APPUNTI SUL TEOREMA DI CLASSIFICAZIONE DEI GRUPPI ABELIANI FINITAMENTE GENERATI

GIOVANNI GAIFFI, CORSO DI ALGEBRA 1 2010/2011

NOTA: FA PARTE DEL PROGRAMMA SOLO LA CONOSCENZA DELL'ENUNCIATO DEL TEOREMA DI CLASSIFICAZIONE (CHE VERRA' DIMOSTRATO NEL CORSO DI ALGEBRA 2). DUNQUE FANNO PARTE DEL PROGRAMMA DI ALGEBRA 1 SOLO IL PRIMO PARAGRAFO, LE PRIME NOVE RIGHE DEL PARAGRAFO 4 (FINO ALL'ESERCIZIO 4.4), E LA PRIMA PARTE DEL PARAGRAFO 5 (FINO ALL'OSSERVAZIONE 5.3). CONTROLLATE DI SAPER FARE GLI ESERCIZI DI VERIFICA 6.1, 6.2, 6.3, 6.4, 6.5, 6.6.
SI INTENDE CHE INCORAGGIAMO TUTTI A LEGGERE LE DISPENSE PER INTERO, COME APPROFONDIMENTO FACOLTATIVO.

1. L'enunciato del teorema

Definizione 1.1. Un gruppo abeliano M si dice *finitamente generato* se esistono degli elementi $m_1, m_2, \dots, m_n \in M$ tali che ogni $m \in M$ si può scrivere come combinazione lineare degli $m_1, m_2, \dots, m_n$ a coefficienti interi:

$$m = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n \qquad \text{con } a_1, a_2, \dots, a_n \in \mathbb{Z}\,.$$

Si dice che l'insieme $\{m_1, m_2, \dots, m_n\}$ è un *insieme di generatori* per M.

Osservazione 1.2. L'idea richiama dunque quella di insieme di generatori per uno spazio vettoriale. Nel contesto dei gruppi abeliani non è detto che da un insieme di generatori si possa estrarre un sottoinsieme di elementi linearmente indipendenti.

Osservazione 1.3. Un gruppo finito è finitamente generato (si potrebbe prendere come insieme di generatori addirittura l'insieme di tutti gli elementi del gruppo!).

Esempio 1.4. Il gruppo abeliano $(\mathbb{Q}, +)$ non è finitamente generato: se per assurdo $\frac{r_1}{s_1}, \frac{r_2}{s_2}, \dots, \frac{r_n}{s_n}$ fosse un insieme di generatori, basta prendere un primo p che non divide nessuno degli s_i e osservare che non è possibile scrivere:

$$\frac{1}{p} = a_1 \frac{r_1}{s_1} + a_2 \frac{r_2}{s_2} + \cdots + a_n \frac{r_n}{s_n}$$

con gli a_i interi.

Definizione 1.5. Se un gruppo abeliano A è isomorfo a $\mathbb{Z}^k$ ($k \geq 1$), A si dice *gruppo abeliano libero* di rango k.

Teorema 1.6. *Sia M un gruppo abeliano finitamente generato.*
a) Vale che

$$M \cong \mathbb{Z}^k$$

con $k \geq 0$ oppure

$$M \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$$

dove $k \geq 0$, d_i numeri interi ≥ 2 e, se $i < j$, d_i divide d_j.
b) I numeri k, $d_1, d_2, \dots, d_r$ sono univocamente determinati da M.

Osservazione 1.7. È importante notare che i numeri $k, d_1, d_2, \ldots, d_r$ sono univocamente determinati, ma la formula del teorema non individua in maniera univoca in M un sottogruppo isomorfo a $\mathbb{Z}_{d_1}$, uno isomorfo a $\mathbb{Z}_{d_2}$ etc..: basti pensare a $M = \mathbb{Z}_2 \times \mathbb{Z}_2$. In M ci sono tre distinti sottogruppi isomorfi a $\mathbb{Z}_2$ e il prodotto di due qualunque di questi è isomorfo a M.

Dimostreremo questo teorema nei paragrafi 3 e 4.

2. Successioni esatte e sottogruppi di gruppi liberi

Definizione 2.1. Una successione di n ($n \geq 2$) omomorfismi di gruppi abeliani

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \to \ldots \to A_{n-1} \xrightarrow{f_n} A_n$$

si dice *esatta in* A_i se $Imm\ f_i = Ker\ f_{i+1}$. Si dice *esatta* se è esatta in A_i per ogni $i = 1, 2, \ldots, n$.

