ALGEBRA I: SOLUZIONI NONA ESERCITAZIONE
31 maggio 2011

Esercizio 1. Calcolare la struttura di $\mathbb{Z}[i]/(3+4i)$ come $\mathbb{Z}$-modulo.

Suggerimento. Considerare l'isomorfismo di $\mathbb{Z}$-moduli $\phi : \mathbb{Z}[i] \to \mathbb{Z}^2$ definito da $\phi(1) = (1,0)$ e $\phi(i) = (0,1)$ ed identificare l'ideale generato da $3+4i$ con l'immagine della matrice

$$\begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix}.$$

Soluzione. Consideriamo l'isomorfismo di $\mathbb{Z}$-moduli

$$\phi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}^2$$

definito da $\phi(1) = (1,0)$ e $\phi(i) = (0,1)$. Osserviamo che come $\mathbb{Z}$-modulo l'ideale principale $I = (3+4i)$ è generato da $3+4i$ e $4-3i = -i(3+4i)$: infatti da una parte questi due elementi appartengono a I e dunque generano un sottomodulo di I, mentre viceversa per ogni $a+bi \in \mathbb{Z}[i]$ allora l'elemento

$$(a+bi)(3+4i) = a(3+4i) - b(4-3i)$$

è nel sottomodulo generato da essi. Pertanto $\phi(I) \subset \mathbb{Z}^2$ coincide con il sottomodulo generato dai vettori $(3,4)$ e $(4,-3)$, vale a dire con l'immagine di $\mathbb{Z}^2$ attraverso la matrice

$$A = \begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix}.$$

Cerchiamo la forma diagonale A' di A mediante operazioni intere sulle righe e sulle colonne:

$$A = \begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 3 & 1 \\ 4 & -7 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 1 & 3 \\ -7 & 4 \end{pmatrix} \xrightarrow{c_3} \begin{pmatrix} 1 & 0 \\ -7 & -25 \end{pmatrix} \xrightarrow{c_4} \begin{pmatrix} 1 & 0 \\ 0 & -25 \end{pmatrix} \xrightarrow{c_5} \begin{pmatrix} 1 & 0 \\ 0 & 25 \end{pmatrix} = A'$$

Pertanto otteniamo gli isomorfismi di $\mathbb{Z}$-moduli (vale a dire di gruppi abeliani):

$$\mathbb{Z}[i]/(3+4i) \simeq \mathbb{Z}^2/\mathrm{Im}(A) \simeq \mathbb{Z}^2/\mathrm{Im}(A') \simeq \mathbb{Z}/(1) \times \mathbb{Z}/(25) \simeq \mathbb{Z}/(25).$$

Esercizio 2. Sia $a+bi$ un intero di Gauss, si denoti $d = \mathrm{MCD}(a,b)$ e $D = (a^2+b^2)/d$. Mostrare che esiste un isomorfismo di gruppi abeliani

$$\mathbb{Z}[i]/(a+bi) \simeq \mathbb{Z}/(d) \times \mathbb{Z}/(D).$$

Osservazione. In particolare, $\mathbb{Z}[i]/(a+bi)$ è un anello di cardinalità a^2+b^2.

Suggerimento. Generalizzare il suggerimento dell'esercizio precedente.

Soluzione. Consideriamo l'isomorfismo di $\mathbb{Z}$-moduli

$$\phi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}^2$$

definito da $\phi(1) = (1,0)$ e $\phi(i) = (0,1)$. Come nell'esercizio precedente si mostra che l'immagine dell'ideale principale $(a+bi)$ coincide con l'immagine di $\mathbb{Z}^2$ attraverso la matrice

$$A = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}.$$

Per determinare la forma diagonale A' di A, supponiamo $|b| \leq |a|$ e consideriamo la successione di divisioni euclidee

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\dots \\ r_{k-1} &= q_{k+1} r_k \end{aligned}$$

dove $r_n = d$ coincide con il massimo comune divisore di a e b. Allora operando sulla matrice A mediante operazioni intere sulle colonne otteniamo

$$A = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \longrightarrow \begin{pmatrix} r_1 & b \\ q_1 a + b & -a \end{pmatrix} \longrightarrow \begin{pmatrix} r_1 & r_2 \\ q_1 a + b & -(q_1 q_2 + 1)a - q_2 b \end{pmatrix} \longrightarrow \ldots \longrightarrow \begin{pmatrix} d & 0 \\ n & m \end{pmatrix}$$

