HK$. Lo stabilizzatore è

$$\{(h,k) \in H \times K : h1k^{-1} = 1\} = \{(h,k) \in H \times K : h = k\}$$

mentre l'orbita è

$$\{h1k^{-1} : (h,k) \in H \times K\} = HK.$$

Per la Proposizione 2.18, abbiamo finito. □

Abbiamo gli strumenti ora per scrivere un *teorema di classificazione dei gruppi finiti* come quello che segue.

Teorema 3.13. Sia G un gruppo finito di cardinalità

$$|G| = \prod_{i=1}^{k} p_i^{n_i}$$

dove $p_1, \dots, p_k$ numeri primi a due a due distinti e $n_1, \dots, n_k > 0$. Per ognuno dei p_i indichiamo con H_i uno qualsiasi dei p_i-Sylow di G. Allora:

1. Se $s_{p_1} = \cdots = s_{p_k} = 1$, ovvero gli H_i sono tutti normali, allora
$$G \cong \prod_{i=1}^{k} H_i.$$
2. Se $G \cong \prod_{i=1}^{k} G_i$ per dei p_i-gruppi G_i con $i \in \{1, \dots, k\}$, allora $s_{p_i} = 1$ e $G_i \cong H_i$ per ogni $i \in \{1, \dots, k\}$.

Dimostrazione. La dimostrazione quindi è in due parti.

1. Per ipotesi, gli H_i sono normali in G e $|H_i| = p_i^{n_i}$. Noi dimostreremo che

   $H_1 \cdots H_j$ è un sottogruppo normale di G che è isomorfo a $\prod_{i=1}^{j} H_i$ per ogni $1 \le j \le k$

   Questo ci permette infatti di provare l'isomorfismo che vogliamo: infatti ha cardinalità $\left|\prod_{i=1}^{k} H_i\right| = \prod_{i=1}^{k} p_i^{n_i}$ è la stessa di G per ipotesi, quindi, trattandosi di gruppi finiti, allora necessariamente $G = H_1 \cdots H_k$.
   Andiamo per induzione su j. Il caso in cui $j = 1$ è ovvio. Se $j > 1$, allora
   $$H_1 \cdots H_{j-1} \lhd G \quad \text{e} \quad H_1 \cdots H_{j-1} \cong \prod_{i=1}^{j-1} H_i$$
   per cui $|H_1 \cdots H_{j-1}| = \prod_{i=1}^{j-1} p_i^{n_i}$. Allora $H_1 \cdots H_j = H_1 \cdots H_{j-1} H_j \lhd G$. Poi sicuramente tutti gli H_i si intersecano banalmente. Quindi $H_1 \cdots H_j \cong H_1 \cdots H_{j-1} \times H_j \cong \prod_{i=1}^{j} H_i$.
2. Qui, necessariamente i G_i sono sottogruppi di Sylow. Scriviamo il prodotto diretto come G' e consideriamo il sottogruppo
   $$G'_j := \{(g_1, \dots, g_k) \in G' : g_i = 1 \text{ per ogni } i \neq j\}.$$
   È facile verificare che è un sottogruppo normale di G ed è isomorfo a G_j. La copia isomorfa di G'_j in G ha quindi $p_j^{n_j}$ elementi ed è normale in G. Poiché gli elementi della copia hanno ordini p_j^r con $0 \le r \le n_j$, allora questa copia è proprio H_j. □

Osservazione 3.14. Questo teorema è piuttosto interessante, anche perché se G è abeliano, si ha quello che in Teoria dei Moduli ha il nome di Teorema di Classificazione dei Gruppi Abeliani. Osserviamo però che questo teorema vale per tutti i gruppi abeliani, non solo quelli finiti ai quali ci siamo ristretti in questi paragrafi.

4 Applicazioni

Nel Teorema di Sylow II (Teorema 3.8), se m è primo, il vincolo su s_p è molto forte: è uguale a 1 oppure a m. Le applicazioni qui sotto si basano proprio su questo.

Proposizione 4.1 (Gruppi di ordine pq)**.** Se G è un gruppo di ordine pq, con p, q primi e $p < q$, allora

1. $s_q = 1$.
2. Se $q \not\equiv 1 \mod p$, allora $s_p = 1$ e $G \cong C_p \times C_q \cong C_{pq}$.

In particolare, G non è semplice.

Dimostrazione. Per il Teorema di Sylow II,

$$\begin{cases} s_p \in \{1 + kp : k \in \mathbb{N}\} \\ s_p \in \{1, q\} \end{cases} \qquad \begin{cases} s_q \in \{1 + hq : h \in \mathbb{N}\} \\ s_q \in \{1, p\} \end{cases}$$

Qui, poiché $p < q$, è sicuro che $s_q = 1$. Se in più assumiamo che $q \notin \{1 + kp : k \in \mathbb{N}\}$, allora possiamo concludere che anche $s_p = 1$. □

Proposizione 4.2 (Gruppi di ordine p^2q)**.** Sia G un gruppo di ordine p^2q, dove p e q sono numeri primi distinti. Allora G ha un sottogruppo *normale* di ordine p^2 oppure di ordine q. In particolare, G non è semplice.

Dimostrazione. Possiamo equivalentemente ridurci a dimostrare che $s_p = 1$ oppure $s_q = 1$. Per il Teorema di Sylow II,

$$s_p \in \{1, 1 + p, 1 + 2p, \dots\} \cap \{1, q\}$$
$$s_q \in \{1, 1 + q, 1 + 2q, \dots\} \cap \{1, p, p^2\}.$$

Se $p > q$, allora $s_p = 1$. Vediamo cosa succede se $p < q$. Dimostriamo che

se $s_q \neq 1$, allora $s_p = 1$.

Se $s_q \neq 1$, allora l'unica possibilità è che $s_q = p^2$. Ricordiamo che s_q è il numero dei q-Sylow ed osserviamo che questi sottogruppi sono tutti ciclici perché hanno ordine primo, e necessariamente si intersecano a due a due banalmente. Allora in G ci sono $s_q(q-1) = p^2(q-1)$ elementi di ordine q. Pertanto il numero di elementi di ordine diverso da q è $p^2q - p^2(q-1) = p^2$. Tutti i p-Sylow devono avere p^2 elementi: eccoli questi p^2 elementi. C'è quindi un unico p-Sylow. □

Osservazione 4.3. In realtà, nel caso $p < q$ e $s_q > 1$, possiamo concludere che $p = 2$ e $q = 3$. Infatti $s_q = p^2 \equiv 1 \mod q$, cioè q divide $(p^2 - 1) = (p-1)(p+1)$. Sicuramente q non divide $p-1$, quindi divide $p+1 \leq q$. La conclusione è $q = p+1$: gli unici primi a fare ciò appunto sono 2 e 3 rispettivamente. Puoi pure rifare la seconda parte della dimostrazione con questi due numeri esplicitamente. Un esempio di questo tipo è $G = A_4$ (esercizio!).

Proposizione 4.4 (Gruppi di ordine pqr)**.** Sia G un gruppo finito di ordine pqr, dove p, q, r primi e $p < q < r$. Allora G ha un un sottogruppo normale di ordine q oppure r. In particolare, G non è semplice.

Dimostrazione. Analogamente a prima, dimostriamo

se $s_r \neq 1$, allora $s_q = 1$.

Per il Teorema di Sylow II,

$$s_q \in \{1, 1+q, 1+2q, \dots\} \cap \{1, p, r, pr\}$$
$$s_r \in \{1, 1+r, 1+2r, \dots\} \cap \{1, p, q, pq\}.$$

Andiamo per esclusione prima. Sicuramente s_r non può essere p oppure q, e quindi rimane solo $s_r = pq$. Per quanto riguarda s_q, non può essere p e rimangono 1, r e pr. Ragioneremo fino ad escludere anche r e pr . Come prima, i sottogruppi di r-Sylow sono pq e sono tutti ciclici. In G ci sono $pqr - pq(r-1) = pq$ elementi di ordine diverso da r. Quanti sono gli elementi di ordine q? Ce ne sono $s_q(q-1)$, il ragionamento è lo stesso. Quindi necessariamente $s_q(q-1) \leq pq$. Per ipotesi, si ha anche $s_q p \leq s_q(q-1)$ e quindi $s_q \leq q$. Chi sopravvive è $s_q = 1$. □

Proposizione 4.5. Sia G un gruppo finito e H un suo sottogruppo non banale. Se $2 \leq [G : H] \leq 4$, allora G non è semplice.

