Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2020/2021
Teoria dei gruppi

Testi di riferimento

Per la parte di teoria dei gruppi possono essere utili soprattutto i seguenti testi.

- J.S. Milne, *Group Theory*, disponibile all'indirizzo `http://www.jmilne.org/math/CourseNotes/gt.html`
  Parti dei capitoli 3 (prodotti semidiretti), 4 (azioni e gruppi di permutazioni), 5 (teorema di Sylow) e 6 (gruppi risolubili).
- I.N. Herstein, *Algebra*
  Sezioni 2.9, 2.11 (alcuni risultati sulle azioni), 2.12 (teorema di Sylow) e 5.7 (gruppi risolubili).

Azioni di gruppi

Definizione

Un'azione di un gruppo G su un insieme X è una funzione

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

tale che $\forall\, g, h \in G$ e $\forall\, x \in X$ si ha:

(A1) $(gh)x = g(hx)$;

(A2) $1x = x$.

Si dice anche che X è un G-insieme.

Osservazione

La condizione (A2) non è ridondante: fissato $x_0 \in X$, la funzione

$$G \times X \to X \qquad (g, x) \mapsto x_0$$

soddisfa (A1), ma non (A2) se $\#X > 1$.

Azioni come omomorfismi

Proposizione

Se X è un G-insieme, $\forall\, g \in G$ la funzione

$$\varphi(g)\colon X \to X \qquad x \mapsto gx$$

è biunivoca. Inoltre $\varphi\colon G \to S(X)$ (dove $S(X)$ indica il gruppo delle permutazioni di X) è un omomorfismo di gruppi.

Viceversa, dato un omomorfismo di gruppi $\varphi\colon G \to S(X)$, la funzione

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

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

Dimostrazione

Se X è un G-insieme, per (A1) $\forall\, g, h \in G$ e $\forall\, x \in X$

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

quindi $\varphi(gh) = \varphi(g) \circ \varphi(h)$, e resta da vedere che $\varphi(g) \in S(X)$. Per (A2) $\varphi(1)(x) = 1x = x = \mathrm{id}_X(x)$, per cui $\varphi(1) = \mathrm{id}_X$. Allora

$$\varphi(g)\circ\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = \mathrm{id}_X = \varphi(g^{-1}g) = \varphi(g^{-1})\circ\varphi(g),$$

il che dimostra che $\varphi(g)$ è biunivoca (con inversa $\varphi(g^{-1})$).

Viceversa, se $\varphi\colon G \to S(X)$ è un omomorfismo di gruppi, $\forall\, g, h \in G$ e $\forall\, x \in X$

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

cioè vale (A1). Inoltre $\varphi(1) = \mathrm{id}_X$, per cui $1x = \varphi(1)(x) = \mathrm{id}_X(x) = x$, cioè vale (A2).

Esempi

- $gx = x \; \forall g \in G$ e $\forall x \in X$ (azione banale), corrispondente all'omomorfismo banale $G \to S(X)$.
- $G < S(X) \implies X$ è un G-insieme con l'omomorfismo di inclusione $G \to S(X)$.
- $H < G \implies$ un G-insieme X definito da un omomorfismo $\varphi\colon G \to S(X)$ è anche un H-insieme con $\varphi|_H\colon H \to S(X)$. Più in generale, dato un omomorfismo di gruppi $f\colon G' \to G$, X è anche un G'-insieme con $\varphi \circ f\colon G' \to S(X)$.
- Se X è munito di qualche struttura (gruppo, spazio vettoriale, spazio topologico, spazio metrico, ...) di solito è interessante vedere X come G-insieme per qualche omomorfismo $G \to \mathrm{Aut}(X) < S(X)$, dove $f \in S(X)$ è un "automorfismo" se preserva la struttura (isomorfismo di gruppi, isomorfismo di spazi vettoriali, omeomorfismo, isometria, ...).

Azione per coniugio

L'azione per coniugio di G su G è definita da

$$G \times G \to G \qquad (g, a) \mapsto gag^{-1}$$

(vale (A1) perché $(gh)a(gh)^{-1} = g(hah^{-1})g^{-1}\ \forall\, g, h, a \in G$ e (A2) perché $1a1^{-1} = a$).
Il corrispondente omomorfismo di gruppi $\Gamma\colon G \to S(G)$ è tale che

$$\mathrm{Int}(G) := \mathrm{im}(\Gamma) < \mathrm{Aut}(G) < S(G)$$

(dove $\mathrm{Aut}(G) := \{f \in S(G) \ :\ f \text{ omomorfismo}\}$ è il gruppo degli automorfismi di G) perché $\forall\, g, a, b, \in G$

$$\Gamma(g)(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \Gamma(g)(a)\Gamma(g)(b).$$

Gli elementi di $\mathrm{Int}(G)$ si dicono automorfismi interni di G.
Ricordiamo anche che

$$\ker(\Gamma) = \{g \in G \ :\ \Gamma(g)(a) = gag^{-1} = a\ \forall\, a \in G\} = Z(G).$$

Azione per traslazione

L'azione per traslazione (o per moltiplicazione) a sinistra di G su G è definita da

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

(vale (A1) perché il prodotto di G è associativo e (A2) perché 1 è elemento neutro). Il corrispondente omomorfismo di gruppi $L\colon G \to S(G)$ è iniettivo (teorema di Cayley).

Analogamente, dato $H < G$, la funzione

$$G \times G/H \to G/H \qquad (g, C) \mapsto gC := \{gc \; : \; c \in C\}$$

(ben definita perché se $C = aH$, $gC = g(aH) = (ga)H$) è un'azione (esercizio). Indicheremo ancora con $L\colon G \to S(G/H)$ il corrispondente omomorfismo di gruppi (in generale non iniettivo).

Sottoinsiemi G-stabili

Un'azione di G su X ne induce una naturale di G su $\mathcal{P}(X)$:

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

(la verifica che questa è davvero un'azione è lasciata per esercizio).

Definizione

Un sottoinsieme X' di un G-insieme X è G-stabile o G-invariante se $gX' = X' \;\forall\, g \in G$.

Osservazione

Un sottoinsieme G-stabile di un G-insieme è in modo naturale un G-insieme (per restrizione dell'azione a $G \times X'$).

Osservazione

Un sottoinsieme X' di un G-insieme X è G-stabile se e solo se $gX' \subseteq X' \;\forall\, g \in G$. Infatti, se quest'ultima condizione è soddisfatta, allora $\forall\, g \in G$ si ha anche (dato che $g^{-1}X' \subseteq X'$)

$$X' = 1X' = (gg^{-1})X' = g(g^{-1}X') \subseteq gX'.$$

Sia H un sottogruppo di G ($H < G$).

- H è G-stabile (rispetto all'azione per coniugio) $\iff$ H è $\mathrm{Int}(G)$-stabile $\iff$ $gHg^{-1} = H \; \forall g \in G$ $\iff$ $gHg^{-1} \subseteq H$ $\forall g \in G$; in questo caso si dice che H è normale in G ($H \lhd G$).
- H è $\mathrm{Aut}(G)$-stabile $\iff$ $f(H) = H \; \forall f \in \mathrm{Aut}(G)$ $\iff$ $f(H) \subseteq H \; \forall f \in \mathrm{Aut}(G)$; in questo caso si dice che H è caratteristico in G.

Osservazione

Ogni sottogruppo caratteristico è normale, ma non viceversa.
Per esempio, i sottogruppi non banali di C_2^2 sono normali ma non caratteristici.

Esempio

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.

Morfismi di G-insiemi

Se X e Y sono G-insiemi, una funzione $f\colon X \to Y$ è un morfismo di G-insiemi (o di azioni di G) se $f(gx) = gf(x)\ \forall\, g \in G$ e $\forall\, x \in X$. f è un isomorfismo di G-insiemi se è anche biunivoco.

Osservazione

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

Esempio

Se X' è un sottoinsieme G-stabile di un G-insieme X, l'inclusione $X' \to X$ è un morfismo di G-insiemi.

Esempio

$H < G \implies G \to G/H$, $a \mapsto aH$ è un morfismo di G-insiemi (rispetto alla traslazione), e è un isomorfismo $\iff H = \{1\}$.

Orbite di un'azione

Su un G-insieme X la relazione definita da

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

è di equivalenza, dato che valgono le proprietà

- riflessiva: $x = 1x$;
- simmetrica: $y = gx \implies x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$;
- transitiva: $y = gx$, $z = hy \implies z = h(gx) = (hg)x$.