Una successione esatta di omomorfismi di gruppi abeliani della forma

$$\{0\} \to A \xrightarrow{f} B \xrightarrow{g} C \to \{0\}$$

si dice *esatta corta*. Dalla definizione segue che in questo caso l'omomorfismo f è iniettivo e g è surgettivo.

Proposizione 2.2. *Data una successione esatta corta*

$$\{0\} \to A \xrightarrow{f} B \xrightarrow{g} \mathbb{Z} \to \{0\}$$

vale che $B \cong A \oplus \mathbb{Z}$.

Dimostrazione. Visto che g è surgettiva, esiste $b \in B$ tale che $g(b) = 1$. Costruisco allora l'omomorfismo $\psi : \mathbb{Z} \to B$ ponendo $\psi(1) = b$. Vale allora che $g \circ \psi : \mathbb{Z} \to \mathbb{Z}$ è l'identità. La mappa

$$\Gamma : A \oplus \mathbb{Z} \to B$$

data da $\Gamma((a, n)) = f(a) + \psi(n)$ fornisce l'isomorfismo cercato.

□

Osservazione 2.3. Attenzione, in generale non è vero che, data la successione esatta corta

$$\{0\} \to A \to B \to C \to \{0\}$$

allora $B \cong A \oplus C$. Basta pensare alla successione

$$\{0\} \to \mathbb{Z}_p \xrightarrow{f} \mathbb{Z}_{p^2} \xrightarrow{g} \mathbb{Z}_p \to \{0\}$$

dove f è l'immersione nell'unico sottogruppo isomorfo a $\mathbb{Z}_p$ e g è la proiezione sul quoziente rispetto a questo sottogruppo. Una dimostrazione molto simile a quella vista sopra ci garantisce che lo "spezzamento" $B \cong A \oplus C$ è vero quando C è un gruppo abeliano libero.

Proposizione 2.4. *Sia M un sottogruppo di un gruppo libero di rango n. Allora $M \cong \mathbb{Z}^r$ per un certo $0 \leq r \leq n$ (con la convenzione $\mathbb{Z}^0 = \{0\}$).*

Dimostrazione. A meno di isomorfismo, possiamo pensare M come sottogruppo di $\mathbb{Z}^n$. Si procede per induzione su n.

Se $n = 1$, sappiamo che il sottogruppo M è della forma $d\mathbb{Z}$ per $d \in \mathbb{N}$, dunque è isomorfo a $\{0\} = Z^0$ se $d = 0$ e a $\mathbb{Z}$ se $d \neq 0$.

Consideriamo ora $n > 1$ e sia $\pi : \mathbb{Z}^n \to \mathbb{Z}$ l'omomorfismo dato dalla proiezione sull'ultima coordinata. Allora $\pi_{|M} : M \to \mathbb{Z}$ ha come immagine un sottogruppo del tipo $d\mathbb{Z}$ per $d \in \mathbb{N}$. Se $d = 0$ allora

$$M \subseteq \{(a_1, a_2, \ldots, a_{n-1}, 0) \mid a_i \in \mathbb{Z}\} \cong \mathbb{Z}^{n-1}$$

e si conclude subito per ipotesi induttiva che M è isomorfo a $\mathbb{Z}^r$ con $0 \leq r \leq n-1$. Se $d \neq 0$ allora abbiamo la seguente successione esatta corta:

$$\{0\} \to Ker\ \pi_{|M} \xrightarrow{i} M \xrightarrow{\pi_{|M}} d\mathbb{Z} \cong \mathbb{Z} \to \{0\}$$

dove i è la (ovvia) immersione di $Ker\ \pi_{|M}$ in M. Per la Proposizione 2.2 sappiamo che

$$M \cong Ker\ \pi_{|M} \oplus \mathbb{Z}$$

Ma, visto che π è la proiezione sull'ultima coordinata,

$$Ker\ \pi_{|M} \subseteq \{(a_1, a_2, \ldots, a_{n-1}, 0) \mid a_i \in \mathbb{Z}\} \cong \mathbb{Z}^{n-1}$$

e dunque per ipotesi induttiva $Ker\ \pi_{|M} \cong \mathbb{Z}^s$ con $0 \leq s \leq n-1$. Si conclude dunque che

$$M \cong \mathbb{Z}^s \oplus \mathbb{Z} = \mathbb{Z}^{s+1}$$

con $s + 1 \leq n$ come volevamo. □

3. Prima parte della dimostrazione del teorema di classificazione

Dimostriamo la parte a) del teorema 1.6.

