1ο Φυλλάδιο Ασκήσεων - Δακτύλιοι και Πρότυπα

Αναστάσιος Φράγκος: ΑΜ 1112201900239 Κυριακή, 07 Νοεμβρίου 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. $\gcd(m,n) = \{d \mid d \text{ είναι μέγιστος κοινός διαιρέτης των } m,n\}$.
3. $\mathbb{C} := \mathbb{R}^2$.
4. $[n] := [1,n] \cap \mathbb{N}$.
5. Έστω R δακτύλιος και $A, B \subseteq R$. Ορίζουμε:

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

Επίσης, για $A \subseteq R,\ b \in R$, ορίζουμε $A \cdot b := A \cdot \{b\},\ b \cdot A := \{b\} \cdot A$.

Άσκηση 1 Θεωρούμε τον δακτύλιο $\mathbb{Z}[i]$.

i. Βρείτε ένα $d \in \mathbb{Z}[i]$ με $d \in \gcd(a,b)$, όπου $a = (4+i)^2 \cdot (1+2i), b = -16+13i$. Στη συνέχεια, βρείτε κάθε τέτοιο d.

ii. Δείξτε ότι οι δακτύλιοι $\mathbb{Z}[i]/(\!(1+2i)\!)$ και $\mathbb{Z}_5$ είναι ισόμορφοι.

iii. Αληθεύει ότι ο δακτύλιος $\mathbb{Z}[i]/(\!(d)\!)$, όπου $d = (4+i)\cdot(1+2i)$, είναι ισόμορφος με ευθύ γινόμενο σωμάτων;

iv. Πόσα μηδενοδύναμα στοιχεία έχει ο δακτύλιος του προηγούμενου ερωτήματος;

■

i. *Λύση:* Έστω $d \in \gcd(a,b)$. Επειδή $d|a$ και $d|b$, για τα μέτρα αυτών ισχύει $|d| \mid |a|$, $|d| \mid |b|$. Ειδικότερα, $|d| \mid 17^2 \cdot 5$, $|d| \mid 425 = 17 \cdot 5^2$. Επειδή $|4+i| = 17$, $|1+2i| = 5$ και $|b| = 17 \cdot 5^2$, υποψιαζόμαστε ότι $b = \sigma \cdot (4+i) \cdot (1+2i)^2$, όπου $\sigma \in U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$. Κατ' επέκταση, ο $d = (4+i)\cdot(1+2i)$ είναι ένας μέγιστος κοινός διαιρέτης. Πράγματι:

$$\begin{aligned}(4+i)\cdot(1+2i)^2 &= (4,1)(1,2)^2 \\ &= (4,1)(1-4,2+2) \\ &= (4,1)(-3,4) \\ &= (-12-4,16-3) \\ &= (-16,13) \\ &= -16+13i\end{aligned}$$

Κάθε άλλος μέγιστος κοινός διαιρέτης $\tilde{d}$ είναι συντροφικός του d, αφού αν $\tilde{d} \in \gcd(a,b)$, τότε $\tilde{d}|d$ και επειδή $d \in \gcd(a,b)$ έπεται $d|\tilde{d}$. Το σύνολο λοιπόν των μεγίστων κοινών διαιρετών είναι το $\gcd(a,b) = U(\mathbb{Z}[i])d = \{\pm d, \pm i \cdot d\}$. □

ii. **Λήμμα 1.1:** *Έστω $a,b \in \mathbb{Z}$ τέτοιοι ώστε $1 \in \gcd(a,b)$. Θεωρούμε τις διοφαντικές εξίσωσεις για $k \in \mathbb{Z}$:*

$$ax + by = ck,\ c \in \mathbb{R}$$

Εάν για $k=1$ μια της λύση είναι η $(x_0,y_0) \neq (0,0)$, τότε κάθε άλλη λύση (x,y) καθεμίας από τις διοφαντικές εξισώσεις, μπορεί να γραφεί στην μορφή $(\tilde{x},\tilde{y})\cdot(x_0,y_0)$, για $(\tilde{x},\tilde{y}) \in \mathbb{Z}[i]$.

Απόδειξη: Εφόσον $1 \in \gcd(a,b)$ υπάρχει μια λύση $(x_0,y_0) \neq (0,0)$ της διοφαντικής εξίσωσης με $k=1$.

Για τυχαίο λοιπόν $k \in \mathbb{Z}$, η $k(x_0, y_0)$ αποτελεί λύση της $k-$οστής διοφαντικής εξίσωσης. Η γενική λοιπόν μορφή των λύσεων θα είναι:

$$x = kx_0 + bt,\ y = ky_0 - at \text{ για } t \in \mathbb{Z}$$

Δείχνοντας ότι για κάθε $(x, y) = (kx_0 + bt,\ ky_0 - at)$ υπάρχει $(\tilde{x}, \tilde{y}) \in \mathbb{Z}[i]$ τέτοιο ώστε $(x, y) = (\tilde{x}, \tilde{y}) \cdot (x_0, y_0)$, θα έχουμε ουσιαστικά αποδείξει το ζητούμενο.

Η ύπαρξη αυτή ισοδυναμεί με ύπαρξη λύσης του συστήματος, ως προς $\tilde{x}, \tilde{y}$:

$$\begin{aligned} \tilde{x}x_0 - \tilde{y}y_0 &= kx_0 + bt \\ \tilde{x}y_0 + \tilde{y}x_0 &= ky_0 - at \end{aligned}$$

Το τελευταίο έχει πάντοτε λύση, αφού:

$$\begin{vmatrix} x_0 & -y_0 \\ y_0 & x_0 \end{vmatrix} = x_0^2 + y_0^2 > 0$$

△

Λύση: Αρχικά θα αναζητήσουμε μια γραμμική απεικόνιση $\varphi : \mathbb{C} \to \mathbb{R}$ η οποία θα μηδενίζεται στο $1 + 2i$. Μια τέτοια απεικόνιση είναι η:

$$\varphi : \varphi(x, y) = x + 2y$$

Έπειτα ορίζουμε την απεικόνιση $\psi : \mathbb{Z}[i] \to \mathbb{Z}_5$:

$$\psi : \psi(x, y) = \varphi|_{\mathbb{Z}[i]}(x, y) + (\!|5|\!)$$

και παρατηρούμε ότι και αυτή είναι ομομορφισμός, με πυρήνα $\ker \psi = (\!|1 + 2i|\!)$. Το ότι ο πυρήνας είναι πράγματι το εν λόγω σύνολο προκύπτει από το **Λήμμα 1.1**. Η ψ είναι ομομορφισμός διότι:

- $\varphi\big((x, y) + (z, w)\big) = x + z + 2(y + w) + (\!|5|\!) = \big[x + 2y + (\!|5|\!)\big] + \big[z + 2w + (\!|5|\!)\big] = \varphi(x, y) + \varphi(z, w).$
- $\varphi\big((x, y)(z, w)\big) = xz - 4yw + 2(yz + xw) + (\!|5|\!) = xz + yw + 2(yz + xw) + (\!|5|\!) = \varphi(x, y) \cdot \varphi(z, w).$

Επιπλέον, η ψ είναι επί του $\mathbb{Z}_5$, αφού $\psi([5] \times \{0\}) = \mathbb{Z}_5$, επομένως είναι και επιμορφισμός.

Τα αποτελέσματα αυτά δίνουν ουσιαστικά το ζητούμενο, αφού από το $1^{\text{ο}}$ θεώρημα ισομορφισμών:

$$\mathbb{Z}[i] \Big/ \ker \psi \simeq \psi(\mathbb{Z}[i]) \Rightarrow \mathbb{Z}[i] \Big/ (\!|1 + 2i|\!) \simeq \mathbb{Z}_5$$

□

iii. *Λύση:* Τα στοιχεία $4 + i$ και $1 + 2i$ είναι ανάγωγα στο $\mathbb{Z}[i]$, αφού $|4 + i| = 17$, $|1 + 2i| = 5$ και οι $17, 5$ είναι πρώτοι αριθμοί. Εφόσον λοιπόν είναι ανάγωγα, το Κινέζικο θεώρημα υπολοίπων δίνει:

$$\mathbb{Z}[i] \Big/ (\!|d|\!) = \mathbb{Z}[i] \Big/ (\!|(4 + i)(1 + 2i)|\!) \simeq \left[\mathbb{Z}[i] \Big/ (\!|4 + i|\!) \right] \oplus \left[\mathbb{Z}[i] \Big/ (\!|1 + 2i|\!) \right]$$

Ο δακτύλιος $\mathbb{Z}[i] \Big/ (\!|1 + 2i|\!)$ είναι σώμα, αφού είναι ισόμορφος του $\mathbb{Z}_5$, το οποίο είναι σώμα. Θα δείξουμε ότι ο δακτύλιος $\mathbb{Z}[i] \Big/ (\!|4 + i|\!)$ είναι ισόμορφος του $\mathbb{Z}_{17}$, κι επομένως είναι κι αυτός σώμα, αφού ο $\mathbb{Z}_{17}$ είναι σώμα. Με αυτό θα έχουμε ουσιαστικά δείξει ότι ο $\mathbb{Z}[i] \Big/ (\!|d|\!)$ είναι ευθύ γινόμενο δύο σωμάτων.

