Φυλλάδιο Γ

Γ1. $S = \{ a + b\sqrt[3]{2} \in \mathbb{R} \mid a, b \in \mathbb{Z} \} \subseteq \mathbb{R}$.

Ισχύει $0 = 0 + 0\sqrt[3]{2} \in S$. Έστω $x, y \in S$.

Τότε $x = a + b\sqrt[3]{2}$, $y = c + d\sqrt[3]{2}$, με $a, b, c, d \in \mathbb{Z}$

- $x - y = \underbrace{(a-c)}_{\in \mathbb{Z}} + \underbrace{(b-d)}_{\in \mathbb{Z}}\sqrt[3]{2} \in S$.

- $xy = (a + b\sqrt[3]{2})(c + d\sqrt[3]{2}) = ac + ad\sqrt[3]{2} + bc\sqrt[3]{2} + bd\sqrt[3]{4}$

$= (ac + bd\sqrt[3]{4}) + (ad + bc)\sqrt[3]{2}$. Ενώ ισχύει $ad + bc \in \mathbb{Z}$, δεν ισχύει $ac + bd\sqrt[3]{4} \in \mathbb{Z}$, εκτός αν $bd = 0$. Πράγματι, αν $bd \neq 0$ και $ac + bd\sqrt[3]{4} = k \in \mathbb{Z}$, τότε:

$\sqrt[3]{4} = \frac{k - ac}{bd} \in \mathbb{Q}$, άτοπο.

Άρα S: όχι υποδακτύλιος του $\mathbb{R}$. ∎

Γ2. Έστω $(r,s) \in U(R\times S)$. Τότε, υπάρχει $(x,y) \in R\times S$ (άρα $x\in R$ και $y\in S$) έτσι ώστε

$$(r,s)\cdot(x,y) = 1_{R\times S} = (x,y)\cdot(r,s), \text{ άρα:}$$

$$(rx, sy) = (1_R, 1_S) = (xr, ys) \Longrightarrow \begin{cases} rx = 1_R = xr \\ sy = 1_S = ys \end{cases}$$

που σημαίνει ότι το $r\in R$ είναι αντιστρέψιμο με $r^{-1} = x$ και το $s\in S$ είναι αντιστρέψιμο με $s^{-1} = y$, οπότε $r\in U(R)$ και $s\in U(S)$, δηλαδή $(r,s)\in U(R)\times U(S)$. Επομένως έχουμε $U(R\times S) \subseteq U(R)\times U(S)$ (i).

Αντίστροφα, έστω $(r,s)\in U(R)\times U(S)$. Τότε $r\in U(R)$ και $s\in U(S)$, δηλαδή: $\begin{cases} rr^{-1} = 1_R = r^{-1}r \\ ss^{-1} = 1_S = s^{-1}s \end{cases}$

Έτσι, $(r^{-1}, s^{-1}) \in R\times S$ και

$$(r,s)(r^{-1},s^{-1}) = (rr^{-1}, ss^{-1}) = (1_R, 1_S) = 1_{R\times S}$$

$$(r^{-1},s^{-1})\cdot(r,s) = (r^{-1}r, s^{-1}s) = (1_R, 1_S) = 1_{R\times S}.$$

Αυτό σημαίνει ότι $(r,s) \in U(R\times S)$. Ώστε,
$U(R)\times U(S) \subseteq U(R\times S)$ (ii).

Από (i), (ii) προκύπτει: $U(R\times S) = U(R)\times U(S)$.

• Εφαρμογή για $R = \mathbb{Z}_5$ και $S = \mathbb{Z}_3$.

