

# Appunti di Algebra 2

Github Repository: [Oxke/appunti/Algebra2](#)

Secondo semestre, 2024 - 2025, prof. Paola Frediani

I testi preferiti sono

- *Algebra*, di Michael Artin
- *Algebra*, di Herstein

## 1 Azioni di gruppi su insiemi

Chiameremo  $G$  un gruppo e  $S$  un insieme

### Definizione 1.1: Azione di gruppo

Un'azione (sinistra) di  $G$  su  $S$  e un'applicazione

$$F : G \times S \rightarrow S$$

tale che

- i)  $F(e, s) = s$  per ogni  $s \in S$
- ii)  $\forall g, h \in G$  e  $\forall s \in S$  vale  $F(g, F(h, s)) = F(gh, s)$

Si usa anche la notazione  $F(g, s) =: g(s)$  che permette la scrittura più concisa

$$e(s) = s \quad \text{e} \quad g(h(s)) = (gh)(s) \quad \forall s \in S, \quad \forall g, h \in G$$

**Proposizione 1.1.** Per ogni  $g \in G$ , l'applicazione  $F_g : S \rightarrow S$  definita da  $F_g(s) = F(g, s) = g(s)$  è una biiezione e in particolare

$$F_g^{-1} = F_{g^{-1}} \tag{1.1}$$

*Dimostrazione.*

$$F_g \circ F_{g^{-1}}(s) = g(g^{-1}(s)) \stackrel{(ii)}{=} e(s) \stackrel{(i)}{=} s$$

e analogamente per l'altra composizione □

**Proposizione 1.2.** L'applicazione  $\psi : G \rightarrow S(S) = \{f : S \rightarrow S \text{ biunivoche}\}$  dove  $S(S)$  il gruppo delle permutazioni di  $S$  è un omomorfismo di gruppi.

*Dimostrazione.*

$$\psi(gh) = F_{gh} \stackrel{(ii)}{=} F_g \circ F_h = \psi(g) \circ \psi(h)$$

□

**Definizione 1.2: Azione fedele**

Un'azione  $F : G \times S \rightarrow S$  si dice **fedele** se  $\psi$  è iniettivo

*Osservazione.* Ovvero se e solo se  $\text{Ker}\psi = \{e\} \iff (\psi(g) = \text{Id}_S \iff g = e)$

**Esempio 1.1.** Se  $S = G$  il gruppo stesso e sia

$$m : G \times G \rightarrow G \quad \text{con} \quad m(g, h) = gh$$

la moltiplicazione a sinistra. Allora  $m$  è un'azione sinistra, infatti

- i)  $m(e, h) = eh = h$  per ogni  $h \in G$
- ii)  $m(gg', h) = (gg')h = g(g'h) = m(g, g'h)$  per ogni  $g, g', h \in G$

Inoltre  $m$  è un'azione fedele, infatti

$$\psi(g)(h) = h \quad \forall h \in G \iff gh = h \implies g = e$$

*Osservazione.* Se  $G$  è un gruppo finito, con  $\#G = n$  allora  $S(G) \cong S_n$  e poiché  $\psi$  è iniettivo,  $G \cong \psi(G) < S(G) \cong S_n$  il teorema di Cayley.

**Esempio 1.2.** Sempre con  $G = S$  possiamo considerare l'azione di coniugio

$$\varphi : G \times G \rightarrow G \quad \text{con} \quad \varphi(g, h) = ghg^{-1}$$

- i)  $\varphi(e, h) = ehe^{-1} = h$  per ogni  $h \in G$
- ii)  $\varphi(gg', h) = (gg')h(gg')^{-1} = gg'hg'^{-1}g^{-1} = g(\varphi(g', h))g^{-1} = \varphi(g, \varphi(g', h))$

