Alma Mater Studiorum · Università di Bologna

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea Triennale in Matematica

Classificazione dei gruppi abeliani finitamente generati

Tesi di Laurea Triennale in Algebra

Relatore:
Chiar.ma Prof.ssa
Rita Fioresi

Presentata da:
Alice Tomba

II Sessione
Anno Accademico 2010-2011

Introduzione

Il concetto di gruppo è di fondamentale importanza nello studio dell'algebra. La teoria dei gruppi aiuta a comprendere meglio altre strutture e a catturarne le simmetrie e le proprietà invarianti. I gruppi abeliani in particolare sono alla base di numerose altre strutture come ad esempio gli anelli, i campi e i moduli.
Uno degli obiettivi principali nello studio dei gruppi è quello di riuscire a classificarli tutti a meno di isomorfismi, in quanto due gruppi sono isomorfi quando sono dal punto di vista della struttura algebrica uguali. Al momento non si è ancora riusciti a classificare tutti i gruppi, tuttavia esistono diversi teoremi di struttura che permettono di descrivere alcune classi ristrette di gruppi ad esempio i gruppi finiti semplici che sono classificati dal cosiddetto *teorema enorme*. Altri esempi di classificazione sono dati dai teoremi di classificazione dei gruppi ciclici, dei gruppi abeliani finiti e dei gruppi abeliani finitamente generati. Questi ultimi sono l'oggetto di studio principale di questa tesi, che descriverà tutti e tre i teoremi di classificazione citati.
Per riuscire a provare tali teoremi di struttura è necessario fornire informazioni sui gruppi e su alcune loro caratteristiche. Abbiamo così diviso la tesi in due capitoli.

Il primo capitolo è incentrato su alcune nozioni preliminari. Inizialmente vengono presentate la struttura algebrica di un gruppo arbitrario e le nozioni di gruppo ciclico e prodotto diretto di gruppi. Sui gruppi ciclici, in particolare, viene mostrato il teorema di classificazione ad essi relativo e poi vengono

studiati i gruppi liberi e i gruppi abeliani liberi.

Il secondo capitolo presenta invece i teoremi di struttura dei gruppi abeliani finiti e dei gruppi abeliani finitamente generati. In entrambi i casi la dimostrazione viene suddivisa in passi intermedi, per rendere più agevole la trattazione dell'argomento. Così nel primo caso si procede prima scomponendo il gruppo nelle sue componenti primarie e poi scomponendo ogni componente primaria in gruppi ciclici. Nel secondo caso, invece, si mostra che il gruppo può essere decomposto come somma diretta di due parti, una finita e una libera, e poi ci si concentra sulla struttura di ciascuna di queste due componenti.

I tre teoremi di struttura presentati sono legati l'uno all'altro. I teoremi di classificazione dei gruppi abeliani finiti e finitamente generati si possono, infatti, dedurre l'uno dall'altro, ed entrambi fanno uso del teorema di classificazione dei gruppi ciclici.

Indice

Capitolo 1

Nozioni Preliminari

In questo capitolo verrano introdotte le nozioni preliminari sui gruppi, il concetto di gruppo libero ed alcune costruzioni fondamentali quali il prodotto e la somma diretta di gruppi.

1.1 Gruppi Ciclici e Gruppi Finitamente Generati

Cominciamo con il definire il concetto di gruppo, gruppo ciclico e gruppo finitamente generato, che si riveleranno fondamentali per gli argomenti trattati in questa tesi.

Definizione 1.1. Sia G un insieme non vuoto, dotato di un'operazione binaria. Si dice che G è un **gruppo** se:

(i) l'operazione è associativa: $a(bc) = (ab)c$, per ogni $a, b, c \in G$;

(ii) esiste un unico elemento $e \in G$, detto **elemento neutro** di G, tale che $ae = ea = a$ per ogni $a \in G$;

(iii) per ogni $a \in G$ esiste un elemento a^{-1} detto **elemento inverso** tale che $a^{-1}a = aa^{-1} = e$.

Un gruppo G si dice **abeliano** o **commutativo** se l'operazione è commutativa, ossia se vale $ab = ba$ per ogni $a, b \in G$.
Si definisce **ordine** di un gruppo G la sua cardinalità, denotata con $|G|$. Se $|G|$ è finita, allora si dice che G è **finito**, altrimenti si dice che G è **infinito**.

Definizione 1.2. Siano $(G, *)$ e $(H, \cdot)$ due gruppi. Una funzione $f : G \to H$ è detta **omomorfismo di gruppi** se:

$$f(a * b) = f(a)f(b) \quad \forall a, b \in G$$

$$f(e_G) = e_H$$

Se f è iniettiva allora si dice che f è un **monomorfismo**, se f è suriettiva **epimorfismo**, se f è biettiva **isomorfismo**. In quest'ultimo caso si dice che G e H sono **isomorfi** e si scrive $G \cong H$.

Definizione 1.3. Siano G e H gruppi e sia $f : G \to H$ un omomorfismo tra essi. Il **Kernel** della funzione f, denotato con $Kerf$ è:

$$Kerf := \{a \in G \mid f(a) = e_H\}.$$

Se A è un sottoinsieme di G, allora

$$f(A) = \{b \in H \mid b = f(a) \text{ per qualche } a \in A\}$$

è detto **immagine di** A. L'insieme $f(G)$ è detto **immagine di f** ed è denotato con Imf.

Riportiamo ora un teorema fondamentale sugli omomorfimsmi.

Teorema 1.1.1 (Primo Teorema di Isomorfismo)**.** *Sia $f : G \to H$ un omomorfismo di gruppi, allora f induce un isomorfismo $G/Kerf \cong Imf$.*

Dimostrazione. Vedi Teorema 5.7. pag. 44 [2] □

Passiamo ora alla nozione di gruppo ciclico.

Definizione 1.4. Fissato un elemento a di un gruppo G, definiamo il **sottogruppo ciclico generato da** a:

$$< a >:= \{a^n | n \in \mathbb{Z}\}$$

Si definisce **ordine** di $a \in G$ il più piccolo intero n tale che $a^n = e$. Si noti che $n = | < a > |$. Se tale n non esiste diremo che a ha **ordine infinito**. Se esiste un elemento $a \in G$ tale che $\langle a \rangle = G$ si dice che G è **gruppo ciclico generato da** a e che a è il **generatore** di G.

Definizione 1.5. Sia G un gruppo e sia X un sottoinsieme di G. Sia $\{H_i | \ i \in I\}$ la famiglia di tutti i sottogruppi di G che contengono X.
Allora

(*i*) $\bigcap_{i \in I} H_i$ è detto **sottogruppo di** G **generato da** X ed è denotato con $\langle X \rangle$. Tale sottogruppo è costituito da tutti i prodotti finiti della forma: $a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}$ con $a_j \in X, n_j \in \mathbb{Z}$ ed è il più piccolo sottogruppo di G contenente X.

(*ii*) Il gruppo G si dice **finitamente generato** se esiste un insieme finito $X = \{a_1, \dots, a_k\} \subseteq G$ tale che $\langle a_1, a_2, \dots, a_k \rangle = G$. In tal caso la cardinalità di X è detta **rango** del gruppo, e $a_1, a_2, \dots, a_k$ sono detti un **sistema di generatori per** G.

Osserviamo che esiste sempre un sottoinsieme X di G che genera G perchè al massimo posso prendere G stesso come sottinsieme. Inoltre osserviamo che $G = \{0\}$ se e solo se X è l'insieme vuoto perchè l'intersezione di tutti i sottogruppi di G che contengono il vuoto è $\{0\}$.
Si noti che se G è gruppo abeliano generato dagli elementi $a_1, a_2, \dots a_k$, allora un elemento a di G si può scrivere nella forma: $a = a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}$ con $n_j \in \mathbb{Z}$.

Mostriamo alcuni esempi di gruppi abeliani ciclici e di gruppi abeliani finitamente generati.

Esempio 1.1. 1. $(\mathbb{Z}, +)$ è un gruppo ciclico infinito con generatore 1. Infatti $m1 = m$ per ogni $m \in \mathbb{Z}$ quindi $\langle 1 \rangle = \mathbb{Z}$.

2. Il gruppo quoziente $(\mathbb{Z}/n\mathbb{Z}, +) = \{[0], [1], [2], \ldots, [n-1]\}$ è un gruppo commutativo finito con n elementi. Poiché ogni elemento di $\mathbb{Z}/n\mathbb{Z}$ si scrive come $[k] = [1] + ... + [1]$ (sommato k volte), $[1]$ è generatore del gruppo. Quindi $(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo ciclico.

3. $(\mathbb{Z}^2, +)$ è un gruppo abeliano finitamente generato, vale infatti: $\mathbb{Z}^2 =< (1,0), (0,1) >$ poichè ogni elemento (m, n) di $\mathbb{Z}^2$ si può scrivere nella forma: $(m, n) = m(1, 0) + n(0, 1)$.

Riportiamo ora alcuni risultati importanti sui gruppi ciclici che saranno utili in seguito.

Teorema 1.1.2. *Ogni sottogruppo H del gruppo addittivo $\mathbb{Z}$ è ciclico. Inoltre si ha o che $H = \{0\}$ o che $H =< m >$ dove m è il più piccolo intero positivo contenuto in H. Nel caso in cui H sia $\neq \{0\}$ allora H è infinito.*

Dimostrazione. Poichè H è un sottogruppo di $\mathbb{Z}$ si ha che $0 \in H$. Se $H = \{0\}$ allora H è il sottogruppo banale, altrimenti H contiene almeno un intero positivo n (e il suo opposto). Sia m il più piccolo intero positivo contenuto in H. Poichè ogni multiplo di m sta in H vale: $< m >= \{km \mid k \in \mathbb{Z}\} \subset H$. D'altra parte se $h \in H$ allora per l'algoritmo di divisione $h = qm + r$ con r e $q \in \mathbb{Z}$, $0 \leqslant r < m$. Da cui $r = h - qm \in H$ e poichè m è il più piccolo intero in H si ha necessariamente che $r = 0$ e $h = qm$. Da cui: $H \subset< m >$. Così $H =< m >= \{km \mid k \in \mathbb{Z}\}$ e chiaramente H è infinito. □

Il teorema seguente permette di classificare completamente i gruppi ciclici e per questo è di fondamentale importanza.

Teorema 1.1.3. *Ogni gruppo ciclico infinito è isomorfo al gruppo additivo $\mathbb{Z}$ e ogni gruppo ciclico finito di ordine n è isomorfo al gruppo additivo $\mathbb{Z}_n$.*

Dimostrazione. Sia G gruppo ciclico e sia a un suo generatore. Allora la funzione

$$f_a : \mathbb{Z} \to G \text{ definita da } f_a(k) = a^k$$

è suriettiva perchè G è generato da a ed è un omomorfismo per le proprietà delle potenze. Il suo nucleo è un sottogruppo di $\mathbb{Z}$ quindi per il teorema (1.1.2) è della forma $m\mathbb{Z}$ con $m \geq 0$. Per il Primo Teorema di Isomorfismo (1.1.1) si ha:

$$Imf = G = \mathbb{Z}/Kerf = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$$

Se $m > 0$ il quoziente $\mathbb{Z}/m\mathbb{Z}$ ha m elementi. Quindi se G è infinito necessariamente $m = 0$ e G è isomorfo a $\mathbb{Z}$. Se invece G è finito con n elementi, allora $m = n$ e G è isomorfo a $\mathbb{Z}_n$. □

Si noti che da questo teorema discende immediatamente che se un gruppo è ciclico allora è abeliano.

1.2 Prodotto e Somma Diretta di Gruppi

Introduciamo il prodotto esterno ed interno di gruppi.

Proposizione 1.2.1. *Siano $(G, \cdot)$ e $(H, *)$ due gruppi con elementi neutri e_G, e_H rispettivamente. Il prodotto cartesiano $G \times H$ con l'operazione definita da:*

$$(a, b)(a', b') = (a \cdot a', b * b') \text{ dove } a, a' \in G \text{ e } b, b' \in H$$

è un gruppo con elemento neutro (e_G, e_H) ed elemento inverso (a^{-1}, b^{-1}). Inoltre tale gruppo è abeliano se lo sono G e H.

Dimostrazione. Mostriamo che $G \times H$ è abeliano se e solo se lo sono G e H. $G \times H$ è abeliano se e solo se $\forall g_1, g_2 \in G, h_1, h_2 \in H$ si ha

$$(g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1) \Leftrightarrow (g_1 \cdot g_2, h_1 * h_2) = (g_2 \cdot g_1, h_2 * h_1),$$

ciò avviene se e solo se $\begin{cases} g_1 \cdot g_2 = g_2 \cdot g_1 \\ h_1 * h_2 = h_2 * h_1 \end{cases}$ cioè se e solo se G e H sono abeliani. □

Definizione 1.6. Il gruppo formato dal prodotto cartesiano di due gruppi G e H con l'operazione definita nella proposizione è detto **prodotto diretto (esterno) di G e H** e si denota con $G \times H$. Nel caso di gruppi abeliani, il gruppo così definito viene detto **somma diretta esterna** e si denota con: $G \oplus H$.