Εφ' όσον $3, 5$: πρώτοι αριθμοί έπεται
$R = \mathbb{Z}_5$: σώμα και $S = \mathbb{Z}_3$: σώμα,

άρα: $U(\mathbb{Z}_5) = \mathbb{Z}_5^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$

$U(\mathbb{Z}_3) = \mathbb{Z}_3^* = \{[1]_3, [2]_3\}$

<u>Συνεπώς</u>: $U(\mathbb{Z}_5\times\mathbb{Z}_3) = U(\mathbb{Z}_5)\times U(\mathbb{Z}_3) =$

$$= \left\{\begin{matrix} ([1]_5,[1]_3), ([1]_5,[2]_3), ([2]_5,[1]_3), ([2]_5,[2]_3), \\ ([3]_5,[1]_3), ([3]_5,[2]_3), ([4]_5,[1]_3), ([4]_5,[2]_3) \end{matrix}\right\}$$

■

Γ3. Γνωρίζουμε ότι $ab = 1_R$ (*) και θα αποδείξουμε ότι $ba = 1_R$. Έστω $ba = x$.

Τότε: $(ba)b = xb \Rightarrow b(ab) = xb \xRightarrow{(*)}$

$b \cdot 1_R = xb \Longrightarrow 1_R \cdot b = x \cdot b$ (**). Αν $b = 0_R$

τότε λόγω (*): $a \cdot 0_R = 1_R \Rightarrow 0_R = 1_R$, άτοπο.

Άρα $b \neq 0_R$. Ο R δεν έχει διαιρέτες του μηδενός, δηλαδή R: περιοχή. Σε κάθε περιοχή ισχύουν οι νόμοι διαγραφής, οπότε:

(**): $1_R \cdot b = x \cdot b \xRightarrow{b \neq 0_R} 1_R = x \Rightarrow \boxed{1_R = ba}$,

όπως θέλαμε. ∎

Γ4. (i) Έστω $f: \mathbb{Z} \to \mathbb{Z}_4$ με $f(x) = [x]_4$.

Ο f είναι (επι)μορφισμός δακτυλίων.

Ο $\mathbb{Z}$ είναι ακέραια περιοχή ενώ ο $\mathbb{Z}_4$: όχι ακέραια περιοχή. (4: σύνθετος)

(ii) Έστω $f: R \to S$ ισομορφισμός δακτυλίων και έστω R: περιοχή. Θα αποδείξουμε ότι και ο S είναι περιοχή. Έστω λοιπόν $x, y \in S$ με $xy = 0_S$ και θα αποδείξουμε ότι $x = 0_S$ ή $y = 0_S$. Πράγματι,

- $x \in S \xRightarrow[\text{του } S]{f:\text{ επί}} \exists\, a \in R,\ f(a) = x$
- $y \in S \xRightarrow[\text{του } S]{f:\text{ επί}} \exists\, b \in R,\ f(b) = y$

Άρα, $xy = 0_S \Rightarrow f(a)f(b) = 0_S \xRightarrow[\text{μορφισμός}]{f:}$

$f(ab) = f(0_R) \xRightarrow[1-1]{f:} ab = 0_R \xRightarrow[\text{περιοχή}]{R:}$

$a = 0_R$ ή $b = 0_R$. Αν $a = 0_R$ τότε $x = f(a) = f(0_R) = 0_S$. Αν $b = 0_R$ τότε $y = f(b) = f(0_R) = 0_S$. $\underline{\underline{\text{ΑΡΑ}}}$: $x = 0_S$ ή $y = 0_S$, όπως θέλαμε. ∎

Γ5. Θέτουμε $R = M_2(\mathbb{R})$

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in R \;\middle|\; a \in \mathbb{R} \right\} \subseteq R.$$

Όπως γνωρίζουμε ο R δεν είναι σώμα (πχ. R: όχι μεταθετικός).

▶ S: υποδακτύλιος του R:

· $\mathbb{O} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$. Επίσης, αν $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in S$

και $B = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \in S$ τότε:

$A - B = \begin{bmatrix} a-b & 0 \\ 0 & a-b \end{bmatrix} \in S$ και $AB = \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix} \in S$

· Τέλος, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$.

Συνεπώς, ο S είναι υποδακτύλιος του R με $1_S = I_2 = 1_R$.

▶ S: μεταθετικός: Για κάθε $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in S$

και κάθε $B = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} \in S$ έχουμε:

$$AB = \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix}$$

$$BA = \begin{bmatrix} ba & 0 \\ 0 & ba \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix} = AB \quad \checkmark$$

▶ S: σώμα: Θα αποδείξουμε $U(S) = S^*$, δηλαδή ότι κάθε μη-μηδενικός πίνακας του S αντιστρέφεται.

