ALGEBRA I: SOLUZIONI OTTAVA ESERCITAZIONE
26 maggio 2011

Esercizio 1. Ridurre ciascuna delle seguenti matrici M alla forma diagonale mediante operazioni intere sulle righe e sulle colonne, determinando matrici intere Q e P tali che $M' = Q^{-1}MP$ è diagonale ed esplicitando le basi in partenza e in arrivo che rendono la trasformazione diagonale:

$$A = \begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, \qquad C = \begin{pmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{pmatrix}$$

Soluzione. Procediamo in ognuno dei tre casi mediante operazioni elementari sulle righe e sulle colonne della matrice M fino ad ottenere la matrice diagonale M', 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 $QM' = MP$.

Consideriamo la matrice A e determiniamo la sua forma diagonale e i cambiamenti di base P e Q:

$$A = \begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 1 & 0 \\ 2 & -7 \end{pmatrix} \xrightarrow{r_1} \begin{pmatrix} 1 & 0 \\ 0 & -7 \end{pmatrix} \xrightarrow{c_3} \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix} = A'$$
$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \xrightarrow{c_3} \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix} = P$$
$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow{r_1} \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} = Q^{-1}$$

Nello schema precedente, c_1, c_2, c_3 indicano le operazioni effettuate sulle colonne e r_1 indica l'unica operazione effettuata sulle righe: più precisamente, c_1 è l'operazione che scambia le due colonne, c_2 è l'operazione che somma alla seconda colonna -3 volte la prima, r_1 è l'operazione che somma alla seconda riga -2 volte la prima, c_3 è l'operazione che cambia il segno della seconda colonna.

Le basi di $\mathbb{Z}^2$ e di $\mathrm{Im}(A) \subset \mathbb{Z}^2$ che rendono diagonale la trasformazione di $\mathbb{Z}^2$ in se stesso associata ad A sono date rispettivamente dalle colonne di P e dalle colonne di $QA' = AP$:

$$AP = \begin{pmatrix} 1 & 0 \\ 2 & 7 \end{pmatrix}.$$

Pertanto le basi di $\mathbb{Z}^2$ e di $\mathrm{Im}(A)$ che rendono A diagonale sono rispettivamente

$$\left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 3 \end{pmatrix} \right\} \subset \mathbb{Z}^2, \qquad \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 7 \end{pmatrix} \right\} \subset \mathrm{Im}(A).$$

Consideriamo ora la matrice B e determiniamo la sua forma diagonale e i cambiamenti di base P e Q:

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 1 & 0 & 3 \\ 4 & -3 & 6 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 1 & 0 & 0 \\ 4 & -3 & -6 \end{pmatrix} \xrightarrow{r_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \end{pmatrix} \xrightarrow{c_3}$$
$$\xrightarrow{c_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{pmatrix} \xrightarrow{c_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} = B'$$
$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_3} \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_4}$$
$$\xrightarrow{c_4} \begin{pmatrix} 1 & 2 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = P$$
$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \xrightarrow{r_1} \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} = Q^{-1}$$

Nello schema precedente, c_1, c_2, c_3, c_4 indicano le operazioni effettuate sulle colonne e r_1 indica l'unica operazione effettuata sulle righe: più precisamente, c_1 è l'operazione che somma alla seconda colonna -2 volte la prima, c_2 è l'operazione che somma alla terza colonna -3 volte la prima, r_1 è l'operazione che somma alla seconda riga -4 volte la prima, c_3 è l'operazione che somma alla terza colonna -2 volte la seconda, c_4 è l'operazione che cambia il segno della seconda colonna.

