Parte I

Richiami di teoria

0.1 Moduli su PID

In questa sezione studiamo gli A moduli nel caso in cui A sia un dominio a ideali principali. In questo caso valgono le seguenti importanti proprietà.

Moduli su dominio ad ideali principali - Prime proprietà

Sia A un dominio a ideali principali, M un A-modulo e $N \subset M$ un suo sottomodulo non nullo. Si ha:

1. Se M è libero, allora N è libero e $\operatorname{rk} N \leq \operatorname{rk} M$.
2. Se M è finitamente generato, allora N è finitamente generato.

EXpid1

T 1. (→ p. 3) Provare le affermazioni precedenti, se M è finitamente generato.

SOLpid1

Soluzione T. 1 1. Dimostriamo l'enunciato per induzione sul rango di M, ovvero sulla la cardinalità di una sua base. Se M è ciclico, i.e. $M \simeq A$, i suoi sottomoduli sono isomorfi ad ideali di A. Poiché A è un dominio ad ideali principali, esiste dunque $0 \neq a \in A$ tale che $N \simeq (a)$; inoltre $ca = 0$ implica $a = 0$, dato che A è un dominio e quindi $(a) = N$ è libero.
Supponiamo ora che M abbia rango $r+1$ e assumiamo vera la tesi per tutti i moduli di rango minore o uguale a r. Sia $\{m_1, \dots, m_{r+1}\}$ una base di M.
Se definiamo $N_r = N \cap \langle m_1, \dots, m_r \rangle$, eventualmente riordinando gli m_i possiamo supporre $N_r \neq 0$ e quindi, per ipotesi induttiva, si ha che N_r è libero. Quindi se $N = N_r$ allora N è libero, altrimenti sia $N_r \subsetneq N$. Per ogni $n \in N$, esistono unici $b_1, \dots, b_r$ e $a_n \in A$, tali che

$$n = b_1 m_1 + \cdots + b_r m_r + a_n m_{r+1}$$

Definiamo $I = \{a_n \in A \colon n \in N\}$; I è un ideale di A, dal momento che $a_{n_1} + a_{n_2} = a_{n_1+n_2}$ e $ca_n = a_{cn}$. Poiché A è un dominio ad ideali principali, esiste allora $0 \neq a \in A$ tale che $I = (a)$ ed esiste $n_0 \in N \setminus N_r$ tale che $n_0 = b_1 m_1 + \cdots + b_r m_r + a m_{r+1}$. Dimostriamo che $N \cong N_r \oplus \langle n_0 \rangle$. Sia $n \in N$, allora $a_n = ka$, per qualche $k \in A$. Di conseguenza, $n - kn_0 \in N_r$, e quindi $n = (n - kn_0) + kn_0 \in N_r + \langle n_0 \rangle$. Dato

che $m_1,\dots,m_r,n_0$ sono linearmente indipendenti, $N_r \cap \langle n_0 \rangle = 0$ e $N \cong N_r \oplus \langle n_0 \rangle$ è libero.
Dalla dimostrazione segue anche che $\mathrm{rk} N \leq \mathrm{rk} M$.

2. Dato che M è finitamente generato esiste $A^m \xrightarrow{f} M \longrightarrow 0$ omomorfismo surgettivo, allora $f^{-1}(N)$ è un sottomodulo di A^n, dunque è libero e finitamente generato. Di conseguenza, N è finitamente generato.

Vediamo ora che, se A è un dominio ad ideali principali, ogni A-modulo M finitamente generato è isomorfo ad una somma diretta di moduli ciclici, inoltre vogliamo costruire questa decomposizione e provare che è essenzialmente unica.
Indichiamo con $\mathscr{C}_n = \left\{ e_1^{(n)},\dots,e_n^{(n)} \right\}$ la base canonica di A^n.
Se $M = \langle m_1,\dots,m_r \rangle$ è un A-modulo finitamente generato, allora M è isomorfo ad un quoziente di A^r e quindi, se $f : A^r \longrightarrow M$ è l'omomorfismo definito da $f(e_i^{(r)}) = m_i$, si ha la successione esatta

$$0 \longrightarrow \ker f \longrightarrow A^r \xrightarrow{f} M \longrightarrow 0$$

dato che $\ker f \subset A^r$, esso è libero di rango $s \leq r$; fissata allora una sua base $w_1,\dots,w_s$, possiamo definire un omomorfismo $\varphi : A^s \longrightarrow A^r$, $\varphi(e_i^{(s)}) = w_i$. In questo modo, $\ker f \simeq \mathrm{Im}\,\varphi$, da cui segue che $M \simeq A^r/\ker f \simeq \mathrm{coker}\,\varphi$.
Inoltre, fissate delle basi di A^s e A^r possiamo rappresentare l'omomorfismo φ con una matrice $r \times s$. Se scegliamo le basi canoniche $\mathscr{C}_s$ e $\mathscr{C}_r$, otteniamo una matrice $X = (x_{ij})$, le cui colonne generano le relazioni fra i generatori di M; in altri termini, vale che $(a_1,\dots,a_r) \in A^r$ è tale che $a_1m_1 + \dots + a_rm_r = 0$ se e solo se esiste $u \in A^s$ tale che $Xu^t = (a_1,\dots,a_r)^t$, ove ^{t} denota l'usuale trasposizione di vettori.
Quindi, per studiare i moduli finitamente generati su un dominio ad ideali principali, possiamo studiare gli omomorfismi tra moduli liberi e i loro conuclei, ovvero studiare le matrici a coefficienti in A. A questo scopo, introduciamo una forma canonica per le matrici a coefficienti in un dominio ad ideali principali, detta *la forma normale di Smith*.

0.2 La forma normale di Smith

Sia X una matrice $r \times s$ a coefficienti in un dominio a ideali principali A. Su X possiamo eseguire le seguenti operazioni, che chiamiamo *operazioni elementari* *di riga, (risp. di colonna)*,

1. scambiare due righe,(risp. colonne),
2. sommare ad una riga, (risp. colonna), un multiplo non nullo di un'altra riga, (risp. colonna),
3. moltiplicare una riga, (risp. colonna), per un elemento *invertibile* di A.

Ognuna di queste operazioni si ottiene moltiplicando a sinistra, (risp. a destra) la matrice data per la *matrice elementare* ottenuta eseguendo sulla matrice identica la corrispondente operazione elementare.
Diciamo che due matrici X e Y, $r \times s$, sono *equivalenti* se esistono una matrice R invertibile (ossia tale che $\det R \in A^*$) $r \times r$ e una matrice S invertibile $s \times s$, tali che $Y = RXS$. Inoltre, una matrice $r \times s$ $D = (d_{ij})$ si dice *diagonale* se $d_{ij} = 0$, per $i \neq j$.

EXSmith1

T 2. ($\rightarrow$ p. 5) Sia A un dominio ad ideali principali. Allora, ogni matrice X con coefficienti in A è equivalente ad una matrice diagonale.

SOLSmith1

Soluzione T. 2 Consideriamo una matrice 2×2 a coefficienti in A, $X = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, supponiamo $a, b \in A$ non entrambi nulli, e indichiamo con $0 \neq x = \gcd(a, b)$ il loro massimo comun divisore. Allora esistono $s, t \in A$ tali che $sa + tb = x$. Se $R = \begin{pmatrix} s & t \\ -\frac{b}{x} & \frac{a}{x} \end{pmatrix}$, si ha che $\det R = 1$, quindi R è invertibile e moltiplicando X a sinistra per R otteniamo

$$RX = \begin{pmatrix} s & t \\ -\frac{b}{x} & \frac{a}{x} \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} x & * \\ 0 & * \end{pmatrix}$$

che è triangolare superiore e il cui primo elemento diverso da zero della prima colonna è proprio il massimo comun divisore degli elementi della prima colonna di X.
Osserviamo che, considerando la matrice trasposta, X^t, che ha gli elementi a, b nella prima riga, e moltiplicando a destra per la matrice R^t si ottiene una matrice triangolare inferiore

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} s & -\frac{b}{x} \\ t & \frac{a}{x} \end{pmatrix} = \begin{pmatrix} x & 0 \\ * & * \end{pmatrix}$$

in cui il primo elemento diverso da zero della prima riga è uguale al massimo comun divisore degli elementi della prima riga di X^t.