Dimostrazione. Supponiamo che G sia semplice e n sia il suo ordine. In tal caso $\ker L$, vedi Esempio 1.8, ha due sole possibilità: è banale oppure tutto G. La seconda chiaramente non è possibile perché questo vorrebbe dire che $G = H$, mentre $[G : H] \neq 1$. Quindi L è iniettivo, e il Primo Teorema di Isomorfismo implica che G ha una copia isomorfa G' dentro $S(G/H)$. Poiché Le classi laterali sono solo $m \in 2, 3, 4$, possiamo identificare $S(G/H)$ con S_m. Osserviamo che così stando le cose, $m \mid n \mid m!$ e $m \neq n$. Ci sono quindi questi scenari, al variare di m:

- Se $m = 2$, allora $n = m$, il che è impossibile.
- Se $m = 3$, allora $n = 6 = 2 \cdot 3$. Per la Proposizione 4.1, segue che G non è semplice, assurdo anche questo.
- Se $m = 4$, allora $n = 8 = 2^3$ o $n = 12 = 2^2 \cdot 3$ oppure $n = 24 = 2^3 \cdot 3$. In ogni caso, G non è semplice. □

Proposizione 4.6. I gruppi non abeliani di ordine < 60 non sono semplici.

Dimostrazione. Sia G un gruppo non abeliano di ordine $n < 60$. Un prima scrematura: i gruppi di ordini p o p^2 per p primo sono abeliani. Quindi gli ordini sotto 60 da esaminare restano: 6, 8, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 39, 40, 42, 44, 45, 46, 48, 50, 51, 52, 54, 55, 56, 57 e 58.

- Se $n = p^k$ con p primo e $k > 2$, allora G non è semplice. Gli ordini della forma p^k con $k > 2$ sotto il 60 sono: $2^3 = 8$, $2^4 = 16$, $2^5 = 32$ e $3^3 = 27$.
- Se n è il prodotto di tre primi distinti, allora G non semplice (Proposizione 4.4). Gli ordini < 60 di questa forma sono: $2 \cdot 3 \cdot 5 = 30$, $2 \cdot 3 \cdot 7 = 42$.

- Se n è prodotto di due primi, allora G non è semplice (Proposizione 4.1). Questa volta abbiamo coperto molti casi: $2 \cdot 3 = 6$, $2 \cdot 5 = 10$, $2 \cdot 7 = 14$, $2 \cdot 11 = 22$, $2 \cdot 13 = 26$, $2 \cdot 17 = 34$, $2 \cdot 19 = 38$, $2 \cdot 23 = 46$, $2 \cdot 29 = 58$, $3 \cdot 5 = 15$, $3 \cdot 7 = 21$, $3 \cdot 11 = 33$, $3 \cdot 13 = 39$, $3 \cdot 17 = 51$, $3 \cdot 19 = 57$, $5 \cdot 7 = 35$ e $5 \cdot 11 = 55$.
- Se n è della forma $p^2 q$ con p, q primi, allora G non è semplice (Proposizione 4.2). Gli ordini sono: $2^2 \cdot 2 = 8$, $2^2 \cdot 3 = 12$, $2^2 \cdot 5 = 20$, $2^2 \cdot 7 = 28$, $2^2 \cdot 11 = 44$, $2^2 \cdot 13 = 52$, $3^2 \cdot 2 = 18$, $3^2 \cdot 3 = 27$, $3^2 \cdot 5 = 45$ e $5^2 \cdot 2 = 50$.

Interrompiamo per elencare gli ordini sopravvissuti: 24, 36, 40, 48, 54 e 56.

- Vediamo i gruppi di ordine $36 = 2^2 \cdot 3^2$. Questi hanno dei 3-Sylow di indice 4: per la Proposizione 4.5, non sono semplici.
- Nei casi $24 = 2^3 \cdot 3$, $48 = 2^4 \cdot 3$ e $54 = 3^3 \cdot 2$, G ha un p-Sylow ha indice 2 o 3 in G, e quindi G non semplice grazie alla Proposizione 4.5.
- Se $n = 40 = 3^2 \cdot 4$, allora per il Teorema di Sylow II si ha $s_5 = 1$ e neanche in questo caso G è semplice.
- Rimane solo $n = 56 = 2^3 \cdot 7$ a questo punto. Il ragionamento non è diverso da quello per dimostrare le Proposizioni 4.1, 4.2 e 4.4. Esercizio! □

5 Permutazioni

Indichiamo con S_n l'insieme delle permutazioni dell'insieme $\{1, \dots, n\}$, con $n \in \mathbb{N}$. Forma un gruppo, chiamato *gruppo simmetrico*, se si considera assieme all'operazione di composizione di permutazioni e alla permutazione identità. Presi $x_1, \dots, x_r \in \{1, \dots, n\}$ a due a due distinti, indichiamo con

$$(x_1, \dots, x_r)$$

l'elemento di S_n che manda x_i in x_{i+1} se $i < n$ e x_{n+1} in x_1. Questo tipo di permutazione prende il nome di *r-ciclo* o di *ciclo di lunghezza r*. I 2-cicli prendono il nome di *trasposizioni*. Due cicli $(x_1, \dots, x_r)$ e $(y_1, \dots, y_s)$ sono detti *disgiunti* qualora $x_i \neq y_j$ per ogni i e j.

Ricapitoliamo alcuni fatti base che dovrebbero essere noti da Algebra I.

- $|S_n| = n!$.
- I cicli disgiunti commutano.
- Ogni permutazione si può decomporre in maniera unica (a meno dell'ordine) in cicli disgiunti.
- Ogni permutazione si può decomporre in 2-cicli; questa volta la decomposizione può non essere unica. Ecco alcune decomposizioni in trasposizioni di uno stesso ciclo:

$$(a_1, a_2, a_3 \dots, a_n) = \begin{cases} (a_1, a_n) \cdots (a_1, a_3)(a_1, a_2) \\ (a_1, a_2)(a_2, a_3) \cdots (a_{n-1}, a_n) \end{cases}.$$

  Osserviamo che S_n non è un gruppo *libero* sull'insieme delle trasposizioni: infatti per ogni trasposizione $\tau \in S_n$ si ha $\tau^2 = \mathrm{id}$.
- Il *segno* di una permutazione è definito come l'omomorfismo di gruppi $\varepsilon : S_n \to \{\pm 1\} \cong C_2$ tale che $\varepsilon(\sigma) = (-1)^{m-1}$ per ogni m-ciclo $\sigma \in S_n$.
- S_n ha un sottogruppo normale, il *gruppo alternante*

$$A_n := \ker \varepsilon.$$

- $|A_n| = \frac{n!}{2}$ per ogni $n \geq 2$

Proposizione 5.1. Ogni elemento di A_n si può decomporre in 3-cicli.

Dimostrazione. Abbiamo visto che una qualsiasi permutazione può essere decomposta in un numero finito di trasposizioni. Poiché il segno delle permutazioni di A_n è 1, allora queste si possono decomporre in un numero *pari* di trasposizioni. Facciamo vedere che il prodotto di due trasposizioni è l'identità oppure il prodotto di 3-cicli. A tal scopo siano $i < j$ e $k < l$ e calcoliamo:

$$(i,j)(k,l) = \begin{cases} \mathrm{id} & \text{se } (i,j) = (k,l) \\ (i,j,l) & \text{se } j = k \\ (i,j,k)(j,k,l) & \text{altrimenti} \end{cases}$$ □

Richiamo 5.2 (Il gruppo diedrale)**.** Richiamiamo il *gruppo diedrale* di ordine $n \geq 3$, cioè il gruppo indicato con D_n e generato da due simboli r e s soddisfacenti le seguenti regole:

$$r^n = 1 \tag{5.1}$$
$$s^2 = 1 \tag{5.2}$$
$$(sr)^2 = 1 \tag{5.3}$$

Si usa scrivere più compattamente:

$$D_n := \left\langle r, s \mid r^n = 1, s^2 = 1, (sr)^2 = 1 \right\rangle.$$

Osserviamo che l'inverso di s è s stesso. Possiamo elencare esplicitamente tutti i $2n$ elementi di questo gruppo:

$$1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}$$

Non è difficile da dimostrare. Consideriamo una generica stringa finita

$$x_1 x_2 \cdots x_n$$

dove $\{x_1, \dots, x_n\} \subseteq \{r, r^{-1}, s\}$. Possiamo pure usare una notazione compatta che fa uso di esponenti interi, ma in questa sede è conveniente un po' di ridondanza. Assumiamo anche che non appaiano sotto-stringe rr^{-1} e $r^{-1}r$. Dalle regole 5.2 e 5.3 discendono due ulteriori relazioni

$$sr = r^{-1}s \quad \text{e} \quad rs = sr^{-1}.$$

La conseguenza è che si possono spostare le s tutte in testa facendo attenzione a cambiare gli esponenti delle r scambiate con le s. Ora è sufficiente ridurre:

- Per la regola 5.2, un numero pari di s le farà sparire, mentre un numero dispari lascerà in testa una sola s.
- La coda fatta di sole r^{α_i}, con $\alpha_i \in \{1, -1\}$, si riduce ad un'unica r^α. Sia ora ρ il resto della divisione Euclidea tra α e n: a causa della regola 5.1, r^α di può ridurre a r^ρ. Per come è definito il resto, si ha $\rho \in \{0, \dots, n-1\}$.