La classe di equivalenza di $x \in X$ è il sottoinsieme

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

di X e si dice orbita di x (rispetto all'azione di G).

Osservazione

Un sottoinsieme di un G-insieme è G-stabile se e solo se è unione (necessariamente disgiunta) di orbite.

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

Se $H < G$, il G-insieme G/H (rispetto all'azione per traslazione a sinistra) è omogeneo: $\forall\, C \in G/H\ \exists\, g \in G$ tale che $C = gH$, cioè C appartiene all'orbita di H.

Esempio

Rispetto all'azione per coniugio di G su G, l'orbita di $a \in G$ è la classe di coniugio $[a] := \{gag^{-1} : g \in G\}$ di a.
Si ha $[a] = \{a\} \iff a \in Z(G)$, e in particolare $[1] = \{1\}$.
Dunque l'azione è transitiva $\iff G = \{1\}$.

Stabilizzatori, azioni libere e azioni fedeli

Se X è un G-insieme, lo stabilizzatore di $x \in X$ è

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

perché $1 \in \mathrm{Stab}(x)$ e $g, h \in \mathrm{Stab}(x) \implies gh^{-1} \in \mathrm{Stab}(x)$:
$(gh^{-1})x = (gh^{-1})(hx) = g((h^{-1}h)x) = gx = x$.

Definizione

Un'azione di G su X è libera (risp. fedele) se $\mathrm{Stab}(x) = \{1\}$ $\forall\, x \in X$ (risp. $\bigcap_{x \in X} \mathrm{Stab}(x) = \{1\}$).

Osservazione

Se l'azione è data da un omomorfismo di gruppi $\varphi \colon G \to S(X)$,

$$\ker(\varphi) = \{g \in G \,:\, gx = x \ \forall\, x \in X\} = \bigcap_{x \in X} \mathrm{Stab}(x).$$

Centralizzatore di un elemento

Lo stabilizzatore di $a \in G$ rispetto all'azione per coniugio è

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

detto centralizzatore o (centralizzante) di a in G.

Osservazione

Poiché $C(1) = G$, l'azione per coniugio è libera $\iff G = \{1\}$.
D'altra parte l'azione è fedele $\iff$

$$\{1\} = \bigcap_{a \in G} C(a) = \ker(\Gamma \colon G \to S(G)) = Z(G).$$

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

Normalizzatore di un sottogruppo

Considerando $\mathcal{P}(G)$ come un G-insieme con l'azione indotta dal coniugio, lo stabilizzatore di $H < G$ è

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

detto normalizzatore o (normalizzante) di H in G.

Osservazione

Chiaramente $N(H)$ soddisfa le seguenti condizioni:

- $H \triangleleft N(H) < G$;
- $H \triangleleft K < G \implies K \subseteq N(H)$.

Dunque $N(H)$ è il più grande sottogruppo di G in cui H è normale. In particolare $N(H) = G \iff H \triangleleft G$.

Relazione tra gli stabilizzatori in un orbita

Proposizione

Se X è un G-insieme, $\forall\, g \in G$ e $\forall\, x \in X$

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

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

Dimostrazione.

$\mathrm{Stab}(gx) \subseteq g\mathrm{Stab}(x)g^{-1}$: $h \in \mathrm{Stab}(gx) \implies gx = hgx \implies x = g^{-1}gx = g^{-1}hgx \implies h' := g^{-1}hg \in \mathrm{Stab}(x) \implies h = gh'g^{-1} \in g\mathrm{Stab}(x)g^{-1}$.

$g\mathrm{Stab}(x)g^{-1} \subseteq \mathrm{Stab}(gx)$: $h = gh'g^{-1} \in g\mathrm{Stab}(x)g^{-1}$ (con $h' \in \mathrm{Stab}(x)$) $\implies hgx = gh'g^{-1}gx = gh'x = gx \implies h \in \mathrm{Stab}(gx)$. □

Esempio

$C(gag^{-1}) = gC(a)g^{-1}\ \forall\, g, a \in G$.

Corollario

$H < G \implies \ker(L\colon G \to S(G/H)) = \bigcap_{g\in G} gHg^{-1}$ è il più grande sottogruppo normale di G contenuto in H.

Dimostrazione.

$\ker(L) \triangleleft G$ perché nucleo di un omomorfismo di gruppi. Poiché

$$\mathrm{Stab}(H) = \{g \in G \,:\, gH = H\} = H,$$

e tenendo conto che $\ker(L) = \bigcap_{C\in G/H} \mathrm{Stab}(C)$, per la Proposizione precedente si ha

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

Resta da dimostrare che $K \triangleleft G$ e $K \subseteq H \implies K \subseteq \ker(L)$:
$K = \bigcap_{g\in G} gKg^{-1} \subseteq \bigcap_{g\in G} gHg^{-1} = \ker(L)$. □

Applicazione

Se $L\colon G \to S(G/H)$ è iniettivo, $G \cong \mathrm{im}(L) < S(G/H)$. Dunque, se $H \neq G$ e $S(G/H)$ non contiene sottogruppi isomorfi a G,

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

e in particolare G non è semplice (dato che $\ker(L) \triangleleft G$).

Osservazione

Per il teorema di Lagrange $S(G/H)$ non contiene sottogruppi isomorfi a G se G è finito e $\#G \nmid [G:H]!$.

Esempio

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 $150 \nmid 6! = 720$.

Proposizione

Sia X un G-insieme. Allora $\forall\, x \in X$ la funzione

$$f\colon G/\mathrm{Stab}(x) \to Gx \qquad \bar{a} := a\mathrm{Stab}(x) \mapsto ax$$

è un isomorfismo di G-insiemi.

Dimostrazione.

f è ben definita: $\overline{a'} = \bar{a}$ (cioè $a' = ab$ con $b \in \mathrm{Stab}(x)$) $\implies$ $a'x = (ab)x = a(bx) = ax$.

f è un morfismo di G-insiemi: $\forall\, g, a \in G$ $f(g\bar{a}) = f(\overline{ga}) = (ga)x = g(ax) = gf(\bar{a})$.

f è suriettiva: $\forall\, a \in G$ $ax = f(\bar{a})$.

f è iniettiva: $a, a' \in G$ tali che $f(\bar{a}) = f(\overline{a'})$ (cioè $ax = a'x$) $\implies$ $x = a^{-1}ax = a^{-1}a'x \implies a^{-1}a' \in \mathrm{Stab}(x) \implies \bar{a} = \overline{a'}$. □

Conseguenze

Sia X un G-insieme.

- X è omogeneo $\iff X \cong G/H$ per qualche $H < G$.
- $\#(Gx) = [G : \mathrm{Stab}(x)]\ \forall\, x \in X$.
- $\#[a] = [G : C(a)]$ (con $[a] := \{gag^{-1} : g \in G\}$) $\forall\, a \in G$.
- $\#[H] = [G : N(H)]$ (con $[H] := \{gHg^{-1} : g \in G\}$) $\forall\, H < G$.
- X finito, $X = \coprod_{i=1}^{n} Gx_i \implies \#X = \sum_{i=1}^{n} [G : \mathrm{Stab}(x_i)]$.
- G finito, $G = \coprod_{i=1}^{n} [a_i] \implies \#G = \sum_{i=1}^{n} [G : C(a_i)]$.
  Posso supporre che esista $0 \le m \le n$ tale che $a_i \in Z(G)$ ($\iff \#[a_i] = [G : C(a_i)] = 1$) $\iff i > m$. Si ottiene allora l'equazione delle classi:

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

(con $1 < [G : C(a_i)] \mid \#G\ \forall\, i = 1, \ldots, m$).

Definizione

Sia p un numero primo. Un p-gruppo è un gruppo (finito) il cui ordine è una potenza di p.

Proposizione

$G \neq \{1\}$ *p-gruppo* $\implies Z(G) \neq \{1\}$.

Dimostrazione.

Per l'equazione delle classi

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

Per ipotesi $\#G = p^n$ per qualche $n > 0$ e $[G : C(a_i)] = p^{n_i}$ con $0 < n_i \leq n$; in particolare $p \mid \#G$ e $p \mid [G : C(a_i)]\ \forall\, i = 1, \ldots, m$. Allora $p \mid \#Z(G)$, e quindi $Z(G) \neq \{1\}$. $\square$

Corollario

$\#G = p^n \implies \forall\, m$ tale che $0 \leq m \leq n \;\exists\, H \lhd G$ tale che $\#H = p^m$. In particolare G è semplice $\iff n = 1 \iff G \cong C_p$.

