Gruppi abeliani finitamente generati

Appunti al corso di Algebra
Anno accademico 2000-2001

1 Preliminari.

Ricordiamo che un gruppo G si dice commutativo o **abeliano** se la sua operazione interna gode della proprietá commutativa. Nel seguito, per un gruppo abeliano G, useremo la notazione additiva. Quindi l'elemento neutro sará denotato con 0 e dato $a \in G$ l'unico elemento $b \in G$ tale che $a + b = 0$ sará denotato con $-a$.

Ricordiamo che se $a \in G$ ed $n \in \mathbb{Z}$ abbiamo convenuto di denotare con na l'elemento di G cosí definito

$$na = 0 \quad \text{se } n = 0,$$

$$na = \underbrace{a + a + \cdots + a}_{n \quad volte} \quad \text{se } n > 0,$$

$$na = \underbrace{(-a) + (-a) + \cdots + (-a)}_{-n \quad volte} \quad \text{se } n < 0.$$

Nella notazione additiva, l'ordine (o periodo) di un elemento $a \in G$ é il piú piccolo intero positivo n tale che $na = 0$. Se tale intero non esiste, diremo che a ha ordine infinito e scriveremo $ord(a) = \infty$.

L'ordine di $a \in G$ é il generatore positivo del sottogruppo di $\mathbb{Z}$ costituito dal nucleo $Ker(\phi)$ dell'omomorfismo

$$\phi : \mathbb{Z} \to G$$

definito da $\phi(s) = sa$. Tale omomorfismo ha come immagine il sottogruppo ciclico generato da a, ossia il sottogruppo $< a >:= \{sa \mid s \in \mathbb{Z}\}$. Pertanto, se $n = ord(a)$, il primo teorema di omomorfismo di gruppi ci assicura che i due gruppi $< a >$ e $\mathbb{Z}/n\mathbb{Z}$ sono isomorfi:

$$< a > \simeq \mathbb{Z}/n\mathbb{Z}. \tag{1}$$

Se invece a ha ordine infinito, allora

$$< a > \simeq \mathbb{Z}. \tag{2}$$

Essendo G un gruppo abeliano, ogni suo sottogruppo H é normale e quindi possiamo considerare il gruppo quoziente G/H che é ancora abeliano.

2 Somme dirette e prodotto diretto.

Siano H e K due sottogruppi di uno stesso gruppo G; la somma di H e K é per definizione l'insieme degli elementi di G della forma $x+y$, al variare di x in H e di y in K. Questo é un sottogruppo di G che si indica con $H+K$ ed é il piú piccolo sottogruppo di G contenente $H \cup K$. Ad esempio $2\mathbb{Z} =< 4 > + < 6 >$. Notiamo che l'elemento $10 \in 2\mathbb{Z}$ si puó scrivere $10 = 4+6$ ma anche $10 = 4(4) + (-1)(6)$.

Proposizione 2.1 *Se G e H sono sottogruppi di G, sono fatti equivalenti:*
1) $H \cap K = \{0\}$.
2) Ogni elemento di $H+K$ si scrive in modo unico come somma di un elemento di H e di uno di K.

Prova. 1) implica 2). Sia $a+b = c+d$ con $a, c \in H$, $b, d \in K$. Allora $a-c = d-b \in H \cap K$. Quindi $a = c$, $b = d$.
2) implica 1). Sia $a \in H \cap K$; allora posso scrivere $a = a+0 = 0+a$. Per l'unicitá si ottiene $a = 0$. □

Definizione 2.2 *Se H e K verificano una delle precedenti condizioni equivalenti, diciamo che la somma $H+K$ é* **diretta** *e scriviamo $H \oplus K$ invece che $H+K$.*

Ad esempio $2\mathbb{Z}$ non é somma diretta di $4\mathbb{Z}$ e $6\mathbb{Z}$, e infatti si ha $12 \in 4\mathbb{Z} \cap 6\mathbb{Z}$.

La somma di due sottogruppi H e K di G é legata al prodotto diretto $H \times K$ da un omomorfismo canonico

$$\phi : H \times K \to H + K$$

definito da:

$$\phi(a, b) = a + b.$$

Chiaramente ϕ é surgettivo e si ha:

Proposizione 2.3 *L'omomorfismo ϕ é iniettivo se e solo se $H \cap K = \{0\}$.*

Prova. Sia ϕ iniettivo e sia $a \in H \cap K$. Allora $(a, -a) \in H \times K$ e si ha $\phi(a, -a) = 0$ Dunque $(a, -a) = (0, 0)$ e quindi $a = 0$.
Se viceversa $H \cap K = \{0\}$, sia $(a, b) \in H \times K$ tale che $\phi(a, b) = 0$. Allora $a+b = 0$ e quindi $a = -b \in H \cap K$. Ne segue $a = b = 0$ e quindi $(a, b) = (0, 0)$. □

Abbiamo cosí dimostrato che la somma di H e K é diretta se e solo se ϕ é isomorfismo.

Esempio. $\mathbb{Z} = 4\mathbb{Z} + 3\mathbb{Z}$ ma $4\mathbb{Z} \cap 3\mathbb{Z} \neq \{0\}$ perché $12 \in 4\mathbb{Z} \cap 3\mathbb{Z}$. Quindi $\mathbb{Z} \neq 4\mathbb{Z} \oplus 3\mathbb{Z}$ e $4\mathbb{Z} \times 3\mathbb{Z}$ non é isomorfo a $4\mathbb{Z} + 3\mathbb{Z}$.

Se invece $G = \{(2n, 3m) \mid n, m \in \mathbb{Z}\}$ é chiaro che

$$G =< (2, 0) > + < (0, 3) > .$$

Avendosi $< (2,0) > \cap < (0,3) >= \{(0,0)\}$, si ottiene

$$G =< (2,0) > \oplus < (0,3) > \simeq < (2,0) > \times < (0,3) > \simeq \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2.$$

Quindi G é sottogruppo proprio di $\mathbb{Z}^2$ ed é al tempo stesso isomorfo a $\mathbb{Z}^2$.

Analogamente, se $H_1, \ldots, H_n$ sono sottogruppi di G, l'insieme degli elementi di G che si possono scrivere nella forma $x_1 + x_2 + \cdots + x_n$ con $x_i \in H_i$, é un sottogruppo di G che si indica con $\sum_{i=1}^n H_i$. Se $G = \sum_{i=1}^n H_i$, diciamo che G é la somma dei suoi sottogruppi $H_1, \ldots, H_n$.

Come per il caso di due sottogruppi, ogni elemento di $\sum_{i=1}^n H_i$ si scrive come somma $x_1 + x_2 + \cdots + x_n$ con $x_i \in H_i$, ma tale scrittura non é necessariamente unica.

Proposizione 2.4 *Nelle notazioni precedenti sono fatti equivalenti:*

1) $H_i \cap \sum_{j \neq i} H_j = \{0\}$ *per ogni* $i = 1, \ldots, n$.

2) Ogni elemento v *di* $\sum_{i=1}^n H_i$ *si scrive in modo unico nella forma*

$$v = x_1 + x_2 + \cdots + x_n$$

con $x_i \in H_i$.

Definizione 2.5 *Se i sottogruppi* $H_1, \ldots, H_n$ *verificano una delle condizioni equivalenti nella precedente proposizione, diciamo che la somma* $\sum_{i=1}^n H_i$ *é* **diretta** *e scriviamo* $\oplus_{i=1}^n H_i$ *invece che* $\sum_{i=1}^n H_i$.

Nel caso in cui $H_1, \ldots, H_n$ sono sottogruppi di uno stesso gruppo G, possiamo dunque parlare della loro somma e del loro prodotto diretto. I due gruppi sono legati da un omomorfismo canonico importante.

Proposizione 2.6 *Se* $H_1, \ldots, H_n$ *sono sottogruppi di* G, *l'omomorfismo*

$$\phi : H_1 \times H_2 \times \cdots \times H_n \to \sum_{i=1}^n H_i,$$

che é definito ponendo

$$\phi(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \cdots + x_n,$$

e' surgettivo.

Inoltre ϕ *é iniettivo se e solo se* $H_i \cap \sum_{j \neq i} H_j = \{0\}$ *per ogni* $i = 1, \ldots, n$, *ossia se e solo se* $\sum H_i = \oplus H_i$.

La proposizione si dimostra esattamente come nel caso di due sottogruppi.

Nel seguito useremo piú volte il seguente facile risultato:

Proposizione 2.7 *Siano G, H, K, L gruppi abeliani e $\phi : G \to K$, $\psi : H \to L$ due omomorfismi di gruppi. Allora l'applicazione*

$$\phi \times \psi : G \times H \to K \times L$$

definita da $(\phi \times \psi)(a, b) = (\phi(a), \psi(b))$ é un omomorfismo di gruppi tale che

$$Im(\phi \times \psi) = Im(\phi) \times Im(\psi), \quad Ker(\phi \times \psi) = Ker(\phi) \times Ker(\psi).$$

Quindi, se ϕ e ψ sono isomorfismi, allora anche $\phi \times \psi$ é isomorfismo.

3 Gruppi liberi

Ricordiamo che se G é un gruppo abeliano ed $a_1, \ldots, a_r \in G$, il sottogruppo generato da $a_1, \ldots, a_r$ é costituito dagli elementi $\sum_{i=1}^{r} n_i a_i$ con $n_i \in \mathbb{Z}$. Tale sottogruppo si indica con $< a_1, \ldots, a_r >$ ed é il piú piccolo sottogruppo di G che contiene $a_1, \ldots, a_r$. Si ha ovviamente:

$$< a_1, \ldots, a_r > = < a_1 > + \cdots + < a_r > .$$

Il gruppo abeliano G si dice **finitamente generato** se esistono $a_1, \ldots, a_r \in G$ tali che $G = < a_1, \ldots, a_r >$. Ció significa che ogni elemento $a \in G$ si puó scrivere $a = \sum_{i=1}^{r} n_i a_i$, $n_i \in \mathbb{Z}$. In tal caso diremo che gli elementi $a_1, \ldots, a_r$ sono un **sistema di generatori** per G. Se $a_1, \ldots, a_r$ sono un sistema di generatori per G, allora

$$G = < a_1, \ldots, a_r > = < a_1 > + < a_2 > + \cdots + < a_r > .$$

Quindi ogni gruppo abeliano finitamente generato é somma di gruppi ciclici.

Ad esempio $\mathbb{Z}^n$ é finitamenete generato. Per fare un esempio di un gruppo abeliano non finitamente generato, consideriamo il gruppo G delle successioni di elementi di $\mathbb{Z}$ che sono definitivamente nulle e operiamo tra gli elementi di G con la somma componente per componente. É chiaro che G non é finitamente generato.

Notare che un gruppo abeliano finitamente generato puó avere piú sistemi di generatori. Ad esempio

$$\mathbb{Z}^2 = < (1, 0), (0, 1) > = < (2, 3), (-1, 1) > .$$

Se G é un gruppo abeliano e $a_1, \ldots, a_r$ sono elementi di G, si ha un omomorfismo

$$\phi : \mathbb{Z}^r \to G$$

definito da $\phi(n_1, \ldots, n_r) = \sum_{i=1}^{r} n_i a_i$.

É chiaro che ϕ ha come immagine $< a_1, \ldots, a_r >$ e quindi ϕ é surgettivo se e solo se $a_1, \ldots, a_r$ sono un sistema di generatori di G.

Diciamo che $a_1, \ldots, a_r$ sono **linearmente indipendenti** se ϕ é iniettivo. Ció significa che se $\sum_{i=1}^{r} n_i a_i = 0$ con $n_i \in \mathbb{Z}$, allora $n_1 = n_2 = \cdots = n_r = 0$.