Sia ora X una matrice $r \times s$. Consideriamo la prima colonna di X. Se è nulla passiamo alla seconda colonna, altrimenti eventualmente con scambi di righe, ossia moltiplicando a sinistra per opportune matrici elementari, possiamo applicare la costruzione precedente alle prime due righe e colonne di X, trovare una matrice $R = \left(\begin{array}{c|c} R_2 & 0 \\ \hline 0 & I_{r-2} \end{array}\right)$ tale che $RX = \left(\begin{array}{c|c} \begin{matrix} x & * \\ 0 & * \end{matrix} & * \\ \hline * & * \end{array}\right)$.

Ripetendo questo passo, otteniamo una matrice equivalente (per riga) ad X che nella posizione $(1,1)$ ha un elemento x_1 che è il massimo comun divisore degli elementi della prima colonna di X e tutti gli altri elementi della prima colonna uguali a zero. Nello stesso modo, moltiplicando a destra la matrice ottenuta per opportune matrici invertibili si può sostituire x_1 con un elemento x_2 che è il massimo comun divisore di tutti gli elementi sulla prima riga e azzerare tutti gli altri elementi della prima riga. In questo modo però possono ricomparire elementi diversi da zero nella prima colonna e quindi si deve ripetere il procedimento sulla prima colonna. Con successive applicazioni di questo metodo si costruisce una successione elementi $x_1, x_2, \ldots, x_i, \ldots,$ che sono alternativamente il massimo comun divisore degli elementi della prima colonna e il massimo comun divisore degli elementi della prima riga, e quindi tali che $x_{i+1} | x_i$. Dal momento he A è PID, da questo segue che esiste n tale che $x_n = x_{n+1}$, ma questo dice che x_n è il massimo comun divisore sia degli elementi della prima colonna che della prima riga, e quindi si possono azzerare tutti gli altri elementi sia della prima riga che della prima colonna con operazioni elementari. Iterando il procedimento sulla matrice ottenuta cancellando la prima riga e la prima colonna si ottiene che la matrice può essere diagonalizzata.

La forma normale di Smith

Sia A un dominio ad ideali principali. Una matrice $r \times s$, $D = (d_{ij})$ con coefficienti in A è *in forma di Smith* se

- D è diagonale;
- $d_{11} \mid d_{22} \mid \cdots \mid d_{tt}$, con $t = min(r,s)$.

EXSmith1b

T 3. (→ p. 8) Ogni matrice X con coefficienti in A è equivalente ad una matrice in forma di Smith.

Sia X una matrice a coefficienti in A e definiamo gli ideali

$$\Delta_i(X) = (\{\text{determinanti delle sottomatrici } i \times i \text{ di } X\}).$$

EXdeti

T 4. (→ p. 8) Se X e Y sono due matrici equivalenti; allora,

$$\Delta_i(X) = \Delta_i(Y), \text{ per ogni } i.$$

EXSmith2

T 5. (→ p. 8) Se X è una matrice equivalente ad una matrice $D = (d_{ij})$ in forma di Smith; allora vale che

- $(d_{11}) = \Delta_1(X)$;
- $(d_{ii})\Delta_{i-1}(X) = \Delta_i(X)$ per ogni $i > 1$.

Se indichiamo con δ_i un generatore dell'ideale $\Delta_i(X)$, dalle relazioni precedenti segue che

- $d_{11} = \delta_1$;
- $d_{ii} = \delta_i/\delta_{i-1}$, per ogni $i > 1$ tale che $\delta_{i-1} \neq 0$.

In particolare, quindi, gli elementi d_{ii}, sono unici a meno di elementi associati in A; in questo senso diciamo che ogni matrice X è equivalente ad una matrice in forma di Smith *essenzialmente* unica.

Osservazione. Gli elementi d_{ii} si chiamano *fattori invarianti*. Da quanto detto segue che due matrici hanno gli stessi fattori invarianti se e solo se sono equivalenti.

SOLSmith1b

***Soluzione T.* 3** Applicando la costruzione precedente, possiamo assumere che $X = (x_{ij})$ sia in forma diagonale. Se la matrice non è in forma di Smith, sia i il minimo indice tale che $x_{11} \nmid x_{ii}$; a meno di scambi di riga e colonna, possiamo supporre senza perdita di generalità che $i = 2$.
Sia $x = \gcd(x_{11}, x_{22})$ e siano $s, t \in A$ tali che $sx_{11} + tx_{22} = x$. Se consideriamo le matrici:

$$R = \left(\begin{array}{cc|c} s & t & \\ -\frac{x_{22}}{x} & \frac{x_{11}}{x} & 0 \\ \hline \multicolumn{2}{c|}{0} & I_{r-2} \end{array}\right), \quad S = \left(\begin{array}{cc|c} 1 & -t\frac{x_{22}}{x} & 0 \\ 1 & s\frac{x_{11}}{x} & \\ \hline \multicolumn{2}{c|}{0} & I_{s-2} \end{array}\right);$$

otteniamo che la matrice prodotto $RXS = (y_{ij})$ è una matrice ancora diagonale, con $y_{ij} = x_{ij}$ se $i, j \neq 2$ e $y_{22} = \frac{x_{11}x_{22}}{x}$ e quindi $y_{11} \mid y_{22}$. Iterando il procedimento si ottiene la tesi.

SOLdeti

***Soluzione T.* 4** Sia R una matrice invertibile; dimostriamo che $\Delta_i(RX) = \Delta_i(X)$. Osserviamo che le righe di RX sono combinazioni lineari delle righe di X e quindi, per la multilinearità del determinante, i determinanti delle sottomatrici $i \times i$ di RX sono combinazione lineare dei determinanti delle sottomatrici $i \times i$ di X. Di conseguenza, $\Delta_i(X) \supseteq \Delta_i(RX)$. D'altonde, R è invertibile e vale anche che $\Delta_i(RX) \supseteq \Delta_i(R^{-1}RX) = \Delta_i(X) = \Delta_1(X)$. Quindi $\Delta_i(RX) = \Delta_i(X)$. Per concludere ci basta ora osservare che $\Delta_i(XR) = \Delta_i((XR)^t) = \Delta_i(R^t X^t) = \Delta_i(X^t) = \Delta_i(X)$.

SOLSmith2

***Soluzione T.* 5** Sia $D = (d_{ij})$ diagonale e in forma di Smith equivalente a X. Dal momento che $d_{11}|d_{22}|\cdots|d_{rr}$, per **T.** 4, certamente $\Delta_1(D) = (d_{11}) = \Delta_1(X)$. Inoltre $\Delta_{i+1}(D) = (d_{(i+1)(i+1)}) \cdot \Delta_i(D) = \Delta_{i+1}(X)$, per ogni $1 \leq i < r$.

0.3 Il teorema di struttura per moduli finitamente generati su un dominio ad ideali principali

Otteniamo dall'esistenza della forma normale di Smith e dalle sue proprietà una classificazione dei moduli finitamente generati su un dominio ad ideali principali.

Notazione Se $N =< n_1,\dots,n_s >$ è un sottomodulo di un modulo $L =< w_1,\dots,w_r >$ allora esistono elementi $x_{ij} \in A$ tali che per ogni h si ha $n_h = \sum_k x_{kh} w_1$. Se $X = (x_{ij})$ è la matrice $r \times s$ formata con gli elementi x_{ij}, possiamo scrivere queste relazioni come : $(n_1,\dots,n_s) = (w_1,\dots,w_r)X$.

EX2basi

T 6. ($\rightarrow$ p. 9) Sia L un A modulo libero di rango r e sia $N \subseteq L$ un sottomodulo. Allora esistono una base $v_1,\dots,v_r$ di L e scalari $d_1,\dots,d_s \in A$ tali che $d_1v_1,\dots,d_sv_s$ sono una base di N.

SOL2basi

Soluzione T. 6 Siano $w_1,\dots,w_r$ una base di L e $n_1,\dots,n_s$ una base di N, (che è sottomodulo di un modulo libero e quindi libero, dato che A è PID), allora esiste X matrice $r \times s$ a coefficienti in A tale che

$$(n_1,\dots,n_s) = (w_1,\dots,w_r)X.$$

Per quanto provato prima (cfr. T.3) X è equivalente ad una matrice in forma di Smith D e quindi esistono due matrici invertibili R e S tali che $RXS = D$. Allora otteniamo che

$$(n_1,\dots,n_s)S = (w_1,\dots,w_r)XS = (w_1,\dots,w_r)R^{-1}D$$

Se definiamo $(v_1,\dots,v_r) = (w_1,\dots,w_r)R^{-1}$, dal momento che R è invertibile otteniamo una base di L. Inoltre da:

$$(n_1,\dots,n_s)S = (w_1,\dots,w_r)R^{-1}D = (v_1,\dots,v_r)D = (d_1v_1,\dots,d_tv_t,0,..,0)$$

dal momento che S è invertibile, segue che $t = s$ e $\{d_1v_1,\dots,d_sv_s\}$ sono una base di N.