[Fare qualche esempio di riduzione?] Può essere anche utile richiamare l'idea geometrica che sta dietro. Consideriamo un poligono regolare Δ_n in cui numeriamo in vertici in senso orario. Visualizziamo r come la rotazione attorno

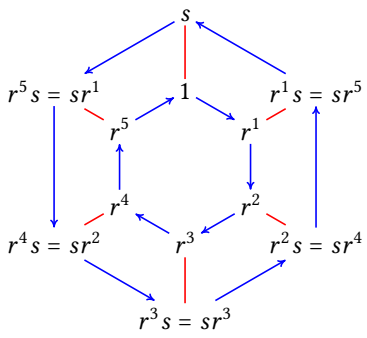


Figura 1. Grafo di Cayley di D_6. Muoversi lungo le frecce blu seguendone il verso significa moltiplicare per r a destra, mentre nel verso opposto significa moltiplicare per r^{-1} a destra. Muoversi lungo i segmenti rossi, in qualunque senso, significa moltiplicare per s (visto che s è l'inverso di se stessa).

al centro del poligono di un angolo $\frac{2\pi}{n}$ e con s la simmetria rispetto all'asse di simmetria della figura che passa per il vertice numerato con 1. Quindi r è identificato con la permutazione $(1, \dots, n)$ mentre s con la permutazione che scambia tra loro i numeri ai vertici simmetrici rispetto all'asse di simmetria verticale. La visualizzazione del prodotto sr è la composizione di una simmetria e di una rotazione. Verifichiamo che le regole vengono mantenute: n rotazioni consecutive riportano i punti dove erano, così due simmetrie consecutive; infine la rotazione porta i in $i+1$, il simmetrico di $i+1$ viene portato in cui punto per rotazione che è il simmetrico di i. Abbiamo realizzato cioè l' omomorfismo inclusione $D_n \hookrightarrow S_n$. A tal scopo osserviamo che esiste una coincidenza fortunata: $D_3 \cong S_3$.

Ricordiamo un fatto carino per quanto riguarda il gruppo diedrale.

Proposizione 5.3 (Gruppi di ordine $2p$)**.** I gruppi di ordine $2p$ con $p \geq 3$ primo sono (a meno di isomorfismo) due: C_{2p} oppure D_p.

Dimostrazione. Per il Teorema di Sylow I, un siffatto gruppo G possiede due sottogruppi ciclici di ordine 2 e p rispettivamente. Sia $H = \langle r \rangle$ con $r \in G$ di ordine p. Per il Teorema di Sylow II, si ha $s_p = 1$ e quindi H è normale. Se $s \in G$ è elemento di ordine 2, allora $s \notin H$ e

$$G = H \cup sH = \left\{1, r, \dots, r^{p-1}, s, sr, \dots, sr^{p-1}\right\}.$$

Questo ricorda tanto il gruppo diedrale, ma non bisogna avere fretta: r e s soddisfano le regole 5.1, 5.2 e 5.3? Le prime due sì, la rimanente non necessariamente. Poiché H è normale, $r^i = srs^{-1} = srs$ per qualche i. Ne segue che $r^{i^2} = (srs)^i = sr^i s = r$ e cioè $i^2 \equiv 1 \mod p$. Ricordando che $\mathbb{Z}/p\mathbb{Z}$ è un campo perché p è primo, si ha $i \equiv 1 \mod p$ oppure $i \equiv -1 \mod p$. Nel primo caso G è abeliano (r e s commutano) di ordine $2p$, mentre nel secondo caso $(sr)^2 = 1$ e siamo nel caso del gruppo diedrale. □

Osservazione 5.4 (Vierergruppe o gruppo di Klein V_4)**.** [Ancora da scrivere...]

Possiamo classificare i sottogruppi di S_4 a questo punto.

Proposizione 5.5 (I sottogruppi di S_4)**.** I sottogruppi di S_4 sono (a meno di isomorfismo): C_2, C_3, C_4, $C_2 \times C_2$, S_3, D_4, A_4.

Dimostrazione. Verifichiamo che ciascuno di quei gruppi ha una copia isomorfa dentro S_4.

- Se σ è un m-ciclo, allora $\langle\sigma\rangle \cong C_m$.
- $V_4 \cong C_2 \times C_2$.
- $H := \{\sigma \in S_4 : \sigma(4) = 4\}$ è isomorfo a S_3.
- Nel richiamo fatto poco sopra sul gruppo diedrale abbiamo visto come realizzare un'inclusione $D_n \hookrightarrow S_n$.
- A_4 è un sottogruppo di S_4 per definizione.

Sia H un sottogruppo di S_4: per il Teorema di Lagrange, $|H|$ è un divisore di $4! = 24$.

- Se $|H| \leq 3$, allora H è ciclico.
- Se $|H| = 4 = 2^2$, allora H è $C_2 \times C_2$ oppure C_4 (vedi Corollario 2.25).
- Se $|H| = 6 = 2 \cdot 3$, allora per la Proposizione 5.3 dobbiamo concludere che è isomorfo a $D_3 \cong S_3$ perché in S_4 non ci sono elementi di ordine 6.
- Sia $|H| = 8$. Osservando che $24 = 2^3 \cdot 3$, i 2-Sylow hanno tutti ordine 8 e sono tutti coniugati. Un sottogruppo di ordine di ordine 8 è una copia di D_4.
- Se $|H| = 12$, allora $[S_4 : H] = 2$ e quindi H è un sottogruppo normale di S_4. Gli unici sottogruppi normali di S_4 sono A_4 e V_4. L'unica possibilità però è A_4 perché tra i due è quello che ha cardinalità 12. □

Osservazione 5.6. $H, K < G \Rightarrow [H : H \cap K] \leq [G : K]$ perché la funzione

$$H/(H \cap K) \to G/K\,,\ a(H \cap K) \mapsto aK$$

è (ben definita e) iniettiva. In particolare $H < S_n \Rightarrow [H : H \cap A_n] \leq [S_n : A_n] = 2$, e quindi $[H : H \cap A_n] = 2$ se $H \nsubseteq A_n$.

Per ogni $\sigma \in A_n$, dato che $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$, si ha allora

$$\begin{cases} C_{A_n}(\sigma) = C_{S_n}(\sigma) & \text{se } C_{S_n}(\sigma) \subseteq A_n \\ [C_{S_n}(\sigma) : C_{A_n}(\sigma)] = 2 & \text{se } C_{S_n}(\sigma) \nsubseteq A_n, \end{cases}$$

da cui segue (ricordando che $|[\sigma]_G| = [G : C_G(\sigma)]$ per $G = S_n$ o $G = A_n$, e tenendo conto che $[\sigma]_{A_n} \subseteq [\sigma]_{S_n}$)

$$\begin{cases} |[\sigma]_{A_n}| = \frac{|A_n|}{|C_{A_n}(\sigma)|} = \frac{|S_n|}{2|C_{S_n}(\sigma)|} = \frac{|[\sigma]_{S_n}|}{2} & \text{se } C_{S_n}(\sigma) \subseteq A_n \\ [\sigma]_{A_n} = [\sigma]_{S_n} & \text{se } C_{S_n}(\sigma) \nsubseteq A_n. \end{cases}$$

- $\sigma \in V_4 \setminus \{1\} \Rightarrow [\sigma]_{S_4} = V_4 \setminus \{1\} \Rightarrow |[\sigma]_{S_4}| = 3$ dispari $\Rightarrow [\sigma]_{A_4} = [\sigma]_{S_4} = V_4 \setminus \{1\}$.
- σ 3-ciclo $\Rightarrow [\sigma]_{S_4} = \{3\text{-cicli}\} \Rightarrow$

$$8 = |[\sigma]_{S_4}| = [S_4 : C_{S_4}(\sigma)] = \frac{24}{|C_{S_4}(\sigma)|}$$

$\Rightarrow |C_{S_4}(\sigma)| = 3 \Rightarrow C_{S_4}(\sigma) = \langle\sigma\rangle \subset A_4 \Rightarrow |[\sigma]_{A_4}| = |[\sigma]_{S_4}|/2 = 4$ (i 3-cicli formano dunque 2 classi di coniugio in A_4).
- L'unico sottogruppo normale non banale di A_4 è V_4 (dunque $\nexists H < A_4$ tale che $|H| = 6$, anche se $6 \mid 12 = |A_4|$):
$H \lhd A_4 \Rightarrow |H| \mid 12$ e H è unione di classi di coniugio $\Rightarrow |H| = 1 + 3a + 4b + 4c$ con $a, b, c \in \{0, 1\} \Rightarrow a = 1$ e $b = c = 0$ se $1 < |H| < 12$.

