2ο Φυλλάδιο Ασκήσεων - Δακτύλιοι και Πρότυπα

Αναστάσιος Φράγκος: AM 1112201900239	Κυριακή, 12 Δεκεμβρίου 2021

Συμβολισμοί - Παρατηρήσεις

1. Έστω $(R, +, \cdot)$ μια αλγεβρική δομή με πράξεις 'πρόσθεσης' και 'πολλαπλασιασμού'. Για κάθε $\emptyset \neq X \subseteq R$, ορίζουμε $(\!|X|\!) := \{r \cdot x \in R \mid (r, x) \in R \times X\}$. Εάν ειδικότερα το X αποτελείται από αριθμήσιμο πλήθος στοιχείων $x_1, x_2, x_3, \cdots$, τότε συμβολίζουμε $(\!|x_1, x_2, x_3, \cdots|\!) := (\!|X|\!)$. Εάν το X είναι κενό, κάνουμε την παραδοχή $(\!|\emptyset|\!) := \{0_R\}$.
2. $\gcd(m, n) = \{d \mid d$ είναι μέγιστος κοινός διαιρέτης των $m, n\}$.
3. $\mathbb{C} := \mathbb{R}^2$.
4. $[n] := [1, n] \cap \mathbb{N}$.
5. Έστω R δακτύλιος και $A, B \subseteq R$. Ορίζουμε:

$$A \cdot B := \left\{ \sum_{(s,t) \in I} a_s b_t \;\middle|\; a_s \in A,\ b_t \in B,\ I \subseteq |A| \times |B| \right\}$$

Επίσης, για $A \subseteq R,\ b \in R$, ορίζουμε $A \cdot b := A \cdot \{b\},\ b \cdot A := \{b\} \cdot A$.
6. Έστω R δακτύλιος και $A, B \subseteq R$. Ορίζουμε:

$$A + B := \{a + b \mid a \in A,\ b \in B\}$$

Επίσης, για $A \subseteq R,\ b \in R$, ορίζουμε $A + b := A + \{b\},\ b + A := \{b\} + A$.
7. $\bigoplus_{i \in I} A_i := \left\{f : I \to \bigcup_{i \in I} A_i \mid f(i) \in A_i\right\}$. Ειδικότερα, εάν το I είναι καλά διατάξιμο (και συγκεκριμένα $\perp < S\perp < SS\perp < \cdots < \overbrace{S \cdots S}^{\eta \in \mathcal{ON}} \perp < \cdots$), τότε θα ταυτίζουμε (συμβατικά) το σύνολο $\bigoplus_{i \in I} A_i$ με το:

$$\left\{(a_{\perp}, a_{S\perp}, \cdots) \in M_{1 \times |I|}\left(\bigcup_{i \in I} A_i\right) \;\middle|\; a_{\frac{\eta}{S \cdots S\perp}} \in A_{\frac{\eta}{S \cdots S\perp}}\right\}$$

Η κλάση $\mathcal{ON}$ είναι η κλάση των διατακτικών αριθμών.
8. Με $\mathrm{Hom}_{\mathrm{R-Mod}}(A, B)$ θα συμβολίζουμε την κλάση των ομορφισμών μεταξύ των (αριστερών) προτύπων A και B.
9. $f : A \twoheadrightarrow B$: Η συνάρτηση f είναι επί του B.
10. $f : A \rightarrowtail B$: Η συνάρτηση f είναι $1-1$.
11. $f : A \rightarrowtail\!\!\!\!\twoheadrightarrow B$: Η συνάρτηση f είναι αμφιμονοσήμαντη.
12. Εάν το A είναι σύνολο, ο πληθάριθμός του θα συμβολίζεται με $|A|$ είτε με $\#A$.
13. Όλοι οι δακτύλιοι έχουν μοναδιαίο στοιχείο και οι ομομορφισμοί δακτυλίων διατηρούν τα μοναδιαία στοιχεία.
14. Στα παρακάτω ο δακτύλιος R θα είναι πάντοτε μη τετριμμένος και μεταθετικός, εκτός κι αν αναφέρεται κάτι άλλο.

Άσκηση 1 Δείξτε ότι το:

$$M = \left\{(x, y, z) \in \bigoplus_{i \in [3]} \mathbb{Z} \;\middle|\; x - 2y + z = 0 \mod 5\right\}$$

είναι ελεύθερο $\mathbb{Z}-$υποπρότυπο του $\bigoplus_{i \in [3]} \mathbb{Z}$ και βρείτε μια βάση του. Αληθεύει ότι κάθε $\mathbb{Z}-$υποπρότυπο του M είναι ελεύθερο; ■

Συμβολισμοί: Στην άσκηση αυτή, για διευκόλυνση της διαδικασίας της συγγραφής, θα χρησιμοποιηθούν οι εξής συμβολισμοί:

- Από την Προβολική γεωμετρία: Θα συμβολίζουμε με $< \alpha, \beta, \gamma >$ τον διανυσματικό υπόχωρο του $\mathbb{R}^3$ που αντιστοιχεί στο επίπεδο με εξίσωση $\alpha x+\beta y+\gamma z=0$ (η $<\alpha,\beta,\gamma>$ είναι δηλαδή μια ευθεία του $\mathbb{P}_2(\mathbb{R})$). Ειδικότερα συμβολίζουμε:

$$(<(\alpha,\beta,\gamma)>=)\ <\alpha,\beta,\gamma>:=\{(x,y,z)\in\mathbb{R}^3 \mid \alpha x+\beta y+\gamma z=0\}$$

