Il teorema di struttura per gruppi abeliani finiti e decomposizione di $(\mathbb{Z}/n\mathbb{Z})^*$

di Gabriel Antonio Videtta

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

In questo documento si dimostra il celebre Teorema di struttura per gruppi abeliani finiti. In realtà questo teorema è un caso particolare del Teorema di struttura per gruppi abeliani finitamente generati (e quindi potenzialmente infiniti), a sua volta caso particolare del Teorema di struttura per moduli finitamente generati su un PID[1]. Per motivi didattici si riporta la dimostrazione semplificata per il semplice caso dei gruppi abeliani finiti.

Il Teorema di struttura trova immediata applicazione nello studio dei gruppi abeliani finiti e, dato $n \in \mathbb{N}^+$, permette di classificare tutti i gruppi abeliani di ordine n (a meno di isomorfismo), come illustra il seguente enunciato:

Teorema (di struttura per gruppi abeliani finiti, decomposizione in fattori invarianti)**.** Sia G un gruppo abeliano finito. Allora esistono unici $n_1, \dots, n_s \in \mathbb{N}^+ \setminus \{1\}$ tali per cui:

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

Tale fattorizzazione di G viene detta **decomposizione in fattori invarianti**, dove i fattori invarianti sono i vari n_i.

Equivalentemente si poteva enunciare il Teorema di struttura utilizzando la *decomposizione in fattori elementari* mediante l'applicazione reiterata del Teorema cinese del resto, come illustra il:

Teorema (di struttura per gruppi abeliani finiti, decomposizione primaria)**.** Sia G un gruppo abeliano finito. Allora esistono unici $p_1, \dots, p_s$ numeri primi e unici $m_{i,1} \geq \cdots \geq m_{i,t_i}$ per ogni $1 \leq i \leq s$ tali per cui:

$$G \cong \mathbb{Z}/\big(p_1^{m_{1,1}}\big)\mathbb{Z} \times \cdots \times \mathbb{Z}/\big(p_1^{m_{1,t_1}}\big)\mathbb{Z} \times \mathbb{Z}/\big(p_2^{m_{2,1}}\big)\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_s^{m_{s,t_s}})\mathbb{Z}.$$

[1] Ho trattato e dimostrato questo teorema in un documento separato, reperibile su `https://git.phc.dm.unipi.it/g.videtta/scritti/src/branch/main/Geometria/Articoli/3.%20Il%20teorema%20di%20struttura%20dei%20moduli%20finitamente%20generati%20su%20un%20PID/main.pdf`

Tale fattorizzazione di G viene detta **decomposizione primaria** (o in fattori elementari), dove i fattori elementari sono i vari $p_i^{m_{i,j}}$.

Prima di dimostrare il Teorema di struttura, si definisce il concetto di p-componente relativa a un numero p primo.

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

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

Osservazione. Si osserva facilmente che $G(p)$ è effettivamente un sottogruppo. Infatti vale chiaramente che $G(p) \subseteq G$; inoltre e appartiene a $G(p)$. Dati allora x, $y \in G(p)$, allora $\text{ord}(xy) \mid \text{mcm}(\text{ord}(x), \text{ord}(y))$, e quindi $\text{ord}(xy) = p^k$ per qualche k. Pertanto anche $xy \in G(p)$. Dal momento che $G(p)$ è finito, la chiusura sull'operazione di gruppo implica anche l'esistenza dell'inverso, e dunque $G(p)$ è un sottogruppo di G.

Osservazione. Si osserva che $G(p)$ ha ordine p^n, dove $p^n \parallel n = |G|$ e che se $H \leq G$ è un sottogruppo di ordine p^i, H è chiaramente un sottogruppo di $G(p)$. Pertanto, si può definire equivalentemente $G(p)$ come il p-sottogruppo[2] massimo per inclusione di G.

Osservazione. La p-componente $G(p)$ è anche un sottogruppo caratteristico di G. Infatti $\varphi \in \text{Aut}(G)$ lascia invariato l'ordine di un elemento di $G(p)$, e quindi $\varphi(G(p)) = G(p)$. Alternativamente si può utilizzare l'osservazione precedente e notare che $G(p)$ è l'unico sottogruppo del suo ordine[3].

Schema della dimostrazione. La dimostrazione del Teorema di struttura si fonda su due teoremi che verranno dimostrati nel seguito e che vengono ora enunciati:

- 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:

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

[2] Chiaramente $G(p)$ è un p-sottogruppo. Infatti, se q fosse un primo diverso da p che divide $|G(p)|$, per il Teorema di Cauchy esisterebbe un elemento di ordine q in $G(p)$, E.