Lemma 5.7. Sia H un sottogruppo normale di A_n non banale. Se $n \geq 5$, allora H contiene un 3-ciclo.

Dimostrazione. [Vedi il Lemma 4.36 in [Mil].] □

Teorema 5.8. A_n è semplice per ogni $n \geq 5$.

Dimostrazione. $\{1\} \neq H \lhd A_n \Rightarrow$ per la Proposizione $\exists \sigma = (a,b,c) \in H$.
$n \geq 5 \Rightarrow \exists \tau = (d,e) \in C_{S_n}(\sigma)$ (con a,b,c,d,e distinti) $\Rightarrow C_{S_n}(\sigma) \nsubseteq A_n \Rightarrow$

$$[\sigma]_{A_n} = [\sigma]_{S_n} = \{3\text{-cicli}\} \subseteq H \lhd A_n$$

$\Rightarrow A_n = \langle \{3\text{-cicli}\} \rangle < H < A_n \Rightarrow H = A_n$. □

Corollario 5.9. A_5 è semplice e $|A_5| = 60$.

Corollario 5.10. A_n è l'unico sottogruppo normale non banale di S_n per ogni $n \geq 5$.

Dimostrazione.
- $H \lhd S_n \Rightarrow H' := H \cap A_n \lhd A_n \Rightarrow H' = \{1\}$ o $H' = A_n$.
- $H \subseteq A_n \Rightarrow H = H' \Rightarrow H = \{1\}$ o $H = A_n$.
- $H \nsubseteq A_n \Rightarrow [H : H'] = 2 \Rightarrow |H| = 2$ o $H = S_n$.
- Per assurdo $|H| = 2 \Rightarrow H = \{1, \tau\}$ (con $\tau \in S_n \setminus A_n$) $\Rightarrow \sigma\tau\sigma^{-1} = \tau$ per ogni $\sigma \in S_n \Rightarrow \tau \in Z(S_n)$, assurdo perché $Z(S_n) = \{1\}$ (per ogni $n \geq 3$). □

Proposizione 5.11. G gruppo semplice non abeliano, $H < G$ tale che $[G : H] = 5 \Rightarrow G \cong A_5$.

Dimostrazione. L'omomorfismo $L : G \to S(G/H) \cong S_5$ è iniettivo (perché G è semplice e $\ker(L) \subseteq H \subsetneq G$) $\Rightarrow \exists G' < S_5$ tale che $G' \cong G$ semplice non abeliano $\Rightarrow$

$$n := |G| = |G'| \mid 120 = |S_5| \text{ , e , } |G'| \geq 60$$

$\Rightarrow n = 60$ o $n = 120$. Non può essere $n = 120$ (se no $G \cong G' = S_5$ non semplice)
$\Rightarrow n = 60 \Rightarrow [S_5 : G'] = 2 \Rightarrow G' \lhd S_5 \Rightarrow G \cong G' = A_5$. □

Osservazione 5.12. In effetti esiste $H < A_5$ tale che $[A_5 : H] = 5$: per esempio $H := \{\sigma \in A_5 : \sigma(5) = 5\} \cong A_4$.

6 Gruppi risolubili

Definizione 6.1. Un gruppo G è *risolubile* se esistono sottogruppi

$$\{1\} = K_r \lhd K_{r-1} \lhd \cdots \lhd K_1 \lhd K_0 = G$$

tali che K_{i-1}/K_i è abeliano per ogni $i = 1, \ldots, r$.

Esempio 6.2. G è risolubile in ciascuno dei seguenti casi:

- G è abeliano ($r = 1$);
- $G = D_n$ ($r = 2$, $K_1 = \langle R \rangle$), quindi anche $G = S_3 \cong D_3$;
- $G = S_4$ ($r = 3$, $K_1 = A_4$, $K_2 = V_4$);
- $|G| = p^n$ ($r = n$ e per induzione $\exists K_i \lhd K_{i-1}$ tale che $|K_i| = p^{n-i}$).

Un gruppo semplice non abeliano (per esempio A_n per ogni $n \geq 5$) non è risolubile.

Proposizione 6.3. 1. $H < G$ e G risolubile $\Rightarrow$ H risolubile.

2. $H \lhd G$ e G risolubile $\Rightarrow$ G/H risolubile.
3. $H \lhd G$, H e G/H risolubili $\Rightarrow$ G risolubile.

Dimostrazione. 1. $\{1\} = K_r \lhd \cdots \lhd K_0 = G \Rightarrow K_i' := K_i \cap H$ per $i = 0, \dots, r$ tali che $\{1\} = K_r' < \cdots < K_0' = H$. Inoltre per ogni $i = 1, \dots, r$

$$K_{i-1}' = K_{i-1} \cap H \xrightarrow{j_i} K_{i-1} \xrightarrow{p_i} K_{i-1}/K_i$$

(con j_i l'inclusione e p_i la proiezione) è un omomorfismo tale che $\ker(p_i \circ j_i) = K_i \cap H = K_i' \lhd K_{i-1}'$. Per il teorema di omomorfismo esiste $K_{i-1}'/K_i' \to K_{i-1}/K_i$ omomorfismo iniettivo, dunque K_{i-1}/K_i abeliano $\Rightarrow K_{i-1}'/K_i'$ abeliano.

2. $\pi : G \to \overline{G} := G/H$ proiezione, $\{1\} = K_r \lhd \cdots \lhd K_0 = G \Rightarrow \overline{K}_i := \pi(K_i)$ per $i = 0, \dots, r$ tali che $\{\overline{1}\} = \overline{K}_r < \cdots < \overline{K}_0 = \overline{G}$. Inoltre per ogni $i = 1, \dots, r$ $\overline{K}_i \lhd \overline{K}_{i-1}$ (perché $\pi(g)\pi(a)\pi(g)^{-1} = \pi(gag^{-1}) \in \overline{K}_i$ per ogni $g \in K_{i-1}$ e per ogni $a \in K_i$, dato che $gag^{-1} \in K_i$) e

$$K_{i-1} \xrightarrow{\pi_i} \pi(K_{i-1}) = \overline{K}_{i-1} \xrightarrow{\overline{p}_i} \overline{K}_{i-1}/\overline{K}_i$$

(con π_i indotto da π e $\overline{p}_i$ la proiezione) è un omomorfismo suriettivo tale che $K_i \subseteq \ker(\overline{p}_i \circ \pi_i)$. Per il teorema di omomorfismo esiste un omomorfismo suriettivo $K_{i-1}/K_i \to \overline{K}_{i-1}/\overline{K}_i$, dunque K_{i-1}/K_i abeliano $\Rightarrow \overline{K}_{i-1}/\overline{K}_i$ abeliano.

3. $\{1\} = K_r' \lhd \cdots \lhd K_0' = H$ e $\{\overline{1}\} = \overline{K}_s \lhd \cdots \lhd \overline{K}_0 = \overline{G}$ (dove $\overline{K}_i = K_i/H$ con $H < K_i < G$ per $i = 0, \dots, s$) $\Rightarrow \{1\} = K_r' \lhd \cdots \lhd K_0' = K_s \lhd \cdots \lhd K_0 = G$. Inoltre per ogni $i = 1, \dots, s$ $K_{i-1}/K_i \cong \overline{K}_{i-1}/\overline{K}_i$ per il terzo teorema di isomorfismo. □

Conseguenze:

- $G \cong H < S_4 \Rightarrow G$ risolubile.
- $n \geq 5 \Rightarrow S_n$ non risolubile: $A_n < S_n$ e A_n non è risolubile.
- $|G| = pq$ o p^2q (con p e q primi distinti) $\Rightarrow G$ risolubile:
  $\exists H \lhd G$ con H di Sylow, quindi H e G/H sono abeliani e pertanto risolubili.
- $|G| = pqr$ (con p, q e r primi distinti) $\Rightarrow G$ risolubile:
  $\exists H \lhd G$ con H di Sylow, quindi H è abeliano e G/H è risolubile per il punto precedente.
- $|G| < 60 \Rightarrow G$ risolubile:
  se G non è abeliano, $\exists H \lhd G$ non banale $\Rightarrow$ induttivamente H e G/H sono risolubili.