Αναζητήτούμε μια γραμμική απεικόνιση $\varphi : \mathbb{C} \to \mathbb{R}$ η οποία θα μηδενίζεται στο $4 + i$. Μια τέτοια απεικόνιση είναι η:

$$\varphi : \varphi(x, y) = x - 4y$$

Έπειτα ορίζουμε την απεικόνιση $\psi : \mathbb{Z}[i] \to \mathbb{Z}_{17}$:

$$\psi : \psi(x, y) = \varphi|_{\mathbb{Z}[i]}(x, y) + (\!|17|\!)$$

και παρατηρούμε ότι και αυτή είναι ομομορφισμός, με πυρήνα $\ker \psi = (\!|4 + i|\!)$. Το ότι ο πυρήνας είναι πράγματι το εν λόγω σύνολο προκύπτει από το **Λήμμα 1.1**. Η ψ είναι ομομορφισμός διότι:

- $\varphi\big((x, y) + (z, w)\big) = x + z + 4(y + w) + (\!|17|\!) = \big[x + 4y + (\!|17|\!)\big] + \big[z + 4w + (\!|17|\!)\big] = \varphi(x, y) + \varphi(z, w).$
- $\varphi\big((x, y)(z, w)\big) = xz - yw - 4(yz + xw) + (\!|17|\!) = xz + 16yw - 4(yz + xw) + (\!|17|\!) = \varphi(x, y) \cdot \varphi(z, w).$

Επιπλέον, η ψ είναι επί του $\mathbb{Z}_{17}$, αφού $\psi([17]\times\{0\})=\mathbb{Z}_{17}$, επομένως είναι και επιμορφισμός.

Τα αποτελέσματα αυτά δίνουν ουσιαστικά το ζητούμενο, αφού από το $1^{\text{ο}}$ θεώρημα ισομορφισμών:

$$\mathbb{Z}[i]\Big/_{\ker\psi}\simeq\psi(\mathbb{Z}[i])\Rightarrow\ \mathbb{Z}[i]\Big/_{(\!(4+i)\!)}\simeq\mathbb{Z}_{17}$$

□

iv. *Λύση:* Θα προσδιορίσουμε τον πληθάριθμο $\#\mathrm{Ann}_{\mathbb{Z}[i]}\left(\mathbb{Z}[i]\Big/_{(\!(d)\!)}\right)$. Παρατηρούμε ότι:

$$\mathbb{Z}d\subseteq\mathrm{Ann}_{\mathbb{Z}[i]}\left(\mathbb{Z}[i]\Big/_{(\!(d)\!)}\right)$$

αφού $\forall k\in\mathbb{Z},\ \forall x+(\!(d)\!)\in\mathbb{Z}[i]\Big/_{(\!(d)\!)}:\ (kd)\big(x+(\!(d)\!)\big)=kdx+(\!(d)\!)=\mathbf{0}_{\mathbb{Z}[i]/_{(\!(d)\!)}}$.

Αυτό μας δείχνει ότι το πλήθος των στοιχείων του μηδενιστή είναι άπειρο.

□

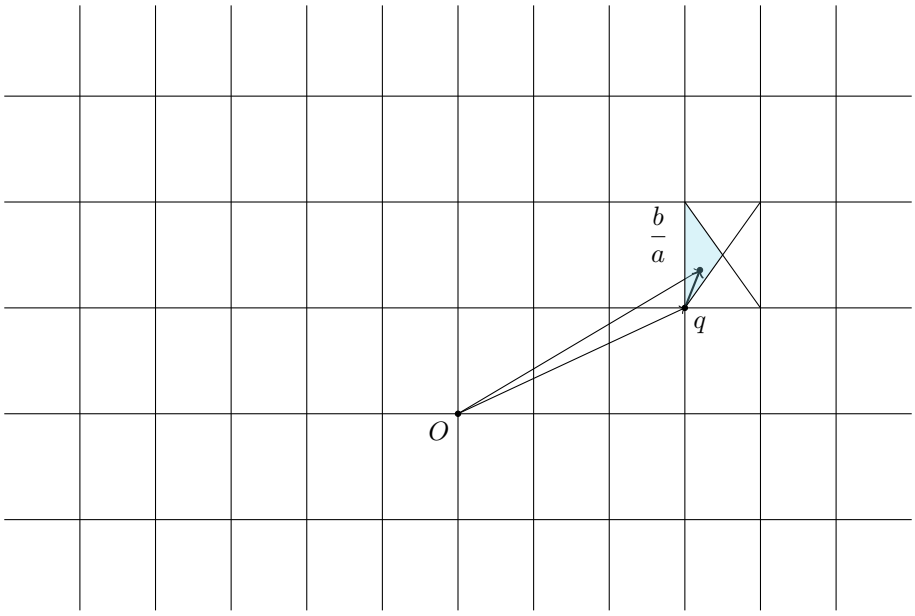
Άσκηση 2 Δείξτε ότι η περιοχή $\mathbb{Z}[i\sqrt{2}]$ είναι ευκλείδεια ως προς τη συνάρτηση $\varphi(z)=|z|^2,\ z\in\mathbb{C}$. ■

Λύση: Έστω $a,b\in\mathbb{Z}[i\sqrt{2}]$. Εάν υπάρχει $c\in\mathbb{Z}[i\sqrt{2}]$ τέτοιο ώστε $b=ac$, τότε $\varphi(b)=b\bar{b}=ac\cdot\overline{ac}=a\bar{a}\cdot c\bar{c}=\varphi(a)\cdot\varphi(c)\Rightarrow\varphi(a)\mid\varphi(b)$ και συνεπώς $\varphi(a)\le\varphi(b)$.

Σε διαφορετική περίπτωση, θεωρούμε στο σύνηθες καρτεσιανό επίπεδο, τον μιγαδικό αριθμό $\dfrac{b}{a}$ (με $a\neq0$). Ο αριθμός αυτός δεν είναι σε κάποια κορυφή της μορφής $(k,m\sqrt{2}),\ (k,m)\in\mathbb{Z}^2$, είναι όμως σίγουρα σε κάποιο παραλληλόγραμο κορυφών $A=(x,y\sqrt{2}),\ B=(x+1,y\sqrt{2}),\ \Gamma=\big(x,(y+1)\sqrt{2}\big),\ \Delta=\big(x+1,(y+1)\sqrt{2}\big)$. Θεωρούμε K το σημείο τομής των διαγωνίων $A\Delta$ και $B\Gamma$, και παρατηρούμε ότι ο αριθμός $\dfrac{b}{a}$ ανήκει σε ένα από τα τρίγωνα $\overset{\triangle}{AB}K,\ \overset{\triangle}{BK}\Delta,\ \overset{\triangle}{AK}\Gamma,\ \overset{\triangle}{\Gamma K}\Delta$, ή στις πλευρές αυτών. Τότε όμως, ο αριθμός $\dfrac{b}{a}$ απέχει το πολύ $|A\Delta|=\dfrac{\sqrt{3}}{2}$ από την κοντυνότερή του κορυφή στο παραλληλόγραμμο. Έστω $q=(x_q,y_q\sqrt{2}),\ (x_q,y_q)\in\mathbb{Z}^2$ να είναι αυτή η κοντυνότερη κορυφή. Θεωρούμε τον μιγαδικό αριθμό $r=b-aq$ και παρατηρούμε ότι $b=aq+r$. Επιπλέον:

$$\varphi(r)=|r|^2=|b-aq|^2=|a|^2\cdot\left|\frac{b}{a}-q\right|^2\le|a|^2\cdot\frac{3}{4}<|a|^2=\varphi(a)$$

Αυτό αποδεικνύει ότι η περιοχή $\mathbb{Z}[i\sqrt{2}]$ είναι ευκλείδεια ως προς τη συνάρτηση $\varphi(z)$.