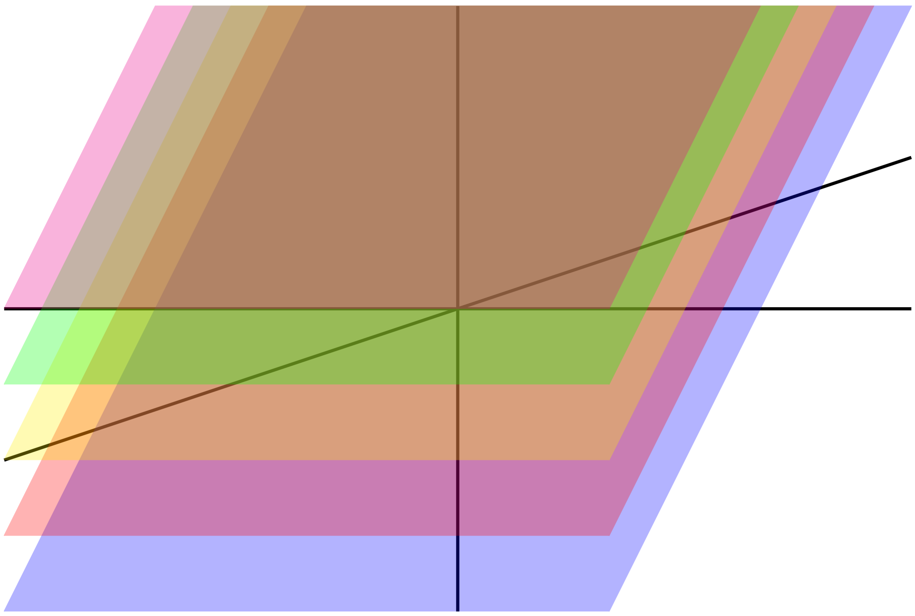
Επειδή οι υπόχωροι $<\alpha,\beta,\gamma>$ βρίσκονται σε $1-1$ αντιστοιχία με επίπεδα του $\mathbb{R}^3$, συμβατικά θα αναφερόμαστε σε αυτά ως επίπεδα.

- $pr_B^A: A\to B$ με $A,B\subseteq\mathbb{R}^3$: Είναι η συνάρτηση - προβολή του A στο B. Στην ειδική περίπτωση που $A=<\alpha,\beta,\gamma>+(0,0,\zeta)$, $B=<\kappa,\lambda,\mu>+(0,0,\xi)$, παρατηρούμε ότι $pr_B^A\in\mathrm{Hom}_{\mathrm{R-Mod}}(A,B)$.

Λύση: Το υποσύνολο $<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$ του $\bigoplus_{i\in[3]}\mathbb{Z}$ είναι κατ' αρχάς υποσύνολο του M. Επιπλέον, το M γεωμετρικά μπορεί να αναπαρασταθεί ως το σύνολο - ένωση όλων των παραλλήλων προς το $<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$ επιπέδων, τα οποία τέμνουν τον άξονα των z σε πολλαπλάσια του 5. Ισχύει λοιπόν ότι:

$$M=\bigcup_{k\in\mathbb{Z}}\Big[<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}\Big]+k(0,0,5)$$

και συνεπώς, εάν μια βάση $\{b_1,b_2\}$ του $<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$ (ως $\mathbb{Z}-$πρότυπο) υπάρχει, το M θα είναι ελεύθερο $\mathbb{Z}-$πρότυπο, και μάλιστα μια βάση του θα αποτελεί η $\{b_1,b_2,(0,0,5)\}$.



Το $<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$ είναι ελεύθερο $\mathbb{Z}-$πρότυπο. Πράγματι, αυτό ισχύει και θα το αποδείξουμε ως εξής: θα προβάλλουμε το $<1,-2,1>$ στο $<0,0,1>$ και θα επιλέξουμε μια βάση του τελευταίου, έτσι ώστε να απεικονίζεται με την αντίστροφη διαδικασία (αντίστροφη προβολή) σε βάση του $<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$.

Έστω $\varphi=pr_{<0,0,1>}^{<1,-2,1>}:<1,-2,1>\to<0,0,1>$, η οποία (παρατηρούμε) έχει τη μορφή $(x,y,z)\mapsto(x,y,0)$. Η φ περιορισμένη στο $<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$ αποτελεί ισομορφισμό $\mathbb{Z}-$προτύπων, ειδικότερα των $<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$ και $<0,0,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$. Το ότι πράγματι είναι ισομορφισμός προκύπτει από το γεγονός ότι η αντίστροφη απεικόνιση υπάρχει (κάθε $(x,y,0)\in<0,0,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$ μπορεί να απεικονιστεί στο $(x,y,2y-x)\in<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$), και επιπλέον η φ είναι ομομορφισμός. Ακόμη, η $\{(1,0,0),(0,1,0)\}$ είναι βάση του $\mathbb{Z}-$προτύπου $<0,0,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$. Σύμφωνα λοιπόν με ό,τι έχει προαναφερθεί, το $<1,-2,1>\cap\bigoplus_{i\in[3]}\mathbb{Z}$ είναι ελεύθερο, αφού η:

$$\{\varphi^{-1}\big((1,0,0)\big),\varphi^{-1}\big((0,1,0)\big),(0,0,5)\}=\{(1,0,-1),(0,1,2),(0,0,5)\}$$

αποτελεί βάση του.

Κάθε $\mathbb{Z}-$υποπρότυπο του M είναι ελεύθερο, αφού το $\mathbb{Z}$ είναι περιοχή κυρίων ιδεωδών, και επίσης γνωρίζουμε ότι κάθε υποπρότυπο ελεύθερου $R-$προτύπου, όπου R είναι περιοχή κυρίων ιδεωδών, είναι ελεύθερο.

$\square$

Άσκηση 2 Δείξτε ότι τα $(a,b),\ (c,d) \in \mathbb{Z}[i]$ αποτελούν βάση του $\mathbb{Z}-$προτύπου $\mathbb{Z}[i]$ αν και μόνο αν $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$. ■

Λύση: Για να αποτελεί το $\{(a,b),\ (c,d)\}$ βάση του $\mathbb{Z}[i]$, ικανή και αναγκαία συνθήκη είναι για κάθε $(z,w) \in \mathbb{Z}[i]$ να υπάρχει μοναδικό $(x,y) \in \mathbb{Z}[i]$ τέτοιο ώστε:

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} z \\ w \end{pmatrix}$$

Δηλαδή να υπάρχει μοναδική γραφή ως προς τις βάσεις. Ισοδύναμα:

$$\det\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U(\mathbb{Z}) = \{\pm 1\}$$

Αυτό εξασφαλίζει την ύπαρξη του (x,y) κατά μοναδικό τρόπο.