La definizione precedente si può generalizzare al prodotto diretto (rispettivamente somma diretta) di un numero finito o infinito di gruppi.

Definizione 1.7. Dato un insieme di indici I e una famiglia di insiemi $\{A_i\}_{i\in I}$ si definisce il **prodotto cartesiano** degli A_i, l'insieme:

$$\prod_{i\in I} A_i := \left\{ f : I \to \bigcup_{i\in I} A_i \mid f(i) \in A_i \right\}$$

Se I è finito con $|I| = n$ con $n \in N^*$, identificando gli elementi di $\prod_{i\in I} A_i$ con le loro immagini, si ottiene la nozione classica di $\prod_{i\in I} A_i$ di un numero finito di insiemi, ossia:

$$\prod_{i\in I} A_i := \{(a_i, \ldots, a_n) \mid a_i \in A_i\}$$

Definizione 1.8. Sia $\{G_i\}_{i\in I}$ una famiglia di gruppi non necessariamente finita. Si dice **prodotto diretto esterno** della famiglia, denotato con $\prod_{i\in I} G_i$, il prodotto cartesiano dei G_i dotato della seguente operazione. Dati due elementi $f, g \in \prod_{i\in I} G_i$, ossia due funzioni $f, g : I \to \bigcup_{i\in I} G_i$ con $f(i), g(i) \in G_i \ \forall i$, il prodotto di f e g è la funzione

$$fg : I \to \bigcup_{i\in I} G_i \ \text{ definita da } \ (fg)(i) = f(i)g(i) \ \ \forall i \in I.$$

Nel caso in cui $|I|$ sia finito allora l'operazione binaria su $\prod_{i\in I} G_i$ è la moltiplicazione componente per componente. Dati due elementi $a = \{a_i\}$, $b = \{b_i\}$ si pone:

$$ab = \{a_i\}\{b_i\} = \{a_i \cdot b_i\},$$

dove il prodotto in parentesi è l'operazione di G_i. Nel caso di notazione additiva si parla di **somma diretta esterna** della famiglia di gruppi $\{G_i\}_{i\in I}$ e si denota con $\bigoplus G_i$.

Definizione 1.9. Il **prodotto esterno debole** di una famiglia di gruppi $\{G_i\}_{i\in I}$, denotato con $\prod_{i\in I}^{w} G_i$ è l'insieme di tutte le funzioni $f \in \prod_{i\in I} G_i$ tali che $f(i) = e_i$ (con e_i identità in G_i) eccetto per un numero finito di indici $i \in I$.

Osservazione 1.1. Se I è finito il prodotto diretto esterno debole coincide con il prodotto diretto esterno. In ogni caso si ha:

(*i*) prodotto esterno debole $\prod_{i\in I}^{w} G_i$ è un sottogruppo normale di $\prod_{i\in I} G_i$;

(*ii*) Per ogni $k \in I$ la mappa detta iniezione canonica:
$j_k : G_k \to \prod_{i\in I} G_i$ tale che $j_k(a) = \{a_i\}_{i\in I}$ con $\begin{cases} a_i = e & \text{per } i \neq k \\ a_k = a & \text{per } k = i \end{cases}$
è un monomorfismo di gruppi;

(*iii*) $\forall\ i \in I$, $j_i(G_i)$ è un sottogruppo normale di $\prod_{i\in I} G_i$.

Teorema 1.2.2. *Sia $\{N_i \mid i \in I\}$ una famiglia di sottogruppi normali di un gruppo G tali che:*

(*i*) $G = \langle \bigcup_{i\in I} N_i \rangle$;

(*ii*) *per ogni* $k \in I$ $N_k \cap \langle \bigcup_{i\neq k} N_i \rangle = \langle e \rangle$.

Allora $G \cong \prod_{i\in I}^{w} N_i$.

Dimostrazione. Vedi Teorema 8.6. pag. 61 [2]. □

Osserviamo che nel caso in cui I sia finito, dati $N_1, N_2, \ldots, N_r$ sottogruppi normali di G vale $\langle N_1 \cup N_2 \ldots \cup N_r \rangle \cong N_1 \times N_2 \times \ldots \times N_r$, o nel caso abeliano $\langle N_1 \cup N_2 \ldots \cup N_r \rangle \cong N_1 \oplus N_2 \oplus \ldots \oplus N_r$, poichè prodotto esterno debole e prodotto esterno coincidono.

Definiamo, ora, il prodotto e la somma diretti interni.

Definizione 1.10. Sia G un gruppo e sia $\{N_i \mid i \in I\}$ una famiglia di sottogruppi normali di G tali che:

$$G = \langle \bigcup_{i \in I} N_i \rangle \qquad \text{e} \qquad N_k \cap \langle \bigcup_{i \neq k} N_i \rangle = \langle e \rangle \quad \forall k \in I,$$

G si dice **prodotto interno debole** della famiglia $\{N_i \mid i \in I\}$.
Se G è abeliano si dice che G è **somma diretta interna**.

Si osservi che c'è distinzione tra prodotto interno ed esterno. Se un gruppo G è il prodotto interno di una famiglia di gruppi N_i, allora dalla definizione segue immediatamente che gli N_i sono sottogruppi di G e che G è isomorfo al prodotto esterno debole di tali N_i per il teorema (1.2.2).

Osservazione 1.2. Sia G un gruppo e sia $\{N_i \mid i = 1, \ldots, n\}$ una famiglia di sottogruppi normali di G. Se G è somma diretta interna degli N_i vale:
dati $a_1 \in N_1, \ldots, a_n \in N_n$ e $m_1, \ldots, m_s$ interi maggiori o uguali a 0, allora

$$m_1 a_1 + m_2 a_2 + \ldots + m_s a_s = 0 \;\Rightarrow\; m_1, m_2, \ldots, m_s = 0$$

Dimostrazione. Se per assurdo uno degli scalari m_i fosse $\neq 0$, sia per esempio $m_1 \neq 0$, si avrebbe:

$$a_1 = \sum_{i=2}^{n} \frac{m_i}{m_1} a_i$$

per cui $a_1 \in N_1$ e $a_1 \in \sum_{i=2}^{n} N_i$. Allora $N_1 \cap \sum_{i=2}^{n} N_i \neq \{0\}$ e la somma non sarebbe diretta. □

Teorema 1.2.3. *Siano $\{G_i \mid i \in I\}$ e $\{H_i \mid i \in I\}$ famiglie di gruppi. Sia $\{f_i : G_i \to H_i \mid i \in I\}$ una famiglia di omomorfismi di gruppi e sia $f = \prod f_i$ la mappa tale che:*

$$f : \prod_{i \in I} G_i \to \prod_{i \in I} H_i \qquad \{a_i\} \mapsto \{f_i(a_i)\}.$$

Allora f è un omomorfismo di gruppi tale che:

$$f(\prod_{i \in I} G_i) \subset \prod_{i \in I} H_i, \quad Ker f = \prod_{i \in I} Ker f_i, \quad Im f = \prod_{i \in I} Im f_i.$$

Di conseguenza si ha anche che f è un monomorfismo (epimorfismo o isomorfismo) se e solo se lo è ogni f_i.

Dimostrazione. Si ha che f è un omomorfismo perchè lo è ogni f_i, infatti dati $a = \{a_i\}$, $b = \{b_i\} \in \prod_{i\in I} G_i$ si ha: $f(ab) = f(\{a_i\}\{b_i\}) = f(\{a_ib_i\}) = \{f_i(a_ib_i)\} = \{f_i(a_i)f_i(b_i)\} = \{f_i(a_i)\}\{f_i(b_i)\} = f(a)f(b)$, inoltre $f(e_G) = f(\{e_{G_i}\}) = \{f_i(e_{Gi})\} = \{e_{H_i}\} = e_H$. □

Corollario 1.2.4. *Siano $\{G_i \mid i \in I\}$ e $\{N_i \mid i \in I\}$ famiglie di gruppi tali che N_i sia un sottogruppo normale di G_i per ogni $i \in I$. Allora*

(*i*) *$\prod_{i\in I} N_i$ è un sottogruppo normale di $\prod_{i\in I} G_i$ e $\prod_{i\in I} G_i/\prod_{i\in I} N_i \cong \prod_{i\in I} G_i/N_i$;*

(*ii*) *$\prod^w_{i\in I} N_i$ è un sottogruppo normale di $\prod^w_{i\in I} G_i$ e $\prod^w_{i\in I} G_i/\prod^w_{i\in I} N_i \cong \prod^w_{i\in I} G_i/N_i$.*

Dimostrazione. Proviamo soltanto (i) perchè (ii) si prova poi analogamente. Per ogni $i \in I$ sia $\pi_i : G_i \to G_i/N_i$ l'epimorfismo canonico. Per il teorema (1.2.3) la mappa $\prod \pi_i : \prod_{i\in I} G_i \to \prod_{i\in I} G_i/\prod_{i\in I} N_i$ è un epimorfismo con kernel $\prod_{i\in I} N_i$. Pertanto per il Primo Teorema di Isomorfismo (1.1.1) si ha che $\prod_{i\in I} G_i/\prod_{i\in I} N_i \cong \prod_{i\in I} G_i/N_i$. □

1.3 Gruppi Liberi

In questa sezione diamo una definizione formale di gruppo libero e ciò ci permetterà di descrivere un gruppi in termini di "generatori e relazioni".

Definizione 1.11. Sia $X \neq \varnothing$ un **alfabeto** cioè un insieme arbitrario (finito o infinito) di simboli. Ad ogni elemento x in X associamo un elemento x^{-1} che chiameremo inverso di x e definiamo X^{-1} l'insieme di tali inversi. Definiamo:

$$X' := X \cup X^{-1} \cup \{1\} = \{1, a, a^{-1}, b, b^{-1}, \ldots\}.$$

Una **parola su** X' è una qualunque sequenza infinita di simboli di X' in cui sono ammesse ripetizioni e che da un certo punto in poi è uguale a 1:

$$a_1a_2a_3\ldots \qquad \text{dove } a_i \in X' \text{ e per un certo } n \in \mathbb{N}^*,\ a_i = 1,\ \forall i \geq n.$$

Ad esempio $abc1bd111\ldots$, $aabbc111\ldots$, $ab^{-1}cc^{-1}111\ldots$ sono parole in X'.
D'ora in avanti denoteremo con W l'insieme di tutte le parole possibili su X'
Si definisce **parola vuota** la sequenza costante $111\ldots$ che viene denotata con 1.

Diremo che un elemento x e il suo inverso x^{-1} **si cancellano** se sono adiacenti. In tal caso sostituiremo xx^{-1} (o $x^{-1}x$) con 1.
Una parola si dice **ridotta** se:

(i) non è possibile fare cancellazioni tra i simboli della parola:
$\forall x \in X, x$ e x^{-1} non sono adiacenti, ossia da $a_i = x$ segue $a_{i+1} \neq x^{-1}$ e da $a_i = x^{-1}$ segue $a_{i+1} \neq x\ \forall\ i \in \mathbb{N}^*$, $x \in X$;

(ii) il simbolo 1 compare solo alla fine:
$a_k = 1$ per un certo $k \in \mathbb{N}^*$ implica che $a_i = 1\ \forall\ i \geq k$.

Dalla definizione segue che ogni parola ridotta è della forma:
$x_1^{\lambda_1}x_2^{\lambda_2}\ldots x_n^{\lambda_n}11\ldots$ dove $n \in \mathbb{N}^*$, $x_i \in X$ e $\lambda_i = \pm 1$ con la condizione: se $x_i = x_{i+1}$ allora $\lambda_i = \lambda_{i+1}$.
D'ora in avanti denoteremo le parole ridotte con $x_1^{\lambda_1}x_2^{\lambda_2}\ldots x_n^{\lambda_n}$, e con F l'insieme delle parole ridotte. Si noti che la parola vuota è ridotta.

Osserviamo che nonostante sia possibile operare le cancellazioni in ordine differente a partire da una parola w si ottiene sempre la stessa parola ridotta w_0. Esiste cioè un'unica forma ridotta w_0 di una parola assegnata w. Ad esempio, la parola $w = x_1^1x_2^{-1}x_3^1x_3^{-1}x_2^{-1}x_2^1$ posso ridurla in maniere diverse: cancellando prima $x_3^1x_3^{-1}$ ottenendo $x_1^1x_2^{-1}x_2^{-1}x_2^1$ e poi $x_2^{-1}x_2^1$ o $x_2^1x_2^{-1}$ ottendendo infine $w_0 = x_1^1x_2^{-1}$ oppure cancellando prima $x_2^1x_2^{-1}$ e poi $x_3^1x_3^{-1}$ ottenendo come prima $w_0 = x_1^1x_2^{-1}$.

Definiamo una funzione $r : W \to F$ che associ ad ogni parola la sua forma ridotta. Tale funzione opera in modo che ogni coppia di inversi adiacenti venga eliminata, e sposta gli 1 dopo tutti gli altri elementi.

