# TEOREMA FONDAMENTALE GRUPPI ABELIANI FINITAMENTE GENERATI

**Lemma** Sia $G$ gr ab. con $\{x_1, \dots, x_n\}$ sist. di gen

Sia $y_1 = a_1 x_1 + \dots + a_n x_n$ con $MCD(a_1, \dots, a_n) = 1$

allora esistono $y_2, \dots, y_n$ t.c. $G = \langle \{y_1, \dots, y_n\} \rangle$.

**Dim:** Sia $m = |a_1| + \dots + |a_n|$ e lavoriamo per induzione su $m$

$\boxed{\text{Se } m = 1}$ $y_1 = \pm x_i$ e la dimostrazione è ovvia

$\boxed{\text{Passo induttivo}}$ $MCD(a_1, \dots, a_n) = 1$ e posso supporre $m > 1$

$\Rightarrow$ esistono $a_i, a_j \neq 0$ con $i \neq j$ (due coeff. diversi da 0)

Supponiamo $|a_i| \geq |a_j| > 0$ allora esiste $e = \pm 1$ tale che $|a_i| > |a_i - e a_j|$

Possiamo scrivere

$$y_1 = a_1 x_1 + \dots + (a_i - e a_j) x_i + \dots + a_j (x_j + e x_i) + \dots$$

[cambio 1 coeff $\boxed{a_i \rightarrow a_i - e a_j}$ e 1 elemento del sist. di gen $\boxed{x_j \rightarrow x_j + e x_i}$]

Osserviamo che:

- $\{x_1, x_2, \dots, x_i, \dots, x_j + e x_i, \dots, x_n\}$ è un sistema di generatori
- $MCD(a_1, a_2, \dots, a_i - e a_j, \dots, a_j, \dots, a_n) = 1$
- $$|a_1| + |a_2| + \dots + |a_i| + \dots + |a_j| + \dots + |a_n|$$
$$\vee$$
$$|a_1| + |a_2| + \dots + |a_i - e a_j| + \dots |a_j| + \dots + |a_n|$$

Per ipotesi induttiva ottengo le tesi

$\boxtimes$

Teorema (fondamentale dei gr. ab. fin gen)

G gruppo ab finitamente gen. allora esistono $E_1, \dots, E_m, I_1, \dots, I_r$ sottogruppi di G t.c.

- $G = E_1 \times \dots \times E_m \times I_1 \times \dots \times I_r$ (Prodotto diretto interno)
- $I_i$ gruppi ciclici infiniti ($I_i \cong \mathbb{Z}$)
- $E_i$ gruppi ciclici finiti di ordine $e_i$ ($E_i \cong \mathbb{Z}_{e_i}$)

Possiamo ottenere gli $E_i$ in maniera da avere che $e_i$ divide $e_{i+1}$ per ogni $i = 1, \dots, m-1$
In questo caso l'$m+1$-pla $(e_1, \dots, e_m; r)$ è unicamente determinata da G

Dim: Fissiamo $\{x_1, \dots, x_n\}$ sist. di generatori di $G$ t.c.

1) $n$ minimale

2) se $G = \langle x_1, \dots, x_{i-1}, y_i, y_{i+1}, \dots, y_n \rangle$

allora $|x_i| \leq |y_i|$

(Se $x_i$ ha ordine infinito poniamo $|x_i| = \infty$)

Nota: per ottenere questo sistema di generatori considero i sistemi di generatori con $n$ elementi

Per ogni sistema di generatori ordino gli elementi in maniera che l'ordine degli elementi sia crescente

Con gli elementi così ordinati seleziono i sistemi di generatori che hanno il primo elemento con ordine minore

Fra questi seleziono quelli con secondo elemento con ordine minore

Continuando così per tutti gli elementi ottengo i sist. di generatori con le proprietà richieste

[è collegato all' "ordine lessicografico"]

Definisco $C_i = \langle x_i \rangle$ e dimostreremo

$G = C_1 \times \dots \times C_n$

Ponendo $e_i = |C_i|$ otterremo $e_i \mid e_{i+1}$

(si usa la convenzione $n$ divide $\infty$ per ogni $n$)

