ALGEBRA 1 PB-Z
XII. 8 VI 2012

Esercizio 1. Siano $a(\mathrm{X}) \in \mathbb{Z}[\mathrm{X}]$ il polinomio definito da

$$a(\mathrm{X}) \;=\; 2\mathrm{X}^3 + 3\mathrm{X}^2 - 11\mathrm{X} - 6$$

e A l'anello definito da

$$\mathrm{A} \;=\; \mathbb{Z}[\mathrm{X}]/\langle a(\mathrm{X})\rangle$$

Si fattorizzi $a(\mathrm{X})$ in $\mathbb{Z}[\mathrm{X}]$ e si dica se A è un campo o un dominio di integrità.

Dato $e(\mathrm{X}) = 4\mathrm{X}^2 - 6\mathrm{X} - 4 \in \mathbb{Z}[\mathrm{X}]$, sia $\overline{e(\mathrm{X})} \in \mathrm{A}$ la classe di equivalenza di $e(\mathrm{X})$ secondo la relazione indotta da A.

Si esibisca una fattorizzazione di $\overline{e(\mathrm{X})}$ in A e si determinino gli ideali dell'anello quoziente $\mathrm{A}/\langle\overline{e(\mathrm{X})}\rangle$.

Soluzione. Iniziamo, osservando che il grado del polinomio $a(\mathrm{X})$ è uguale a tre. Quindi, per quanto stabilito dalla teoria, $a(\mathrm{X})$ è irriducibile su $\mathbb{Z}$ se e solo se non ammette zeri in $\mathbb{Q}$. Ossia, nel caso specifico del polinomio $a(\mathrm{X})$, il problema della sua (ir)riducibilità su $\mathbb{Z}$ e quello dell'esistenza di suoi (eventuali) zeri razionali sono equivalenti. Ora, poiché il problema della ricerca di zeri razionali per un polinomio di terzo grado è, in virtù del "criterio di ricerca di eventuali zeri razionali di un polinomio a coefficienti interi" ([1]), algoritmicamente più agevole, rivolgiamo la nostra attenzione proprio alla ricerca degli eventuali zeri razionali di $a(\mathrm{X})$.

In base a quanto stabilito dal suddetto criterio e tenuto conto che, nel nostro caso, scrivendo $a(\mathrm{X}) = a_3\mathrm{X}^3 + a_2\mathrm{X}^2 + a_1\mathrm{X} + a_0$, abbiamo $a_0 = -6$ e $a_3 = 2$, gli eventuali zeri razionali di $a(\mathrm{X})$ sono i numeri $\{\pm 1, \pm 2, \pm 3, \pm\frac{1}{2}, \pm\frac{3}{2}\}$.

Ora, una semplice verifica diretta, consente di affermare che i tre numeri 2, -3 e $-\frac{1}{2}$ sono (tutti e soli gli) zeri di $a(\mathrm{X})$. Ossia,

$$\mathrm{Zeri}_{a(\mathrm{X})} \;=\; \{2, -3, -\frac{1}{2}\}$$

Quindi, il polinomio $a(\mathrm{X})$, possedendo (ben tre) zeri razionali è riducibile su $\mathbb{Z}$. Proseguendo per un istante lungo questo cammino, arriviamo al punto di poter affermare che, per quanto trovato in precedenza, esiste un numero $\kappa \in \mathbb{Q}$ tale che

$$2\mathrm{X}^3 + 3\mathrm{X}^2 - 11\mathrm{X} - 6 \;=\; a(\mathrm{X}) \;=\; \kappa \cdot (\mathrm{X} - 2) \cdot (\mathrm{X} - (-3)) \cdot (\mathrm{X} - (-\frac{1}{2})).$$

[1] Ricordiamo l'enunciato di questo criterio. Dato $p(\mathrm{X}) \in \mathbb{Z}[\mathrm{X}]$, $p(\mathrm{X}) = \sum_{\iota=0}^{n} a_\iota \mathrm{X}^\iota$, sia $\alpha \in \mathbb{Q}$, $\alpha = \frac{\nu}{\delta}$ con $(\nu, \delta) = 1$, tale che $p(\alpha) = 0$. Allora $\nu | a_0$ e $\delta | a_n$.

A questo punto una seconda e altrettanto semplice verifica diretta, effettuata moltiplicando i fattori del membro di destra dell'uguaglianza riportata appena sopra e confrontando il polinomio risultato di questa operazione con l'espressione originale di $a(\mathrm{X})$, permette di dire che $\kappa = 2$. Così,

$$2\mathrm{X}^3 + 3\mathrm{X}^2 - 11\mathrm{X} - 6 \;=\; 2(\mathrm{X}-2)(\mathrm{X}+3))(\mathrm{X}+\frac{1}{2})).$$

Rispondiamo, ora, alla domanda circa le proprietà dell'anello $\mathrm{A} = \mathbb{Z}[\mathrm{X}]/\langle a(\mathrm{X})\rangle$. Affermo che A non è un dominio di integrità né, dunque, un campo. A, infatti, possiede degli elementi che dividono 0_{A}, lo zero di A. Questo fatto può esser verificato così. Detta $\pi_{\mathrm{A}} : \mathbb{Z}[\mathrm{X}] \to \mathrm{A}$ la proiezione canonica, consideriamo i seguenti elementi di A: $\pi_{\mathrm{A}}(2(\mathrm{X}-2))$ e $\pi_{\mathrm{A}}((\mathrm{X}+3))(\mathrm{X}+\frac{1}{2})))$. Allora, come il seguente semplice calcolo dimostra, il loro prodotto è uguale a 0_{A}.

$$\pi_{\mathrm{A}}(2(\mathrm{X}-2)) \cdot \pi_{\mathrm{A}}((\mathrm{X}+3))(\mathrm{X}+\frac{1}{2}))) = \pi_{\mathrm{A}}(2(\mathrm{X}-2)(\mathrm{X}+3)\mathrm{X}+\frac{1}{2}) = \pi_{\mathrm{A}}(0) = 0_{\mathrm{A}}$$

Dunque, come detto poco sopra, A possiede divisori dello zero. Quindi, A non è un dominio di integrità né, a maggior ragione, un campo.