Esempio. Gli elementi $(1,1),(1,5) \in \mathbb{Z}^2$ sono linearmente indipendenti: infatti $n(1,1)+m(1,5)=(0,0)$ implica $n+m=n+5m=0$ e quindi $n=m=0$.

Ma non sono generatori per $\mathbb{Z}^2$: ad esempio $(4,3) \notin < (1,1),(1,5) >$. Infatti se fosse $(4,3)=n(1,1)+m(1,5)$ sarebbe $n+m=4$ e $n+5m=3$. Poiché $n,m \in \mathbb{Z}$, tale sistema non ha soluzione.

D'altra parte possiamo vedere che $(1,1),(1,5),(0,1)$ generano $\mathbb{Z}^2$ ma non sono linearmente indipendenti. Quindi, come negli spazi vettoriali, le due nozioni di indipendenza lineare e sistema di generatori sono scorrelate.

Definizione 3.1 *Diciamo che gli elementi $a_1,\ldots,a_s$ di un gruppo G sono una* **base** *di G se l'omomorfismo $\phi : \mathbb{Z}^s \to G$ sopra definito é un isomorfismo, ossia se tali elementi sono un sistema di generatori per G e sono linearmente indipendenti.*

Definizione 3.2 *I gruppi abeliani che ammettono una base sono detti* **gruppi liberi**.

Esempio 3.3 *Il gruppo $\mathbb{Z}^s$ é libero per ogni $s \geq 1$.*

Infatti gli elementi $(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,0,\ldots,0,1)$ sono una base di $\mathbb{Z}^s$ che chiameremo **base canonica** di $\mathbb{Z}^s$.

Dalle considerazioni precedenti, si ha subito che

Proposizione 3.4 *Per un gruppo abeliano G sono fatti equivalenti:*

1) G é libero.

2) G é isomorfo a $\mathbb{Z}^s$ per qualche $s \geq 0$.

Osserviamo che questa proposizione ci dice che ogni gruppo libero é infinito. Quindi $\mathbb{Z}/n\mathbb{Z}$, essendo finito, non é mai un gruppo libero, qualunque sia $n \geq 1$.

É chiaro che un gruppo infinito non é necessariamente libero. Ad esempio il gruppo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ é infinito ma non libero perché in un gruppo libero non ci sono elementi di ordine finito. Ció é conseguenza delle seguenti osservazioni.

Se G é un gruppo abeliano, indicheremo con $T(G)$ il sottoinsieme di G costituito dagli elementi di periodo finito,

$$T(G)=\{a \in G \mid na=0, n>0\}.$$

Proposizione 3.5 *Se G é un gruppo abeliano allora si ha:*

1) $T(G)$ é un suo sottogruppo.

2) Se G é libero allora $T(G)=\{0\}$.

Prova. Se $a,b \in T(G)$ si ha $na=mb=0$ con $n,m>0$. Ma allora $nm(a-b)=0$ e $nm>0$. Quindi $a-b \in T(G)$. Ció prova che $T(G)$ é un sottogruppo di G.

Se poi G é libero e $a_1,\ldots,a_s$ é una sua base, per ogni $a \in T(G)$ possiamo scrivere $a=\sum_{i=1}^{s} n_i a_i$ e quindi, se $na=0$, si ottiene $\sum_{i=1}^{s} nn_i a_i=0$. La indipendenza di

$a_1, \ldots, a_s$ implica allora $nn_i = 0$ per ogni i e quindi, essendo $n > 0$, deve essere $n_i = 0$ per ogni i.

□

Una diversa condizione per avere una base é data dalla seguente proposizione.

Proposizione 3.6 *Gli elementi $a_1, \ldots, a_s$ sono una* **base** *di G se e solo se*

$$G =< a_1 > \oplus < a_2 > \oplus \cdots \oplus < a_s >$$

e inoltre $ord(a_i) = \infty$ per ogni $i = 1, \ldots, s$.

Prova. Sia $a_1, \ldots, a_s$ una base di G; allora G é libero e ogni suo elemento ha periodo infinito. Essendo $a_1, \ldots, a_s$ generatori di G, sappiamo che $G = \sum_{i=1}^{s} < a_i >$. Se fosse $na_i \in < a_i > \cap \sum_{j \neq i} < a_j >$, allora $na_i = \sum_{j \neq i} n_j a_j$ e quindi, per la indipendenza di $a_1, \ldots, a_s$, si avrebbe $n = 0$ e di conseguenza $na_i = 0$. Quindi la somma $G = \sum_{i=1}^{s} < a_i >$ é diretta.

Viceversa, se $G = \oplus_{i=1}^{s} < a_i >$, é chiaro che $a_1, \ldots, a_s$ generano G. Se poi fosse $\sum_{i=1}^{s} n_i a_i = 0$, allora per ogni $i = 1, \ldots, s$ si avrebbe $n_i a_i \in \sum_{j \neq i} < a_j >$ e quindi $n_i a_i = 0$; essendo a_i di ordine infinito, ció implica $n_i = 0$. Dunque gli elementi $a_1, \ldots, a_s$ sono anche linearmente indipendenti. □

Avevamo visto che un gruppo abeliano finitamente generato é sempre la somma di gruppi ciclici. Ora abbiamo visto che un gruppo libero é la somma diretta di gruppi ciclici infiniti. Proveremo che ogni gruppo abeliano finitamente generato é somma diretta di gruppi ciclici (non necessariamente infiniti).

Ad esempio se $G = \mathbb{Z}/6\mathbb{Z}$, é chiaro che

$$G =< \overline{2} > \oplus < \overline{3} >,$$

ma G non é libero e $\overline{2}, \overline{3}$ generano G ma non sono linearmente indipendenti perché $3\ \overline{2} = 2\ \overline{3} = \overline{0}$.

Se G é libero con base $a_1, \ldots, a_s$, ogni elemento $a \in G$ si scrive in modo unico come combinazione lineare $\sum_{i=1}^{s} n_i a_i$ di $a_1, \ldots, a_s$ con coefficienti $n_i \in \mathbb{Z}$. Ossia se $\sum_{i=1}^{s} n_i a_i = \sum_{i=1}^{s} m_i a_i$ e $n_i, m_i \in \mathbb{Z}$, allora $n_i = m_i$ per ogni i. Questo implica che:

Proposizione 3.7 *Sia H un gruppo abeliano e G un gruppo libero con base $a_1, \ldots, a_s$. Fissati gli elementi $w_1, \ldots, w_s$ nel gruppo H, anche non distinti, esiste ed é unico un omomorfismo $\phi : G \to H$ tale che $\phi(a_i) = w_i$ per ogni $i = 1, \ldots, s$.*

Prova. Definiamo $\phi : G \to H$ nel modo seguente: se $a \in G$, possiamo scrivere $a = \sum_{i=1}^{s} n_i a_i$ con $n_i \in \mathbb{Z}$, e allora poniamo

$$\phi(a) := \sum_{i=1}^{s} n_i w_i.$$

Poiché la scrittura $a = \sum_{i=1}^{s} n_i a_i$ é unica, tale applicazione é ben definita. Inoltre é facila vedere che ϕ é omomorfismo di gruppi e che $\phi(a_i) = w_i$. L'unicitá di tale omomorfismo segue dal fatto che se $\psi : G \to H$ é un altro omomorfismo tale che $\psi(a_i) = w_i$ per ogni $i = 1, \dots s$, allora

$$\psi(a) = \psi(\sum_{i=1}^{s} n_i a_i) = \sum_{i=1}^{s} n_i \psi(a_i) = \sum_{i=1}^{s} n_i w_i = \phi(a).$$

□

Notare che se $a_1, \dots, a_s$ generano G ma non sono una base di G, un tale omomorfismo non é detto che esista. Ad esempio se $G = \mathbb{Z}^2$ e $H = \mathbb{Z}$, gli elementi $a_1 = (1,1), a_2 = (1,5), a_3 = (1,3)$ generano $\mathbb{Z}^2$ ma non sono una base di $\mathbb{Z}^2$. Se fissiamo in $\mathbb{Z}$ gli elementi $w_1 = 3$, $w_2 = 2$, $w_3 = -1$, allora non esiste nessun omomorfismo $\phi : \mathbb{Z}^2 \to \mathbb{Z}$ tale che $\phi(a_i) = w_i$ per ogni $i = 1, \dots, 3$. Infatti se tale ϕ esistesse, si avrebbe la contraddizione

$$-2 = 2\phi(a_3) = \phi(2a_3) = \phi(a_1 + a_2) = \phi(a_1) + \phi(a_2) = 5.$$

Si potrebbe pensare che la teoria dei gruppi liberi e quella degli spazi vettoriali siano parallele. Le seguenti osservazioni mostrano che cosí non é.

Osservazione 3.8 *In un gruppo libero non é sempre vero che da un sistema di generatori si possa estrarre una base.*

Ad esempio nel gruppo abeliano $G = 2\mathbb{Z}$ dei numeri pari, gli elementi 4 e 6 sono un sistema di generatori per G, ma né 4 né 6 formano una base.

Osservazione 3.9 *In un gruppo libero non sempre un sistema di elementi linearmente indipendenti si puó estendere ad una base.*

Ad esempio se $G = \mathbb{Z}$, 7 é linearmente indipendente ma non é una base e non puó far parte di una base perché 2 elementi di $\mathbb{Z}$ non sono mai linearmente indipendenti:

$$n(m) - m(n) = 0.$$

Peró siamo capaci di dimostrare che tutte le basi di uno stesso gruppo libero sono equipotenti. Per far ció abbiamo bisogno di un pó di teoria delle matrici ad entrate in $\mathbb{Z}$.

4 Matrici ad elementi in $\mathbb{Z}$

Nell'insieme $M_{m,n}(\mathbb{Z})$ delle matrici di m righe ed n colonne ad entrate in $\mathbb{Z}$, possiamo definire la somma di due matrici al solito modo:

$$\begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ . & . & . & . \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & ... & b_{1n} \\ b_{21} & b_{22} & ... & b_{2n} \\ . & . & . & . \\ b_{m1} & b_{m2} & ... & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & ... & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & ... & a_{2n}+b_{2n} \\ . & . & . & . \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & ... & a_{mn}+b_{mn} \end{pmatrix}$$

La somma é commutativa ed associativa. Possiamo anche definire il prodotto di due matrici X e Y, purché X sia di tipo $m \times n$ e Y di tipo $n \times q$. Il prodotto non é commutativo. É chiaro che se $t \in \mathbb{Z}$ e $X \in M(\mathbb{Z})$si ha

$$t \begin{pmatrix} x_{11} & x_{12} & ... & x_{1n} \\ x_{21} & x_{22} & ... & x_{2n} \\ . & . & . & . \\ x_{m1} & x_{m2} & ... & x_{mn} \end{pmatrix} = \begin{pmatrix} tx_{11} & tx_{12} & ... & tx_{1n} \\ tx_{21} & tx_{22} & ... & tx_{2n} \\ . & . & . & . \\ tx_{m1} & tx_{m2} & ... & tx_{mn} \end{pmatrix}$$

Data la matrice X di tipo $n \times m$, la sua trasposta é quella matrice di tipo $m \times n$ che si ottiene da X sostituendo le righe con le colonne. La trasposta di X si indicherá con ${}^tX$.

É chiaro che data una matrice quadrata $X = (x_{ij}) \in M_n(\mathbb{Z})$, possiamo definire il suo determinante in questo modo:

$$det(X) = \sum_{\sigma} (\pm) x_{1\ \sigma(1)} x_{2\ \sigma(2)} \dots x_{n\ \sigma(n)}$$

ove σ varia nell'insieme delle permutazioni di $\{1, 2, \dots, n\}$.