EXsomma-dir

T 7. ($\rightarrow$ p. 10) **Corollario** Sia L un A modulo libero di rango r, $N \subset L$ un sottomodulo di L di rango s . Se $v_1,\dots,v_r$ è una base di L tale che esistono $d_1,\dots,d_s \in A$ tali che $d_1v_1,\dots,d_sv_s$ sono una base di N allora

$$L/N \cong < \bar{v}_1 > \oplus \dots < \bar{v}_r >$$

Inoltre si ha $(0 : \bar{v}_i) = (d_i)$ per ogni $i = 1,\dots s$ e $(0 : \bar{v}_i) = (0)$ per $i = s+1,\dots,r$. Quindi

$$L/N \cong A/(d_1) \times \dots \times A/(d_s) \times A^{r-s}$$

SOLsomma-dir

Soluzione T. 7 Certamente $\overline{v}_1,\ldots,\overline{v}_r$ generano L/N. Proviamo che la somma è diretta. Sia $a\overline{v}_i \in \sum_{i\neq j} < \overline{v}_j >$, allora $a\overline{v}_i = \sum_{i\neq j} a_j\overline{v}_j$ da cui segue che $av_i - \sum_{i\neq j} a_j v_j \in N$. Esistono quindi $b_1,\ldots,b_s \in A$ tali che $av_i - \sum_{i\neq j} a_j v_j = \sum_{k=1}^{s} b_k d_k v_k$, da cui segue che $a = 0$ se $i > s$ e $a = b_i d_i$ se $i \leq s$. In ogni caso $a\overline{v}_i = 0$ e quindi la somma è diretta. Per concludere vediamo che $a\overline{v}_i = 0$ se e solo se $av_i = \sum_{j=1}^{s} b_j(d_j v_j)$. Se $i \leq s$ questo può succedere se e solo se $a = b_i d_i$ ossia se $a \in (d_i)$, mentre se $i > s$ ciò avviene se e solo se $a = 0$.
Infine lisomorfismo $L/N \cong A/(d_1)\times\ldots\times A/(d_s)\times A^{r-s}$ segue immediatamente dal fatto che $< \overline{v}_i > \cong A/(0:\overline{v}_i)$.

Possiamo ora provare il seguente:

Il teorema di struttura - I

EXdirs

T 8. (→ p. 10) Sia A un dominio a ideali principali e sia M un A-modulo finitamente generato. Allora, esistono ideali principali $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_r$ tali che

$$M \simeq \bigoplus_{i=1}^{r} A\diagup_{I_i} = < m_1 > \oplus \ldots \oplus < m_r > .$$

dove per ogni i, m_i è tale che $I_i = (0:m_i)$.

SOLdirs

Soluzione T. 8 Siano $m_1,\ldots,m_r$ generatori di M allora se $f: A^r \longrightarrow M$ l'omomorfismo definito da $f(e_i) = m_i$, Si ha che $M \cong A^r/\mathrm{Ker}(f)$. Dal momento che $\ker f$ è libero esistono una base $v_1,\ldots,v_r$ di A^r e costanti $d_i,\ldots d_s$ tali che $d_1 v_1,\ldots,d_s v_s$ è una base di di $\ker f$ allora dal corollario precedente segue immediatamente che: $M \cong A^r/\ker(f) = < \overline{v}_1 > \oplus \ldots < \overline{v}_r >$
da cui segue che $M = < f(v_1) > \oplus \ldots < f(v_r) > \cong A/(d_1)\times\ldots\times A/(d_s)\ A^{r-s}$, dove $(0:f(v_i) = (d_i)$ per $i = 1,\ldots,s$ e $(0:f(v_i)) = 0$ per $i = s+1,\ldots,r$. Inoltre se $I_i = (d_i)$ la relazione $I_i \supset I_2 \supset \ldots$ segue al fatto che $d_1|d_2|\ldots$.

In riferimento alla dimostrazione di **T.** 8, è importante osservare che, per quanto visto in precedenza, ogni matrice a coefficienti in A è equivalente ad una matrice in forma normale di Smith; dato che la forma normale di Smith è essenzialmente unica e matrici equivalenti hanno la stessa forma di Smith, è allora chiaro che, scelta un'altra base $w'_1, \ldots, w'_s$ del modulo delle relazioni $\ker f$ la rappresentazione di M come somma diretta di moduli ciclici che si ottiene è la stessa. Non è evidente però che che sarebbe stata la stessa se avessimo scelto un diverso insieme di generatori di M. Vale però il seguente risultato, al quale premettiamo due esercizi:

EXsm-dir

E 1. (→ p. 11) Siano $I, J_1, J_2 \subset A$ ideali e sia M un A-modulo. Se $M = A/J_1 \oplus A/J_2$ allora

$$M/IM \simeq A/(J_1+I) \oplus A/(J_2+I).$$

SOLsm-dir

Soluzione E. 1 Per il secondo teorema di isomorfismo

$$IM \simeq I(A/J_1 \oplus A/J_2) \simeq (I+J_1)/J_1 \oplus (I+J_2)/J_2$$

Dunque:

$$M/IM \simeq \left(A/J_1\right)/\left((J_1+I)/J_1\right) \oplus \left(A/J_2\right)/\left((J_2+I)/J_2\right) \simeq A/(J_1+I) \oplus A/(J_2+I)$$

EXsm-dir2

E 2. (→ p. 11) Sia $J \subset A$ un ideale e $a \in A$. Allora se $M = A/J$ si ha

$$aM \simeq A/(J:a).$$

SOLsm-dir2

Soluzione E. 2

Consideriamo l'omomorfismo di A-moduli $f : A \longrightarrow aM$, $f(b) = b(a+J)$. f è surgettivo e $\ker(f) = \{b \in A \mid ab \in J\} = (J : a)$, quindi, per il primo teorema di omomorfismo, abbiamo la tesi.

EXstrup

T 9. (→ p. 12) Sia A un anello e siano $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m$ e $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_n$ ideali di A, con $m \leq n$, e supponiamo che

$$M \simeq \bigoplus_{i=1}^{m} A/I_i \simeq \bigoplus_{h=1}^{n} A/J_h.$$

Allora

i) $J_1 = J_2 = \cdots = J_{n-m} = A$;

ii) $J_{n-m+i} = I_i$, per ogni $i = 1, \ldots, m$.

SOLstrup

Soluzione T. 9 i) Proviamo che se $n > m$ allora $J_1 = J_2 = \cdots = J_{n-m} = A$; per questo scopo, consideriamo dapprima $B = {}^{A}\!/_{J_1}$ e dimostriamo che $B = 0$. Notiamo subito che, per ipotesi, $J_1 + J_h = J_1$ per ogni $h > 1$, e quindi da **E.** 1 segue che

$$B^n \simeq \bigoplus_{h=1}^{n} {}^{A}\!/_{J_1} \simeq \bigoplus_{h=1}^{n} {}^{A}\!/_{(J_1 + J_h)} \simeq {}^{M}\!/_{J_1 M} \simeq \bigoplus_{i=1}^{m} {}^{A}\!/_{(J_1 + I_i)}.$$

Possiamo dunque proiettare B^m su $\bigoplus_{i=1}^{m} {}^{A}\!/_{(J_1 + I_i)}$ per ottenere un omomorfismo surgettivo da B^m in B^n; dato che $m < n$ questo implica che $B = 0$, cf. **E. ??**. Iterando il ragionamento otteniamo similmente che $J_1 = J_2 = \cdots = J_{n-m} = A$.

ii) Per il punto precedente, possiamo supporre che $m = n$ e, per simmetria ci basta dimostrare che $I_h \subseteq J_h$, per ogni $h = 1, \ldots, m$. Sia allora $a \in I_h$; da **E.** 2 discende che

$$aM \simeq a \left(\bigoplus_{i=1}^{m} {}^{A}\!/_{I_i} \right) \simeq \bigoplus_{i=1}^{m} {}^{A}\!/_{(I_i : a)}$$

Poiché $I_i \subseteq I_{i-1}$, abbiamo anche che $a \in I_i$ per ogni $i \leq h$ e quindi $I_i : a = A$ per tali i. Di conseguenza avremo che

$$\bigoplus_{i=h+1}^{m} {}^{A}\!/_{(I_i : a)} \simeq aM \simeq a \left(\bigoplus_{i=1}^{m} {}^{A}\!/_{J_i} \right) \simeq \bigoplus_{i=1}^{m} {}^{A}\!/_{(J_i : a)}$$

Dal punto i) discende allora che $J_i : a = A$ per ogni $i \leq h$ e dunque che $a \in J_h$.