Consideriamo, ora, il polinomio $e(\mathrm{X}) = 4\mathrm{X}^2 - 6\mathrm{X} - 4 \in \mathbb{Z}[\mathrm{X}]$ e studiamone la riducibilità su $\mathbb{Z}$. La stessa tecnica or ora usata per lo studio della riducibilità su $\mathbb{Z}$ di di $a(\mathrm{X})$ ([2]), permette di affermare che, in $\mathbb{Z}[\mathrm{X}]$, $e(\mathrm{X})$ ammette la seguente fattorizzazione

$$e(\mathrm{X}) \;=\; 4(\mathrm{X}-2)(\mathrm{X}+\frac{1}{2})$$

Dunque, il polinomio $e(\mathrm{X})$ è riducibile su $\mathbb{Z}$. Inoltre, invito ad osservare esplicitamente che (tutti e soli) gli zeri del polinomio $e(\mathrm{X})$ sono i numeri razionali 2 e $-\frac{1}{2}$. Ossia,

$$\mathrm{Zeri}_{e(\mathrm{X})} \;=\; \{2, -\frac{1}{2}\}$$

Una fattorizzazione in A di $\overline{e(\mathrm{X})} = \pi_{\mathrm{A}}(e(\mathrm{X}))$ può essere ottenuta sfruttando la fattorizzazione di $e(\mathrm{X})$ in $\mathbb{Z}[\mathrm{X}]$. Infatti, procedendo in questa maniera, otteniamo la seguente fattorizzazione di $\overline{e(\mathrm{X})} = \pi_{\mathrm{A}}(e(\mathrm{X}))$ in A.

$$\pi_{\mathrm{A}}(e(\mathrm{X})) = \pi_{\mathrm{A}}(4(\mathrm{X}-2)(\mathrm{X}+\frac{1}{2})) = \pi_{\mathrm{A}}(4) \cdot \pi_{\mathrm{A}}((\mathrm{X}-2)) \cdot \pi_{\mathrm{A}}((\mathrm{X}+\frac{1}{2}))$$

Osserviamo, qui, che, sebbene $\mathrm{Zeri}_{e(\mathrm{X})} \subsetneq \mathrm{Zeri}_{a(\mathrm{X})}$, risulta $2 \notin 4\mathbb{Z}$. Dunque, gli ideali $\langle a(\mathrm{X})\rangle$ e $\langle e(\mathrm{X})\rangle$ di $\mathbb{Z}[\mathrm{X}]$ son tra loro **inconfrontabili**. Ossia,

$$\langle a(\mathrm{X})\rangle \;\not\leq\; \langle e(\mathrm{X})\rangle \;\text{ e }\; \langle a(\mathrm{X})\rangle \;\not\geq\; \langle e(\mathrm{X})\rangle$$

[2]Che possiamo utilizzare questa tecnica è conseguenza del fatto che il grado di $e(\mathrm{X})$ è uguale a due.

Passiamo, ora, a determinare gli ideali dell'anello $\mathrm{E} \overset{def}{=} \mathrm{A}/\langle\overline{e(\mathrm{X})}\rangle$. A tal fine, detta $\pi_{\mathrm{E}} : \mathrm{A} \to \mathrm{E}$ la proiezione canonica, consideriamo il seguente diagramma di applicazioni

$$\mathbb{Z}[\mathrm{X}] \xrightarrow{\pi_{\mathrm{A}}} \mathrm{A} \xrightarrow{\pi_{\mathrm{E}}} \mathrm{E}$$

Ricordiamo che, per quanto stabilito dalla teoria, gli ideali di A sono in corrispondenza biunivoca, tramite π_{A}, con gli ideali di $\mathbb{Z}[\mathrm{X}]$ che contengono $\pi_{\mathrm{A}}^{-1}(0_{\mathrm{A}}) = \langle a(\mathrm{X})\rangle \leq \mathbb{Z}[\mathrm{X}]$. Analogamente, gli ideali di E, tramite π_{E}, corrispondono biunivocamente agli ideali di A che contengono $\pi_{\mathrm{E}}^{-1}(0_{\mathrm{E}}) = \langle\pi_{\mathrm{A}}(e(\mathrm{X}))\rangle) = \langle\overline{e(\mathrm{X})}\rangle \leq \mathrm{A}$. Ne segue che gli ideali di E, tramite $\pi_{\mathrm{E}} \circ \pi_{\mathrm{A}}$, sono in corrispondenza biunivoca con gli ideali di $\mathbb{Z}[\mathrm{X}]$ che contengono l'ideale $[\pi_{\mathrm{E}} \circ \pi_{\mathrm{A}}]^{-1}(0_{\mathrm{E}}) = [\pi_{\mathrm{E}} \circ \pi_{\mathrm{A}}]^{-1}(\langle[\pi_{\mathrm{E}} \circ \pi_{\mathrm{A}}](e(\mathrm{X}))\rangle)$. Ossia, detto $\mathrm{Idl}_{\mathrm{E}}$ l'insieme degli ideali di E, abbiamo

$$\mathrm{Idl}_{\mathrm{E}} \;=\; [\pi_{\mathrm{E}} \circ \pi_{\mathrm{A}}]\{I \in \mathrm{Idl}_{\mathbb{Z}[\mathrm{X}]} \mid I \supseteq [\pi_{\mathrm{E}} \circ \pi_{\mathrm{A}}]^{-1}(\langle[\pi_{\mathrm{E}} \circ \pi_{\mathrm{A}}](e(\mathrm{X}))\rangle)\}$$