Dimostrazione.

Per induzione su n: $n = 0$ ovvio.

Se $n > 0$, posso supporre $m > 0$. Per la Proposizione precedente $\#Z(G) = p^{n'}$ con $0 < n' \leq n$. Esiste $K < Z(G)$ tale che $\#K = p$ (perché $p \mid \#Z(G)$ e $Z(G)$ è abeliano). Poiché $K \lhd G$ ($\forall\, g \in G$ e $\forall\, a \in K$ si ha $gag^{-1} = a \in K$), $\overline{G} := G/K$ è un gruppo tale che

$$\#\overline{G} = \frac{\#G}{\#K} = \frac{p^n}{p} = p^{n-1}.$$

Per l'ipotesi induttiva esiste $\overline{H} \lhd \overline{G}$ tale che $\#\overline{H} = p^{m-1}$; inoltre $\exists!\, H \lhd G$ tale che $\overline{H} = H/K$, per cui

$$\#H = (\#\overline{H})(\#K) = p^{m-1}p = p^m.$$

Lemma

Un gruppo G è abeliano $\iff$ $G/Z(G)$ è ciclico.

Dimostrazione.

$\implies$ $Z(G) = G \implies \overline{G} := G/Z(G) = \{\bar{1}\}$ è ciclico.

$\impliedby$ $\overline{G} = \langle \bar{g} \rangle$ (con $g \in G$) $\implies \forall\, a \in G\ \exists\, n \in \mathbb{Z}$ tale che $\bar{a} = \bar{g}^n$ $\implies \exists\, b \in Z(G)$ tale che $a = g^n b \implies a \in C(g)$ (perché $g, b \in C(g)$) $\implies C(g) = G \implies g \in Z(G) \implies \bar{g} = \bar{1}$ $\implies \overline{G} = \langle \bar{1} \rangle = \{\bar{1}\} \implies Z(G) = G \implies G$ abeliano.

□

Corollario

$\#G = p^2 \implies G$ abeliano (quindi $G \cong C_{p^2}$ o $G \cong C_p^2$).

Dimostrazione.

Per la Proposizione $1 < \#Z(G) \mid p^2 \implies \#Z(G) = p$ o $p^2 \implies \#(G/Z(G)) = p$ o $1 \implies G/Z(G)$ ciclico $\implies G$ abeliano. □

Il teorema di Sylow (prima parte)

Teorema (Sylow)

G gruppo finito, p numero primo, $l \in \mathbb{N}$ tali che $p^l \mid \#G \implies \exists\, H < G$ tale che $\#H = p^l$.

Corollario (teorema di Cauchy)

G gruppo finito, p numero primo tale che $p \mid \#G \implies \exists\, H < G$ tale che $\#H = p$ e $\exists\, g \in G$ tale che $\mathrm{ord}(g) = p$.

Osservazione

Per dimostrare il teorema di Cauchy basta trovare $a \in G$ tale che $\mathrm{ord}(a) = pm$ per qualche $m > 0$, (poi $g := a^m$ e $H := \langle g \rangle$).
Se G è abeliano, ciò può essere dimostrato facilmente per induzione su $n := \#G$. Per $n > p$ (il caso $n = p$ è chiaro) sia $b \in G \setminus \{1\}$:

- $p \mid \mathrm{ord}(b) \implies a := b$;
- $p \nmid \mathrm{ord}(b) \implies \overline{G} := G/\langle b \rangle$ tale che $p \mid \#\overline{G} < n \implies$ per induzione $\exists\, \bar{a} \in \overline{G}$ (con $a \in G$) tale che $p \mid \mathrm{ord}(\bar{a}) \mid \mathrm{ord}(a)$.

Dimostrazione della prima parte del teorema di Sylow

Per induzione su $n := \#G$. Per $n > p^l$ (il caso $n = p^l$ è chiaro) considero l'equazione delle classi:

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

con $1 < [G : C(a_i)] \mid n$ (quindi $C(a_i) \subsetneq G$) $\forall\, i = 1, \ldots, m$.

- Se $\exists\, i = 1, \ldots, m$ tale che $p^l \mid \#C(a_i)$, allora per induzione $\exists\, H < C(a_i) < G$ tale che $\#H = p^l$.
- Altrimenti $p \mid [G : C(a_i)]\ \forall\, i = 1, \ldots, m$.
- Posso supporre $l > 0 \implies p \mid \#G \implies p \mid \#Z(G)$.
- Per il teorema di Cauchy per gruppi abeliani $\exists\, K < Z(G)$ tale che $\#K = p$; inoltre $K \lhd G$.
- $\overline{G} := G/K$ tale che $p^{l-1} \mid \#\overline{G} = n/p < n \implies$ per induzione $\exists\, \overline{H} < \overline{G}$ tale che $\#\overline{H} = p^{l-1}$.
- $\exists!\, H < G$ tale che $\overline{H} = H/K \implies \#H = (\#\overline{H})(\#K) = p^l$.

Definizione

G gruppo finito, p numero primo, r, m interi positivi tali che $\#G = p^r m$ e $p \nmid m$. Un p-sottogruppo di Sylow (o semplicemente un p-Sylow) di G è un sottogruppo di G di ordine p^r.
Indichiamo con $s_p = s_p(G)$ il numero di p-Sylow di G.

Osservazione

$s_p \geq 1$ per la prima parte del teorema di Sylow.

Teorema (Sylow)

G gruppo finito, p numero primo, r, m interi positivi tali che $\#G = p^r m$ e $p \nmid m$ $\implies$

1. *due qualunque p-Sylow di G sono coniugati;*
2. *$s_p \equiv 1 \mod p$ e $s_p = [G : N(H)] \mid m \ \forall H$ p-Sylow di G;*
3. *ogni p-sottogruppo di G è contenuto in un p-Sylow di G.*

Richiami sul prodotto di sottogruppi

$H, K < G$.

- $HK := \{ab \,:\, a \in H,\; b \in K\} < G \iff HK = KH$.
- $H \lhd G$ o $K \lhd G \implies HK < G$.
- $H, K \lhd G \implies HK \lhd G$.
- la funzione (con immagine HK)

  $$H \times K \to G \qquad (a, b) \mapsto ab$$

  è un omomorfismo di gruppi $\iff ab = ba \; \forall\, a \in H$ e $\forall\, b \in K$, e in tal caso il suo nucleo è $H \cap K$.
- $H, K \lhd G$ e $H \cap K = \{1\} \implies HK \cong H \times K$.
- H e K finiti $\implies$

  $$\#(HK) = \frac{(\#H)(\#K)}{\#(H \cap K)}.$$

Orbite di un p-Sylow

$\forall\, H, K < G$ sia $[K]_H := \{aKa^{-1} \,:\, a \in H\} \subseteq [K] = [K]_G$.
Chiaramente $[K]_H = \{K\} \iff H \subseteq N(K)$.

Lemma

$H, K < G$ con H p-gruppo e K p-Sylow.
Allora $[K]_H = \{K\} \iff H \subseteq K$. Altrimenti $p \mid \#[K]_H$.

Dimostrazione.

$\#[K]_H = [H : N(K) \cap H] \mid \#H = p^l$ per qualche $l \in \mathbb{N}$, quindi $p \mid \#[K]_H$ se $\{K\} \subsetneq [K]_H$.
Resta allora da dimostrare che $H \subseteq N(K) \implies H \subseteq K$.
$H < N(K)$, $K \lhd N(K) \implies HK < N(K) < G$.
$H' := H \cap K < H$ tale che $\#H' = p^{l'}$ (con $l' \leq l$). Se $\#K = p^r$,

$$\#(HK) = \frac{(\#H)(\#K)}{\#H'} = \frac{p^l p^r}{p^{l'}} = p^{r+l-l'} \mid \#G = p^r m$$

con $p \nmid m \implies r + l - l' \leq r \implies l' = l \implies H' = H \subseteq K$. $\square$

Dimostrazione della seconda parte del teorema di Sylow

Sia H un p-Sylow di G.
Se $K \in [H]_G$, chiaramente $[K]_H \subseteq [K]_G = [H]_G$ e per il Lemma $[K]_H = \{K\} \iff H \subseteq K \iff H = K$ (perché $\#H = \#K$), e altrimenti $p \mid \#[K]_H$. Ne segue che

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

Sia ora $H' < G$ un p-gruppo: analogamente a prima $[K]_{H'} \subseteq [K]_G = [H]_G \; \forall \, K \in [H]_G$, e per il Lemma $p \mid \#[K]_{H'}$ se $H' \not\subseteq K$. 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

Se $H < G$ è un p-Sylow, allora

$$H \triangleleft G \iff H \text{ caratteristico in } G \iff s_p = 1.$$

È infatti chiaro che $s_p = 1 \implies H$ caratteristico in $G \implies H \triangleleft G$.
D'altra parte, $H \triangleleft G \implies N(H) = G$, quindi $s_p = [G : N(H)] = 1$.