Dalla definizione segue che $det(X)$ é un elemento di $\mathbb{Z}$ ed é facile provare che le solite proprietá dei determinanti restano valide. In particolare si puó dimostrare il Teorema di Binet che afferma:

Teorema 4.1 *Il determinante del prodotto di due matrici quadrate é uguale al prodotto dei determinanti.*

Al solito modo possiamo definire per una matrice quadrata $X \in M_n(\mathbb{Z})$ la sua aggiunta X^* che é ancora una matrice quadrata dello stesso tipo. Si ha la formula

$$X\ X^* = X^*\ X = det(X) I_n$$

ove I_n é la matrice identica $n \times n$.

Definizione 4.2 *Diciamo che la matrice quadrata $X \in M_n(\mathbb{Z})$ é invertibile se esiste una matrice quadrata $Y \in M_n(\mathbb{Z})$ tale che $XY = YX = I_n$.*

Come sempre si ha:

Proposizione 4.3 *Se X é invertibile allora la sua inversa é unica.*

Si ottiene cosí:

Teorema 4.4 *Se $X \in M_n(\mathbb{Z})$ é una matrice quadrata, allora X é invertibile se e solo se $det(X) = \pm 1$.*

Prova. Se $XY = I_n$, allora $det(X)det(Y) = det(I_n) = 1$ e quindi $det(X)$ é invertibile in $\mathbb{Z}$.

Se invece $det(X) = \pm 1$, allora

$$XX^* = X^*X = \pm I_n$$

e X é invertibile con inversa $\pm X^*$. □

Ad esempio la matrice $\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$ ha determinante diverso da zero ma non é una matrice invertibile in $M_2(\mathbb{Z})$.

5 Matrici elementari

Ci sono matrici invertibili molto importanti che useremo successivamente. Sono le matrici elementari che si definiscono nel modo seguente. Ve ne sono di tre tipi:

1. Matrice $E_{i,j}(n)$, con $i \neq j$ interi positivi e $n \in \mathbb{Z}$. Questa é la matrice che ha tutti 1 sulla diagonale principale e tutti 0 altrove escluso l'elemento di posto (i, j) che é n.

2. Matrice $E_{i,j}$ con $i \neq j$ interi positivi. Questa é la matrice che ha tutti 0 fuori della diagonale principale escluso le posizioni (i, j) e (j, i) ove ha 1, e sulla diagonale principale ha tutti 1 escluso le posizioni (i, i) e (j, j) dove ha 0.

3. Matrice E_i ove i é un intero positivo. Questa é la matrice che é eguale alla matrice identica, solo che nella posizione (i, i) ha -1.

Ad esempio le matrici elementari 2×2 sono

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

al variare di $n \in \mathbb{Z}$.

Sia X una matrice $t \times s$, Y una matrice $r \times t$ e supponiamo che $E_{i,j}(n)$, $E_{i,j}$, E_i siano matrici elementari $t \times t$. Allora:

Lemma 5.1 *1) La matrice $E_{i,j}(n)X$ é la matrice che si ottiene da X aggiungendo alla riga i la riga j moltiplicata per n, mentre $YE_{i,j}(n)$ é la matrice che si ottiene da Y aggiungendo alla colonna j la colonna i moltiplicata per n.*

2) La matrice $E_{i,j}X$ é la matrice che si ottiene da X scambiando la riga i con la riga j, mentre $YE_{i,j}$ é la matrice che si ottiene operando allo stesso modo sulle colonne.

3) Infine E_iX é la matrice che si ottiene da X moltiplicando la riga i per -1, mentre YE_i é quella che si ottiene da Y moltiplicando la colonna i per -1.

Lemma 5.2 *Tutte le matrici elementari sono invertibili, e infatti la inversa di $E_{i,j}(n)$ é la matrice $E_{i,j}(-n)$, mentre $E_{i,j}$ e E_i sono inverse di se stesse.*

Facciamo qualche esempio. Sia

$$X = \begin{pmatrix} 1 & -1 & 2 & 3 \\ 2 & 0 & 1 & 0 \\ 3 & 4 & 0 & -5 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Allora

$$E_2X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 2 & 3 \\ 2 & 0 & 1 & 0 \\ 3 & 4 & 0 & -5 \\ 1 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 2 & 3 \\ -2 & 0 & -1 & 0 \\ 3 & 4 & 0 & -5 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$XE_2 = \begin{pmatrix} 1 & -1 & 2 & 3 \\ 2 & 0 & 1 & 0 \\ 3 & 4 & 0 & -5 \\ 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 & 3 \\ 2 & 0 & 1 & 0 \\ 3 & -4 & 0 & -5 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$E_{2,3}(-7) \begin{pmatrix} 2 & -1 & 3 \\ 0 & 1 & 4 \\ -5 & 2 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -7 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & -1 & 3 \\ 0 & 1 & 4 \\ -5 & 2 & 6 \end{pmatrix} = \begin{pmatrix} 2 & -1 & 3 \\ 35 & -13 & -38 \\ -5 & 2 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 & 4 \\ -5 & 1 & 0 \end{pmatrix} E_{2,3}(-7) = \begin{pmatrix} 2 & 1 & 4 \\ -5 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -7 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & -3 \\ -5 & 1 & -7 \end{pmatrix}$$

Avremo bisogno anche di questa definizione.

Definizione 5.3 *Se $A \in M_{r,s}(\mathbb{Z})$, diciamo che A é* **invertibile a destra** *se esiste una matrice $B \in M_{s,r}(\mathbb{Z})$ tale che $AB = I_r$.*

Diremo che A é **invertibile a sinistra** *se esiste una matrice $C \in M_{s,r}(\mathbb{Z})$ tale che $CA = I_s$.*

L'eventuale inversa destra (o sinistra) di una matrice A non sono necessariamente uniche. Ad esempio:

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ -3 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

6 Basi diverse di un gruppo libero

Supponiamo di avere un sistema di generatori di un gruppo G, siano $e_1, e_2, \ldots, e_s$. Se $v_1, \ldots, v_t$ sono elementi di G, allora possiamo scrivere per ogni $i = 1, \ldots, t$

$$v_i = \sum_{j=1}^{s} n_{ji} e_j$$

con $n_{ji} \in \mathbb{Z}$. Se si introduce la matrice $A := (n_{ij})$ che é di tipo $s \times t$, possiamo chiaramente compendiare questa scrittura con la notazione

$$(v_1, \ldots, v_t) = (e_1, e_2, \ldots, e_s)A.$$

Osservazione 6.1 *Fare attenzione che abbiamo moltiplicato una matrice di elementi di G con una matrice di interi: non si potrá peró moltiplicare una matrice di elementi di G con una altra di elementi di G.*

Ad esempio la notazione

$$(v_1, v_2, v_3) = (e_1, e_2) \begin{pmatrix} 2 & -3 & 5 \\ 4 & 7 & -5 \end{pmatrix}$$

significa

$$v_1 = 2e_1 + 4e_2,\ v_2 = -3e_1 + 7e_2,\ v_3 = 5e_1 - 5e_2.$$

Possiamo allora dimostrare il seguente risultato:

Teorema 6.2 *Sia G un gruppo libero e siano $e_1, \ldots, e_s$ una base di G. Siano poi $v_1, \ldots, v_t$ elementi di G; possiamo scrivere $(v_1, \ldots, v_t) = (e_1, e_2, \ldots, e_s)A$ ove A é una matrice in $M_{s,t}(\mathbb{Z})$. Allora*

$v_1, \ldots, v_t$ generano $G \iff A$ é invertibile a destra $\implies t \geq s$.

Prova. É chiaro che $v_1, \ldots, v_t$ generano G se e solo se $e_1, \ldots, e_s \in < v_1, \ldots, v_t >$, ossia se e solo se esiste una matrice $B \in M_{t,s}(\mathbb{Z})$ tale che

$$(e_1, e_2, \ldots, e_s) = (v_1, \ldots, v_t)B.$$

Quindi se $v_1, \ldots, v_t$ generano G si ha:

$$(e_1, e_2, \ldots, e_s) = (v_1, \ldots, v_t)B = (e_1, e_2, \ldots, e_s)AB.$$

Per la indipendenza di $e_1, e_2, \ldots, e_s$ ció implica $AB = I_s$ e quindi A é invertibile a destra.

Se viceversa A é invertibile a destra, allora $AB = I_s$ con $B \in M_{t,s}(\mathbb{Z})$ e quindi

$$(e_1, e_2, \ldots, e_s) = (e_1, e_2, \ldots, e_s)I_s = (e_1, e_2, \ldots, e_s)AB = (v_1, \ldots, v_t)B.$$

Ció prova che $v_1, \ldots, v_t$ generano G.

Sia ora A invertibile a destra, e sia $AB = I_s$ con $B \in M_{t,s}(\mathbb{Z})$. Se per assurdo si avesse $t < s$, consideriamo la matrice A' ottenuta da A completandola con delle colonne di 0 ad una matrice quadrata $s \times s$ e la matrice B' ottenuta da B completandola con delle righe di 0 ad una matrice quadrata $s \times s$. É chiaro che si ha

$$A'B' = AB = I_s.$$

Ció implica che $det(A')$ é invertibile, ma questo é assurdo perché A' ha almeno una riga di 0, e quindi il suo determinante é 0. □

É chiaro che la implicazione "$t \geq s \Longrightarrow v_1, \ldots, v_t$ generano G" non vale: se si considera $v_1 = (1,1), v_2 = (2,2), v_3 = (3,3) \in G = \mathbb{Z}^2$, questi 3 elementi non generano G.

Corollario 6.3 *Due basi di un gruppo libero G sono equipotenti.*

Prova. Siano $e_1, \ldots, e_s$ e $a_1, \ldots, a_t$ basi di G. Applicando il teorema precedente alle due basi a ruoli invertiti, si ha $t \geq s$, e $s \geq t$. □

La cardinalitá di una gruppo libero G non dipende dunque dalla base scelta e quindi é un invariante di G. Lo chiameremo il **rango** di G e lo indicheremo con $rg(G)$. Ad esempio $rg(\mathbb{Z}^s) = s$.

Come conseguenza del teorema precedente si ha:

Corollario 6.4 *Se si ha un isomorfismo $\phi : \mathbb{Z}^s \to \mathbb{Z}^t$, allora $t = s$.*

Corollario 6.5 *Se si ha un epimorfismo $\phi : \mathbb{Z}^s \to \mathbb{Z}^t$, allora $t \geq s$.*

Osserviamo che se G é un gruppo libero di rango s, é possibile che G possieda un sottogruppo libero H di rango s che non coincide con G.

Ad esempio $\mathbb{Z}$ é libero di rango 1 e il sottogruppo H dei numeri pari non coincide con G ed é libero di rango 1.

Un altro importante risultato é il seguente.

Teorema 6.6 *Sia G un gruppo libero e siano $e_1, \ldots, e_s$ una base di G. Siano poi $v_1, \ldots, v_t$ elementi di G; possiamo scrivere $(v_1, \ldots, v_t) = (e_1, e_2, \ldots, e_s)A$ ove A é una matrice in $M_{s,t}(\mathbb{Z})$. Allora*

A é invertibile a sinistra $\Longrightarrow v_1, \ldots, v_t$ sono linearmente indipendenti.