<u>Oss</u>: le propriete richieste e $\{x_1, \dots, x_n\}$ implica

che $c_i \leq c_{i+1}$ (atrimenti scambiando $x_i$

e $x_{i+1}$ le 2 viene negate)

Supponiamo

$$a_i x_i + \dots + a_j x_j = 0$$

ordiniamo con indici crescenti e possiamo supporre $a_k \neq 0$

Possiamo quindi considerare coefficienti t.c. $0 < |a_k| \leq e_k$

Definiamo $d = MCD(a_i, \dots, a_j)$, $b_k = \frac{a_k}{d}$, $y_i = b_i x_i + \dots + b_j x_j$

Allora per il Lemma esistono $y_{i+1}, \dots, y_n$ tali che

$\langle x_i, \dots, x_n \rangle = \langle y_i, \dots, y_n \rangle$ da cui otteniamo

$\langle x_1, \dots, x_n \rangle = \langle x_1, \dots, x_{i-1}, y_i, \dots, y_n \rangle$

Per le proprietà richiesta a $\{x_1, \dots, x_n\}$

si ha $|g_i| \geq |x_i| = e_i$

D'altra parte $d g_i = d b_i x_i + \dots + d b_j x_j = a_i x_i + \dots + a_j x_j = 0$

per cui $e_i \geq |a_i| \geq d \geq |g_i|$

Concludiamo $d = e_i = |a_i|$ e $a_i x_i = 0$

Reitero e ottengo $a_k x_k = 0$ per ogni $k$

Abbiamo dimostrato

$$a_i x_i + \dots + a_j x_j = 0 \implies a_k x_k = 0 \quad \forall k$$

Questo implica che $g \in G$ può essere rappresentato in maniera unica come somma degli elementi dei $C_i$

Infatti se $a_1 x_1 + \dots + a_n x_n = b_1 x_1 + \dots + b_n x_n$

$\implies (a_1 - b_1) x_1 + \dots + (a_n - b_n) x_n = 0$

$\implies (a_k - b_k) x_k = 0 \quad \forall k$

$\implies a_k x_k - b_k x_k = 0 \quad \forall k$

$\implies a_k x_k = b_k x_k \quad \forall k$

Per le caratterizzazioni del prodotto diretto interno con più fattori abbiamo che

$$G = C_1 \times \dots \times C_n$$

Inoltre se $e_i, e_{i+1} < \infty$ possiamo considerare $e_i x_i + e_{i+1} x_{i+1} = 0$ e usare le stesse tecnice ottenendo

$d = MCD(e_i, e_{i+1}) = e_i$ da cui $e_i \backslash e_{i+1}$

Supponiamo $m$ sia l'ultimo indice per cui $e_k < \infty$

Definiamo $E_i \overset{def}{=} C_i$ per $1 \leq i \leq m$

$r \overset{def}{=} n - m$

$I_i \overset{def}{=} C_{i+m}$ per $1 \leq i \leq r$

ottenendo

$$\boxed{\begin{array}{l} G = E_1 \times \dots \times E_m \times I_1 \times \dots \times I_r \\ \text{con } e_i \backslash e_{i+1} \text{ per } i = 1, \dots, m-1 \end{array}}$$

Manca da dimostrare l'unicità di $(e_1, \dots, e_m; r)$ (104)

Osservazione: Se $G = E_1 \times \dots \times E_m \times I_1 \times \dots \times I_r$ vale che: $E_1 \times \dots + E_m = \{g \in G \mid g \text{ di ordine finito}\}$

Dim dell'osservazione:

- se $y \in E_1 \times \dots \times E_m$ allora $y^{e_m} = 1_G$
- se $y \notin E_1 \times \dots \times E_m$ allora

$y = z_1 + \dots + z_m + w_1 + \dots + w_r$ con $z_i \in E_i, w_i \in I_i$

e $\exists k$ tale che $w_k \neq 0$

Questo implica che $|y| = \infty$

$\blacksquare$ (fine dim oss)

Def: $T(G) \overset{def}{=} \{y \in G \mid y \text{ di ordine finito}\}$

Si chiama il sottogruppo di torsione di $G$

[Torniamo alla dimostrazione del teorema]