Corollario

$\#G = \prod_{i=1}^k p_i^{n_i}$ con $p_1, \dots, p_k$ numeri primi distinti e $n_1, \dots, n_k > 0$. Sia H_i un p_i-Sylow di G $\forall\, i = 1, \dots, k$.

1. $s_{p_1} = \cdots = s_{p_k} = 1 \implies G \cong \prod_{i=1}^k H_i$.
2. $G \cong \prod_{i=1}^k G_i$ *con* G_i p_i*-gruppo* $\forall\, i = 1, \dots, k \implies s_{p_i} = 1$ *e* $G_i \cong H_i$ $\forall\, i = 1, \dots, k$.

Dimostrazione

1. Per ipotesi $H_i \lhd G$ e $\# H_i = p_i^{n_i}$ $\forall\, i = 1, \dots, k$.
   Dimostro per induzione su j che
   $$H'_j := H_1 \cdots H_j \lhd G \quad \text{e} \quad H'_j \cong \prod_{i=1}^{j} H_i \quad \forall\, j = 1, \dots, k.$$
   È ovvio per $j = 1$; se $j > 1$, per induzione $H'_{j-1} \lhd G$ e $H'_{j-1} \cong \prod_{i=1}^{j-1} H_i$ (per cui $\# H'_{j-1} = \prod_{i=1}^{j-1} p_i^{n_i}$). Allora $H'_j = H'_{j-1} H_j \lhd G$ e (tenendo conto che $H'_{j-1} \cap H_j = \{1\}$ perché $\mathrm{mcd}(\# H'_{j-1}, \# H_j) = 1$) $H'_j \cong H'_{j-1} \times H_j \cong \prod_{i=1}^{j} H_i$.
   Se ne deduce che $G = H'_k \cong \prod_{i=1}^{k} H_i$ perché $\# G = \# H'_k$.
2. $G' := \prod_{i=1}^{k} G_i \implies \forall\, i = 1, \dots, k$
   $$G'_i := \{(a_1, \dots, a_k) \in G' \,:\, a_j = 1 \;\forall\, j \neq i\} \lhd G',$$
   G'_i è un p_i-Sylow di G' e $G'_i \cong G_i$. Allora $s_{p_i}(G) = s_{p_i}(G') = 1$ e $H_i \cong G'_i \cong G_i$ $\forall\, i = 1, \dots, k$.

$\#G = pq$ con $p < q$ numeri primi. Allora

- $s_q = 1$ (perché $s_q \equiv 1 \mod q$ e $s_q \mid p$), e quindi G non è semplice;
- $q \not\equiv 1 \mod p \implies s_p = 1$ (perché $s_p \equiv 1 \mod p$ e $s_p \mid q$) e

$$G \cong C_p \times C_q \cong C_{pq}$$

(perché per il Corollario $G \cong H_p \times H_q$ con $H_p \cong C_p$ p-Sylow e $H_q \cong C_q$ q-Sylow).

Osservazione

Si vedrà che $q \equiv 1 \mod p \implies \exists!$ (a meno di isomorfismo) un gruppo non abeliano di ordine pq. Un esempio (per $p = 2$) è il gruppo diedrale D_q.

Gruppi di ordine $p^2 q$

$\#G = p^2 q$ con p e q numeri primi distinti $\implies s_p = 1$ o $s_q = 1$ (quindi G non è semplice).

- Se $p > q$, allora $s_p = 1$ (perché $s_p \equiv 1 \mod p$ e $s_p \mid q$).
- Se $p < q$ e $s_q > 1$, allora $s_q = p^2$ (perché $s_q \equiv 1 \mod q$ e $s_q \mid p^2$). Poiché ogni q-Sylow ha $q - 1$ elementi di ordine q e q-Sylow distinti si intersecano banalmente,

  $$T := \{a \in G \,:\, \mathrm{ord}(a) = q\}$$

  è tale che $\#T = s_q(q-1) = p^2(q-1)$.
  H p-Sylow $\implies H \subseteq G \setminus T \implies H = G \setminus T$ (perché $\#(G \setminus T) = p^2 = \#H$) $\implies s_p = 1$.

Osservazione

Se $p < q$ e $s_q > 1$, allora $p = 2$ e $q = 3$:
infatti $s_q = p^2 \equiv 1 \mod q$, cioè $q \mid (p^2 - 1) = (p-1)(p+1)$;
poiché $q \nmid (p-1)$, deve essere $q \mid (p+1) \leq q$, e quindi $q = p + 1$.
Un esempio di questo tipo è $G = A_4$ (esercizio).

Gruppi di ordine *pqr*

$\#G = pqr$ con $p < q < r$ numeri primi $\implies s_q = 1$ o $s_r = 1$ (quindi G non è semplice).

- $T_n := \{a \in G \,:\, \mathrm{ord}(a) = n\}\ \forall\, n > 0 \implies$ analogamente a prima $\#T_q = s_q(q-1)$ e $\#T_r = s_r(r-1)$. Deve essere
$$s_q(q-1) + s_r(r-1) = \#(T_q \cup T_r) \le \#G = pqr,$$
dato che $T_q \cap T_r = \emptyset$.
- $s_r > 1 \implies s_r = pq$ (perché $s_r \equiv 1 \mod r$ e $s_r \mid pq$) $\implies s_q(q-1) \le pq \implies s_q \le q$ (dato che $q - 1 \ge p$) $\implies s_q = 1$ (perché $s_q \equiv 1 \mod q$).

$\{1\} \neq H < G$ tale che $2 \leq [G : H] \leq 4 \implies G$ non semplice.

- Per assurdo G semplice $\implies L\colon G \to S(G/H)$ è un omomorfismo iniettivo $\implies G' := \mathrm{im}(L) < S(G/H) \cong S_m$ (con $m := [G : H]$) tale che $G' \cong G$ e $n := \#G = \#G'$ soddisfa $m \mid n \mid m!$ (per il teorema di Lagrange) e $n > m$ (perché $H \neq \{1\}$).
- $m = 2 \implies 2 \mid n \mid 2$ e $n > 2$, impossibile.
- $m = 3 \implies 3 \mid n \mid 6$ e $n > 3 \implies n = 6 = 2 \cdot 3 \implies G$ non semplice, assurdo.
- $m = 4 \implies 4 \mid n \mid 24$ e $n > 4 \implies n = 8 = 2^3$ o $n = 12 = 2^2 \cdot 3$ o $n = 24$ ($\implies G \cong S_4$) $\implies G$ non semplice, assurdo.

Osservazione

Segue che G non è semplice se $\exists\, p$ primo tale che $p \mid \#G$ e $s_p = 3$ ($\implies p = 2$) o $s_p = 4$ ($\implies p = 3$).

Esercizio

G non abeliano, $n := \#G < 60 \implies G$ non semplice.