[3] In ogni caso G è abeliano e quindi, poiché tutti i p-Sylow sono coniugati, $G(p)$ è l'unico p-Sylow di G, e dunque è caratteristico perché unico del suo ordine. Più elementarmente, ogni p-sottogruppo di G è contenuto in $G(p)$, e quindi è l'unico del suo ordine.

Sia $t = \max\{t_1, \ldots, t_r\}$. 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 riapplicando prima il primo teorema e poi il secondo teorema. □

Esempio ($\mathbb{Z}/26\mathbb{Z}\times\mathbb{Z}/169\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$)**.** Si scrive il gruppo $G = \mathbb{Z}/26\mathbb{Z}\times\mathbb{Z}/169\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ seguendo le regole del Teorema di struttura. Poiché $26 = 2 \cdot 13$, $169 = 13^2$ e $12 = 2^2 \cdot 3$, applicando il Teorema cinese del resto si può scrivere G come:

$$G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}) \times (\mathbb{Z}/13^2\mathbb{Z}) \times (\mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}).$$

Facendo commutare i fattori come nella dimostrazione del Teorema di struttura otteniamo che:

$$G \cong (\mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/13^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}),$$

e quindi vale la seguente decomposizione in fattori invarianti per G:

$$G \cong \mathbb{Z}/2028\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z},$$

dove si osserva che $26 \mid 2028$.

Si dimostrano adesso i due teoremi impiegati nella dimostrazione del Teorema di struttura:

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. □

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 $G \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{r_s}\mathbb{Z}$.

Dimostrazione. □

I gruppi moltiplicativi $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ e $\left(\mathbb{Z}/2p^k\mathbb{Z}\right)^*$, con p numero primo, sono completamente classificati e sono note le loro decomposizioni in fattori invarianti, come mostra il fondamentale:

Teorema. Sia p un numero primo dispari e $k \in \mathbb{N}^+$. Allora, $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ e $\left(\mathbb{Z}/2p^k\mathbb{Z}\right)^*$ sono gruppi ciclici. Per $k > 2$, vale inoltre che $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$, mentre $(\mathbb{Z}/2\mathbb{Z})^* \cong \{e\}$ e $(\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$.

In particolare per $n \geq 1$, $(\mathbb{Z}/n\mathbb{Z})^*$ è ciclico se e solo se n è 1, 2, p^k o $2p^k$ con p primo dispari.

Dimostrazione. Chiaramente $(\mathbb{Z}/2\mathbb{Z})^* \cong \{e\}$ e $(\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$ dacché hanno uno ordine 1 e l'altro ordine 2.

Sia ora p un numero primo dispari. Allora l'ordine di $G = \left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ è $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. È dunque sufficiente trovare in $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ un elemento x di ordine p^{k-1} e uno y di ordine $p-1$ per concludere che $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ è ciclico. Infatti $\text{MCD}(p^{k-1}, p-1) = 1$ e x e y commutano, dunque, in tal caso, si avrebbe che $\text{ord}(xy) = |G|$.

Si mostra che $1+p$ ha ordine esattamente p^{k-1} in $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ mostrando per induzione che

$$(1+p)^{p^{i-2}} \equiv 1 + p^{i-1} \quad (p^i),$$

per $i \geq 2$. Per $i = 2$, la tesi è banale. Si assuma allora l'ipotesi induttiva.

Per l'ipotesi induttiva vale allora che $(1+p)^{p^{i-3}} = 1 + p^{i-2} + \alpha p^{i-1}$ per qualche $\alpha \in \mathbb{Z}$, e quindi:

$$(1+p)^{p^{i-2}} \equiv ((1+p)^{p^{i-3}})^p \equiv (1 + p^{i-2}(1+\alpha p))^p \quad (p^i).$$

Applicando allora il Teorema del binomio di Newton, vale che:

$$(1+p)^{p^{i-2}} \equiv 1 + p^{i-1}(1+\alpha p) + \sum_{j=2}^{p} \binom{p}{j} p^{j(i-2)}(1+\alpha p)^j \quad (p^i).$$

Si osserva che $\binom{p}{j}$ è sempre divisibile per p con $2 \leq j \leq p$, e dunque ogni termine della somma è divisibile per p^i. Infatti $j(i-2)+1 \geq i$ per $j \geq \lfloor 1 + \frac{1}{i-2} \rfloor = 1$. Allora si conclude che:

$$(1+p)^{p^{i-2}} \equiv 1 + p^{i-1}(1+\alpha p) \equiv 1 + p^{i-1} \quad (p^i),$$

completando l'induzione.