□

Γενίκευση: *Έστω $\mathbb{B} = \big\{b_1 = (b_{1,1},\cdots,b_{1,n}),\cdots,b_n = (b_{n,1},\cdots,b_{n,n})\big\}$ ένα σύνολο διανυσμάτων του $\bigoplus_{k\in[n]}\mathbb{Z}$. Το $\mathbb{B}$ αποτελεί βάση του $\mathbb{Z}-$προτύπου $\bigoplus_{k\in[n]}\mathbb{Z}$ αν και μόνο αν:*

$$\det\mathbb{B} = \det\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,n} \end{pmatrix} = \pm 1$$

Απόδειξη: Για να αποτελεί το $\mathbb{B}$ βάση του $\bigoplus_{k\in[n]}\mathbb{Z}$, ικανή και αναγκαία συνθήκη είναι για κάθε $(y_1,\cdots,y_n) \in \bigoplus_{k\in[n]}\mathbb{Z}$ να υπάρχει μοναδικό $(x_1,\cdots,x_n) \in \bigoplus_{k\in[n]}\mathbb{Z}$ τέτοιο ώστε:

$$\begin{pmatrix} b_{1,1} & b_{2,1} & \cdots & b_{n,1} \\ b_{1,2} & b_{2,2} & \cdots & b_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1,n} & b_{2,n} & \cdots & b_{n,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

Δηλαδή να υπάρχει μοναδική γραφή ως προς τις βάσεις. Ισοδύναμα:

$$\det\mathbb{B} = \det\begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,n} \end{pmatrix} = \det\begin{pmatrix} b_{1,1} & b_{2,1} & \cdots & b_{n,1} \\ b_{1,2} & b_{2,2} & \cdots & b_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{1,n} & b_{2,n} & \cdots & b_{n,n} \end{pmatrix} \in U(\mathbb{Z}) = \{\pm 1\}$$

Αυτό εξασφαλίζει την ύπαρξη του $(x_1,\cdots,x_n)$ κατά μοναδικό τρόπο.

△

Άσκηση 3 Έστω F ελεύθερο $R-$πρότυπο και $\mathbb{B} = \{b_1,\cdots,b_k\} \subseteq F$. Δείξτε ότι αν το $\mathbb{B}$ παράγει το F, τότε $|\mathbb{B}| = k \geq \text{rank}F$. ■

Λύση: Στην λύση αυτής της άσκησης θα ακολουθηθεί ανάλογη διαδικασία με την απόδειξη του θεωρήματος του van de Waerden (οπότε η ανάλυσή μας θα είναι συνοπτική).

Έστω $\mathbb{F} = \{f_1,\cdots,f_{\text{rank}F}\}$ μία βάση του F. Υποθέτουμε προς άτοπο ότι $k < \text{rank}F = n$. Θεωρούμε $A_{\mathbb{F}\to\mathbb{B}} \in M_n(R)$ πίνακα τέτοιον ώστε:

$$\begin{pmatrix} f_1 \\ \vdots \\ f_k \\ f_{k+1} \\ \vdots \\ f_n \end{pmatrix} = A_{\mathbb{F}\to\mathbb{B}} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_k \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Ο πίνακας αυτός ουσιαστικά είναι μία γενίκευση του πίνακα αλλαγής βάσης - είναι ο πίνακας που προκύπτει από μία αναγραφή των στοιχείων της $\mathbb{F}$ με στοιχεία του $\mathbb{B}$, εάν αυτός επεκταθεί κατάλληλα με μηδενικό πίνακα

$n \times (n-k)$ ώστε να γίνει τετραγωνικός. Αναλόγως, θεωρούμε $A_{\mathbb{B}\to\mathbb{F}} \in M_n(R)$ πίνακα τέτοιον ώστε:

$$\begin{pmatrix} b_1 \\ \vdots \\ b_k \\ 0 \\ \vdots \\ 0 \end{pmatrix} = A_{\mathbb{B}\to\mathbb{F}} \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_k \\ f_{k+1} \\ \vdots \\ f_n \end{pmatrix}$$

Ο πίνακας αυτός ουσιαστικά είναι μία γενίκευση του πίνακα αλλαγής βάσης - είναι ο πίνακας που προκύπτει από την αναγραφή των στοιχείων του $\mathbb{B}$, με στοιχεία της $\mathbb{F}$, εάν αυτός επεκταθεί κατάλληλα με μηδενικό πίνακα $(n-k) \times n$ ώστε να γίνει τετραγωνικός.

Εφόσον $k < \mathrm{rank} F = n$, στον πίνακα $A_{\mathbb{F}\to\mathbb{B}}$ έχει προστεθεί τουλάχιστον μία μηδενική στήλη και στον $A_{\mathbb{B}\to\mathbb{F}}$ έχει προστεθεί τουλάχιστον μία μηδενική γραμμή. Οι ορίζουσες λοιπόν των δύο αυτών πινάκων είναι 0.

Παρατηρούμε τέλος ότι το σύστημα:

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \overbrace{[A_{\mathbb{B}\to\mathbb{F}} \cdot A_{\mathbb{F}\to\mathbb{B}}]}^{A_{\mathbb{F}\to\mathbb{B}\to\mathbb{F}} = A_{\mathbb{F}\to\mathbb{F}}} \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$$

ισοδυναμεί με αναγραφή των στοιχείων της βάσης $\mathbb{F}$ με στοιχεία της βάσης $\mathbb{F}$, οπότε ορίζει ταυτοτικό πίνακα $A_{\mathbb{F}\to\mathbb{F}} = Id_n$. Αυτό θα μας οδηγήσει σε άτοπο, αφού υπεράνω μεταθετικών δακτυλίων:

$$1 = \det Id_n = \det A_{\mathbb{F}\to\mathbb{F}} = \det [A_{\mathbb{B}\to\mathbb{F}} \cdot A_{\mathbb{F}\to\mathbb{B}}] \overset{\star}{=} \det [A_{\mathbb{B}\to\mathbb{F}}] \cdot \det [A_{\mathbb{F}\to\mathbb{B}}] = 0 \cdot 0 = 0$$

(Ακριβέστερα, στην ισότητα '$\overset{\star}{=}$' γίνεται χρήση της μεταθετικότητας του δακτυλίου).

□

Άσκηση 4 Έστω R περιοχή κυρίων ιδεωδών, F ελεύθερο $R-$πρότυπο και $\mathbb{B} = \{b_1, \cdots, b_k\} \subseteq F$, όπου $|\mathbb{B}| = k = \mathrm{rank} F$.

i. Δείξτε ότι αν το $\mathbb{B}$ παράγει το F, τότε το B είναι βάση του F.

ii. Αληθεύει η ακόλουθη πρόταση; "*Αν το $\mathbb{B}$ είναι γραμμικά ανεξάρτητο, τότε το $\mathbb{B}$ είναι βάση του F*".

iii. Δείξτε ότι αν $\mathrm{Hom}_{\mathrm{R-Mod}}(F, F) \ni f : F \twoheadrightarrow F$, τότε επιπλέον $f : F \rightarrowtail F$.