Definiamo su F un'operazione binaria $\star : F \times F \to F$ mediante giustapposizione:

$$((x_1^{\lambda_1} x_2^{\lambda_2} \dots x_m^{\lambda_m}), (y_1^{\delta_1} y_2^{\delta_2} \dots y_n^{\delta_n})) \mapsto r(x_1^{\lambda_1} x_2^{\lambda_2} \dots x_n^{\lambda_n} y_1^{\delta_1} y_2^{\delta_2} \dots y_n^{\delta_n}).$$

Osserviamo che la parola che si ottiene per giustapposizione non è detto che sia ridotta, per questo applichiamo la funzione di riduzione r.

Teorema 1.3.1. *L'insieme F delle parole ridotte dotato dell'operazione binaria $\star$ definita sopra è un gruppo in cui l'elemento neutro è la parola vuota.*

Dimostrazione. Vedi Teorema 9.1 pag. 65 [2]. □

Definizione 1.12. Il gruppo F delle parole ridotte sull'alfabeto X' è detto **gruppo libero** sull'insieme X.

Vediamo alcune osservazioni utili in seguito.

Osservazione 1.3. Osserviamo che:

(*i*) L'insieme X può essere considerato un sottoinsieme di F mediante l'inclusione: $X \to F$ definita da $x \mapsto (x, 1, 1, 1, \dots)$. E' facile vedere che X genera F nel senso della definizione data di insieme di generatori per un gruppo.

(*ii*) Se $|X| \geq 2$ allora il gruppo libero su X non è abeliano (dati $x, y \in X$ con $x \neq y$ si ha che la parola $x^{-1}y^{-1}xy$ è ridotta, quindi $x^{-1}y^{-1}xy \neq 1$ e così $xy \neq yx$).

(*iii*) Ogni elemento eccetto 1 in un gruppo libero ha ordine infinito.

(*iv*) Se $X = \{a\}$ allora il gruppo libero su X è il gruppo ciclico infinito $< a >$.

(v) I sottogruppi di gruppi liberi sono anch'essi liberi.

Teorema 1.3.2. *Sia F il gruppo libero sull'insieme X e sia $i : X \hookrightarrow F$ la mappa inclusione. Se G è un gruppo e $f : X \to G$ allora esiste un unico omomorfismo di gruppi $\bar{f} : F \to G$ tale che $\bar{f} \circ i = f$.*

Dimostrazione. Data $w = x_1^{\lambda_1} \dots x_n^{\lambda_n}$ parola ridotta in X, definiamo $\bar{f}$ nel modo seguente:

$$\bar{f}(1) = e, \quad \bar{f}(x_1^{\lambda_1} \dots x_n^{\lambda_n}) = f(x_1)^{\lambda_1} f(x_2)^{\lambda_2} \dots f(x_n)^{\lambda_n}.$$

Poichè G è gruppo e $\lambda_i = \pm 1$ il prodotto $f(x_1)^{\lambda_1} f(x_2)^{\lambda_2} \dots f(x_n)^{\lambda_n}$ è un elemento ben definito di G. Quindi per come è definita $\bar{f}$ è omomorfismo tale che $\bar{f} \circ i = f$. $\bar{f}$ è unico, infatti se $g : F \to G$ è un omomorfismo tale che $g \circ i = f$ allora: $g(x_1^{\lambda_1} \dots x_n^{\lambda_n}) = g(x_1^{\lambda_1}) \dots g(x_n^{\lambda_n}) = g(x_1)^{\lambda_1} \dots g(x_n)^{\lambda_n} = g \circ i(x_1)^{\lambda_1} \dots g \circ i(x_n)^{\lambda_n} = f(x_1)^{\lambda_1} f(x_2)^{\lambda_2} \dots f(x_n)^{\lambda_n} = \bar{f}(x_1^{\lambda_1} \dots x_n^{\lambda_n})$. □

Corollario 1.3.3. *Ogni gruppo G è l'immagine di un gruppo libero attraverso un omomorfismo di gruppi.*

Dimostrazione. Sia X un insieme di generatori di G e si consideri F gruppo libero sull'insieme X. Sia $i : X \to G$, l'inclusione per il teorema (1.3.2) si ha che questa induce un omomorfismo $\bar{f} : F \to G$ tale che $x \mapsto x \in G$. Poichè $G = \langle X \rangle$ allora $\bar{f}$ è un epimorfismo, infatti, fissato $a \in G$ vale: $a = x_1^{\lambda_1} \dots x_n^{\lambda_n}$ con $\lambda_i = \pm 1$ e quindi $x_i^{\lambda_i} \in X$, e, per come è costruita $\bar{f}$ segue che $\bar{f} = (x_1^{\lambda_1} \dots x_n^{\lambda_n}) = a$. □

Corollario 1.3.4. *Siano F ed F' gruppi liberi rispettivamente sugli insiemi X e X' con $|X| = |X'|$. Allora $F \cong F'$.*

Dimostrazione. Poichè $|X| = |X'|$ c'è una biezione $f : X \to X'$. Siano $i : X \hookrightarrow F$ e $j : X' \hookrightarrow F'$ le inclusioni. Poichè F è libero per il teorema (1.3.2) esiste un omomorfismo di gruppi $\phi : F \to F'$ che rende comutativo il diagramma:

$$\begin{array}{ccc} X & \xrightarrow{f} & X' \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} \\ F & \xrightarrow[\phi]{} & F' \end{array}$$

Analogamente, poichè la biezione f ha un'inversa $f^{-1} : X' \to X$ e F' è libero esiste un omomorfismo di gruppi $\psi : F' \to F$ tale che:

$$\begin{array}{ccc} X & \xleftarrow{f^{-1}} & X' \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle j} \\ F & \xrightarrow[\psi]{} & F' \end{array}$$

Da questi due diagrammi si ottengono le seguenti relazioni:

$$j \circ f = \phi \circ i$$
$$\psi \circ j = i \circ f^{-1}$$

Da cui:

$$\psi \circ \phi \circ i = \psi \circ j \circ f = i \circ f^{-1} \circ f = i$$
$$\phi \circ \psi \circ j = \phi \circ i \circ f^{-1} = j \circ f \circ f^{-1} = j.$$

D'altra parte dal teorema (1.3.2) considerando $i : X \to F$ esiste un unico omomorfismo $1_F : F \to F$ tale che $i_F \circ i = i$ per cui si ha $\psi \circ \phi = 1_F$. Analogamente si prova che $\phi \circ \psi = 1_{F'}$. Così poichè ϕ è una funzione biettiva la cui inversa è ψ ed è un omomorfismo per quanto detto sopra, si conclude che F è isomorfo a F'. □

Sia G un gruppo $G = \langle X \rangle$. Sia F il gruppo libero su X e sia $f : X \to G$ una mappa che induce l'omomorfismo $\bar{f} : F \to G$ del teorema (1.3.2). Dalla dimostrazione del corollario (1.3.3) segue che $\bar{f}$ è un epimorfismo poichè $G =< X >$. Allora per il Primo Teorema di Isomorfismo $G \simeq F/Ker\bar{f}$.
Supponiamo ora che $w = x_1^{\lambda_1} \dots x_n^{\lambda_n} \in F$ sia un generatore di $Ker\bar{f}$. L' epimorfismo $\bar{f}$ manderà: $w \mapsto x_1^{\lambda_1} \dots x_n^{\lambda_n} = e_G$. L'equazione $x_1^{\lambda_1} \dots x_n^{\lambda_n} = e_G$ è detta **relazione** sui generatori x_i.

Sia ora X un insieme di generatori di G e Y un sottoinsieme di parole ridotte sull'insieme X. Il gruppo G può essere descritto a partire dall'insieme dei generatori X e dalle relazioni: $w = e_G$ con $w \in Y$.
Sia F il gruppo libero su X e N il sottogruppo normale di F generato da Y

(si può definire il sottogruppo normale di F generato da Y come l'intersezione di tutti i sottogruppi normali di F che contengono Y), questo è il più piccolo sottogruppo normale di F che contiene Y, quindi è ben definita la struttura di gruppo sul quoziente F/N. Sia $G = F/N$ allora G è il gruppo generato da X che soddisfa tutte le relazioni $w = e_G$ con $w \in Y$.

Un gruppo G può essere completamente descritto a partire dall'insieme dei suoi generatori X e dall'insieme R delle relazioni tra questi generatori. Questa descrizione non è unica in quanto sono possibili diverse scelte sia di X che di R. Diamo una definizione formale di quanto abbiamo detto fino ad ora.

Definizione 1.13. Sia X un insieme e Y un sottoinsieme di ridotte parole di X. Un gruppo G è detto **gruppo definito dai generatori** $x \in X$ **e dalle relazioni** $w = e$ $(w \in Y)$ se $G \simeq F/N$ dove F è il gruppo libero su X e N il sottogruppo normale di F generato da Y. In questo caso si dice anche che $(X|Y)$ è una **presentazione di** G.
Se l'insieme delle relazioni tra i generatori è finito si dice che G è **finitamente presentato**.

Poichè li tratteremo anche nel seguito, vediamo come esempio il caso dei gruppi abeliani.

Esempio 1.2. Nell'osservazione (1.3) abbiamo visto che se $|X| \geq 2$ il gruppo libero costruito su un insieme X di generatori non commuta.
Consideriamo il gruppo generato da due elementi x, y, cioè $X = \{x, y\}$, tra i quali intercorre le relazione: $xyx^{-1}y^{-1} = 1$, cioè $R = \{xyx^{-1}y^{-1} = 1\}$, otteniamo un gruppo i cui generatori x e y commutano tra loro. Sia ora F il gruppo libero generato da x e y e sia N il sottogruppo normale di F generato dal loro commutatore $xyx^{-1}y^{-1}$. Dimostriamo che il gruppo quoziente $G = F/N$ cioè il gruppo generato da x e y con relazione R è abeliano.
Indichiamo le classi $xN = \overline{x}$ e $yN = \overline{y}$. Poichè il commutatore appartiene ad N gli elementi $\overline{x}, \overline{y}$ commutano in F/N, allora $\overline{yx}\overline{y^{-1}} = \overline{xy}\overline{y^{-1}} = \overline{x}$. E questo

implica che: $\overline{x}\overline{y^{-1}} = \overline{y^{-1}}\overline{x}$ ossia $\overline{x}$ commuta anche con $\overline{y^{-1}}$. Poichè $\overline{x}$ commuta ovviamente anche con se stesso e il suo inverso, si ha che $\overline{x}$ commuta con qualsiasi parola in $W = \{\overline{x}, \overline{y}, \overline{x^{-1}y^{-1}}\}$ e così anche $\overline{y}$. Segue per induzione che due qualsiasi parole in W commutano tra loro (sono formate da elementi che commutano tra loro). Inoltre poichè $\overline{x}$ e $\overline{y}$ generano il gruppo F/N si ha che tale gruppo è abeliano. Il gruppo $G = F/N$ appena costruito è detto **gruppo abeliano libero su due elementi**. I suoi elementi non soddisfano altra relazione che quelle derivanti dagli assiomi di gruppo e della proprietà commutativa.
In generale per costruire un gruppo abeliano libero su n elementi, bisogna imporre la commutatività sugli n elementi $x_1, x_2, \ldots, x_n$ che generano il gruppo libero F e quozientare F con il sottogruppo normale generato da tutti i commutatori dei generatori, cioè:

$$X =< x_1, x_2, \ldots, x_n > \text{ e } R = \{x_i x_j x_i^{-1} x_j^{-1} \mid i, j = 1, \ldots, n; i \neq j\}$$

1.4 Gruppi Abeliani Liberi

Nel seguito usiamo principalmente la notazione additiva in quanto più usuale per i gruppi abeliani che trattiamo nella tesi. Così:

(i) l'operazione binaria viene indicata con $+$;

(ii) l'elemento neutro con 0;

(iii) l'unico elemento inverso di a viene espresso con $-a$;

(iv) l'elevamento a potenza con $na = \underbrace{a + a + \ldots + a}_{n\text{volte}}$;

Osservazione 1.4. Si noti che conseguentemente si ha:

(i) il sottogruppo generato da un elemento è $\langle a \rangle = \{na \mid n \in \mathbb{Z}\}$

(*ii*) il sottogruppo generato da $X = \{a_1, a_2, \ldots, a_k\}$ consiste in tutte le combinazioni lineari degli elementi di X:

$$\langle a_1, a_2, \ldots, a_k \rangle = \Big\{ \sum_{j=1}^{k} n_j a_j \text{ con } n_j \in \mathbb{Z} \Big\}.$$

Definizione 1.14. Sia G è un gruppo abeliano e siano $a_1, a_2, \ldots, a_k$ un sistema di generatori per G. Se vale:

$$n_1 a_1 + n_2 a_2 + \ldots + n_k a_k = 0 \Rightarrow n_i = 0 \forall i = 1 \ldots k$$

allora $X = \{a_1, a_2, \ldots, a_k\}$ è una **base** di G.
La cardinalità di una base di G è detta **rango** di G.