Ricordiamo che il sottogruppo dei commutatori di un gruppo G è

$$[G, G] := \left\langle aba^{-1}b^{-1} : a, b \in G \right\rangle \lhd G$$

tale che, se $H \lhd G$, allora G/H è abeliano $\iff [G, G] \subseteq H$. Definendo $G^{(0)} := G$ e induttivamente $G^{(i)} := [G^{(i-1)}, G^{(i-1)}]$ per ogni $i > 0$, si ha allora $G^{(i)} \lhd G^{(i-1)}$ e $G^{(i-1)}/G^{(i)}$ è abeliano per ogni $i > 0$.

Proposizione 6.4 (Caratterizzazione dei gruppi risolubili)**.** G è risolubile $\iff$ $\exists r \in \mathbb{N}$ tale che $G^{(r)} = \{1\}$.

Dimostrazione. $\Longleftarrow$ Chiaro.

$\Rightarrow$ $\{1\} = K_r \lhd \cdots \lhd K_0 = G$ con K_{i-1}/K_i abeliano per ogni $i = 1, \dots, r \Rightarrow G^{(i)} \subseteq K_i$ per ogni $i = 0, \dots, r$ per induzione su i: vero se $i = 0$; se $i > 0$ per induzione $G^{(i-1)} \subseteq K_{i-1} \Rightarrow G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subseteq [K_{i-1}, K_{i-1}] \subseteq K_i$
perché K_{i-1}/K_i è abeliano. Dunque $G^{(r)} = \{1\}$. □

7 Prodotto semidiretto

Definizione 7.1 (Prodotto semidiretto di sottogruppi)**.** Sia G un gruppo e $H < G$ e $N \lhd G$. Diciamo che G è *prodotto semidiretto* dei sottogruppi N e H qualora

$$H \cap N = \{1\}$$
$$HN = G$$

In tal caso, si scrive $G = N \rtimes H$ oppure $G = H \ltimes N$.

Osservazione 7.2. Se nella Definizione 7.1 anche $H \lhd G$, allora

$$H \ltimes N \cong H \times N$$

e si può dire anche che G è *prodotto diretto* di H e N. Vedi il Richiamo 3.12.

Ecco un lista di semplici esempi, ma comunque utile per battere il terreno.

Esempio 7.3. Il gruppo diedrale

$$D_n = \left\langle r, s \mid r^n = 1, s^2 = 1, (sr)^2 = 1 \right\rangle$$

ha due sottogruppi ciclici, $\langle r \rangle$ e $\langle s \rangle$, dei quali il primo è sicuramente normale. [Inserire la verifica di questo fatto?] Osserviamo che si intersecano banalmente (ricorda che $n \geq 3$) e $\langle r \rangle \langle s \rangle$ è un sottogruppo di D_n che ha $2n$ elementi, come D_n. (Vedi il Richiamo 3.12.) Pertanto possiamo concludere che

$$D_n = \langle r \rangle \rtimes \langle s \rangle .$$

Esempio 7.4. Sia G un gruppo di ordine pq, con p e q primi tali che $p < q$. Per la Proposizione 4.1, questo gruppo ha qualche sottogruppo di Sylow di ordine p e uno solo di ordine q che è anche normale. Indichiamoli con H_p e H_q rispettivamente. Questi due sottogruppi si intersecano banalmente e $H_p H_q$ è un sottogruppo di G che ha la stessa cardinalità di G. (Vedi il Richiamo 3.12.) Anche in questo caso,

$$G = H_q \rtimes H_p.$$

Gli esempi appena illustrati sono un'importante occasione: se $p \geq 3$ è primo, allora D_p e C_{2p} sono il prodotto semidiretto sottogruppi che sono isomorfi a C_2 e a C_p, ma $D_p \ncong C_{2p}$ (C_{2p} ha qualche elemento di ordine $2p$ mentre D_p no). È una delle ragioni che ci porterà a introdurre il concetto di prodotto semidiretto "esterno".

Esempio 7.5. Sappiamo che gli elementi di S_n si possono decomporre in trasposizioni e che gli elementi di A_n si possono decomporre in un numero *pari* di trasposizioni. Non è difficile verificare che, presa una qualsiasi trasposizione $\sigma \in S_n$, si ha $\langle \sigma \rangle A_n = S_n$. Infatti, se $\phi \in A_n$, allora $\phi \in \langle \sigma \rangle A_n$; se invece, $\phi \in S_n \setminus A_n$, allora $\sigma\phi \in A_n$ e pertanto $\phi = \sigma\sigma\phi \in \langle \sigma \rangle A_n$. I due sottogruppi $\langle \sigma \rangle$ e A_n si intersecano banalmente e A_n è pure normale (da definizione A_n è il nucleo di un certo omomorfismo). Pertanto $S_n = A_n \rtimes \langle \sigma \rangle$.

Esempio 7.6. Se guardiamo S_4 come un sottogruppo di S_4 (ad esempio lo identifichiamo con $\{\sigma \in S_4 : \sigma(4) = 4\} < S_4$), allora $S_4 = V_4 \rtimes S_3$ e $A_4 = V_4 \rtimes A_3$.

Proposizione 7.7. Sia G un gruppo e $H < G$ e $N \lhd G$. Indichiamo con $i : H \hookrightarrow G$ l'inclusione e con $\pi : G \to G/N$ la proiezione al quoziente. Allora sono equivalenti:

1. $G = N \rtimes H$.
2. $\pi \circ i : H \to G/N$ è un isomorfismo.
3. Esiste $f : G \to H$ tale che $\ker f = N$ e $f \circ i = \mathrm{id}_H$.

[Leggere anche Wikipedia.] In sostanza, $(1 \Rightarrow 2)$ risponde alla domanda: che cos'è $\frac{N \rtimes H}{N}$? È proprio H sotto un preciso isomorfismo. Mentre $(3 \Rightarrow 1)$ ci dice che un omomorfismo $f : G \to H$ che fissa gli elementi di H permette di scrivere G come un prodotto semidiretto: $G = \ker f \rtimes H$.

Esempio 7.8. Per ritornare ad uno dei nostri primi esempi, consideriamo l'omomorfismo

$$f : D_n \to \langle s \rangle$$

che manda $s^j r^k$, per $j \in \{0, 1\}$ e $k \in \{0, \dots, n-1\}$, in s^j. (Verificare che questo è effettivamente un omomorfismo!) Questo omomorfismo tiene fissi gli elementi di $\langle s \rangle$ è il suo nucleo è chiaramente $\langle r \rangle$. Abbiamo quindi riprovato in un'altra maniera che $D_n = \langle r \rangle \rtimes \langle s \rangle$.
Un altro modo per ottenere lo stesso risultato è di calcolare esplicitamente $D_n/\langle r \rangle$: le classi laterali sono due, $\langle r \rangle$ e $s\langle r \rangle$, ed è evidente che

$$\langle s \rangle \to D_n/\langle r \rangle, \ s^j \to s^j \langle r \rangle$$

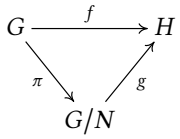
è un isomorfismo.

Esercizio 7.9. Riprovare a riformulare altri esempi nello spirito della Proposizione 7.7.

Dimostrazione della Proposizione 7.7. $(1 \Rightarrow 2)$ Mostriamo che $\pi \circ i$ è iniettivo: se $hN = N$ con $h \in H$, allora $h \in N$, e che quindi $h = 1$ perché H e N si intersecano banalmente. Proviamo che $\pi \circ i$ è suriettivo: poiché $G = HN$, allora ogni elemento di G/N può essere scritto come hN.
$(2 \Rightarrow 3)$ Poiché $\pi \circ i$ è un isomorfismo, possiamo considerare l'omomorfismo $f : G \to H$ ottenuto componendo gli omomorfismi

$$G \xrightarrow{\pi} G/N \xrightarrow{(\pi \circ i)^{-1}} H$$

Qui $1 = f(x) = (\pi \circ i)^{-1} \circ \pi(x)$ se e solo se $\pi(x) = \pi \circ i(1) = N$, ovvero $x \in N$. Infine $f \circ i = \mathrm{id}_H$ per come è definito f.
$(3 \Rightarrow 1)$ Per il Primo Teorema di Isomorfismo, esiste un unico omomorfismo g per cui commuta il diagramma



Qui g è un isomorfismo perché f è suriettivo. Osserviamo che $g(hN) = f(h) = h$ per ogni $h \in H$ e quindi le classi laterali hN al variare di $h \in H$ bastano per formare una partizione di G. Da questa considerazione è immediata la verifica delle condizioni per essere prodotto semidiretto. □

Quello che abbiamo appena visto è il prodotto semidiretto "interno". Si può fare in generale il prodotto semidiretto di due gruppi non necessariamente sottogruppi di un unico gruppo. Questo richiede un po' di attenzione preliminare.

