

Εξέταση Άλγεβρας Ι (Τμήμα Β)

14/06/2024

Λύσεις θεμάτων

ΘΕΜΑ 1ο

$$(i) \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 8 & 6 & i & 4 & j & 1 \end{pmatrix}$$

Για τα i και j υπάρχουν δύο περιπτώσεις:

(α') $i=5, j=2$, οπότε

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 8 & 6 & 5 & 4 & 2 & 1 \end{pmatrix} \quad \text{και}$$

$$\begin{aligned} \text{άρα } \sigma &= (1 \ 3 \ 8) \circ (2 \ 7) \circ (4 \ 6) \\ &= (1 \ 8) \circ (1 \ 3) \circ (2 \ 7) \circ (4 \ 6) \end{aligned}$$

που σημαίνει σ : άρτια.

(α'') $i=2, j=5$, οπότε:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 8 & 6 & 2 & 4 & 5 & 1 \end{pmatrix}, \text{ οπότε}$$

$$\begin{aligned} \sigma &= (1 \ 3 \ 8) \circ (2 \ 7 \ 5) \circ (4 \ 6) \\ &= (1 \ 8) \circ (1 \ 3) \circ (2 \ 5) \circ (2 \ 7) \circ (4 \ 6) \end{aligned}$$

που σημαίνει ότι σ : περιττή.

. Τελικά, $\boxed{i=2, j=5}$

$$(ii) \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 8 & 6 & 2 & 4 & 5 & 1 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 7 & 6 & 8 & 2 & 3 & 1 \end{pmatrix}$$

$$\text{Είναι: } \sigma = (1 \ 3 \ 8) \circ (2 \ 7 \ 5) \circ (4 \ 6)$$

$$\tau = (1 \ 5 \ 8) \circ (2 \ 4 \ 6) \circ (3 \ 7)$$

Έλεγχος τάσεων: $o(\sigma) = [3, 3, 2] = 6$

$$o(\tau) = [3, 3, 2] = 6$$

✓

Έλεγχος άρτια - περιττή :

$$\sigma = (1\ 8) \circ (1\ 3) \circ (2\ 5) \circ (2\ 7) \circ (4\ 6) : \text{περιττή}$$

$$\tau = (1\ 8) \circ (1\ 5) \circ (2\ 6) \circ (2\ 4) \circ (3\ 7) : \text{περιττή} \quad \checkmark$$

Αν $\rho \in S_8$ τέτοια, ώστε $\rho \circ \tau \circ \rho^{-1} = \sigma$, τότε

$$\rho \circ (1\ 5\ 8) \circ (2\ 4\ 6) \circ (3\ 7) \circ \rho^{-1} = \sigma \Rightarrow$$

$$(\rho \circ (1\ 5\ 8) \circ \rho^{-1}) \circ (\rho \circ (2\ 4\ 6) \circ \rho^{-1}) \circ (\rho \circ (3\ 7) \circ \rho^{-1}) = \sigma$$

$$\Rightarrow (\rho(1)\ \rho(5)\ \rho(8)) \circ (\rho(2)\ \rho(4)\ \rho(6)) \circ (\rho(3)\ \rho(7)) = \sigma$$

$$\text{Επειδή } \sigma = (1\ 3\ 8) \circ (2\ 7\ 5) \circ (4\ 6),$$

επιδέχεται: $\rho(1) = 1, \rho(5) = 3, \rho(8) = 8, \rho(2) = 2,$

$\rho(4) = 7, \rho(6) = 5, \rho(3) = 4, \rho(7) = 6$, δηλαδή

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 7 & 3 & 5 & 6 & 8 \end{pmatrix}$$

. Εύκολα επαληθεύουμε ότι για την

παράπάνω ρ ισχύει $\rho \circ \tau \circ \rho^{-1} = \sigma$.