Definizione 1.15. I gruppi abeliani che ammettono una base sono detti **gruppi abeliani liberi**

Teorema 1.4.1 (Caratterizzazione dei Gruppi Liberi)**.** *Sia F un gruppo abeliano. Sono equivalenti le seguenti affermazioni:*

(*i*) *F ammette una base;*

(*ii*) *F è somma diretta (interna) di una famiglia di sottogruppi ciclici infiniti;*

(*iii*) *F è isomorfo alla somma diretta di copie del gruppo additivo $\mathbb{Z}$ degli interi;*

(*iv*) *Esistono un insieme non vuoto X e una funzione $i : X \to F$ con la seguente proprietà:*
Dato un gruppo abeliano H ed una funzione $f : X \to H$ esiste un unico omomorfismo di gruppi $\bar{f} : F \to H$ tale che $\bar{f} i = f$.

Dimostrazione. (*i*) $\Rightarrow$ (*ii*) Se X è una base di F allora $\forall x \in X\ nx = 0 \Leftrightarrow n = 0$. Perciò ogni sottogruppo $< x >$ è ciclico infinito e abeliano (quest'ultimo perchè F è abeliano). Inoltre dato che $F =< X >$ abbiamo anche che $F = \langle \bigcup_{x \in X} < x > \rangle$. Ora, per assurdo, se esiste $z \in X$ tale che $< z >$

$\cap\langle\bigcup_{x\in X,x\neq z} < x >\rangle \neq 0$, allora esiste $n \neq 0 \in \mathbb{Z}$ tale che: $nz = n_1x_1 + n_2x_2 + \ldots + n_kx_k$ con $z, x_1, \ldots, x_k$ elementi distinti di X e questo contraddice il fatto che X sia una base per F. Così $< z > \cap\langle\bigcup_{x\in X,x\neq z} < x >\rangle = 0$, e quindi per la definizione data: $F = \sum_{x\in X} < x >$.
$(ii) \Rightarrow (iii)$ Per ipotesi: $F = \sum_{x\in X} < x >$ con $< x >$ sottogruppi ciclici infiniti. Per il teorema di classificazione di gruppi ciclici (1.1.3) ogni $< x >$ è isomorfo al gruppo additivo $\mathbb{Z}$. Per la definizione data di somma diretta interna vale inoltre: $\forall k \in I < x > \cap\langle\sum_{i\neq k} < x_i >\rangle = 0$. Così per i teoremi (1.2.2), (1.2.3) si ha: $F \cong \bigoplus_{i\in I} < x_i >$ con $< x_i > \cong \mathbb{Z}\ \forall\ i \in I$.
$(iii) \Rightarrow (i)$ Supponiamo $F \cong \sum \mathbb{Z}$ e che le copie di $\mathbb{Z}$ siano indicizzate da un insieme X. Per ogni $x \in X$ sia θ_x l'elemento $\{u_i\}$ di $\sum \mathbb{Z}$ dove $u_i = 0$ per $i \neq x$ e $u_x = 1$. L'insieme $\{\theta_x | x \in X\}$ è una base di $\sum \mathbb{Z}$ e poichè vale $F \cong \sum \mathbb{Z}$ considerando l'isomorfismo inverso a questo si ottiene una base di F.
$(i) \Rightarrow (iv)$ Sia $X = \{x_1, x_2, \ldots, x_k\}$ una base di F e sia $i : X \hookrightarrow F$ la mappa inclusione. Supponiamo esista $f : X \to G$ tale che $x_k \mapsto f(x_k)$. Definiamo $\bar{f} : F \to G$ nel modo seguente: $\bar{f}(1) = e$, $\bar{f}(n_1x_1 \ldots n_kx_k) = n_1f(x_1) \ldots n_kf(x_k)$. Se $\bar{f}$ è ben definita è ovviamente un omomorfismo ed è tale che $\bar{f} = if$. Proviamo che è ben definita: se $u \in F$ allora poichè X è insieme di generatori si ha $u = n_1x_1 + n_2x_2 + \ldots + n_kx_k (n_i \in \mathbb{Z}), x_i \in X)$. Se $u = m_1x_1 + m_2x_2 + \ldots + m_kx_k, (m_k \in \mathbb{Z})$ allora per definizione di base vale: $\sum_{i=1}^{k}(n_i - m_i) = 0 \Rightarrow n_i = m_i\ \forall i$. Quindi la funzione $\bar{f}$ è ben definita. Proviamo che $\bar{f}$ è unica. Sia $g : F \to G$ un omomorfismo tale che $gi = f$, allora per ogni $x \in X g(x) = g(i(x)) = f(x) = \bar{f}(x)$. Così $\bar{f}$ è unica.
$(iv) \Rightarrow (iii)$ Dato un insieme X e la mappa inclusione $i : X \to F$ si deve costruire una somma diretta di copie di $\mathbb{Z}$ indicizzate da X. Sia $Y = \{\theta_x |\ x \in X\}$ una base di $\sum \mathbb{Z}$ come nella prova di $(iii) \Rightarrow (i)$. Allora poichè abbiamo visto che $(iii) \Rightarrow (i) \Rightarrow (iv)$ sia ha che vale l'affermazione (iv) per $\sum \mathbb{Z}$. Poichè $|X| = |Y|$ allora l'enunciato è vero per il corollario (1.3.4). □

Osservazione 1.5. Si noti che dal punto (iii) di questo teorema di caratterizzazione dei gruppi abeliani liberi, segue che se F è un gruppo abeliano libero

finitamente generato di rango r allora:

$$F \cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{r \text{ volte}} = \mathbb{Z}^r \tag{1.1}$$

Teorema 1.4.2. *Sia G un gruppo abeliano finitamente generato e sia X l'insieme dei suoi generatori. Allora G è l'immagine attraverso un omomorfismo di un gruppo abeliano libero F di rango $|X|$.*

Dimostrazione. Sia F il gruppo abeliano libero sull'insieme X. Allora $F = \sum_{x \in X} \mathbb{Z}x$ e il rango di $F = |X|$. Per il teorema (1.4.1) la mappa inclusione $X \to G$ induce un omomorfismo $\bar{f} : F \to G$ tale che $1x \mapsto x \in G$, quindi $X \subset Im\bar{f}$. Per cui da X genera G abbiamo che $Im\bar{f} = G$. □

Lemma 1.4.3. *Sia G gruppo abeliano, m un intero e $\{G_i\}_{i \in I}$ una famiglia di gruppi abeliani. Allora:*

(*i*) *$mG = \{mu \mid u \in G\}$ è un sottogruppo di G;*

(*ii*) *se $g : G \to \sum_{i \in I} G_i$ è un isomorfismo, allora la restrizione di G a mG è ancora un' isomorfismo: $mG \cong \sum_{i \in I} mG_i$.*

Dimostrazione. (*i*) Per provare che mG è un sottogruppo bisogna provare che è chiuso rispetto allo 0, all'opposto, e alla somma di due elementi. Ma: $0 \in mG$, infatti: $0 \in G \Rightarrow m0 = 0 \in mG$; se x in mG allora $x = mu$ con $u \in G$ e poichè G è gruppo esiste $-u \in G \Rightarrow -x = -mu = m(-u) \in mG$; infine dati $x, y \in mG \Rightarrow x = mu$ con $u \in G$, $y = mv$ con $v \in G \Rightarrow x + y = mu + mv = m(u + v) conu + v$ in G perchè gruppo $\Rightarrow x + y \in mG$.

(*ii*) se $g : G \to \sum_{i \in I} G_i$ è l'isomorfismo definito da $x \mapsto g(x)$ allora si può considerare l'isomorfismo $mx \mapsto g(mx)$.

□

Teorema 1.4.4. *Sia F un gruppo abeliano libero. Due qualsiasi basi di F hanno la stessa cardinalità.*

Dimostrazione. Supponiamo che F abbia un numero finito di elementi e che S sia una base di F con cardinalità finita tale che $|S| = m$. Sia T un'altra base di F e supponiamo che T abbia almeno r elementi: $|T| \geq r$. E' sufficiente provare che $r \leq m$ poichè per simmetria dopo si prova analogamente che $r \geq m$. Sia p un numero primo. Dal teorema (1.4.1) sappiamo che

$$F \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$$

con m addendi. Per ogni sottogruppo G di F si ha per il lemma (1.4) che $pG := \{pu \mid u \in G\}$ è sottogruppo di G e che $F \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ induce un isomorfismo $pF \cong p\mathbb{Z} \oplus \ldots \oplus p\mathbb{Z}$. Così vale:

$$F/pF \cong \mathbb{Z}/p\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p.$$

Allora

$$|F/pF| = p^m.$$

Usando la base T al posto della base S si trova analogamente che $|F/pF| \geq p^r$. Mettendo insieme i due risultati si ha allora che $p^r \leq p^m$ e quindi che $r \leq m$. Se F ha una base infinita allora tutte le basi sono infinite. Se per assurdo ne esistesse una finita di cardinalità m allora, per quanto appena dimostrato, ogni altra base avrebbe cardinalità m. □

Osserviamo che per il teorema (1.4.4) il rango di un gruppo abeliano libero F è un invariante di F.

Proposizione 1.4.5. *Siano F_1 e F_2 due gruppi abeliani liberi con basi X_1, X_2 rispettivamente. Allora $F_1 \cong F_2$ se e solo se F_1 e F_2 hanno lo stesso rango (ossia $|X_1| = |X_2|$).*

Dimostrazione. Supponiamo $F_1 \cong F_2$. Sia $f : F_1 \to F_2$ l'isomorfismo tra essi, allora $f(X_1)$ è base di F_2 per cui vale: $|X_1| = |f(X_1)| = |X_2|$ pochè per il teorema (1.4.4) due basi di uno stesso gruppo abeliano libero hanno stessa cardinalità. L'implicazione inversa è dimostrata dal corollario (1.3.4). □

Lemma 1.4.6. *Sia F un gruppo abeliano libero. Sia $\{x_1, \ldots, x_n\}$ una base di F, e $a \in \mathbb{Z}$. Allora per ogni $i \neq j$ si ha che anche $\{x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n\}$ è una base di F.*

Dimostrazione. Poichè $x_j = -ax_i + (x_j + ax_i)$ segue che

$$F =< x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n > .$$

Se $k_1x_1 + \ldots + k_j(x_j + ax_i) + \ldots + k_nx_n = 0$ con $k_i \in \mathbb{Z}$. Allora $k_1x_1 + \ldots + (k_i + k_ja)x_i + \ldots + k_jx_j + \ldots k_nx_n = 0$ che implica: $k_t = 0$ per tutti i t. □

Teorema 1.4.7. *Sia F gruppo abeliano libero di rango finito n e sia G un sottogruppo non banale di F. Allora esistono una base $x_1, \ldots, x_n$ di F, un intero r tale che $1 \leq r \leq n$ e una lista di interi positivi $d_1, \ldots, d_r$ tali che $d_1|d_2| \ldots |d_r$ e G è gruppo abeliano libero con base $d_1, \ldots, d_rx_r$*

Dimostrazione. Se $n = 1$ allora $F =< x_1 >$ e per il teorema di classificazione dei gruppi ciclici (1.1.3) si ha $F =< x_1 > \cong \mathbb{Z}$. Poichè G è sottogruppo di F per il teorema (1.1.2) si ha o che $G =< dx_1 > \cong d_1\mathbb{Z}$ con $d_1 \in \mathbb{N}^*$ e l'asserto è verificato.
Procediamo induttivamente e assumiamo che il teorema sia vero per ogni gruppo abeliano libero di rango minore di n. Sia S l'insieme di tutti gli interi s tali che esiste una base $\{y_1, y_2 \ldots, y_n\}$ di F e un elemento in G della forma $sy_1 + k_2y_2 + \ldots + k_ny_n$ con $k_i \in \mathbb{Z}$. Si noti che così anche $\{y_2, y_1 \ldots, y_n\}$ è una base di F da cui segue che $k_2 \in S$. Ragionando analogamente si ha che anche tutti i $k_j \in S$ con $j = 3, 4, \ldots, n$. Poichè $G \neq 0$ allora $S \neq$. Da cui per il prinicipio del minimo esiste un intero positivo d_1 minimo in S e per una certa base $\{y_1, y_2 \ldots, y_n\}$ di F si ha che esiste un elemento $v \in G$ tale che $v = d_1y_1 + k_2y_2 + \ldots + k_ny_n$. Per l'algoritmo di divisione per ogni $i = 2, \ldots, n$ si ha $k_i = d_1q_i + r_i$ con $0 \leq r_i \leq d_1$ da cui segue che:

$$v = d_1(y_1 + q_2y_2 + \ldots + q_ny_n) + r_2y_2 + \ldots + r_ny_n.$$

Sia:

$$x_1 := y_1 + q_2y_2 + \ldots + q_ny_n$$

allora per il lemma (1.4.6) vale che: $W = \{x_1, y_2, \dots y_n\}$ è ancora una base di F. Poichè $v \in G$, e W in qualsiasi modo la si riordini è sempre base di F allora ogni $r_i \in S$, ma poichè $r_i < d_1$ per ogni $i = 2, \dots, n$ allora la minimalità di d_1 implica che tutti gli r_i siano nulli, così: $r_2 = r_3 = \dots = r_n = 0$. Allora si ha:

$$d_1 x_1 = v \ \in G.$$

Sia ora

$$H =< y_2, y_3, \dots, y_n > .$$

Allora H è gruppo abeliano libero di rango $n-1$ tale che $F =< x_1 > \oplus H$ Mostriamo che $G =< v >= \oplus(G \cap H) =< d_1 x_1 > \oplus(G \cap H)$.
Innanzitutto osserviamo che poichè $\{x_1, y_2, \dots, y_n\}$ è una base di F vale $< v > \cap(G \cap H) = 0$. Mostriamo ora che $G =< v > +(G \cap H)$. Se $u = t_1 x_1 + t_2 y_2 + \dots + t_n y_n \in G$ con $t_i \in \mathbb{Z}$, allora per l'algoritmo di divisione $t_1 = d_1 q_1 + r_1$ con $0 \leq r_1 < d_1$ quindi G contiene $u - q_1 v = r_1 x_1 + t_2 y_2 + \dots + t_n y_n$. Poichè d_1 è il più piccolo elemento di S allora $r_1 = 0$ da cui $t_2 y_2 + \dots + t_n y_n \in (G \cap H)$. Così:

$$u = q_1 v + (t_2 y_2 + \dots + t_n y_n)$$

con $q_1 v \in < v >$ e $t_2 y_2 + \dots + t_n y_n \in (G \cap H)$. Pertanto:

$$G =< v > +(G \cap H)$$

E poichè $< v > \cap(G \cap H) = 0$ vale allora:

$$G =< v > \oplus(G \cap H).$$

Ora se $(G \cap H) = 0$ vale $G =< d_1 x_1 >$ e l'asserto è provato.
Supponiamo $(G \cap H) \neq 0$. Allora applicando l'ipotesi induttiva a H e $G \cap H$ esiste una base $\{x_2, x_3, \dots, x_n\}$ di H e degli interi positivi $r, d_2, \dots, d_r$ tali che $d_2 | d_3 | \dots | d_r$ e $G \cap H$ è abeliano libero con base $\{d_2 x_2, \dots, d_r x_r\}$. Poichè $F =< x_1 > \oplus H$ e $G =< d_1 x_1 > \oplus(G \cap H)$, allora $\{x_1, \dots, x_n\}$ è base di F e $\{d_1 x_1, \dots, d_r x_r\}$ è base di G. Per completare la prova dobbiamo mostrare

che $d_1|d_2$. Per l'algoritmo di divisione $d_2 = qd_1 + r_0$ con $0 \leq r_0 < d_1$. Per il lemma (1.4.6) si ha che: $\{x_2, x_1 + qx_2, x_3, \ldots, x_n\}$ è base di F e

$$d_1x_1 + d_2x_2 = d_1x_1 + (qd_1 + r_0)x_2 = r_0x_2 + d_1(x_1 + qx_2) \in G$$

allora $r_0 \in S$ e per la minimalità di d_1 in S si ha necessariamente $r_0 = 0$, da cui $d_1|d_2$. □

Corollario 1.4.8. *Sia G gruppo abeliano libero finitamente generato e siano n i suoi generatori, allora ogni sottogruppo H di G è generato da m elementi con $m \leq n$.*

Dimostrazione. Per il teorema (1.4.2) esistono un gruppo abeliano libero F di rango n e un epimorfismo $\pi : F \to G$. $\pi^{-1}(H)$ è un sottogruppo di F e per il teorema (1.4.7) è libero e di rango $m \leq n$. L'immagine attraverso π di una qualsiasi base di $\pi^{-1}(H)$ è un insieme con al più m elementi (poichè π è epimorfismo) che genera $\pi(\pi^{-1}(H)) = H$. □

Capitolo 2

Classificazione dei Gruppi Abeliani Finitamente Generati

In questo capitolo studieremo la struttura dei gruppi abeliani finiti e dei gruppi abeliani finitamente generati. Dopo aver dato qualche nozione preliminare utile alla trattazione di entrambi gli argomenti, il capitolo verrà diviso in tre parti. Nella prima parte studieremo rispettivamente la classificazione dei gruppi abeliani finiti mentre nella seconda quella dei gruppi abeliani finitamente generati. Nella terza parte invece tratteremo l'unicità di tali decomposizioni.

2.1 Definizioni Preliminari

Definizione 2.1. Sia G un gruppo, non necessariamente abeliano. Un elemento a di G si dice **primario** se esiste un numero primo p tale che l'ordine di a sia una potenza di p, cioè se $a^{p^n} = 1$ per un opportuno intero positivo n. Se il primo p è specificato si dice che a è un elemento p**-primario**.
Il gruppo G si dice **primario** o p**-gruppo** se esiste un numero primo p tale che ogni elemento di G sia p-primario.

Esempio 2.1. Esempi di p-gruppo sono i gruppi $\mathbb{Z}_p$ o gli $\mathbb{Z}_{p^a}$.
$\mathbb{Z}_9 = \{[0], [1], [2], [3], [4], [5], [6], [7], [8]\}$ è un 3-gruppo infatti ogni suo elemento ha periodo 3 o 9.
Sono esempi di 2-gruppi il gruppo di Klein V_4 che è di ordine 4 e il gruppo D_4 di ordine 8.

Definizione 2.2. Sia G un gruppo abeliano. Un elemento a di G si dice **elemento di torsione** se ha periodo finito. Il gruppo G è detto **gruppo di torsione** se tutti gli elementi di G hanno periodo finito.

Esempio 2.2. Esempi di gruppi di torsione sono gli $\mathbb{Z}_m$ poichè ogni elemento di questi ha periodo finito. Un esempio di gruppo senza torsione è invece $\mathbb{Z}$ poichè nessun elemento di $\mathbb{Z}$ ha periodo finito.

Diamo ora alcuni risultati che saranno utili nel seguito.

Lemma 2.1.1. *Sia G un gruppo abeliano. Sia $a \in G$ un elemento di ordine finito e sia n un intero. Allora $na = 0$ se e solo se $|a|$ divide n.*

Dimostrazione. Sia $|a| = k$. Se $k|n$ scriviamo $n = qk$. Allora $na = (qk)a = q(na) = 0$. D'altra parte mostriamo che $k|n$ facendo vedere che $k = MCD(k, n)$. Se $d = MCD(k, n)$ allora per l'algoritmo euclideo si ha: esistono $x, y \in \mathbb{Z}$ tali che $d = xk + yn$. Ne segue: $da = (xk + yn)a = xka + yna = x0 + 0y = 0$. Poichè k per definizione di ordine è il più piccolo intero positivo tale che $ka = 0$ e d è un intero positivo che divide k deve essere $d = k$. □

Proposizione 2.1.2. *Sia G un gruppo abeliano. Abbiamo le seguenti proprietà.*

(*i*) *Siamo a, b elementi di G di ordine rispettivamente m ed n. Allora $|a+b|$ divide mn.*

(*ii*) *Sia p un numero primo. Allora l'insieme G_p dei p-elementi di G è un sottogruppo di G.*

(*iii*) *Il sottoinsieme G_{tor} contenente tutti gli elementi di torsione di G è un sottogruppo di G.*

Dimostrazione. (*i*) Vale: $mn(a+b) = mna + mnb = n(ma) + m(nb) = n0 + m0 = 0$. L'asserto segue ora dal lemma (2.1.1).

(*ii*) Siano a e b due elementi di G_p tali che $|a| = p^n, |b| = p^m$ allora l'ordine di $a+b$ per (*i*) divide $p^n p^m = p^{(n+m)}$. Quindi l'ordine di $a+b$ è sempre potenza del primo p e $a + b \in G_p$.

(*iii*) Siano a e b due elementi di G_{tor} tali che $|a| = m$ e $|b| = n$ allora l'ordine di $a + b$ per (*i*) divide mn. Quindi l'ordine di $a + b$ è ancora finito e $a + b \in G_{tor}$.

□

Definizione 2.3. I sottogruppi di G:

$$G_p := G(p) := \{a \in G \mid |a| = p^n \text{ per un certo } n \geq 0\}$$

$$G_{tor} := \{a \in G \mid |a| \text{ è finito}\}$$

sono detti rispettivamente **componente p-primaria** di G e **sottogruppo di torsione** di G.

2.2 Classificazione Gruppi Abeliani Finiti

Nel primo capitolo abbiamo visto come esempi di gruppi abeliani ciclici il gruppo additivo dei numeri interi $\mathbb{Z}$ ed i suoi quozienti $\mathbb{Z}_n$. Con il teorema sulla classificazione dei gruppi ciclici, poi, abbiamo visto che ogni gruppo ciclico è isomorfo a $\mathbb{Z}$ oppre a $\mathbb{Z}_n$ e in particolare che è abeliano. Osservando che la somma diretta di gruppi abeliani è ancora un gruppo abeliano, segue così che ogni somma diretta di gruppi ciclici finiti è un gruppo abeliano finito. Quello che ci proponiamo di dimostrare ora è il viceversa: cioè *ogni gruppo abeliano finito è somma diretta di gruppi ciclici.*
La dimostrazione verrà divisa in due parti: nella prima parte mostreremo che

un gruppo abeliano finito è somma diretta di gruppi primari (cioè di gruppi aventi come ordine una potenza di un primo), e nella seconda che ogni gruppo primario è, a sua volta, somma diretta di gruppi ciclici.

Prima di dare la dimostrazione enunciamo alcuni risultati importanti sui gruppi abeliani finiti: il Teorema di Lagrange e qualche sua applicazione.

Teorema 2.2.1 (Teorema di Lagrange)**.** *Sia G un gruppo abeliano finito e sia H un suo sottogruppo. Allora l'ordine di H divide l'ordine di G*

Dimostrazione. Vedi Teorema 4.5 pag 39 [2]. □

Corollario 2.2.2. *Valgono i seguenti risultati:*

(*i*) *Se a è un elemento di un gruppo abeliano finito G, allora l'ordine di a divide $|G|$.*

(*ii*) *Se a è un elemento di un gruppo abeliano finito G di ordine n allora $na = 0$.*

(*iii*) *Se m, n sono interi positivi e a è un elemento di ordine mn in un gruppo abeliano, allora na ha ordine m.*

(*iv*) *Un gruppo abeliano finito non nullo contiene un sottogruppo non banale se e solo se ha ordine che non è primo.*

(*v*) *Un gruppo abeliano di ordine primo è ciclico.*

Dimostrazione. (*i*) L'ordine di a è l'ordine del sottogruppo generato da a, dunque per il Teorema di Lagrange (2.2.1) l'ordine del sottogruppo generato da a divide l'ordine di G.

(*ii*) Per il lemma (2.1.1) dato un intero n vale: se $|a|$ divide n allora $na = 0$, ma per (*i*) $|a|$ divide $|G|$.

(*iii*) Per il lemma (2.1.1) si ha che $kna = 0$ se e solo se mn divide kn, cioè se e solo se m divide k.

(*iv*) Sia G un gruppo abeliano non nullo. Ovviamente $|G| \neq 1$ perchè G non è nullo. Dal Teorema di Lagrange (2.2.1) segue che se $|G| = p$ con p primo allora G non ha sottogruppi banali. Supponiamo che $|G|$ non sia primo. Allora esisteranno degli interi m ed n con $|G| = mn$, $1 < m, n < |G|$. Prendiamo un elemento $a \in G$. Se a ha ordine minore di mn allora il sottogruppo $< a >$ è non nullo e diverso da G. Supponiamo che l'ordine di a sia mn, allora per (*iii*) l'elemento na ha ordine m, e il sottogruppo $< na >$ è così un sottogruppo proprio.

(*v*) Sia G un gruppo abeliano finito con $|G| = p$, p primo, e sia $a \neq 0$ un elemento di G. Allora $< a >$ è un sottogruppo non nullo di G e quindi $< a >= G$ per (*iv*). Quindi G è ciclico.

□

Teorema 2.2.3. *Sia G un gruppo abeliano finito. Allora G è somma diretta delle sue componenti primarie non identiche.*

Dimostrazione. Sia $g \in G$, $g \neq 1$ e sia n il suo ordine. Per il teorema fondamentale dell'aritmetica n si fattorizza come prodotto di numeri primi. Sia

$$n = p_1^{t_1} p_2^{t_2} \dots p_h^{t_h}$$

la fattorizzazione di n con i p_i primi distinti per ogni $i = 1, \dots, h$. Poniamo

$$n_i = n/p_i^{t_i}.$$

Si osservi che il massimo comun divisore positivo di $n_1, n_2, \dots, n_h$ è 1 e quindi per l'algoritmo Euclideo si ha che esistono $x_1, \dots, x_n$ interi tali che:

$$1 = \sum_{i=1}^{h} n_i x_i. \tag{2.1}$$

Poniamo ora $g_i = n_i x_i g$. Allora

$$p_i^{t_i} g_i = p_i^{t_i} n_i x_i g = x_i p_i^{t_i} n_i g = x_i (ng) = x_i 0 = 0.$$

Quindi per il lemma (2.1.1) $|g_i|$ divide $p_i^{t_i}$ e g_i è un elemento p_i-primario. Inoltre per l'equazione (2.1) si ha:

$$1g = (\sum_{i=1}^{h} n_i x_i)g = \sum_{i=1}^{h} g_i$$

dunque ogni elemento g di G si scrive come somma di elementi primari e quindi G è la somma delle sue componenti primarie:

$$G = G_{p_1} + G_{p_2} + \ldots + G_{p_h}.$$

Mostriamo ora che questa somma è diretta, cioè che se $G_{p_1}, G_{p_2}, \ldots, G_{p_h}$ sono le componenti primarie di G allora per ogni $j = 1, \ldots, h$ risulta:

$$G_{p_j} \cap (G_{p_1} + \ldots + G_{p_{j-1}} + G_{p_{j+1}} + \ldots + G_{p_h}) = \{0\}.$$

Infatti se $g \in G_{p_1} + \ldots + G_{p_{j-1}} + G_{p_{j+1}} + \ldots + G_{p_h}$ allora $g = \sum_{i=1, i\neq j}^{h} g_i$ e l'insieme dei divisori primi di $|g|$ per l'osservazione (2.1.2)(i) è non vuoto e contenuto in

$$\{p_1, \ldots, p_{j-1}, \ldots, p_{j+1}, \ldots, p_h\}.$$

D'altra parte gli elementi di G_{p_j} sono p_j-primari e poichè

$$p_j \notin \{p_1, \ldots, p_{j-1}, \ldots, p_{j+1}, \ldots, p_h\}$$

allora $g \notin G_{p_j}$.