Ricordiamo che se A è un dominio, e M è un A-modulo il *sottomodulo di torsione*, $T(M)$ di M è definito come l'insieme

$$\{m \in M \mid \exists\, 0 \neq a \in A \text{ t.c. } am = 0\}$$

si dice che M è un modulo di torsione se $M = T(M)$. Se A è un dominio a ideali principali e M è finitamente generato si ha il seguente:

EXdecp1

T 10. (→ p. 13) Sia A un dominio a ideali principali e sia M un A-modulo finitamente generato. Allora, il sottomodulo di torsione $T(M)$ di M è finitamente generato e $M \simeq A^k \oplus T(M)$, per qualche $k \geq 0$. Inoltre, $\{d \in A \colon dT(M) = 0\}$ è un ideale principale diverso da zero.

SOLdecp1

Soluzione T. *10* Dal teorema di struttura **T.** 8, sappiamo che esistono ideali principali $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_r$ tali che $M \simeq \bigoplus_{i=1}^{r} {}^{A}\!/\!_{I_i}$. Se $I_i = 0$ per ogni i, allora $M \simeq A^r$ e $T(M) = 0$. Altrimenti, sia s tale che $I_h \neq 0$ per $h \leq s$ e $I_i = 0$ per $i > s$; allora $T(M) = \bigoplus_{i=1}^{s} {}^{A}\!/\!_{I_i}$ e $M \simeq A^{r-s} \oplus T(M)$. Possiamo concludere osservando che $I_s = \{d \in A \mid dT(M) = 0\}$.

Il risultato precedente mostra come ogni modulo M finitamente generato su un dominio ad ideali principali A si possa decomporre come somma diretta della sua parte libera e della sua parte di torsione. Per decomporre ulteriormente M introduciamo la seguente definizione.

DefinizioneSe M è un A-modulo e $p \in A$ definiamo la *p-componente* di M come $M_p = \{m \in M \mid \exists k \in \mathbb{N}, \text{ t.c. } p^k m = 0\}$. M_p è un sottomodulo di M. Nel caso in cui p sia un elemento primo e $M = M_p$ allora M si dice *p-primario*.

Teorema di struttura - II

Sia A un dominio ad ideali principali e sia $p \in A$ un elemento primo.

EXdcomp1

T 11. (→ p. 14) Sia M un A-modulo p-primario finitamente generato. Allora,

$$M \simeq A/(p^{k_1}) \oplus A/(p^{k_2}) \oplus \cdots \oplus A/(p^{k_s})$$

per certi $k_1 \leq k_2 \leq \ldots \leq k_s$.

EXdcomp2

T 12. (→ p. 14) Sia M un A-modulo finitamente generato. Allora,

$$M \simeq A^k \bigoplus \oplus_{i=1}^{h} A/(q_i)$$

con $(q_i) \subset A$ ideali primari e h, k interi positivi o nulli. Inoltre, l'insieme degli ideali primari che compaiono nella decomposizione è unico, la decomposizione è unica a meno dell'ordine degli addendi, e un ideale può comparire più di una volta. Gli elementi q_i sono unici a meno di associati e si chiamano i *divisori elementari* di M. Il numero $k \geq 0$ si chiama il *numero di Betti* di M.

SOLdcomp1

Soluzione T. *11* Osserviamo innanzittutto che in un PID gli ideali primari non nulli sono potenze di elementi primi, cf. XXX. Per il teorema di struttura **T.** 8 esistono ideali principali $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ tali che $M \simeq \bigoplus_{i=1}^{n} A/I_i$. Dato che M è p-primario, ogni ideale I_i contiene una potenza positiva di p, ma se $p^m \in I_i = (a_i)$ allora $p^m = ba_i$ e quindi $a_i = u_i p^{k_i}$ con u_i unità e $k_i \in \mathbb{N}$, e da ciò segue che $I_i = (p^{k_i})$.

SOLdcomp2

Soluzione T. *12* Ancora per il teorema di struttura **T.** 8 esistono ideali principali $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ tali che $M \simeq \bigoplus_{i=1}^{n} A/I_i$. Se $I_i = (a_i)$ e $a_i = \prod_{j=1}^{h_i} p_{ij}^{e_j}$ è la decomposizione di a_i come prodotto di primi distinti, per il teorema cinese del resto si ha che $A/I_i \simeq \bigoplus_{j=1}^{h_i} A/(p_{ij}^{e_j})$ e quindi

$$M \simeq \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{h_i} A/(p_{ij}^{e_j}),$$

ove gli ideali $(p_{ij}^{e_j})$ sono gli ideali primari cercati.

EXpid3

T 13. (→ p. 15) Sia A un dominio ad ideali principali; allora, un modulo è proiettivo se e solo se è libero.

SOLpid3

Soluzione T. 13 Se M è un A-modulo proiettivo, allora è addendo diretto di un modulo libero ed è dunque isomorfo ad un sottomodulo di un modulo libero; per **T.** 1, tale sottomodulo, e quindi M, è libero. Il viceversa è sempre vero.

0.4 Esercizi PID E SMITH

————-

Forma di Smith

EXec073

E 3. (→ p. 15) Sia $\varphi : \mathbb{Q}[x]^4 \to \mathbb{Q}[x]^4$ l'omomorfismo dato da

$$\varphi(a,b,c,d) = (a+3c, b+2xc+3d, (x^2-x)(a+3c)+2xd, (x^2-x)(b+3d))$$

Trovare la dimensione su $\mathbb{Q}$ di $coker(\varphi)$.

SOLec073

Soluzione E. 3 La forma di Smith della matrice associata a φ (rispetto alle basi canoniche) e' :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x & 0 \\ 0 & 0 & 0 & x^2(x-1) \end{pmatrix}$$

da cui $coker(\varphi) \cong \mathbb{Q}[x]/(x) \oplus \mathbb{Q}[x]/(x^2) \oplus \mathbb{Q}[x]/(x-1) \cong \mathbb{Q} \oplus < 1, x > \mathbb{Q} \oplus \mathbb{Q}$ e $\dim_{\mathbb{Q}} coker(\varphi) = 4$.

Oppure: Se d_1, d_2, d_3, d_4 sono i fattori invarianti nella forma di Smith della matrice M che rappresenta φ si ha che $coker(\varphi) \cong \oplus_i \mathbb{Q}[x]/(d_i)$. Quindi $\dim_{\mathbb{C}} coker(\varphi) = \sum \deg(d_i) = \deg\det(M)$.

EXec071

E 4. (→ p. 16) Sia $\varphi : \mathbb{Z}^3 \to \mathbb{Z}^3$ l'omomorfismo $\varphi(x,y,z) = (6x+2y+4z, ay+4z, 2x+2y+2z)$ con a numero intero. Determinare la classe di isomorfismo di coker(φ) in funzione di a. Esistono valori di a per cui coker(φ) e' infinito?

SOLec071

Soluzione E. 4 La matrice che rappresenta φ (rispetto alle basi canoniche) è :

$$\begin{pmatrix} 6 & 2 & 4 \\ 0 & a & 4 \\ 2 & 2 & 2 \end{pmatrix}$$

Dopo eventuali semplificazioni, calcolando gli ideali Δ_i dei determinanti dei minori $i \times i$ si ottiene:
Se $a = 2k+1$: $\Delta_1 = 1$, $\Delta_2 = 2$ e $\Delta_3 = 4(a-8)$ da cui $\operatorname{coker}(\varphi) \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2a-16)$ e quindi per ogni a dispari $\operatorname{coker}(\varphi)$ e' finito.
Se $a = 2k$: $\Delta_1 = 2$, $\Delta_2 = 4$ e $\Delta_3 = 4(a-8)$ da cui $\operatorname{coker}(\varphi) \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(a-8)$.
Quindi $\operatorname{coker}(\varphi)$ è finito per ogni valore di $a \neq 8$ ed infinito solo se $a = 8$

EXec065

E 5. (→ p. 16) Sia $\varphi : \mathbb{Z}^3 \to \mathbb{Z}^3$ l'omomorfismo definito dalla matrice

$$\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix}$$

con $a, b, c \in \mathbb{Z}$. Provare che :

i) $\operatorname{coker}(\varphi)$ è ciclico se e solo se $\gcd(a,b) = 1$
ii) $\operatorname{coker}(\varphi)$ ha al più due generatori se e solo se $\gcd(a,b,c) = 1$.