□

Άσκηση 3 Θεωρούμε την περιοχή $R = \mathbb{Z}[i\sqrt{2}]$.

i. Δείξτε ότι $U(R) = \{\pm 1\}$.

ii. Συμπληρώστε και αποδείξτε την πρόταση: *'Εάν p είναι πρώτος τέτοιος ώστε δεν υπάρχουν ακέραιοι x, y με $p = x^2 + 2y^2$, τότε στο R το στοιχείο είναι _____'.*

iii. Ποιά από τα στοιχεία $23, 17, 3 + 2i\sqrt{2}$ είναι ανάγωγα στο R;

iv. Αφού διαβάσετε τις σελίδες 225-226 από το [ΒΔΕΜΤ][a], διατυπώστε (χωρίς απόδειξη) μια εικασία που εμπλέκει $\bmod 8$ και που απαντάει στο ερώτημα: 'ποιοί πρώτοι παραμένουν ανάγωγα στοιχεία στο R;'

v. Βρείτε ένα m ώστε $R/(\!(1 + i\sqrt{2})\!) \simeq \mathbb{Z}_m$.

vi. Αληθεύει ότι ο δακτύλιος R/I είναι πεπερασμένος, για κάθε μη μηδενικό ιδεώδες I του R;

■

[a] Βάρσος, Δεριζιώτης, Εμμανουήλ, Μαλιάκας, Ταλέλλη: *Μια εισαγωγή στην Άλγεβρα*, Γ' έκδοση, Εκδόσεις 'Σοφία', 2012.

i. *Λύση:*[1] Έστω $(a, b\sqrt{2}) \in \mathbb{Z}[i\sqrt{2}]$. Εάν το στοιχείο αυτό είναι αντιστρέψιμο, τότε θα υπάρχει αριθμός $(c, d\sqrt{2}) \in \mathbb{Z}[i\sqrt{2}]$ τέτοιος ώστε $(a, b\sqrt{2}) \cdot (c, d\sqrt{2}) = (1, 0)$. Ισοδύναμα:

$$\begin{aligned}(1,0) &= (a, b\sqrt{2}) \cdot (c, d\sqrt{2}) \\ &= (ac - 2bd, bc\sqrt{2} + ad\sqrt{2}) \\ &\Rightarrow ac - 2bd = 1,\ (bc + ad)\sqrt{2} = 0\end{aligned}$$

Από την δεύτερη σχέση έπεται ότι $bc = -ad$. Εάν $c = 0$, τότε από την πρώτη σχέση, $-2bd = 1$. Αυτό είναι αδύνατον, αφού $b, d \in \mathbb{Z}$. Κατ' επέκταση, $c \neq 0$ και $b = -\dfrac{ad}{c}$. Με αντικατάσταση στην $ac - 2bd = 1$, μπορεί να ληφθεί ότι:

$$ac + 2d\frac{ad}{c} = 1 \Rightarrow ac^2 + 2ad^2 = c \Rightarrow a(c^2 + 2d^2) = c$$

Εάν $a, d \neq 0$ τότε $|a(c^2 + 2d^2)| > |c|$, οπότε $a = 0$ ή $d = 0$. Αν $a = 0$ τότε $c = 0$ (το οποίο αποδείξαμε ότι δεν γίνεται), οπότε αναγκαστικά $d = 0$. Για $d = 0, a \neq 0$, η ποσότητα ac^2 γίνεται (κατ' απόλυτη τιμή) μεγαλύτερη του c, εάν έστω κι ένα από τα a, c δεν είναι ± 1.

Τελικά έχουμε δείξει ότι $a, c \in \{\pm 1\}$, και κατεπέκταση, $U(\mathbb{Z}[i\sqrt{2}]) = \{(\pm 1, 0)\} = \{\pm 1\}$.

□

ii. *Λύση:* Έστω p ένας πρώτος αριθμός για τον οποίον δεν υπάρχουν $x, y \in \mathbb{Z}$ τέτοιοι ώστε $p = x^2 + 2y^2$. Τότε το p είναι ανάγωγο. Πράγματι, εάν το p δεν ήταν ανάγωγο στο $\mathbb{Z}[i\sqrt{2}]$, τότε θα υπήρχαν $(a, b\sqrt{2}),\ (c, d\sqrt{2}) \in \mathbb{Z}[i\sqrt{2}]$ τέτοια ώστε:

$$\begin{aligned}p &= (a, b\sqrt{2}) \cdot (c, d\sqrt{2}) \\ |p|^2 &= (a^2 + 2b^2) \cdot (c^2 + 2d^2) \\ p^2 &\mid (a^2 + 2b^2) \cdot (c^2 + 2d^2)\end{aligned}$$

Επειδή το p είναι πρώτος, $p = a^2 + 2b^2$ και $p = c^2 + 2d^2$. Σε κάθε περίπτωση, για $x = a,\ y = b$ ή $x = c,\ y = d$, η υπόθεση της μορφής του p δεν ισχύει. Αυτό είναι άτοπο, και συνεπώς το p είναι ανάγωγο.

□

iii. *Λύση:* Το στοιχείο 23 είναι ανάγωγο, αφού δεν υπάρχουν ακέραιοι $x, y \in \mathbb{Z}$ τέτοιοι ώστε $23 = x^2 + 2y^2$. Πράγματι, κανένας από τους αριθμούς $23 - 2 \cdot 0^2 = 23$, $23 - 2 \cdot 1^2 = 21$, $23 - 2 \cdot 2^2 = 15$, $23 - 2 \cdot 3^2 = 5$ δεν είναι τέλειο τετράγωνο.

Το 17 δεν είναι ανάγωγο, αφού γράφεται στη μορφή $17 = 3^2 + 2 \cdot 2^2$.

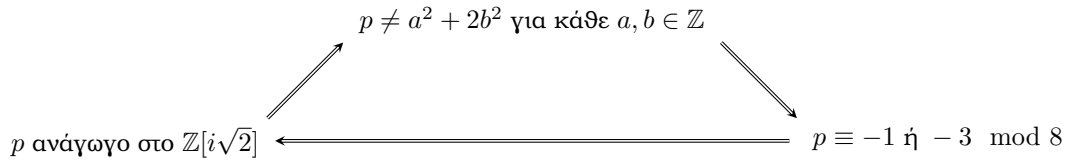
Το $3 + 2i\sqrt{2}$ είναι ανάγωγο, κι αυτό θα το αποδείξουμε μέσω του γενικότερου αποτελέσματος: *"Κάθε στοιχείο $z \in \mathbb{Z}[i\sqrt{2}]$ τέτοιο ώστε ο αριθμός $|z|^2$ να είναι πρώτος, είναι ανάγωγο στο $\mathbb{Z}[i\sqrt{2}]$"*. Πράγματι, εάν ο z δεν ήταν ανάγωγο, τότε θα μπορούσε να αναπαρασταθεί στην μορφή $z = xy$, όπου τα x και y δεν είναι αντιστρέψιμα. Από αυτό προκύπτει ότι $|z|^2 = |x|^2 \cdot |y|^2$. Επειδή ο αριθμός $|z|^2$ είναι πρώτος, κάποιο από τα x, y έχει μέτρο 1.

[1] Απλούστερα θα μπορούσε να είχε παρθεί το μέτρο του $(a, b\sqrt{2}) \cdot (c, d\sqrt{2}) = (1, 0)$.

Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $|x| = 1 \Rightarrow x \in \{\pm 1\}$. Αυτό είναι άτοπο, αφού τότε το x θα ήταν αντιστρέψιμο. Αποδεικνύεται λοιπόν ο εν λόγω ισχυρισμός και κατ' επέκταση το $3 + 2i\sqrt{2}$ είναι ανάγωγο, αφού ο $3^2 + 2 \cdot 2^2 = 17$ είναι πρώτος.

□

iv. *Λύση:* Έστω $p > 2$ πρώτος:



v. *Λύση:* Έστω $\varphi : \mathbb{Z}[i\sqrt{2}] \to \mathbb{Z}_3$ η απεικόνιση που ορίζεται ως:

$$\varphi : \varphi(x, y) = x + y\sqrt{2} + (\!|3|\!)$$

Η φ είναι ομομορφισμός, αφού:

- $\varphi\big((x, y) + (z, w)\big) = x + z + (y + w)\sqrt{2} + (\!|3|\!) = \big[x + y\sqrt{2} + (\!|3|\!)\big] + \big[z + w\sqrt{2} + (\!|3|\!)\big] = \varphi(x, y) + \varphi(z, w).$
- $\varphi\big((x, y)(z, w)\big) = xz - 2yw + (yz + xw)\sqrt{2} + (\!|3|\!) = xz + yw + (yz + xw)\sqrt{2} + (\!|3|\!) = \varphi(x, y) \cdot \varphi(z, w).$

Η φ είναι επίσης επιμορφισμός $\mathbb{Z}[i\sqrt{2}] \to \mathbb{Z}_3$, αφού $\varphi([3] \times \{0\}) = \mathbb{Z}_3$. Επειδή $\ker \varphi = (\!|1 + i\sqrt{2}|\!)$, από το 1ο θεώρημα ισομορφισμών έπεται ότι:

$$\mathbb{Z}[i\sqrt{2}] \Big/ (\!|1 + i\sqrt{2}|\!) \simeq \mathbb{Z}_3$$

□

vi. **Λήμμα 3.1:** *Κάθε ευκλείδεια περιοχή είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη: Έστω I ένα ιδεώδες της ευκλειδείου περιοχής R και φ η αντίστοιχη συνάρτηση που καθιστά την περιοχή ευκλείδεια. Ισχυριζόμαστε ότι το στοιχείο $\lambda \neq 0$ για το οποίο η φ παίρνει ελάχιστη τιμη ($\varphi(\lambda) = \min \varphi(I - \{0\})$) παράγει το ιδεώδες.

Πράγματι, εάν προς άτοπο υπήρχε στοιχείο $s \in I - (\!|\lambda|\!)$, τότε θα υπήρχαν $q, r \in R$ τέτοια ώστε:

$$s = q\lambda + r, \text{ με } \varphi(\lambda) > \varphi(r)$$

Επειδή $s, \lambda \in I$, το $0 \neq r = s - q\lambda$ είναι στοιχείο του ιδεώδους. Αυτό είναι άτοπο, αφού τότε στο λ η φ δεν παίρνει ελάχιστη τιμή. Οπότε $I - (\!|\lambda|\!) = \emptyset \Rightarrow I = (\!|\lambda|\!)$.