Al fine di rendere più esplicita la descrizione di $\mathrm{Idl}_{\mathrm{E}}$, studiamo $\mathrm{Idl}_{\mathrm{A}}$, l'insieme degli ideali di A. Questo insieme, detto $\mathrm{Idl}_{\mathbb{Z}[\mathrm{X}]}(a(\mathrm{X}))$ l'insieme i cui elementi sono gli ideali di $\mathbb{Z}[\mathrm{X}]$ che contengono l'ideale $\langle a(\mathrm{X})\rangle$ generato da $a(\mathrm{X})$, come accennato poco sopra, ammette la seguente descrizione

$$\mathrm{Idl}_{\mathrm{A}} \;=\; \pi_{\mathrm{A}}\{I \in \mathrm{Idl}_{\mathbb{Z}[\mathrm{X}]} \mid I \supseteq \langle a(\mathrm{X})\rangle\} \;=\; \pi_{\mathrm{A}}(\mathrm{Idl}_{\mathbb{Z}[\mathrm{X}]}(a(\mathrm{X})))$$

Considerando, ora, la fattorizzazione in $\mathbb{Z}[\mathrm{X}]$ di $a(\mathrm{X})$, abbiamo la seguente descrizione esplicita dell'insieme $\mathrm{Idl}_{\mathbb{Z}[\mathrm{X}]}(a(\mathrm{X}))$. Esso coincide con l'insieme qui appresso descritto

$\{\ \mathbb{Z}[\mathrm{X}]\ ,\ \langle 2\rangle,\ \langle \mathrm{X}-2\rangle,\ \langle \mathrm{X}+3\rangle,\ \langle \mathrm{X}+\tfrac{1}{2}\rangle\ ,\ \langle 2(\mathrm{X}-2)\rangle,\ \langle 2(\mathrm{X}+3)\rangle,\ \langle 2(\mathrm{X}+\tfrac{1}{2})\rangle,\ \langle(\mathrm{X}-2)(\mathrm{X}+3)\rangle,\ \langle(\mathrm{X}-2)(\mathrm{X}+\tfrac{1}{2})\rangle,\ \langle(\mathrm{X}+3)(\mathrm{X}+\tfrac{1}{2})\rangle\ ,\ \langle 2(\mathrm{X}-2)(\mathrm{X}+3)\rangle,\ \langle 2(\mathrm{X}-2)(\mathrm{X}+\tfrac{1}{2})\rangle,\ \langle 2(\mathrm{X}+3)(\mathrm{X}+\tfrac{1}{2})\rangle,\ \langle(\mathrm{X}-2)(\mathrm{X}+3)(\mathrm{X}+\tfrac{1}{2})\rangle\ ,\ \langle 2(\mathrm{X}-2)(\mathrm{X}+3)(\mathrm{X}+\tfrac{1}{2})\rangle\ \}$

Allora, da $\mathrm{Idl}_{\mathrm{A}} \;=\; \pi_{\mathrm{A}}(\mathrm{Idl}_{\mathbb{Z}[\mathrm{X}]}(a(\mathrm{X})))$, otteniamo la seguente descrizione esplicita di $\mathrm{Idl}_{\mathrm{A}}$

$\{\ \mathrm{A}\ ,\ \pi_{\mathrm{A}}(\langle 2\rangle),\ \pi_{\mathrm{A}}(\langle \mathrm{X}-2\rangle),\ \pi_{\mathrm{A}}(\langle \mathrm{X}+3\rangle),\ \pi_{\mathrm{A}}(\langle \mathrm{X}+\tfrac{1}{2}\rangle)\ ,\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}-2)\rangle),\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}+3)\rangle),\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}+\tfrac{1}{2})\rangle)\ ,\ \pi_{\mathrm{A}}(\langle(\mathrm{X}-2)(\mathrm{X}+3)\rangle),\ \pi_{\mathrm{A}}(\langle(\mathrm{X}-2)(\mathrm{X}+\tfrac{1}{2})\rangle),\ \pi_{\mathrm{A}}(\langle(\mathrm{X}+3)(\mathrm{X}+\tfrac{1}{2})\rangle)\ ,\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}-2)(\mathrm{X}+3)\rangle),\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}-2)(\mathrm{X}+\tfrac{1}{2})\rangle),\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}+3)(\mathrm{X}+\tfrac{1}{2})\rangle),\ \pi_{\mathrm{A}}(\langle(\mathrm{X}-2)(\mathrm{X}+3)(\mathrm{X}+\tfrac{1}{2})\rangle)\ ,\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}-2)(\mathrm{X}+3)(\mathrm{X}+\tfrac{1}{2})\rangle)\ \}$

Ora, detto $\mathrm{Idl}_{\mathrm{A}}(\pi_{\mathrm{A}}(e(\mathrm{X})))$ l'insieme degli ideali di A che contengono $\pi_{\mathrm{A}}(e(\mathrm{X})) = \overline{e(\mathrm{X})}$, abbiamo $\mathrm{Idl}_{\mathrm{E}} = \pi_{\mathrm{E}}(\mathrm{Idl}_{\mathrm{A}}(\pi_{\mathrm{A}}(e(\mathrm{X}))))$. Dunque, la risposta alla domanda sarà data non appena avremo individuato gli elementi di $\mathrm{Idl}_{\mathrm{A}}(\pi_{\mathrm{A}}(e(\mathrm{X}))) \subsetneq \mathrm{Idl}_{\mathrm{A}}$. La risoluzione di quest'ultimo problema è, a questo punto, estremamente semplice, 'ché può esser fatta a mano, essendo $\mathrm{Idl}_{\mathrm{A}}$ un insieme finito che, per di più, contiene un numero esiguo di elementi. Il risultato di questa verifica è il seguente

$\mathrm{Idl}_{\mathrm{A}}(\pi_{\mathrm{A}}(e(\mathrm{X}))) \;=\; \{\ \mathrm{A}\ ,\ \pi_{\mathrm{A}}(\langle 2\rangle),\ \pi_{\mathrm{A}}(\langle \mathrm{X}-2\rangle),\ \pi_{\mathrm{A}}(\langle \mathrm{X}+\tfrac{1}{2}\rangle)\ ,\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}-2)\rangle),\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}+\tfrac{1}{2})\rangle)\ ,\ \pi_{\mathrm{A}}(\langle 2(\mathrm{X}-2)(\mathrm{X}+\tfrac{1}{2})\rangle)\ \}$

Quindi, da $\mathrm{Idl}_{\mathrm{E}} \;=\; \pi_{\mathrm{E}}(\mathrm{Idl}_{\mathrm{A}}(\pi_{\mathrm{A}}(e(\mathrm{X}))))$, abbiamo