Sia $\{m_1, m_2, \ldots, m_n\}$ un insieme di generatori per M. Consideriamo l'omomorfismo $\phi : \mathbb{Z}^n \to M$ definito da

$$\phi(a_1, a_2, \ldots, a_n) = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n.$$

È surgettivo visto che $m_1, m_2, \ldots, m_n$ sono generatori. Abbiamo allora la successione esatta corta

$$\{0\} \to Ker\ \phi \xrightarrow{i} \mathbb{Z}^n \xrightarrow{\phi} M \to \{0\}$$

Per la Proposizione 2.4 sappiamo che $Ker\ \phi$ è isomorfo a $\mathbb{Z}^r$ con $0 \leq r \leq n$. Se $r = 0$ allora ϕ è un isomorfismo e $M \cong \mathbb{Z}^n$.

Se $r \geq 1$, identificando $Ker\ \phi$ con $\mathbb{Z}^r$ possiamo riscrivere così la precedente successione esatta:

$$\{0\} \to \mathbb{Z}^r \xrightarrow{i} \mathbb{Z}^n \xrightarrow{\phi} M \to \{0\}$$

L'omomorfismo i (per semplicità abbiamo continuato a chiamarlo così anche dopo l'identificazione) è rappresentato, nelle basi[1] standard di $\mathbb{Z}^r$ e Z^n, da una matrice L di dimensione $n \times r$. Sappiamo, per il primo teorema di omomorfismo, che

$$M \cong \frac{\mathbb{Z}^n}{Ker\ \phi} \cong \frac{\mathbb{Z}^n}{Imm\ i}$$

Per studiare bene questo quoziente, dobbiamo innanzitutto trovare il modo migliore di scrivere $Imm\ i$. Osserviamo che può essere di aiuto cambiare base sia in partenza che in arrivo, in modo da avere la matrice nella forma più leggibile possibile. Utilizzando l'algoritmo di Gauss, possiamo cambiare base facendo le "mosse" elementari di riga e di colonna nella loro versione "intera" ossia:

- possiamo scambiare fra di loro le righe (o le colonne);
- possiamo moltiplicare una riga o una colonna per -1;

[1] Anche nel contesto dei gruppi abeliani, in piena analogia con quanto accade per gli spazi vettoriali, chiamiamo base un insieme di generatori che sono linearmente indipendenti.

- possiamo sommare ad una riga un'altra riga moltiplicata per un intero m (lo stesso per le colonne).

Come sappiamo dall'algebra lineare, queste operazioni corrispondono infatti a moltiplicare a destra o a sinistra per matrici invertibili, dunque si tratta di operazioni reversibili, appunto cambiamenti di base. Ricordiamo (lo dimostreremo alla fine) il seguente:

Teorema 3.1. *Data una matrice L non nulla di dimensione $t \times s$ a coefficienti interi di rango h è possibile, attraverso una sequenza di mosse intere elementari di riga e di colonna, trasformarla nella matrice L' tale che $L'_{ij} = 0$ se $i \neq j$ e, per quel che riguarda gli elementi "diagonali" vale che $L'_{ii} > 0$ se $i \leq h$, $L'_{ii} = 0$ se $i > h$ ed inoltre*

$$L'_{11} = MCD\{L_{ij}\}_{\substack{i=1,\dots,t \\ j=1,\dots,s}}$$

e $L'_{11}|L'_{22}|\cdots|L'_{hh}$.

Applicando questo teorema possiamo dunque trasformare la matrice L che è di dimensione $n \times r$ ($r \leq n$) e di rango r (è infatti associata ad una applicazione iniettiva) in una matrice del tipo

$$\begin{pmatrix} k_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & k_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & k_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & ... & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & ... & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & k_r \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

dove i k_i sono interi positivi e $k_1|k_2|\cdots|k_r$.