△

Λήμμα 3.2: *Για κάθε ευκλείδεια περιοχή R (με αντίστοιχη συνάρτηση φ) και για κάθε ιδεωδες I αυτής, το $R-$πρότυπο R/I είναι κυκλικό.*

Απόδειξη: Αναγράφουμε το R/I σε τέτοια μορφή, έτσι ώστε κάθε του στοιχείο να είναι γραμμένο ως $a + I$, όπου $\varphi(a) = \min\{\varphi(x) \mid x \in a + I\}$. Επιλέγουμε από τις κλάσεις αυτήν την $\mu + I$ για την οποία ισχύει $\varphi(\mu) = \min\left\{\varphi(x) \mid x + I \in R/I\right\}$, και υποθέτουμε προς άτοπο ότι υπάρχει κλάση $s + I$ τέτοια ώστε:

$$s + I \notin (\!|\mu + I|\!)$$

Παρατηρούμε τότε ότι υπάρχουν $q, r \in R$ με την ιδιότητα:

$$s = q\mu + r \Rightarrow s + I = (q\mu + r) + I \Rightarrow r + I \in R/I$$

Αυτό είναι άτοπο, από τον ορισμό της $\mu + I$. Κατ' επέκταση:

$$R/I = (\!|\mu + I|\!)$$

△

Λύση: Από το **Λήμμα 3.2**, για κάθε ιδεώδες I, το σύνολο $\mathbb{Z}[i\sqrt{2}]/I$ μπορεί ισοδύναμα να γραφεί στη μορφή:

$$\mathbb{Z}[i\sqrt{2}] \Big/ I = (\!|\mu + I|\!)$$

για κάποια κλάση $\mu + I$. Από το **Λήμμα 3.1**, το ιδεώδες I γράφεται στη μορφή $I = (\!|\lambda|\!)$. Κάθε τυχαίο λοιπόν στοιχείο του $\mathbb{Z}[i\sqrt{2}]/_I$, έστω $x + I$, είναι της μορφής:

$$x + I = k\mu + (\!|\lambda|\!), \text{ για } k \in \mathbb{Z}[i\sqrt{2}]$$

Επειδή υπάρχουν μόνο πεπερασμένοι αριθμοί των οποίων η εικόνα μέσω της φ γίνεται μικρότερη του $\varphi(\lambda)$, τα προηγούμενα δείχνουν ότι το σύνολο $\mathbb{Z}[i\sqrt{2}]/_I$ είναι πεπερασμένο.

□

Άσκηση 4 Έστω R μια περιοχή κυρίων ιδεωδών και $a, b \in R$. Δείξτε ότι αν $(\!|a|\!) + (\!|b|\!) = R$, τότε για κάθε $n \in \mathbb{N}$ ισχύει $(\!|a^n|\!) + (\!|b^n|\!) = R$. ■

Λήμμα 4.1: *Έστω R μια περιοχή κυρίων ιδεωδών. Ισχύει ότι:*

$$(\!|a|\!) + (\!|b|\!) = (\!|d|\!), \text{ όπου } d \in \gcd(a, b)$$

Απόδειξη: Πράγματι, το $(\!|a|\!) + (\!|b|\!)$ είναι ιδεώδες και η περιοχή R είναι περιοχή κυρίων ιδεωδών. Επομένως, υπάρχει $d \in R\gcd(a, b)$ τέτοιος ώστε $(\!|a|\!) + (\!|b|\!) = (\!|d|\!)$.

Ισχυριζόμαστε ότι $d \in \gcd(a, b)$. Πράγματι, αν $c|a,\ c|b$, τότε $c|f$ για κάθε $f \in R\gcd(a, b)$. Επομένως, $c|d$, και το ζητούμενο αποδεικνύεται.

△

Λύση: Εφόσον $(\!|a^n|\!) + (\!|b^n|\!) = R = (\!|1|\!)$, από το **Λήμμα 4.1** έπεται ότι $1 \in \gcd(a, b)$. Κατ' επέκταση, τα a, b γράφονται ως γινόμενα αναγώγων, έτσι ώστε τα ανάγωγα του πρώτου να συνηστούν ξένο σύνολο με το αντίστοιχο σύνολο των αναγώγων του δεύτερου. Υποθέτουμε ότι:

$$a = \sigma \cdot \prod_i p_i,\ b = \tau \cdot \prod_j q_j, \text{ όπου } \sigma, \tau \in U(R) \text{ και } p_i, q_j \text{ είναι ανάγωγα.}$$

Εφόσον κάθε περιοχή είναι αντιμεταθετικός δακτύλιος, ισοδύναμα μπορούμε να γράψουμε:

$$a^n = \left[\sigma \cdot \prod_i p_i,\right]^n = \sigma^n \cdot \prod_i p_i^n \text{ και } b^n = \left[\tau \cdot \prod_j q_j,\right]^n = \tau^n \cdot \prod_j q_j^n$$

και να παρατηρήσουμε ότι η εν λόγω γραφή εξασφαλίζει ότι τα $a^n,\ b^n$ δεν έχουν μη τετριμμένο (αντιστρέψιμο) κοινό διαιρέτη. Οπότε, $1 \in \gcd(a^n, b^n)$, και από το **Λήμμα 4.1**, $(\!|a^n|\!) + (\!|b^n|\!) = (\!|1|\!) = R$. Αυτό αποδεικνύει το ζητούμενο αποτέλεσμα.

□

Άσκηση 5 Εξετάστε ποιές από τις ακόλουθες προτάσεις αληθεύουν:

i. Αν R είναι περιοχή μοναδικής παραγοντοποίησης και $a, b \in R$ είναι ανάγωγα, μη συντροφικά, τότε υπάρχουν $r, s \in R$ τέτοια ώστε $ra + sb = 1$.

ii. Αν R είναι περιοχή κυρίων ιδεωδών και $a, b \in R$ είναι ανάγωγα, μη συντροφικά, τότε υπάρχουν $r, s \in R$ τέτοια ώστε $ra + sb = 1$.

iii. Κάθε υποδακτύλιος περιοχής μοναδικής παραγοντοποίησης είναι περιοχή μοναδικής παραγοντοποίησης.

iv. Κάθε υποδακτύλιος περιοχής κυρίων ιδεωδών είναι περιοχή κυρίων ιδεωδών.

v. Κάθε πηλίκο περιοχών κυρίων ιδεωδών είναι περιοχή κυρίων ιδεωδών.

■

i. *Λύση:* Ο ισχυρισμός δεν ισχύει, αφού στην περιοχή $\mathbb{Z}[x]$ τα στοιχεία $x,\ 2$ δεν έχουν γραμμικό συνδυασμό που να δίνει μονάδα[2]. Πράγματι, αν τέτοιος συνδυασμός (έστω $a(x)x + b(x)2 = 1$) υπήρχε, τότε ο σταθερός του όρος θα ήταν πολλαπλάσιο του 2 (άτοπο).

□

ii. *Λύση:* Εάν τα στοιχεία $a,\ b$ είναι ανάγωγα και μη συντροφικά, τότε $1 \in \gcd(a, b)$. Από το **Λήμμα 4.1**,

[2] Εννοείται ότι $x := id(x)$ και $\mathbf{1}_{\mathbb{Z}[x]}(x) := \mathbf{1}_{\mathbb{Z}}$.

$(\!|a|\!) + (\!|b|\!) = (\!|1|\!)$, οπότε υπάρχει γραμμικός συνδιασμός $\sigma a + \tau b \in (\!|a|\!) + (\!|b|\!)$ τέτοιος ώστε $\sigma a + \tau b = 1$.

□

iii. *Λύση:* Το σώμα $\mathbb{C}$ είναι περιοχή μοναδικής παραγοντοποίησης με τετριμμένο τρόπο:

- "*Κάθε* $a \in \mathbb{C},\ a \neq 0,\ a \notin U(\mathbb{C})$ *γράφεται ως γινόμενο αναγώγων*": Τέτοιο a δεν υπάρχει, οπότε ισχύει τετριμμένα (ισχύει για το κενό σύνολο).
- "*Εάν* $p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_n$ *τότε υπάρχει αναδιάταξη* $s \in S_n$ *τέτοια ώστε κάθε* $p_i,\ q_{s(i)}$ *να είναι συντροφικά*": Δεν υπάρχουν τέτοιες γραφές στο $\mathbb{C}$, οπότε και πάλι ισχύει τετριμμένα (ισχύει για το κενό σύνολο).

Εν γένει, κάθε σώμα είναι περιοχή μοναδικής παραγοντοποίησης, και τα επιχειρήματα για την απόδειξη αυτού του ισχυρισμού είναι εντελώς ανάλογα.

Ο υποδακτύλιος $\mathbb{Z}[i\sqrt{5}]$ κατ' αρχάς είναι υποδακτύλιος του $\mathbb{C}$, αφού:

- $\forall x, y \in \mathbb{Z}[i\sqrt{5}],\ x - y \in \mathbb{Z}[i\sqrt{5}]$
- $\forall x, y \in \mathbb{Z}[i\sqrt{5}],\ xy \in \mathbb{Z}[i\sqrt{5}]$
- $1 = 1 + 0i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$

Εϊναι περιοχή, αφού ο πολλαπλασιασμός είναι αντιμεταθετικός και $xy = 0 \Leftrightarrow 0 \in \{x, y\}$.