Segue dall'algoritmo che n è una combinazione lineare di a e b, pertanto esso è divisibile per il loro massimo comune divisore d. Dunque operando sulle righe al passaggio successivo otteniamo la forma diagonale

$$\begin{pmatrix} d & 0 \\ n & m \end{pmatrix} \longrightarrow \begin{pmatrix} d & 0 \\ 0 & m \end{pmatrix} = A'.$$

Poiché tutte le operazioni elementari effettuate sulle righe e sulle colonne coincidono con la moltiplicazione per una matrice il cui determinante ha modulo 1, a meno del segno otteniamo l'uguaglianza

$$dm = \det(A) = a^2 + b^2,$$

vale a dire (a meno del segno) $m = (a^2 + b^2)/d = D$. Pertanto otteniamo i seguenti isomorfismi di gruppi abeliani:

$$\mathbb{Z}[i]/(a + bi) \simeq \mathbb{Z}^2/\mathrm{Im}(A) \simeq \mathbb{Z}^2/\mathrm{Im}(A') \simeq \mathbb{Z}/(d) \times \mathbb{Z}/(D).$$

Esercizio 3. Sia A una matrice quadrata a coefficienti interi il cui determinante è privo di quadrati (vale a dire per cui non esistono interni n tali che n^2 divide $\det(A)$). Determinare la forma diagonale di A.

Soluzione. Dal teorema di diagonalizzazione, otteniamo che esiste una matrice diagonale A' con lo stesso determinante di A della forma

$$\begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & d_n \end{pmatrix}$$

dove n è l'ordine di A e dove ogni d_i divide d_{i+1}. In particolare $\det(A) = d_1 d_2 \cdots d_n$ e d_{n-1}^2 divide $\det(A)$. Poiché $\det(A)$ è privo di quadrati, otteniamo allora $d_1 = \ldots = d_{n-1} = 1$ e $d_n = \det(A)$.

Esercizio 4. Mostrare che due vettori a coefficienti interi (a_1, a_2, a_3), (b_1, b_2, b_3) si completano a una base di $\mathbb{Z}^3$ se e solo se il massimo comune divisore dei minori della matrice

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$$

è uno.

Soluzione. Dalla teoria sappiamo che tre vettori interi formano una base di $\mathbb{Z}^3$ se e solo se la matrice che li ha per colonne ha determinante ± 1. Pertanto i vettori (a_1, a_2, a_3), (b_1, b_2, b_3) si completano a una base di $\mathbb{Z}^3$ se e solo se esiste un vettore (c_1, c_2, c_3) tale che la matrice

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}$$

ha determinante uno. Sviluppando il determinante della precedente matrice lungo l'ultima riga otteniamo allora la condizione

$$1 = c_1 \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} - c_2 \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix} + c_3 \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}.$$

Sfruttando l'esistenza dell'identità di Bézout, otteniamo allora che un vettore (c_1, c_2, c_3) come sopra esiste se e solo se i minori

$$\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, \quad \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}, \quad \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}$$

hanno massimo comune divisore 1.

Esercizio 5. Sia A la matrice di un omomorfismo $\phi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ tra due $\mathbb{Z}$-moduli liberi relativamente a due basi fissate.

i) Mostrare che ϕ è iniettivo se e solo se $\det(A) \neq 0$.

ii) Mostrare che ϕ è suriettivo se e solo se $|\det(A)| = 1$.

Osservazione. L'esercizio mostra che, mentre la suriettività implica l'iniettività, il viceversa è falso (a differenza degli spazi vettoriali di dimensione finita).

Soluzione. i) A patto di cambiare le basi, possiamo assumere che A sia diagonale. Inoltre, se $d_1, \ldots, d_n$ sono gli elementi sulla diagonale, allora $\det(A) = d_1 \cdot \ldots \cdot d_n$. Siano $v_1, \ldots, v_n$ e $w_1, \ldots, w_n$ le basi di $\mathbb{Z}^n$ (rispettivamente in partenza e in arrivo) rispetto a cui A è diagonale.