■

$\boxed{\text{i.}}$ *Λύση:* Έστω $\{f_1, \cdots f_k\}$ μια βάση του F και $\mathrm{Hom}_{\mathrm{R-Mod}}(F, F) \ni \varphi : F \twoheadrightarrow F$ η οποία ορίζεται ως:

$$\varphi : f_i \mapsto b_i$$

Η φ είναι επιμορφισμός, επομένως $F \simeq \ker \varphi \oplus F \Rightarrow \mathrm{rank} F = \mathrm{rank} \ker \varphi + \mathrm{rank} F \Rightarrow \mathrm{rank} \ker \varphi = 0$. Εφόσον $\mathrm{rank} \ker \varphi = 0$, έπεται ότι $\ker \varphi = \{0\}$, και κατ' επέκταση ότι το $\mathbb{B}$ είναι βάση του F. Αξίζει να παρατηρηθεί ότι η προαναφερθήσα ισότητα των rank ισχύει επειδή ο πυρήνας είναι ελεύθερο υποπρότυπο, ως υποπρότυπο ελεύθερου σε περιοχή κυρίων ιδεωδών.

□

$\boxed{\text{ii.}}$ *Λύση:* Η πρόταση δεν αληθεύει. Το $\mathbb{Z}$ ως $\mathbb{Z}-$πρότυπο είναι ελεύθερο (αφού $(\!(1)\!) = \mathbb{Z}$), το $\{2\}$ αποτελεί γραμμικά ανεξάρτητο σύνολο και δεν επεκτείνεται σε βάση του $\mathbb{Z}$.

Το $\{2\}$ είναι γραμμικά ανεξάρτητο αφού το $\mathbb{Z}$ είναι περιοχή. Επειδή το $\mathbb{Z}$ είναι αντιμεταθετικός δακτύλιος, το rank είναι καλώς ορισμένο και μάλιστα (αφού το $\mathbb{Z}$ παράγεται από το 1) $\mathrm{rank}\mathbb{Z} = 1$. Το $\{2\}$ λοιπόν, εάν επεκτείνεται σε βάση του $\mathbb{Z}$, θα πρέπει το ίδιο να είναι βάση. Αυτό είναι άτοπο.

□

$\boxed{\text{iii.}}$ *Λύση:* Υπό αυτές τις υποθέσεις γνωρίζουμε ότι $F \simeq \ker f \oplus F \Rightarrow \mathrm{rank} F = \mathrm{rank} \ker f + \mathrm{rank} F \Rightarrow \mathrm{rank} \ker \varphi = 0$. Εφόσον $\mathrm{rank} \ker f = 0$, έπεται ότι $\ker f = \{0\}$, και κατ' επέκταση ότι $f : F \rightarrowtail F$.

□

Άσκηση 5 Εξετάστε ποιές από τις ακόλουθες προτάσεις αληθεύουν:

i. Κάθε υποπρότυπο ελεύθερου προτύπου είναι ελεύθερο πρότυπο.

ii. Αν F είναι ελεύθερο πρότυπο και $a \in F,\ a \neq 0$, τότε υπάρχει βάση του F που περιέχει το a.

iii. Αν F είναι ένα ελεύθερο πρότυπο και $\mathbb{B}$ μια βάση του, τότε δεν υπάρχει γνήσιο υποσύνολο του $\mathbb{B}$ που να είναι βάση του F.

$\boxed{\text{i.}}$ *Λύση:* Στη λύση αυτής της άσκησης θα χρησιμοποιηθεί ότι η περιοχή $\mathbb{Z}[x]$ δεν είναι κυρίων ιδεωδών και ότι το ιδεώδες αυτής $(\!|2, x|\!)$ δεν είναι ελεύθερο (ως πρότυπο) ούτε κύριο (ως ιδεώδες). Ο πρώτος και ο τρίτος ισχυρισμός δεν θα αποδειχθούν - έχει γίνει σχετική ανάλυση στο 1ο Φυλλάδιο. Όσον αφορά τον δεύτερο, είναι άμεση συνέπεια του γεγονότος ότι οποιαδήποτε δύο στοιχεία $f, g \in \mathbb{Z}[x]$ δεν είναι γραμμικώς ανεξάρτητα. Πράγματι είναι άμεση συνέπεια, αφού αν κάθε δύο στοιχεία δεν είναι γραμμικώς ανεξάρτητα και το $(\!|2, x|\!)$ ελεύθερο, θα παράγεται από ένα στοιχείο. Θα είναι λοιπόν κύριο ως ιδεώδες, το οποίο είναι άτοπο. Πρέπει λοιπόν να αποδείξουμε την εν λόγω πρόταση για να τελειώσουμε με τα εισαγωγικά της άσκησης. Αυτή ισχύει διότι $gf + (-f)g = 0$.

Εν γένει, δηλαδή για περιοχές R και όχι κατ' ανάγκη περιοχές κυρίων ιδεωδών, ένα τυχόν υποπρότυπο F' ενός ελεύθερου προτύπου $F \subseteq R$ δεν είναι ελεύθερο. Για παράδειγμα, το υποπρότυπο $(\!|2, x|\!)$ του ελεύθερου $\mathbb{Z}[x]-$προτύπου $\mathbb{Z}[x]$ δεν είναι ελεύθερο. 'Στην τάξη' έχει δειχθεί ότι κάθε υποπρότυπο F' ελεύθερου προτύπου $F \subseteq R$ είναι ελεύθερο, στην περίπτωση όπου η περιοχή R είναι κυρίων ιδεωδών. Το επιχείρημα λοιπόν δεν λειτουργεί σε αυτήν την περίπτωση, επειδή η περιοχή $\mathbb{Z}[x]$ δεν είναι κυρίων ιδεωδών.

□

$\boxed{\text{ii.}}$ *Λύση:* Η πρόταση δεν αληθεύει. Για το $\mathbb{Z}$ ως $\mathbb{Z}-$πρότυπο, το $\{2\}$ είναι γραμμικώς ανεξάρτητο σύνολο. Δεν επεκτείνεται όμως σε βάση. Αυτό διότι ο $\mathbb{Z}$ είναι αντιμεταθετικός δακτύλιος, και άρα έχει καλώς ορισμένο rank. Επειδή το $\{1\}$ είναι βάση του $\mathbb{Z}$, θα πρέπει $\text{rank}\mathbb{Z} = 1$, και άρα αν το $\{2\}$ επεκτείνεται σε βάση, το ίδιο είναι βάση. Αυτό είναι άτοπο.