$\mathrm{Idl_E} = \{ \mathrm{E} , [\pi_\mathrm{E} \circ \pi_\mathrm{A}](\langle 2 \rangle), [\pi_\mathrm{E} \circ \pi_\mathrm{A}](\langle \mathrm{X} - 2 \rangle), [\pi_\mathrm{E} \circ \pi_\mathrm{A}](\langle \mathrm{X} + \frac{1}{2} \rangle) , [\pi_\mathrm{E} \circ \pi_\mathrm{A}](\langle 2(\mathrm{X} - 2) \rangle), [\pi_\mathrm{E} \circ \pi_\mathrm{A}](\langle 2(\mathrm{X} + \frac{1}{2}) \rangle) , [\pi_\mathrm{E} \circ \pi_\mathrm{A}](\langle 2(\mathrm{X} - 2)(\mathrm{X} + \frac{1}{2}) \rangle) \}$

Esercizio 2. Si diagonalizzi la seguente matrice a coefficienti interi

$$\begin{pmatrix} -21 & 12 & 3 & 24 \\ -14 & 6 & -2 & 11 \\ -35 & -18 & -50 & -118 \end{pmatrix}$$

Soluzione. ono riuscito a trovare una successione di operazioni elementari che mi ha permesso di trasformare la matrice data

$$A = \begin{pmatrix} -21 & 12 & 3 & 24 \\ -14 & 6 & -2 & 11 \\ -35 & -18 & -50 & -118 \end{pmatrix}$$

nella matrice

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

EccoVi la successione di operazioni da me trovata.

1. sostituisco la IV colonna con la colonna ottenuta sottraendo 2 volte la II colonna alla IV colonna ([3])

2. sostituisco la III colonna con la colonna ottenuta sottraendo la IV colonna alla III colonna ([4])

3. sostituisco la I colonna con la colonna ottenuta addizionando 2 volte la II colonna alla I colonna ([5])

4. sostituisco la I colonna con la colonna ottenuta sottraendo la III colonna alla I colonna ([6])

---

[3]La matrice che descrive questa operazione e che bisogna moltiplicare a destra di A è $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

[4]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A l'operazione 1. è $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}$.

[5]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-2. è $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

[6]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-3. è $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

5. sostituisco la I colonna con la colonna ottenuta sottraendo la IV colonna alla I colonna ([7])

6. sostituisco la IV colonna con la colonna ottenuta sottraendo 4 volte la I colonna alla IV colonna ([8])

7. sostituisco la III colonna con la colonna ottenuta sottraendo la IV colonna alla III colonna ([9])

8. sostituisco la IV colonna con la colonna ottenuta addizionando la I colonna alla IV colonna ([10])

9. sostituisco la II colonna con la colonna ottenuta sottraendo 9 volte la I colonna alla II colonna ([11])

10. sostituisco la III colonna con la colonna ottenuta addizionando 15 volte la I colonna alla III colonna ([12])

11. sostituisco la II colonna con la colonna ottenuta addizionando 6 volte la IV colonna alla II colonna ([13])

---

[7]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-4. è $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$.

[8]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-5. è $\begin{pmatrix} 1 & 0 & 0 & -4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

[9]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-6. è $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}$.

[10]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-7. è $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

[11]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-8. è $\begin{pmatrix} 1 & -9 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

[12]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-9. è $\begin{pmatrix} 1 & 0 & 15 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

[13]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-10. è $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 6 & 0 & 1 \end{pmatrix}$.

12. sostituisco la II colonna con la colonna ottenuta sottraendo 4 volte la III colonna alla II colonna ([14])

13. sposto la I colonna al posto della II colonna e la II colonna al posto della I colonna ([15])

14. sposto la I colonna al posto della III colonna e la III colonna al posto della I colonna ([16])

15. sposto la III colonna al posto della IV colonna e la IV colonna al posto della III colonna ([17])

16. sposto la II riga al posto della III riga e la III riga al posto della II riga ([18])

Il risultato delle operazioni elementari qui sopra elencate può essere descritto come il risultato della moltiplicazione di A a destra con P^{-1} e a sinistra con Q, essendo

$$P^{-1} \stackrel{def}{=} \begin{pmatrix} 19 & 1 & -3 & -103 \\ 42 & 2 & -8 & -233 \\ -38 & -3 & 7 & 212 \\ -2 & 0 & 1 & 14 \end{pmatrix}$$

e

$$Q \stackrel{def}{=} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Ossia, $A' = QAP^{-1}$ o, più esplicitamente,

---

[14]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-11. è $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & -4 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

[15]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-12. è $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

[16]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-13. è $\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

[17]La matrice che descrive questa operazione e che bisogna moltiplicare a destra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-14. è $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

[18]La matrice che descrive questa operazione e che bisogna moltiplicare a sinistra della matrice ottenuta dopo aver applicato ad A le operazioni 1.-15. è $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

$$\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} -21 & 12 & 3 & 24 \\ -14 & 6 & -2 & 11 \\ -35 & -18 & -50 & -118 \end{pmatrix} \begin{pmatrix} 19 & 1 & -3 & -103 \\ 42 & 2 & -8 & -233 \\ -38 & -3 & 7 & 212 \\ -2 & 0 & 1 & 14 \end{pmatrix}$$

Esercizio 3. Nell'anello $\mathbb{Z}[i]$ degli interi di Gauß si consideri l'elemento 10.

Si fattorizzi 10 in $\mathbb{Z}[i]$, si determinino gli ideali dell'anello

$$\mathrm{D} = \mathbb{Z}[i]/\langle 10\rangle$$

e si dica quali degli ideali di D sono primi.

Soluzione. L'intero di Gauß 10 amette, in $\mathbb{Z}[i]$, la seguente fattorizzazione

$$10 \;=\; 2\cdot 5 \;=\; (1+i)\cdot(1-i)\cdot(2+i)\cdot(2-i)$$

Ragionando sulle loro norme, è facile verificare che gli elementi dell'insieme

$$\{\ (1+i), (1-i), (2+i), (2-i)\ \}$$

ossia, i fattori or ora trovati, sono irriducibili. Inoltre, $\mathbb{Z}[i]$ essendo euclideo, questi elementi sono anche primi.