SOLec065

Soluzione E. 5 Se $\Delta_1 = \gcd(a,b,c)$, $\Delta_2 = \gcd(a^2, ab, b^2 - ac)$ e $\Delta_3 = a^3$ la forma di Smith della matrice data è :

$$\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}$$

dove i d_i sono dati da: $d_1 = \Delta_1$, $d_2 = \frac{\Delta_2}{\Delta_1}$ $d_3 = \frac{\Delta_3}{\Delta_2}$, e $d_1 | d_2 | d_3$. Da questo segue che $\operatorname{coker}(\varphi) \cong \mathbb{Z}/(d_1) \oplus \mathbb{Z}/(d_2) \oplus \mathbb{Z}/(d_3)$.
(ii) Dalle proprietà dei d_i segue immediatamente che $\operatorname{coker}(\varphi)$ ha al più due generatori se e solo se $d_1 = \gcd(a,b,c) = 1$.
(i) Se $\gcd(a,b) = 1$ allora $\gcd(a^2, ab) = a$, e quindi $d_1 = 1$,

$d_2 = \gcd(a^2, ab, b^2 - ac) = \gcd(a, b^2) = 1$ e quindi coker(φ) è ciclico. Se viceversa coker(φ) e' ciclico innanzitutto da $d_1|d_2|d_3$ otteniamo che $d_1 = d_2 = 1$. Se $k = \gcd(a, b)$ si ha che $k| \gcd(a^2, ab, b^2 - ac) = d_2 = 1$ e quindi $k = 1$.

EXec063

E 6. (→ p. 17) Sia $\varphi : \mathbb{Z}^3 \to \mathbb{Z}^3$ l'omomorfismo definito dalla matrice

$$\begin{pmatrix} a & 6 & 6 \\ -3 & 6 & 0 \\ a & 3 & 3 \end{pmatrix}$$

con $a \in \mathbb{Z}$. Trovare, se esistono, i valori di a per cui:

i) coker(φ) non e' ciclico
ii) coker(φ) è finito.

SOLec063

Soluzione E. 6 Con alcune operazioni elementari possiamo ridurre la matrice e ottenere:

$$\begin{pmatrix} a & 0 & 0 \\ -3 & 6 & 0 \\ 0 & 3 & 3 \end{pmatrix}$$

quindi sicuramente affinché coker(φ) sia finito si deve avere $a \neq 0$ e questo è anche l'unico valore da escludere dato che $\det(A) = -18a$. Considerando $\Delta_1 = (a, 3)$ si ha che $d_1 = \Delta_1 = 1$ se $gcd(a, 3) = 1$ e $d_1 = 3$ altrimenti. In questo ultimo caso, sicuramente coker(φ) non è ciclico. Se $(a, 3) = 1$ otteniamo che $\Delta_2 = (3a, 9) = (3(a, 3)) = (3)$ e quindi anche in questo caso coker(φ) non è ciclico.

EXec064

E 7. (→ p. 17) Sia $M = \mathbb{Z}^3/N$, con N sottomodulo generato da $m_1 = (0, a, b)$, $m_2 = (3, 3, 0)$ e $m_3 = (3, -1, 0)$, con $a, b \in \mathbb{Z}$. Trovare per quali valori di $a, b \in \mathbb{Z}$, M è finito e per quali valori, M è ciclico.

SOLec064

Soluzione E. 7 Troviamo la forma di Smith della matrice A le cui colonne sono i vettori m_1, m_2, m_3, ossia $A = \begin{pmatrix} 0 & 3 & 3 \\ a & 3 & -1 \\ b & 0 & 0 \end{pmatrix}$.

Se Δ_i indica il massimo comun divisore dei determinanti $i \times i$ e $S = diag(d_1, d_2, d_3)$ e' la forma di Smith della matrice A si ha: $d_1 = \Delta_1 = 1$,$d_2 = \Delta_2$ e $d_3 = \frac{\Delta_3}{\Delta_2}$. Si ha $\Delta_2 = (b, 3a, 12), \Delta_3 = 12b$. Quindi affinche' $\#M$ sia finita dobbiamo avere $b \neq 0$.

Se $b \neq 0$ affinche' M sia ciclico dovra' essere $d_2 = (b, 3a, 12) = 1$. Dato che $(b, 3a, 12) = (b, 3(a, 4)) = (b, 3)(b, (a, 4))$ e $(a, 4) = 2$ oppure $(a, 4) = 4$ dovremo avere che $b \not\equiv 0 \pmod 3$ e $(a, b) \not\equiv 0 \pmod 2$.

EXec062

E 8. (→ p. 18) Sia M lo $\mathbb{Z}$-modulo definito da $M = \mathbb{Z}^3/N$, con N sottomodulo generato da $m_1 = (2, 4, -4)$, $m_2 = (4, 12, -12)$ e $m_3 = (2, -4, -4)$. Trovare l'annullatore di M.

SOLec062

Soluzione E. *8* La forma di Smith della matrice A le cui righe sono i vettori m_1, m_2, m_3, e' $A = \begin{pmatrix} 2\,0\,0 \\ 0\,4\,0 \\ 0\,0\,8 \end{pmatrix}$.

Quindi $M \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(4) \oplus \mathbb{Z}/(8)$ e quindi $Ann(M) = (8) \subset \mathbb{Z}$.

EXec059

E 9. (→ p. 18) Siano A, B, C matrici intere 3×3 e sia D la matrice $\begin{pmatrix} A\ C \\ 0\ B \end{pmatrix}$

Supponiamo che $\det A = 28$, e $\det B = 7$. Trovare le possibili forme di Smith di D, esibendo un esempio di ciascuna.

SOLec059

Soluzione E. *9* Dato che $\det A = 28$, e $\det B = 7$ le possibili forme di Smith per A sono matrici che hanno sulla diagonale $1, 1, 28$ e $1, 2 14$, mentre per B abbiamo solo una possibilita' e si ha $B = \mathrm{diag}(1, 1, 7)$

Analogamente, dal momento che il deteminante di $D = 196$ le possibili forme di Smith per D ci sono le seguenti possibilita' che possono essere realizzate per A e C rispettivamente dei deguenti tipi:

1) $D = \mathrm{diag}(1, 1, 1, 1, 1, 196)$, $A = \mathrm{diag}(1, 1, 28)$, $C = \mathrm{diag}(0, 0, 1)$
2) $D = \mathrm{diag}(1, 1, 1, 1, 7, 28)$, $A = \mathrm{diag}(1, 1, 28)$, $C = 0$
3) $D = \mathrm{diag}(1, 1, 1, 1, 2, 98)$, $A = \mathrm{diag}(1, 2, 14)$, $C = \mathrm{diag}(0, 0, 2)$
4) $D = \mathrm{diag}(1, 1, 1, 1, 14, 14)$, $A = \mathrm{diag}(1, 2, 14)$, $C = 0$

EXsm-15

E 10. (→ p. 18) Sia M il gruppo abeliano generato da elementi m_1, m_2 e m_3 che soddisfano le relazioni $3m_1 + m_3 = 0$, $2m_1 - 2m_2 + m_3 = 0$ e $m_1 + 4m_2 + 2m_3 = 0$. Trovare i possibili ordini degli elementi di M.

SOLsm-15

Soluzione E. *10* La matrice delle relazioni tra gli elementi di M è

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

e ha forma di Smith

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 14 \end{pmatrix}.$$

Quindi $M \cong \mathbb{Z}/14$ e i possibili ordini degli elementi di M sono 1,2, 7 e 14.

EXec060

E 11. ($\rightarrow$ p. 19) Sia M una matrice a coefficienti interi $n \times n$ tale che posto $A = \mathbb{Z}^n/M\mathbb{Z}^n$ si abbia che $\forall x \in A$ esiste un primo p_x tale che $p_x x = 0$.
Dimostrare che M è di rango n, e che esiste $p \in \mathbb{Z}$ primo tale che $\det(M) = \pm p^k$ con $k \leq n$.