(iii) Επειδή τ : περιττή προκύπτει τ^{-1} : περιττή.
 Πράγματι, αν τ^{-1} : άρτια, δηλαδή $\tau^{-1} \in A_8$
 τότε εφόσον $A_8 \leq S_8$ θα είχαμε:

$$(\tau^{-1})^{-1} \in A_8 \Rightarrow \tau \in A_8 \Rightarrow \tau: \text{άρτια, άτοπο.}$$

$$\text{Άρα, } \left. \begin{array}{l} \sigma: \text{περιττή} \\ \tau^{-1}: \text{περιττή} \end{array} \right\} \Rightarrow \sigma\tau^{-1}: \text{άρτια}$$

$$\text{οπότε: } \sigma\tau^{-1} \in A_8 \xRightarrow{A_8 \leq S_8} (\sigma\tau^{-1})^{17} \in A_8$$

και συνεπώς $\sigma\tau^{-1}$: άρτια. •

ΘΕΜΑ 2^ο

$$(i) \mathbb{Z}_8 = \{ [0]_8, [1]_8, [2]_8, \dots, [7]_8 \} = \langle [1]_8 \rangle$$

Εφόσον η $\mathbb{Z}_8$ είναι κυκλική τότε κάθε υποομάδα της είναι κυκλική. Από γνωστή

θεωρία έχουμε: ότι οι υποομάδες της

είναι οι ακόλουθες, και μόνο αυτές:

$$\bullet H_0 = \langle [0]_8 \rangle = \{ [0]_8 \} \quad (\text{τάξης } 1)$$

$$\bullet H_1 = \langle [1]_8 \rangle = \mathbb{Z}_8 \quad (\text{τάξης } 8)$$

$$\bullet H_2 = \langle [2]_8 \rangle = \langle 2[1]_8 \rangle = \langle d_2[1]_8 \rangle, \text{ όπου}$$

$$d_2 = (8, 2) = 2, \quad \text{οπότε: } |H_2| = \frac{8}{2} = 4$$

$$H_2 = \langle 2[1]_8 \rangle = \langle [2]_8 \rangle = \{ 0 \cdot [2]_8, 1 \cdot [2]_8, 2 \cdot [2]_8, 3 \cdot [2]_8 \} = \{ [0]_8, [2]_8, [4]_8, [6]_8 \}$$

$$\bullet \text{Επειδή } (3, 8) = (5, 8) = (7, 8) = 1 \text{ έπεται:}$$

$$H_3 = \langle [3]_8 \rangle = \mathbb{Z}_8 = \langle [1]_8 \rangle$$

$$H_5 = \langle [5]_8 \rangle = \mathbb{Z}_8 = \langle [1]_8 \rangle$$

$$H_7 = \langle [7]_8 \rangle = \mathbb{Z}_8 = \langle [1]_8 \rangle$$

$$\bullet \text{Αντίστοιχα βρίσκουμε:}$$

$$H_4 = \langle [4]_8 \rangle = \{ [0]_8, [4]_8 \}$$

$$H_6 = \langle [6]_8 \rangle = \langle [2]_8 \rangle$$

$$\begin{aligned} \cdot U(\mathbb{Z}_8) &= \{ [k]_8 \in \mathbb{Z}_8 \mid 1 \leq k \leq 8, (k, 8) = 1 \} \\ &= \{ [1]_8, [3]_8, [5]_8, [7]_8 \} \quad (\varphi(8) = 4). \end{aligned}$$

$\cdot$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[1]_8$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[3]_8$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$[5]_8$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$[7]_8$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

$\cdot U(\mathbb{Z}_8)$: αβελιανή, όπου κάθε στοιχείο
 έχει τάξη 2, άρα μη-κυκλική και
 $|U(\mathbb{Z}_8)| = 4 = \varphi(8)$.

Συνεπώς: $U(\mathbb{Z}_8) \cong V_4$
 $\uparrow$
 η ομάδα του
 Klein.