Επίσης δεν είναι περιοχή μοναδικής παραγοντοποίησης, αφού $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ και τα στοιχεία $2,\ 3,\ 1 + i\sqrt{5},\ 1 - i\sqrt{5}$ είναι ανάγωγα.

□

iv. *Λύση:* Ο ισχυρισμός δεν αληθεύει, αφού η περιοχή $\mathbb{R}[x]$ είναι περιοχή κυρίων ιδεωδών, ο δακτύλιος $\mathbb{Z}[x]$ είναι υποδακτύλιος του $\mathbb{R}[x]$ (και μάλιστα υποπεριοχή), και τέλος ο $\mathbb{Z}[x]$ δεν είνα περιοχή κυρίων ιδεωδών.

Ο $\mathbb{Z}[x]$ είναι υποπεριοχή του $\mathbb{R}[x]$, αφού:

- $\forall x, y \in \mathbb{Z}[x],\ x - y \in \mathbb{Z}[x]$
- $\forall x, y \in \mathbb{Z}[x],\ xy \in \mathbb{Z}[x]$
- $1 \in \mathbb{Z}[x]$
- Ο πολλαπλασιασμός είναι αντιμεταθετικός
- $xy = 0 \Leftrightarrow 0 \in \{x, y\}$

Ο $\mathbb{Z}[x]$ δεν είναι περιοχή κυρίων ιδεωδών, αφού το ιδεώδες $(\!|x, 2|\!)$ δεν είναι κύριο. Το $(\!|x, 2|\!)$ δεν είναι κύριο διότι αν ήταν, θα υπήρχε $\delta \in \mathbb{Z}[x]$ τέτοιο ώστε:

$$(\!|x, 2|\!) = (\!|\delta|\!) \Rightarrow \delta | 2,\ \delta | x$$

Επειδή $\delta | 2,\ \delta \in \{\pm 1, \pm 2\}$. Εάν $\delta = \pm 1$, τότε $1 \in (\!|\delta|\!) - (\!|x, 2|\!) = \emptyset$ (άτοπο). Εάν $\delta = \pm 2$, τότε $3x \in (\!|x, 2|\!) - (\!|\delta|\!) = \emptyset$ (και πάλι άτοπο).

□

v. *Η λύση αυτή έγινε με τη βοήθεια της φοιτήτριας 'Τσουτσουλοπούλου Ελευθερίας'.*

Λύση: Έστω R, Q δύο περιοχές κυρίων ιδεωδών και η αντίστοιχη περιοχή-πηλίκο ${}^{R}/_{Q}$. Εάν I είναι τυχόν ιδεώδες του ${}^{R}/_{Q}$, θα δείξουμε ότι το I είναι κύριο.

Θεωρούμε το σύνολο $J = \bigcup I = \bigcup_{s \in I} s$ και παρατηρούμε ότι αυτό είναι ιδεώδες του R, αφού:

- $\forall x, y \in J:\ x + Q - y + Q = x - y + Q \in I \Rightarrow x - y \in J$
- $\forall r \in R,\ x \in J : (r + Q)(x + Q) = rx + Q \in I \Rightarrow rx \in J$

Το R είναι περιοχή κυρίων ιδεωδών, επομένως υπάρχει $\rho \in R$ τέτοιο ώστε $J \in (\!|\rho|\!)$.

Ισχυριζόμαστε ότι $I = (\!|\rho + Q|\!)$. Πράγματι, κατ' αρχάς παρατηρούμε ότι $\rho \in J \Rightarrow \rho + Q \in I$. Επιπλέον, κάθε κλάση $r + Q$ στο I μπορεί να πάρει την ισοδύναμη μορφή $r + Q = k\rho + Q$ (για κάποιο $k \in R$), επομένως $I \subseteq (\!|\rho + Q|\!)$. Τα δύο προηγούμενα δίνουν το ζητούμενο, ότι δηλαδή $I = (\!|\rho + Q|\!)$.

Το I είναι λοιπόν κύριο ιδεώδες.

□

Άσκηση 6 Δείξτε ότι το $\mathbb{Z}-$πρότυπο $\mathbb{Q}/\mathbb{Z}$ δεν είναι πεπερασμένα παραγόμενο. ■

Λύση: Έστω προς άτοπο ότι το $\mathbb{Z}-$πρότυπο $\mathbb{Q}/\mathbb{Z}$ είναι πεπερασμένα παραγόμενο, και μάλιστα από το σύνολο $\left\{\frac{a_i}{b_i}+\mathbb{Z} \mid i\in[n]\right\}$.

Έστω $\mathcal{B}=\prod_{i\in[n]} b_i$. Θεωρούμε:

$$\mu=\min\left[\left(\mathcal{B}\left\{\frac{a_i}{b_i} \mid i\in[n]\right\}\right)\cap\mathbb{N}\right]$$

(Όλα αυτά εντός του πλαισίου δεν χρειάζονται στην απόδειξη - είναι για περαιτέρω κατανόηση της μορφής του μ.)

Ο φυσικός αριθμός μ είναι (ο μοναδικός θετικός) μέγιστος κοινός διαιρέτης των ακεραίων του $\mathcal{B}\left\{\frac{a_i}{b_i} \mid i\in[n]\right\}$. Αυτό διότι, εφαρμόζοντας διαδοχικά το **Λήμμα 4.1**, ο μέγιστος κοινός διαιρέτης των στοιχείων του $\mathcal{B}\left\{\frac{a_i}{b_i} \mid i\in[n]\right\}$ γράφεται ως γραμμικός συνδυασμός των ίδιων. Επειδή τα ±1 είναι αντιστρέψιμα στους ακεραίους, μπορεί να υπάρξει πάντοτε θετικός μέγιστος κοινός διαιρέτης δ. Παρατηρούμε ότι κάθε γραφή:

$$0<c=\sum_{k\in\mathcal{B}\left\{a_i/b_i \mid i\in[n]\right\}} kx_k,\ \text{για τα διάφορα } x_k\in\mathbb{Z}$$

διαιρείται από το δ, αφού καθένα από τα k διαιρείται από το δ. Κατ' επέκταση, $\delta|c\Rightarrow\delta\leq c$ και ο μέγιστος κοινός διαιρέτης δ ταυτίζεται του μ.

Θεωρούμε τώρα την κλάση $\frac{\mu}{2\mathcal{B}}+\mathbb{Z}$ και παρατηρούμε ότι αυτή δεν μπορεί να παραχθεί από το $\left\{\frac{a_i}{b_i}+\mathbb{Z} \mid i\in[n]\right\}$. Πράγματι, αν μπορούσε:

$$\frac{\mu}{2\mathcal{B}}=\sum_{k\in\left\{a_i/b_i \mid i\in[n]\right\}} kx_k\Rightarrow\mu=\sum_{k\in\left\{a_i/b_i \mid i\in[n]\right\}} 2[\mathcal{B}k]x_k$$

το μ θα ήταν πολλαπλάσιο του 2. Κατ' επέκταση:

$$\frac{\mu}{2}=\sum_{k\in\left\{a_i/b_i \mid i\in[n]\right\}} [\mathcal{B}k]x_k=\sum_{\mathcal{B}k\in\mathcal{B}\left\{a_i/b_i \mid i\in[n]\right\}} [\mathcal{B}k]x_k$$

το $0<\frac{\mu}{2}<\mu$ ανήκει στο σύνολο στο οποίο το μ είναι ελάχιστο. Αυτό είναι άτοπο, και το ζητούμενο αποδεικνύεται. □

Άσκηση 7 Έστω M,N δύο $R-$πρότυπα και $A\leq M,\ B\leq N$. Δείξτε ότι $A\oplus B\leq M\oplus N$ και επιπλέον:

$$M\oplus N/A\oplus B\simeq\left[M/A\right]\oplus\left[N/B\right]$$

■

Λύση: Αρχικά θα δείξουμε ότι $A\oplus B\leq M\oplus N$. Προφανώς, ο πολλαπλασιασμός εδώ θα οριστεί με τον φυσικό τρόπο, κατά συντεταγμένες: $(a,b)(c,d)=(ac,bd)$.

- Η $A\oplus B$ είναι υποομάδα της $M\oplus N$, αφού:

  $$\forall(a,b),\ (c,d)\in A\oplus B:\ (a,b)-(c,d)=(a-c,\ b-d)\in A\oplus B$$

  όπου το τελευταίο 'ανήκειν' προκύπτει από το γεγονός ότι τα A,B είναι ομάδες.

- Για κάθε $(a,b)\in A\oplus B$ και για κάθε $(r,r')\in M\oplus N$, το στοιχείο $(r,r')(a,b)$ ανήκει στο $A\oplus B$:

  $$(r,r')(a,b)=(ra,r'b)\in A\oplus B,\ \text{αφού τα } A,B \text{ είναι υποπρότυπα των } M,N$$

Έχουμε λοιπόν δείξει ότι το $A\oplus B$ είναι υποπρότυπο του $M\oplus N$.