$\psi : G \rightarrow S(G)$  e  $\text{Im}\psi = \text{Inn}(G) < \text{Aut}(G)$ . Non è necessariamente un'azione fedele, infatti

$$\text{Ker}(\psi) = \{g \in G : \forall h \in G \quad ghg^{-1} = h\} = Z(G)$$

da cui per il primo teorema di isomorfismo

$$G/Z(G) = \text{Inn}(G)$$

**Esempio 1.3.** Con  $G = S_n$  e  $S = \{1, \dots, n\}$  allora la funzione

$$(\sigma, i) \mapsto \sigma(i)$$

è ovviamente un'azione

**Esempio 1.4.** Preso  $G \cong \mathbb{Z}/2\mathbb{Z} \cong \{1, \sigma\}$  con  $\sigma^2 = 1$  e  $S = \mathbb{C}$  allora la funzione

$$F : G \times \mathbb{C} \rightarrow \mathbb{C} \quad \text{con} \quad F(1, z) = z \quad \text{e} \quad F(\sigma, z) = \bar{z} \quad \forall z \in \mathbb{C}$$

è un'azione.

**Definizione 1.3: Orbita e Stabilizzatore**

Sia  $F : G \times S \rightarrow S$  un'azione di un gruppo  $G$  su  $S$ . Allora per ogni  $s \in S$  si definisce **orbita** di  $s$  l'insieme

$$O_s = \{g(s) : g \in G\}$$

e si definisce **stabilizzatore** di  $s$  l'insieme

$$\text{stab}_s = \{g \in G : g(s) = s\}$$

**Esempio 1.5.** Nell'esempio dell'azione di coniugio lo stabilizzatore di  $h$  è

$$\text{stab}_h = \{g \in G : ghg^{-1} = h\} = \{g \in G : gh = hg\} = C_G(h)$$

**Proposizione 1.3.** Le orbite  $O_s$  per un'azione di  $G$  sono classi di equivalenza per la relazione di equivalenza su  $S$  seguente:

$$S \sim S' \iff \exists g \in G : s' = g(s) = F(g, s)$$

*Dimostrazione.*  $\sim$  è in effetti una relazione di equivalenza, infatti:

- *riflessiva:*  $s = e(s)$
- *simmetrica:* se  $s' = g(s)$  allora  $s = g^{-1}(s')$  per la proposizione 1.1
- *transitiva:* se  $s' = g(s)$  e  $s'' = h(s')$  allora  $s'' = h(s') = h(g(s)) \stackrel{(ii)}{=} (hg)(s)$

Ne segue chiaramente che  $O_s = [s]_{\sim}$  e allora  $S = \coprod_{s \in S} O_s$  □

**Proposizione 1.4.**  $\text{stab}_s < G$

*Dimostrazione.* Supponiamo  $g, h \in \text{stab}_s$ . Allora  $g(s) = h(s) = s$ , ne consegue che

$$F_{gh^{-1}}(s) = F_g(F_{h^{-1}}(s)) \stackrel{(1.1)}{=} F_g(F_h^{-1}(s)) = F_g(s) = s$$

□

#### Definizione 1.4: Azione transitiva

Un'azione  $F : G \times S \rightarrow S$  si dice **transitiva** se per ogni  $s, s' \in S$  esiste  $g \in G$  tale che  $s' = g(s)$

**Proposizione 1.5.** Sia  $F : G \times S \rightarrow S$  un'azione di gruppo. Allora fissato un  $s \in S$ , consideriamo  $O_s \subseteq S$  e  $H := \text{stab}_s < G$ . Allora esiste un'applicazione naturale biettiva

$$\begin{aligned} \Phi : G/H &\longrightarrow O_s \\ gH &\longmapsto \Phi(gH) = g(s) = F(g, s) \end{aligned}$$

Inoltre per ogni  $C \in G/H$ ,  $g(\Phi(C)) = \Phi(g(C))$  dove la prima azione è quella di  $G$  su  $O_s$  e la seconda è quella di  $G$  su  $G/H$