□

$\boxed{\text{iii.}}$ *Λύση:* Η πρόταση αληθεύει. Έστω f ένα στοιχείο του F και $\{b_1, b_2, \cdots, b_m\}$, $\{b_1, b_2, \cdots, b_n\}$ δύο βάσεις του F με $\{b_1, b_2, \cdots, b_m\} \subset \{b_1, b_2, \cdots, b_n\}$. Θεωρούμε τις αναγραφές του f ως προς τις δύο βάσεις:

$$f = \sum_{i \in [m]} r_i b_i = \sum_{i \in [n]} s_i b_i \Rightarrow 0 = \sum_{i \in [m]} (r_i - s_i) b_i + \sum_{i \in [n] \cap (m,n]} r_i s_i$$

Επειδή η $\{b_i, \cdots, b_n\}$ είναι βάση του F, $\forall i \in [m],\ r_i = s_i$ και για τα υπόλοιπα $i \in [n] \cap (m, n],\ r_i = 0$. Οι σχέσεις αυτές προκύπτουν για τυχόν $f \in F$, επομένως οι βάσεις είναι ισοπληθείς ($m = n$, αφού τα στοιχεία $b_i,\ i \in [n] \cap (m, n]$ δεν δύνανται να υφίστανται). Αυτό δίνει το ζητούμενο.

□

Άσκηση 6 Έστω $\mathbb{K}$ σώμα. Δείξτε ότι το σώμα πηλίκων $\mathbb{K}(x)$ του $\mathbb{K}[x]$ δεν είναι ελεύθερο $\mathbb{K}[x]-$πρότυπο.

Λύση: Υποθέτουμε προς άτοπο ότι υπάρχει πεπερασμένη βάση του $\mathbb{K}(x)$. Έστω $\mathbb{B} = \left\{ \dfrac{P_i}{Q_i} \mid i \in [n] \right\}$ μια πεπερασμένη βάση και $\mathcal{B} = \prod_{i \in [n]} Q_i$. Θεωρούμε $\mu \in \gcd(\mathcal{B} \cdot \mathbb{B})$ και παρατηρούμε ότι το $\dfrac{\mu}{x\mathcal{B}}$ δεν παράγεται από την $\mathbb{B}$. Πράγματι, αν παράγοταν:

$$\frac{\mu}{x\mathcal{B}} = \sum_{i \in [n]} a_i b_i \Rightarrow \frac{\mu}{x} = \sum_{i \in [n]} a_i [\mathcal{B} b_i] \Rightarrow \mu \;\Big|\; \frac{\mu}{x}$$

Αυτό είναι άτοπο, αφού $\deg \mu > \deg \dfrac{\mu}{x}$.

□

Άσκηση 7

i. Εξετάστε αν οι πίνακες:

$$A = \begin{pmatrix} 2 & 0 & 2 \\ 4 & 6 & 2 \\ 2 & 0 & 2 \end{pmatrix} \text{ και } B = \begin{pmatrix} 2 & 4 & 2 \\ 0 & 2 & 0 \\ 2 & 4 & 2 \end{pmatrix} \in M_3(\mathbb{Z})$$

είναι ισοδύναμοι.

ii. Για ποιά $a \in \mathbb{Z}$ οι πίνακες:

$$A = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 3 & a \end{pmatrix} \text{ και } B = \begin{pmatrix} 1 & 2 & 2 \\ 4 & 1 & 3 \end{pmatrix} \in M_{2\times 3}(\mathbb{Z})$$

είναι ισοδύναμοι;

iii. Βρείτε μια κανονική μορφή Smith του πίνακα $A = \begin{pmatrix} 2x & 0 \\ x & 2 \end{pmatrix} \in M_2(\mathbb{Q}[x])$. Δείξτε ότι, ως στοιχείο του $M_2(\mathbb{Z}[x])$, ο A δεν είναι ισοδύναμος με διαγώνιο πίνακα. Συνεπώς, το θεώρημα κανονικής μορφής του Smith γενικά δεν αληθεύει για περιοχές στη θέση περιχών κυρίων ιδεωδών.

Πρόταση 7.1: *Έστω R να είναι μία περιοχή κυρίων ιδεωδών. Έστω επίσης πίνακες $N, M \in M(R)$ με κανονικές μορφές Smith, $\mathrm{Diag}(n_1, \cdots, n_k)$ και $\mathrm{Diag}(m_1, \cdots, m_k)$, με τα στοιχεία n_i και m_i να είναι συντροφικά. Οι πίνακες N, M είναι πάντοτε μεταξύ τους ισοδύναμοι.*

Απόδειξη: Εφόσον οι κανονικές μορφές Smith διαφέρουν μόνο 'κατά συντροφικότητα', μπορούμε να υποθέσουμε ότι υπάρχουν αντιστρέψιμοι πίνακες $X, Y, \tilde{X}, \tilde{Y}$ τέτοιοι ώστε:

$$N = X \cdot \mathrm{Diag}(n_1, \cdots, n_k) \cdot Y \textbf{ και } M = \tilde{X} \cdot \mathrm{Diag}(n_1, \cdots, n_k) \cdot \tilde{Y}$$

Επομένως:

$$N = X\tilde{X}^{-1} \cdot M \cdot \tilde{Y}^{-1}Y$$

Επειδή οι $X\tilde{X}^{-1}$, $\tilde{Y}^{-1}Y$ είναι αντιστρέψιμοι, το ζητούμενο αποδεικνύεται.

△

Πρόταση 7.2: *Ισχύει το αντίστροφο της προηγούμενης πρότασης.*

Απόδειξη: Έστω $D = \mathrm{Diag}(n_1, \cdots n_k)$ μία κανονική μορφή Smith του N και $N = X \cdot D \cdot Y$, με τους X, Y να είναι αντιστρέψιμοι. Εάν οι N, M είναι ισοδύναμοι, υπάρχουν αντιστρέψιμοι $\tilde{X}, \tilde{Y}$ τέτοιοι ώστε $M = \tilde{X} \cdot N \cdot \tilde{Y}$, και επομένως:

$$M = \tilde{X}X \cdot D \cdot Y\tilde{Y}$$

Αυτό δείχνει ότι η D μπορεί να αποτελέσει κανονική μορφή Smith του B, κι άρα κάθε κανονική μορφή του B διαφέρει μόνο 'κατά συντροφικότητα' από την D.