Al fine di determinare gli ideali dell'anello D, consideriamo l'applicazione canonica $\pi_{\mathrm{D}} : \mathbb{Z}[i] \to \mathrm{D}$. Allora

$$\mathrm{Idl}_{\mathrm{D}} \;=\; \pi_{\mathrm{D}}\{I \in \mathrm{Idl}_{\mathbb{Z}[i]} \mid I \supseteq \langle 10\rangle\}$$

Ricordiamo, ora, che, essendo addirittura euclideo, l'anello $\mathbb{Z}[i]$ è a ideali principali. Ossia, per ogni suo ideale I esiste un elemento $\iota \in I$ tale che $I = \langle\iota\rangle$. Questo permette di determinare in maniera più fine gli ideali di $\mathbb{Z}[i]$ che contengono 10. Infatti, abbiamo che

$$I = \langle\iota\rangle \supseteq \langle 10\rangle \iff \iota \mid 10$$

Enumeriamo qui di seguito questi ideali. Essi sono gli elementi dell'insieme $\mathrm{Idl}_{\mathbb{Z}[i]}(10)$ definito da

$\{\ \mathbb{Z}[i]\ ,\ \langle 1+i\rangle, \langle 1-i\rangle, \langle 2+i\rangle, \langle 2-i\rangle\ ,\ \langle (1+i)(1-i)\rangle, \langle (1+i)(2+i)\rangle, \langle (1+i)(2-i)\rangle,$
$\langle (1-i)(2+i)\rangle, \langle (1-i)(2-i)\rangle, \langle (2+i)(2-i)\rangle\ ,\ \langle (1+i)(1-i)(2+i)\rangle, \langle (1+i)(1-i)(2-i)\rangle,$
$\langle (1+i)(2+i)(2-i)\rangle, \langle (1-i)(2+i)(2-i)\rangle\ ,\ \langle (1+i)(1-i)(2+i)(2-i)\rangle\ \}$

Finalmente, possiamo elencare gli elementi di $\mathrm{Idl}_{\mathrm{D}}$. Essi sono l'immagine secondo π_{D} degli elementi di $\mathrm{Idl}_{\mathbb{Z}[i]}(10)$.

Per determinare quali degli ideali di D sono primi, basta osservare

- che gli elementi dell'insieme

$$\mathrm{S} \stackrel{def}{=} \pi_{\mathrm{D}}\{\langle 1+i\rangle, \langle 1-i\rangle, \langle 2+i\rangle, \langle 2-i\rangle\}$$

son massimali e, dunque, primi

- che gli elementi di $\mathrm{C} \stackrel{def}{=} \mathrm{Idl}_{\mathrm{D}} \setminus \mathrm{S}$ son tali che l'anello ottenuto quozientando D per uno di essi ammette divisori dello zero. Ossia, preso comunque un ideale C di D che sia un elemento di C, cioè $C \in \mathrm{C}$, risulta che l'anello D/C ammette divisori

dello zero ([19]). Conseguentemente, gli ideali di D che sono anche elementi di C **non** sono primi.

[19]A titolo illustrativo, consideriamo l'ideale $C = \pi_{\mathrm{D}}(\langle(1+i)(1-i)\rangle) \leq \mathrm{D}$. Allora, detta $\pi_C : \mathrm{D} \to \mathrm{D}/C$ la proiezione canonica, gli elementi $[\pi_C \circ \pi_{\mathrm{D}}](1+i)$ e $[\pi_C \circ \pi_{\mathrm{D}}](1-i)$ di D/C dividono lo zero dell'anello D/C. Infatti, $[\pi_C \circ \pi_{\mathrm{D}}](1+i)\cdot[\pi_C \circ \pi_{\mathrm{D}}](1-i) = [...] = [\pi_C \circ \pi_{\mathrm{D}}]((1+i)(1-i)) = 0_C$.

Esercizio 4. Si dica se $(17, 34, 51) \in \mathbb{Z}^3$ può far parte di una base di $\mathbb{Z}^3$.

Si spieghi come si è giunti alla conclusione.

Soluzione. Lo $\mathbb{Z}$-vettore $(17, 34, 51)$ di $\mathbb{Z}^3$ **non** può far parte di alcuna base di $\mathbb{Z}^3$. Dimostreremo questa affermazione, cui d'ora in poi ci riferiremo chiamandola "affermazione M", procedendo "per assurdo".

Iniziamo col fissare alcune notazioni. Definito $\mathbf{W} = (W_1, W_2, W_3) = (17, 34, 51)$ e posto $W = \mathrm{MCD}(w_1, w_2, w_3) = 17$, sia $\mathbf{w} = (w_1, w_2, w_3)$ tale che $\mathbf{W} = W\mathbf{w}$. Ossia, poniamo $\mathbf{w} = (w_1, w_2, w_3) = (1, 2, 3)$.

Siano, ora, $\mathbf{U} = (U_1, U_2, U_3)$ e $\mathbf{V} = (V_1, V_2, V_3)$ qualsivoglia elementi di $\mathbb{Z}^3$. La prova dell'affermazione M consisterà nel mostrare che, se gli $\mathbb{Z}$-vettori $\mathbf{U}, \mathbf{V}, \mathbf{W} \in \mathbb{Z}^3$ sono $\mathbb{Z}$-linearmente indipendenti, allora essi **non** possono generare $\mathbb{Z}^3$.

Supponiamo, dunque, dati $\mathbf{U}, \mathbf{V} \in \mathbb{Z}^3$ tali che $\mathbf{U}, \mathbf{V}, \mathbf{W} \in \mathbb{Z}^3$ siano $\mathbb{Z}$-linearmente indipendenti. Introduciamo, qui, alcune altre notazioni che risulteranno utili nel seguito. Poniamo $U = \mathrm{MCD}(U_1, U_2, U_3)$, $V = \mathrm{MCD}(V_1, V_2, V_3)$ e definiamo $\mathbf{u} = (u_1, u_2, u_3)$, $\mathbf{v} = (v_1, v_2, v_3)$ in modo tale che $\mathbf{U} = U\mathbf{u}$ e $\mathbf{V} = V\mathbf{v}$.

