Fogli NON riletti. Grazie per ogni segnalazione di errori.

Esempi di gruppi abeliani finiti

Alcune premesse generali:
Sia $N \subseteq \mathbb{Z}^m$ un sottomodulo generato da dei vettori $v_1, \ldots, v_n$. Fissiamo in $\mathbb{Z}^m$ la base canonica $b_1, \ldots, b_m$ e consideriamo la matrice:

$$A = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ \ldots & & & \ldots \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{pmatrix}$$

le cui colonne sono i generatori di N espressi rispetto alla base fissata. Se consideriamo un nuovo sistema di generatori di N in cui al posto di v_i prendiamo il vettore $v_i' = v_i + \alpha v_j$ ($i \neq j$ fissati), la matrice corrispondente si ottiene da A con l'operazione elementare di colonna sommando alla colonna i la colonna j moltiplicata per α. Se invece cambiamo la base di $\mathbb{Z}^m$ prendendo $b_j = b_j + \alpha b_i$ ($i \neq j$ fissati) la matrice corrispondente associata ad N si ottiene da A con l'operazione elementare che somma alla riga i la riga j moltiplicata per α.

Supponiamo ora che, per un'opportuna base di $\mathbb{Z}^m$ e un opportuno sistema di generatori di N la matrice associata sia quadrata diagonale, cioè della forma:

$$A = \begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ \ldots & \ldots & & \ldots \\ 0 & 0 & \ldots & a_m \end{pmatrix}$$

Allora è facile vedere che il modulo $\mathbb{Z}^m/N$ è isomorfo a $\mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \cdots \oplus \mathbb{Z}_{a_m}$. Basta infatti considerare la mappa

$$\phi : \mathbb{Z}^m \longrightarrow \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_m}$$

data da $\phi(b_i) = (0, \ldots, 1, \ldots, 0)$ (dove 1 sta all'i-imo posto). La mappa è suriettiva e il suo nucleo è N, quindi si ottiene l'isomorfismo indicato sopra.

Consideriamo ora l'esempio $N = \langle (2,2), (2,6) \rangle \subseteq \mathbb{Z}^2$. Si può rappresentare $\mathbb{Z}^2$ con tutti i punti a coordinate intere del piano e N risulta un opportuno reticolo, come nella figura 1.

La matrice corrispondente è data da:

$$\begin{pmatrix} 2 & 2 \\ 2 & 6 \end{pmatrix}$$

Detto $v_1 = (2,2)$ e $v_2 = (2,6)$ ed e_1, e_2 sono la base canonica di $\mathbb{Z}^2$, l'operazione di colonna $C_2 \leftarrow C_2 - C_1$ corrisponde a considerare per generatori di N i vettori $v_1, v_2 - v_1 = (0,4)$. L'operazione di riga $R_2 \leftarrow R_2 - R_1$ corrisponde a cambiare la base da e_1, e_2 alla base $e_1 = e_1' - e_2,\ e_2 = e_2'$. Quindi il modulo N si può rappresentare con la matrice diagonale:

$$\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$$

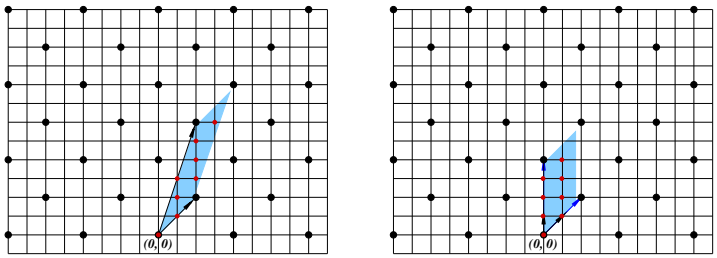

Figura 1: A sinistra: il reticolo dato dal sottomodulo $N = \langle (2,2),(2,6) \rangle$. I bollini rossi rappresentano gli elementi del quoziente $\mathbb{Z}^2/N$. A destra: lo stesso modulo N generato ora dai vettori $(2,0)$ e $(0,4)$ (vettori in blu) e riferito alla base $(1,1),\ (0,1)$ di $\mathbb{Z}^2$ (vettori in nero). I bollini rossi rappresentano gli elementi del quoziente $\mathbb{Z}^2/N$.

ed è riferita alla base di $\mathbb{Z}^2$ data da $e_1' = (1,1),\ e_2 = (0,1)$.

Per quanto detto, dalla seconda rappresentazione di N si trova che il quoziente $\mathbb{Z}^2/N$ è isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_4$. Si noti che diagonalizzare la matrice corrisponde a trovare una base di $\mathbb{Z}^2$ tale per cui ciascun generatore di N sia multiplo di un elemento della base.

Il problema di capire come sono fatti i moduli quozienti di $\mathbb{Z}^m$ si riconduce quindi al problema di diagonalizzare una matrice di interi con operazioni elementari di righe e colonne. Poiché ogni modulo (finitamente generato) è quoziente di $\mathbb{Z}^m$, saper diagonalizzare matrici di interi comporta saper trovare la struttura dei moduli finitamente generati su $\mathbb{Z}$ e quindi la struttura dei gruppi abeliani finitamente generati.

Prendiamo ad esempio il modulo N generato dalle colonne della seguente matrice:

$$\begin{pmatrix} 1 & 1 & 4 \\ 3 & 5 & -8 \\ 0 & 4 & -4 \end{pmatrix}$$

Si può vedere che con operazioni di riga e colonna la matrice si può trasformare in:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

Pertanto il modulo quoziente $\mathbb{Z}^3/N$ è isomorfo a:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$$

Si può vedere che con altre operazioni di riga e colonna la matrice di partenza si può anche trasformare in:

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

Pertanto il modulo quoziente è anche isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_{12}$.

Una conseguenza dei teoremi generali sulla struttura di moduli su PID è che ogni matrice (quadrata di ordine m) di interi si può trasformare, con operazioni elementari di riga e colonna, in una matrice diagonale (come visto negli esempi precedenti), in più però si può avere la condizione che i numeri naturali $d_1, d_2, \ldots, d_m$ che costituiscono la diagonale sono tali che $d_1|d_2$, $d_2|d_3$, $\ldots$, $d_{m-1}|d_m$.