Riassumendo, sappiamo che il gruppo M è isomorfo a $\mathbb{Z}^n$ modulo il sottogruppo H generato dalle colonne di questa matrice. L'omomorfismo

$$\gamma : \mathbb{Z}^n \to \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_r} \oplus \mathbb{Z}^{n-r}$$

data da $\gamma((a_1, a_2, \dots, a_n)) = ([a_1], [a_2], \dots, [a_r], a_{r+1}, a_{r+2}, \dots, a_n)$ è surgettivo e ha per nucleo proprio H, dunque

$$M \cong \frac{\mathbb{Z}^n}{H} \cong \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_r} \oplus \mathbb{Z}^{n-r}\,.$$

Questo conclude la dimostrazione della parte a) del teorema 1.6. Naturalmente, se alcuni (o tutti) i k_i sono uguali a 1, possiamo trascurare le relative componenti $\mathbb{Z}_1$ nel prodotto; ecco perché nell'enunciato del teorema compaiono solo dei $d_i \geq 2$. Resta da dimostrare il teorema 3.1: proponiamo qui una dimostrazione simile nella sostanza a quella vista a lezione (a lezione abbiamo dato più rilievo all'aspetto algoritmico).

Dimostrazione del teorema 3.1.
Per induzione sulla dimensione della matrice (rappresentata dal prodotto ts del numero delle sue righe per il numero delle sue colonne). I casi $ts = 1, ts = 2$ sono immediati, e in generale sono immediati i casi con $t = 1$ o $s = 1$.

Data una matrice non nulla $A = (A_{ij})$ chiamiamo $min\ A$ il minimo fra i valori assoluti dei coefficienti non nulli di A:

$$min\ A = min\ \{|A_{ij}|\ |\ A_{ij} \neq 0\}$$

Consideriamo ora matrici $t \times s$ con $t > 1$ e $s > 1$. Sulle matrici non nulle B di dimensione $t \times s$ iniziamo una induzione su $min\ B$. Se $min\ B = 1$ agiamo con mosse elementari di riga e colonna in modo da ottenere una nuova matrice B^1 con $B^1_{11} = 1$. A questo punto usiamo la prima colonna di B^1 per porre uguali a 0, attraverso le mosse elementari di colonna, i coefficienti $B^1_{12}, B^1_{13}, \ldots, B^1_{1s}$ della prima riga. Dopodiché, con procedimento simile, attraverso mosse elementari di riga possiamo rendere uguali a zero i coefficienti della prima colonna (a parte ovviamente quello più in alto, che rimane uguale a 1), e otteniamo una matrice B^2 della seguente forma:

$$\begin{pmatrix} 1 & 0 \\ 0 & T \end{pmatrix}$$

dove T è una matrice $(t-1)\times(s-1)$. Se T è nulla abbiamo già finito, altrimenti possiamo concludere usando l'ipotesi induttiva sulla dimensione $(t-1)(s-1)$.

Consideriamo adesso una matrice L di dimensione $t \times s$ con $t > 1$ e $s > 1$ e tale che $min\ L > 1$. Ci sarà un coefficiente L_{ij} tale che $|L_{ij}| = min\ L$. Possiamo, con mosse elementari di riga e di colonna trasformare L in modo da avere una nuova matrice L^1 in cui $L^1_{11} = |L_{ij}|$. A questo punto cerchiamo di usare la prima colonna di L^1 per rendere uguali a 0, attraverso mosse elementari, i coefficienti della prima riga $L^1_{12}, L^1_{13}, \ldots, L^1_{1s}$. Se L^1_{11} non divide L^1_{1i} allora la divisione euclidea ci fa ottenere una nuova matrice L^2 in cui al posto di L^1_{1i} c'è un numero intero positivo $k < L^1_{11}$. In tal caso concludiamo per l'ipotesi induttiva su "min" perché $min\ L^2 < min\ L^1$. Se invece L^1_{11} divide tutti i L^1_{1i} possiamo ottenere una matrice L^3 in cui la prima riga è $(L_{11}, 0, 0, \ldots, 0)$. Agiamo allora con mosse di riga per rendere uguali a 0 tutti i coefficienti $L^3_{21}, L^3_{31}, \ldots, L^3_{t1}$ della prima colonna. Anche qui, come prima, o uno di tali coefficienti non è diviso da L_{11}, e allora si conclude per l'ipotesi induttiva su "min", oppure si riesce ad ottenere una matrice L^4 della forma:

$$\begin{pmatrix} L_{11} & 0 \\ 0 & C \end{pmatrix}$$

dove C è una matrice $(t-1)\times(s-1)$. Se C è nulla abbiamo finito. Se C non è nulla e L_{11} divide tutti i coefficienti di C possiamo concludere per l'ipotesi induttiva sulla dimensione. Se invece c'è un coefficiente C_{hl} che non è diviso da L_{11} allora possiamo sommare la riga h-esima alla prima riga. A questo punto possiamo sottrarre alla colonna l-esima un multiplo della prima colonna in modo da ottenere (in posizione $(1, l)$) un coefficiente positivo $< L_{11}$. Si conclude allora per induzione su "min".