Ora, dimostrare che $\mathbf{U}, \mathbf{V}, \mathbf{W} \in \mathbb{Z}^3$ non generano $\mathbb{Z}^3$ è equivalente a dimostrare la **non** suriettività dell'applicazione $\mathbb{Z}$-lineare

$$\begin{array}{rccc} T_{\mathbf{U},\mathbf{V},\mathbf{W}}: & \mathbb{Z}^3 & \longrightarrow & \mathbb{Z}^3 \\ & (x_1, x_2, x_3) & \longmapsto & x_1\mathbf{U} + x_2\mathbf{V} + x_3\mathbf{W} \end{array}$$

Detta $\mathbb{Z}^3 \overset{\iota}{\hookrightarrow} \mathbb{Q}^3$ l'immersione naturale di $\mathbb{Z}^3$ in $\mathbb{Q}^3$, l'insieme $\{\iota(\mathbf{U}), \iota(\mathbf{V}), \iota(\mathbf{W})\}$ è una $\mathbb{Q}$-base del $\mathbb{Q}$-spazio vettoriale $\mathbb{Q}^3$ ([20]).

Per determinare l'immagine di $T_{\mathbf{U},\mathbf{V},\mathbf{W}}$ e capire se essa coincide o non coincide con l'intero $\mathbb{Z}^3$, utilizzeremo la regola di Cramer. Sia, dunque, A la matrice associata all'operatore $T_{\mathbf{U},\mathbf{V},\mathbf{W}}$ e alla scelta, sia nel dominio sia nel codominio di $T_{\mathbf{U},\mathbf{V},\mathbf{W}}$, della base canonica $(1,0,0), (0,1,0), (0,0,1)$ di $\mathbb{Z}^3$. Ossia,

$$A = \begin{pmatrix} U_1 & V_1 & W_1 \\ U_2 & V_2 & W_2 \\ U_3 & V_3 & W_3 \end{pmatrix} = \begin{pmatrix} U_1 & V_1 & 17 \\ U_2 & V_2 & 34 \\ U_3 & V_3 & 51 \end{pmatrix} = \begin{pmatrix} U \cdot u_1 & V \cdot v_1 & 17 \cdot 1 \\ U \cdot u_2 & V \cdot v_2 & 17 \cdot 2 \\ U \cdot u_3 & V \cdot v_3 & 17 \cdot 3 \end{pmatrix}$$

Accanto alla matrice A consideriamo anche la matrice

$$D = \begin{pmatrix} u_1 & v_1 & 1 \\ u_2 & v_2 & 2 \\ u_3 & v_3 & 3 \end{pmatrix}$$

Ora, uno $\mathbb{Z}$-vettore $\mathbf{B} = (b_1, b_2, b_3)$ è nell'immagine di $T_{\mathbf{U},\mathbf{V},\mathbf{W}}$ se e solo se esiste uno $\mathbb{Z}$-vettore $\mathbf{X} = (x_1, x_2, x_3)$ tale che

$$\Sigma. \quad \mathbf{B} = A\mathbf{X}$$

[20] A proposito, ricordiamo il seguente risultato. Sia E un κ-spazio vettoriale di dimensione finita n. Se $\{e_1, ..., e_n\} \subseteq E$ è un insieme di n vettori tra loro κ-linearmente indipendenti, allora $\{e_1, ..., e_n\}$ è una base di E.

Osserviamo che questo sistema è sempre risolubile in $\mathbb{Q}^3$. Il nostro obiettivo, però, è un altro. Dobbiamo trovare uno $\mathbb{Z}$-vettore $\mathbf{B}$ per cui esista $\mathbf{X}$ un $\mathbb{Q}$-vettore che
- soddisfi $\mathbf{B} = A\mathbf{X}$
- non sia uno $\mathbb{Z}$-vettore

A questo punto invertiamo il sistema Σ e, supponendo di conoscere $\mathbf{B}$, applichiamo la regola di Cramer in $\mathbb{Q}^3$. Questa regola permette di determinare l'unico vettore $\mathbf{X} \in \mathbb{Q}^3$ tale che $\mathbf{B} = A\mathbf{X}$ ([21]). Per poter applicare la regola di Cramer abbiamo bisogno di calcolare il determinante delle matrici A e D. Risulta

$$\det A = UVW[(u_2v_3 - u_3v_2) - 2(u_1v_3 - u_3v_1) + 3(u_1v_2 - u_2v_1)],$$

con $W = 17$, e

$$\det D = [(u_2v_3 - u_3v_2) - 2(u_1v_3 - u_3v_1) + 3(u_1v_2 - u_2v_1)],$$

da cui $\det A = UVW \cdot \det D = 17UV \cdot \det D$.

Ora, dato $\mathbf{B}$, secondo la regola di Cramer, l'unico vettore $\mathbf{X} \in \mathbb{Q}^3$ tale che $\mathbf{B} = A\mathbf{X}$ è

$$\mathbf{X} = (\det A_1/\det A,\ \det A_2/\det A,\ \det A_3/\det A),$$

con

$$A_1 = \begin{pmatrix} b_1 & V_1 & 17 \\ b_2 & V_2 & 34 \\ b_3 & V_3 & 51 \end{pmatrix},$$
$$A_2 = \begin{pmatrix} U_1 & b_1 & 17 \\ U_2 & b_2 & 34 \\ U_3 & b_3 & 51 \end{pmatrix},$$
$$A_3 = \begin{pmatrix} U_1 & V_1 & b_1 \\ U_2 & V_2 & b_2 \\ U_3 & V_3 & b_3 \end{pmatrix}.$$