Έστω $A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in S$ με $A \neq \mathbb{0}$. Τότε:

$a \neq 0$ και $\det(A) = a^2 \neq 0$, οπότε

υπάρχει ο $A^{-1} = \dfrac{1}{\det(A)} \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} \frac{a}{a^2} & \frac{0}{a^2} \\ \frac{0}{a^2} & \frac{a}{a^2} \end{bmatrix}$

$\Longrightarrow A^{-1} = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{a} \end{bmatrix}$ με $A^{-1} \in S$ και

$AA^{-1} = I_2 = A^{-1}A$, άρα $A \in U(S)$ ∎

Γ6. (i) Ο $\mathbb{Z}[i]$ δεν είναι σώμα διότι (Θεωρία) έχουμε δείξει ότι:

$$U(\mathbb{Z}[i]) = \{-i, i, -1, 1\} \neq \mathbb{Z}[i]^*$$

(ii) Ο $\mathbb{Q} \times \mathbb{Q}$ δεν είναι σώμα: Γενικά, έχουμε δείξει ότι το ευθύ γινόμενο $R \times S$ δύο δακτυλίων R και S δεν είναι περιοχή (τα $(0_R, 1_S)$, $(1_R, 0_S)$ είναι διαιρέτες του μηδενός) οπότε ούτε σώμα.

(iii) Θεωρία: $\mathbb{Z}_n$: σώμα $\Longleftrightarrow$ n: πρώτος

Άρα, $\mathbb{Z}_{13}$: σώμα.

Γ7. (i) Έστω $f: \mathbb{Z} \to \mathbb{Z}$ μορφισμός δακτυλίων. Ισχύει ότι $f(1) = 1$.

• $\forall n \in \mathbb{N}$: $f(n) = f(\underbrace{1+1+\dots+1}_{n\text{-φορές}}) \overset{f:\ \text{μορφισμός}}{=}$

$$\underbrace{f(1)+f(1)+\dots+f(1)}_{n\text{-φορές}} = n \cdot f(1) = n$$

• <u>Ισχύει</u>: $f(-1)+f(1) \xlongequal[\text{μορφ.}]{f:} f(-1+1) = f(0) = 0$,

άρα $f(-1) = -f(1) = -1$. (*)

• <u>$\forall n<0$</u>: $f(n) = f((-n)\cdot(-1)) \xlongequal[f:\text{μορφ}]{-n\in\mathbb{N}} f(-n)f(-1)$

$\xlongequal[(*)]{-n\in\mathbb{N}} (-n)\cdot(-1) = n.$

<u>Τελικά</u>, $f(n) = n$, $\forall n\in\mathbb{Z}$ $(f = Id_{\mathbb{Z}})$

(ii) <u>Θεωρία</u>: Αν $f: R \to S$ είναι μορφισμός δακτυλίων τότε ο πυρήνας $Ker(f)$ της f είναι ιδεώδες του R.

• Αν υπάρχει μορφισμός δακτυλίων $f: \mathbb{Q} \to \mathbb{M}_2(\mathbb{R})$ τότε $Ker(f)$: ιδεώδες του $\mathbb{Q}$. Αφού $\mathbb{Q}$: σώμα, έπεται $Ker(f) = \{0\}$ ή $Ker(f) = \mathbb{Q}$.

Συνεπώς, δεν υπάρχει μορφισμός δακτυλίων $f: \mathbb{Q} \to \mathbb{M}_2(\mathbb{R})$ με $Ker(f) = \mathbb{Z}$.

(iii) Έστω $f: \mathbb{Z}_p \to \mathbb{Z}_3$ μορφισμός δακτυλίων.
Επειδή $\mathbb{Z}_p$: σώμα και $Ker(f)$: ιδεώδες
του $\mathbb{Z}_p$, έπεται $Ker(f) = \{[0]_p\}$ ή $Ker(f) = \mathbb{Z}_p$

1η περίπτωση: $Ker(f) = \{[0]_p\}$: Τότε η f
είναι και 1-1 και από 1ο θεώρημα
Ισομορφισμών Δακτυλίων, $\mathbb{Z}_p \cong Im(f)$,
άρα: $p = |\mathbb{Z}_p| = |Im(f)| \leq |\mathbb{Z}_3| = 3$, άτοπο.