Le basi di $\mathbb{Z}^3$ e di $\mathrm{Im}(B) \subset \mathbb{Z}^2$ che rendono B diagonale sono date rispettivamente dalle colonne di P e dalle colonne di $QB' = BP$:

$$BP = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 3 & 0 \end{pmatrix}.$$

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

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \right\} \subset \mathbb{Z}^3, \qquad \left\{ \begin{pmatrix} 1 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix} \right\} \subset \mathrm{Im}(B).$$

Consideriamo infine la matrice C e determiniamo la sua forma diagonale e i cambiamenti di base P e Q:

$$C = \begin{pmatrix} 3 & 1 & -4 \\ 2 & -3 & 1 \\ -4 & 6 & -2 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 1 & 3 & -4 \\ -3 & 2 & 1 \\ 6 & -4 & -2 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 1 & 0 & -4 \\ -3 & 11 & 1 \\ 6 & -22 & -2 \end{pmatrix} \xrightarrow{c_3} \begin{pmatrix} 1 & 0 & 0 \\ -3 & 11 & -11 \\ 6 & -22 & 22 \end{pmatrix} \xrightarrow{r_1}$$
$$\xrightarrow{r_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 11 & -11 \\ 6 & -22 & 22 \end{pmatrix} \xrightarrow{r_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 11 & -11 \\ 0 & -22 & 22 \end{pmatrix} \xrightarrow{c_4} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 11 & 0 \\ 0 & -22 & 0 \end{pmatrix} \xrightarrow{r_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 11 & 0 \\ 0 & 0 & 0 \end{pmatrix} = C'$$
$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_1} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_2} \begin{pmatrix} 0 & 1 & 0 \\ 1 & -3 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_3} \begin{pmatrix} 0 & 1 & 0 \\ 1 & -3 & 4 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{c_4} \begin{pmatrix} 0 & 1 & 1 \\ 1 & -3 & 1 \\ 0 & 0 & 1 \end{pmatrix} = P$$
$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{r_1} \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{r_2} \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ -6 & 0 & 1 \end{pmatrix} \xrightarrow{r_3} \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} = Q^{-1}$$

Nello schema precedente, c_1, c_2, c_3, c_4 indicano le operazioni effettuate sulle colonne e r_1, r_2, r_3 indicano le operazioni effettuata sulle righe: più precisamente, c_1 è l'operazione che scambia le prime due colonne, c_2 è l'operazione che somma alla seconda colonna -3 volte la prima, c_3 è l'operazione che somma alla terza colonna 4 volte 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 -6 volte la prima, c_4 è l'operazione che somma alla terza colonna la seconda, r_3 è l'operazione che somma alla terza riga 2 volte la prima.

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

$$CP = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 11 & 0 \\ 6 & -22 & 0 \end{pmatrix}.$$

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

$$\left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -3 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\} \subset \mathbb{Z}^3, \qquad \left\{ \begin{pmatrix} 1 \\ -3 \\ 6 \end{pmatrix}, \begin{pmatrix} 0 \\ 11 \\ -22 \end{pmatrix} \right\} \subset \mathrm{Im}(C).$$

Esercizio 2. Si consideri la matrice A (risp. C) dell'esercizio precedente. Disegnare $\mathrm{Im}(A)$ (risp. $\mathrm{Im}(C)$) come sottoreticolo di $\mathbb{Z}^2$ (risp. di $\mathbb{Z}^3$) e determinare due basi proporzionali di $\mathbb{Z}^2$ e di $\mathrm{Im}(A)$ (risp. di $\mathbb{Z}^3$ e di $\mathrm{Im}(C)$) che mostrano la diagonalizzazione.

Soluzione. i) Sia $A' = Q^{-1}AP$ la matrice diagonale associata ad A e consideriamo la base $\mathcal{B}$ di $\mathbb{Z}^2$ data dalle colonne di

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

Dalla relazione $QA' = AP$ segue allora che l'insieme $\mathcal{B}'$ delle colonne di

$$AP = \begin{pmatrix} 1 & 0 \\ 2 & 7 \end{pmatrix}$$

è una base di $\mathrm{Im}(A)$ i cui elementi sono proporzionali agli elementi di $\mathcal{B}$ e i fattori di proporzionalità che legano $\mathcal{B}$ e $\mathcal{B}'$ coincidono coincidono con gli elementi sulla diagonale di A'.