Ora osserviamo che quando si passa da una matrice D ad una matrice F applicando una mossa elementare intera di riga o di colonna vale $MCD\{D_{ij}\} = MCD\{F_{ij}\}$. Dunque il coefficiente L'_{11} della matrice descritta nell'enunciato del teorema, che, come si verifica immediatamente, è uguale a $MCD\{L'_{ij}\}$, è anche uguale a $MCD\{L_{ij}\}$.

4. Seconda parte della dimostrazione del teorema di classificazione: la questione dell'unicità

Cominciamo con alcune definizioni.

Definizione 4.1. Sia A un gruppo abeliano. Chiamiamo $T(A)$ il *sottogruppo di torsione*

$$T(A) = \{x \in A \mid \exists n \in \mathbb{N}, n > 0 \text{ tale che } nx = 0\}.$$

Si tratta dunque del sottogruppo formato da tutti gli elementi che hanno ordine finito.

Esercizio 4.2. A voi il facile compito di verificare che $T(A)$ è un sottogruppo.

Definizione 4.3. Sia A un gruppo abeliano. Dato un numero primo p chiamiamo $A(p)$ il *sottogruppo di p-torsione*

$$A(p) = \{x \in T(A) \mid \exists a \in \mathbb{N} \text{ tale che } o(x) = p^a\}$$

Esercizio 4.4. A voi il facile compito di verificare che $A(p)$ è un sottogruppo.

Dimostriamo dunque la parte b) del Teorema 1.6. Supponiamo che per un gruppo abeliano finitamente generato M valga

$$M \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$$

ma anche

$$M \cong \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}_{b_i}$$

con $d_i \geq 2$ e tali che se $i < j$ allora $d_i | d_j$ e lo stesso per i b_i[2] Esiste dunque un isomorfismo

$$\gamma \, : \, \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \to \mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}_{b_i}$$

Osserviamo innanzitutto che γ, essendo un isomorfismo, preserva gli ordini degli elementi e dunque manda la parte di torsione del dominio bigettivamente sulla parte di torsione del codominio. Abbiamo cioè un isomorfismo:

$$\gamma' = \gamma_{|\bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}} \, : \, \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \to \bigoplus_{i=1}^{t} \mathbb{Z}_{b_i}$$

Supponiamo che $d_r > b_t$: questo si rivela subito assurdo perché non ci sarebbe nel codominio di γ' nessun elemento di ordine d_r (mentre tali elementi ci sono nel dominio) e γ' non potrebbe essere un isomorfismo.

Allo stesso modo si esclude $d_r < b_t$, dunque vale $d_r = b_t$. Allora $d_1 d_2 \cdots d_{r-1} = b_1 b_2 \cdots b_{t-1}$. Se $r - 1 = t - 1 = 1$ abbiamo finito, altrimenti confrontiamo d_{r-1} e b_{t-1}: se fosse $b_{t-1} \neq d_{r-1}$, allora ci sarebbe un primo p che appare nelle fattorizzazioni di b_{t-1} e d_{r-1} con diverso esponente, diciamo con esponente α nella fattorizzazione di b_{t-1} e con esponente β in quella di d_{r-1}, con $\alpha > \beta$.

A questo punto si osserva che gli elementi di ordine p^α nel codominio di γ' sarebbero di più di quelli presenti nel dominio[3]. Si trova dunque $d_{r-1} = b_{t-1}$. Proseguendo in maniera simile si conclude che, se $r = t$, deve essere $d_i = b_i$ per ogni i. D'altra parte non può valere $r \neq t$. Se per esempio valesse $r > t$ allora il procedimento dimostrerebbe che $d_r = b_t$,

[2]Questo è uno dei casi da analizzare. Va anche studiato il caso in cui M viene presentato in due modi diversi $M \cong \mathbb{Z}^k$ e $M \cong \mathbb{Z}^s$ che non hanno elementi non banali di torsione. Si tratta però di una situazione più facile e basterà applicare solo una versione ridotta della dimostrazione che stiamo per descrivere. Il caso in cui una presentazione abbia torsione non banale e l'altra no si esclude molto rapidamente....