2η περίπτωση: $Ker(f) = \mathbb{Z}_p$. Τότε $[1]_p \in \mathbb{Z}_p$
$\Rightarrow [1]_p \in Ker(f) \Rightarrow f([1]_p) = [0]_3$
$$\xrightarrow[\text{μορφ.}]{f:} [1]_3 = [0]_3, \text{ άτοπο.}$$

• Σε κάθε περίπτωση καταλήγουμε σε άτοπο.

Ώστε, δεν υπάρχουν μορφισμοί δακτυλίων
από τον $\mathbb{Z}_p$ στον $\mathbb{Z}_3$ ∎

Γ8. Θεωρούμε τον δακτύλιο $R = \mathbb{Z} \times \mathbb{Z}$ και την απεικόνιση $f: \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$ με $f(n,m) = n$.

(i) Ο $\mathbb{Z}\times\mathbb{Z}$ έχει διαιρέτες του μηδενός (όπως κάθε ευθύ γινόμενο δακτυλίων)

(ii) <u>f: μορφισμός δακτυλίων</u>:

▸ $$\begin{aligned} f((n,m)+(n',m')) &= f(n+n', m+m') \\ &= n+n' \\ &= f(n,m)+f(n',m') \end{aligned} \quad , \forall (n,m),(n',m') \in \mathbb{Z}\times\mathbb{Z}$$

▸ $$\begin{aligned} f((n,m)\cdot(n',m')) &= f(nn', mm') \\ &= nn' \\ &= f(n,m)\cdot f(n',m') \end{aligned} \quad , \forall (n,m),(n',m') \in \mathbb{Z}\times\mathbb{Z}.$$

▸ $f(1_{\mathbb{Z}\times\mathbb{Z}}) = f(1,1) = 1 = 1_{\mathbb{Z}}$

(iii) <u>f: επιμορφισμός</u>: Έστω $k \in \mathbb{Z}$. Τότε $(k,0) \in \mathbb{Z}\times\mathbb{Z}$ και $f(k,0) = k$.

Από (ii), (iii) και 1º Θεώρημα Ισομορφισμών Δακτυλίων προκύπτει: $\mathbb{Z}\times\mathbb{Z}/_{\ker(\phi)} \cong \mathbb{Z}$.

Επειδή ο $\mathbb{Z}$ δεν έχει διαιρέτες του μηδενός (ως ακέραια περιοχή) έπεται λόγω ισομορφισμού ότι και ο δακτύλιος-πηλίκο $\mathbb{Z}\times\mathbb{Z}/_{\ker(\phi)}$ δεν έχει διαιρέτες του μηδενός (βλέπε και Άσκηση Γ4(ii))

· Για $R=\mathbb{Z}\times\mathbb{Z}$ και $J=\ker(\phi) \trianglelefteq R$ έχουμε το παράδειγμα για την Γ8. ∎

Γ9. $I+J = \{ x+y \in R \mid x \in I, y \in J \} \trianglelefteq R$.

(i) Αρχικά, γνωρίζουμε ότι $J \subseteq I+J$.

Σχόλιο: Έχουμε αποδείξει ότι το $I+J$ είναι ιδεώδες του R, άρα και υποδακτύλιος του R, με μηδενικό στοιχείο το 0_R αλλά δεν γνωρίζουμε αν το $I+J$ έχει μονάδα.

- $0_R \in J$ (διότι J: ιδεώδες του R):
- Αν $x, y \in J$ τότε $\in J$ οριστικά $x-y \in J$.
- Έστω $r \in I+J$ και $x \in J$. Θα αποδείξουμε ότι $rx \in J$ και $xr \in J$. Πράγματι, αφού $r \in I+J$, έπεται $r = a+b$ με $a \in I$, $b \in J$.