Quindi,

$$\mathbf{X} = \frac{1}{UVW \cdot \det D}(\det A_1,\ \det A_2,\ \det A_3)$$

Ora, da

$$\det A_1 = 17V[(b_2v_3 - b_3v_2) - 2(b_1v_3 - b_3v_1) + 3(b_1v_2 - b_2v_1)],$$

$$\det A_2 = 17U[(b_3u_2 - b_2v_3) - 2(b_3u_1 - b_1u_3) + 3(b_2u_1 - b_1u_2)],$$

$$\det A_3 = UV[b_1(u_2v_3 - u_3v_2) - b_2(u_1v_3 - u_3v_1) + b_3(u_1v_2 - u_2v_1)],$$

[21] L'unicità di $\mathbf{X}$ segue dal fatto che $T_{\mathbf{U},\mathbf{V},\mathbf{W}}$, considerato come operatore da $\mathbb{Q}^3$ a $\mathbb{Q}^3$ è invertibile.

abbiamo $\mathbf{X} = (x_1, x_2, x_3)$, con

$$\Xi. \quad \begin{cases} x_1 &= \frac{(b_2v_3 - b_3v_2) - 2(b_1v_3 - b_3v_1) + 3(b_1v_2 - b_2v_1)}{U \cdot \det D} \\ x_2 &= \frac{(b_3u_2 - b_2v_3) - 2(b_3u_1 - b_1u_3) + 3(b_2u_1 - b_1u_2)}{V \cdot \det D} \\ x_3 &= \frac{b_1(u_2v_3 - u_3v_2) - b_2(u_1v_3 - u_3v_1) + b_3(u_1v_2 - u_2v_1)}{17 \cdot \det D} \end{cases}$$

Siamo ora in grado di individuare almeno un elemento $\mathbf{B} \in \mathbb{Z}^3$ che non appartiene all'immagine di $\mathbb{Z}^3$ secondo $T_{\mathbf{U},\mathbf{V},\mathbf{W}}$.

Sia, infatti, $h \in \mathbb{Z}$ tale che $n \not\equiv_{17} 0$; cioè sia n un intero in $\mathbb{Z} \setminus 17\mathbb{Z}$. Allora il vettore $\mathbf{B} = (h, 2h, 3h) = h(1, 2, 3)$ **non** appartiene all'immagine di $\mathbb{Z}^3$ secondo $T_{\mathbf{U},\mathbf{V},\mathbf{W}}$. Infatti, l'unico $\mathbb{Q}$-vettore $\mathbf{X} = (x_1, x_2, x_3)$ che soddisfa il sistema Ξ associato a questo $\mathbf{B}$ è $\mathbf{X} = (0, 0, h/17)$, che è razionale ma non intero.

In particolare e a titolo illustrativo, lo $\mathbb{Z}$-vettore $(1, 2, 3)$ non è nell'immagine secondo $T_{\mathbf{U},\mathbf{V},\mathbf{W}}$ di $\mathbb{Z}$. Dunque, $(1, 2, 3)$ non può essere generato da alcun sistema di $\mathbb{Z}$-vettori linearmente indipendenti che contenga lo $\mathbb{Z}$-vettore $(17, 34, 51)$.

La verità dell'affermazione M è stata dunque provata.

Esercizio 5. Dello $\mathbb{Z}$-modulo $\mathbb{Z}^3$ si consideri il sottomodulo L definito come segue

$$L = \langle\ (2,4,6),\ (3,6,9),\ (15,10,5)\ \rangle\ \subseteq\ \mathbb{Z}^3$$

Si dica se L è uno $\mathbb{Z}$-modulo libero; in caso lo sia, si determini una base di L.
Si dica se $\mathbb{Z}^3/L$ è uno $\mathbb{Z}$-modulo libero; in caso lo sia, si determini una base di $\mathbb{Z}^3/L$.

Soluzione. Iniziamo osservando che

$$\mathrm{rg}\begin{pmatrix} 2 & 4 & 6 \\ 3 & 6 & 9 \\ 15 & 10 & 5 \end{pmatrix}\ =\ 2$$

e

$$\mathrm{rg}\begin{pmatrix} 2 & 4 & 6 \\ 3 & 6 & 9 \end{pmatrix} = 1 \quad \mathrm{rg}\begin{pmatrix} 2 & 4 & 6 \\ 15 & 10 & 5 \end{pmatrix} = 2 \quad \mathrm{rg}\begin{pmatrix} 3 & 6 & 9 \\ 15 & 10 & 5 \end{pmatrix} = 2$$

Ne segue che
I. i tre vettori che generano L son tra loro $\mathbb{Z}$-linearmente dipendenti
II.- L può essere generato su $\mathbb{Z}$ da due $\mathbb{Z}$-vettori
III. esiste uno $\mathbb{Z}$-vettore $(a_1,a_2,a_3) \in \mathbb{Z}^3$ e interi $\kappa_1, \kappa_2 \in \mathbb{Z}$ tali che

$$(2,4,6) = \kappa_1(a_1,a_2,a_3)\ \text{ e }\ (3,6,9) = \kappa_2(a_1,a_2,a_3)$$

Approfondiamo l'affermazione III. Abbiamo

$$\langle\ (2,4,6),\ (3,6,9)\ \rangle\ =\ \langle\ (1,2,3)\ \rangle$$

Proviamo questo fatto. Da un lato abbiamo $\langle (2,4,6),(3,6,9)\rangle \supseteq \langle (1,2,3)\rangle$, 'ché, da

$$(1,2,3) = (3,6,9) - (2,4,6),$$

abbiamo che ogni elemento $x(1,2,3) \in \langle (1,2,3)\rangle$ appartiene a $\langle (2,4,6),(3,6,9)\rangle$. Infatti,

$$\begin{array}{rcl} x(1,2,3) & = & x((3,6,9)-(2,4,6)) \\ & = & x(3,6,9) - x(2,4,6) \in \langle (2,4,6),(3,6,9)\rangle \end{array}$$

Da un altro lato abbiamo $\langle (2,4,6),(3,6,9)\rangle \subseteq \langle (1,2,3)\rangle$, 'ché, da

$$(2,4,6) = 2(1,2,3)\ \text{ e }\ (3,6,9) = 3(1,2,3),$$

abbiamo che ogni elemento $y_1(2,4,6) + y_2(3,6,9) \in \langle (2,4,6),(3,6,9)\rangle$ appartiene a $\langle (1,2,3)\rangle$. Infatti,

$$\begin{array}{rcl} y_1(2,4,6) + y_2(3,6,9) & = & 2y_1(1,2,3) + 3y_2(1,2,3)) \\ & = & (2y_1 + 3y_3)(1,2,3) \in \langle (1,2,3)\rangle \end{array}$$