[3]Nel dominio tali elementi sono quelli che hanno l'ultima coordinata in $\mathbb{Z}_{d_r}$ di ordine p^α e la cui proiezione su $\bigoplus_{i=1}^{r-1} \mathbb{Z}_{d_i}$ è un qualunque elemento di ordine una potenza di p. Nel codominio hanno ordine p^α elementi di diverso tipo: consideriamo innanzitutto gli elementi con l'ultima coordinata in $\mathbb{Z}_{b_t} = \mathbb{Z}_{d_r}$ di ordine p^α e la cui proiezione su $\bigoplus_{i=1}^{t-1} \mathbb{Z}_{b_i}$ è un elemento di ordine una potenza di p. Dal fatto che i sottogruppi i p-torsione di $\bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$ e di $\bigoplus_{i=1}^{t} \mathbb{Z}_{b_i}$ sono isomorfi (un isomorfismo è proprio quello indotto da γ') segue che gli elementi il cui ordine è una potenza di p sono lo stesso numero in in $\bigoplus_{i=1}^{r-1} \mathbb{Z}_{d_i}$ e in $\bigoplus_{i=1}^{t-1} \mathbb{Z}_{b_i}$, dunque finora abbiamo mostrato che nel codominio di γ' gli elementi di ordine p^α sono almeno tanti quanti quelli che si trovano nel dominio.

Ma nel codominio hanno ordine p^α anche gli elementi che hanno la penultima coordinata di ordine p^α e tutte le altre coordinate uguali a [0]...

$d_{r-1} = b_{t-1}, \ldots, d_2 = b_{t-r+2}$. Ma avremmo $d_1 = b_{t-r+1}b_{t-r}\cdots b_1$, da cui $d_1 > b_{t-r+1}$ che ci porterebbe ad un assurdo contando gli elementi di ordine d_1.

Abbiamo dimostrato che le parti di torsione sono isomorfe. Possiamo dunque rileggere così il nostro isomorfismo γ:

$$\gamma \,:\, \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \to \mathbb{Z}^s \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i}$$

Resta da dimostrare che $k = s$. Consideriamo l'omomorfismo $\gamma'' \,:\, \mathbb{Z}^k \to \mathbb{Z}^s$ ottenuto dalla composizione

$$\mathbb{Z}^k \xrightarrow{i} \mathbb{Z}^k \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \xrightarrow{\gamma} \mathbb{Z}^s \oplus \bigoplus_{i=1}^{r} \mathbb{Z}_{d_i} \xrightarrow{\pi} \mathbb{Z}^s$$

dove i e π sono rispettivamente l'immersione e la proiezione ovvie. Si osserva che γ'' è iniettivo. Infatti se vale $\gamma''((a_1, a_2, \ldots, a_k)) = \gamma''((b_1, b_2, \ldots, b_k))$, questo vuole dire che $\pi \circ \gamma((a_1 - b_1, a_2 - b_2, \ldots, a_k - b_k, [0], \ldots, [0])) = (0, 0, \ldots, 0)$. Dunque $\gamma((a_1 - b_1, a_2 - b_2, \ldots, a_k - b_k, [0], \ldots, [0]))$ o è $(0, 0, 0 \ldots, 0, [0], \ldots, [0])$ oppure è un elemento non nullo che ha componenti non nulle solo nella parte di torsione. In ogni caso è un elemento di ordine finito. Ma sappiamo che γ, che è un isomorfismo, non può mandare elementi di ordine infinito in elementi di ordine finito. L'unica possibilità rimasta è che $a_1 = b_1, a_2 = b_2, \ldots, a_k = b_k$ e dunque l'iniettività della γ'' è dimostrata.

Supponiamo ora per assurdo che $k \neq s$, per esempio $k > s$. Posso esprimere γ'' con una matrice a coefficienti interi con s righe e k colonne. Possiamo "leggere" le colonne come vettori colonna $v_1, v_2, \ldots, v_k$ a coefficienti in $\mathbb{Q}$. Tali vettori non possono essere linearmente indipendenti su $\mathbb{Q}$, visto che $s < k$. Allora devono esistere coefficienti $q_1, q_2, \ldots, q_k$ razionali non tutti nulli tali che

$$q_1 v_1 + q_2 v_2 + \cdots + q_k v_k = \underline{0}.$$

Moltiplicando per il minimo comune multiplo dei denominatori dei q_i ottengo una relazione a coefficienti interi non tutti nulli

$$n_1 v_1 + n_2 v_2 + \cdots + n_k v_k = \underline{0}.$$

Questo vuol dire che $\gamma''((n_1, n_2, \ldots, n_k)) = (0, 0, \ldots, 0)$ contraddicendo l'iniettività di γ''. Abbiamo così dimostrato che $k = s$.