(ii) Εφ' όσον $|G| = p \geq 2$, υπάρχει στοιχείο $a \in G$ με $a \neq e$. Τότε: $\langle a \rangle \leq G$ και από θεώρημα Lagrange: $|\langle a \rangle| \mid |G|$
 $\Rightarrow |\langle a \rangle| \mid p \xrightarrow[\text{πρώτος}]{p:} |\langle a \rangle| = 1 \text{ ή } |\langle a \rangle| = p.$

Αν $|\langle a \rangle| = 1$ τότε: $o(a) = |\langle a \rangle| = 1$ και

άρα: $a^1 = e \Rightarrow a = e$, άτοπο. Άρα.

$|\langle a \rangle| = p = |G|$ και επειδή $\langle a \rangle \leq G$ έχουμε

$G = \langle a \rangle$, άρα G : κυκλική.

• G : απλή: Έστω $H \trianglelefteq G$ με $H \neq \{e\}$
 και θα δείξουμε ότι αναγκαστικά $H = G$.

Πράγματι, από θεώρημα Lagrange:

$$|H| \mid |G| \Rightarrow |H| \mid p \xrightarrow[\text{πρώτος}]{p:} |H| = 1 \text{ ή } |H| = p.$$

Εφόσον $H \neq \{e\}$ έπεται $|H| = p = |G|$

$\xRightarrow{|H| = |G|} H = G$, όπως θέλαμε.

ΘΕΜΑ 3°

(i) Επειδή η G είναι κυκλική, είναι και αβελιανή, οπότε $H \trianglelefteq G$ και ορίζεται η ομοείδα-πηλίκο G/H . Θα αποδείξουμε ότι $G/H = \langle \alpha H \rangle$. Επειδή $\langle \alpha H \rangle \subseteq G/H$, αρκεί να δείξουμε ότι $G/H \subseteq \langle \alpha H \rangle$. Έστω

$gH \in G/H$. Τότε $g \in G \Rightarrow g \in \langle \alpha \rangle \Rightarrow$

$\exists k \in \mathbb{Z}: g = \alpha^k$, οπότε:

$$gH = \alpha^k H = (\alpha H)^k \in \langle \alpha H \rangle, \text{ όπως θέλαμε.} \blacksquare$$

(ii) Έστω $\varphi: \mathbb{Z}_7 \rightarrow S_5$ μορφισμός ομάδων.

Επειδή $\text{Ker}(\varphi) \leq \mathbb{Z}_7$, από Θεώρημα Lagrange

$$|\text{Ker}(\varphi)| \mid |\mathbb{Z}_7| \Rightarrow |\text{Ker}(\varphi)| \mid 7 \xrightarrow{7: \text{πρώτος}}$$

$$\bullet |\text{Ker}(\varphi)| = 1 \quad \text{ή} \quad \bullet |\text{Ker}(\varphi)| = 7$$

Αν ισχύει $|\text{Ker}(\varphi)| = 1$ τότε $\text{Ker}(\varphi) = \{[0]_7\}$,
που σημαίνει φ : μονομορφισμός. Από το 1^ο
θεώρημα ισομορφισμών ομάδων θα είχαμε

$$\mathbb{Z}_7 \cong \text{Im}(\varphi), \text{ άρα: } |\text{Im}(\varphi)| = |\mathbb{Z}_7| = 7.$$

Όμως $\text{Im}(\varphi) \leq S_5$ και από Lagrange θα
έπρεπε: $|\text{Im}(\varphi)| \mid |S_5| \Rightarrow 7 \mid 5!, \underline{\underline{\text{άτοπο}}}.$

Έστω, $|\text{Ker}(\varphi)| = 7 \Rightarrow \text{Ker}(\varphi) = \mathbb{Z}_7$, οπότε:

$\varphi([x]_7) = \text{Id}, \forall [x]_7 \in \mathbb{Z}_7$, δηλαδή φ : ο
τετριμμένος.