Prova. Supponiamo di avere $\sum_{i=1}^{t} n_i v_i = 0$. Allora possiamo scrivere in forma matriciale

$$0 = (v_1, \ldots, v_t) \begin{pmatrix} n_1 \\ \vdots \\ n_t \end{pmatrix} = (e_1, \ldots, e_s)A \begin{pmatrix} n_1 \\ \vdots \\ n_t \end{pmatrix}.$$

Poiché $e_1, \ldots, e_s$ sono linearmente indipendenti, ció implica

$$A \begin{pmatrix} n_1 \\ \vdots \\ n_t \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Ma esiste $B \in M_{t,s}(\mathbb{Z})$ tale che $BA = I_t$ e quindi si ottiene

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = BA \begin{pmatrix} n_1 \\ \vdots \\ n_t \end{pmatrix} = I_t \begin{pmatrix} n_1 \\ \vdots \\ n_t \end{pmatrix} = \begin{pmatrix} n_1 \\ \vdots \\ n_t \end{pmatrix}.$$

Dunque $n_1 = n_2 = \cdots = n_t = 0$, come volevasi. □

É chiaro che la implicazione "$v_1, \ldots, v_t$ sono linearmente indipendenti $\Longrightarrow$ A é invertibile a sinistra" non vale. Sia $v = (2, 0) \in \mathbb{Z}^2$, ed e_1, e_2 la base canonica di $\mathbb{Z}^2$. Allora

$$v = 2e_1 = (e_1, e_2) \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Ora v é linearmente indipendente, ma la matrice $\begin{pmatrix} 2 \\ 0 \end{pmatrix}$ non ha inversa a sinistra: se infatti $(n, m) \begin{pmatrix} 2 \\ 0 \end{pmatrix} = 1$, si avrebbe $2n = 1$, impossibile in $\mathbb{Z}$.

Possiamo ora dimostrare il seguente teorema che illustra come ottenere tutte le basi di un gruppo libero, a partire dalla conoscenza di una base fissata.

Teorema 6.7 *Sia $e_1, \ldots, e_s$ una base di G e $(v_1, \ldots, v_s) = (e_1, \ldots, e_s)A$ ove A é una matrice in $M_s(\mathbb{Z})$.*

Allora sono equivalenti:

1) A é invertibile.
2) $v_1, \ldots, v_s$ é base di G.
3) $v_1, \ldots, v_s$ generano G.

Prova. Se A e' invertibile, allora e' invertibile a destra e a sinistra e quindi $v_1, \ldots, v_s$ sono linearmente indipendenti e sistema di generatori per G. Ció prova che 1) implica 2). Resta solo da provare che 3) implica 1). Ció segue dal fatto che se una matrice quadrata A é invertibile a destra, $AB = I_s$, allora $det(A) = \pm 1$ e quindi A é invertibile. □

Se in particolare $G = \mathbb{Z}^n$, si consideri la base canonica $e_1, \ldots, e_n$ di G ed elementi $v_1, \ldots, v_n \in G$. Allora é chiaro che $(v_1, \ldots, v_n) = (e_1, \ldots, e_n)A$ ove A é la matrice che ha come colonne le coordinate di $v_1, \ldots, v_n$. Quindi $v_1, \ldots, v_n$ sono una base di $\mathbb{Z}^n$ se e solo se la matrice delle loro coordinate ha determinante ± 1.

Ad esempio $v_1 = (2,1), v_2 = (3,1)$ sono una base di $\mathbb{Z}^2$ perché

$$det \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix} = -1.$$

7 Sottogruppi e quozienti di un gruppo libero

I sottogruppi di $\mathbb{Z}$ sono del tipo $n\mathbb{Z}$ per qualche $n \geq 0$. Quindi, quelli non nulli, sono tutti liberi di rango 1. Proveremo ora che ogni sottogruppo di un gruppo libero di rango n e ' anche lui libero di rango $m \leq n$.

Iniziamo a provare che ogni sottogruppo di un gruppo libero di rango n e' finitamente generato. Bastera' naturalmente provare il risultato per i sottogruppi di $\mathbb{Z}^n$.

Teorema 7.1 *I sottogruppi di $\mathbb{Z}^n$ sono finitamente generati.*

Prova. Se $n = 1$ i sottogruppi di $\mathbb{Z}$ sono del tipo $n\mathbb{Z}$ e quindi sono finitamente generati. Dimostriamo il teorema per induzione su n. Sia $n \geq 2$ e consideriamo la proiezione

$$\pi : \mathbb{Z}^n \to \mathbb{Z}^{n-1}$$

definita da $\pi(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1})$.

E' chiaro che π e' surgettiva e che $Ker(\pi) = \{(0, \ldots, 0, a_n)\} \simeq \mathbb{Z}$. Se consideriamo la restrizione ad H di π, sia $f : H \to \mathbb{Z}^{n-1}$, allora $Im(f)$ e' finitamente generato per l'ipotesi induttiva e $Ker(f) = Ker(\pi) \cap H$ e' un sottogruppo di $\mathbb{Z}$ e quindi finitamente generato. Se $Im(f) =< w_1, \ldots, w_r >$ e $Ker(f) =< v_1, \ldots, v_s >$, si ha facilmente $H =< v_1, \ldots, v_s, z_1, \ldots, z_r >$ ove $w_i = f(z_i)$. □

Per provare che i sottogruppi di $\mathbb{Z}^n$ sono liberi, lo strumento essenziale e' il seguente teorema sulla diagonalizzazione delle matrici intere.

Teorema 7.2 *Sia A una matrice $s \times t$ ad entrate in $\mathbb{Z}$. Allora esistono matrici U e V prodotto di matrici elementari, tali che $UAV = \Delta$ ove Δ e' una matrice diagonale che ha interi non negativi $d_1, \ldots, d_r$, $r = min(s,t)$, sulla diagonale principale e 0 altrove.*

Prova. Per la dimostrazione di questo risultato vedere il libro di Artin a pagina 541. □

Vediamo su esempi concreti come procedere con operazioni elementari per trasformare una matrice data in una matrice diagonale.

$$A = \begin{pmatrix} 3 & 4 \\ 2 & -5 \end{pmatrix} \overset{E_{1,2}(-1)}{\longrightarrow} \begin{pmatrix} 1 & 9 \\ 2 & -5 \end{pmatrix} \overset{E_{2,1}(-2)}{\longrightarrow} \begin{pmatrix} 1 & 9 \\ 0 & -23 \end{pmatrix} \underset{E_{1,2}(-9)}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & -23 \end{pmatrix} \overset{}{\underset{E_2}{\longrightarrow}} \begin{pmatrix} 1 & 0 \\ 0 & 23 \end{pmatrix}$$

$$A = \begin{pmatrix} 6 & 2 \\ 3 & 8 \end{pmatrix} \underset{E_{1,2}}{\longrightarrow} \begin{pmatrix} 2 & 6 \\ 8 & 3 \end{pmatrix} \overset{E_{2,1}(-4)}{\longrightarrow} \begin{pmatrix} 2 & 6 \\ 0 & -21 \end{pmatrix} \underset{E_{1,2}(-3)}{\longrightarrow} \begin{pmatrix} 2 & 0 \\ 0 & -21 \end{pmatrix} \underset{E_2}{\longrightarrow} \begin{pmatrix} 2 & 0 \\ 0 & 21 \end{pmatrix}$$

Ma anche

$$A = \begin{pmatrix} 6 & 2 \\ 3 & 8 \end{pmatrix} \overset{E_{1,2}(-2)}{\longrightarrow} \begin{pmatrix} 0 & -14 \\ 3 & 8 \end{pmatrix} \overset{E_{1,2}(1)}{\longrightarrow} \begin{pmatrix} 3 & -6 \\ 3 & 8 \end{pmatrix} \overset{E_{2,1}(-1)}{\longrightarrow} \begin{pmatrix} 3 & -6 \\ 0 & 14 \end{pmatrix} \underset{E_{1,2}(2)}{\longrightarrow} \begin{pmatrix} 3 & 0 \\ 0 & 14 \end{pmatrix}$$

e si trova una matrice diagonale diversa!

$$A = \begin{pmatrix} 21 & 14 \\ 3 & 2 \\ 6 & 4 \end{pmatrix} \overset{E_{3,2}(-2)}{\longrightarrow} \begin{pmatrix} 21 & 14 \\ 3 & 2 \\ 0 & 0 \end{pmatrix} \overset{E_{1,2}(-7)}{\longrightarrow} \begin{pmatrix} 0 & 0 \\ 3 & 2 \\ 0 & 0 \end{pmatrix} \overset{E_{1,2}}{\longrightarrow} \begin{pmatrix} 3 & 2 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 3 & 2 \\ 1 & -4 \\ 5 & 1 \end{pmatrix} \overset{E_{1,2}}{\longrightarrow} \begin{pmatrix} 1 & -4 \\ 3 & 2 \\ 5 & 1 \end{pmatrix} \overset{E_{2,1}(-3)}{\longrightarrow} \begin{pmatrix} 1 & -4 \\ 0 & 14 \\ 5 & 1 \end{pmatrix} \overset{E_{3,1}(-5)}{\longrightarrow} \begin{pmatrix} 1 & -4 \\ 0 & 14 \\ 0 & 21 \end{pmatrix} \underset{E_{1,2}(4)}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 14 \\ 0 & 21 \end{pmatrix}$$

$$\overset{E_{3,2}(-1)}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 14 \\ 0 & 7 \end{pmatrix} \overset{E_{2,3}(-2)}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 7 \end{pmatrix} \overset{E_{2,3}}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 7 \\ 0 & 0 \end{pmatrix}$$

Notiamo esplicitamente che il teorema ci indica un modo per giungere alla diagonalizzazione della matrice data; naturalmente il procedimento non é unico e abbiamo visto negli esempi che, seguendo procedimenti diversi, si puó giungere a matrici diagonali diverse. Vedremo nel seguito cosa abbiano in comune tali matrici, ma per il momento facciamo un altro esempio interessante. Sia

$$A = \begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$$

e sia d il massimo comun divisore tra n e m e c il loro minimo comune multiplo. Allora possiamo scrivere $n = da, \quad m = db$ ove a e b sono interi primi tra loro. Ne segue che per qualche $x, y \in \mathbb{Z}$ si ha $1 = ax + by$ e quindi $d = nx + my$. Si ha cosi'

$$\begin{pmatrix} x & y \\ -b & a \end{pmatrix} \begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} \begin{pmatrix} 1 & -by \\ 1 & ax \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix}.$$

Quindi $\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$ e $\begin{pmatrix} d & 0 \\ 0 & e \end{pmatrix}$ sono due diverse forme diagonali della stessa matrice.

Una semplice applicazione del teorema di diagonalizzazione prova che ogni sottogruppo di $\mathbb{Z}^n$ e' libero con base formata dai "multipli" di una opportuna base di $\mathbb{Z}^n$.

Teorema 7.3 *Sia H un sottogruppo non banale di $\mathbb{Z}^n$. É possibile determinare una base $e_1, \ldots, e_n$ di $\mathbb{Z}^n$, un intero $t \leq n$ ed interi $d_1, \ldots, d_t > 0$, tali che $d_1 e_1, \ldots, d_t e_t$ e' una base di H.*

Prova. Sia $v_1, \ldots, v_s$ base di $\mathbb{Z}^n$; per il teorema 7.1 H e' finitamente generato e allora siano $w_1, \ldots, w_r$ generatori di H. Potremo scrivere

$$(w_1, \ldots, w_r) = (v_1, \ldots, v_n)A$$

dove $A \in M_{n,r}(\mathbb{Z})$. Per il teorema precedente possiamo determinare due matrici invertibili $U \in M_n(\mathbb{Z})$ e $V \in M_r(\mathbb{Z})$ ed interi positivi $d_1, \ldots, d_t$, $t \leq min(n, r)$, tali che

$$UAV = \Delta = \begin{pmatrix} d_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & d_t & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Allora si ha

$$(w_1, \ldots, w_r)V = (v_1, \ldots, v_n)AV = (v_1, \ldots, v_n)U^{-1}\Delta.$$

Siccome U^{-1} é invertibile, il Teorema 6.7 ci assicura che gli elementi $(e_1, \ldots, e_n) := (v_1, \ldots, v_n)U^{-1}$ sono un base di G. Sostituendo si ottiene

$$(w_1, \ldots, w_r)V = (e_1 d_1, \ldots, e_t d_t, 0, \ldots, 0).$$

Ne segue che $e_1 d_1, \ldots, e_t d_t \in H$ ed infatti, essendo V invertibile, tali elementi sono generatori di H. Resta da provare che sono linearmente indipendenti. Ma se fosse $\sum_{i=1}^{t} n_i e_i d_i = 0$, allora per ogni i sarebbe $n_i d_i = 0$ e quindi $n_i = 0$ perche' $d_i > 0$.