Lemma 7.10. Siano H e N due gruppi e $\theta : H \to \mathrm{Aut}(N)$ un omomorfismo. Allora l'operazione

$$\begin{aligned} \bullet_\theta &: (N \times H) \times (N \times H) \to (N \times H) \\ (n_1, h_1) \bullet_\theta (n_2, h_2) &:= (n_1 \theta_{h_1}(n_2), h_1 h_2) \end{aligned}$$

è associativa, $(1_N, 1_H)$ è l'identità e l'inverso di (a, b) è $(\theta_{b^{-1}}(a^{-1}), b^{-1})$.

Dimostrazione. [Da scrivere.] □

Definizione 7.11 (Prodotto semidiretto di gruppi)**.** Siano H e N due gruppi e $\theta : H \to \mathrm{Aut}(N)$ un omomorfismo. Il *prodotto semidiretto* di N e H rispetto a θ è il gruppo denotato con $N \rtimes_\theta H$ oppure $H \ltimes_\theta N$ ed è dato dall'insieme $N \times H$ con l'operazione $\bullet_\theta$ introdotta nel Lemma precedente. Per comodità e quando non crea ambiguità, ci dimenticheremo spesso del simbolo $\bullet_\theta$ e moltiplicheremo due elementi (a_1, b_1) e (a_2, b_2) di $N \rtimes_\theta H$ scrivendo semplicemente $(a_1, b_1)(a_2, b_2)$.

Quindi $N \rtimes_\theta H$ è $N \times H$ ma munita di un'operazione da quella del classico prodotto diretto.

Esempio 7.12. Partiamo nell'esplorazione di questo nuovo oggetto col caso più banale: $\varepsilon : H \to \mathrm{Aut}(N)$ è l'omomorfismo banale, cioè $\varepsilon_h = \mathrm{id}_N$ per ogni $h \in H$. Quindi il prodotto semidiretto è un semplice prodotto diretto:

$$N \rtimes_\varepsilon H = N \times H.$$

Esempio 7.13 (Gruppo diedrale come prodotto semidiretto)**.** Sia $n \geq 2$ e scriviamo r un generatore di C_n e s un generatore di C_2. Cos'è $C_n \rtimes_\rho C_2$ con $n \geq 3$ e dove $\rho : C_2 \to \mathrm{Aut}(C_n)$ è l'omomorfismo tale che $\theta_s : C_n \to C_n$ manda un elemento nel suo inverso? Da definizione, gli elementi di $C_n \rtimes_\rho C_2$ sono quelli di $C_n \times C_2$, cioè delle forma

$$(r^j, s^k) \quad \text{per } j \in \{0, \dots, n-1\} \text{ e } k \in \{0, 1\},$$

ma l'operazione è diversa da quella di del classico prodotto diretto! Verifichiamo che si tratta del gruppo diedrale D_n, ovvero che è isomorfo, verificando le relazioni 5.1, 5.2 e 5.3:

$$\begin{aligned} (r, 1)^n &= 1 \\ (1, s)^2 &= 1 \\ (r, s)^2 &= \left(r\rho_s(r), s^2\right) = \left(rr^{-1}, 1\right) = 1 \end{aligned}$$

Qui $(r, 1)$ è nel ruolo di r e $(1, s)$ nel ruolo di s del Richiamo 5.2, e in generale (r^k, s^j) riveste il ruolo di $s^j r^k$.

Osservare il notevole balzo in avanti. Scrivere che $D_n = \langle r \rangle \rtimes \langle s \rangle$ significa dire ha dei sottogruppi che combinati in qualche modo danno D_n stesso. Tuttavia questo è un fatto di un oggetto, D_n, già introdotto a monte. Invece $C_n \rtimes_\rho C_2$ è proprio un gruppo costruito con il solo ausilio di C_2 e C_n e un particolare morfismo $C_2 \to \mathrm{Aut}(C_n)$ e che potrebbe essere anche preso come definizione di D_n. Il vantaggio sulla definizione data nel Richiamo 5.2 potrebbe essere che $C_n \rtimes_\rho C_2$ ha subito dichiarata in maniera esplicita l'operazione di cui è dotata.

Richiamo 7.14. Una classe importante di prodotti semidiretti è formato da quelli della forma $N \rtimes_\theta C_n$, dove n spesso e volentieri è un numero primo. E spesso e volentieri, anche N è ciclico. E, se così è, bisogna farsi qualche idea di $\mathrm{Aut}(N)$. A tal proposito, ricordiamo un risultato di Algebra 1:

$$\mathrm{Aut}(C_n) \cong \mathbb{Z}/n\mathbb{Z}^* \text{ per ogni } n \geq 1.$$

L'omomorfismo che realizza questo isomorfismo è

$$\mathbb{Z}/n\mathbb{Z}^* \to \mathrm{Aut}(C_n)\,,\ \overline{k} \mapsto \lambda g.g^k.$$

(Ricordiamo che $\overline{k} \in \mathbb{Z}/n\mathbb{Z}^*$ se e solo se $\mathrm{mcd}(n,k) = 1$.) Questo ci dice anche esplicitamente quali sono gli elementi di $\mathrm{Aut}(C_n)$. Inoltre ricordiamo che se m e n sono coprimi, allora

$$\mathrm{Aut}(C_m \times C_n) \cong \mathrm{Aut}(C_m) \times \mathrm{Aut}(C_n).$$

Esempio 7.15 (Presentazione dei gruppi $C_n \rtimes_\theta C_m$)**.** Abbiamo i due gruppi ciclici C_m e C_n, i cui generatori sono a e b rispettivamente. Vogliamo avere un'idea più esplicita sui prodotti semidiretti $C_n \rtimes_\theta C_m$ con $\theta : C_m \to \mathrm{Aut}(C_n)$ omomorfismo. La presentazione che inizia con le informazioni sugli ordini degli elementi:

$$a^m = 1\,,\ b^n = 1.$$

Abbiamo richiamato poi che elementi di $\mathrm{Aut}(C_n)$ sono esattamente della forma

$$\lambda g.g^k \quad \text{per ogni } 0 \leq k < n\,,\ \mathrm{mcd}(k,n) = 1.$$

Poi se devo cercare gli omomorfismi $C_m \to \mathrm{Aut}(C_n)$ devo anche rispettare dei vincoli sugli ordini: $\left(\lambda g.g^k\right)^m = \lambda g.g^{k^m}$ deve essere l'identità, cioè deve valere anche

$$k^m \equiv 1 \mod n.$$

[Basta questo?] Quindi i prodotti semidiretti presentabili in questo modo:

$$\left\langle a, b \mid a^m = 1, b^n = 1, \theta_b(a) = a^k \right\rangle.$$

Sappiamo quindi come si presentano i prodotti semidiretti di due gruppi ciclici. Anche se a volte una presentazione può non essere la scelta più trasparente che ci sia, a volte si rincontrano certi gruppi notevoli che per presentazione si identificano immediatamente.

Rincontriamo il prodotto semidiretto di sottogruppi della Definizione 7.1.

Proposizione 7.16. Siano G un gruppo, $H < G$ e $N \lhd G$ tali che $G = N \rtimes H$. Consideriamo anche l'omomorfismo

$$\lambda : H \to \mathrm{Aut}(N)\,,\ \lambda_h(n) := hnh^{-1}.$$

Allora $G \cong N \rtimes_\lambda H$.

Questo è davvero notevole. Se di un gruppo sappiamo che è il prodotto semidiretto "interno" di due suoi sottogruppi, abbiamo lo strumento per scriverlo come prodotto semidiretto "esterno", il che ci dà un descrizione piuttosto esplicita. [Spiega perché e ritorna sull'esempio del gruppo diedrale di nuovo.]

Esempio 7.17 (Gruppo diedrale, di nuovo)**.** Riprendiamo in mano quello che avevamo detto all'inizio della sezione: $D_n = \langle r \rangle \rtimes \langle s \rangle$, che, come abbiamo già detto, questo è un fatto su un gruppo assegnato a priori. Ecco il passo che la Proposizione 7.16 ci permette di fare: scrivere D_n come $\langle s \rangle \rtimes_\rho \langle r \rangle$, dove

$$\rho : \langle s \rangle \to \operatorname{Aut} \langle r \rangle \ , \ \rho_{s^j} \left(r^k \right) := s^j r^k s^{-j}.$$

Qui ρ_s è il morfismo di inversione, quindi tutto torna ed è compatibile con quando abbiamo dato D_n come $C_n \rtimes_\rho C_2$ qualche esempio fa.