*Dimostrazione.*

- *Ben definita:* se  $aH = bH$  allora  $b^{-1}a \in H$  e quindi esiste un  $h \in H$  tale che  $b^{-1}a = h$  e quindi  $a = bh$ . Allora  $F(a, s) = F(bh, s) = F(b, F(h, s)) = F(b, s)$
- *Iniettiva:* supponiamo che esistano  $a, b \in G$  tali che  $\Phi(aH) = \Phi(bH)$ , allora  $F(a, s) = F(b, s)$  ma allora

$$F(b^{-1}a, s) = F(b^{-1}, F(a, s)) = F(b^{-1}, F(b, s)) = F(b^{-1}b, s) = F(e, s) = s$$

e quindi  $b^{-1}a \in H \iff aH = bH$

- *Suriettiva:* per ogni  $s' \in O_s$  esiste  $g \in G$  tale che  $s' = g(s)$  e quindi  $s' = g(s) = \Phi(gH)$

□

**Corollario 1.5.1.** Se  $G$  è un gruppo finito e ho un'azione  $F : G \times S \rightarrow S$ , allora per ogni  $s \in S$  vale  $\#O_s = [G : \text{stab}_s]$  o equivalentemente

$$\#G = \#O_s \cdot \#\text{stab}_s$$

e inoltre

$$\#G = \sum_{[s] \in S} \#O_s$$

**Corollario 1.5.2.** Sia  $F : G \times G \rightarrow G$  l'azione di coniugio  $(g, h) \mapsto ghg^{-1}$ . Ricordiamo che  $\text{stab}_a = C(a)$  e la formula delle classi si traduce in

$$\#G = \#C(a) \cdot \#O_a = \sum_{[g] \in G} \#O_g = \sum_{[g] \in G} \frac{\#G}{\#C(g)}$$

inoltre se  $g \in Z(G)$  allora  $C(g) = G$  e dunque

$$\#G = \#Z + \sum_{[g] \in G \setminus Z} \#O_g = \#Z + \sum_{[g] \in G \setminus Z} \frac{\#G}{\#C(g)} \quad (1.2)$$

#### Teorema 1.6

Sia  $G$  un gruppo tale che  $\#G = p^n$  con  $p$  primo. Allora  $Z(G) \neq \{e\}$

*Dimostrazione.* Se  $a \notin Z$  allora  $C(a) = p^{n_a}$  con  $n_a < n$  e quindi da

$$p^n = \#G = \#Z + \sum_{[g] \in G \setminus Z} \# \frac{p^n}{p^{n_a}}$$

ne deduciamo che  $p \mid \#Z$  □

**Corollario 1.6.1.** Sia  $G$  un gruppo di cardinalità  $p^2$ , con  $p$  primo. Allora  $G$  è abeliano.

*Dimostrazione.* Per il teorema sappiamo che  $Z \neq \{e\}$  e quindi  $\#Z = p$  oppure  $\#Z = p^2$ . Nel secondo caso  $G = Z$  e quindi è abeliano. Nel primo caso invece esiste un  $a \in G \setminus Z$  e dunque  $C(a) \neq G$ . Ma

$$\{e\} < Z < C(a) < G$$

e quindi  $C(a) = Z$  per cardinalità che è assurdo perché  $a \in C(a)$  e  $a \notin Z$ . □

**Esempio 1.6.** Riprendendo l'esempio della moltiplicazione a sinistra  $m : G \times G \rightarrow G$ . Allora  $m$  è un'azione transitiva. Infatti per ogni  $g', g'' \in G$  se prendo  $h = (g')^{-1}g''$  allora  $m(g', h) = g'(g'^{-1}g'') = g''$

**Esempio 1.7.** Se prendo  $GL(V)$  il gruppo lineare delle trasformazioni invertibili su uno spazio vettoriale  $V$ , allora l'azione  $(T, v) \mapsto Tv$  è transitiva su  $V \setminus \{0\}$

#### Teorema 1.7: Cauchy per gruppi abeliani

Sia  $G$  un gruppo abeliano finito e  $p$  un primo tale che  $p \mid \#G$ . Allora

$$\exists e \neq a \in G \text{ tale che } a^p = e$$

*Dimostrazione.* Procediamo per induzione su  $n = \#G$ . Se  $2 = \#G$  allora  $G = \{e, a\}$  e dunque  $a^2 = e$ . Supponiamo ora  $\#G \geq 3$ .