□

Notiamo che, nel precedente teorema, la nuova base di G é determinata dalla matrice U^{-1}. Quindi, nel procedere, **dobbiamo solo ricordarci delle operazioni sulle righe che sono state compiute nel processo di diagonalizzazione**. Infatti le operazioni sulle righe corrispondono alla moltiplicazione a sinistra per matrici elementari e quindi sono quelle che determinano U (vedi Lemma 5.1).

Facciamo un esempio. Sia $G = \mathbb{Z}^3$ e $H =< (3, 1, 5), (2, -4, 1) >$. Se si considera la base canonica di $\mathbb{Z}^3$ che indichiamo con v_1, v_2, v_3, si ha:

$$((3, 1, 5), (2, -4, 1)) = (v_1, v_2, v_3) \begin{pmatrix} 3 & 2 \\ 1 & -4 \\ 5 & 1 \end{pmatrix}$$

Abbiamo visto che esistono matrici invertibili $U \in M_3(\mathbb{Z})$ e $V \in M_2(\mathbb{Z})$ tali che

$$U \begin{pmatrix} 3 & 2 \\ 1 & -4 \\ 5 & 1 \end{pmatrix} V = \begin{pmatrix} 1 & 0 \\ 0 & 7 \\ 0 & 0 \end{pmatrix}$$

Quindi $d_1 = 1, d_2 = 7$. La nuova base di $\mathbb{Z}^3$ é

$$(e_1, e_2, e_3) := (v_1, v_2, v_3)U^{-1}.$$

Si ha

$$U = E_{2,3}E_{2,3}(-2)E_{3,2}(-1)E_{3,1}(-5)E_{2,1}(-3)E_{1,2}$$

e quindi

$$U^{-1} = E_{1,2}E_{2,1}(3)E_{3,1}(5)E_{3,2}(1)E_{2,3}(2)E_{2,3}.$$

Ricordandosi come le matrici elementari operano per moltiplicazione a destra (vedi Lemma 5.1), si ottiene:

$$(v_1, v_2, v_3) \xrightarrow{E_{1,2}} (v_2, v_1, v_3) \xrightarrow{E_{2,1}(3)} (v_2 + 3v_1, v_1, v_3)$$

$$\xrightarrow{E_{3,1}(5)} (v_2 + 3v_1 + 5v_3, v_1, v_3) \xrightarrow{E_{3,2}(1)} (3v_1 + v_2 + 5v_3, v_1 + v_3, v_3)$$

$$\xrightarrow{E_{2,3}(2)} (3v_1 + v_2 + 5v_3, v_1 + v_3, v_3 + 2v_1 + 2v_3) \xrightarrow{E_{2,3}} (3v_1 + v_2 + 5v_3, 2v_1 + 3v_3, v_1 + v_3).$$

Quindi la nuova base di $\mathbb{Z}^3$ é

$$e_1 = (3, 1, 5),\ e_2 = (2, 0, 3), e_3 = (1, 0, 1),$$

quella di H é

$$e_1 = (3, 1, 5),\ 7e_2 = (14, 0, 21).$$

Notare che si ha

$$(14, 0, 21) = 4(3, 1, 5) + (2, -4, 1)$$

che conferma

$$H =< (3, 1, 5), (2, -4, 1) >=< (3, 1, 5), (14, 0, 21) > .$$

Una altra applicazione del teorema precedente si ha quando si voglia determinare una base di un sottogruppo di $\mathbb{Z}^n$.

Ad esempio sia H l'immagine dell'omomorfismo

$$f : \mathbb{Z}^3 \to \mathbb{Z}^2$$

definito da $f(a, b, c) = (2a - 5b + 4c, 4a + 3b + 6c)$. E' chiaro che H e' generato da $(2, 4), (-5, 3), (4, 6)$. Determiniamo una base di H.

Seguendo il procedimento usato nella dimostrazione del teorema, si ha:

$$((2,4),(-5,3),(4,6)) = (v_1, v_2)\begin{pmatrix} 2 & -5 & 4 \\ 4 & 3 & 6 \end{pmatrix}$$

ove abbiamo indicato con v_1, v_2 la base canonica di $\mathbb{Z}^2$.

Diagonalizziamo la matrice

$$\begin{pmatrix} 2 & -5 & 4 \\ 4 & 3 & 6 \end{pmatrix} \overset{E_{12}}{\to} \begin{pmatrix} 4 & 3 & 6 \\ 2 & -5 & 4 \end{pmatrix} \to \begin{pmatrix} 1 & 3 & 6 \\ 7 & -5 & 4 \end{pmatrix} \overset{E_{21}(-7)}{\to} \begin{pmatrix} 1 & 3 & 6 \\ 0 & -26 & -38 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 26 & 38 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 26 & 12 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 12 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

Si ha $U = E_{21}(-7)E_{12}$ e quindi $U^{-1} = E_{12}E_{21}(7)$ da cui si deduce la nuova base di $\mathbb{Z}^2$

$$(v_1, v_2)E_{12}E_{21}(7) = (v_2, v_1)E_{21}(7) = (v_2 + 7v_1, v_1) = ((7,1),(1,0)).$$

Quindi la base di H e' $(7,1), 2(1,0)$ ossia $(7,1),(2,0)$.

Corollario 7.4 *Ogni sottogruppo di un gruppo libero di rango n e' libero di rango $t \leq n$.*

Questo importante risultato ha due conseguenze rilevanti.

Proposizione 7.5 *Se $\phi : \mathbb{Z}^r \to \mathbb{Z}^s$ é un omomorfismo iniettivo di gruppi, allora $r \leq s$.*

Proposizione 7.6 *Un sistema lineare omogeneo di s equazioni in t incognite a coefficienti in $\mathbb{Z}$ ha sempre una soluzione non banale in $\mathbb{Z}^t$ se $s < t$.*

Prova. Dato il sistema

$$\sum_{j=1}^{t} n_{ij}x_j = 0$$

$i = 1, \ldots, s$, consideriamo in $\mathbb{Z}^s$ gli elementi

$$v_i = (n_{1i}, n_{2i}, \ldots, n_{si})$$

per $i = 1, \ldots, t$ e sia G il sottogruppo di $\mathbb{Z}^s$ generato da $v_1, \ldots, v_t$. Necessariamente $v_1, \ldots, v_t$ sono linearmente dipendenti, altrimenti G sarebbe libero di rango $t > s$, contro il corollario precedente. Dunque esistono interi non tutti nulli $m_1, \ldots, m_t$ tali che $0 = \sum_{j=1}^{t} m_j v_j$. Ne segue

$$0 = \sum_{j=1}^{t} m_j(\sum_{i=1}^{s} n_{ij}e_i) = \sum_{i=1}^{s}(\sum_{j=1}^{t} m_j n_{ij})e_i$$

e quindi $\sum_{j=1}^{t} n_{ij}m_j = 0$ per ogni $i = 1, \ldots, s$.

□

Siamo ora in grado di provare che il quoziente di un gruppo libero di rango finito con un suo sottogruppo e' somma diretta di gruppi ciclici.

Proposizione 7.7 *Se G e' un gruppo libero di rango n e H e' un suo sottogruppo, allora G/H e' somma diretta di gruppi ciclici.*

Prova. Per il Teorema 7.3 esiste una base $e_1, \ldots, e_n$ di G, un intero $t \leq n$ e interi positivi $d_1, \ldots, d_t$ tali che $d_1e_1, \ldots, d_te_t$ e' una base di H.

Consideriamo allora G/H e proviamo che e' somma diretta dei sottogruppi ciclici generati dagli $\overline{e}_i$, ossia

$$G/H = \oplus_{i=1}^{n} < \overline{e}_i > .$$

Siccome chiaramente tali elementi generano G/H, si ha $G/H = \sum_{i=1}^{n} < \overline{e}_i > .$ Per provare che la somma é diretta, sia $n\overline{e}_i \in \sum_{j\neq i} < \overline{e}_j > .$ Allora $n\overline{e}_i = \sum_{j\neq i} n_j\overline{e}_j$ e quindi $ne_i - \sum_{j\neq i} n_je_j \in H$. Questo implica

$$ne_i - \sum_{j\neq i} n_je_j = \sum_{r=1}^{t} m_rd_re_r.$$

Usando la indipendenza di $e_1, \ldots, e_s$ si ottiene $n = 0$ se $i > t$, $n = m_id_i$ se $i \leq t$. Quindi $ne_i = 0$ oppure $ne_i = m_i(d_ie_i) \in H$. In ogni caso $\overline{ne_i} = n\overline{e}_i = \overline{0}$. Ció prova che la somma $\sum_{i=1}^{s} < \overline{e}_i >$ é diretta. □

Osservazione 7.8 *Osserviamo che nella proposizione precedente il gruppo ciclico $< \overline{e}_i >$ ha rango d_i se $i \leq t$ mentre ha rango infinito se $i > t$. Quindi si avra'*

$$G/H \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z} \times \mathbb{Z}^{n-t}.$$

Infatti sia n un intero positivo tale che $n\overline{e}_i = \overline{0}$. Allora $ne_i = \sum_{j=1}^{t} n_j(d_je_j)$; se $i \leq t$, ció avviene se e solo se $n = n_id_i$, mentre, se $i > t$, ció avviene se e solo se $n = 0$. Quindi, se $i > t$, $\overline{e_i}$ ha ordine infinito. Se $i \leq t$, l'ordine di $\overline{e_i}$ é d_i perché $d_ie_i \in H$ e quindi $d_i\overline{e_i} = \overline{d_ie_i} = \overline{0}$, e d'altra parte si é visto che, nel caso $i \leq t$, se $n\overline{d_i} = \overline{0}$, allora $n = n_id_i \geq d_i$. Si ha dunque $< \overline{e_i} > \simeq \mathbb{Z}/d_i\mathbb{Z}$ se $i \leq t$, $< \overline{e_i} > \simeq \mathbb{Z}$ se $i > t$. Cio' prova l'isomorfismo

$$G/H \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z} \times \mathbb{Z}^{n-t}.$$

Avendo giá osservato che il risultato della diagonalizzazione della matrici intere non e' unico, rimarchiamo che anche gli interi d_i nella osservazione precedente non sono univocamente determinati. Discuteremo in seguito di questo problema di non unicitá.

Infine osserviamo che nella descrizione precedente qualche d_i puó essere uguale ad 1. In tal caso $\overline{e_i}$ ha ordine 1 e quindi $\overline{e_i} = \overline{0}$ e quindi tale addendo non porta contributo nella somma diretta e si puó cancellare.