■

ΘΕΜΑ 4^ο

$$(1) \quad S = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in M_2(\mathbb{R}) \mid a, b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R}).$$

► S : υποδακτύλιος του $M_2(\mathbb{R})$:

$$\cdot \quad 0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$$

$$\cdot \quad \text{Αν } X = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}, Y = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \in S \text{ τότε:}$$

$$\cdot \quad X - Y = \begin{bmatrix} a-c & -b+d \\ b-d & a-c \end{bmatrix} = \begin{bmatrix} a-c & -(b-d) \\ b-d & a-c \end{bmatrix} \in S$$

$$\cdot \quad XY = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -ab-bc \\ bc+ad & -bd+ac \end{bmatrix} =$$

$$= \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix} \in S$$

Άρα ο S είναι υποδακτύλιος του $M_2(\mathbb{R})$.

Μάλιστα, επειδή $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$, έχουμε

$$\text{επιπλέον ότι } 1_S = I_2 (= 1_{M_2(\mathbb{R})})$$

► S: σώμα: Θα αποδείξουμε ότι ο S είναι μεταθετικός και ότι κάθε μη-μηδενικός πίνακας του S είναι αντιστρέψιμος με αντίστροφο που ανήκει πάλι στο S .

• Για κάθε $X = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in S$, $Y = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \in S$

έχουμε:

$$XY = \begin{bmatrix} ac - bd & -ad - bc \\ bc + ad & -bd + ac \end{bmatrix}$$

$$YX = \begin{bmatrix} ca - db & -cb - da \\ cb + da & -db + ca \end{bmatrix} = \begin{bmatrix} ac - bd & -ad - bc \\ bc + ad & -bd + ac \end{bmatrix} = XY$$

Εφ' όσον $XY = YX$, $\forall X, Y \in S$, ο S είναι μεταθετικός.

• Έστω τώρα $X = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in S$ με $X \neq \mathbf{0}$.

Τότε $a \neq 0$ ή $b \neq 0$ και συνεπώς:

$\det(X) = a^2 + b^2 \neq 0$, που σημαίνει ότι

υπάρχει ο $X^{-1} = \begin{bmatrix} \frac{a}{a^2+b^2} & \frac{b}{a^2+b^2} \\ -\frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix}$.

Παρατηρώμε ότι $X^{-1} \in S$ και

$$X X^{-1} = \underbrace{I_2}_{1_S} = X^{-1} X, \text{ όπως δείξαμε.}$$

$$[\text{Δηλαδή } U(S) = S \cdot \{0\}].$$

► S : όχι ιδεώδες του $M_2(\mathbb{R})$:

(α)' τρόπος: Αν το S ήταν ιδεώδες του $M_2(\mathbb{R})$ τότε, επειδή $\underset{M_2(\mathbb{R})}{1} = I_2 \in S$, θα είχαμε $S = M_2(\mathbb{R})$, άτοπο.

(β)' τρόπος: Επειδή $\mathbb{R}$ σώμα έπεται ότι ο $M_2(\mathbb{R})$ είναι απλός δακτύλιος, δηλαδή τα μόνα τω ιδεώδη είναι: $\{0\}$ και $M_2(\mathbb{R})$.

Άρα S : όχι ιδεώδες

(γ)' τρόπος : $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{R})$, $I_2 \in S$ και

$$I_2 \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \notin S$$

άρα S : όχι ιδεώδες.

(ii) Ο $R = \mathbb{Z} \times \mathbb{Z}$ έχει διακρίτες του μηδενός,
 π_x : $(0, 1) \cdot (1, 0) = (0, 0)$ και $(0, 1), (1, 0) \neq (0, 0)$.

Θεωρούμε $f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ με $f(n, m) = n$.