- $n = p^k$ (p primo, $k > 2$) $\implies G$ non semplice (già visto).
- n divisibile per 3 primi distinti p, q e $r \implies n = pqr$ (se no $n \geq 2pqr \geq 2 \cdot 2 \cdot 3 \cdot 5 = 60$) $\implies G$ non semplice (già visto).
- Resta il caso $n = p^i q^j$ con p, q primi distinti e $i, j > 0$.
- $i, j \geq 2 \implies i = j = 2$ (se no $n \geq 2p^2q^2 \geq 2 \cdot 2^2 \cdot 3^2 = 72$) $\implies n = 2^2 \cdot 3^2 = 36$ (se no $n \geq 2^2 \cdot 5^2 = 100$) $\implies$ un 3-Sylow ha indice 4 in $G \implies G$ non semplice (già visto).
- Posso supporre $j = 1$.
- $i = 1$ o $i = 2 \implies G$ non semplice (già visto).
- $q \leq 3 \implies$ un p-Sylow ha indice 2 o 3 in $G \implies G$ non semplice (già visto).
- Resta il caso $n = p^i q$ con $i > 2$ e $q \geq 5 \implies p^i < 60/5 = 12 \implies p = 2$, $i = 3 \implies q < 60/2^3 < 8 \implies q = 5$ o $q = 7 \implies n = 2^3 \cdot 5 = 40$ o $n = 2^3 \cdot 7 = 56$.
- $n = 40 \implies s_5 = 1$ (perché $s_5 \equiv 1 \mod 5$ e $s_5 \mid 8$) $\implies G$ non semplice.

Gruppi di ordine 56

$\#G = 56 \implies s_7 \equiv 1 \mod 7$ e $s_7 \mid 8 \implies s_7 = 1$ ($\implies G$ non semplice) o $s_7 = 8 \implies$

$$T := \{a \in G \,:\, \mathrm{ord}(a) = 7\}$$

tale che $\#T = s_7(7-1) = 8 \cdot 6 = 48$.
H 2-Sylow di $G \implies H \subseteq G \setminus T$, $\#H = 8 = \#(G \setminus T) \implies$
$H = G \setminus T \implies s_2 = 1 \implies G$ non semplice.

Richiami su S_n e A_n

- $\#S_n = n!$, $S_n = \langle\{2\text{-cicli}\}\rangle$.
- $\varepsilon\colon S_n \to \{\pm 1\} \cong C_2$ omomorfismo (suriettivo se $n \geq 2$) tale che $\varepsilon(\sigma) = (-1)^{m-1}$ se σ è un m-ciclo.
- $A_n := \ker(\varepsilon) \lhd S_n$, $\#A_n = n!/2 \ \forall\, n \geq 2$, $A_n = \langle\{3\text{-cicli}\}\rangle$.
- $A_3 = \{1, (1,2,3), (1,3,2)\}$ e $S_3 \setminus A_3 = \{(1,2), (1,3), (2,3)\}$.
- Gli unici sottogruppi non banali di S_3 sono A_3 (normale) e $\langle(1,2)\rangle$, $\langle(1,3)\rangle$, $\langle(2,3)\rangle$ (non normali).
- $A_4 = V_4 \coprod \{3\text{-cicli}\}$ e $S_4 \setminus A_4 = \{2\text{-cicli}\} \coprod \{4\text{-cicli}\}$ con

$$C_2^2 \cong V_4 := \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \lhd S_4$$

  ($\implies V_4 \lhd A_4$), $\#\{3\text{-cicli}\} = 8$, $\#\{2\text{-cicli}\} = \#\{4\text{-cicli}\} = 6$.
- Gli unici sottogruppi normali non banali di S_4 sono V_4 e A_4: $H \lhd S_4 \implies \#H \mid 24$ e H è unione di classi di coniugio $\implies$ $\#H = 1 + 3a + 8b + 6c + 6d$ con $a, b, c, d \in \{0, 1\} \implies$ $a = 1$ e $c = d = 0$ se $1 < \#H < 24$.

I sottogruppi di S_4

$\exists\, H < S_4$ non banale tale che $H \cong G \iff G$ è isomorfo a uno dei seguenti gruppi: C_2, C_3, C_4, C_2^2, S_3, D_4, A_4.

$\Longleftarrow$ $H = \langle \sigma \rangle$ con σ m-ciclo $\implies H \cong C_m$ per $m = 2, 3, 4$.
$H = V_4 \implies H \cong C_2^2$.
$H = \{\sigma \in S_4 \,:\, \sigma(4) = 4\} \implies H \cong S_3$.
$H = \mathrm{im}(f_4) \implies H \cong D_4$, dove $f_n \colon D_n \to S_n$ indica l'omomorfismo (iniettivo per $n \geq 3$) che manda un elemento di $D_n \subset S(\mathbb{R}^2)$ nella sua restrizione ai vertici di Δ_n.
$H = A_4 \implies H \cong A_4$.

$\Longrightarrow$ $\#H \leq 4 \implies H \cong C_2$, C_3, C_4 o C_2^2.
$\#H = 6 \implies H \not\cong C_6$ (perché S_4 non ha elementi di ordine 6) $\implies H \cong S_3$.
$\#H = 8 \implies H$ 2-Sylow $\implies H \cong D_4$ perché tutti i 2-Sylow sono isomorfi e so già che ce n'è uno di questa forma.
$\#H = 12 \implies [S_4 : H] = 2 \implies H \triangleleft S_4 \implies H = A_4$ perché A_4 e V_4 sono gli unici sottogruppi normali non banali di S_4.

Il coniugio in A_n

Osservazione

$H, K < G \implies [H : H \cap K] \leq [G : K]$ perché la funzione

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

è (ben definita e) iniettiva. In particolare $H < S_n \implies [H : H \cap A_n] \leq [S_n : A_n] = 2$, e quindi $[H : H \cap A_n] = 2$ se $H \not\subseteq A_n$.
$\forall\, \sigma \in A_n$, dato che $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n$, si ha allora

$$\begin{cases} C_{A_n}(\sigma) = C_{S_n}(\sigma) & \text{se } C_{S_n}(\sigma) \subseteq A_n \\ [C_{S_n}(\sigma) : C_{A_n}(\sigma)] = 2 & \text{se } C_{S_n}(\sigma) \not\subseteq A_n, \end{cases}$$

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

$$\begin{cases} \#[\sigma]_{A_n} = \frac{\#A_n}{\#C_{A_n}(\sigma)} = \frac{\#S_n}{2\#C_{S_n}(\sigma)} = \frac{\#[\sigma]_{S_n}}{2} & \text{se } C_{S_n}(\sigma) \subseteq A_n \\ [\sigma]_{A_n} = [\sigma]_{S_n} & \text{se } C_{S_n}(\sigma) \not\subseteq A_n. \end{cases}$$

Il coniugio in A_4

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

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

$\implies \#C_{S_4}(\sigma) = 3 \implies C_{S_4}(\sigma) = \langle\sigma\rangle \subset A_4 \implies \#[\sigma]_{A_4} = \#[\sigma]_{S_4}/2 = 4$ (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 $6 \mid 12 = \#A_4$): $H \lhd A_4 \implies \#H \mid 12$ e H è unione di classi di coniugio $\implies \#H = 1 + 3a + 4b + 4c$ con $a, b, c \in \{0, 1\} \implies a = 1$ e $b = c = 0$ se $1 < \#H < 12$.

Proposizione

$n \geq 5$, $\{1\} \neq H \lhd A_n \implies H$ contiene un 3-ciclo.

Teorema

A_n è semplice $\forall\, n \geq 5$.

Dimostrazione.

$\{1\} \neq H \lhd A_n \implies$ per la Proposizione $\exists\, \sigma = (a, b, c) \in H$.
$n \geq 5 \implies \exists\, \tau = (d, e) \in C_{S_n}(\sigma)$ (con a, b, c, d, e distinti) $\implies$
$C_{S_n}(\sigma) \not\subseteq A_n \implies$

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

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

Corollario

A_5 è semplice e $\#A_5 = 60$.

Corollario

A_n è l'unico sottogruppo normale non banale di S_n $\forall\, n \geq 5$.

Dimostrazione.

- $H \lhd S_n \implies H' := H \cap A_n \lhd A_n \implies H' = \{1\}$ o $H' = A_n$.
- $H \subseteq A_n \implies H = H' \implies H = \{1\}$ o $H = A_n$.
- $H \not\subseteq A_n \implies [H : H'] = 2 \implies \#H = 2$ o $H = S_n$.
- Per assurdo $\#H = 2 \implies H = \{1, \tau\}$ (con $\tau \in S_n \setminus A_n$) $\implies \sigma\tau\sigma^{-1} = \tau\ \forall\, \sigma \in S_n \implies \tau \in Z(S_n)$, assurdo perché $Z(S_n) = \{1\}$ ($\forall\, n \geq 3$).

$\square$

Dimostrazione della Proposizione

$n \geq 5$, $\{1\} \neq H \lhd A_n \implies H$ contiene un 3-ciclo.