ii) Sia $C' = Q^{-1}CP$ la matrice diagonale associata ad A e consideriamo la base $\mathcal{B}$ di $\mathbb{Z}^2$ data dalle colonne di

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 6 & -2 & -1 \end{pmatrix}.$$

Dalla relazione $QC' = CP$ segue allora che l'insieme delle colonne di

$$CP = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 11 & 0 \\ 6 & -22 & 0 \end{pmatrix}.$$

è una base di $\mathrm{Im}(C)$ i cui elementi sono proporzionali agli elementi di $\mathcal{B}$ e i fattori di proporzionalità che legano $\mathcal{B}$ e $\mathcal{B}'$ coincidono coincidono con gli elementi sulla diagonale di C'.

Definizione. Sia A un anello commutativo unitario. Un A-modulo non nullo è detto *semplice* se è privo di sottomoduli non banali.

Esercizio 3. Sia A un anello commutativo unitario.

i) Mostrare che ogni A-modulo semplice ammette una struttura di anello rispetto alla quale è isomorfo a un quoziente di A per un suo ideale massimale.

ii) (*Lemma di Schur*) Mostrare che un omomorfismo non nullo tra due A-moduli semplici è necessariamente un isomorfismo.

Soluzione. i) Sia V un A-modulo semplice e sia $v_0 \in V$ un elemento non nullo. Consideriamo l'insieme $Av_0 \subset V$: per definizione $av_0 \pm bv_0 = (a \pm b)v_0$, dunque Av_0 è un sottomodulo non nullo (in quanto $v_0 \in Av_0$) e pertanto $Av_0 = V$ poiché V è semplice. Consideriamo l'applicazione

$$\begin{array}{rccc} \phi: & A & \longrightarrow & V \\ & a & \longmapsto & av_0 \end{array}$$

che è suriettiva per la precedente osservazione. Considerando A come modulo su se stesso, ϕ è un omomorfismo di A-moduli e il suo nucleo è un sottomodulo di A, vale a dire un ideale. Dal teorema fondamentale di omomorfismo otteniamo dunque un isomorfismo di A-moduli $V \simeq A/\ker\phi$ e V eredita una naturale struttura di anello da A. Rispetto a tale struttura, l'elemento neutro moltiplicativo coincide con v_0, mentre la moltiplicazione tra elementi di V è definita come segue:

$$vw = (ab)v_0 \qquad \text{se } v = av_0,\ w = bv_0.$$

Mostriamo che V è un campo rispetto a tale struttura di anello: questo in particolare implica che $\ker\phi \subset A$ è un ideale massimale. Sia dunque $w \in V$ un elemento non nullo e consideriamo l'insieme $Aw \subset V$: come nel caso di v_0, la semplicità di V implica che $Aw = V$. Pertanto $v_0 \in Aw$ ed esiste $a \in A$ tale che $aw = v_0$: ma allora $v_0 = w(av_0)$, vale a dire w è invertibile ed il suo inverso coincide con av_0.

ii) Sia $\phi : V \longrightarrow V'$ un omomorfismo tra due A-moduli semplici. Allora $\phi(V) \subset V'$ è un sottomodulo di V' non nullo poiché ϕ è non nullo. Similmente $\ker\phi$ è un sottomodulo di V diverso da V poiché ϕ è non nullo, dunque esso è il sottomodulo nullo. Pertanto ϕ è un isomorfismo di A-moduli.

Esercizio 4. Sia A un anello commutativo unitario e sia M un A-modulo, si definisca l'*annullatore* di V come l'insieme

$$\mathrm{Ann}(V) = \{a \in A \ :\ av = 0 \text{ per ogni } v \in V\}.$$

i) Mostrare che $\mathrm{Ann}(V)$ è un ideale di A.