□

Abbiamo così ridotto il problema della classificazione di gruppi abeliani finiti al problema della struttura dei gruppi primari finiti. Per classificare tali gruppi abbiamo bisogno dei seguenti risultati.

Lemma 2.2.4. *Sia G un p-gruppo abeliano finito. Sia b un elemento di G, $b \neq 0$. Sia $k \geq 0$ un intero tale che $p^k b \neq 0$ e sia p^m il periodo di $p^k b$. Allora b ha periodo p^{k+m}.*

Dimostrazione. Poiche $|p^k b| = p^m$ allora $p^{k+m} b = p^m p^k b = 0$. Quindi sicuramente p^{k+m} divide $|b|$. Ma un $n < m + k$ tale che $p^n b = 0$ non può esistere perchè altrimenti il periodo di $p^k b$ sarebbe più piccolo di p^m. □

Lemma 2.2.5. *Sia G un p-gruppo abeliano finito. Sia a_1 un elemento di periodo massimale $|a_1| = p^{r_1}$ in G. Sia G_1 il sottogruppo ciclico generato da a_1. Sia $\bar{b}$ un elemento di G/G_1 di periodo p^r allora esiste un rappresentante a di $\bar{b}$ in G avente lo stesso periodo p^r.*

Dimostrazione. Sia b un rappresentante di $\bar{b}$ in G. Allora $p^r b$ sta in G_1 e si può scrivere $p^r b = na_1$ per un certo intero $n \geq 0$. Ora se $n = 0$ allora $p^r b = 0$ quindi b ha periodo p^r in G e l'assunto è provato. Se $n > 0$ scriviamo $n = p^k m$ dove $(m, p) = 1$, allora ma_1 è anch'esso un generatore di G_1 e quindi ha periodo p^{r_1}. Assumiamo che $k \leq r_1$ allora $p^k ma_1$ ha periodo p^{r_1-k}, così per il lemma precedente $b \in G$ ha periodo p^{r+r_1-k}. Ma per ipotesi p^{r_1} è periodo massimale in G pertanto:

$$r + r_1 - k \leq r_1 \text{ e } r \leq k.$$

Questo prova che esiste un elemento $c \in G_1$ tale che $p^r b = p^r c$. Sia $a = b - c$. Allora a è rappresentante di $\bar{b}$ in G e $p^r a = 0$. Poichè $|a| \leq p^r$ possiamo concludere che $|a| = p^r$. □

Osserviamo che l'ipotesi che a_1 sia di periodo massimale è fondamentale. Se non ci fosse il lemma non sarebbe vero. Infatti un controesempio è dato da: $\mathbb{Z}_9$ e $\mathbb{Z}_9/\mathbb{Z}_3 = \mathbb{Z}_3$. I rappresentanti di $[1]_3$ in $\mathbb{Z}_9$ sono $[1]_9$, $[4]_9$, $[7]_9$ e nessuno di loro ha periodo 3. Osserviamo inoltre che se G è ciclico, e lo si quozienta con il sottogruppo generato dall'elemento di periodo massimale si ottiene $G/G_1 = 0$.

Teorema 2.2.6. *Ogni p-gruppo abeliano finito è somma diretta di p-gruppi ciclici.*

Dimostrazione. Sia G il p-gruppo abeliano finito. Proviamo l'esistenza della somma diretta per induzione. Se $|G| = p$ allora per il corollario al Teorema di Lagrange (2.2.2) G è ciclico, quindi l'assunto è vero. Se $|G| > p$, $|G| = p^n$. Assumiamo che G non sia ciclico, altrimenti l'assunto sarebbe vero. Sia $a_1 \in G$ un elemento di periodo massimale $|a_1| = p^{r_1}$, e sia G_1 il sottogruppo ciclico

generato da a_1 tale che $|G_1| = p^{r_1}$. Per il corollario al Teorema di Lagrange (2.2.2) poichè G è finito allora $|a_1| = p^{r_1}$ divide $p^n = |G|$ e considerando G/G_1 si ha $|G/G_1| = p^n/p_1^r = p^{n-r_1}$. Dunque G/G_1 è ancora un p-gruppo finito applicando l'ipotesi induttiva a G/G_1 si ha che G/G_1 si può scrivere come somma diretta di gruppi ciclici

$$G/G_1 = \bar{G}_2 \oplus \ldots \oplus \bar{G}_s \tag{2.2}$$

di ordini $p^{r_2}, \ldots, p^{r_s}$. Sia $\bar{a}_i$ il generatore di $\bar{G}_i$ per $i = 2, \ldots, s$ e sia a_i il rappresentante in G di $\bar{a}_i$ avente stesso periodo di $\bar{a}_i$ (tale rappresentante esiste per il lemma). Sia G_i il sottogruppo ciclico generato da a_i.
Mostriamo, ora, che G è somma di $G_1, \ldots, G_s$. Dato x in G sia $x = \bar{x} + G_1$ la sua scrittura in G/G_1. Allora poichè G/G_1 è somma diretta come in (2.2) si ha che esistono $m_2, \ldots, m_s$ interi con $m_i \geq 0$ per $i = 2, \ldots, s$ tali che:

$$\bar{x} = m_2\bar{a}_2 + \ldots + m_s\bar{a}_s$$

Così

$$x - m_2a_2 + \ldots + m_sa_s \text{ sta in } G_1$$

esiste allora un intero $m_1 \geq 0$ tale che:

$$m_1a_1 = x - m_2a_2 + \ldots + m_sa_s$$

e, pertanto:

$$x = m_1a_1 + m_2a_2 + \ldots + m_sa_s.$$

Da cui, abbiamo che G è somma dei G_i:

$$G = G_1 + G_2 + \ldots + G_s$$

Mostriamo ora che tale somma è diretta. Per l'osservazione (1.2) è sufficiente provare che dati $m_1, \ldots, m_s$ interi ≥ 0 vale:

$$m_1a_1 + m_2a_2 + \ldots + m_sa_s = 0 \Rightarrow m_1, \ldots, m_s = 0.$$

Siano allora $m_1, \ldots, m_s$ interi ≥ 0 tali che per ogni $i = 1, \ldots, s$ che $m_i < p^{r_i}$ e per i quali valga:

$$m_1 a_1 + m_2 a_2 + \ldots + m_s a_s = 0$$

per come sono stati scelti gli m_i questa equazione resta valida anche per gli elementi $\bar{a_i}$:

$$0 = m_2 \bar{a_2} + \ldots + m_s \bar{a_s}$$

e poichè $\bar{G_2} \oplus \ldots \oplus \bar{G_s}$ è somma diretta vale $m_2, \ldots, m_s = 0$. Ma a questo punto anche $m_1 = 0$ perchè $m_1 a_1 = 0$, con $a_1 \neq 0 \Rightarrow m_1 = 0$. Da cui $m_i = 0$ per ogni $i = 1, \ldots, s$. Quindi la somma dei G_i è diretta:

$$G = G_1 \oplus G_2 \oplus \ldots \oplus G_s$$

□

Sia G un p-gruppo abeliano finito. Siano $r_1, \ldots, r_s$ interi ≥ 1. Diremo che un p-gruppo è del **tipo** $(p^{r_1}, \ldots, p^{r_s})$ se ha una scomposizione in somma diretta di gruppi ciclici di ordini p^{r_i} con $i = 1, \ldots, s$.

Possiamo ora dimostrare il teorema di classificazione dei gruppi abeliani finiti.

Teorema 2.2.7. *Sia G un gruppo abeliano finito, allora G è somma diretta di gruppi ciclici primari.*

Dimostrazione. Per il teorema (2.2.3) G è somma diretta delle sue componenti primarie e per il teorema (2.2.6) ogni componente primaria è somma diretta di gruppi ciclici. □

Corollario 2.2.8. *Per ogni gruppo abeliano finito G vale:*

$$G = \mathbb{Z}_{p_1}^{s_1} \oplus \ldots \oplus \mathbb{Z}_{p_k}^{s_k}$$

con i p_i primi e s_i interi

Dimostrazione. Per il teorema (2.2.7) ogni gruppo abeliano finito si può scrivere come somma diretta di gruppi ciclici aventi ordini $p_i^{s_i}$, ma per il teorema (1.1.3) ogni gruppo ciclico finito avente ordine potenza di un primo è isomorfo a $\mathbb{Z}_{p_i}^{s_i}$. Così si ottiene la somma diretta voluta. □

Teorema 2.2.9. *Sia G un gruppo abeliano finito, allora G è somma diretta di gruppi ciclici:*

$$G = C_1 \oplus C_2 \oplus \ldots \oplus C_t$$

tali che:

$$|C_1| \Big| |C_2| \Big| \ldots \Big| |C_t|.$$

Dimostrazione. Sia $G = G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{p_s}$ la decomposizione primaria di G e, per ogni $i = 1 \ldots s$, sia $G_{p_i} = X_{i,1} \oplus X_{i,2} \oplus \ldots \oplus X_{i,t_i}$ la decomposizione di G_{p_i} come somma diretta di gruppi ciclici. A meno di aggiungere degli addendi diretti uguali a $\{1\}$ possiamo supporre $t_i = t_j =: t$ per ogni i, j. Ordiniamo ora gli indici in modo che per ogni $i \in \{1, \ldots s\}$ risulti:

$$|X_{i,1}| \Big| |X_{i,2}| \Big| \ \ldots \Big| |X_{i,t}|$$

e poniamo per ogni $j \in \{1, \ldots, t\}$:

$$C_j := X_{1,j} \oplus X_{2,j} \oplus \ldots \oplus X_{r,j}$$

Allora:

$$G = C_1 \oplus C_2 \oplus \ldots \oplus C_t$$

dove C_j è gruppo ciclico perchè somma diretta di gruppi ciclici di ordine coprimo, ed infine vale:

$$|C_1| \Big| |C_2| \Big| \ldots \Big| |C_t|.$$

□

Corollario 2.2.10. *Per ogni gruppo abeliano finito G vale:*

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_t} \tag{2.3}$$

con

$$m_1 | m_2 | \ldots | m_t.$$

Dimostrazione. Per il teorema (2.2.9) si ha: $G = C_1 \oplus C_2 \oplus \ldots \oplus C_t$ con $|C_1| \mid |C_2| \mid \ldots \mid |C_t|$. Poniamo $|C_1| = m_1, |C_2| = m_2, \ldots, |C_t| = m_t$. Applicando i teoremi (1.1.3) e (1.2.3) la somma diretta del teorema (2.2.9) diventa:

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_t}$$

con $m_1|m_2|\ldots|m_t$. □

2.3 Classificazione Gruppi Abeliani Finitamente Generati

In questa sezione ci proponiamo di dimostrare che ogni gruppo abeliano finitamente generato si può scomporre in una somma diretta di un gruppo libero che rappresenta la componente infinita del gruppo dato e di una somma diretta di gruppi ciclici che rappresenta la componente finita.
E' possibile dividere il problema in due parti. Nella prima si mostra che un gruppo abeliano finitamente generato è isomorfo alla somma diretta di un gruppo libero e del suo gruppo di torsione. Nella seconda che il gruppo di torsione è finito e pertanto, per quanto già visto, somma diretta di gruppi ciclici. Per effettuare tale scomposizione ci riconduciamo, allora, alla struttura dei gruppi finiti studiata nella sezione precedente.