$M(\sigma) := \{i = 1, \dots, n : \sigma(i) \neq i\}$ e $l(\sigma) := \# M(\sigma)$ $\forall \sigma \in S_n$.

- $\sigma \neq 1 \implies l(\sigma) \geq 2$.
- $l(\sigma) = 2 \iff \sigma$ è un 2-ciclo e $l(\sigma) = 3 \iff \sigma$ è un 3-ciclo.
- Basta dimostrare che $m := \min\{l(\sigma) : 1 \neq \sigma \in H\} = 3$.
- Per assurdo sia $m > 3$ e sia $\sigma \in H \setminus \{1\}$ tale che $l(\sigma) = m$.
- σ può essere di una di queste due forme:
    1. $\sigma = (i_1, i_2, i_3, \dots) \dots$ e $\sigma \neq (i_1, i_2, i_3)$;
    2. $\sigma = (i_1, i_2)(i_3, i_4) \cdots$ prodotto di trasposizioni disgiunte.
- Nel caso 1 $l(\sigma) \geq 5 \implies \exists\, i_4, i_5 \in M(\sigma) \setminus \{i_1, i_2, i_3\}$ distinti.
- Nel caso 2 $\exists\, i_5 \notin \{i_1, i_2, i_3, i_4\}$.
- $\tau := (i_3, i_4, i_5) \implies \tilde{\sigma} := \tau\sigma\tau^{-1} \in H$ e $\tilde{\sigma} \neq \sigma$ (nel caso 1 $\tilde{\sigma}(i_2) = i_4 \neq i_3 = \sigma(i_2)$ e nel caso 2 $\tilde{\sigma}(i_4) = i_5 \neq i_3 = \sigma(i_4)$).
- $\sigma' := \tilde{\sigma}\sigma^{-1} \in H \setminus \{1\}$ tale che $M(\sigma') \subseteq M(\sigma) \cup \{i_5\}$, $\sigma'(i_2) = i_2$ e nel caso 2 $\sigma'(i_1) = i_1$.
- $l(\sigma') < l(\sigma) = m$, assurdo.

Esercizio

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

Dimostrazione.

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

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

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

Osservazione

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

Gruppi risolubili

Definizione

Un gruppo G è risolubile se esistono sottogruppi

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

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

Esempio

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 $\exists\, K_i \triangleleft K_{i-1}$ tale che $\#K_i = p^{n-i}$).

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

Proposizione

1. *$H < G$ e G risolubile $\implies$ H risolubile.*
2. *$H \lhd G$ e G risolubile $\implies$ G/H risolubile.*
3. *$H \lhd G$, H e G/H risolubili $\implies$ G risolubile.*

Dimostrazione.

1. $\{1\} = K_r \lhd \cdots \lhd K_0 = G \implies K'_i := K_i \cap H$ per $i = 0, \ldots, r$ tali che $\{1\} = K'_r < \cdots < K'_0 = H$. Inoltre $\forall\, i = 1, \ldots, r$

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

(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 $\implies$ K'_{i-1}/K'_i abeliano.

Dimostrazione di 2 e 3

2. $\pi\colon G \to \overline{G} := G/H$ proiezione, $\{1\} = K_r \lhd \cdots \lhd K_0 = G \implies \overline{K}_i := \pi(K_i)$ per $i = 0, \dots, r$ tali che $\{\bar{1}\} = \overline{K}_r < \cdots < \overline{K}_0 = \overline{G}$. Inoltre $\forall\, i = 1, \dots, r$ $\overline{K}_i \lhd \overline{K}_{i-1}$ (perché $\pi(g)\pi(a)\pi(g)^{-1} = \pi(gag^{-1}) \in \overline{K}_i$ $\forall\, g \in K_{i-1}$ e $\forall\, a \in K_i$, dato che $gag^{-1} \in K_i$) e
$$K_{i-1} \xrightarrow{\pi_i} \pi(K_{i-1}) = \overline{K}_{i-1} \xrightarrow{\bar{p}_i} \overline{K}_{i-1}/\overline{K}_i$$
(con π_i indotto da π e $\bar{p}_i$ la proiezione) è un omomorfismo suriettivo tale che $K_i \subseteq \ker(\bar{p}_i \circ \pi_i)$. 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 $\implies \overline{K}_{i-1}/\overline{K}_i$ abeliano.
3. $\{1\} = K'_r \lhd \cdots \lhd K'_0 = H$ e $\{\bar{1}\} = \overline{K}_s \lhd \cdots \lhd \overline{K}_0 = \overline{G}$ (dove $\overline{K}_i = K_i/H$ con $H < K_i < G$ per $i = 0, \dots, s$) $\implies \{1\} = K'_r \lhd \cdots \lhd K'_0 = K_s \lhd \cdots \lhd K_0 = G$. Inoltre $\forall\, i = 1, \dots, s$ $K_{i-1}/K_i \cong \overline{K}_{i-1}/\overline{K}_i$ per il terzo teorema di isomorfismo.

Conseguenze

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

Ricordiamo che il sottogruppo dei commutatori di un gruppo G è

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

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

Proposizione

G è risolubile $\iff \exists\, r \in \mathbb{N}$ tale che $G^{(r)} = \{1\}$.

Dimostrazione.

$\Longleftarrow$ Chiaro.

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

Definizione

Se $H < G$, $K \lhd G$, $H \cap K = \{1\}$ e $HK(= KH) = G$, si dice che G è prodotto semidiretto dei sottogruppi K e H, e si indica $G = K \rtimes H$ o $G = H \ltimes K$.

Osservazione

Se anche $H \lhd G$, si dice che G è prodotto (diretto) di K e H e si può scrivere $G = K \times H$ o $G = H \times K$.

Esempio

- $D_n = \langle R \rangle \rtimes \langle S \rangle$.
- $S_n = A_n \rtimes \langle \sigma \rangle$ con σ trasposizione.
- $S_4 = V_4 \rtimes S_3$ (con $S_3 = \{\sigma \in S_4 \, : \, \sigma(4) = 4\} < S_4$) e $A_4 = V_4 \rtimes A_3$.
- $\#G = pq$ con $p < q$ primi $\implies G = K \rtimes H$ con $H \cong C_p$ p-Sylow e $K \cong C_q$ q-Sylow.

Proposizione

$K \lhd G$, $\pi\colon G \to G/K$ proiezione $\implies$ sono equivalenti:

1. *$\exists\, H < G$ tale che $G = K \rtimes H$;*
2. *$\exists\, H < G$ tale che $\pi|_H\colon H \to G/K$ è un isomorfismo;*
3. *$\exists\, f\colon G/K \to G$ omomorfismo tale che $\pi \circ f = \mathrm{id}_{G/K}$.*

Osservazione

- Se in 1 (o in 2) $H \lhd G$ (e quindi $G = K \times H$), allora $\exists\, p\colon G \to K$ omomorfismo tale che $p|_K = \mathrm{id}_K$ (e $\ker(p) = H$).
- In generale le condizioni 1, 2, 3 possono non essere soddisfatte e, anche quando lo sono, H e f possono non essere unici. In particolare, se G è abeliano (additivo), le condizioni valgono $\iff$ K è addendo diretto di G (Proposizione 11.4 delle dispense sui moduli), e in questo caso H ne è un complementare.

Dimostrazione della Proposizione

$1 \implies 2$ $\pi|_H = \pi \circ i$ omomorfismo (con $i \colon H \to G$ inclusione).

$$\ker(\pi|_H) = H \cap \ker(\pi) = H \cap K = \{1\} \implies \pi|_H \text{ iniettivo.}$$
$$\mathrm{im}(\pi|_H) = \pi(H) = (HK)/K = G/K \implies \pi|_H \text{ suriettivo.}$$

$2 \implies 3$ $f := i \circ (\pi|_H)^{-1} \colon G/K \to G$ omomorfismo tale che

$$\pi \circ f = \pi \circ i \circ (\pi|_H)^{-1} = \pi|_H \circ (\pi|_H)^{-1} = \mathrm{id}_{G/K}.$$

$3 \implies 1$ $H := \mathrm{im}(f) < G$.

$g \in H \cap K \implies \exists x \in G/K$ tale che $g = f(x)$ (perché $g \in H$) $\implies x = \pi(f(x)) = \pi(g) = \bar{1}$ (perché $g \in K$) $\implies g = f(x) = f(\bar{1}) = 1 \implies H \cap K = \{1\}$.