SOLec060

Soluzione E. *11* A è uno $\mathbb{Z}$-modulo finitamente generato, quindi dal teorema di struttura segue che $A \cong \mathbb{Z}^h \oplus T(A)$ con $k \geq 0$ e $T(A)$ di torsione. Lipotesi che $\forall x \in A$ esiste un primo p_x tale che $p_x x = 0$ implica che $k = 0$ e che A è tutto di torsione. Inoltre, sempre dal teorema di struttura segue che $T(A) = \oplus \mathbb{Z}/I_i = \oplus_i^n < v_i >$ con $I_i \supseteq I_{i+1}$, per ogni i, e $I_i = \mathrm{Ann}(v_i)$. Dal momento che che per gli I tali che $\mathrm{Ann}(v_i) \neq 1$ si ha $\mathrm{Ann}(v_i) = (p_{v_i})$, che è un ideale primo, esiste $s \geq 0$ tale che $I_i = 1$ per $i < s$ e se $p = p_{v_s}$, $I_i = (p)$ per ogni $i \geq s$. Questo implica che M è equivalente ad una matrice con determinante $\pm p^{n-s}$ e quindi la tesi.

EXec061

E 12. ($\rightarrow$ p. 19) Sia $A = K[x,y]/(y^3 - xy^2 - y + x, x^2 - xy + x - y)$.

1. Provare che A e' finitamente generato come $K[x]$ modulo.
2. Rappresentare A come il conucleo di un omomorfismo di $K[x]$ moduli e decomporlo come prodotto diretto di moduli ciclici.

SOLec061

Soluzione E. *12* A e' generato come $K[x]$ modulo da $1, y, y^2$. Se indichiamo con $B = K[x,y]/(y^3 - xy^2 - y + x)$ si ha che B e' un $K[x]$ modulo libero di rango 3. Sia $f : K[x]^3 \longrightarrow B$ l'omomorfismo di $K[x]$ moduli definito come $f(e_1) = x^2 - xy + x - y = h$, $f(e_2) = yh$ e $f(e_3) = y^2 h$ si ha che $\mathrm{Im}(f) =< h, yh, y^2 h > B$ ossia $(x^2 - xy + x - y) = \mathrm{Im}(f)$. Da questo deduciamo che $A \cong B/\mathrm{Im}(f) = \mathrm{coker}\, f$. La matrice che rappresenta f (rispetto alla base $1, y, y^2$ e' data da:

$$\begin{pmatrix} x^2+x & 0 & x^2+x \\ -x-1 & x^2+x & -x-1 \\ 0 & -x-1 & 0 \end{pmatrix}.$$

Riducendo in forma di Smith otteniamo che $d_1 = d_2 = x+1$ e $d_3 = 0$ e quindi $A \cong K \oplus K \oplus K[x]$.

EXec075

E 13. ($\rightarrow$ p. 20) Sia M lo $\mathbb{Z}$-modulo generato dagli elementi m_1, m_2, m_3 che soddisfano le seguenti relazioni:

$$\begin{cases} 2m_1 - 4m_2 - 2m_3 = 0 \\ 10m_1 - 6m_2 + 4m_3 = 0\,, a \in \mathbb{Z} \\ 6m_1 - 12m_2 + am_3 = 0 \end{cases}$$

Rappresentare M come somma diretta di moduli ciclici al variare di $a \in \mathbb{Z}$. Se esistono, trovare per quali valori di a, $\mathrm{Ann}(M) = 0$.

SOLec075

Soluzione E. *13* Consideriamo $\varphi : \mathbb{Z}^3 \longrightarrow M$ data da $\varphi(e_i) = m_i$, allora $M \cong \mathbb{Z}/Ker(\varphi)$. Sia

$$A = \begin{pmatrix} 2 & -4 & -2 \\ 10 & -6 & 4 \\ 6 & -12 & a \end{pmatrix}$$

la matrice delle relazioni tra i generatori di M , riducendo A con alcune operazioni elementari di riga e di colonna si ottiene la matrice:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 6+a \end{pmatrix}$$

da cui segue che la forma di Smith di A è data da:
1. se $a \equiv 8 \pmod{14}$

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 6+a \end{pmatrix}$$

e quindi $M \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(14) \oplus \mathbb{Z}/(a+6)$

2. Se $a \equiv 0 \pmod 2$ e $a \not\equiv 1 \pmod 7$

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 7(6+a) \end{pmatrix}$$

e quindi $M \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/7(a+6)$
3. Se $a \equiv 1 \pmod 2$ e $a \equiv 1 \pmod 7$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 2(6+a) \end{pmatrix}$$

e quindi $M \cong \mathbb{Z}/(14) \oplus \mathbb{Z}/2(a+6)$
4. Se $a \equiv 1 \pmod 2$ e $a \not\equiv 1 \pmod 7$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 14(6+a) \end{pmatrix}$$

e quindi $M \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/14(a+6)$.
L'unico caso in cui $Ann(M) = 0$ si ha per $a = -6$

EXec076

E 14. ($\rightarrow$ p. 22) Sia G_1 il gruppo abeliano generato dagli elementi $\{a, b, c, d\}$ che soddisfano le relazioni

$$\begin{cases} 2a + 2b + c + 3d = 0 \\ -2b + c + 3d = 0 \\ -4a + 4b - 3c - 15d = 0 \\ 6a + 4b + c + 9d = 0 \\ 12a + 4b + c + 21d = 0 \end{cases}$$

e $G_2 \cong \operatorname{coker}(\varphi_\alpha)$ dove $\varphi_\alpha : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ è l'omomorfismo di $\mathbb{Z}$-moduli dato da

$$\varphi_\alpha(x, y, z) = (2x + 8y - 4z, \alpha x + 6y + \alpha z, -2x - 2y + 4z).$$

Determinare se esistono valori di $\alpha \in \mathbb{Z}$, tali che G_1 e G_2 siano isomorfi (come $\mathbb{Z}$-moduli).

SOLec076

Soluzione E. *14* G_1, G_2 sono gruppi abeliani finitamente generati, quindi rappresentabili come somma diretta di gruppi ciclici: saranno isomorfi se e solo se le loro rappresentazioni sono uguali. Consideriamo la matrice

$$A = \begin{pmatrix} 2 & 0 & -4 & 6 & 12 \\ 2 & -2 & 4 & 4 & 4 \\ 1 & 1 & -3 & 1 & 1 \\ 3 & 3 & -15 & 9 & 21 \end{pmatrix}$$

$G_1 \cong coker(\psi)$, dove $\psi : \mathbb{Z}^5 \longrightarrow \mathbb{Z}^4$ è l'omomorfismo associato ad A (rispetto alle basi canoniche). Calcolando la forma di Smith di A si ottiene la matrice:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Da cui otteniamo che $G_1 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}$. Affinché $G_1 \cong G_2 \cong coker(\varphi)$ dobbiamo avere che i fattori invarianti della matrice

$$C = \begin{pmatrix} 2 & 8 & -4 \\ \alpha & 6 & \alpha \\ -2 & -2 & 4 \end{pmatrix}$$

che rappresenta φ siano $2, 6, 0$. Dato che $\Delta_3(C) = \det C = -36a$ l'unico valore possibile è $\alpha = 0$. Poiché si ha anche $d_1(C) = \Delta_1(C) = 2$ e $d_2(C) = \frac{\Delta_2(C)}{d_1(C)} = 6$, per $\alpha = 0$ si ha $G_1 \cong G_2 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/6 \oplus \mathbb{Z}$.

EXec077

E 15. ($\rightarrow$ p. 23) Sia $M_\alpha \cong coker(\varphi_\alpha)$ dove $\varphi_\alpha : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$, $\alpha \in \mathbb{Z}$, è l'omomorfismo di $\mathbb{Z}$ moduli dato da $\varphi_\alpha(x, y, z) = (9\alpha x - 8\alpha y - \alpha z, 4\alpha x - 3\alpha y - \alpha z, -6\alpha x + 7\alpha y - \alpha z)$.

i) Esprimere M_α come somma diretta di $\mathbb{Z}$- moduli ciclici, al variare di $\alpha \in \mathbb{Z}$.
ii) Trovare se esistono i $p \in \mathbb{Z}$ primi e gli $\alpha \in \mathbb{Z}$ tali che $M_\alpha \otimes_{\mathbb{Z}} \mathbb{Z}/(p\mathbb{Z})$ sia ciclico.
iii) Descrivere, al variare di $\alpha \in \mathbb{Z}$ lo $\mathbb{Z}$-modulo $(M_\alpha)_{(5)}$.

Giustificare le risposte.