Dimostrazione della Proposizione 7.16. Consideriamo

$$f : N \rtimes_\lambda H \to G, \ f(n,h) := nh$$

Anzitutto è un omomorfismo: presi $(n_1, h_2), (n_2, h_2) \in N \rtimes_\lambda H$ si ha

$$\begin{aligned} f[(n_1,h_1)(n_2,h_2)] &= f\left(n_1 h_1 n_2 h_1^{-1}, h_1 h_2\right) = \\ &= n_1 h_1 n_2 h_1^{-1} h_1 h_2 = \\ &= f(n_1,h_1) f(n_2,h_2). \end{aligned}$$

La biettività è immediata, perché da ipotesi gli elementi possono essere scritti in maniera unica come prodotto di un elemento di N e di H. □

Esempio 7.18. Avevamo fornito una classificazione di questo risultato nella sezione sulle permutazioni, ma vogliamo rifarlo con le nuove idee appena introdotte. Sia G un gruppo di ordine $2p$, con $p \geq 3$ primo. Mostriamo che

$$G \cong C_{2p} \quad \text{oppure} \quad G \cong D_p.$$

Per la Proposizione 4.1, G ha esattamente un p-Sylow N, che quindi è normale, di ordine p. Ha anche qualche 2-Sylow H di ordine 2. In ogni caso, è facile verificare che $G = N \rtimes H$. La Proposizione 7.16 ci viene in contro:

$$G \cong N \rtimes_\zeta H$$

dove $\zeta : H \to \operatorname{Aut}(N)$, $\zeta_h(n) := hnh^{-1}$. Per comodità

$$H := \left\langle s \mid s^2 = 1 \right\rangle, \quad N := \langle r \mid r^p = 1 \rangle$$

Quindi: cosa fa ζ? È determinato da dove viene mandato il generatore s, la cui immagine deve essere quindi di ordine 1 (l'identità) oppure 2. Nel primo caso ζ è banale e

$$G \cong N \rtimes_\zeta H \cong N \times H.$$

Invece, nel secondo caso l'unica possibilità è che $\zeta_s : N \to N$ sia l'omomorfismo di inversione. (Questo perché Aut$N$ è ciclico e per ogni divisore d di $|\operatorname{Aut}(N)|$ ha un unico sottogruppo di ordine d. Se $d = 2$, questo ovviamente implica anche l'unicità dell'elemento di ordine 2.) Siamo quindi di nuovo al gruppo diedrale D_p:

$$G \cong N \rtimes_\zeta H \cong D_p.$$

Esempio 7.19 (Gruppi di ordine 30)**.** Vogliamo classificare un gruppo G di ordine 30.
Osservando che $30 = 2 \cdot 3 \cdot 5$, siamo nell'ambito della Proposizione 4.4: G ha quindi un unico 3-Sylow oppure un unico 5-Sylow. Se indichiamo con H_3

uno dei 3-Sylow e con H_5 uno dei 5-Sylow, abbiamo quindi che uno dei due è normale in G. Per il Richiamo 3.12, H_3H_5 è sottogruppo di G, e in particolare $H_3H_5 \cong C_3C_5 \cong C_{15}$. Questo sottogruppo è anche normale perché $[G : H_3H_5] = 2$. Sia ora H_2 uno qualunque dei 2-Sylow di G: allora si dimostra subito che $G = (H_3H_5) \rtimes H_2$. In questo caso ci viene in soccorso la Proposizione 7.16:

$$G \cong (H_3H_5) \rtimes_\zeta H_2$$

dove, al solito, $\zeta : H \to \mathrm{Aut}(N)$, $\zeta_h(n) := hnh^{-1}$. Abbiamo due casi.

- ζ è banale. Ne segue subito che $G \cong C_{30}$.
- ζ *non* è banale. Bisogna quindi vedere quali possono essere eventualmente gli omomorfismi non banali

  $$H_2 \to \mathrm{Aut}(H_3H_5).$$

  Abbiamo visto che $H_3H_5 \cong C_{15}$ e quindi di $\mathrm{Aut}(H_3H_5)$ possiamo elencare esplicitamente gli elementi e selezionare solo quelli di ordine 2:

  $$\lambda g.g^k \quad \text{per } k \in \{-4, -1, 4\}.$$

Quindi G è isomorfo ad uno di questi gruppi così presentati (vedi Esempio 7.15):

$$\left\langle r, s \mid r^{15} = 1, s^2 = 1, srs = r^k \right\rangle$$

dove con r e s abbiamo indicato rispettivamente i generatori di H_3H_5 rispettivamente. Osserviamo che per $k = -1$ riconosciamo il gruppo diedrale D_{15}. [Riusciamo a riconoscere anche gli altri due?]

Rincontreremo presto anche anche la classificazione dei gruppi di ordine pq, con p, q primi distinti. Ma prima di fare ciò è meglio armarsi di qualche strumento che può sempre far comodo.

Vediamo qui dei criteri per dire due prodotti semidiretti $N \rtimes_\alpha H$ e $N \rtimes_\beta H$ sono isomorfi. [Vedi anche i criteri proposti da [Mil] a pagina 49.]

Proposizione 7.20 (Isomorfismo tra prodotti semidiretti)**.** Siano H e N due gruppi e $\theta, \eta : H \to \mathrm{Aut}(N)$ due omomorfismi tali che $\theta = \eta \circ \alpha$ per qualche $\alpha \in \mathrm{Aut}(H)$. Allora $N \rtimes_\theta H \cong N \rtimes_\eta H$.

Dimostrazione. Poiché α è biunivoca, anche la funzione

$$f : N \rtimes_\theta H \to N \rtimes_\eta H\,,\ f(a, b) := (a, \alpha(b))$$

lo è. Inoltre f è un omomorfismo: per $a, a' \in N$ e $b, b' \in H$ si ha infatti

$$\begin{aligned} f[(a, b)(a', b')] &= f(a\theta_b(a'), bb') = \\ &= (a\theta_b(a'), \alpha(bb')) = \\ &= (a\eta_{\alpha(b)}(a'), \alpha(b)\alpha(b')) = \\ &= (a, \alpha(b))(a', \alpha(b')) = \\ &= f(a, b)f(a', b'). \end{aligned}$$

□

La Proposizione che segue è un trucchetto che useremo qualche volta negli esempi che seguono. Risponde sostanzialmente alle domande:

Esistono prodotti semidiretti $N \rtimes_\theta C_p$ con p primo che non siano prodotti diretti? Quando? Se ce ne sono, quanti ce ne sono?

Proposizione 7.21. Se H e N sono gruppi e $H \cong C_p$ per qualche primo p, allora:

1. Esiste un omomorfismo non banale $\theta : H \to \mathrm{Aut}(N)$ se e solo se p divide $|\mathrm{Aut}(N)|$.
2. Se $\mathrm{Aut}(N)$ ha un unico sottogruppo di ordine p, allora $N \rtimes_\theta H \cong N \rtimes_\eta H$ comunque scelti due omomorfismi non banali $\theta, \eta : H \to \mathrm{Aut}(N)$.

Dimostrazione. 1. Poiché θ è un omomorfismo, le immagini degli elementi di $H \cong C_p$ che non sono l'identità hanno ordine p. Se θ non è banale, allora qualcuna di queste immagini deve avere ordine p, e quindi per il Teorema di Lagrange si ha che $\mathrm{Aut}(N)$ ha ordine multiplo di p. Viceversa, $\mathrm{Aut}(N)$ ha un sottogruppo di ordine p grazie al Teorema di Sylow I, il quale è anche ciclico perché p è primo. È facile a questo punto realizzare qualche omomorfismo iniettivo $H \to \mathrm{Aut}(N)$.

2. Se H' è l'unico sottogruppo di ordine p di $\mathrm{Aut}(N)$ e θ, η sono non banali, allora sono iniettivi (qui è importante che p sia primo) e $\operatorname{im}\theta = \operatorname{im}\eta = H'$. Dunque, se scriviamo l'inclusione $i : H' \to \mathrm{Aut}(N)$, esistono isomorfismi $\widetilde{\theta}, \widetilde{\eta} : H \to H'$ tali che $\theta = i \circ \widetilde{\theta}$ e $\eta = i \circ \widetilde{\eta}$. Allora $\widetilde{\theta} = \widetilde{\theta} \circ \alpha$ e quindi $\theta = \eta \circ \alpha$ con $\alpha := \widetilde{\eta}^{-1} \circ \widetilde{\theta} \in \mathrm{Aut}(H)$. □

Una prima applicazione di questi due fatti è la Proposizione 4.1 ridimostrata alla nuova maniera.