Στην συνέχεια θα δείξουμε τον ισομορφισμό των προτύπων ως $R \oplus R-$πρότυπα, αλλά η διαδικασία για να δείξει κανείς ότι τα πρότυπα είναι ισόμορφα και ως $R-$πρότυπα είναι εντελώς ανάλογη.

Θεωρούμε φ τον ομομορφισμό $\varphi : M \oplus N \to \left[M/A\right] \oplus \left[N/B\right]$ που ορίζεται ως:

$$\varphi : \varphi(x, y) = (x + A,\ y + B)$$

Η φ είναι πράγματι ομομορφισμός, αφού:

- Για $(x, y),\ (z, w) \in M \oplus N$: $\varphi\big((x, y) + (z, w)\big) = \varphi(x + z, y + w) = (x + z + A, y + w + B) = (x + A, y + B) + (z + A, y + B) = \varphi(x, y) + \varphi(z, w)$
- Για $(r, s) \in R \oplus R,\ (x, y) \in M \oplus N$: $\varphi\big((r, s) \cdot (x, y)\big) = \varphi(rx + sy) = (rx + A, sy + B) = (r, s) \cdot (x + A, y + B) = (r, s) \cdot \varphi(x, y)$

Ο πυρήνας $\ker \psi$ είναι ακριβώς το σύνολο $A \oplus B$, αφού $(x, y) \in \ker \psi \Leftrightarrow (x + A, y + B) = (0, 0) \Leftrightarrow x \in A,\ y \in B \Leftrightarrow (x, y) \in A \oplus B$.

Η φ είναι επί, αφού για κάθε $(s, t) \in \left[M/A\right] \oplus \left[N/B\right]$, εάν x και y είναι αντιπρόσωποι των s και t αντίστοιχα, τότε $\varphi(x, y) = (s, t)$.

Από το $1^{\text{ο}}$ θεώρημα ισομορφισμών έπεται το ζητούμενο:

$$M \oplus N \Big/ \ker \varphi \simeq \operatorname{Im} \varphi \Rightarrow\ M \oplus N \Big/ A \oplus B \simeq \left[M \Big/ A\right] \oplus \left[N \Big/ B\right]$$

□

Άσκηση 8 Ένα μη μηδενικό $R-$πρότυπο M λέγεται *απλό* εάν τα μόνα του υποπρότυπα είναι το $\{0\}$ και το M.

i. Δείξτε ότι κάθε απλό πρότυπο είναι κυκλικό.

ii. Δείξτε ότι τα απλά $\mathbb{Z}-$πρότυπα είναι ως προς τον ισομορφισμό τα $\mathbb{Z}_p$, όπου p πρώτος. Δώστε παράδειγμα κυκλικού προτύπου που δεν είναι απλό.

iii. Αληθεύει ότι ο δακτύλιος $\mathbb{Q}[x]$ έχει απλό $\mathbb{Q}[x]-$υποπρότυπο;

iv. Αν το M είναι απλό $R-$πρότυπο, τότε κάθε μη μηδενικός ομομορφισμός προτύπων $f : M \to M$ είναι ισομορφισμός.

■

i. *Λύση:* Έστω M ένα απλό $R-$πρότυπο. Θα δείξουμε ότι για οποιοδήποτε $m \in M$, το M ισοδύναμα μπορεί να γραφεί ως $R \cdot m$. Κατ' επέκταση, $M = (\!|m|\!)$, αφού $R \cdot m = (\!|m|\!)$.

Έστω $m \in M$. Το σύνολο $R \cdot m$ είναι υποπρότυπο του M, αφού (συνοπτικά):

- Για κάθε $am, bm \in R \cdot m : am - bm = (a - b)m \in R \cdot m$ (αφού το M είναι πρότυπο).
- Για κάθε $am \in R \cdot m,\ c \in R : cam = (ca)m \in R \cdot m$ (αφού το M είναι πρότυπο).

Επειδή το M είναι απλό πρότυπο, $R \cdot m = M$, και το ζητούμενο αποδεικνύεται.

□

ii. **Λήμμα 8.1:** *Έστω G, H δύο ισόμορφα $R-$πρότυπα. Εάν A είναι ένα υποπρότυπο του G, υπάρχει B υποπρότυπο του H, ισόμορφο του A.*

Απόδειξη: Εφόσον τα πρότυπα G, H είναι ισόμορφα, υπάρχει ισομορφισμός $\varphi : G \to H$. Θα αποδείξουμε επιπλέον ότι αν $\{\mathbf{0}_G\} \neq A \neq G$, το $\varphi(A)$ είναι υποπρότυπο του H, το οποίο δεν είναι κανένα από τα $\{\mathbf{0}_H\},\ H$. Το τελευταίο δεν χρειάζεται πουθενά στην απόδειξη, θα χρειαστεί όμως στις ασκήσεις. Οπότε το αποδεικνύουμε.

Το $\varphi(A)$ είναι ισόμορφο του A υποπρότυπο, αφού η $\varphi|_A : A \to \varphi(A)$ είναι ισομορφισμός και επιπλέον:

- Για κάθε $b, \tilde{b} \in \varphi(A)$, υπάρχουν $a, \tilde{a} \in A$ τέτοια ώστε $\varphi(a) = b,\ \varphi(\tilde{a}) = \tilde{b}$. Επομένως, $b - \tilde{b} = \varphi(a) - \varphi(\tilde{a}) = \varphi(a - \tilde{a}) \in \varphi(A)$, αφού $a - \tilde{a} \in A$ (το A είναι πρότυπο, άρα και ομάδα).
- Για κάθε $b = \varphi(a) \in \varphi(A)$ και $r \in R$, ισχύει ότι $rb = r\varphi(a) = \varphi(ra) \in \varphi(A)$, αφού $ra \in A$ (το A είναι πρότυπο).

Το $\varphi(A)$ δεν είναι κανένα από τα $\{\mathbf{0}_H\},\ H$, μιας και αν το αντίθετο συνέβαινε, $A = \varphi^{-1}(\{\mathbf{0}_H\}) = \{\mathbf{0}_G\}$ (άτοπο) και αντίστοιχα $\varphi^{-1}(H) = G$ (και πάλι άτοπο).

△

Λύση: Για κάθε $m \in M$ θεωρούμε την απεικόνιση $\varphi_m : \mathbb{Z} \to (\!|m|\!)$ που ορίζεται ως:

$$\varphi_m : x \mapsto xm$$

Από το 1ο θεώρημα ισομορφισμών έχουμε ότι:

$$\mathbb{Z}\Big/_{\ker \varphi_m} \simeq (\!|m|\!)$$

και από το **Λήμμα 8.1**, αρκεί να μελετηθούν τα απλά υποπρότυπα της μορφής $\mathbb{Z}/_{\ker \varphi_m}$ για να προσδιοριστούν τα απλά υποπρότυπα του M.

Επειδή η περιοχή $\mathbb{Z}$ είναι περιοχή κυρίων ιδεωδών, για κάθε συνάρτηση φ_m, υπάρχει $n_m \in \mathbb{Z}$ τέτοιο ώστε $\ker \varphi_m = (\!|n_m|\!)$. Κατ' επέκταση:

$$\mathbb{Z}\Big/_{\ker \varphi_m} = \mathbb{Z}_{n_m}$$

Ισχυριζόμαστε ότι το υποπρότυπο $\mathbb{Z}_{n_m}$ είναι απλό εάν και μόνο αν ο αριθμός n_m είναι πρώτος. Πράγματι, εάν το $\mathbb{Z}_{n_m}$ είναι απλό, για κάθε $x + \mathbb{Z} \cdot n_m \in \mathbb{Z}_{n_m}$:

$$\mathbb{Z}_{n_m} \cdot (1 + \mathbb{Z} \cdot n_m) = \mathbb{Z}_{n_m} \cdot (x + \mathbb{Z} \cdot n_m) \Leftrightarrow 1 + \mathbb{Z} \cdot n_m = (y + \mathbb{Z} \cdot n_m)(x + \mathbb{Z} \cdot n_m),\ \text{για κάποιο } y + \mathbb{Z} \cdot n_m \in \mathbb{Z}_{n_m}$$

Αυτό ουσιαστικά δείχνει ότι κάθε στοιχείο του υποπροτύπου $\mathbb{Z}_{n_m}$ έχει αντίστροφο, δηλαδή το $\mathbb{Z}_{n_m}$ είναι σώμα. Έπεται πλέον ότι ο αριθμός n_m είναι πρώτος, κι επειδή όλες οι ισοδυναμίες που χρησιμοποιήσαμε αντιστρέφονται, ο ισχυρισμός αποδεικνύεται.

Συνεπώς κάθε απλό $\mathbb{Z}-$υποπρότυπο του M είναι ισόμορφο με κάποιο $\mathbb{Z}_p$, όπου p πρώτος.