Lemma 2.3.1. *Siano G e G' due gruppi abeliani, assumiamo che G' sia libero. Sia poi $f : G \to G'$ un epimorfismo di gruppi abeliani. Sia K il nucleo di f. Allora esiste un sottogruppo H di G tale che la restrizione di f ad H induce un isomorfismo tra H e G' tale che*

$$G = K \bigoplus H.$$

Dimostrazione. Sia $\{x'_i\}_{i \in I}$ una base di G'. Poichè f è suriettiva per ogni $i \in I$ si può considerare un elemento x_i di G tale che $f(x_i) = x'_i$. Sia H il sottogruppo di G generato da tutti gli elementi x_i con $i \in I$. Supponiamo

valga la relazione:

$$\sum_{i\in I} n_i x_i \text{ con gli interi } n_i \geq 0$$

allora:

$$0 = f(0) = \sum_{i\in I} n_i f(x_i) = \sum_{i\in I} n_i x_i'.$$

Ora, poichè $\{x_i'\}_{i\in I}$ è una base, vale:

$$\sum_{i\in I} n_i x_i' = 0 \;\Rightarrow\; n_i = 0 \;\forall\; i \in I$$

Da cui $\{x_i\}_{i\in I}$ è una base per H:

$$H = \{h = \sum_{i\in I} m_i x_i \text{ per certi } m_i \text{ interi}\}.$$

Vogliamo ora mostrare che $G = H \oplus K$. Sia ora $x \in G$ e sia $f(x) \in G'$ la sua immagine attraverso f. Si ha che $f(x)$ si può scrivere come combinazione lineare della base $\{x_i'\}_{i\in I}$: esistono $m_i, i \in I$ interi tali che:

$$f(x) = \sum_{i\in I} m_i x_i' \tag{2.4}$$

così, considerando $x - \sum_{i\in I} m_i x_i$ in G e applicando a questo elemento f si trova:

$$f(x) - \sum_{i\in I} m_i f(x_i) = f(x) - \sum_{i\in I} m_i x_i' = 0 \text{ per (2.4)}.$$

Da cui:

$$x - \sum_{i\in I} m_i x_i = b \in K \Rightarrow x = b + \sum_{i\in I} m_i x_i = b + c \text{ con } b \in K \text{ e } c \in H$$

Pertanto: $x \in H + K$.

Bisogna ora provare che la somma sia diretta. Supponiamo $z \in H \cap K$ e proviamo che $z = 0$. Poichè $z \in H$ allora esistono m_i interi ≥ 0 tali che $z = \sum_{i\in I} m_i x_i$ e $f(z) = \sum_{i\in I} m_i x_i'$ Poichè $z \in Kerf \Rightarrow f(z) = 0$ allora:

$$0 = f(z) = \sum_{i\in I} n_i x_i' \Rightarrow n_i = 0 \;\forall i \in I$$

perchè $\{x_i'\}_{i\in I}$ è base. Quindi: $z = \sum_{i\in I} m_i x_i = 0$ perchè tutti gli $n_i = 0$. Per cui $H \cap K = \{0\}$ e $H \oplus K$ è diretta. □

Teorema 2.3.2. *Sia G un gruppo abeliano finitamente generato senza torsione. Allora G è libero.*

Dimostrazione. Supponiamo $G \neq \{0\}$. Sia X un insieme finito di generatori di G e sia $\{x_1, \dots x_n\}$ il sottoinsieme massimale di X avente la seguente proprietà:

$$\begin{aligned} &\text{data una qualunque } n\text{-upla di interi } v_1, \dots, v_n \text{ tali che} \\ &v_1x_1 + \dots + v_nx_n = 0 \text{ allora } v_j = 0 \text{ per ogni } j. \end{aligned} \tag{2.5}$$

Sia H il sottogruppo generato da $x_1, \dots, x_n$. Allora H è libero, per la proprietà (2.5), gli x_i sono linearmente indipendenti, quindi gli x_i formano una base per H. Dato y in G, poichè abbiamo assunto che $\{x_1, \dots x_n\}$ formino un insieme massimale, esistono degli interi $m_1, \dots, m_n, m$ non tutti nulli tali che:

$$my + m_1x_1 + \dots + m_nx_n = 0.$$

Inoltre si ha $m \neq 0$, altrimenti per la proprietà (2.5) tutti gli $m_j = 0$. Da cui: $my \in H$ poichè mi posso scrivere my come combinazione lineare di $x_1, \dots, x_n$. Prendendo un qualsiasi insieme di generatori di G questo resta vero per ogni generatore y dell'insieme. Così esiste un intero $m \neq 0$ tale che $mG \subset H$. Poichè G è senza torsione, allora la mappa:

$$f : G \to G \text{ definita da } f(x) = mx$$

è un omomorfismo avente $Kerf = 0$. Ne viene che f è un isomorfismo da G nel sottogruppo $mG \subset H$ per cui, poichè H è libero, per il teorema (1.4.7) mG è libero. Pertanto G è libero.

□

Teorema 2.3.3. *Sia G un gruppo abeliano finitamente generato, e sia G_{tor} il sottogruppo di G contenente tutti gli elementi di G aventi periodo finito. Allora G_{tor} è finito e G/G_{tor} è libero. Inoltre vale:*

$$G = G/G_{tor} \oplus G_{tor} \tag{2.6}$$

Dimostrazione. Osserviamo che un gruppo di torsione abeliano finitamente generato è finito poichè ogni suo generatore ha periodo finito. Sia G finitamente generato da n elementi e sia F il gruppo libero costruito sugli n generatori. Per la proprietà universale dei gruppi liberi del teorema (1.4.2), esiste un epimorfismo:

$$f : F \to G.$$

Il sottogruppo $f^{-1}(G_{tor})$ di F è finitamente generato per il teorema (1.4.7) Quindi anche G_{tor} è finitamente generato e pertanto finito. Proviamo ora che G/G_{tor} non ha torsione. Sia $\bar{x}$ un elemento di G/G_{tor} tale che $m\bar{x} = 0$ per un certo intero $m \neq 0$. Allora per ogni rappresentante x di $\bar{x}$ in G abbiamo che $mx \in G_{tor}$, da cui $qmx = 0$ per un certo intero $q \neq 0$. Allora $x \in G_{tor}$ e $\bar{x} = 0$. Ne viene che G/G_{tor} non ha torsione. Per il teorema (2.3.2) G/G_{tor} è libero. Per provare (2.6) osserviamo che siamo nelle condizioni del lemma (2.3.1). Scegliamo la mappa quoziente $\pi : G \to G/G_{tor}$ allora $Ker\pi$ per il lemma (2.3.1) esiste un sottogruppo H di G tale che $G = G_{tor} \oplus H$ con H isomorfo a G/G_{tor}. □

Teorema 2.3.4. *Sia G gruppo abeliano finitamente generato e siano F gruppo abeliano libero, $m_1, m_2, \ldots, m_t$ interi tali che $m_1|m_2|\ldots|m_t$, $p_1, \ldots p_k$ numeri primi e $s_1, \ldots s_k$ interi. Allora per G valgono le scritture:*

$$G \cong F \oplus \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_t}. \tag{2.7}$$

$$G = F \oplus \mathbb{Z}_{p_1}^{s_1} \oplus \ldots \oplus \mathbb{Z}_{p_k}^{s_k} \tag{2.8}$$

Dimostrazione. Per il teorema (2.3.3) si ha:

$$G = G/G_{tor} \oplus G_{tor}$$

con G_{tor} finito e G/G_{tor} libero. Poichè G_{tor} è finito per ottenere l'assunto è sufficiente applicare ad esso i corollari (2.2.10) e (2.2.8). □

Osserviamo che il teorema (2.3.3) è il teorema chiave per la scomposizione dei gruppi abeliani finitamente generati, è questo infatti che permette di

suddividere il gruppo G nelle sue componenti: libera e finita. Utilizzando questo teorema abbiamo fatto uso della scomposizione di un gruppo finito già vista in precedenza, tuttavia si può dare una dimostrazione della possibilità di scomporre un gruppo finitamente generato senza utilizzare direttamente la scomposizione della sua parte finita.

Teorema 2.3.5. *Ogni gruppo abeliano finitamente generato G è isomorfo a una somma diretta di gruppi ciclici in cui gli addendi ciclici finiti, se ci sono, sono di ordine $m_1, m_2, \ldots, m_t$ dove $m_1 > 1$ e $m_1|m_2|\ldots|m_t$.*

Dimostrazione. Se $G \neq 0$ e G è generato da n elementi, allora per il teorema (1.4.2) esiste un gruppo abeliano libero F di rango n e un epimorfismo $\pi : F \to G$. Se π è isomorfismo allora per il teorema (1.4.1)

$$G \cong F \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z} \text{ (n addendi)}$$

e si ha che G è somma diretta di gruppi ciclici infiniti e quindi l'asserto è provato.
Se π non è isomorfismo allora per il teorema (1.4.7) esiste una base $\{x_1, \ldots, x_n\}$ di F e una lista di interi positivi $d_1, d_2, \ldots, d_r$ con $1 \leq r \leq n$ tali che $d_1|d_2|\ldots|d_r$ e $\{d_1x_1, d_2x_2, \ldots d_rx_r\}$ è una base di $K = Ker\pi$. Così:

$$F = \sum_{i=1}^{n} < x_i > \text{ e } K = \sum_{i=1}^{r} < d_ix_i >$$

dove per il teorema di classificazione dei gruppi cilici (1.1.3) si ha: $< x_i > \cong \mathbb{Z}$ e $< d_ix_i > \cong d_i\mathbb{Z}$. Poniamo ora $d_i = 0$ per $i = r+1, r+2, \ldots, n$, così: $K \cong \sum_{i=1}^{n} < d_ix_i >$. Ora per il I Teorema di Isomorfismo (1.1.1) e il corollario (1.2.4) si ha:

$$G \cong F/K = \sum_{i=1}^{n} < x_i > / \sum_{i=1}^{n} < d_ix_i > \cong \sum_{i=1}^{n} < x_i > / < d_ix_i > \cong \sum_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z}.$$

Osserviamo che

$$\begin{aligned} &\text{se } d_i = 1 \quad \text{allora} \quad \mathbb{Z}/d_i\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = 0 \\ &\text{se } d_i \geq 1 \quad \text{allora} \quad \mathbb{Z}/d_i\mathbb{Z} \cong \mathbb{Z}_{d_i} \\ &\text{se } d_i = 0 \quad \text{allora} \quad \mathbb{Z}/d_i\mathbb{Z} = \mathbb{Z}/0 = \mathbb{Z} \end{aligned}$$

Sia t il numero di $d_i \neq 0, 1$ poniamo $m_1, \dots m_t$ tali che $m_i = d_i$ (in ordine) per ogni i tale che $d_i \neq 0, 1$. Sia s il numero di d_i tali che $d_i = 0$. Allora:

$$G = \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_t} \oplus (\mathbb{Z} \oplus \dots \oplus \mathbb{Z})$$

dove $\mathrm{m}_1 > 1, m_1|m_2| \dots |m_t$ e $\mathbb{Z} \oplus \dots \oplus \mathbb{Z}$ ha rango s. □

Questo Teorema dà un'altra dimostrazione dell'esistenza di una scomposizione di un gruppo abeliano G finitamente generato come somma diretta di gruppi ciclici senza utilizzare la scomposizione di un gruppo abeliano finito. In questa seconda dimostrazione l'attenzione è focalizzata maggiormente sulla parte libera del gruppo. Ciò su cui è basata la prova sono, infatti, le particolarità dei gruppi liberi: si fa uso di quanto visto nel primo capitolo sui gruppi abeliani liberi e le loro basi. Si noti che questo è un approccio diverso da quello visto precedentemente che si focalizzava maggiormente sulla parte finita del gruppo.

2.4 Unicità Delle Decomposizioni

In questa sezione proveremo l'unicità della decomposizione in gruppi ciclici di un gruppo abeliano finitamente generato e definiremo alcuni importanti invarianti numerici per i gruppi.

Nella sezione precedente abbiamo visto che dato un gruppo abeliano G finitamente generato esso può essere scritto come

$$G \cong G_{tor} \bigoplus G/G_{tor} = \bigoplus_{i=1}^{t} \mathbb{Z}_{m_i} \bigoplus F, \tag{2.9}$$

dove gli m_i sono interi positivi tali che $m_1 > 1$, $m_1|m_2| \dots |m_t$ ed F è un gruppo abeliano libero di rango s.
Più precisamente:

$$G \cong G_{tor} \bigoplus G/G_{tor} = \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{a_i}} \bigoplus F, \tag{2.10}$$

dove i $p_i^{a_i}$ sono interi positivi tali che i p_i siano primi e gli a_i siano interi positivi, ed F come sopra.