△

$\boxed{\text{i.}}$ *Λύση:* Σύμφωνα με την **Πρόταση 7.1**, αρκεί να ελέγξουμε αν οι κανονικές μορφές των πινάκων διαφέρουν 'κατά συντροφικότητα'.

$$\begin{pmatrix} 2 & 0 & 2 \\ 4 & 6 & 2 \\ 2 & 0 & 2 \end{pmatrix} \xrightarrow{\Gamma_3 \rightsquigarrow \Gamma_3 - \Gamma_1} \begin{pmatrix} 2 & 0 & 2 \\ 4 & 6 & 2 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\Gamma_2 \rightsquigarrow \Gamma_2 - 2\Gamma_1} \begin{pmatrix} 2 & 0 & 2 \\ 0 & 6 & -2 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\Sigma_3 \rightsquigarrow \Sigma_3 - \Sigma_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & -2 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\Sigma_2 \rightsquigarrow \Sigma_2 + 3\Sigma_1}$$

$$\xrightarrow{\Sigma_2 \rightsquigarrow \Sigma_2 + 3\Sigma_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\Sigma_3 \leftrightarrow \Sigma_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

και:

$$\begin{pmatrix} 2 & 4 & 2 \\ 0 & 2 & 0 \\ 2 & 4 & 2 \end{pmatrix} \xrightarrow{\Gamma_3 \rightsquigarrow \Gamma_3 - \Gamma_1} \begin{pmatrix} 2 & 4 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\Gamma_1 \rightsquigarrow \Gamma_1 - 2\Gamma_2} \begin{pmatrix} 2 & 0 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{\Sigma_3 \rightsquigarrow \Sigma_3 - \Sigma_1} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Οι κανονικές λοιπόν μορφές Smith διαφέρουν μόνο 'κατά συντροφικότητα'.

□

$\boxed{\text{ii.}}$ *Λύση:* Από την **Πρόταση 7.2**, αρκεί να μελετήσουμε τις κανονικές μορφές Smith των δύο πινάκων.

Για τον πρώτο:

$$\begin{pmatrix} 1 & 2 & 4 \\ 3 & 3 & a \end{pmatrix} \xrightarrow{\Sigma_3 \rightsquigarrow \Gamma_2 - 3\Gamma_1} \begin{pmatrix} 1 & 2 & 4 \\ 0 & -3 & a-12 \end{pmatrix} \xrightarrow{\Gamma_3 \rightsquigarrow \Sigma_3 - 4\Sigma_1} \begin{pmatrix} 1 & 2 & 0 \\ 0 & -3 & a-12 \end{pmatrix} \xrightarrow{\Sigma_2 \rightsquigarrow \Sigma_2 - 2\Sigma_1}$$

$$\xrightarrow{\Sigma_2 \rightsquigarrow \Sigma_2 - 2\Sigma_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & a-12 \end{pmatrix} \xrightarrow{\Sigma_3 \rightsquigarrow \Sigma_3 - 4\Sigma_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & a \end{pmatrix}$$

Για τον δεύτερο:

$$\begin{pmatrix}1 & 2 & 2\\ 4 & 1 & 3\end{pmatrix} \xrightarrow{\Sigma_3 \rightsquigarrow \Sigma_3 - \Sigma_2} \begin{pmatrix}1 & 2 & 0\\ 4 & 1 & 2\end{pmatrix} \xrightarrow{\Gamma_2 \rightsquigarrow \Gamma_2 - 4\Gamma_1} \begin{pmatrix}1 & 2 & 0\\ 0 & -7 & 2\end{pmatrix} \xrightarrow{\Sigma_2 \rightsquigarrow \Sigma_2 + 3\Sigma_2} \begin{pmatrix}1 & 2 & 0\\ 0 & -1 & 2\end{pmatrix} \xrightarrow{\Sigma_2 \rightsquigarrow \Sigma_2 - 2\Sigma_1}$$

$$\xrightarrow{\Sigma_2 \rightsquigarrow \Sigma_2 - 2\Sigma_1} \begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 2\end{pmatrix} \xrightarrow{\Sigma_3 \rightsquigarrow \Sigma_3 + 2\Sigma_2} \begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\end{pmatrix}$$

Για να ισχύει η ισότητα μεταξύ των δύο πινάκων, ισχυριζόμαστε ότι η συνθήκη $1 \in \gcd(3, a)$ είναι ικανή και αναγκαία. Πράγματι, αν $1 \in \gcd(3, a)$, υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $ax - 3y = 1$. Επομένως:

$$\begin{pmatrix}1 & 0 & 0\\ 0 & -3 & a\end{pmatrix} \xrightarrow{\Sigma_2 \rightsquigarrow -y\Sigma_2 - x\Sigma_3} \begin{pmatrix}1 & 0 & 0\\ 0 & -1 & a\end{pmatrix} \xrightarrow{\Sigma_3 \rightsquigarrow \Sigma_3 + a\Sigma_2} \begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\end{pmatrix}$$

η κανονική μορφή Smith του δεύτερου αποτελεί κανονική μορφή Smith και του πρώτου. Αντιστρόφως, αν $1 < \delta \in \gcd(3, a)$ (μπορούμε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι $\delta > 0$), τότε υπάρχουν $x, y \in \mathbb{Z}$ τέτοια ώστε $ax - 3y = \delta$. Επομένως:

$$\begin{pmatrix}1 & 0 & 0\\ 0 & -3 & a\end{pmatrix} \xrightarrow{\Sigma_2 \rightsquigarrow -y\Sigma_2 - x\Sigma_3} \begin{pmatrix}1 & 0 & 0\\ 0 & -\delta & a\end{pmatrix} \xrightarrow{\Sigma_3 \rightsquigarrow \Sigma_3 + (a/\delta)\Sigma_2} \begin{pmatrix}1 & 0 & 0\\ 0 & -\delta & 0\end{pmatrix}$$

η κανονική μορφή Smith του δεύτερου δεν μπορεί να αποτελεί κανονική μορφή Smith του πρώτου, αφού δεν διαφέρουν μόνο 'κατά συντροφικότητα'.