Proposizione 7.22 (Classificazione dei gruppi di ordine pq)**.** Sia G un gruppo di ordine pq, p e q primi tali che $p < q$. Allora

1. Se $q \not\equiv 1 \mod p$, allora $G \cong C_{pq}$.
2. Se $q \equiv 1 \mod p$, allora $G \cong C_{pq}$ oppure $G \cong C_q \rtimes_\theta C_p$ per qualche omomorfismo non banale $\theta : C_p \to \mathrm{Aut}(C_q)$. Inoltre $C_q \rtimes_\theta C_p$ non è abeliano e, a meno di isomorfismo, non dipende da θ.

Dimostrazione. Usando il Teorema di Sylow notiamo che G ha unico q-Sylow N, che è anche normale, ed un qualche p-Sylow che indichiamo con H. Sono di ordine q e p rispettivamente e quindi sono ciclici: ne segue subito che $G = N \rtimes H$ e quindi per la Proposizione 7.16 abbiamo

$$G \cong N \rtimes_\zeta H$$

per qualche omomorfismo $\zeta : N \to \mathrm{Aut}(H)$. Osserviamo che $\mathrm{Aut}(N) \cong C_{q-1}$, poiché q è primo. Se $q \not\equiv 1 \mod p$ (cioè p non divide $q-1$), allora ζ è per forza di cose l'omomorfismo banale e $G \cong C_{pq}$. Se invece $q \equiv 1 \mod p$ (ovvero p divide $q-1$), allora ζ ha qualche possibilità: banale oppure no. Nel primo caso $G \cong C_{pq}$. Supponiamo che non sia banale. Qui viene in aiuto la Proposizione precedente: $\mathrm{Aut}(N) \cong C_{q-1}$ ha esattamente un sottogruppo di ordine p. Quindi a meno di isomorfismi,

$$G \cong C_q \rtimes_\theta C_p$$

dove θ è uno qualunque degli omomorfismi non banali $C_p \to \mathrm{Aut}(C_q)$. □

Richiamo 7.23 (Gruppo Q_8)**.** Il *gruppo dei quaternioni* è

$$Q_8 := \left\langle a, b \mid a^4 = 1, a^2 = b^2, bab = b^{-1} \right\rangle.$$

Un altro gruppo di ordine 8 è proprio D_4, di cui è immediato vedere che $D_4 \not\cong Q_8$. Nell'esempio che segue vediamo come i gruppi non abeliani di ordine 8 sono proprio questi due.

Esempio 7.24 (Gruppi di ordine 8)**.** [Da completare. Alcune parti sono da riscrivere meglio pure.] Sia G un gruppo non abeliano di ordine 8. Mostriamo che $G \cong Q_8$ oppure $G \cong D_4$.
Per il Teorema di Lagrange, i suoi elementi diversi dall'identità hanno ordine 2, 4 oppure 8. Una prima osservazione da fare è che G non può avere elementi di ordine 8, perché questo vorrebbe dire che G è ciclico e quindi abeliano. Quindi gli elementi di G che non sono l'identità hanno ordine 2 oppure 4.
Notiamo anche che ce ne deve essere per forza qualcuno di ordine 4. Infatti se fossero tutti di ordine 2, avremmo che per ogni $g, h \in G$

$$ghgh = 1 = gghh$$

da cui segue che $gh = hg$, e cioè G risulterebbe abeliano.
Chiamiamo a uno degli elementi di G di ordine 4 e $K := \langle a \rangle$. Poiché $[G : K] = 2$, allora K è normale in G. Sia $b \in G \setminus N$.
Poiché N è normale, allora $bab^{-1} \in N$ ed ha lo stesso ordine di a, vale a dire 4. [La coniugazione rispetta l'ordine di un elemento. Ne ho scritto?] Quindi bab^{-1} è a oppure a^{-1}. Se è a, allora vuole dire che $ab = ba$, e che quindi l'intero gruppo è abeliano. [Riscrivere meglio.] Quindi rimane

$$bab^{-1} = a.$$

Se ord $b = 2$, allora è isomorfo a D_4 mentre se ord $b = 4$, allora è Q_8. (Vedi le presentazioni dei gruppi premesse a questo esempio.)

Osservazione 7.25. Sia G un gruppo non abeliano di ordine 12. Classifichiamolo.
Per la Proposizione 4.2, uno dei suoi sottogruppi di Sylow è normale. I suoi gruppi di Sylow sono di ordine 3 oppure 4. Quindi, tanto per iniziare da qualche parte, possiamo scrivere

$$G = N \rtimes H$$

dove N è un sottogruppo di Sylow normale e H è un sottogruppo di Sylow di cardinalità diversa da N. I 3-Sylow sono tutti ciclici, mentre per i 4-Sylow bisogna discuterne: hanno cardinalità 4 e quindi possono essere C_4 oppure $C_2 \times C_2$.
Caso $N \cong C_4$ e $H \cong C_3$. Qui $\mathrm{Aut}(C_4)$ è di ordine 2, quindi è ciclico. Allora c'è un unico omomorfismo $C_3 \to \mathrm{Aut}(C_4)$, quello banale. Ma allora G è abeliano, e quindi questa strada è da abbandonare.
Caso $N \cong C_2 \times C_2$ e $H \cong C_3$. Allora $\mathrm{Aut}(C_2 \times C_2) \cong S_3$. [Scrivere di questo da qualche parte!] Esiste allora un omomorfismo non banale $\theta : H \to \mathrm{Aut}(N)$. Inoltre, S_3, e quindi $\mathrm{Aut}(C_2 \times C_2)$, ha un solo sottogruppo di ordine 3. [Chiaro, no?] E quindi $G \cong N \rtimes_\theta H$. Possiamo concludere che $G \cong A_4$. [Non ho capito perché.]
Caso $N \cong C_3$ e $H \cong C_4$. Allora $\mathrm{Aut}(K) \cong C_2$ e c'è un omomorfismo non banale $H \to \mathrm{Aut}(N)$. Ed è unico anche! In questo caso $G \cong C_3 \rtimes_! C_4$.
Rimane da prendere in esame il caso in cui $K \cong C_3$ e $H \cong C_2 \times C_2$. [Qui non si è capito niente invece.]

A questo punto siamo in grado di classificare i gruppi di ordine ≤ 15: in Figura 2 c'è un riassunto.

n	classi di isomorfismo di gruppi di ordine n			
2	C_2			
3	C_3			
4	C_4	$C_2 \times C_2$		
5	C_5			
6	C_6	$C_3 \rtimes C_2 \cong D_3$		
7	C_7			
8	C_8	$C_4 \times C_2$	C_2^3	$C_4 \rtimes C_2 \cong D_4$	Q_8
9	C_9	$C_3 \times C_3$		
10	C_{10}	$C_5 \rtimes C_2 \cong D_5$		
11	C_{11}			
12	C_{12}	$C_6 \times C_2$	$C_2^2 \rtimes C_3 \cong A_4$	$C_3 \rtimes C_2^2 \cong D_6$	$C_3 \rtimes C_4$
13	C_{13}			
14	C_{14}	$C_7 \rtimes C_2 \cong D_7$		
15	C_{15}			

Figura 2. Classificazione dei gruppi di ordine ≤ 15.

8 Gruppi abeliani finiti

9 Esercizi

Esercizio 9.1. 1. $|G| = p^3$ (p primo), G non abeliano $\Rightarrow Z(G) = [G, G] \cong C_p$ e $G/Z(G) \cong C_p^2$.

2. Per ogni primo p esiste un gruppo non abeliano di ordine p^3.

Svolgimento. 1. $G \neq \{1\}$ p-gruppo $\Rightarrow Z(G) \neq \{1\} \Rightarrow [G : Z(G)] \neq p^3$. G non abeliano $\Rightarrow G/Z(G)$ non ciclico $\Rightarrow [G : Z(G)] \neq 1, p$. Dunque $[G : Z(G)] = p^2 \Rightarrow G/Z(G) \cong C_p^2$ abeliano $\Rightarrow [G, G] < Z(G) \cong C_p$ semplice. G non abeliano $\Rightarrow [G, G] \neq \{1\} \Rightarrow [G, G] = Z(G)$.

2. $\exists \theta : C_p \to \mathrm{Aut}(C_{p^2})$ omomorfismo non banale (perché $p \mid \left|\mathrm{Aut}(C_{p^2})\right| = |\mathbb{Z}/p^2\mathbb{Z}^*| = p(p-1)$) $\Rightarrow G := C_{p^2} \rtimes_\theta C_p$ non abeliano tale che $|G| = \left(\left|C_{p^2}\right|\right)\left(\left|C_p\right|\right) = p^2 p = p^3$. □