Se ad esempio $G = \mathbb{Z}^2$ e $H =< (3,0),(0,1) >$, allora $H =< 3e_1, e_2 >$ e quindi

$$G/H =< \overline{e_1} > \oplus < \overline{e_2} >=< \overline{e_1} >\simeq \mathbb{Z}/3\mathbb{Z}.$$

8 Il Teorema di struttura per i gruppi abeliani finitamente generati.

Possiamo ora dimostrare che ogni gruppo abeliano finitamente generato é la somma diretta di un numero finito di sottogruppi ciclici.

Teorema 8.1 *Sia G un gruppo abeliano finitamente generato. Allora G é la somma diretta di un numero finito di sottogruppi ciclici.*

Prova. Sia infatti $v_1, \ldots, v_n$ un sistema di generatori di G. Allora si ha un epimorfismo canonico

$$\phi : \mathbb{Z}^n \to G$$

definito da $\phi(a_1, \ldots, a_n) = \sum_{i=1}^n a_i v_i$. Un tale epimorfismo si dirá **una presentazione** di G. Per il primo teorema di omomorfismo si ha

$$\mathbb{Z}^n/Ker(\phi) \simeq G$$

ove l'isomorfismo é quello che manda $\overline{v}$ in $\phi(v)$.

Se $Ker(\phi) = \{0\}$, $v_1, \ldots, v_n$ sono una base di G che é quindi somma diretta di sottogruppi ciclici infiniti (Proposizione 3.6).

Se invece $Ker(\phi) \neq \{0\}$, allora $Ker(\phi)$ é un sottogruppo libero di $\mathbb{Z}^n$ di rango $1 \leq t \leq n$. Per la Proposizione 7.7 esiste una base $e_1, \ldots, e_n$ di $\mathbb{Z}^n$ e interi positivi $d_1, \ldots, d_t$, tali che $d_1 e_1, \ldots, d_t e_t$ é base di $Ker(\phi)$.

Inoltre

$$\mathbb{Z}^n/Ker(\phi) =< \overline{e_1} > \oplus < \overline{e_2} > \oplus \cdots \oplus < \overline{e_n} >$$

con

$$ord(\overline{e_i}) = \begin{cases} d_i & i \leq t \\ \infty & i \geq t+1. \end{cases}$$

Ne segue

$$G =< \phi(e_1) > \oplus < \phi(e_2) > \oplus \cdots \oplus < \phi(e_n) >$$

ove

$$ord(\phi(e_i)) = \begin{cases} d_i & i \leq t \\ \infty & i \geq t+1. \end{cases}$$

□

Osserviamo che se nel teorema precedente poniamo

$$L :=< a_{t+1} > \oplus < a_{t+2} > \oplus \cdots \oplus < a_n >,$$

allora L é un sottogruppo libero di G di rango $n-t$ e quindi $L \simeq \mathbb{Z}^{n-t}$. Inoltre, se $i \leq t$, si ha $< \phi(e_i) > \simeq \mathbb{Z}/d_i\mathbb{Z}$ e quindi per la Proposizione 2.7 si ha:

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z} \times \mathbb{Z}^{n-t}.$$

Esempio. Consideriamo il gruppo libero $G = \mathbb{Z}^2$ e sia H il sottogruppo di G generato da $(3,2)$ e $(4,-5)$. Vogliamo decomporre il gruppo G/H come somma diretta di gruppi ciclici.

Si ha:

$$((3,2),(4,-5)) = ((1,0),(0,1)) \begin{pmatrix} 3 & 4 \\ 2 & -5 \end{pmatrix}.$$

Diagonalizziamo la matrice:

$$\begin{pmatrix} 3 & 4 \\ 2 & -5 \end{pmatrix} \overset{E_{1,2}(-1)}{\longrightarrow} \begin{pmatrix} 1 & 9 \\ 2 & -5 \end{pmatrix} \overset{E_{2,1}(-2)}{\longrightarrow} \begin{pmatrix} 1 & 9 \\ 0 & -23 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -23 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 23 \end{pmatrix}$$

Dunque si ha $d_1 = 1$, $d_2 = 23$, e se scegliamo come nuova base di G i vettori

$$(e_1, e_2) := ((1,0),(0,1))U^{-1} = ((3,2),(1,1)),$$

la base cercata di H é $\{d_1e_1, d_2e_2\} = \{e_1, 23e_2\} = \{(3,2),(23,23)\}$. Si ha dunque

$$G/H =< \overline{e_1} > \oplus < \overline{e_2} >$$

con $ord(\overline{e_1}) = 1$, $ord(\overline{e_2}) = 23$. Dunque

$$G/H =< \overline{e_2} > =< \overline{(1,1)} > \simeq \mathbb{Z}/23\mathbb{Z}.$$

Esempio. Sia G il sottogruppo di $\mathbb{Z}^2$ generato da $(5,12),(3,10),(2,14)$. Vogliamo determinare una base di G, che é sicuramente libero in quanto abbiamo visto che ogni sottogruppo di un gruppo libero é libero. Il procedimento che seguiamo ora e' diverso da quello seguito nell'esempio che precede il Corollario 7.4.

Si ha una presentazione

$$\phi : \mathbb{Z}^3 \to G$$

ove ϕ é definito cosí:

$$\phi(a,b,c) = a(5,12) + b(3,10) + c(2,14).$$

Cerchiamo una base di $Ker(\phi)$. Dobbiamo risolvere il sistema

$$\begin{cases} 5a + 3b + 2c & = 0 \\ 12a + 10b + 14c & = 0. \end{cases}$$

Si vede facilmente che una base di $Ker(\phi)$ é il vettore $(-11, 23, -7)$. Si completa subito questo elemento ad una matrice invertibile

$$\begin{pmatrix} -11 & -1 & 0 \\ 23 & 2 & 0 \\ -7 & 0 & 1 \end{pmatrix}$$

e quindi gli elementi $e_1 = (-11, 23, -7), e_2 = (-1, 2, 0), e_3 = (0, 0, 1)$ sono una base di $\mathbb{Z}^3$ tale che e_1 é base di $Ker(\phi)$. Notiamo che in questo caso non c'é stato bisogno di diagonalizzare per trovare la base opportuna di $\mathbb{Z}^3$.

Dunque $d_1 = 1$ e si ha:

$$G =< \phi(e_1) > \oplus < \phi(e_2) > \oplus < \phi(e_3) >=< -(5, 12) + 2(3, 10) > \oplus < (2, 14) >=$$

$$=< (1, 8) > \oplus < (2, 14) > .$$

Gli elementi $(1, 8), (2, 14)$ sono dunque una base di G.

Esempio. Sia G il sottogruppo di $(\mathbb{Z}/30\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$ generato da $(\overline{13}, \overline{5}), (\overline{2}, \overline{2})$. Vogliamo scrivere G come somma diretta di gruppi ciclici. Si ha una presentazione

$$\phi : \mathbb{Z}^2 \to G$$

con $\phi(n, m) = n(\overline{13}, \overline{5}) + m(\overline{2}, \overline{2})$. Dobbiamo determinare $Ker(\phi)$. É chiaro che $Ker(\phi)$ é costitutito dalle coppie $(n, m) \in \mathbb{Z}^2$ tali che

$$\begin{cases} 13n + 2m = 30t \\ 5n + 2m = 12s \end{cases}$$

Dalla seconda equazione si ottiene $n = 2p, 6s - m = 5p$. Ma allora

$$13(2p) + 2(6s - 5p) = 30t$$

e quindi

$$16p + 12s = 30t.$$

Si ottiene

$$p = 3q,\ 5t - 2s = 8q$$

ossia

$$p = 3q,\ 5t = 2(4q + s).$$

Finalmente

$$p = 3q,\ t = 2l,\ 4q + s = 5l.$$

Quindi

$$Ker(\phi) = \{(6q, 6(5l - 4q) - 15q) = (6q, 30l - 39q)\} =< (6, -39), (0, 30) > .$$

Si ha:

$$((6,-39),(0,30)) = ((1,0),(0,1))\begin{pmatrix} 6 & 0 \\ -39 & 30 \end{pmatrix}$$

Diagonalizziamo la matrice.

$$\begin{pmatrix} 6 & 0 \\ -39 & 30 \end{pmatrix} \overset{E_{2,1}(6)}{\longrightarrow} \begin{pmatrix} 6 & 0 \\ -3 & 30 \end{pmatrix} \overset{E_{1,2}(2)}{\longrightarrow} \begin{pmatrix} 0 & 60 \\ -3 & 30 \end{pmatrix} \overset{E_{1,2}}{\longrightarrow} \begin{pmatrix} -3 & 30 \\ 0 & 60 \end{pmatrix}$$

$$\longrightarrow \begin{pmatrix} -3 & 0 \\ 0 & 60 \end{pmatrix} \longrightarrow \begin{pmatrix} 3 & 0 \\ 0 & 60 \end{pmatrix}$$

Quindi $d_1 = 3, d_2 = 60$. Se si pone $e_1 = (1,0)$, $e_2 = (0,1)$, si ha:

$$(e_1, e_2) \overset{E_{2,1}(-6)}{\longrightarrow} (e_1 - 6e_2, e_2) \overset{E_{1,2}(-2)}{\longrightarrow} (e_1 - 6e_2, e_2 - 2(e_1 - 6e_2)) = (e_1 - 6e_2, -2e_1 + 13e_2)$$

$$\overset{E_{1,2}}{\longrightarrow} (-2e_1 + 13e_2, e_1 - 6e_2).$$

Quindi rispetto alla nuova base $(-2,13),(1,-6)$ di $\mathbb{Z}^2$, $ker(\phi)$ ha come base $3(-2,13), 60(1,-6)$ ossia $(-6,39),(60,-360)$. Dunque

$$\mathbb{Z}^2/Ker(\phi) = < \overline{(-2,13)} > \oplus < \overline{(1,-6)} > .$$

Infine

$$G = < \phi(-2,13) > \oplus < \phi(1,-6) > = < (\overline{0},\overline{4}) > \oplus < (\overline{1},\overline{5}) > \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}.$$

Da questa decomposizione deduciamo che G ha 180 elementi e che G non é ciclico, informazioni difficili da dedurre dalla sola conoscenza dei generatori di G. Ad esempio, gli elementi di G sono descrivibili esplicitamente:

$$G = \{n(\overline{0},\overline{4}) + m(\overline{1},\overline{5}),\ n = 0,1,2,\ m = 0,1,\ldots,59\}.$$

Un elemento di ordine 5 in G é $(\overline{12},\overline{0})$. Che tale elemento ha ordine 5 é chiaro, ma che stia in G non é cosi chiaro senza la decomposizione ottenuta.

Esempio. Determinare le ultime due cifre del numero 23^{143}.

Consideriamo il gruppo abeliano $G = U(100)$ costituito dai naturali minori di 100 e primi con 100, con la operazione "prodotto modulo 100". Ció significa che la moltiplicazione $a \circ b$ é definita come il resto della divisione di ab per 100, o anche come **il numero costituito dalle ultime due cifre di** ab. Ad esempio, avendosi $(100-1)^2 = 100^2 - 200 + 1$, si ha

$$99 \circ 99 = 1$$

e quindi

$$1 = 3 \circ 3 \circ 3 \circ 3 \circ 11 \circ 11.$$

$G = U(100)$ é un gruppo abeliano con 1 come identitá. Gli elementi di G sono i naturali minori di 100 che terminano con 1,3,7,9. Ossia sono i naturali del tipo

$$G = \{10s+1\} \cup \{10s+3\} \cup \{10s+7\} \cup \{10s+9\}$$

con $0 \leq s \leq 9$.