Lemma 2.4.1. *Siano G e H gruppi abeliani isomorfi, sia f un isomorfismo fra G ed H e sia p un primo. Allora le restrizioni di f a G_{tor} e G_p sono isomorfismi rispettivamente fra G_{tor} e H_{tor} e fra G_p e H_p.*

Dimostrazione. Essendo f un isomorfismo, se $x \in G_p$ ha ordine p^n, allora $p^n f(x) = f(p^n x) = f(0) = 0$. Quindi $f : G_p \to H_p$. Analogamente, $f^{-1} : H_p \to G_p$ e così $ff^{-1} = 1_{H_p}$ e $f^{-1}f = 1_{G_p}, G_p \cong H_p$.
Per quanto riguarda G_{tor} si procede nello stesso modo. □

Lemma 2.4.2. *Siano G e G' gruppi abeliani isomorfi e sia f un isomorfismo da G a G'. Siano poi H e H' due sottogruppi rispettivamente di G e di G' tali che la restrizione di f ad H sia un isomorfismo tra H e H'. Allora $G/H \cong G'/H'$.*

Dimostrazione. Sia $\phi : G/H \to G'/H'$ definita da $\phi(g + H) := f(g) + H'$. La definizione è ben posta: se $g' + H$ è un altro rappresentante di $g + H$ in G/H, allora, poichè $g - g' = h \in H$, $f(g') = f(g) + f(h)$ e dunque $f(g') + f(H) = f(g) + f(H)$. Dalle proprietà di f segue poi facilmente che ϕ è un isomorfismo fra i quozienti, con inversa $\phi^{-1} : G'/H' \to G/H$ definita da $\phi^{-1}(g' + H') = f^{-1}(g') + H$. □

Lemma 2.4.3. *Vale il seguente isomorfismo:*

$$p^m \mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-m}}.$$

Dimostrazione. Lemma 2.5 pag. 77 di [2]. □

Teorema 2.4.4. *Sia G un gruppo abeliano finitamente generato. Allora in ogni scomposizione di G come somma diretta di gruppi ciclici il numero di addendi di gruppi ciclici infiniti è sempre lo stesso.*

Dimostrazione. Siano $G \cong G_{tor} \oplus G/G_{tor} = G_{tor}$ e $G \cong G'_{tor} \oplus G/G'_{tor}$ due scomposizioni di G del tipo visto nelle equazioni (2.9) o (2.10) con G/G_{tor} e

G/G'_{tor} di rango rispettivamente s ed s'. Allora per i lemmi (2.4.1) (2.4.2) e il teorema (1.2.3) vale:

$$G_{tor} \oplus G/G_{tor} \cong G'_{tor} \oplus G/G'_{tor} \iff G_{tor} \cong G'_{tor} \text{ e } G/G_{tor} \cong G/G'_{tor}.$$

Consideriamo ora la parte libera di G. Per la proposizione (1.4.5) si ha:

$$G/G_{tor} \cong G/G'_{tor} \iff s = s'.$$

□

Teorema 2.4.5. *Sia G un p-gruppo abeliano finito. Supponiamo abbia una scomposizione in somma diretta di gruppi ciclici del tipo $(p^{r_1}, p^{r_2}, \dots p^{r_s})$ con*

$$r_1 \geq r_2 \geq \dots \geq r_s \geq 1,$$

allora la sequenza di interi $(r_1, \dots r_s)$ è univocamente determinata.

Dimostrazione. Procediamo per induzione sull'ordine di G. Supponiamo che

$$(p^{r_1}, p^{r_2}, \dots p^{r_s}) \text{ e } (p^{m_1}, p^{m_2}, \dots p^{m_k})$$

con $r_1 \geq r_2 \geq \dots \geq r_s \geq 1$ e $m_1 \geq m_2 \geq \dots \geq m_k \geq 1$ siano due scomposizioni di G in somma diretta di p-gruppi ciclici. Allora pG è anch'esso un p-gruppo di ordine strettamente minore dell'ordine di G ed avrà due scomposizioni del tipo

$$(p^{r_1-1}, p^{r_2-1}, \dots p^{r_s-1}) \text{ e } (p^{m_1-1}, p^{m_2-1}, \dots p^{m_k-1}),$$

dove si intende che se $r_i - 1 = 0$ o $m_j - 1 = 0$ per qualche indice i o j, il corrispondente p-Gruppo che compare nella scomposizione di pG è il sottogruppo banale. Siano ν il numero di indici i tali che $r_i = 1$ e μ il numero di indici j tali che $m_j = 1$. Per ipotesi induttiva, si ha che $s - \nu = k - \mu$ ed $r_i - 1 = m_i - 1$ per ogni $i = 1, \dots, s - \nu$. Inoltre, confrontando le due scomposizioni alla luce delle suddette uguaglianze, ricaviamo che

$$p^{r_1} \dots p^{r_{s-\nu}} p^{\nu} = |G| = p^{r_1} \dots p^{r_{s-\nu}} p^{\mu},$$

da cui $\nu = \mu$ e la dimostrazione è conclusa. □

Teorema 2.4.6. *Sia G un gruppo abeliano finitamente generato. Valgono:*

(*i*) *G è gruppo abeliano libero oppure esistono un gruppo abeliano libero F ed una lista di interi positivi $p_1^{s_1}, \ldots, p_k^{s_k}$, unica a meno dell'ordine dei suoi membri, con $p_1, \ldots, p_k$ primi (non necessariamente distinti) ed $s_1, \ldots, s_k$ interi positivi (non necessariamente distinti) tali che:*

$$G \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{p_i^{s_i}} \bigoplus F;$$

(*ii*) *G è gruppo abeliano libero oppure esistono un gruppo abeliano libero F ed un'unica lista di interi positivi (non necessariamente distinti) $m_1, m_2, \ldots, m_t$, con $m_1 > 1$, $m_1 | m_2 | \ldots | m_t$, tali che:*

$$G \cong \bigoplus_{i=1}^{t} \mathbb{Z}_{m_i} \bigoplus F.$$

Dimostrazione. (*i*) Supponiamo che G abbia due decomposizioni del tipo

$$G \cong \sum_{i=1}^{r} \mathbb{Z}_{n_i} \oplus F \text{ e } G \cong \sum_{j=1}^{d} \mathbb{Z}_{k_j} \oplus F'$$

con n_i, k_j potenze di primi (differenti) ed F, F' gruppi abeliani liberi. Dobbiamo mostrare che $r = d$ e $n_i = k_i$ per ogni i (dopo averli riordinati). Per quanto già visto si ha che

$$\sum_{i=1}^{r} \mathbb{Z}_{n_i} \cong G_{tor} \cong \sum_{j=1}^{d} \mathbb{Z}_{k_j}.$$

Inoltre per ogni primo p si ha che la componente p-primaria di $\sum_{i=1}^{r} \mathbb{Z}_{n_i}$ è isomorfa alla somma diretta degli $\mathbb{Z}_{n_i}$ tali che n_i è potenza del primo p. Analogamente per l'altra scomposizione. Poichè per il lemma (2.4.1) vale

$$(\sum_{i=1}^{r} \mathbb{Z}_{n_i})(p) \cong (\sum_{j=1}^{d} \mathbb{Z}_{k_j})(p)$$

per ogni primo p, per il teorema (1.2.3) è sufficiente assumere che $G = G_{tor}$ e che ogni n_i, k_j è potenza di un primo fissato p. In quest'ipotesi, $G = G(p)$ e ci possiamo ricondurre al teorema (2.4.5).

(*ii*) Supponiamo che G abbia due scomposizioni del tipo

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_t} \oplus F$$

$$G \cong \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \ldots \oplus \mathbb{Z}_{k_d} \oplus F'$$

con $m_1 > 1$, $m_1|m_2|\ldots|m_t$, $k_1 > 1$, $k_1|k_2|\ldots|k_d$ ed F, F' gruppi abeliani liberi. Ogni m_i, k_j ha una decomposizione in fattori primi e inserendo in caso di necessità dei fattori p^0 possiamo assumere che nelle due scomposizioni compaiano gli stessi primi distinti $p_1, \ldots, p_r$, ossia:

$$\begin{array}{ll} m_1 = p_1^{a_{11}} p_2^{a_{12}} \ldots p_r^{a_{1r}} & k_1 = p_1^{c_{11}} p_2^{c_{12}} \ldots p_r^{c_{1r}} \\ m_2 = p_1^{a_{21}} p_2^{a_{22}} \ldots p_r^{a_{2r}} & k_2 = p_1^{c_{21}} p_2^{c_{22}} \ldots p_r^{c_{2r}} \\ \vdots & \vdots \\ m_t = p_1^{a_{t1}} p_2^{a_{t2}} \ldots p_r^{a_{tr}} & k_d = p_1^{c_{d1}} p_2^{c_{d2}} \ldots p_r^{c_{dr}} \end{array}$$

Poichè $m_1|m_2|\ldots|m_t$ per ogni j si deve avere $0 \leq a_{1j} \leq a_{2j} \leq \ldots \leq a_{tj}$. Analogamente $0 \leq c_{1j} \leq c_{2j} \leq \ldots \leq c_{dj}$ per ogni j. Per il lemma (2.4.3) e teorema (2.2.3) vale:

$$\sum_{i,j} \mathbb{Z}_{p_j^{a_{ij}}} \cong \sum_{i=1}^{t} \mathbb{Z}_{m_i} \cong G_{tor} \cong \sum_{i=1}^{d} \mathbb{Z}_{k_i} \cong \sum_{i,j} \mathbb{Z}_{p_j^{c_{ij}}}$$

dove alcuni addendi possono essere 0. Da ciò segue che per ogni $j = 1, 2, \ldots, r$

$$\sum_{i,j} \mathbb{Z}_{p_j^{a_{ij}}} \cong \sum_{i,j} \mathbb{Z}_{p_j^{c_{ij}}}.$$

Poichè $m_1 > 1$ esiste un p_j tale che $1 \leq a_{1j} \leq \ldots \leq a_{tj}$ e quindi $\sum_{i,j} \mathbb{Z}_{p_j^{a_{ij}}}$ ha t addendi diversi da 0. Per il punto (i), $\sum_{i,j} \mathbb{Z}_{p_j^{c_{ij}}}$ ha esattamente t addendi diversi da 0, pertanto $t \leq d$. Analogamente $k_1 > 1$ implica $d \leq t$ perciò $d = t$. Ancora per il punto (i) bisogna avere $a_{ij} = c_{ij}$ per ogni i, j e questo implica che $m_i = n_i$ per ogni $i = 1, 2, \ldots, t$.

□

Definizione 2.4. Se G è un gruppo abeliano finitamente generato, allora gli interi $m_1, \ldots, m_t$ che soddisfano le condizioni del teorema (2.4.6) sono detti **fattori invarianti** di G. I numeri $p_i^{s_i}$ potenze di primi che soddisfano le condizioni del teorema (2.4.6) sono detti **divisori elementari**.

Se i fattori invarianti $m_1, \ldots, m_t$ di un gruppo G abeliano finitamente generato sono noti, allora i divisori elementari di G sono le potenze di primi p^n $(n > 0)$ che appaiono nella fattorizzazione in numeri primi di $m_1, \ldots, m_t$. D'altra parte, se sono noti i divisori elementari di G allora a partire da questi si possono dedurre i fattori invarianti nel modo seguente.
Possiamo organizzare i divisori elementari nella matrice

$$\begin{matrix} p_1^{n_{1,1}} & p_2^{n_{1,2}} & \ldots & p_r^{n_{1,r}} \\ p_1^{n_{2,1}} & p_2^{n_{2,2}} & \ldots & p_r^{n_{2,r}} \\ \vdots & & & \\ p_1^{n_{t,1}} & p_2^{n_{t,2}} & \ldots & p_r^{n_{t,r}} \end{matrix} \tag{2.11}$$

in modo tale che i p_j siano primi distinti, per ogni colonna j valga $0 \leq n_{1,j} \leq \ldots \leq n_{t,j}$ ed esista un indice i tale che $n_{i,j} \neq 0$ ed infine esista j tale che $n_{1,j} \neq 0$. Per la definizione di divisori elementari $G \cong \sum_{i=1}^{t} \sum_{j=1}^{r} \mathbb{Z}_{p_j^{n_{i,j}}} \oplus F$ dove F è abeliano libero.
Per ogni $i = 1, 2, \ldots, t$ sia

$$m_i = p_1^{n_{i,1}} p_2^{n_{i,2}} \ldots p_r^{n_{i,r}}.$$

Di conseguenza, $m_1 > 1$ e per costruzione $m_1 | m_2 | \ldots | m_t$. Per il teorema (2.2.3):

$$G \cong \sum_{i=1}^{t} (\sum_{j=1}^{r} \mathbb{Z}_{p_j^{n_{ij}}}) \oplus F \cong \sum_{i=1}^{t} \mathbb{Z}_{m_i} \oplus F.$$

Pertanto, $m_1, \ldots, m_t$ sono i fattori invarianti.

Esempio 2.3. Sia $G = \mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{54}$. Allora per il teorema (2.2.3) si ha:

$$G \cong \mathbb{Z}_5 \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_{25} \oplus (\mathbb{Z}_9 \oplus \mathbb{Z}_4) \oplus (\mathbb{Z}_{27} \oplus \mathbb{Z}_2).$$

Pertanto i divisori elementari di G sono $2, 2^2, 3, 3^2, 3^3, 5, 5, 5^2$ che possono essere organizzati:

$$\begin{array}{ccc} 2^0 & 3 & 5 \\ 2 & 3^2 & 5 \\ 2^2 & 3^3 & 5^2. \end{array}$$

Da ciò segue che i fattori invarianti di G sono:

$$1 \cdot 3 \cdot 5 = 15,\ 2 \cdot 3^2 \cdot 5 = 90,\ 2^2 \cdot 3^3 \cdot 5^2 = 2700.$$

Così:

$$G \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{90} \oplus \mathbb{Z}_{2700}.$$

Bibliografia

[1] S. Lang, *Algebra*, Springer, 2002.

[2] T. Hungerford, *Algebra*, Springer, 1974.

[3] A. Vistoli, *Note di Algebra*, Bononia, 1994.

[4] M. Mainardi, *Appunti di teoria dei Gruppi*, users.dimi.uniud.it/~mario.mainardis/LIBRO02.pdf .