$\square$

$\boxed{\text{iii.}}$ <u>*Λύση:*</u> Στο $M_2(\mathbb{Q}[x])$ έχουμε ότι:

$$\begin{pmatrix}2x & 0\\ x & 2\end{pmatrix} \xrightarrow{\Sigma_1 \leftrightarrow \Sigma_2} \begin{pmatrix}0 & 2x\\ 2 & x\end{pmatrix} \xrightarrow{\Gamma_1 \rightsquigarrow \Gamma_1 - 2\Gamma_2} \begin{pmatrix}-4 & 0\\ 2 & x\end{pmatrix} \xrightarrow{(\star)\ \Gamma_2 \rightsquigarrow \Gamma_2 + (1/2)\Gamma_1} \begin{pmatrix}-4 & 0\\ 0 & x\end{pmatrix}$$

Στο $M_2(\mathbb{Z}[x])$ οι ίδιοι μετασχηματισμοί μπορούν να ακολουθηθούν αυτούσια ως το βήμα $(\star)$. Το ίδιο το βήμα $(\star)$ δεν μπορεί να γίνει σε αυτήν την περίπτωση, αφού $2 \notin U(\mathbb{Z}[x])$.

Στο $M_2(\mathbb{Z}[x])$ λοιπόν ο A δεν είναι ισοδύναμος με διαγώνιο πίνακα. Πράγματι, έστω ότι υπάρχει διαγώνιος πίνακας $D = \begin{pmatrix}P(x) & 0\\ 0 & Q(x)\end{pmatrix} \in M_2(\mathbb{Z}[x])$ τέτοιος ώστε:

$$A = X \cdot D \cdot Y, \text{ με } X, Y \in U(M_2(\mathbb{Z}[x]))$$

Τότε παρατηρούμε ότι $\det A = \sigma \cdot \det D,\ \sigma \in U(\mathbb{Z}[x]) = \{\pm 1\}$. Επομένως, $4x = \pm P(x) \cdot Q(x)$, το οποίο σημαίνει ότι κάποιο από τα $P(x), Q(x)$ είναι σταθερό. Έστω (κι αυτό χωρίς βλάβη της γενικότητας) ότι το P είναι σταθερό. Οι μορφές των $P, Q(x)$ είναι λοιπόν οι ακόλουθες:

$$P = \pm 1, Q(x) = \pm 4x \textbf{ ή } P = \pm 2, Q(x) = \pm 2x \textbf{ ή } P = \pm 4, Q(x) = \pm x$$

Σε κάθε περίπτωση παρατηρούμε ότι τα ιδεώδη Fitting $J_1(A), J_1(D)$ δεν ισούνται, οπότε οι A και D δεν είναι ισοδύναμοι. Αυτό είναι άτοπο, και κατ' επέκταση ο A στο $M_2(\mathbb{Z}[x])$ δεν είναι ισοδύναμος με κανέναν διαγώνιο[1].

$\square$

Άσκηση 8 Αν οι πίνακες $A_1, A_2, A_3, A_4 \in M_7(\mathbb{Z}[i])$ έχουν ορίζουσα $(6-i)^3$, τότε δύο εξ αυτών είναι ισοδύναμοι. ■

<u>*Λύση:*</u> Η περιοχή $\mathbb{Z}[i]$ είναι κυρίων ιδεωδών, επομένως κάθε πίνακας του $M_n(\mathbb{Z}[i])$ ορίζει μια κανονική μορφή Smith.

Ορίζουμε μια σχέση ισοδυναμίας '$\sim$' στο $[M_n(\mathbb{Z}[i])]^2$ ως εξής: Έστω $\mathrm{Diag}(a_1, \cdots, a_n), \mathrm{Diag}(b_1, \cdots, b_n)$ δύο κανονικές μορφές Smith των A και B αντίστοιχα.

$$A \sim B :\Leftrightarrow \exists\, \sigma_1, \cdots, \sigma_n \in U(\mathbb{Z}[i]) : \forall i \in [n],\ a_i = \sigma_i \cdot b_i$$

Σύμφωνα με τις **Προτάσεις 7.1, 7.2**, δύο πίνακες A, B του $M_n(\mathbb{Z}[i])$ είναι ισοδύναμοι αν και μόνο αν $A \sim B$.

Επιπλέον, εάν $D_A = \mathrm{Diag}(a_1, \cdots, a_n)$ είναι μια κανονική μορφή Smith του A:

$$D_A = X \cdot A \cdot Y \Rightarrow \det D_A = \sigma \cdot \det A \Rightarrow \det(A) = \det\left[\frac{1}{\sigma} D_A\right],\ \sigma \in U(\mathbb{Z}[i])$$

[1] Εδώ θα πρέπει να ευχαριστήσω θερμά τη φοιτήτρια 'Τσουτσουλοπούλου Ελευθερία', που εντόπισε μία τεράστια  που έκανα.

υπάρχει κανονική μορφή Smith $\frac{1}{\sigma}D_A = \mathrm{Diag}\left(a_1, \cdots, \frac{a_n}{\sigma}\right)$ του A η οποία έχει ορίζουσα ίση με αυτήν του A. Επιπλέον, $D_A \sim A \sim \frac{1}{\sigma}D_A$.

Έχοντας πει όλα αυτά, θεωρούμε όλες τις κλάσεις ισοδυναμίας πινάκων του $M_7(\mathbb{Z}[i])$, ως προς τη σχέση '$\sim$', οι οποίοι έχουν ορίζουσα $(6-i)^3$. Εφόσον για κάθε πίνακα A_i υπάρχουν κανονικές μορφές Smith με ορίζουσα αυτήν του A_i, ο A_i θα είναι ισοδύναμος με κάποιον διαγώνιο πίνακα με ορίζουσα $\det A_i = (6-i)^3$. Στις κλάσεις ισοδυναμίας που θα βρούμε λοιπόν, οι πίνακες A_i δεν γίνεται να μην ανήκουν σε καμμία απ' αυτές.

$$\{M \in M_7(\mathbb{Z}[i]) \mid \det M = (6-i)^3\}\big/_{\sim} = \Big\{ \mathrm{Diag}(1, \cdots, 1, (6-i)^3)\big/_{\sim},\ \mathrm{Diag}(1, \cdots, 1, (6-i), (6-i)^2)\big/_{\sim},$$
$$\mathrm{Diag}(1, \cdots, 1, (6-i), (6-i), (6-i))\big/_{\sim}\Big\}$$

Οι προηγούμενες κλάσεις είναι στο πλήθος 3, οπότε από την αρχή του περιστεριώνα, υπάρχουν δύο πίνακες A_i οι οποίοι ανήκουν στην ίδια κλάση.