Approfondiamo, ora, l'affermazione II. Abbiamo

$$L \;=\; \langle\ (1,2,3),\ (15,10,5)\ \rangle$$

Infatti

$$\begin{aligned} L &= \langle\ (2,4,6),(3,6,9),(15,10,5)\ \rangle \\ &= \{\ x_1(2,4,6)+x_2(3,6,9)+x_3(15,10,5) \mid x_1,x_2,x_3\in\mathbb{Z}\ \} \\ &= \{\ (2x_1+3x_2)(1,2,3)+x_3(15,10,5) \mid x_1,x_2,x_3\in\mathbb{Z}\ \} \\ \star &= \{\ x_0(1,2,3)+x_3(15,10,5) \mid x_0,x_3\in\mathbb{Z}\ \} \\ &= \langle\ (1,2,3),(15,10,5)\ \rangle \end{aligned}$$

Il passaggio $\star$ è giustificato dal seguente semplice fatto. Per ogni $x_0\in\mathbb{Z}$ esistono $h',h''\in\mathbb{Z}$ tali che $x_0=h'\cdot 2+h''\cdot 3$. Infatti, per esempio, da $1=1\cdot 3+(-1)\cdot 2$ abbiamo $x_0=x_0\cdot 1=x_0\cdot(1\cdot 3+(-1)\cdot 2)=x_0\cdot 3+(-x_0)\cdot 2$; così che $h'=x_0$ e $h''=-x_0$ servono la nostra causa. Più sinteticamente, abbiamo che l'ideale $\langle 2,\ 3\rangle$ generato da 2 e 3, come ogni ideale di $\mathbb{Z}$ è principale e coincide con l'ideale generato dal massimo comun divisore di 2 e 3 che è 1. Ossia, $\langle 2,\ 3\rangle=\langle \mathrm{MCD}(2,3)\rangle=\langle 1\rangle=\mathbb{Z}$.

A questo punto possiamo affermare che L è
- un sotto-$\mathbb{Z}$-modulo di $\mathbb{Z}^3$
- uno $\mathbb{Z}$-modulo libero di rango 2
- ammette come base i vettori $(1,2,3)$ e $(15,10,5)$.

Ossia, $L\ =\ \langle\ (1,2,3),\ (15,10,5)\ \rangle\ \subseteq\ \mathbb{Z}^3$.

Passiamo ora allo studio dello $\mathbb{Z}$-modulo quoziente $\mathbb{Z}^3/L$.

Com'è facile verificare, mediante una successione di trasformazioni elementari ([22]), è possibile trasformare la matrice

$$\begin{pmatrix} 1 & 2 & 3 \\ 15 & 10 & 5 \end{pmatrix}$$

nella matrice

[22]Qui di seguito una descrizione delle operazioni elementari da me trovate per trasformare $\begin{pmatrix} 1 & 2 & 3 \\ 15 & 10 & 5 \end{pmatrix}$ in $\begin{pmatrix} 20 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

A. sostituisco la II colonna con la colonna ottenuta sottraendo la III colonna alla II colonna

B. sostituisco la III colonna con la colonna ottenuta sottraendo la II colonna alla III colonna

C. sostituisco la II colonna con la colonna ottenuta sommando la I colonna alla II colonna

D. sostituisco la III colonna con la colonna ottenuta sottraendo la 4 volte la I colonna alla III colonna

E. sostituisco la III colonna con la colonna ottenuta sommando la 3 volte la II colonna alla III colonna

F. sposto la I colonna al posto della II colonna e la II colonna al posto della I colonna

G. sostituisco la II riga con la riga ottenuta sottraendo la 15 volte la I riga alla II riga

H. sposto la I riga al posto della II riga e la II riga al posto della I riga

$$\begin{pmatrix} 20 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Esiste, dunque, una base $\mathbf{i}, \mathbf{j}, \mathbf{k}$ di $\mathbb{Z}^3$ tale che

$$\mathbb{Z}^3 \;=\; \mathbb{Z}\mathbf{i} \oplus \mathbb{Z}\mathbf{j} \oplus \mathbb{Z}\mathbf{k} \;\text{ e }\; L \;=\; 20\mathbb{Z}\mathbf{i} \oplus 1\mathbb{Z}\mathbf{j} \oplus 0\mathbb{Z}\mathbf{k}$$

Espressa nella base $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$, l'azione di L su $\mathbb{Z}^3$ è diagonale. Ossia,

$$\begin{aligned} \mathbb{Z}^3/L \;&=\; \mathbb{Z}\mathbf{i} \oplus \mathbb{Z}\mathbf{j} \oplus \mathbb{Z}\mathbf{k} \;/\; 20\mathbb{Z}\mathbf{i} \oplus \mathbb{Z}\mathbf{j} \oplus 0\mathbb{Z}\mathbf{k} \\ &\approx\; \mathbb{Z}\mathbf{i}/20\mathbb{Z}\mathbf{i} \;\oplus\; \mathbb{Z}\mathbf{j}/1\mathbb{Z}\mathbf{j} \;\oplus\; \mathbb{Z}\mathbf{k}/0\mathbb{Z}\mathbf{k} \\ \diamond \;&\approx\; \mathbb{Z}_{20} \;\oplus\; \mathbb{Z}_1 \;\oplus\; \mathbb{Z}_0 \\ &\approx\; \mathbb{Z}_{20} \;\oplus\; \mathbb{Z} \end{aligned}$$

Conseguentemente $\mathbb{Z}^3/L$ **non** è uno $\mathbb{Z}$-modulo libero.

Il passaggio $\diamond$ è giustificato dal seguente fatto, già incontrato più volte nel corso dell'anno

$$\mathbb{Z}_1 \;\approx\; \{\square\} \;\text{ e }\; \mathbb{Z}_0 \;\approx\; \mathbb{Z}$$