Άρα: $rx = (a+b)x = ax + bx \in J$ διότι

$$\left.\begin{array}{l} a \in I \subseteq R,\ b \in J \subseteq R,\ x \in J \\ \quad J: \text{ιδεώδες} \end{array}\right\} \Longrightarrow ax, bx \in J$$

$$\xRightarrow{J \leq (R,+)} ax + bx \in J.$$

Με ανάλογα επιχειρήματα:

$$xr = x(a+b) = xa + xb \in J.$$

Ώστε J: ιδεώδες του $I+J$.

(ii) Θεωρούμε $f : I \longrightarrow I+J/J$ με

$f(x) = x + J$. $\left(x \in I \xRightarrow{I \subseteq I+J} x \in I+J \right)$.

▶ f: μορφισμός δακτυλίων: Για κάθε $x, y \in I$ έχουμε:

$\cdot\ f(x+y) = (x+y)+J = (x+J)+(y+J) = f(x) + f(y)$

$\cdot\ f(xy) = xy + J = (x+J)\cdot(y+J) = f(x)\cdot f(y)$

▶ f: επί του $I+J/J$: Έστω $r+J \in I+J/J$.

Τότε $r \in I+J$, δηλαδή: $r = a+b$ με $\begin{array}{l} a \in I \\ b \in J \end{array}$

Έτσι: $f(a) = a+J = (a+J) + J \xlongequal[b+J=J]{b \in J}$

$(a+J)+(b+J) = (a+b)+J = r+J.$

▸ $Ker(f) = \{ x \in I \mid f(x) = 0_{I+J/J} \} =$

$= \{ x \in I \mid x + J = J \} = \{ x \in I \mid x \in J \} = I \cap J \trianglelefteq I.$

Από 1ο Θεώρημα Ισομορφισμών Δακτυλίων,

$I/_{Ker(f)} \cong Im(f) \Longleftrightarrow \boxed{I/_{I \cap J} \cong I+J/_{J}}$

Ισομορφισμός δακτυλίων που δεν έχουν απαραίτητα μονάδα.

Γ10. Εφ' όσον I, J ιδεώδη του δακτυλίου R, ορίζονται οι δακτύλιοι - πηλίκα R/I και R/J. Θεωρούμε την απεικόνιση

$f: R/I \longrightarrow R/J$ με $f(x+I) = x+J$

(A) <u>f: καλά ορισμένη</u>: Έστω $x+I = y+I \in R/I$ και θα αποδείξουμε ότι $f(x+I) = f(y+I)$.

Πράγματι, $x+I = y+I \Longleftrightarrow x-y \in I \xRightarrow{I \subseteq J}$

$x-y \in J \Rightarrow x+J = y+J \Rightarrow f(x+I) = f(y+I)$,

όπως θέλαμε.

(B) f: μορφισμός δακτυλίων: Για κάθε

$x+I, y+I \in R/I$ έχουμε:

- $f((x+I)+(y+I)) = f((x+y)+I) = (x+y)+J$
$$= (x+J)+(y+J)$$
$$= f(x+I)+f(y+I)$$

- $f((x+I)\cdot(y+I)) = f(xy+I) = xy+J$
$$= (x+J)\cdot(y+J)$$
$$= f(x+I)\cdot f(y+I)$$

- $f(1_{R/I}) = f(1_R+I) = 1_R+J = 1_{R/J}$

(Γ) f: επί του R/J: Έστω $\tilde{y} \in R/J$. Τότε

$\tilde{y} = x+J$ με $x \in R$. Θέτω $\tilde{x} = x+I \in R/I$

και έτσι: $f(\tilde{x}) = f(x+I) = x+J = \tilde{y}$

Δ $Ker(f) = \{ x+I \in R/I \mid f(x+I) = 0_{R/J} \}$

$= \{ x+I \in R/I \mid x+J = J \}$

$= \{ x+I \in R/I \mid x \in J \}$

$= J/I \trianglelefteq R/I$

Από Α - Δ και το 1ο Θεώρημα Ισομορφισμών Δακτυλίων έχουμε:

$R/I \,/\, Ker(f) \cong Im(f) \iff$

$\iff \boxed{R/I \,/\, J/I \cong R/J}$