Supponiamo:

$G = E_1 \times \dots \times E_m \times I_1 \times \dots \times I_r = E_1' \times \dots \times E_n' \times I_1' \times \dots \times I_s'$

con $E_i, E_i'$ ciclici finiti, $I_i, I_i'$ ciclici infiniti,

$|E_i| \setminus |E_{i+1}|$ e $|E_i'| \setminus |E_{i+1}'|$

Otteniamo subito

- $T(G) = E_1 \times \dots \times E_m = E_1' \times \dots \times E_n'$

- $\frac{G}{T(G)} \cong \underbrace{I_1 \times \dots \times I_r}_{\substack{\text{gr. ab. lib.} \\ \text{di rango } r}} \cong \underbrace{I_1' \times \dots \times I_s'}_{\substack{\text{gr. ab. lib.} \\ \text{di rango } s}} \Rightarrow r = s$

Supponiamo ora $T(G)$ sia un $p$-gruppo

$|E_m| =$ ordine massimo di un elemento in $T(G)$ $= |E_n'|$

definiamo $k$ t.c. $p^k = |E_m| = |E_n'|$

Sia $w$ tale che $\langle w \rangle = E_n'$

$\Rightarrow w = v_1 + \dots + v_m$ con $v_i \in E_i$

Almeno uno dei $v_i$ deve avere ordine $p^k$

Possiamo supporre $|v_m| = p^k$ (altrimenti effettuiamo un riordinamento) per cui $\langle v_m \rangle = E_m$

Otteniamo quindi

$(E_1 \times \dots \times E_{m-1}) + E_n' = G$

Siccome $|E_1 \times \dots \times E_{m-1}| \cdot |E_m| = |G|$, $|E_m| = |E_n'|$ e $\frac{|E_1 \times \dots \times E_{m-1}||E_n'|}{|(E_1 \times \dots \times E_{m-1}) \cap E_n'|} = |G|$ otteniamo $|(E_1 \times \dots \times E_{m-1}) \cap E_n'| = 1$

e quindi $(E_1 \times \ldots \times E_{m-1}) \cap E'_n = \{1_G\}$

$G = E_1 \times \ldots \times E_{m-1} \times E'_n = E'_1 \times \ldots \times E'_{n-1} \times E'_n$

$\Rightarrow \dfrac{G}{E'_n} \cong E_1 \times \ldots \times E_{m-1} \cong E'_1 \times \ldots \times E'_{n-1}$

Reiterando il procedimento ottengo

$m = n$ e $|E_i| = |E'_i|$ per ogni $i$

Consideriamo ora il caso generale in cui $T(G)$ non è un p-gruppo

[ Ricordo che $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m \Leftrightarrow M.C.D.(n,m) = 1$ ]

$T(G)$ abeliano $\Rightarrow$ ha un unico p-gruppo

Posso considerare $|E_i| = a_i p^{k_i}$ con $MCD(a_i, p) = 1$

$|E'_i| = b_i p^{h_i}$ con $MCD(b_i, p) = 1$

Prendo $p \mid |E_1|$ e considero

$S_p \cong \underbrace{\mathbb{Z}_{p^{k_1}} \times \ldots \times \mathbb{Z}_{p^{k_m}}}_{\text{tutti non banali } (k_i > 0)} \cong \underbrace{\mathbb{Z}_{p^{h_1}} \times \ldots \times \mathbb{Z}_{p^{h_m}}}_{\text{a priori i primi fattori potrebbero essere banali}}$

perchè $p \mid |E_1| \mid |E_2| \mid \ldots$

$k_1 \leq k_2 \leq \ldots \leq k_m$

per il caso precedente (con $T(G)$ $p$-gruppo) otteniamo $n \geq m$ e $p^{k_i} = p^{k_i + (n-m)}$

Ma se prendo $q$ primo che divide $|E_1|$ ottengo $m \geq n$ che mi assicura $n = m$

In particolare ottengo $p^{k_i} = p^{h_i}$

Rifaccio lo stesso procedimento per tutti i primi che dividono $|G|$ e ottengo la tesi

$\blacksquare$

---

<u>Definizione</u> Siano $e_i$ e $r$ come da enunciato del teorema:

- $e_i$ si dicono <u>coefficienti di torsione</u> di $G$
- $r$ si dice il <u>rango</u> (o <u>numero di Betti</u>) di $G$

I coeff. di torsione ed il rango sono unicamente determinati

Esempi: 1) [Uso $MCD(n,m)=1 \Leftrightarrow \mathbb{Z}_{n\cdot m} \cong \mathbb{Z}_n \times \mathbb{Z}_m$]

$G \cong \mathbb{Z}_{24} \times \mathbb{Z}_{33} \times \mathbb{Z}_{20} \times \mathbb{Z}_{75} \times \mathbb{Z}_{126}$

$\cong \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{25} \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_7$

$\cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8}_{\substack{\text{2-Sylow} \\ \text{3 fattori}}} \times \underbrace{\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9}_{\substack{\text{3-Sylow} \\ \text{4 fattori}}} \times \underbrace{\mathbb{Z}_5 \times \mathbb{Z}_{25}}_{\substack{\text{5-Sylow} \\ \text{2 fattori}}} \times \underbrace{\mathbb{Z}_7}_{\substack{\text{7-Sylow} \\ \text{1 fatt.}}} \times \underbrace{\mathbb{Z}_{11}}_{\substack{\text{11-Sylow} \\ \text{1 fatt}}}$

[Per ottenere i coeff di torsione: il numero degli $E_i$ è pari al numero dei fattori del p-Sylow con più fattori, per i p-Sylow con meno fattori si completa con fattori banali]

$\cong \mathbb{Z}_3 \times (\mathbb{Z}_3 \times \mathbb{Z}_2) \times (\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5) \times (\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \times \mathbb{Z}_7 \times \mathbb{Z}_{11})$

$\cong \mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{60} \times \mathbb{Z}_{138600}$

coefficienti di torsione $3, 6, 60, 138600$ (univocamente determinati)

2) Classificare i gruppi abeliani di ordine 72

$72 = 8 \cdot 9 = 2^3 \cdot 3^2$

2-Sylow possibili: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ o $\mathbb{Z}_2 \times \mathbb{Z}_4$ o $\mathbb{Z}_8$

3-Sylow possibili: $\mathbb{Z}_3 \times \mathbb{Z}_3$ o $\mathbb{Z}_9$

Quindi i gruppi ab. di ordine 72 sono:

$\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{18}$, $\mathbb{Z}_6 \times \mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_{36}$

$\mathbb{Z}_3 \times \mathbb{Z}_{24}$, $\mathbb{Z}_{72}$ (a meno di isomorfismi)

3) Classificare i gruppi di ordine $p^5$

Cerco $\alpha_1, \dots, \alpha_k$ tale che $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \dots \times \mathbb{Z}_{p^{\alpha_k}} \cong \mathbb{Z}_{p^5}$

(quindi $\alpha_1 + \alpha_2 + \dots + \alpha_k = 5$) e $\alpha_1 \leq \alpha_2 \leq \dots \leq \alpha_k$ (coeff di tors.)

In questo caso ho le seguenti possibilità per gli $\alpha_i$:
$(1,1,1,1,1)$ $(1,1,1,2)$ $(1,2,2)$ $(1,1,3)$ $(2,3)$ $(1,4)$ $(5)$

Da cui otteniamo: se $G$ t.c. $|G| = p^5$ allora

$G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p = (\mathbb{Z}_p)^5$ oppure
$G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2} = \mathbb{Z}_p^3 \times \mathbb{Z}_{p^2}$ oppure
$G \cong \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} = \mathbb{Z}_p \times (\mathbb{Z}_{p^2})^2$ oppure
$G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^3} = (\mathbb{Z}_p)^2 \times \mathbb{Z}_{p^3}$ oppure $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^3}$
oppure $G \cong \mathbb{Z}_p \times \mathbb{Z}_{p^4}$ oppure $G \cong \mathbb{Z}_{p^5}$

<u>Osservazione</u>: Gli $I_i$ e gli $E_i$ <u>non</u> sono unicamente determinati

<u>Problema</u>: trovare degli esempi che dimostrano che gli $I_i$ e gli $E_i$ non sono unici.