$g \in G \implies b := f(\pi(g)) \in H$; $a := gb^{-1}$ tale che $\pi(a) = \pi(g)\pi(b)^{-1} = \pi(g)\pi(f(\pi(g)))^{-1} = \pi(g)\pi(g)^{-1} = \bar{1}$ $\implies a \in K \implies g = ab \in KH \implies G = KH$.

Operazione in un prodotto semidiretto

$g, g' \in G = K \rtimes H \implies \exists!\, a, a' \in K$ e $b, b' \in H$ tali che
$g = ab$ e $g' = a'b' \implies$

$$gg' = aba'b' = aba'b^{-1}bb' \quad \text{con} \quad aba'b^{-1} \in K \text{ e } bb' \in H.$$

Se $\Gamma \colon G \to \mathrm{Aut}(G)$ è l'omomorfismo che definisce l'azione per coniugio, $\forall\, c \in G$ posso considerare $\Gamma(c)|_K \in \mathrm{Aut}(K)$ (perché $K \lhd G$) e ottengo un omomorfismo

$$\theta \colon H \to \mathrm{Aut}(K) \qquad b \mapsto \Gamma(b)|_K$$

tale che $ba'b^{-1} = \Gamma(b)(a') = \theta(b)(a')$, e quindi

$$gg' = a\theta(b)(a')bb' \quad \text{con} \quad a\theta(b)(a') \in K \text{ e } bb' \in H.$$

Definizione-Proposizione

H e K gruppi, $\theta\colon H \to \mathrm{Aut}(K)$ omomorfismo. Il prodotto semidiretto di K e H rispetto a θ, denotato con $K \rtimes_\theta H$ o $H \ltimes_\theta K$, è il gruppo costituito dall'insieme $K \times H$ con l'operazione

$$(a,b)(a',b') := (a\theta(b)(a'), bb').$$

In particolare $K \rtimes_\theta H = K \times H$ se θ è l'omomorfismo banale.

Osservazione

È facile vedere che $G = K \rtimes_\theta H \implies G = K' \rtimes H'$ con $K \cong K' := K \times \{1\} \lhd G$ e $H \cong H' := \{1\} \times H < G$ (esercizio). Inoltre $H' \lhd G \iff \theta$ è banale: se θ è banale, $G = K \times H$, quindi $H' \lhd G$. Viceversa, se $H' \lhd G$, allora $\forall\, a \in K$ e $\forall\, b \in H$ $(a,1)(1,b)(a,1)^{-1} = (a,b)(a^{-1},1) = (a\theta(b)(a^{-1}), b) \in H' \implies 1 = a\theta(b)(a^{-1}) = a\theta(b)(a)^{-1} \implies \theta(b)(a) = a \implies \theta$ è banale. In particolare $K \rtimes_\theta H$ abeliano $\iff H, K$ abeliani e θ banale.

Dimostrazione della Definizione-Proposizione

- L'operazione è associativa: $\forall\, a, a', a'' \in K$ e $\forall\, b, b', b'' \in H$

$$\begin{aligned}((a,b)(a',b'))(a'',b'') &= (a\theta(b)(a'), bb')(a'',b'') \\ &= (a\theta(b)(a')\theta(bb')(a''), bb'b'')\end{aligned}$$

$$\begin{aligned}(a,b)((a',b')(a'',b'')) &= (a,b)(a'\theta(b')(a''), b'b'') \\ &= (a\theta(b)(a'\theta(b')(a'')), bb'b'')\end{aligned}$$

e le due espressioni sono uguali perché (tenendo conto che $\theta(b)\colon K \to K$ è un omomorfismo e che $\theta(bb') = \theta(b) \circ \theta(b')$)

$$\theta(b)(a'\theta(b')(a'')) = \theta(b)(a')\theta(b)(\theta(b')(a'')) = \theta(b)(a')\theta(bb')(a'').$$

- L'elemento neutro è $(1,1)$ (esercizio).
- $(a,b)^{-1} = (\theta(b^{-1})(a^{-1}), b^{-1})\ \forall\, a \in K$ e $\forall\, b \in H$ (esercizio):

Alcuni gruppi di automorfismi

$\mathrm{Aut}(C_n) \cong \mathbb{Z}/n\mathbb{Z}^*$ $\forall\, n > 0$. Infatti la funzione

$$f\colon \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}^* \qquad \alpha \mapsto \alpha(\bar{1})$$

è un isomorfismo:

- f è ben definita perché α isomorfismo $\implies$ $\mathrm{ord}(\alpha(\bar{1})) = \mathrm{ord}(\bar{1}) = n \implies \alpha(\bar{1}) \in \mathbb{Z}/n\mathbb{Z}^*$;
- f è biunivoca perché $\forall\, a \in \mathbb{Z}\ \exists!\, \alpha\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ omomorfismo tale che $\alpha(\bar{1}) = \bar{a}$ e α iniettivo $\iff$ α suriettivo $\iff$ $\mathrm{ord}(\alpha(\bar{1})) = n \iff \alpha(\bar{1}) \in \mathbb{Z}/n\mathbb{Z}^*$;
- f è un omomorfismo perché $\forall\, \alpha, \beta \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, se $f(\alpha) = \alpha(\bar{1}) = \bar{a}$ e $f(\beta) = \beta(\bar{1}) = \bar{b}$, allora

$$f(\alpha\circ\beta) = \alpha(\beta(\bar{1})) = \alpha(\bar{b}) = b\alpha(\bar{1}) = b\bar{a} = \overline{ba} = \bar{a}\bar{b} = f(\alpha)f(\beta).$$

$\mathrm{Aut}(C_2^2) \cong S_3$: è infatti facile vedere che ogni permutazione di C_2^2 che lascia fisso l'elemento neutro è un automorfismo.

Isomorfismo tra prodotti semidiretti

Proposizione

$\theta, \theta' \colon H \to \mathrm{Aut}(K)$ *omomorfismi tali che* $\theta = \theta' \circ \alpha$ *per qualche* $\alpha \in \mathrm{Aut}(H) \implies K \rtimes_\theta H \cong K \rtimes_{\theta'} H$.

Dimostrazione.

Poiché α è biunivoca, anche la funzione

$$f \colon K \rtimes_\theta H \to K \rtimes_{\theta'} H \qquad (a, b) \mapsto (a, \alpha(b))$$

lo è. Inoltre f è un omomorfismo perché

$$f((a, b)(a', b')) = f((a\theta(b)(a'), bb')) = (a\theta(b)(a'), \alpha(bb')) = (a\theta'(\alpha(b))(a'), \alpha(b)\alpha(b')) = (a, \alpha(b))(a', \alpha(b')) = f((a, b))f((a', b'))$$

$\forall\, a, a' \in K$ e $\forall\, b, b' \in H$. $\square$

Corollario

H e K gruppi con $H \cong C_p$ per qualche primo p.

1. $\exists\, \theta \colon H \to \mathrm{Aut}(K)$ omomorfismo non banale $\iff$ $p \mid \#\mathrm{Aut}(K)$.
2. Se $\mathrm{Aut}(K)$ ha un unico sottogruppo di ordine p, allora $K \rtimes_\theta H \cong K \rtimes_{\theta'} H$ per ogni coppia $\theta, \theta' \colon H \to \mathrm{Aut}(K)$ di omomorfismi non banali.

Dimostrazione.

1. Poiché H è semplice, $\exists\, \theta$ non banale $\iff$ $\exists\, \theta$ iniettivo $\iff$ $\exists\, H' < \mathrm{Aut}(K)$ tale che $H' \cong H$ $\iff$ $p \mid \#\mathrm{Aut}(K)$.
2. Se H' è l'unico sottogruppo di ordine p di $\mathrm{Aut}(K)$ e θ e θ' sono non banali, allora sono iniettivi e $\mathrm{im}(\theta) = \mathrm{im}(\theta') = H'$. Dunque esistono isomorfismi $\tilde{\theta}, \tilde{\theta}' \colon H \to H'$ tali che $\theta = i \circ \tilde{\theta}$ e $\theta' = i \circ \tilde{\theta}'$ (con $i \colon H' \to \mathrm{Aut}(K)$ l'inclusione). Allora $\tilde{\theta} = \tilde{\theta}' \circ \alpha$ e quindi $\theta = \theta' \circ \alpha$ con $\alpha := \tilde{\theta}'^{-1} \circ \tilde{\theta} \in \mathrm{Aut}(H)$.