► f : μορφισμός δακτυλίων : Για κάθε (n, m) ,

$(n', m') \in \mathbb{Z} \times \mathbb{Z}$ έχουμε :

$$\begin{aligned} \bullet f((n, m) + (n', m')) &= f(n + n', m + m') \\ &= n + n' \\ &= f(n, m) + f(n', m') \end{aligned}$$

$$\begin{aligned} \bullet f((n, m) \cdot (n', m')) &= f(nn', mm') \\ &= nn' \\ &= f(n, m) f(n', m') \end{aligned}$$

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

► f : επιμορφισμός, δηλαδή $\text{Im}(f) = \mathbb{Z}$:

Έστω $n \in \mathbb{Z}$. Τότε $(n, 0) \in \mathbb{Z} \times \mathbb{Z}$ και

$$\underline{f(n, 0) = n}$$

$$\begin{aligned} \text{Ker}(f) &= \{ (n, m) \in \mathbb{Z} \times \mathbb{Z} \mid f(n, m) = 0 \} \\ &= \{ (n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n = 0 \} \\ &= \{ (0, m) \in \mathbb{Z} \times \mathbb{Z} \mid m \in \mathbb{Z} \} \triangleq \mathbb{Z} \times \mathbb{Z}. \end{aligned}$$

Θέτουμε $I = \text{Ker}(f) \triangleq \mathbb{Z} \times \mathbb{Z}$, από 1^ο

Θεώρημα ισομορφ. Δακτυλίων έχουμε:

$$\mathbb{Z} \times \mathbb{Z} / \text{Ker}(f) \cong \text{Im}(f) \Rightarrow R/I \cong \mathbb{Z}$$

Ο $\mathbb{Z}$ δεν έχει διαιρετές του μηδενός

και συνεπώς ο R/I δεν έχει διαιρετές του μηδενός.

ΘΕΜΑ 5^ο

(i) Έστω I ένα μη-μηδενικό ιδεώδες των $\mathbb{Z}[i]$. Τότε υπάρχει $z \in I$ με $z \neq 0$.
Είπω $z = a + bi$ με $a, b \in \mathbb{Z}$, $a \neq 0$ ή $b \neq 0$.

$$\left. \begin{array}{l} z \in I \\ \bar{z} \in \mathbb{Z}[i] \\ I: \text{ιδεώδες} \end{array} \right\} \Rightarrow z\bar{z} \in I \Rightarrow |z|^2 \in I, \text{ όπου}$$

$|z|^2 = a^2 + b^2 \in \mathbb{N}$, άρα το I περιέχει τον θετικό ακέραιο $a^2 + b^2$.

(ii) Αρκεί να αποδείξουμε ότι κάθε μη-μηδενικό στοιχείο του R είναι αντιστρέψιμο.
Έστω λοιπόν $a \in R$, $a \neq 0_R$. Επειδή $|R| = p$ και p πρώτος, έπεται ότι η προσθετική ομάδα $(R, +)$ είναι κυκλική [ΘΕΜΑ 2 ii)] και άρα οι μόνες υποομάδες της είναι

οι $\{0_R\}$ και R . Θεωρούμε τώρα το
 κύριο ιδεώδες $\langle a \rangle = \{ra \in R \mid r \in R\}$ που
 παράγεται από το a . Επειδή το ιδεώδες
 είναι και υποομάδα της $(R, +)$, έπεται
 $\langle a \rangle = \{0_R\}$ ή $\langle a \rangle = R$. Όμως $a \neq 0_R$ και
 άρα δεν είναι δυνατόν να ισχύει $\langle a \rangle = \{0_R\}$
 οπότε, $\langle a \rangle = R$. Τότε: $1_R \in R \Rightarrow 1_R \in \langle a \rangle$
 $\Rightarrow \exists b \in R: 1_R = ba = ab$,
 $\uparrow$
 R : μεταθετικός

οπότε a : αντιστρέψιμο, όπως θέλαμε.