Il teorema di struttura per gruppi abeliani finiti

di Gabriel Antonio Videtta

Nota. Nel corso del documento con G si indicherà un qualsiasi gruppo.

Teorema (di struttura per gruppi abeliani finiti)**.** Sia G un gruppo abeliano finito. Allora esistono unici $n_1, \ldots, n_s \in \mathbb{N}$ tali per cui:

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}, \qquad n_s \mid n_{s-1} \mid \cdots \mid n_2 \mid n_1.$$

Definizione (p-componente)**.** Si definisce p**-componente** $G(p)$ (o p-torsione) di G il sottogruppo di G tale per cui:

$$G(p) = \{x \in G \mid \operatorname{ord}(x) = p^k \text{ per qualche } k\}.$$

Osservazione. Si dimostra facilmente che $G(p)$ è un sottogruppo. Chiaramente $G(p) \subseteq G$; inoltre e chiaramente appartiene a $G(p)$. Se poi x, $y \in G(p)$, allora $\operatorname{ord}(xy) \mid \operatorname{mcm}(\operatorname{ord}(x), \operatorname{ord}(y))$, e quindi $\operatorname{ord}(xy) = p^k$ per qualche k. Pertanto anche $xy \in G(p)$. Dal momento che $G(p)$ è finito, questo dimostra che $G(p)$ è un sottogruppo.

Osservazione. $G(p)$ è un sottogruppo caratteristico di G. Infatti $\varphi \in \operatorname{Aut}(G)$ lascia invariato l'ordine di un elemento di $G(p)$, e quindi $\varphi(G(p)) = G(p)$.

Osservazione. La dimostrazione del teorema di struttura segue il seguente schema:

- Se G è abeliano con $|G| = p_1^{e_1} \cdots p_r^{e_r}$, allora $G \cong G(p_1) \times \cdots \times G(p_r)$, ossia G è isomorfo al prodotto diretto tra le sue p-componenti. Tale decomposizione di G come prodotto di p-gruppi di ordini tra loro coprimi è unica.
- Se G è un p-gruppo abeliano. Allora esistono e sono univocamente determinati degli interi positivi $r_1 \geq \cdots \geq r_s$ tali che $G \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{r_s}\mathbb{Z}$.

Dimostrazione a priori. Per il primo teorema, G si può decomporre nelle sue p-componenti:

$$G \cong G(p_1) \times \cdots \times G(p_s).$$

Allora, per il secondo teorema, ogni $G(p_i)$ può decomporsi come prodotto diretto di $\mathbb{Z}/p_i^k\mathbb{Z}$, e quindi:

$$G \cong (\mathbb{Z}/p_1\mathbb{Z}^{e_{1,1}} \times \cdots \times \mathbb{Z}/p_1\mathbb{Z}^{e_{1,t_1}}) \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z}^{e_{r,1}} \times \cdots \times \mathbb{Z}/p_1\mathbb{Z}^{e_{r,t_r}}).$$

Sia $t = \max\{t_1, \dots, t_r\}$. Posso allungare le fattorizzazioni di $G(p_i)$ fino ad ottenere t fattori aggiungendo eventualmente dei gruppi banali nella fattorizzazione.

Applicando allora il Teorema cinese del resto si ottiene l'esistenza della fattorizzazione secondo il Teorema di struttura per gruppi abeliani finiti.
L'unicità segue dal primo teorema riapplicando il Teorema cinese del resto al contrario.

$\square$

Si dimostrano i due teoremi:

Teorema. Se G è abeliano con $|G| = p_1^{e_1} \cdots p_r^{e_r}$, allora $G \cong G(p_1) \times \cdots \times G(p_r)$, ossia G è isomorfo al prodotto diretto tra le sue p-componenti. Tale decomposizione di G come prodotto di p-gruppi di ordini tra loro coprimi è unica.

Dimostrazione. Si dimostra per induzione sul numero s di primi distinti nella fattorizzazione di $|G|$. Se $s = 1$, G coincide con l'unica sua p-componente. Sia ora $s \geq 2$. Se $|G| = mm'$ con $m' > 1$ e $\mathrm{MCD}(m, m') = 1$. Mostro che $G \cong mG \times m'G$.

$\square$

Teorema. Se G è un p-gruppo abeliano. Allora esistono e sono univocamente determinati degli interi positivi $r_1 \geq \cdots \geq r_s$ tali che $G \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{r_s}\mathbb{Z}$.