$\#G = pq$ con $p < q$ primi.

- $q \not\equiv 1 \mod p \implies G \cong C_{pq}$.
- $q \equiv 1 \mod p \implies G \cong C_{pq}$ o $G \cong C_q \rtimes_\theta C_p$ con $\theta\colon C_p \to \mathrm{Aut}(C_q)$ omomorfismo non banale; inoltre $C_q \rtimes_\theta C_p$ non è abeliano e, a meno di isomorfismo, non dipende da θ.

Dimostrazione.

So già che $G \cong C_q \rtimes_\theta C_p$ per qualche omomorfismo

$$\theta\colon C_p \to \mathrm{Aut}(C_q) \cong \mathbb{Z}/q\mathbb{Z}^* \cong C_{q-1}.$$

Se θ è banale $G \cong C_q \times C_p \cong C_{pq}$, e θ è banale se $q \not\equiv 1 \mod p$, perché in quel caso $p \nmid \#\mathrm{Aut}(C_q) = q - 1$.
Se invece $q \equiv 1 \mod p$, esiste θ non banale, $C_q \rtimes_\theta C_p$ non è abeliano e, a meno di isomorfismo, non dipende da θ perché $\mathrm{Aut}(C_q) \cong C_{q-1}$ ha un unico sottogruppo di ordine p. $\square$

Gruppi di ordine 8

$\#G = 8 = 2^3$, G non abeliano.

- $\mathrm{ord}(g) = 2$ o $4 \ \forall\, g \in G \setminus \{1\}$ (altrimenti G ciclico).
- $\exists\, a \in G$ tale che $\mathrm{ord}(a) = 4$ (altrimenti $g^2 = 1 \ \forall\, g \in G \implies gghh = 1 = ghgh \implies gh = hg \ \forall\, g, h \in G$, cioè G abeliano).
- $C_4 \cong K := \langle a \rangle \lhd G$ (perché $[G : K] = 2$).
- Se $\exists\, b \in G \setminus K$ tale che $\mathrm{ord}(b) = 2$, allora $C_2 \cong H := \langle b \rangle < G$ tale che $G = K \rtimes H \cong C_4 \rtimes_\theta C_2$ con $\theta \colon C_2 \to \mathrm{Aut}(C_4) \cong C_2$ l'unico omomorfismo non banale. In questo caso $G \cong D_4$.
- Se invece $\mathrm{ord}(g) = 4 \ \forall\, g \in G \setminus K$, scelgo $b \in G \setminus K \implies bab^{-1} \in K$ e $\mathrm{ord}(bab^{-1}) = \mathrm{ord}(a) \implies bab^{-1} = a$ o a^{-1}.
- $G = \langle a, b \rangle \implies ab \neq ba \implies bab^{-1} = a^{-1}$.
- $\#(K \cap \langle b \rangle) = 2 \implies K \cap \langle b \rangle = \{1, z := a^2 = b^2\}$ con $z \in Z(G)$ (dato che $a, b \in C(z)$) e $a^{-1} = za$, $b^{-1} = zb$.
- $c := ab$ tale che $c^2 = z$, $c^{-1} = zc$, $ba = zc$, $bc = a$, $cb = za$, $ca = b$, $ac = zb$. In questo caso $G \cong Q := \{\pm 1, \pm i, \pm j, \pm k\}$.

$\#G = 12 = 2^2 \cdot 3$, G non abeliano.

- $G = K \rtimes H$ con H non normale, K 2-Sylow e H 3-Sylow o K 3-Sylow e H 2-Sylow.
- Non può essere $K \cong C_4$ e $H \cong C_3$ perché l'unico omomorfismo $C_3 \to \mathrm{Aut}(C_4) \cong C_2$ è quello banale.
- $K \cong C_2^2$ e $H \cong C_3 \implies G \cong C_2^2 \rtimes_\theta C_3$ con $\theta\colon C_3 \to \mathrm{Aut}(C_2^2) \cong S_3$ omomorfismo non banale. A meno di isomorfismo G non dipende da θ perché S_3 ha un unico sottogruppo di ordine 3. In questo caso $G \cong A_4$.
- $K \cong C_3$ e $H \cong C_4 \implies G \cong C_3 \rtimes_\theta C_4$ con $\theta\colon C_4 \to \mathrm{Aut}(C_3) \cong C_2$ l'unico omomorfismo non banale.
- $K \cong C_3$ e $H \cong C_2^2 \implies G \cong C_3 \rtimes_\theta C_2^2$ con $\theta\colon C_2^2 \to \mathrm{Aut}(C_3) \cong C_2$ omomorfismo non banale. A meno di isomorfismo G non dipende da θ perché se θ' è un altro omomorfismo non banale, $\exists\, \alpha \in \mathrm{Aut}(C_2^2) \cong S_3$ tale che $\theta = \theta' \circ \alpha$. In questo caso $G \cong D_6$.

Gruppi di ordine < 16

n	classi di isomorfismo di gruppi di ordine n				
2	C_2				
3	C_3				
4	C_4	C_2^2			
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
9	C_9	C_3^2			
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}				

Gruppi di ordine 30

$\#G = 30 = 2 \cdot 3 \cdot 5$.

1. $\exists\, K < G$ tale che $\#K = 15$.
2. $G \cong C_{15} \rtimes_\theta C_2$ per qualche omomorfismo $\theta \colon C_2 \to \mathrm{Aut}(C_{15})$.
3. G è isomorfo a uno e uno solo dei seguenti gruppi: C_{30}, D_{15}, $D_3 \times C_5$ e $D_5 \times C_3$.

1. $H_5 < G$ 5-Sylow e $H_3 < G$ 3-Sylow tali che $H_5 \lhd G$ o $H_3 \lhd G$ $\implies K := H_5 H_3 < G$ e $\#K = (\#H_5)(\#H_3) = 5 \cdot 3 = 15$.
2. $K \lhd G$ perché $[G : K] = 2 \implies G = K \rtimes H$ con $H < G$ $2-$ *Sylow*, e basta osservare che $K \cong C_{15}$ e $H \cong C_2$.
3. $\mathrm{Aut}(C_{15}) \cong \mathbb{Z}/15\mathbb{Z}^* \cong \mathbb{Z}/5\mathbb{Z}^* \times \mathbb{Z}/3\mathbb{Z}^* \cong C_4 \times C_2 \implies$

$$\#\mathrm{Hom}(C_2, \mathrm{Aut}(C_{15})) = \#\mathrm{Hom}(C_2, C_4 \times C_2)$$
$$= \#\{g \in C_4 \times C_2 \, : \, \mathrm{ord}(g) \mid 2\} = 4$$

$\implies$ ci sono al più 4 classi di isomorfismo e basta verificare che i 4 elencati sono a due a due non isomorfi (esercizio).

Esercizio sui gruppi di ordine p^3

1. $\#G = p^3$ (p primo), G non abeliano $\implies$ $Z(G) = [G, G] \cong C_p$ e $G/Z(G) \cong C_p^2$.
2. Per ogni primo p esiste un gruppo non abeliano di ordine p^3

1. $G \neq \{1\}$ p-gruppo $\implies$ $Z(G) \neq \{1\}$ $\implies$ $[G : Z(G)] \neq p^3$.
   G non abeliano $\implies$ $G/Z(G)$ non ciclico $\implies$ $[G : Z(G)] \neq 1, p$.
   Dunque $[G : Z(G)] = p^2$ $\implies$ $G/Z(G) \cong C_p^2$ abeliano $\implies$ $[G, G] < Z(G) \cong C_p$ semplice.
   G non abeliano $\implies$ $[G, G] \neq \{1\}$ $\implies$ $[G, G] = Z(G)$.
2. $\exists\, \theta \colon C_p \to \mathrm{Aut}(C_{p^2})$ omomorfismo non banale (perché $p \mid \#\mathrm{Aut}(C_{p^2}) = \#\mathbb{Z}/p^2\mathbb{Z}^* = p(p-1))$ $\implies$ $G := C_{p^2} \rtimes_\theta C_p$ non abeliano tale che $\#G = (\#C_{p^2})(\#C_p) = p^2 p = p^3$.