Quindi G ha 40 elementi. Incominciamo a provare che i numeri del tipo $10s+1$ sono in G potenze di 11, o piú precisamente che per ogni s tale che $0 \leq s \leq 9$ si ha

$$\underbrace{11 \circ 11 \circ \cdots \circ 11}_{s \ volte} = 10s+1.$$

L'uguaglianza e' vera se $s = 0$ e allora, per induzione su s, sia $s \geq 1$; si ha

$$\underbrace{11 \circ 11 \circ \cdots \circ 11}_{s \ volte} = \underbrace{11 \circ 11 \circ \cdots \circ 11}_{s-1 \ volte} \circ 11 = (10(s-1)+1) \circ 11 = 10s+1$$

perche ' le ultime due cifre di $(10(s-1)+1) \times 11 = 100(s-1)+10s+1$ costituiscono il numero $10s+1$.

Ció prova che in G l'elemento $10s+1$ é una potenza di 11 per ogni $s = 0, \ldots, 9$. In particolare

$$\underbrace{11 \circ 11 \circ \cdots \circ 11}_{10 \ volte} = \underbrace{11 \circ 11 \circ \cdots \circ 11}_{8 \ volte} \circ 11 \circ 11 = 81 \circ 11 \circ 11 = 91 \circ 11 = 1.$$

Possiamo scrivere

$$(10s+3) = (10s+3) \circ 1 = (10s+3) \circ 27 \circ 3 \circ 11 \circ 11$$

$$(10s+7) = (10s+7) \circ 1 = (10s+7) \circ 3 \circ 3 \circ 3 \circ 3 \circ 11 \circ 11$$

$$(10s+9) = (10s+9) \circ 1 = (10s+9) \circ 9 \circ 3 \circ 3 \circ 11 \circ 11.$$

Poiché i numeri $(10s+3)27, (10s+7)3, (10s+9)9$ finiscono per 1, essi sono in G potenze di 11 e dunque ogni elemento di G e' del tipo

$$\underbrace{3 \circ 3 \circ \cdots \circ 3}_{t \ volte} \circ \underbrace{11 \circ 11 \circ \cdots \circ 11}_{s \ volte}.$$

Quindi il gruppo abeliano G é generato da 3 e da 11. Allora si ha una presentazione

$$\phi : \mathbb{Z}^2 \to G$$

definita da

$$\phi(t,s) = \underbrace{3 \circ 3 \circ \cdots \circ 3}_{t \ volte} \circ \underbrace{11 \circ 11 \circ \cdots \circ 11}_{s \ volte}.$$

Dobbiamo determinare il nucleo della presentazione. Ma avendosi

$$1 = 3 \circ 3 \circ 3 \circ 3 \circ 11 \circ 11$$

e

$$1 = \underbrace{11 \circ 11 \circ \cdots \circ 11}_{10\ volte},$$

si ha $(4,2),(0,10) \in Ker(\phi)$ e quindi il sottogruppo

$$H =< (4,2),(0,10) > \subseteq Ker(\phi).$$

Si ha

$$((4,2),(0,10)) = ((1,0),(0,1)) \begin{pmatrix} 4 & 0 \\ 2 & 10 \end{pmatrix}$$

Diagonalizziamo la matrice.

$$\begin{pmatrix} 4 & 0 \\ 2 & 10 \end{pmatrix} \overset{E_{1,2}(-2)}{\longrightarrow} \begin{pmatrix} 0 & -20 \\ 2 & 10 \end{pmatrix} \overset{E_{1,2}}{\longrightarrow} \begin{pmatrix} 2 & 10 \\ 0 & -20 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 \\ 0 & -20 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 \\ 0 & 20 \end{pmatrix}.$$

Quindi $d_1 = 2, d_2 = 20$. Si ha poi

$$(e_1, e_2) \overset{E_{1,2}(2)}{\longrightarrow} (e_1, e_2 + 2e_1) \overset{E_{1,2}}{\longrightarrow} (e_2 + 2e_1, e_1).$$

Quindi se si considera la nuova base $(2,1),(1,0)$ di $\mathbb{Z}^2$, H ha come base $2(2,1), 20(1,0)$ ossia $(4,2),(20,0)$. Dunque

$$\mathbb{Z}^2/H =< \overline{(2,1)} > \oplus < \overline{(1,0)} > \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}.$$

Ció prova che $\mathbb{Z}^2/H$ ha 40 elementi, cosí come G. Ma abbiamo un epimorfismo

$$\mathbb{Z}^2/H \to \mathbb{Z}^2/Ker(\phi),$$

quindi $Ker(\phi) = H$. Si ha cosí:

$$G =< \phi(2,1) > \oplus < \phi(1,0) > =< 99 > \oplus < 3 >,$$

con $ord(99) = 2$, $ord(3) = 20$. Dunque $< 99 > \simeq \mathbb{Z}/2\mathbb{Z}$, $< 3 > \simeq \mathbb{Z}/20\mathbb{Z}$ e quindi per la Proposizione 2.7

$$G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}.$$

Ció che conta per il nostro problema é che da tale decomposizione capiamo che ogni elemento $a \in G$ é tale che

$$\underbrace{a \circ a \circ \cdots \circ a}_{20\ volte} = 1.$$

Dunque, essendo $23 \in G$ si ottiene

$$\underbrace{23 \circ 23 \circ \cdots \circ 23}_{143\ volte} = 23 \circ 23 \circ 23 = 29 \circ 23 = 67.$$

Quindi le le ultime due cifre di 23^{143} sono sono 6 e 7.

9 Invarianti primari e rango.

Il Teorema 8.1 fornisce un procedimento per ottenere la decomposizione di un gruppo G finitamente generato nella somma diretta di un numero finito di sottogruppi ciclici:

$$G =< a_1 > \oplus < a_2 > \oplus \cdots \oplus < a_s > .$$

Una domanda naturale é se tale decomposizione é in qualche modo unica. Ma si capisce subito che tale unicitá non esiste. Ad esempio, poiché $det \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} = 1$, gli elementi $(2,3), (1,2)$ sono una base di $\mathbb{Z}^2$ e quindi usando la Proposizione 3.6,

$$\mathbb{Z}^2 =< (1,0) > \oplus < (0,1) >=< (2,3) > \oplus < (1,2) > .$$

Oppure, é facile vedere che

$$\mathbb{Z}/42\mathbb{Z} =< \overline{1} >=< \overline{21} > \oplus < \overline{2} >=< \overline{14} > \oplus < \overline{3} >=< \overline{14} > \oplus < \overline{6} > \oplus < \overline{21} >\simeq$$

$$\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Procediamo allora ad una decomposizione piú fine di un gruppo abeliano finitamente generato. Per ottenere tale decomposizione, osserviamo che un gruppo ciclico finito di ordine composito si puó ulteriormente spezzare nella somma diretta di sottogruppi ciclici. Piú precisamente abbiamo il seguente teorema.

Teorema 9.1 *Sia G un gruppo abeliano, $a \in G$ un suo elemento di ordine finito d e $d = q_1 q_2 \dots q_n$ la decomposizione di d in prodotto di potenze di primi distinti. Allora*

$$< a >=< d_1 a > \oplus < d_2 a > \oplus \cdots \oplus < d_n a >$$

ove $d_i := d/q_i$. Inoltre $ord(d_i a) = q_i$.

Prova. Osserviamo che se $i \neq j$ allora si ha

$$d_i(d_j a) = 0. \tag{3}$$

Inoltre é chiaro che gli interi $d_1, \dots, d_s$ sono primi tra loro e quindi possiamo scrivere $1 = \sum_{i=1}^n m_i d_i$. Ne segue $a = \sum_{i=1}^n m_i(d_i a)$ e quindi $< a >= \sum_{i=1}^n < d_i a >$. Dobbiamo provare che la somma é diretta. Ma se $x \in \sum_{j \neq i} < d_j a >$, allora per (2) $d_i x = 0$; se anche $x \in < d_i a >$ si ha $x = t d_i a$ e quindi $q_i x = q_i t(d_i a) = t(da) = 0$. Essendo $(d_i, q_i) = (1)$, possiamo scrivere $1 = r d_i + s q_i$ e quindi $x = r(d_i x) + s(q_i x) = 0$. Il che prova che la somma é diretta.

Infine si ha $m(d_i a) = 0$ se e solo se $m d_i = dc$, se e solo se $m = q_i c$. Ció prova che $ord(d_i a) = q_i$ e conclude la dimostrazione.

□

Quindi se $d = q_1 q_2 \dots q_n$ e' la decomposizione di d in prodotto di potenze di primi distinti (tali potenze saranno dette numeri **primari**) si ha

$$\mathbb{Z}/d\mathbb{Z} \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_n\mathbb{Z}.$$

Si avra' ad esempio:

$$\mathbb{Z}/20\mathbb{Z} \simeq \mathbb{Z}/4z \times \mathbb{Z}/5\mathbb{Z}, \quad \mathbb{Z}/36\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}.$$

Come conseguenza si ha anche il seguente risultato.

Corollario 9.2 *Se m e n sono primi tra loro, allora*

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Notiamo pero' che $\mathbb{Z}/4\mathbb{Z}$ non e' isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ perche' nel primo gruppo ci sono elementi di ordine 4 mentre nel secondo ogni elemento ha ordine al piú due.

Abbiamo cosí provato che dato un gruppo abeliano G finitamente generato, esiste sempre una decomposizione di G in somma diretta di sottogruppi ciclici primari o infiniti. Una tale decomposizione si dice **decomposizione standard** di G per distinguerla dalle altre possibili decomposizioni.

Per ottenere una decomposizione standard di G, si procede prima ad individuare una decomposizione di G in somma diretta di sottogruppi ciclici e poi si usa la Proposizione precedente.

Esempio Sia $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$. Una decomposizione di G é la seguente:

$$G = <(\overline{1},\overline{0},\overline{0})> \oplus <(\overline{0},\overline{1},\overline{0})> \oplus <(\overline{0},\overline{0},\overline{1})> .$$

Ma $ord(\overline{1},\overline{0},\overline{0}) = 6 = 2 \times 3$, $ord(\overline{0},\overline{1},\overline{0}) = 20 = 4 \times 5$, $ord(\overline{0},\overline{0},\overline{1}) = 36 = 4 \times 9$ e quindi, applicando la proposizione precedente, si ottiene:

$$G = <(\overline{3},\overline{0},\overline{0})> \oplus <(\overline{2},\overline{0},\overline{0})> \oplus$$

$$\oplus <(\overline{0},\overline{5},\overline{0})> \oplus <(\overline{0},\overline{4},\overline{0})> \oplus <(\overline{0},\overline{0},\overline{9})> \oplus <(\overline{0},\overline{0},\overline{4})>$$

con $ord(\overline{3},\overline{0},\overline{0}) = 2$, $ord(\overline{2},\overline{0},\overline{0}) = 3$, $ord(\overline{0},\overline{5},\overline{0}) = 4$, $ord(\overline{0},\overline{4},\overline{0}) = 5$, $ord(\overline{0},\overline{0},\overline{9}) = 4$, $ord(\overline{0},\overline{0},\overline{4}) = 9$.

Osserviamo ora che una decomposiizone standard di un gruppo abeliano G ha la proprietá che tutti gli addendi che compaiono in essa sono indecomponibili, ossia sono sottogruppi ciclici che non si possono ulteriormente spezzare in somma diretta di sottogruppi ciclici non banali.

Infatti é facile provare che i gruppi ciclici infiniti sono isomorfi a $\mathbb{Z}$ e quindi indecomponibili, perché due sottogruppi non nulli $n\mathbb{Z}$ e $m\mathbb{Z}$ di $\mathbb{Z}$ hanno sempre una intersezione non nulla (infatti la intersezione dei due sottogruppi contiene nm).

Proviamo allora che ogni gruppo ciclico primario é indecomponibile.