Ένα παράδειγμα ενός κυκλικού προτύπου που δεν είναι απλό είναι το $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. Είναι πράγματι πρότυπο, αφού είναι αβελιανή ομάδα κλειστή ως προς τον εξωτερικό $\mathbb{Z}-$πολλαπλασιασμό, και είναι πράγματι κυκλική αφού $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = (\!|(1,1)|\!) = (\!|(1,2)|\!)$. Το $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ δεν είναι απλό, αφού το $\mathbb{Z}_2 \oplus \{0\}$ είναι πρότυπο ($\mathbb{Z}_2 \oplus \{0\} \simeq \mathbb{Z}_2$) και μάλιστα υποπρότυπο του $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

□

iii. *Λύση 1η:* Προς άτοπο υποθέτουμε ότι υπάρχει απλό υποπρότυπο N του $\mathbb{Q}[x]$. Θα δείξουμε ότι το $N \cdot x$ είναι υποτρότυπο του N, και κατ' επέκταση $N \cdot x = N$, αφού το N είναι απλό. Πράγματι:

- Έστω $\tilde{n}, \tilde{\nu}$ δύο στοιχεία του $N \cdot x$. Εξ' ορισμού του $N \cdot x$, υπάρχουν $n, \nu \in N$ τέτοια ώστε $\tilde{n} = nx,\ \tilde{\nu} = \nu x$. Επομένως, $\tilde{n} - \tilde{\nu} = nx - \nu x = (n - \nu)x \in N \cdot x$, αφού $n - \nu \in N$ (το N είναι υποπρότυπο).
- Έστω $\tilde{n} \in N,\ h \in \mathbb{Q}[x]$. Και πάλι είναι δυνατόν να βρεθεί $n \in N$ τέτοιο ώστε $\tilde{n} = nx$, εξ' ορισμού του N. Επομένως, $h \cdot \tilde{n} = h \cdot nx = (h \cdot n)x \in N \cdot x$, αφού $h \cdot n \in N$ (το N είναι υποπρότυπο).

Οπότε το $N \cdot x$ είναι υποπρότυπο του N.

Θεωρούμε $\tilde{\eta} \in N$ ένα μη μηδενικό πολυώνυμο με ελάχιστο βαθμό. Εφόσον $N = N \cdot x$, το $\tilde{\eta}$ ανήκει στο $N \cdot x$, κι άρα γράφεται στην μορφή $\eta \cdot x$, για κάποιο μη μηδενικό $\eta \in N$. Επειδή όμως $\deg \eta < \deg \tilde{\eta}$, το $\tilde{\eta}$ δεν είναι στοιχείο ελαχίστου βαθμού στο N. Αυτό είναι άτοπο, και συνεπώς αποδεικνύεται ότι δεν υπάρχουν απλά υποπρότυπα του $\mathbb{Q}[x]$.

□

Λύση 2η - γιατί δεν είχα πειστεί με το πρώτο αποτέλεσμα: Υποθέτουμε προς άτοπο ότι υπάρχει απλό υποπρότυπο N του $\mathbb{Q}[x]$. Σύμφωνα με την απόδειξη του υποερωτήματος i., εάν n είναι ένα στοιχείο του N, τότε $N = \mathbb{Q}[x] \cdot n$. Εφόσον $N = \mathbb{Q}[x] \cdot n$ μπορούμε να θεωρήσουμε $qn,\ q \in \mathbb{Q}[x]$ ένα οποιοδήποτε στοιχείο του N, και ισοδύναμα να παραστήσουμε το N ως $N = \mathbb{Q}[x] \cdot (qn)$. Επειδή $n \in N = \mathbb{Q}[x] \cdot (qn)$, υπάρχει $g \in \mathbb{Q}[x]$ τέτοιο ώστε $gqn = n \Rightarrow gq = 1 \Rightarrow q \in U(\mathbb{Q}[x])$. Αυτό ουσιαστικά μας δείχνει ότι κάθε (μη μηδενικό) στοιχείο qn του συνόλου N γράφεται στην μορφή $qn,\ q \in U(\mathbb{Q}[x])$, κι επομένως $N = U(\mathbb{Q}[x]) \cdot n \cup \{0\}$. Αυτό είναι άτοπο, αφού $U(\mathbb{Q}[x]) \neq \mathbb{Q}[x] - \{0\}$.

□

iv *Λύση:* Έστω $f : M \to M$ ένας ομομορφισμός προτύπων. Ο πυρήνας $\ker f$ είναι υποπρότυπο του M, αφού:

- $0 \in \ker f$
- Για κάθε $a, b \in \ker f$: $f(a - b) = f(a) - f(b) = 0 \Rightarrow a - b \in \ker f$

- Για κάθε $a \in \ker f,\ r \in M$: $f(ra) = rf(a) = 0 \Rightarrow ra \in \ker f$

Εφόσον το M είναι απλό πρότυπο, $\ker f = \{0\}$ ή $\ker f = M$. Η δεύτερη περίπτωση δεν μπορεί να ισχύει, αφού ο ομομορφισμός υποτέθηκε μη μηδενικός, επομένως η πρώτη αληθεύει. Σε αυτήν την περίπτωση, η f είναι $1-1$.

Από το 1ο θεώρημα ισομορφισμών έχουμε ότι $M/_{\{0\}} \simeq f(M)$, κι επειδή $M/_{\{0\}} \simeq M$ (μέσω του τετριμμένου ισομορφισμού $x + \{0\} \mapsto x$), θα πρέπει $M \simeq f(M)$. Επειδή $M \leq M$ και $M \simeq f(M)$, από το **Λήμμα 8.1**, το $f(M)$ είναι υποπρότυπο του M. Επειδή το M είναι απλό και η f μη μηδενική, $f(M) = M$. Ισοδύναμα, η f είναι επί του M.

Με αυτά έχουμε δείξει ότι η f είναι ισομορφισμός $M \to M$.

□

Άσκηση 9 Έστω M, N δύο $R-$πρότυπα τέτοια ώστε $\mathrm{Ann}_R M + \mathrm{Ann}_R N = R$. Δείξτε ότι κάθε ομομορφισμός προτύπων $M \to N$ είναι ο μηδενικός. ■

Λύση: Εφόσον $\mathrm{Ann}_R M + \mathrm{Ann}_R N = R$, υπάρχουν $s \in \mathrm{Ann}_R M,\ t \in \mathrm{Ann}_R N$ τέτοια ώστε $\mathbf{1}_R = s + t$. Έστω τώρα $\varphi : M \to N$ ένας τυχαίος ομομορφισμός. Για κάθε $x \in M$ παρατηρούμε ότι:

$$\varphi(x) = \varphi(\mathbf{1}_R x) = \varphi(sx + tx) = \varphi(sx) + t\varphi(x)$$

Επειδή $x \in M$, $sx = \mathbf{0}_R$ και επειδή $\varphi(x) \in N$, $t\varphi(x) = \mathbf{0}_R$. Κατ' επέκταση, $\varphi(x) = \mathbf{0}_R \Rightarrow \varphi = \mathbf{0}_{(M \to N)}$.

□

Άσκηση 10 Έστω $\mathbb{K}$ ένα σώμα και V ένας $\mathbb{K}-$διανυσματικός χώρος με $\dim V < \infty$.

i. Εάν $U \leq V$, δείξτε ότι:
$$\dim\left[V/_U\right] = \dim V - \dim U$$

ii. Αν $U, W \leq V$, δείξτε (χρησιμοποιώντας το 2ο θεώρημα ισομορφισμών προτύπων) ότι:
$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

■

i. *Λύση:* Εφόσον το U είναι υποπρότυπο του διανυσματικού χώρου V, είναι ακριβώς ένας $\mathbb{K}-$υπόχωρος του V. Μάλιστα έχει πεπερασμένη διάσταση, αφού ο V έχει πεπερασμένη διάσταση. Έστω λοιπόν $\vec{u} = (u_1, \cdots, u_n)$ μια διατεταγμένη βάση του U. Η βάση $\vec{u}$ του U μπορεί να επεκταθεί κατάλληλα σε βάση $\vec{v}$ του V, η οποία θα έχει την μορφή $\vec{v} = (u_1, \cdots, u_n, v_1, \cdots, v_m)$. Παρατηρούμε ότι κάθε στοιχείο $x + U \in V/_U$ γράφεται στην μορφή:

$$x + U = \sum_{i\in[n]} (k_i \cdot u_i) + \sum_{i\in[m]} (h_i \cdot v_i) + U = \sum_{i\in[m]} (h_i \cdot v_i) + U,\ k_i, h_i \in \mathbb{K}$$

κι επομένως τα στοιχεία $v_i + U,\ i \in [m]$ παράγουν τον χώρο πηλίκο. Ισχυριζόμαστε ότι είναι επιπλέον γραμμικώς ανεξάρτητα. Πράγματι:

$$\sum_{i\in[m]} (h_i \cdot v_i + U) = 0 \Rightarrow \sum_{i\in[m]} h_i \cdot v_i + U = 0 \Rightarrow \sum_{i\in[m]} h_i \cdot v_i = \sum_{j\in[n]} k_j \cdot u_j \Rightarrow \sum_{i\in[m]} h_i \cdot v_i + \sum_{j\in[n]} (-k_j) \cdot u_j = 0$$

Επειδή η $\vec{v}$ είναι βάση, τα στοιχεία της είναι γραμμικώς ανεξάρτητα και κατ' επέκταση $h_i = -k_j = 0$ για κάθε $i \in [m],\ j \in [n]$. Από αυτό έπεται η γραμμική ανεξαρτησία των $v_i + U$. Ακόμη, όλα τα στοιχεία της μορφής $v_i + U$ απαιτούνται για να παραχθεί ο χώρος πηλίκο (αφού όλα τους ανήκουν στον χώρο και είναι ανά δύο διαφορετικά), κι επομένως η $\vec{n} = (v_1, \cdots, v_m)$ αποτελεί μια βάση του χώρου πηλίκο.