Se  $G$  non ha sottogruppi  $e \neq H \neq G$  allora  $G$  è ciclico di ordine primo. Infatti se  $G$  non è ciclico allora esistono due elementi  $e \neq g_1, g_2$  e  $g_2 \notin \langle g_1 \rangle$ . Ma allora  $\{e\} \neq \langle g_1 \rangle \neq G$  è un sottogruppo. Dunque  $G$  è ciclico, inoltre è di ordine primo perché se così non fosse (ad esempio  $n = ab$ ) allora  $\{e\} \neq \langle g^a \rangle \neq G$  è un sottogruppo, con  $g$  tale che  $\langle g \rangle = G$ .

Allora se  $G$  non ha sottogruppi propri esistono  $p - 1$  elementi in  $G$  di ordine  $p$ .

Supponiamo ora che  $G$  abbia qualche sottogruppo non banale. Sia  $N < G$  con  $\{e\} \neq N \neq G$ . Allora se  $p \mid \#N$  per ipotesi induttiva si conclude. Se invece  $p \nmid \#N$  allora  $G/N$  è un gruppo abeliano con  $\#G/N < \#G$  e quindi per ipotesi induttiva (infatti  $G/N$  ha ordine multiplo di  $p$  poiché  $N$  non lo è) esiste  $bN \in G/N$ ,  $b \notin N$  e tale che  $b^p \in N$ . Allora  $b^{p\#N} = e$  e ci resta solo da dimostrare che  $c := b^{\#N} \neq e$ .

Supponiamo che  $c = b^{\#N} = e$ . Sappiamo che  $MCD(p, \#N) = 1$  e dunque per il teorema di Bézout esistono  $\alpha, \beta \in \mathbb{Z}$  tali che  $\alpha p + \beta \#N = 1$ . Allora

$$bN = (bN)^{\alpha p + \beta \#N} = (bN)^{\alpha p} \cdot (bN)^{\beta \#N}$$

e poiché  $b^p \in N$  e  $b^{\#N} = e$  otteniamo che  $bN = N$  che è assurdo perché  $b \notin N$ .  $\square$

#### Teorema 1.8: Cauchy

Sia  $G$  è un gruppo finito e  $p$  è un primo tale che  $p \mid \#G$ . Allora

$$\exists a \in G \text{ tale che } \# \langle a \rangle = p$$

*Dimostrazione.* Vogliamo procedere per induzione su  $\#G$ . Se  $\#G = 2$  è già dimostrato. Se esiste  $H < G$  tale che  $p \mid \#H$  concludo per ipotesi induttiva.

Supponiamo dunque che  $p$  non divide l'ordine di nessun sottogruppo proprio di  $G$ . Nella formula delle classi (1.2), tutti i termini della serie sono divisibili per  $p$ , infatti se  $a \notin Z$ ,  $C(a) \neq G$  è un sottogruppo proprio e quindi  $p \nmid \#C(a)$ . Allora  $p \mid \#Z$  ma quindi  $Z = G$  e quindi  $G$  è abeliano. Concludiamo con il teorema di Cauchy per gruppi abeliani.  $\square$

#### Teorema 1.9: Sylow (prima parte)

Sia  $G$  un gruppo finito e  $p$  un primo tale che esiste  $\mathbb{Z} \ni m \geq 1$  tale che  $p^m \mid \#G$  ma  $p^{m+1} \nmid \#G$ . Allora

$$\exists H < G \text{ tale che } \#H = p^m$$

*Dimostrazione.* Procediamo per induzione su  $\#G$  e su  $m$ . Se  $\#G = 2$  allora  $H = G$ . Supponiamo ora  $\#G > 2$  e il risultato vero per ogni gruppo di cardinalità minore di  $G$ . Se  $m = 1$  allora ci si riduce al teorema di Cauchy. Supponiamo ora che  $m \geq 2$  e  $\#G \geq 3$ .

Se esiste  $H < G$  proprio con  $p^m \mid \#H$  allora concludo per ipotesi induttiva.