SOLec077

Soluzione E. 15

1. La matrice che rapresenta φ_α (rispetto alle basi canoniche) è:

$$\begin{pmatrix} 9\alpha & -8\alpha & -\alpha \\ 4\alpha & -3\alpha & -\alpha \\ -6\alpha & 7\alpha & -\alpha \end{pmatrix}$$

   riducendo con operazioni elementari si ottiene la matrice:

$$A_\alpha = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & 5\alpha & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

   Quindi
   a) se $\alpha = 0$, $M_0 \cong \mathbb{Z}^3$,
   b) se $\alpha \neq 0$, $M_\alpha \cong \mathbb{Z}/(\alpha\mathbb{Z}) \times \mathbb{Z}/(5\alpha\mathbb{Z}) \times \mathbb{Z}$
2. Dall'analisi del punto precedente, otteniamo che:
   a) se $\alpha = 0$, $M_0 \otimes_{\mathbb{Z}} \mathbb{Z}/(p\mathbb{Z}) \cong (\mathbb{Z}/(p\mathbb{Z}))^3$.
   b) se $\alpha \neq 0$, $M_\alpha \otimes_{\mathbb{Z}} \mathbb{Z}/(p\mathbb{Z}) \cong \mathbb{Z}/((\alpha, p)\mathbb{Z}) \times \mathbb{Z}/((5\alpha, p)\mathbb{Z}) \times \mathbb{Z}/(p\mathbb{Z})$. Quindi se $(\alpha, p) = (5\alpha, p) = 1$ ossia se $p \neq 5$ e $(\alpha, p) = 1$, allora $M_\alpha \otimes_{\mathbb{Z}} \mathbb{Z}/(p\mathbb{Z})$ è ciclico.
   Se $p = 5$ e $(\alpha, 5) = 1$ otteniamo $M_\alpha \otimes_{\mathbb{Z}} \mathbb{Z}/(5\mathbb{Z}) \cong (\mathbb{Z}/(5\mathbb{Z}))^2$.
   Se $(\alpha, p) = p$, $M_\alpha \otimes_{\mathbb{Z}} \mathbb{Z}/(p\mathbb{Z}) \cong (\mathbb{Z}/(p\mathbb{Z}))^3$ e quindi in entrambi i casi non è ciclico.
3. Ancora considerando l'analisi del punto i) otteniamo che:
   a) se $\alpha = 0$, $(M_0)_{(5)} \cong (\mathbb{Z}_5)^3$.
   b) se $\alpha = 5^k\beta$ con $k \geq 0$ e $\gcd(\beta, 5) = 1$ allora

$$M_\alpha \cong \mathbb{Z}/(5^k\mathbb{Z}) \times \mathbb{Z}/(5^{k+1}\mathbb{Z}) \times \mathbb{Z}/(\beta\mathbb{Z}) \times \mathbb{Z}.$$

   Dato che se $(\beta, 5) = 1$, $\beta \in S = \mathbb{Z} \setminus (p)$ e quindi $(\mathbb{Z}/(\beta\mathbb{Z}))_{(5)} = 0$ e $(\mathbb{Z}/(5^k\mathbb{Z}))_{(5)} \cong \mathbb{Z}/(5^k\mathbb{Z})$ si ha

$$(M_\alpha)_{(5)} \cong \mathbb{Z}/(p^k\mathbb{Z}) \times \mathbb{Z}/(p^{k+1}\mathbb{Z}) \times \mathbb{Z}_{(p)}$$

EXec079

E 16. (→ p. 24) Sia $A_{\alpha,\beta}$ una matrice 6×6 a coefficienti in $\mathbb{R}$, con polinomio caratteristico $p_A(x)=(x-1)^{\alpha}(x-2)^{\beta}(x^2+1)$, $\alpha,\beta\in\mathbb{N}$. Esistono valori di α e β per cui le possibili forme canoniche di Smith delle matrici caratteristiche $A_{\alpha,\beta}-xI$ sono esattamente 4.

SOLec079

Soluzione E. *16* Le possibili forme di Smith di $a-xI$ sono matrici diagonali con sulla diagonale elementi $d_1|d_2|..|d_6$ tali che $d_1..d_6=(x-1)^{\alpha}(x-2)^{\beta}(x^2+1)$. Dalle condizioni di divisibilità segue che (x^2+1) deve essere un fattore di d_6, che $d_1=d_2=1$, che $\alpha+\beta=4$ e che le successioni dei possibili esponenti γ_i di $(x-1)$ in d_i devono soddisfare le seguenti relazioni: $\gamma_3+\gamma_4+\gamma_5+\gamma_6=\alpha$, $\gamma_3\le\gamma_4\le\gamma_5\le\gamma_6$, (analogamente per gli esponenti di $(x-2)$). Si ha quindi:

$$\cup_{\alpha=0}^{4}\{(\gamma_3,\gamma_4,\gamma_5,\gamma_6,\alpha)\}=\{((0,0,0,0,0)\}\cup\{(0,0,0,1,1\}\cup$$

$$\cup\{(0,0,0,2,2),(0,0,1,1,2)\}\cup\{(0,0,0,3,3),(0,0,1,2,3),(0,1,1,1,3)\}\cup$$

$$\cup\{(0,0,0,4,4),(0,0,1,3,4),(0,0,2,2,4),(0,1,1,2,4),(1,1,1,1,4)\}.$$

EXec080

E 17. (→ p. 24) Sia M lo $\mathbb{Z}$-modulo generato da elementi v_1,v_2,v_3,v_4 che soddisfano le relazioni:

$$3v_1=0,\ av_1+3v_2=0,\ bv_2+3v_3=0$$

con $a,b,\in\mathbb{Z}$, $\gcd(a,b)=1$.
Descrivere $T(M)$, il sottodulo di torsione di M, al variare di $a,b,\in\mathbb{Z}$.

SOLec080

Soluzione E. *17* $M\cong\mathbb{Z}^4/coker(\varphi)$, dove $\varphi:\mathbb{Z}^4\longrightarrow\mathbb{Z}^4$ è l'omomorfismo rappresentato dalla matrice

$$A=\begin{pmatrix}3&a&0&0\\0&3&b&0\\0&0&3&0\\0&0&0&0\end{pmatrix}$$

Per calcolare la forma di Smith di A consideriamo gli ideali $\Delta_1=(3,a,b)=(1)$, $\Delta_2=(9,3a,3b,ab)$, $\Delta_3=(27)$.
Se $(3,ab)=1$ allora $\Delta_2=1$, $\Delta_3=(27)$ quindi $M\cong\mathbb{Z}\oplus\mathbb{Z}/(27)$ e $T(M)\cong\mathbb{Z}/(27)$.

Se $(3,ab) = 3$ allora, $\Delta_2 = 3$, $\Delta_3 = (27)$ quindi $M \cong \mathbb{Z} \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(9)$ e $T(M) \cong \mathbb{Z}/(3) \oplus \mathbb{Z}/(9)$.

EXec081

E 18. (→ p. 25) Sia M_a lo $\mathbb{Z}$-modulo generato da elementi m_1, m_2, m_3 che soddisfano le relazioni $2m_1 - m_2 = 0, m_1 + m_2 + m_3 = 0, m_1 + am_2 = 0$, $a \in \mathbb{Z}$. Per ogni $0 < a \in \mathbb{Z}$ esistono dei valori $n \in \mathbb{N}$ per cui $M_a \otimes_{\mathbb{Z}} \mathbb{Z}/n \neq 0$.

SOLec081

Soluzione E. 18

MANCA

EXec082

E 19. (→ p. 25) Sia $N_a \subset \mathbb{Z}^3$ il sottomolulo di $\mathbb{Z}^3$ generato da $m_1 = (2,2,a), m_2 = (2,a,0), m_3 = (0,4,2)$ e sia $M_a = \mathbb{Z}^3/N$. Trovare le classi di isomorfismo di $M_a = \mathbb{Z}^3/N$, al variare di $a \in \mathbb{Z}$. Trovare, se esistono, i valori di $a \in \mathbb{Z}$ per i quali $Hom_{\mathbb{Z}}(\mathbb{Z}/(7), M_a) \neq 0$.

SOLec082

Soluzione E. 19 Sia

$$A = \begin{pmatrix} 2 & 2 & 0 \\ 2 & a & 4 \\ a & 0 & 2 \end{pmatrix}$$

Dato che $\Delta_1 = \gcd(2,a), \Delta_2 = \gcd(4, 2a, a^2)$ e $\Delta_3 = 4(2-3a)$ otteniamo 2 casi:
1) se $\gcd(a,2) = 1$ la forma di Smith è

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4(2-3a) \end{pmatrix}$$

Quindi $M_a \cong \mathbb{Z}/4(2-3a)$.
2) Se $a \equiv 0 \pmod 2$ la forma di Smith è

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & (2-3a) \end{pmatrix}$$

Quindi $M_a \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2-3a)$.
Allora affinché esista $\varphi \in Hom_{\mathbb{Z}}(\mathbb{Z}/(7), M_a)$ non nullo si deve avere $2 - 3a \equiv 0 \pmod 7$.