5. Una diversa presentazione del teorema

Proposizione 5.1. *Un gruppo abeliano finito A è il prodotto diretto dei suoi sottogruppi di Sylow, che coincidono con i sottogruppi di p-torsione.*

Dimostrazione. Per il "secondo teorema di Sylow" un elemento di ordine p^a è contenuto in un p-Sylow. In questo caso, dato che il gruppo è abeliano, c'è un solo p-Sylow. Dunque $A(p)$ è tutto contenuto nel p-Sylow. L'altra inclusione è ovvia.

Dimostriamo la parte sul prodotto diretto per induzione sul numero dei sottogruppi di Sylow (ossia sul numero dei primi p che dividono l'ordine del gruppo). Nel caso con un solo Sylow non c'è nulla da dimostrare. Sia allora A un gruppo abeliano finito. e siano N_{p_1}, N_{p_2},..N_{p_k} i suoi sottogruppi di Sylow. Si osserva (usiamo la notazione moltiplicativa) che $N_{p_1} \cap (N_{p_2} N_{p_3} \cdots N_{p_k}) = \{e\}$ per ragioni legate all'ordine degli elementi. Allora per motivi di cardinalità $N_{p_1}(N_{p_2} N_{p_3} \cdots N_{p_k}) = A$. Visto che siamo in ambito commutativo questo basta a garantire che N_{p_1} e $N_{p_2} N_{p_3} \ldots N_{p_k}$ sono in prodotto diretto. Si conclude osservando che per ipotesi induttiva $N_{p_2} N_{p_3} \cdots N_{p_k}$ è prodotto diretto di N_{p_2},..,N_{p_k}.

□

In virtù della proposizione precedente possiamo esprimere il teorema di classificazione dei gruppi abeliani finitamente generati in un altro modo, mettendo in risalto le componenti di p-torsione:

Teorema 5.2. *Sia M un gruppo abeliano finitamente generato.*
a) Vale che

$$M \cong \mathbb{Z}^k$$

con $k \geq 0$ oppure, se $T(M) \neq \{0\}$,

$$M \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{t} A(p_i)$$

dove $k \geq 0$ e $p_1, p_2, \ldots, p_t$ sono i primi che dividono $|T(M)|$. Inoltre, per ogni $1 \leq i \leq t$, vale che

$$A(p_i) \cong \mathbb{Z}_{p_i^{a_{i1}}} \oplus \mathbb{Z}_{p_i^{a_{i2}}} \cdots \oplus \mathbb{Z}_{p_i^{a_{ir(i)}}}$$

dove $r(i)$ è un intero ≥ 1 e $1 \leq a_{i1} \leq a_{i2} \leq \ldots \leq a_{ir(i)}$.
b) I numeri k,$r(i)$ e a_{ij} sono univocamente determinati da M.

Osservazione 5.3. Osserviamo che, dato M, gruppo abeliano (non necessariamente finitamente generato), i sottogruppi $T(M)$ e $A(p_i)$ sono univocamente individuati, mentre il solito esempio $\mathbb{Z}_2 \times \mathbb{Z}_2$ ci mostra che i sottogruppi isomorfi a $\mathbb{Z}_{p_i^{a_{ij}}}$ che compaiono nella formula del teorema di classificazione per i gruppi abeliani finitamente generati non sono individuati in maniera univoca dentro $A(p_i)$.

Dimostrazione. Possiamo limitarci a studiare $T(M)$ che è la parte di M presentata diversamente in questo teorema rispetto al Teorema 1.6. Il fatto che $T(M)$ sia isomorfo al prodotto diretto degli $A(p_i)$ deriva dalla Proposizione 5.1. A questo punto il Teorema 1.6, applicato ad $A(p_i)$, ci permette di scrivere

$$A(p_i) \cong \mathbb{Z}_{p_i^{a_{i1}}} \oplus \mathbb{Z}_{p_i^{a_{i2}}} \cdots \oplus \mathbb{Z}_{p_i^{a_{ir(i)}}}$$

dove $r(i) \geq 1$ e $1 \leq a_{i1} \leq a_{i2} \leq \ldots \leq a_{ir(i)}$ e ci dice che tali numeri sono univocamente determinati.