Supponiamo dunque che  $p^m \nmid \#K$  per ogni  $K < G$  proprio.

Come nel teorema di Cauchy usiamo (1.2), otteniamo che  $p \mid \#Z$  e quindi per il teorema di Cauchy abbiamo che esiste  $e \neq b \in Z$  tale che  $b^p = e$ . Allora  $\langle b \rangle \trianglelefteq G$ .

Ma allora poiché  $\#(G/\langle b \rangle) = \#G/p$  abbiamo che  $p^{m-1} \mid \#(G/\langle b \rangle)$  e dunque per ipotesi induttiva esiste  $\bar{S} < G/\langle b \rangle$  tale che  $\#\bar{S} = p^{m-1}$ . Allora  $S = \pi^{-1}(\bar{S})$  è un sottogruppo di  $G$  e  $\bar{S} = S/B$ . Ne consegue infine che  $\#S = p^m$ .  $\square$

*Osservazione.* Il sottogruppo  $H$  viene detto  $p$ -sottogruppo di Sylow di  $G$ .

## 2 Gruppi di permutazioni

### Definizione 2.1: Definizioni riguardo alle permutazioni

Una permutazione  $\sigma \in S_n$  si dice **pari** se si può scrivere come prodotto di un numero pari di trasposizioni. Questo è ben definito perché esiste un unico omomorfismo  $\varepsilon : S_n \rightarrow \mathbb{Z}/2$   $\varepsilon(\sigma) = 1$  se  $\sigma$  è una trasposizione. Tale omomorfismo è detto **segno** della permutazione.

Il **gruppo alterno**  $A_n$  è il nucleo di  $\varepsilon$ .

Poiché  $A_n$  ha indice 2 in  $S_n$ ,  $A_n \trianglelefteq S_n$ .

*Osservazione* (Ogni  $\sigma \in A_n$  si può esprimere come prodotto di 3-cicli). Basta mostrare che ogni prodotto di 2 trasposizioni è scrivibile come prodotto di 3-cicli. Se  $\sigma = (ab)(bc) = (abc)$  è facile. Se invece  $\sigma = (ab)(cd)$  disgiunti allora  $\sigma = (cba)(acd)$ . Notando che i 3-cicli sono pari si conclude anche che il sottogruppo generato dai 3-cicli è esattamente  $A_n$ .

**Esempio 2.1** (Per  $n \geq 5$  tutti i 3-cicli sono tra loro coniugati in  $A_n$ ). Prendiamo  $\sigma = (ijk)$  e  $\sigma' = (i'j'k')$  due 3-cicli. Allora esiste  $\gamma \in S_n$  tale che  $\gamma\sigma\gamma^{-1} = \sigma'$ . Supponiamo  $\gamma \notin A_n$ . Siccome  $n \geq 5$  allora esistono  $r, s \in \{1, \dots, n\} \setminus \{i, j, k\}$ . Ma allora  $\theta = \gamma \cdot (rs) \in A_n$  e  $\theta\sigma\theta^{-1} = \sigma'$ .

### Esercizio 2.1 2 elementi coniugati in $S_5$ ma non in $A_5$

Mostrare che  $(12345)$  e  $(21345)$  non sono coniugati in  $A_5$  (ma lo sono in  $S_5$ ).

### Definizione 2.2: Gruppo semplice

$G$  si dice **semplice** se gli unici sottogruppi normali sono  $\{e\}$  e  $G$  stesso.

#### Teorema 2.1

$\forall n \geq 5$ ,  $A_n$  è semplice

*Dimostrazione.* Sia  $N \trianglelefteq A_n$  con  $N \neq \{e\}$ . Dimostriamo che  $N$  contiene un 3-ciclo  $\sigma$  allora  $N$  contiene tutti i coniugati di  $\sigma$  perché è normale.

Sia  $\sigma \in N$  con  $\sigma \neq 1$  con il massimo numero di punti fissi. Vogliamo mostrare che  $\sigma$  è un 3-ciclo.