EXec083

E 20. ($\rightarrow$ p. 26) Indichiamo con M_a lo $\mathbb{Z}$-modulo generato da elementi v_1, v_2, v_3 che soddisfano le relazioni $2v_1 = v_2$, $v_1 = 3v_2, v_1 + v_2 = av_3$, con $a \in \mathbb{Z}$. Posto $a = 3$, costruire, se possibile, un omomorfismo non banale (di $\mathbb{Z}$ moduli) $g : \mathbb{Z}/(20) \longrightarrow M_3$. Descrivere al variare di $a \in \mathbb{Z}$, $Hom_{\mathbb{Z}}(\mathbb{Z}/(20), M_a)$.

SOLec083

Soluzione E. *20* Si ha $M \cong coker(f)$, dove $f : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ ha matrice associata B_f. Calcoliamo la forma di Smith B_f. associata ad f.

$$\mathrm{Smith}(B_f) = \mathrm{Smith}\begin{pmatrix} 2 & -1 & 0 \\ 1 & 3 & 0 \\ 1 & 1 & -a \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5a \end{pmatrix}.$$

da cui segue che $M \cong \mathbb{Z}/(5a)$. Se $a = 3$ basta definire $h : \mathbb{Z}/(20) \longrightarrow \mathbb{Z}(15)$, come $h(n) = 3n$.
Infine, se $a = 0$ si ha $M_0 \cong \mathbb{Z}$ e $Hom_{\mathbb{Z}}(\mathbb{Z}/(20), \mathbb{Z}) = (0)$, se $a \neq 0$, $M_a \cong \mathbb{Z}/(5a)$ quindi dato che $Hom_{\mathbb{Z}}(\mathbb{Z}/(20), M_a) \cong Hom_{\mathbb{Z}}(\mathbb{Z}/(20), \mathbb{Z}/(5a)) \cong \mathbb{Z}/(20, 5a)$ si ha:

- $Hom_{\mathbb{Z}}(\mathbb{Z}/(20), M_a) \cong \mathbb{Z}/(5)$ se $(a, 4) = 1$,
- $Hom_{\mathbb{Z}}(\mathbb{Z}/(20), M_a) \cong \mathbb{Z}/(10)$ se $a = 4k + 2$
- $Hom_{\mathbb{Z}}(\mathbb{Z}/(20), M_a) \cong \mathbb{Z}/(20)$ se $a = 4k$.

EXec084

E 21. ($\rightarrow$ p. 26) Se M uno $\mathbb{Z}$-modulo tale che la successione:

$$0 \longrightarrow \mathbb{Z}^3 \xrightarrow{f} \mathbb{Z}^4 \longrightarrow M \longrightarrow 0$$

con $f(x, y, z) = (x + y + z, -3x + y + z, x - 3y - 3z, x + 3y + z)$ è esatta. Esprimere M come somma diretta di $\mathbb{Z}$-moduli ciclici.

SOLec084

Soluzione E. *21* $M \cong \mathrm{coker} f$, cerchiamo quindi la forma di Smith della matrice che rappresenta f

$$\mathrm{Smith}(B_f) = \mathrm{Smith}\begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & -3 \\ 1 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix}.$$

da cui deduciamo che $M \cong \mathbb{Z} \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(4)$

EXec086

E 22. (→ p. 27) Un A modulo M si dice irriducibile se $M \neq 0$ e se 0 e M sono i soli sottomoduli di M.

1. Provare che un A modulo M è irriducibile se e solo se $M \neq 0$ e $\forall\, 0 \neq m \in M$ si ha $< m >= M$.
2. Determinare tutti gli $\mathbb{Z}$-moduli irriducibili.
3. Sia $\psi : \mathbb{Z}^3 \longrightarrow M$ un omomorfismo surgettivo di $\mathbb{Z}-moduli$, tale che $Ker(\psi) =< m_1, m_2, m_3 >$, dove $m_1 = (2,4,6), m_2 = (0,a,2a), m_3 = (b,4,6)$, $a,b \in \mathbb{Z}$. Trovare se esistono $a,b \in \mathbb{Z}$ tali che lo $\mathbb{Z}$-modulo M è irriducibile.

SOLec086

Soluzione E. 22

1. Sia M irriducibile e sia $m \in M$. Allora il sottomodulo ciclico $< m >\subset M$ è un sottomodulo di M e quindi per ipotesi $< m >= M$, ossia M è ciclico e ogni elemento non zero di M è un suo generatore. Viceversa supponiamo che M sia ciclico generato da un qualunque elemento diverso da zero sia $N \subset M$ un sottomodulo di M. Per ogni $0 \neq n \in N \subset M$, $< n >$ è un sottomodulo non zero di M Allora per ogni elemento $0 \neq n \in N$, $< n >= M$ e quindi $N = M$. Dato che ogni sottomodulo diverso da zero contiene almeno un sottomodulo $< n >$, M è irriducibile.
2. Ogni $\mathbb{Z}$-modulo è un gruppo abeliano, dovendo essere ciclico e tale che ogni elemento non zero sia un generatore, devono essere gruppi ciclici di ordine primo.
3. Se $\varphi : \mathbb{Z}^3 \longrightarrow \mathbb{Z}^3$ è dato da $\varphi(e_i) = m_i$, $M \cong \mathbb{Z}^3/Ker(\psi) \cong coker(\varphi)$. La matrice che rappresenta φ (rispetto alle basi canoniche) è
$$\begin{pmatrix} 2 & 0 & b \\ 4 & a & 4 \\ 6 & 2a & 6 \end{pmatrix}.$$
Riducendo con operazioni elementari otteniamo
$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b-2 \end{pmatrix}.$$
quindi scegliendo ad esempio $a = 1$ e $b = 3$ si ha $M \cong \mathbb{Z}/2\mathbb{Z}$ che e' irriducibile.

EX0165

E 23. ($\rightarrow$ p. 28) Sia $A = k[x,y,z]$, $I = (x^2 + y^2 - z, xy - 1)$.

i) Dimostrare che A/I è un $k[z]$ modulo finitamente generato.

ii) Trovarne un insieme di generatori

iii) decomporre A/I come somma diretta di $k[z]$ moduli ciclici

SOL0165

Soluzione E. 23 i)-ii) Calcolando una base di Gröbner lex, $x > y > z$, di I Si ha $I = (x + y^3 - yz, y^4 - y^2z + 1)$, da cui $A \cong k[z][y]/(y^4 - y^2z + 1)$ e' generato come $k[z]$-modulo da $< 1, y, y^2, y^3 >$ (il polinomio $y^4 - y^2z + 1$ e' monico quindi si puo' fare la divisione su $k[z]$). iii) dato che $< 1, y, y^2, y^3 >$ sono indipendenti modulo I essi sono una base e quindi $A \cong k[z]^4$.

EXec070

E 24. ($\rightarrow$ p. 28) Sia $I = (z^2 + xy, x^2y - y^2z + z^2, x^2 + xy + 2yz, x^2 - yz) \subset k[x,y,z]$

1. Provare che I e' un ideale monomiale
2. Determinare un insieme di generatori del $k[y]$-modulo $M = k[x,y,z]/I$.
3. Il $k[y]$-modulo M e' un modulo libero?
4. Rappresentare M come conucleo di un omomorfismo di $k[y]$-moduli e decomporlo come prodotto diretto di moduli ciclici e calcolarne la forma di Smith

SOLec070

Soluzione E. 24

1. La base di Gröbner di I rispetto all'ordinamento lessicografico con $x > y > z$ e' data da $\{x^2, xy, yz, z^2\}$ quindi I e' monomiale.
2. M come $k[y]$-modulo e' generato da $1, x, z, xz$.
3. Dato che $yx = 0$ in M, M contiene un elemento di torsione diverso da zero e quindi non e' libero.
4. Consideriamo l'omorfismo $\varphi : k[y]^4 \longrightarrow M$ dato da $\varphi(e_1) = 1$, $\varphi(e_2) = x$, $\varphi(e_3) = z$ e $\varphi(e_4) = xz$. Se $(a_1, a_2, a_3a_4) \in Ker(\varphi)$ otteniamo che $(a_1, a_2, a_3, a_4) = (0, yb_2, yb_3, yb_4)$ quindi $M \cong k^3 \times k[y]$.