□

Άσκηση 9 Να παρασταθεί η αβελιανή ομάδα $\mathbb{Z}^3\big/_{\mathrm{Im}\varphi}$ ως ευθύ άθροισμα κυκλικών ομάδων, όπου:

$$\varphi : \mathbb{Z}^2 \to \mathbb{Z}^3,\ (x, y) \mapsto (4x + 2y,\ 6x + 6y,\ 10x + 8y)$$

<u>*Λύση:*</u> Έστω A, B δύο ελεύθερα $R-$πρότυπα και R περιοχή κυρίων ιδεωδών. Έστω επίσης $\varphi \in \mathrm{Hom}_{\mathrm{R-Mod}}(A, B)$ με πίνακα $(\varphi : \mathbb{A}, \mathbb{B}) \in M_{s\times t}(R)$ ως προς τις βάσεις $\mathbb{A}, \mathbb{B}$ των A και B αντίστοιχα. Γνωρίζουμε (κι αυτό ως πόρισμα της κανονικής μορφής Smith) ότι:

$$\mathrm{coker}\varphi \simeq \left[\bigoplus_{i\in[\min\{s,t\}]} \left[R\big/_{(\!|d_i|\!)}\right]\right] \oplus R^{s-\min\{s,t\}}$$

όπου τα $d_1|d_2|\cdots|d_{\min\{s,t\}}$ αποτελούν στοιχεία της διαγωνίου μίας κανονικής μορφής Smith του $(\varphi : \mathbb{A}, \mathbb{B})$.

Αυτό το πόρισμα είναι που ουσιαστικά θα λύσει την άσκηση. Θεωρούμε M_φ τον πίνακα της φ ως προς τις συνήθεις βάσεις:

$$M_\varphi = \begin{pmatrix} 4 & 2 \\ 6 & 6 \\ 10 & 8 \end{pmatrix}$$

καθώς επίσης και μια κανονική μορφή Smith αυτού:

$$\begin{pmatrix} 4 & 2 \\ 6 & 6 \\ 10 & 8 \end{pmatrix} \xrightarrow{\Sigma_1 \rightsquigarrow \Sigma_1 - \Sigma_2} \begin{pmatrix} 2 & 2 \\ 0 & 6 \\ 2 & 8 \end{pmatrix} \xrightarrow{\Sigma_2 \rightsquigarrow \Sigma_2 - \Sigma_1} \begin{pmatrix} 2 & 0 \\ 0 & 6 \\ 2 & 6 \end{pmatrix} \xrightarrow{\Gamma_3 \rightsquigarrow \Gamma_3 - \Gamma_1} \begin{pmatrix} 2 & 0 \\ 0 & 6 \\ 0 & 6 \end{pmatrix} \xrightarrow{\Gamma_3 \rightsquigarrow \Gamma_3 - \Gamma_2} \begin{pmatrix} 2 & 0 \\ 0 & 6 \\ 0 & 0 \end{pmatrix}$$

Συμφωνα με το προηγούμενο πόρισμα, έχουμε ότι:

$$\mathbb{Z}^3\big/_{\mathrm{Im}\varphi} = \mathrm{coker}\varphi \simeq \left[\mathbb{Z}\big/_{(\!|2|\!)}\right] \oplus \left[\mathbb{Z}\big/_{(\!|6|\!)}\right] \oplus \mathbb{Z} = \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}$$

□

Άσκηση 10 Έστω $\varphi \in \mathrm{Hom}_{\mathrm{R-Mod}}(\mathbb{Z}^n, \mathbb{Z}^n)$, όπου το $\mathbb{Z}^n$ θεωρείται $\mathbb{Z}-$πρότυπο. Έστω επίσης α μια διατεταγμένη βάση του $\mathbb{Z}^n$ και $A = (\varphi : \alpha, \alpha) \in M_n(\mathbb{Z})$. Δείξτε ότι αν $\det A \neq 0$, τότε $\#\left[\mathbb{Z}^n\big/_{\mathrm{Im}\varphi}\right] = |\det A|$

Λήμμα 10.1 *Έστω R μία περιοχή κυρίων ιδεωδών και A ένας πίνακας στο $M_n(R)$. Υπάρχει μια κανονική μορφή Smith D του A τέτοια ώστε $\det D = \det A$.*

Απόδειξη: Έστω $D_A = \mathrm{Diag}(a_1, \cdots, a_n)$ μία κανονική μορφή Smith του A. Παρατηρούμε ότι:

$$D_A = X \cdot A \cdot Y \Rightarrow \det D_A = [\det(X)\det(Y)] \cdot \det A = \sigma \cdot \det A,\ \sigma \in U(R)$$

κι επομένως η κανονική μορφή Smith $D = \dfrac{1}{\sigma} D_A = \mathrm{Diag}\left(a_1, \cdots, \dfrac{a_n}{\sigma}\right)$ έχει ορίζουσα $\det D = \det A$.

$\triangle$

Λύση: Έστω $D = \mathrm{Diag}(d_1, \cdots, d_n)$ μία κανονική μορφή Smith του A με $\det D = \det A$ (τέτοια μορφή υπάρχει, από το **Λήμμα 10.1**). Παρατηρούμε ότι επειδή $\det A \neq 0$ και $\det D = \det \mathrm{Diag}(d_1, \cdots, d_n) = \prod_{k \in [n]} d_i$, κανένα από τα στοιχεία d_i δεν είναι μηδενικό.

Επιπλέον, γνωρίζουμε ως πόρισμα της κανονικής μορφής Smith ότι:

$$\mathbb{Z}^n \big/ \mathrm{Im}\varphi = \mathrm{coker}\varphi \simeq \bigoplus_{k \in [n]} \left[\mathbb{Z} \big/ (\!| d_k |\!) \right] = \bigoplus_{k \in [n]} \mathbb{Z}_{d_k}$$

κι επομένως:

$$\# \left[\mathbb{Z}^n \big/ \mathrm{Im}\varphi \right] = \# \bigoplus_{k \in [n]} \mathbb{Z}_{d_k} = \prod_{k \in [n]} |d_k| = \left| \prod_{k \in [n]} d_k \right|$$

Επειδή $\det A = \det D = \det \mathrm{Diag}(d_1, \cdots, d_n) = \prod_{k \in [n]} d_k$, έχουμε το ζητούμενο:

$$\# \left[\mathbb{Z}^n \big/ \mathrm{Im}\varphi \right] = \left| \prod_{k \in [n]} d_k \right| = |\det A|$$

$\square$