Consideriamo l'azione  $\langle \sigma \rangle \times \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  data da  $(\sigma^k, i) \mapsto \sigma^k(i)$ . Siccome  $\sigma \neq e$  esiste un  $i$  tale che  $\sigma(i) = j \neq i$ . Dunque  $O_i \ni \{i, j\}$  e quindi  $\#O_i \geq 2$ .

1. Supponiamo che tutte le orbite di elementi non fissati da  $\sigma$  abbiano cardinalità 2.
2. Poiché  $\sigma$  è pari ci devono essere almeno 2 orbite  $O_i, O_r$  di cardinalità 2 (porta ad assurdo)

Quindi esiste almeno un'orbita di  $\langle \sigma \rangle$  con 3 elementi  $i, j, k$ . Se  $\sigma = (ijk)$  ho finito. Altrimenti,  $\sigma$  necessariamente deve muovere altri due elementi, essendo pari. Siano essi  $r$  e  $s$ . Allora prendiamo  $\tau = (krs)$ . A questo punto

$$\sigma' = \underbrace{\tau\sigma\tau^{-1}}_{\in N} \sigma^{-1} \in N$$

Allora tutti i punti fissi di  $\sigma$  lo sono anche per  $\sigma'$  e inoltre  $\sigma'(j) = j$  che non è punto fisso di  $\sigma$ , dunque  $\sigma'$  ha più punti fissi di  $\sigma$ , assurdo.  $\square$

**Esempio 2.2** ( $A_4$  non è semplice).  $A_4 = \{e, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (3\ 4\ 2), (3\ 2\ 4)\}$  e  $H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$  è normale in  $A_4$  e non è  $\{e\}$  o  $A_4$ . Infatti è l'unione dell'intera classe di coniugio del tipo di due trasposizioni disgiunte (e l'identità).

### Definizione 2.3: Gruppo risolubile

Un gruppo  $G$  si dice **risolubile** se esiste una catena di sottogruppi

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 < \dots \trianglelefteq G_n = G$$

dove tutti i quozienti  $G_{i+1}/G_i$  sono abeliani per ogni  $i = 0, \dots, n-1$

*Osservazione.* Non è detto che  $G_i \trianglelefteq G$  per ogni  $i$ .

**Esempio 2.3** (Gruppi abeliani). Ogni gruppo abeliano è risolubile, con la catena  $\{1\} \trianglelefteq G$

**Esempio 2.4** ( $S_3$ ).  $S_3$  è risolubile con la catena

$$\{1\} \trianglelefteq A_3 \trianglelefteq S_3$$

Infatti  $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$  è abeliano e  $A_3/\{1\} \cong \mathbb{Z}/3\mathbb{Z}$  è abeliano.

**Esempio 2.5.**  $D_n$  è risolubile con la catena

$$\{1\} \trianglelefteq \langle r \rangle \trianglelefteq D_n$$

Infatti  $D_n = \langle r, s \mid r^n = 1, s^2 = 2, rs = sr^{-1} \rangle = \langle r \rangle \rtimes_{\varphi} \langle s \rangle$

**Esempio 2.6.**  $S_4$  è risolubile con la catena

$$\{1\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$$

con  $V_4$  il gruppo di Klein (in particolare anche  $A_4$  è risolubile). Notare l'osservazione precedente: Il sottogruppo  $\langle (1\ 2)(3\ 4) \rangle$  è normale in  $V_4$  ma non in  $S_4$

**Gruppi di ordine 12** Vogliamo mostrare che esistono esattamente 5 classi di isomorfismo di gruppi di ordine 12:

- $\mathbb{Z}/12\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
- $D_6$
- $A_4$
- $\langle x, y \mid x^4 = 1, y^3 = 1, xyx^{-1} = y^2 \rangle = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$

*Dimostrazione.*  $12 = 2^2 \cdot 3$  quindi per il teorema di Sylow esiste un 2-Sylow e un 3-Sylow. Sia  $H$  un 2-Sylow e  $K$  un 3-Sylow. Allora  $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$  oppure  $H \cong \mathbb{Z}_4$ ,  $K \cong \mathbb{Z}_3$ . Per il teorema di Sylow il numero  $r$  di 2-Sylow deve essere 1 oppure 3. Inoltre  $s$  il numero di 3-Sylow deve essere 1 oppure 4.