Supponiamo $\det(A) = 0$: allora $d_i = 0$ per qualche i, e di conseguenza $v_i \in \ker(\phi)$: pertanto ϕ non è iniettiva. Viceversa, se $\det(A) \neq 0$, ogni vettore v_i è mandato in un multiplo non nullo di w_i: pertanto $\phi(v_1), \ldots, \phi(w_n)$ sono vettori linearmente indipendenti di $\mathbb{Z}^n$ e ϕ è iniettiva.

ii) Supponiamo che $|\det(A)| = 1$: allora ϕ è un isomorfismo di moduli liberi, e in particolare è suriettivo. Supponiamo viceversa che ϕ sia suriettivo. Allora applicando un cambiamento di base in arrivo possiamo assumere che le due basi di $\mathbb{Z}^n$ in partenza e in arrivo coincidano, vale a dire $v_i = w_i$ per ongi i. Pertanto in queste nuove basi ϕ è espresso dalla matrice identità, dunque $|\det(A)| = \det(I) = 1$.

Esercizio 6. Ridurre la matrice

$$A = \begin{pmatrix} 10 & 7 & 3 \\ 9 & 5 & 4 \\ 6 & 5 & 8 \end{pmatrix}$$

in forma diagonale mediante operazioni intere sulle righe e sulle colonne, determinando matrici intere Q e P tali che $A' = Q^{-1}AP$ è diagonale ed esplicitando le basi in partenza e in arrivo che rendono la trasformazione diagonale.

Soluzione. Procediamo mediante operazioni elementari sulle righe e sulle colonne della matrice A fino ad ottenere la matrice diagonale A', ed effettuiamo contemporaneamente tutte le operazioni sulle colonne (risp. sulle righe) su una matrice di appoggio che allo stato iniziale è l'identità nel modulo di partenza (risp. nel modulo di arrivo). Operando in questo modo, alla fine le due matrici di appoggio forniranno rispettivamente i cambiamenti di base P e Q^{-1}: mentre la base del modulo di partenza che rende la trasformazione diagonale sarà fornita dalle colonne di P, la base del modulo immagine che rende la trasformazione diagonale sarà fornita dalle colonne di $QA' = AP$.

$$A = \begin{pmatrix} 10 & 7 & 3 \\ 9 & 5 & 4 \\ 6 & 5 & 8 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 3 & 7 & 10 \\ 4 & 5 & 9 \\ 8 & 5 & 6 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 3 & 1 & 10 \\ 4 & -3 & 9 \\ 8 & -11 & 6 \end{pmatrix} \xrightarrow{c_3} \begin{pmatrix} 3 & 1 & 1 \\ 4 & -3 & -3 \\ 8 & -11 & -18 \end{pmatrix} \xrightarrow{c_4}$$
$$\xrightarrow{c_4} \begin{pmatrix} 1 & 3 & 1 \\ -3 & 4 & -3 \\ -11 & 8 & -18 \end{pmatrix} \xrightarrow{c_5} \begin{pmatrix} 1 & 0 & 1 \\ -3 & 13 & -3 \\ -11 & 41 & -18 \end{pmatrix} \xrightarrow{c_6} \begin{pmatrix} 1 & 0 & 0 \\ -3 & 13 & 0 \\ -11 & 41 & -7 \end{pmatrix} \xrightarrow{r_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 13 & 0 \\ -11 & 41 & -7 \end{pmatrix} \xrightarrow{r_2}$$
$$\xrightarrow{r_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 13 & 0 \\ 0 & 41 & -7 \end{pmatrix} \xrightarrow{r_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 13 & 0 \\ 0 & 2 & -7 \end{pmatrix} \xrightarrow{r_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -7 \\ 0 & 13 & 0 \end{pmatrix} \xrightarrow{c_7} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 13 & 52 \end{pmatrix} \xrightarrow{c_8}$$
$$\xrightarrow{c_8} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 52 & 13 \end{pmatrix} \xrightarrow{c_9} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 52 & -91 \end{pmatrix} \xrightarrow{r_5} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -91 \end{pmatrix} \xrightarrow{r_6} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 91 \end{pmatrix} = A'$$