Allora vale che $(1+p)^{p^{k-1}} \equiv 1 + p^k \ (p^{k+1})$, e quindi $(1+p)^{p^{k-1}} \equiv 1 \ (p^k)$. Pertanto l'ordine di $(1+p)$ è della forma p^i con $i \leq k-1$. Si mostra che $\text{ord}(1+p) \nmid p^{k-2}$. Infatti vale che:

$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \not\equiv 1 \quad (p^k).$$

Si conclude dunque che $\text{ord}(1+p) = p^{k-1}$.

Si consideri ora l'omomorfismo $\pi : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ tale per cui $[x]_{p^k} \overset{\pi}{\mapsto} [x]_p$. Si verifica facilmente che tale mappa è ben definita, infatti $a \equiv b \ (p^k) \implies a \equiv b \ (p)$.

Sia π^* la restrizione di π a $\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Si osserva che tale restrizione è ben definita dacché $\text{MCD}(p^k, a) = 1 \iff \text{MCD}(p, a) = 1$. Allora anche π^* è un omomorfismo e, come π, è surgettivo. Poiché $(\mathbb{Z}/p\mathbb{Z})^*$ è ciclico in quanto gruppo moltiplicativo finito del campo $(\mathbb{Z}/p\mathbb{Z})^*$, allora, dacché $|(\mathbb{Z}/p\mathbb{Z})^*| = \varphi(p) = p-1$, esiste $x \in (\mathbb{Z}/p\mathbb{Z})^*$ tale per cui $\text{ord}(x) = p-1$.

Dal momento che π^* è surgettivo, esiste $y \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ tale per cui $p-1 = \text{ord}(x) \mid \text{ord}(y)$. Allora esiste $z \in \langle y \rangle$ tale per cui $\text{ord}(z) = p-1$. Pertanto $(1+p)z$ ha ordine $p^{k-1}(p-1)$, e dunque $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$ è ciclico.

Dacché p è dispari, vale che $\left(\mathbb{Z}/2p^k\mathbb{Z}\right)^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times \left(\mathbb{Z}/p^k\mathbb{Z}\right)^* \cong \left(\mathbb{Z}/p^k\mathbb{Z}\right)^*$, e quindi anche $\left(\mathbb{Z}/2p^k\mathbb{Z}\right)^*$ è ciclico.

Sia ora $k > 2$. Chiaramente $[5]_{2^n} \in \left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ dal momento che $\text{MCD}(5, 2^k) = 1$. Si mostra che $\text{ord}([5]_{2^n})$ ha ordine 2^{n-2} in $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$. Analogamente a prima si dimostra per induzione che per $n \geq 3$:

$$(1+4)^{2^{n-3}} \equiv 1 + 2^{n-1} \quad (2^n).$$

Chiaramente per $n = 3$, $(1+4) \equiv 1+4$ (8). Si assuma ora l'ipotesi induttiva. Allora $(1+4)^{2^{n-4}} = 1 + 2^{n-2} + \alpha 2^{n-1}$ per qualche $\alpha \in \mathbb{Z}$. Vale dunque che:

$$(1+4)^{2^{n-3}} \equiv (1 + 2^{n-2} + \alpha 2^{n-1})^2 \quad (2^n),$$

e quindi:

$$(1+4)^{2^{n-3}} \equiv 1 + 2^{2(n-2)} + \alpha^2 2^{2(n-1)} + 2^{n-1} + \alpha 2^n + \alpha 2^{2n-3} \quad (2^n).$$

Pertanto vale che $(1+4)^{2^{n-3}} \equiv 1 + 2^{n-1}$ (2^n), concludendo l'induzione.

Allora $(1+4)^{2^{k-2}} \equiv 1 + 2^k$ (2^{k+1}), e quindi $(1+4)^{2^{k-2}} \equiv 1$ (2^k). Pertanto $\text{ord}([5]_{2^k}) = 2^i$ con $i \leq k-2$. Tuttavia $(1+4)^{2^{k-3}} \equiv 1 + 2^{k-1}$ (2^k), e quindi $\text{ord}([5]_{2^k})$ vale esattamente 2^{k-2}.

Per il Teorema di struttura, $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ può dunque essere isomorfo solo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$ o a $\mathbb{Z}/2^{k-1}\mathbb{Z}$. È dunque sufficiente mostrare che $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ non può essere ciclico. Si considerino i due sottogruppi $H_1 = \langle 5^{2^{k-3}} \rangle$ e $H_2 = \langle -5^{2^{k-3}} \rangle$. Entrambi i sottogruppi sono di ordine 2 e sono distinti. Infatti, $5^{2^{k-3}} \equiv -5^{2^{k-3}}$ (2^k) implicherebbe $2 \cdot 5^{2^{k-3}} \equiv 0$ (2^k), e quindi varrebbe $2^{k-1} \mid 5^{2^{k-3}}$, ↯. Se però $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ fosse ciclico, esisterebbe un unico sottogruppo di ordine 2. Pertanto $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$, come desiderato.