Ora necessariamente  $H \trianglelefteq G$  oppure  $K \trianglelefteq G$ . Infatti supponiamo che  $K$  non sia normale in  $G$ , allora esistono 4 3-Sylow tra loro coniugati. Li chiamiamo  $K_1, K_2, K_3, K_4$ . Allora poiché 3 è primo,  $K_i \cap K_j = \{1\}$  per ogni  $i \neq j$ . Allora  $\#\bigcup_{i=1}^4 K_i = 9$  ma quindi gli unici elementi che non prende sono 3 elementi. Allora  $H$ , un 2-Sylow, deve contenere tali 3 elementi. Essendocene uno solo, è normale. Ora possiamo procedere nei casi seguenti:

1.  $H \trianglelefteq G$  e  $K \trianglelefteq G$ .

Allora  $H \cap K = \{e\}$ .  $HK < G$  e  $\#HK = \frac{\#H \cdot \#K}{\#H \cap K} = 12$ . Allora  $HK = G$  e  $G \cong H \times K$  tramite l'isomorfismo  $(h, k) \mapsto hk$

Allora ne consegue che  $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 = \mathbb{Z}_{12}$  oppure  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_6$

2.  $K$  non è normale e  $H \triangleleft G$ .

Sia  $\psi : G \rightarrow A(S) \cong S_4$ . Allora  $\text{Stab}_{K_i} = \{g \in G : gK_i g^{-1} = K_i\} = N(K_i)$ . Ma allora  $\#N(K_i) = 3$  (formula delle classi) e poiché  $K_i \subseteq N(K_i)$  e ha la stessa cardinalità, essi coincidono. Ma allora  $\text{Ker}\psi = \{e\}$  e  $\psi$  è iniettivo.

$G$  ha 4 3-Sylow e dunque ha 8 elementi di ordine 3. Ma questi sono anche tutti i 3-cicli di  $S_4$ , e dunque per cardinalità  $G \cong A_4$

3.  $K \triangleleft G$  e  $H$  non è normale.

□

#### Definizione 2.4

Sia  $G$  un gruppo abeliano di ordine  $p^n$  con  $p$  primo. Allora  $G \cong A_1 \times \dots \times A_k$  con  $\langle a_i \rangle = A_i$  e  $o(a_i) = p^{n_i}$  e  $n_1 \geq n_2 \geq \dots \geq n_k > 0$ .

Allora gli  $n_i$  si dicono invarianti di  $G$  e

$$\#G = p^n = p^{n_1} \cdot \dots \cdot p^{n_k}$$

gli invarianti danno una partizione di  $n$ .

*Osservazione.*  $\forall m \in \mathbb{Z} \quad G(m) = \{x \in G : x^m = e\} \leq G$

**Lemma 2.2.** Sia  $G$  un gruppo abeliano come nella definizione precedente. Sia  $m \in \mathbb{Z}$  tale che  $n_t > m \geq n_{t+1}$ . Allora

$$G(p^m) \cong B_1 \times \dots \times B_t \times A_{t+1} \times \dots \times A_k$$

dove  $B_i$  è ciclico di ordine  $p^m$  e

$$\#G(p^m) = p^u \quad u = tm + \sum_{j=t+1}^k n_j$$

*Dimostrazione.*

□

**Corollario 2.2.1.** Nelle ipotesi del lemma 2.2,  $\#G(p) = p^k$

#### Teorema 2.3: Classificazione

Due gruppi abeliani di ordine  $p^n$ , con  $p$  primo sono isomorfi se e solo se hanno gli stessi invarianti.