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{r_1} \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{r_2} \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 11 & 0 & 1 \end{pmatrix} \xrightarrow{r_3} \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 2 & -3 & 1 \end{pmatrix} \xrightarrow{r_4} \begin{pmatrix} 1 & 0 & 0 \\ 2 & -3 & 1 \\ 3 & 1 & 0 \end{pmatrix} \xrightarrow{r_5}$$
$$\xrightarrow{r_5} \begin{pmatrix} 1 & 0 & 0 \\ 2 & -3 & 1 \\ -101 & 157 & -52 \end{pmatrix} \xrightarrow{r_6} \begin{pmatrix} 1 & 0 & 0 \\ 2 & -3 & 1 \\ 101 & -157 & 52 \end{pmatrix} = Q^{-1}$$
$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & -2 & 0 \end{pmatrix} \xrightarrow{c_3} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & -2 & -3 \end{pmatrix} \xrightarrow{c_4} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ -2 & 1 & -3 \end{pmatrix} \xrightarrow{c_5}$$
$$\xrightarrow{c_5} \begin{pmatrix} 0 & 0 & 1 \\ 1 & -3 & 0 \\ -2 & 7 & -3 \end{pmatrix} \xrightarrow{c_6} \begin{pmatrix} 0 & 0 & 1 \\ 1 & -3 & -1 \\ -2 & 7 & -1 \end{pmatrix} \xrightarrow{c_7} \begin{pmatrix} 0 & 0 & 1 \\ 1 & -3 & -13 \\ -2 & 7 & 27 \end{pmatrix} \xrightarrow{c_8}$$
$$\xrightarrow{c_8} \begin{pmatrix} 0 & 1 & 0 \\ 1 & -13 & -3 \\ -2 & 27 & 7 \end{pmatrix} \xrightarrow{c_9} \begin{pmatrix} 0 & 1 & -2 \\ 1 & -13 & 23 \\ -2 & 27 & -47 \end{pmatrix} = P$$

Nello schema precedente, $c_1, \ldots, c_9$ indicano le operazioni effettuate sulle colonne e $r_1, \ldots, r_6$ indicano le operazioni effettuata sulle righe: più precisamente, c_1 è l'operazione che scambia la prima colonna con la terza, c_2 è l'operazione che sottrae alla seconda colonna 2 volte la prima, c_3 è l'operazione che sottrae alla terza colonna 3 volte la prima, c_4 è l'operazione che scambia la prima colonna con la seconda, c_5 è l'operazione che sottrae alla seconda colonna 3 volte la prima, c_6 è l'operazione che sottrae alla terza colonna la prima, r_1 è l'operazione che somma alla seconda riga 3 volte la prima, r_2 è l'operazione che somma alla terza riga 11 volte la prima, r_3 è l'operazione che sottrae alla terza riga 3 volte la seconda, r_4 è l'operazione che scambia la seconda riga con la terza, c_7 è l'operazione che somma alla terza colonna 4 volte la seconda, c_8 è l'operazione che scambia la seconda colonna con la terza, c_9 è l'operazione che sottrae alla terza colonna 2 volte la seconda, r_5 è l'operazione che sottrae alla terza riga 52 volte la seconda, r_6 è l'operazione che cambia il segno alla terza riga.

Le basi di $\mathbb{Z}^3$ e di $\mathrm{Im}(A) \subset \mathbb{Z}^3$ che rendono A diagonale sono date rispettivamente dalle colonne di P e dalle colonne di $QA' = AP$:

$$AP = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 52 & -92 \\ -11 & 157 & -273 \end{pmatrix}.$$

Pertanto le basi di $\mathbb{Z}^3$ e di $\mathrm{Im}(A)$ che rendono A diagonale sono rispettivamente

$$\left\{ \begin{pmatrix} 0 \\ 1 \\ -2 \end{pmatrix}, \begin{pmatrix} 1 \\ -13 \\ 27 \end{pmatrix}, \begin{pmatrix} -2 \\ 23 \\ -47 \end{pmatrix} \right\} \subset \mathbb{Z}^3, \qquad \left\{ \begin{pmatrix} 1 \\ -3 \\ -11 \end{pmatrix}, \begin{pmatrix} 0 \\ 52 \\ 157 \end{pmatrix}, \begin{pmatrix} 0 \\ -92 \\ -273 \end{pmatrix} \right\} \subset \mathrm{Im}(A).$$