Έπεται πλέον ότι:
$$\dim\left[V/_U\right] = m = (n + m) - n = \dim V - \dim U$$

□

ii. *Λύση:* Σύμφωνα με το 2ο θεώρημα ισομορφισμών προτύπων:

$$U + W/_W \simeq U/_{U \cap W}$$

Επειδή ο V είναι διανυσματικός χώρος, τα U και W είναι υπόχωροι του V, και μάλιστα πεπερασμένης διάστασης (αφού ο V είναι πεπερασμένης διάστασης). Επομένως το αποτέλεσμα του ερωτήματος i. αληθεύει:

$$\dim(U+W) - \dim W = \dim\left[{U+W}\Big/{W}\right] = \dim\left[{U}\Big/{U\cap W}\right] = \dim U - \dim(U\cap W)$$

και άρα:

$$\dim(U+W) = \dim U + \dim W - \dim(U\cap W)$$

□

Άσκηση 11 Έστω V ένας $\mathbb{R}-$διανυσματικός χώρος με διατεταγμένη βάση $\vec{\beta} = (v_1, v_2, v_3)$ και $\alpha : V \to V$ γραμμική απεικόνιση με πίνακα A ως προς την πορηγούμενη βάση:

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

Να βρεθούν όλα τα $\mathbb{R}[x]-$υποπρότυπα του V. ■

Λύση: Θα μελετηθούν ουσιαστικά οι $\alpha-$αναλλοίωτοι υπόχωροι U του V (εννοείται ως προς τη βάση).

Γνωρίζουμε ότι ένας υπόχωρος U της μορφής $(\!|u|\!)$ είναι $\alpha-$αναλλοίωτος εάν και μόνο αν το u είναι ιδιοδιάνυσμα του α. Προσωρινά λοιπόν η μελέτη θα περιοριστεί στην εύρεση των ιδιοδιανυσμάτων του A.

Το χαρακτηριστικό πολυώνυμο του A είναι ακριβώς το:

$$\mathcal{X}_A(\lambda) = (\lambda-2)^2(\lambda-1)^2$$

επομένως οι ιδιοτιμές του A είναι οι $1, 2$.

Για $\lambda = 1$, τα ιδιοδιανύσματα $v = (x, y, z)$ είναι τα:

$$Av = v \Rightarrow \begin{pmatrix} 2x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \Rightarrow v = \begin{pmatrix} 0 \\ y \\ z \end{pmatrix}$$

Για $\lambda = 2$, τα ιδιοδιανύσματα $v = (x, y, z)$ είναι τα:

$$Av = 2v \Rightarrow \begin{pmatrix} 2x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x \\ 2y \\ 2z \end{pmatrix} \Rightarrow v = \begin{pmatrix} x \\ 0 \\ 0 \end{pmatrix}$$

Έστω G ένα σύνολο ιδιοδιανυσμάτων του A. Παρατηρούμε ότι ο χώρος $(\!|G|\!)$ είναι $\alpha-$αναλλοίωτος, αφού η α είναι γραμμική. Επειδή τα ιδιοδιανύσματα του A παράγουν κάθε υπόχωρο του V, κάθε υπόχωρος του V είναι $\alpha-$αναλλοίωτος.

Ουσιαστικά η απόδειξη σε αυτό το σημείο τελειώνει, αφού κάθε $\alpha-$αναλλοίωτος υπόχωρος U είναι υπόχωρος του V.

≈ □

Άσκηση 12 Έστω $\mathbb{K}$ σώμα. Θεωρούμε τον δακτύλιο $R = M_{2\times 2}(\mathbb{K})$ και το $R-$πρότυπο $V = M_{2\times 1}(\mathbb{K}) = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \,\middle|\, x, y \in \mathbb{K} \right\}$. Εδώ ο εξωτερικός πολλαπλασιασμός ορίζεται ως $R \times V \ni (A, X) \mapsto AX \in V$. Δείξτε τα εξής:

i. Ως $R-$πρότυπο, το V είναι απλό.

ii. Ως $R-$πρότυπα, $R \simeq V \oplus V$.

iii. Από το ερώτημα i., το V παράγεται από το $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Δείξτε ότι $\mathrm{Ann}_R(V) \neq \mathrm{Ann}_R(v)$.

iv. Δείξτε ότι κάθε απλό $R-$πρότυπο είναι ισόμορφο με το V.

Λήμμα 12.1: *Εάν ένα πρότυπο R είναι διαιρετικός δακτύλιος, τότε κάθε κυκλικό $R-$πρότυπο είναι απλό.*

Απόδειξη: Έστω ότι το R είναι διαιρετικός δακτύλιος, και κατ' επέκτασην ότι $R = U(R) \cup \{0\}$. Έστω επίσης $M = R \cdot m$ ένα κυκλικό $R-$πρότυπο και S ένα (μη μηδενικό) υποπρότυπο του M. Εφόσον $S \leq M$, θα πρέπει για κάθε στοιχείο $s \in S$ να ισχύει $s \in M \Rightarrow s = t \cdot m$, για αντίστοιχα $t \in R - \{0\}$. Επειδή το R είναι διαιρετικός δακτύλιος, υπάρχει ο αντίστροφος του t και συνεπώς $m = t^{-1} \cdot s \Rightarrow m \in S$. Εφόσον $m \in S$, το S υποπρότυπο και το M κυκλικό, $M \subseteq S$. Ο άλλος εγκλεισμός είναι προφανής, οπότε ουσιαστικά έχουμε δείξει ότι $M = S$. Κάθε λοιπόν υποπρότυπο του M είναι είτε το $\{0\}$ είτε το M, κι άρα το M είναι απλό.

△

i. *Λύση:* (Συνοπτικά) Ορίζουμε μια σχέση ισοδυναμιας ($\sim$) στο R τέτοια ώστε:

- Για κάθε $x \in R$ τέτοιο ώστε $\det x \neq 0$, $[x/\sim] = \{x\}$
- $\left[\mathbf{0}_{2\times 2}/\sim\right] = \{x \mid \det x = 0\}$

και παρατηρούμε ότι εξ' ορισμού ο $R/\sim$ καθίσταται διαιρετικός δακτύλιος.

Το V είναι κυκλικό $R/\sim-$πρότυπο και μάλιστα παράγεται από το $v = \begin{pmatrix}1\\0\end{pmatrix}$. Σύμφωνα με το **Λήμμα 12.1**, το V είναι απλό.

Το V ως $R-$πρότυπο είναι απλό. Πράγματι, έστω S ένα $R-$υποπρότυπο του V. Το S (όπως και το V) ορίζει $R/\sim-$πρότυπο S, το οποίο είναι υποπρότυπο του V:

- $\begin{pmatrix}a\\b\end{pmatrix} - \begin{pmatrix}c\\d\end{pmatrix} = \begin{pmatrix}a-c\\b-d\end{pmatrix}$
- Εάν $\det \begin{pmatrix}a & b\\c & d\end{pmatrix} \neq 0$, τότε $\left[\begin{pmatrix}a & b\\c & d\end{pmatrix} \Big/ \sim\right] \cdot \begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}a & b\\c & d\end{pmatrix} \cdot \begin{pmatrix}x\\y\end{pmatrix}$
- Εάν $\det \begin{pmatrix}a & b\\c & d\end{pmatrix} = 0$, τότε $\left[\begin{pmatrix}a & b\\c & d\end{pmatrix} \Big/ \sim\right] \cdot \begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$

Επειδή το τελευταίο είναι απλό, $S = \{0\}$ ή $S = V$. Αυτή είναι ισότητα μεταξύ συνόλων (πλέον), επομένως δείχνεται έτσι ότι το V είναι απλό ως $R-$πρότυπο.

≈ □

ii. *Λύση:* (Συνοπτικά) Η συνάρτηση:

$$\begin{pmatrix}a & b\\c & d\end{pmatrix} \mapsto \left(\begin{pmatrix}a\\c\end{pmatrix}, \begin{pmatrix}b\\d\end{pmatrix}\right)$$

είναι ισομορφισμός, εάν ο πολλαπλασιασμός στο $V \oplus V$ οριστεί ως:

$$(x, y) \cdot (z, w) = \big((x, y)z, (x, y)w\big)$$

≈ □

iii. *Λύση:* (Συνοπτικά) $\mathrm{Ann}_R(V) = \{0\}$ ενώ $\mathrm{Ann}_R(v) \supset \left\{\begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}\right\}$.

≈ □

iv. *Λύση:* (Συνοπτικά) Εφόσον το V είναι απλό $R-$πρότυπο, θα γράφεται στην μορφή $R \cdot m$, για $m \in V$. Έστω S ένα άλλο απλό $R-$πρότυπο, το οποίο γράφεται στην μορφή $R \cdot s$, για $s \in S$. Η συνάρτηση:

$$xm \mapsto xs,\ x \in R$$

είναι ισομορφισμός.

≈ □