Equivalentemente se  $G$  e  $G'$  sono due gruppi abeliani con  $\#G = \#G' = p^n$  e

$$G \cong A_1 \times \dots \times A_k \quad A_i = \langle a_i \rangle \quad (o(a_i) = p^{n_i}) \quad n_1 \geq n_2 \geq \dots \geq n_k > 0$$

$$G' \cong A'_1 \times \dots \times A'_s \quad A'_i = \langle a'_i \rangle \quad o(a'_i) = p^{n'_i} \quad n'_1 \geq n'_2 \geq \dots \geq n'_s > 0$$

*Dimostrazione.*

$\implies$  Se  $G \cong G'$  allora  $G(p) \cong G'(p)$  e dunque  $\#G(p) = \#G'(p)$  e quindi  $k = s$ .

Supponiamo ora che esista un  $i$  tale che  $n_i \neq n'_i$ . Sia  $t$  il primo tale intero, supponendo che  $m := n_t > n'_t$ . Sia  $H = \{x^{p^m} : x \in G\} \leq G$  perché  $G$  è abeliano e  $H' = \{x'^{p^m} : x' \in G'\} \leq G'$  perché  $G'$  è abeliano.



$\Leftarrow$  se  $k = s$  e  $n_i = n'_i \forall i$  allora

$$\begin{aligned} \Phi : G &\longrightarrow G' \\ (a_1^{\alpha_1} \dots a_k^{\alpha_k}) &\longmapsto \Phi((a_1^{\alpha_1} \dots a_k^{\alpha_k})) = (a_1'^{\alpha_1} \dots a_k'^{\alpha_k}) \end{aligned}$$

□

**Corollario 2.3.1.** *Il numero di classi di isomorfismo di gruppi abeliani di ordine  $p^n$  è il numero di partizioni di  $n$*

**Corollario 2.3.2.** *Il numero di classi di isomorfismo di gruppi abeliani di ordine  $p_1^{\alpha_1} \dots p_r^{\alpha_r}$  con  $p_i$  primi distinti è uguale a  $p(\alpha_1) \dots p(\alpha_r)$  dove  $p^{\alpha_i}$  è il numero di partizioni di  $\alpha_i$*

**Esempio 2.7.** I gruppi abeliani di ordine 8 sono 3, infatti  $8 = 2^3$  e 3 ha 3 partizioni:

- $3 = 3 \implies C_8$
- $3 = 2 + 1 \implies C_4 \times C_2$
- $3 = 1 + 1 + 1 \implies C_2 \times C_2 \times C_2$

che per il teorema sono sicuramente non isomorfi e tutti.

**Esempio 2.8.** I gruppi abeliani di ordine 12 sono 2, infatti  $12 = 2^2 \cdot 3$  e le partizioni di 2 sono 2:  $2 = 2$  e  $2 = 1 + 1$ , e i gruppi sono  $C_2 \times C_2 \times C_3$  e  $C_4 \times C_3$

### Esercizio 2.2

Elencare i gruppi abeliani di ordine 36

### Esercizio 2.3

Supponiamo di avere un gruppo  $G$  di ordine  $1125 = 3^2 \cdot 5^3$  a tale che un suo 5-Sylow sia ciclico. Allora:

- Mostrare che  $G$  è abeliano
- Determinare tutte le classi di isomorfismo possibili per  $G$

Esiste solo un 5-Sylow, infatti  $1 + 5k \mid 3^2 \iff k = 0$  e quindi è normale. Per questioni di ordine deve essere quindi che  $G \cong H \rtimes_{\varphi} K$  con  $H$  il 5-Sylow e  $K$  un 3-Sylow. Allora sapendo che  $H$  è ciclico,  $\text{Aut}(G) = C_{125}^*$  che ha ordine  $\varphi(125) = 100$ . Allora  $\text{Im}(\varphi) < \text{Aut}(H)$  ma inoltre  $\text{Im}(\varphi) < K$  e dunque necessariamente  $\#\text{Im}(\varphi) = 1$  e quindi  $G \cong H \times K$  è abeliano.

Sapendo che  $K$  è abeliano di ordine 9 possiamo trovare le due possibili classi di isomorfismo, ossia  $C_{1125}$  e  $C_{375} \times C_3$