Proposizione 9.3 *Se q e' un numero primario, ogni gruppo ciclico G di ordine q é indecomponibile.*

Prova. Si ha $q = p^n$ con p numero primo. Ogni sottogruppo proprio di G e' anche lui ciclico di ordine p^r con $r < n$. Se dunque H e K sono due sottogruppi propri di G di ordine p^r e p^s rispettivamente con $r \leq s < n$, allora $H \times K$ ha elementi di ordine al piú p^s e quindi non puó aversi $G \simeq H \times K$. □

Abbiamo dunque visto che ogni gruppo abeliano G finitamente generato si puó decomporre

$$G =< a_1 > \oplus < a_2 > \oplus \cdots \oplus < a_t > \oplus < a_{t+1} > \oplus \cdots \oplus < a_n >$$

dove $ord(a_i)$ é un numero primario q_i se $i \leq t$ e infinito se $i > t$. Vediamo che tale decomposizione ha finalmente una qualche sorta di unicitá. Precisamente proviamo che gli interi q_i e $n - t$ sono univocamente determinati (i q_i a meno dell'ordine) dal gruppo G.

Basterá naturalmente provare che se $q_1, \ldots, q_t, c_1, \ldots, c_s$ sono numeri primari e si ha un isomorfismo

$$\mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \times \cdots \times \mathbb{Z}/q_t\mathbb{Z} \times \mathbb{Z}^n \simeq \mathbb{Z}/c_1\mathbb{Z} \times \mathbb{Z}/c_2\mathbb{Z} \times \cdots \times \mathbb{Z}/c_s\mathbb{Z} \times \mathbb{Z}^m$$

allora $m = n$, $s = t$ e, a meno dell'ordine, $q_i = c_i$.

Abbiamo bisogno di ricordare alcune proprietá del sottogruppo di torsione di un gruppo abeliano G.

Se G é un gruppo abeliano, indichiamo con $T(G)$ il sottoinsieme degli elementi a di G di periodo finito.É chiaro che $T(G)$ é un sottogruppo di G che si chiama il **sottogruppo di torsione** di G. Raccogliamo nel seguente lemma le proprietá piú rilevanti di questo sottogruppo.

Lemma 9.4 *Siano G e H due gruppi abeliani. Si ha:*

1. Se G é libero, allora $T(G) = \{0\}$.

2. Se G é finito, allora $T(G) = G$.

3. $T(G \times H) = T(G) \times T(K)$.

4. Se $\phi : G \to H$ é un isomorfismo di gruppi, allora la restrizione di ϕ a $T(G)$ é un isomorfismo tra $T(G)$ e $T(H)$.

Prova. La prima proprietá é giá stata dimostrata. La seconda segue dal fatto che se G é finito, allora ogni elemento di G ha periodo finito e quindi $G = T(G)$.

La terza proprietá si dimostra cosi': Se $(a, b) \in T(G \times H)$ allora $n(a, b) = (0, 0)$ con $n > 0$ e quindi $na = 0$, $nb = 0$ e dunque $a \in T(G)$ e $b \in T(H)$. L'altra inclusione si prova similmente.

Infine l'ultima proprietá discende dal fatto che se $n \geq 1$ e $a \in G$, si ha

$$na = 0 \iff \phi(na) = 0 \iff n\phi(a) = 0.$$

Quindi ϕ manda $T(G)$ in $T(H)$ surgettivamente e la conclusione segue. $\square$

Applicando queste facili proprietá si ottiene un primo passo nella soluzione del nostro problema.

Lemma 9.5 *Siano G e F due gruppi abeliani finiti ed n e m due interi positivi. Se*

$$\phi : G \times \mathbb{Z}^n \to F \times \mathbb{Z}^m$$

é un isomorfismo, allora $n = m$ e G é isomorfo a F.

Prova. Usando il Lemma 9.4 si ha:

$$T(G \times \mathbb{Z}^n) = T(G) \times T(\mathbb{Z}^n) = G \times \{0\}$$

e similmente

$$T(F \times \mathbb{Z}^m) = F \times \{0\}.$$

Quindi, se $\phi : G \times \mathbb{Z}^n \to F \times \mathbb{Z}^m$ é un isomorfismo, per il lemma 9.4, 4), la restrizione di ϕ a $G \times \{0\}$ é un isomorfismo con $F \times \{0\}$. Ció prova naturalmente che G e F sono isomorfi.

Proviamo ora che $n = m$; consideriamo la composizione di omomorfismi

$$\mathbb{Z}^n \xrightarrow{i} G \times \mathbb{Z}^n \xrightarrow{\phi} F \times \mathbb{Z}^m \xrightarrow{p} \mathbb{Z}^m$$

ove i e p sono rispettivamente la immersione e la proiezione canonica sul secondo addendo. Proviamo che tale omomorfismo é iniettivo. Se $v \in \mathbb{Z}^n$ e' tale che $p\phi i(v) = 0$, allora $\phi(0, v) = (x, 0)$; per la surgettivitá della restrizione di ϕ, si ha $(x, 0) = \phi(t, 0)$ per qualche $t \in G$, e quindi $(0, v) = (t, 0)$. Dunque $v = 0$ e la composizione e' iniettiva. Cio' prova che $n \leq m$ e per simmetria si conclude che $n = m$.

$\square$

Per completare la nostra analisi dobbiamo ancora chiederci se due gruppi, che sono prodotto diretto di gruppi ciclici primari, possono essere isomorfi pur non avendo gli stessi addendi primari. Ad esempio é possibile che $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ sia isomorfo a $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$? La risposta e' negativa perché se cerchiamo gli elementi di periodo 2 nel primo gruppo ne troviamo 7, nel secondo gruppo ne troviamo 3. Questo metodo di calcolo funziona sempre e pertanto si puó dimostrare il seguente teorema.

Teorema 9.6 *Se $q_1, \ldots, q_t, c_1, \ldots, c_s$ sono numeri primari e si ha un isomorfismo*

$$\mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \times \cdots \times \mathbb{Z}/q_t\mathbb{Z} \simeq \mathbb{Z}/c_1\mathbb{Z} \times \mathbb{Z}/c_2\mathbb{Z} \times \cdots \times \mathbb{Z}/c_s\mathbb{Z}$$

allora $s = t$ e, a meno dell'ordine, $q_i = c_i$.

Abbiamo dunque visto che se G é un gruppo abeliano e

$$G =< a_1 > \oplus < a_2 > \oplus \cdots \oplus < a_s >,$$

é una qualunque decomposizione di G come somma diretta di sottogruppi ciclici primari o infiniti ossia con

$$ord(a_i) = \begin{cases} q_i & 1 \leq i \leq t \\ \infty & t < i \end{cases},$$

i numeri primari $q_1, \ldots q_t$ e l'intero $s - t$ non dipendono dalla decomposizione scelta ma soltanto da G. Pertanto possiamo dare la seguente definizione.

Definizione 9.7 *Il numero intero $s - t$ sará detto il* **rango** *di G.*

In tal modo si estende la nozione di rango a tutti i gruppi abeliani finitamente generati. Puó essere $rg(G) = 0$, ma ció avviene se e solo se G é finito.

Definizione 9.8 *I numeri primari che compaiono nella decomposizione standard di G sono detti gli* **invarianti primari** *di G.*

Ad esempio il gruppo $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z} \times \mathbb{Z}^{23}$ ha come rango 23 e come invarianti primari $2, 3, 4, 5, 4, 9$.

Il rango e gli invarianti primari di un gruppo abeliano G costituiscono un **sistema completo di invarianti** per il gruppo, nel senso che due gruppi abeliani finitamente generati sono isomorfi se e solo se hanno lo stesso rango e gli stessi invarianti primari. Ció é naturalmente conseguenza della analisi che abbiamo portato avanti in questo paragrafo.

Un corollario molto importante del teorema precedente ci assicura che in un gruppo abeliano finito di ordine n, per ogni divisore m di n possiamo sempre trovare un sottogruppo di ordine m.

Corollario 9.9 *Sia G un gruppo finito di ordine n e sia m un divisore di n. Allora esiste in G un sottogruppo di ordine m.*

Prova. Se $n = p_1^{t_1} \ldots p_s^{t_s}$ é la decomposizione di n in numeri primari, il divisore m di n si scriverá $m = p_1^{r_1} \ldots p_s^{r_s}$ ove $r_i \leq t_i$ per ogni i. Quindi basterá dimostrare che in un gruppo ciclico $< a >$ di ordine p^t con p primo c'é sempre un sottogruppo di ordine p^r se $r \leq t$. Ma infatti l'elemento $a^{p^{t-r}}$ ha ordine p^r. □

Osserviamo che non é vero peró che in un gruppo di ordine n c'é sempre un sottogruppo ciclico di ordine m se m divide n. Infatti in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ non ci sono elementi di periodo 4.

Esempio. Si ha

$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}.$$

Infatti si hanno le decomposizioni: $6 = 2\times 3, 20 = 4\times 5, 36 = 4\times 9, 12 = 3\times 4, 180 = 4 \times 5 \times 9$. Quindi gli invarianti primari di entrambi i gruppi sono $(2, 3, 4, 5, 4, 9)$.

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ non é isomorfo a $\mathbb{Z}/4320\mathbb{Z}$ perché gli invarianti primari del primo sono $(2, 3, 4, 5, 4, 9)$, quelli del secondo sono $(5, 27, 32)$.

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$ non é isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2160\mathbb{Z}$ perché gli invarianti primari del primo sono $(2, 3, 4, 5, 4, 9)$, mentre quelli del secondo sono $(2, 16, 27, 5)$.

Esempio. Consideriamo i gruppi di ordine 36. Si ha $36 = 4 \times 9$ e quindi i possibili spezzamenti di un gruppo di ordine 36 nel prodotto diretto di gruppi ciclici sono:

$$\mathbb{Z}/36\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

con invarianti primari $\{4, 9\}$,

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

con invarianti primari $\{2, 2, 9\}$,

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

con invarianti primari $\{2, 2, 3, 3\}$,

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$$

con invarianti primari $\{3, 3, 4\}$.

Esempio Determiniamo tutte le classi di isomorfismo dei gruppi abeliani di ordine 360.

Si ha

$$360 = 2^3 3^2 5$$

e quindi abbiamo queste possibilitá per i corrispondenti invarianti primari:

$$\{2, 2, 2, 3, 3, 5\},\ \{2, 2, 2, 9, 5\},\ \{2, 4, 3, 3, 5\},\ \{2, 4, 9, 5\},$$

$$\{8, 3, 3, 5\},\ \{8, 9, 5\}.$$

Dunque ci sono sei classi di isomorfismo per i gruppi abeliani finiti di ordine 360, nel senso che un gruppo abeliano di ordine 360 é isomorfo ad uno e uno solo di questi gruppi:

$$G_1 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

$$G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

$$G_3 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$G_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$
$$G_5 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$G_6 = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}.$$

Esercizio. Proviamo che ogni gruppo abeliano di ordine 45 ha un elemento di ordine 15.

Si ha $45 = 5 \times 9$ e quindi i possibili invarianti primari sono $\{3, 3, 5\}$ e $\{5, 9\}$. Quindi si hanno due classi di isomorfismo individuate da

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}, \quad \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}.$$

Ora in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ l'elemento $(\overline{1}, \overline{1}, \overline{1})$ ha ordine 15 e in $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ l'elemento $(\overline{2}, \overline{6})$ ha ordine 15.

Esercizio. É vero che ogni gruppo abeliano di ordine 45 ha un elemento di ordine 9?

Questa volta la risposta é no perché il gruppo $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ non ha elementi di ordine 9.