ii) Determinare l'annullatore dei seguenti $\mathbb{Z}$-moduli:

$$\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4), \qquad \mathbb{Z}.$$

Soluzione. i) Sia $\mathrm{End}(V)$ l'insieme degli omomorfismi di A-moduli di V in se stesso: $\mathrm{End}(V)$ è dotato di una naturale struttura di anello unitario, dove la somma è definita da

$$(\alpha + \beta)(v) = \alpha(v) + \beta(v), \qquad \forall \alpha, \beta \in \mathrm{End}(V), \quad \forall v \in V$$

e dove il prodotto è la composizione naturale di endomorfismi. Rispetto a tale struttura di anello, l'applicazione $\psi : A \times V \longrightarrow V$ definita dalla struttura di A-modulo definisce un omomorfismo di anelli

$$\begin{array}{rccc} \phi: & A & \longrightarrow & \mathrm{End}(V) \\ & a & \longmapsto & \Psi(a) \end{array}$$

dove $\Psi(a) : V \longrightarrow V$ è l'omomorfismo definito da $\Psi(a)(v) = \psi(a, v)$. L'annullatore di V coincide allora con il nucleo di Ψ, e pertanto è un ideale di A.

ii) La struttura di $\mathbb{Z}$-modulo di $\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4)$ è definita mediante la naturale moltiplicazione per un numero intero, pertanto l'annullatore $\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4)$ è descritto come segue:

$$\mathrm{Ann}(\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4)) = \{n \in \mathbb{Z} \ : \ na = nb = nc = 0, \ \forall a \in \mathbb{Z}/(2) \ \forall b \in \mathbb{Z}/(3) \ \forall c \in \mathbb{Z}/(4)\}.$$

Ma allora da $na = 0$ per ogni $a \in \mathbb{Z}/(2)$ otteniamo che $n \in 2\mathbb{Z}$, da $nb = 0$ per ogni $b \in \mathbb{Z}/(3)$ otteniamo che $n \in 3\mathbb{Z}$ e da $nc = 0$ per ogni $c \in \mathbb{Z}/(4)$ otteniamo che $n \in 4\mathbb{Z}$: pertanto $n \in 3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$. Viceversa è facile vedere che $12\mathbb{Z}$ è contenuto nell'annullatore di $\mathbb{Z}/(2) \times \mathbb{Z}/(3) \times \mathbb{Z}/(4)$, dunque l'annullatore cercato è $12\mathbb{Z}$.

Consideriamo ora $\mathbb{Z}$ come $\mathbb{Z}$-modulo: in questo caso, la struttura di modulo coincide con la struttura di anello di $\mathbb{Z}$, e in particolare il prodotto $n \cdot m$ in $\mathbb{Z}$ come $\mathbb{Z}$-modulo coincide con l'usuale prodotto nm. Pertanto gli elementi non nulli contenuti nell'annullatore di $\mathbb{Z}$ coincidono con i divisori dello zero. D'altra parte $\mathbb{Z}$ è un dominio d'integrità, dunque otteniamo $\mathrm{Ann}(\mathbb{Z}) = \{0\}$

Esercizio 5. Sia $d \in \mathbb{Z}$ privo di radici quadrate intere e sia $\mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$ il sottoanello dei numeri complessi della forma $a + b\sqrt{d}$ con $a, b \in \mathbb{Z}$. Mostrare che un numero primo $p \in \mathbb{Z}$ è un elemento primo di $\mathbb{Z}[\sqrt{d}]$ se e solo se $x^2 - d$ è irriducibile in $\mathbb{F}_p[x]$.

Soluzione. Consideriamo l'anello quoziente $\mathbb{Z}[\sqrt{d}]/(p)$. Allora valgono i seguenti isomorfismi:

$$\mathbb{Z}[\sqrt{d}]/(p) \simeq \mathbb{Z}[x]/(p, x^2 - d) \simeq \mathbb{F}_p[x]/(x^2 - d).$$

Poiché $\mathbb{F}_p$ è un campo, otteniamo allora che p è primo in $\mathbb{Z}[\sqrt{d}]$ se e solo se $\mathbb{Z}[\sqrt{d}]/(p)$ è un dominio d'integrità se e solo se $\mathbb{F}_p[x]/(x^2 - d)$ è un dominio d'integrità se e solo se $x^2 - d$ è irriducibile in $\mathbb{F}_p[x]$.