Si consideri ora $(\mathbb{Z}/n\mathbb{Z})^*$. Se n è 1, 2, 4, p^k o $2p^k$ con p dispari, $(\mathbb{Z}/n\mathbb{Z})^*$ è ciclico per quanto dimostrato.

Si mostra ora per induzione su $n \geq 1$ che $(\mathbb{Z}/n\mathbb{Z})^*$ è ciclico se e solo se n è 1, 2, 4, p^k o $2p^k$ con p dispari. Per $(\mathbb{Z}/\mathbb{Z})^*$, la tesi è banale. Sia ora $(\mathbb{Z}/n\mathbb{Z})^*$ ciclico. Allora, se n fosse uguale ad ab con $\text{MCD}(a, b) = 1$ e $a, b > 1$, varrebbe $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/a\mathbb{Z})^* \times (\mathbb{Z}/b\mathbb{Z})^*$. Dal momento che $(\mathbb{Z}/a\mathbb{Z})^* \cong (\mathbb{Z}/a\mathbb{Z})^* \times \{e\}$, che a sua volta si identifica come sottogruppo di $(\mathbb{Z}/n\mathbb{Z})^*$, e quindi ciclico, $(\mathbb{Z}/a\mathbb{Z})^*$ stesso è ciclico, e analogamente anche $(\mathbb{Z}/b\mathbb{Z})^*$. Pertanto deve valere $\text{MCD}(\varphi(a), \varphi(b)) = 1$.

Dal momento che $\varphi(a)$ può essere o 1 o un numero pari, così come $\varphi(b)$, si può assumere senza perdita di generalità che $\varphi(a) = 1$, e dunque che a sia 1 o 2. Poiché $(\mathbb{Z}/b\mathbb{Z})^*$ è ciclico e b è strettamente minore di n, per il passo induttivo b può essere 1, 2, p^k o $2p^k$. Dal momento che $\text{MCD}(a, b) = 1$, b può essere solo 1 o p^k, e quindi $n = 2$ o $n = 2p^k$.

Se invece $n = ab$ con $\text{MCD}(a, b) = 1$ implica che uno tra a e b sia 1, allora n è 1 o una potenza di un primo, detto p^k. Se $p = 2$, allora, per $k \geq 3$, $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ conterrebbe una

copia isomorfa di $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In tal caso, non essendo $(\mathbb{Z}/8\mathbb{Z})^*$ ciclico, nemmeno $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ è ciclico, e quindi 2^k può essere solo 1, 2 o 4. Si conclude così la dimostrazione del teorema. □

Osservazione (La funzione $\lambda(n)$ di Carmichael)**.** Si definisce la funzione $\lambda : \mathbb{N}^+ \to \mathbb{N}^+$ di Carmichael in modo tale che $\lambda(n)$ sia il più piccolo intero positivo m tale per cui $a^m \equiv 1 \ (n)$ per ogni a coprimo con n.

Grazie al Teorema sulla decomposizione di $(\mathbb{Z}/n\mathbb{Z})^*$, calcolare $\lambda(n)$ risulta piuttosto semplice. Infatti, $\lambda(n)$ è esattamente il minimo comune multiplo di tutti gli ordini di $(\mathbb{Z}/n\mathbb{Z})^*$. In particolare, $\lambda(n)$ divide sempre $\varphi(n)$ e vale l'uguaglianza se e solo se esiste un elemento x in $(\mathbb{Z}/n\mathbb{Z})^*$ di ordine $\varphi(n)$, ossia se e solo se $(\mathbb{Z}/n\mathbb{Z})^*$ è ciclico (e dunque se e solo se n è 1, 2, 4, p^k o $2p^k$ per p primo dispari).

Esempio ($\lambda(1000)$)**.** Si calcola $\lambda(1000)$. Dal momento che $1000 = 2^3 \cdot 5^3$, vale che $(\mathbb{Z}/1000\mathbb{Z})^* \cong (\mathbb{Z}/2^3\mathbb{Z})^* \times (\mathbb{Z}/5^3\mathbb{Z})^*$. Dacché 5 è dispari e $\varphi(5^3) = 5^3 - 5^2 = 100$, $(\mathbb{Z}/5^3\mathbb{Z})^* \cong \mathbb{Z}/100\mathbb{Z}$, mentre $(\mathbb{Z}/2^3\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Pertanto vale che:

$$(\mathbb{Z}/1000\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z},$$

e quindi $\lambda(1000) = \text{mcm}(2, 2, 100) = 100$.