□

Esercizio 5.4. Mostrare con un esempio che il sottogruppo isomorfo a $\mathbb{Z}^k$ che appare nella formula del teorema di classificazione per i gruppi abeliani finitamente generati non è individuato in maniera univoca in M.

6. Qualche esercizio

Esercizio 6.1. I gruppi $\mathbb{Z}_{12} \times \mathbb{Z}_{72}$ e $\mathbb{Z}_{18} \times \mathbb{Z}_{48}$ sono isomorfi? E i gruppi $\mathbb{Z}_{72} \times \mathbb{Z}_{84}$ e $\mathbb{Z}_{36} \times \mathbb{Z}_{168}$?

Esercizio 6.2. Trovare tutte le coppie di numeri interi positivi (a, b) tali che il gruppo $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ sia isomorfo a $\mathbb{Z}_a \times \mathbb{Z}_b$.

Esercizio 6.3. Quanti gruppi abeliani di ordine 100 esistono (a meno di isomorfismo)?

Esercizio 6.4. Consideriamo il gruppo $A = \mathbb{Z}_2 \times \mathbb{Z}_{12}$ e i sottogruppi $H = \mathbb{Z}_2 \times \{[0]\}$ e $K = \{[0]\} \times \{[0], [6]\}$. Vale che $H \cong \mathbb{Z}_2 \cong K$, ma è vero o falso che $G/H \cong G/K$?

Esercizio 6.5. Si dimostri che esiste un prodotto semidiretto $\mathbb{Z} \rtimes \mathbb{Z}_2$ non abeliano. Si mostri che in tale gruppo il sottoinsieme degli elementi di torsione non è un sottogruppo. *Questo gruppo può essere pensato come un gruppo diedrale D_∞: la rotazione r va pensata come una rotazione di un angolo $2\pi\rho$ con ρ irrazionale...*

Esercizio 6.6. Mostrare che gruppo abeliano M di torsione, ossia tale che $M = T(M)$, non è necessariamente finito. In M esiste un limite superiore per l'ordine degli elementi o si trova un esempio in cui ci sono elementi di ordine arbitrariamente grande?

Esercizio 6.7. La definizione di gruppo abeliano libero si estende anche al caso di rango "infinito". Un gruppo abeliano A si dice libero se, detto S un insieme di indici,

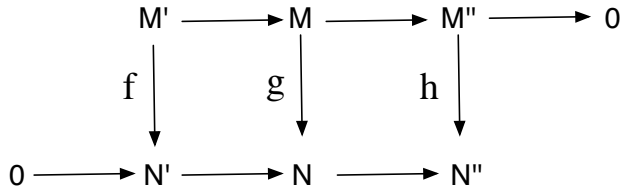
$$A \cong \bigoplus_{s \in S} \mathbb{Z}\,.$$

Se un gruppo abeliano A non ha torsione, ossia $T(A) = \{0\}$, si può concludere che è libero?

Esercizio 6.8. Ripensare ai teoremi esposti in queste note e alla dimostrazioni. Si potrebbero estendere enunciati e dimostrazioni al caso di moduli finitamente generati sull'anello dei polinomi $K[x]$ su un campo K?

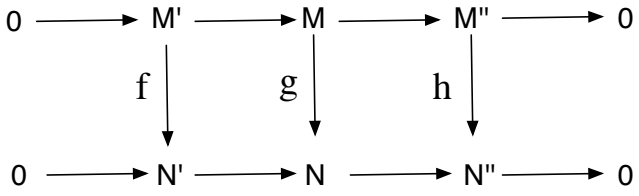
Esercizio 6.9. Sia Γ un sottogruppo discreto (rispetto alla topologia standard) non nullo di $\mathbb{R}^n$. Dimostrare che Γ è un gruppo abeliano libero con generatori $g_1, g_2, \ldots, g_r$ linearmente indipendenti su $\mathbb{R}$.

Esercizio 6.10. Consideriamo il seguente diagramma di gruppi abeliani e omomorfismi in cui tutti i quadrati "commutano" e le successioni orizzontali sono esatte:



Dimostrare che:
a) se f e h sono iniettive allora lo è anche g;
b) se f e h sono surgettive allora lo è anche g.

Esercizio 6.11. Consideriamo il seguente diagramma di gruppi abeliani e omomorfismi in cui tutti i quadrati "commutano" e le successioni orizzontali sono esatte:



Dimostrare che se due qualunque fra gli omomorfismi f, h, g sono isomorfismi allora lo è anche il terzo.