Φυλλάδιο 9

Date. No. 20/5/19

(6) R πεπερασμένος δακτύλιος με μοναδιαίο στοιχείο 1 και τουλάχιστον δύο στοιχεία. Υποθέτουμε ότι αν $a,b \in R \setminus \{0\}$ τότε $ab \neq 0$ (δηλ δεν έχει διαιρέτες του μηδένος). Δείξτε ότι ο R είναι δακτύλιος διαίρεσης.

Λύση: $R = \{0, 1, a_1, a_2, \dots, a_n\}$ έστω $a \neq 0 \Rightarrow$ ($a_0 = 1$)

$\Rightarrow a \in \{a_0, a_1, \dots, a_n\}$. Τα στοιχεία $aa_0, aa_1, \dots, aa_n$ είναι διαφορετικά μεταξύ τους.

(Απόδ: Έστω $aa_i = aa_j \Rightarrow aa_i - aa_j = 0 \Rightarrow$
$\Rightarrow a(a_i - a_j) = 0 \xrightarrow[\text{διαιρέτες του 0}]{\text{δεν έχει}} a_i - a_j = 0 \Rightarrow a_i = a_j$)

Το $a \neq 0, a_i \neq 0$ $\left.\begin{matrix} \\ 0 \leq i \leq n \end{matrix}\right\} \Rightarrow aa_i \neq 0$

$n+1$ στοιχεία

$\{aa_0, aa_1, \dots, aa_n\} \subseteq \{a_0, a_1, \dots, a_n\} \Rightarrow$

$\Rightarrow \{aa_0, aa_1, \dots, aa_n\} = \{a_0, a_1, \dots, a_n\} \Rightarrow$ ($a_0 = 1$)

$\Rightarrow 1 \in \{aa_0, aa_1, \dots, aa_n\} \Rightarrow aa_i = 1$

Όμοια, πολλαπλασιάζοντας με a από δεξιά, έχουμε $a_j a = 1$ για κάποιο $j$:

$a_i = 1a_i = (a_j a)a_i = a_j(aa_i) = a_j \cdot 1 = a_j$

Άρα κάθε $a \neq 0$ έχει αντίστροφο $\Rightarrow$ R δακτύλιος διαίρεσης

Date. No.

**Ορισμός**: Έστω $R$ δακτύλιος και $I \subset R$. Το $I$ ονομάζεται **ιδεώδες** του $R$ αν:

i) $0 \in R$ $I$
ii) Αν $a, b \in I \Rightarrow a - b \in I$
iii) Αν $r \in R$ και $a \in I \Rightarrow ra \in I$ και $ar \in I$

$\left.\begin{array}{l} \\ \\ \end{array}\right]$ $I \leq (R, +)$ ($\Leftrightarrow$ $I \trianglelefteq R$)

**Παρατήρηση**: Το $I$ είναι δακτύλιος. $(I, +, \cdot)$ με τις πράξεις του $R$. Το $I$ υποδακτύλιος του $R$

**Ορισμός**: Έστω $R'$ υποσύνολο ενός δακτυλίου $(R, +, \cdot)$. Το $R'$ ονομάζεται υποδακτύλιος του $R$ αν είναι δακτύλιος με τις πράξεις του $R$ (δηλ. $R'$, $+_R$, $\cdot_R$ είναι δακτύλιος)

**Παραδείγματα**: Το $\{0\}$ είναι ιδεώδες του $R$
Το $R$ είναι ιδεώδες του $R$

**Άσκ**: Βρείτε όλα τα ιδεώδη του δακτυλίου $\mathbb{Z}$

**Λύση**:

Έστω $I$ ιδεώδες του $\mathbb{Z} \Rightarrow I$ υποομάδα της προσθετικής ομάδας $\mathbb{Z} \Rightarrow I$ κυκλική υποομάδα $\Rightarrow$
$\Rightarrow I = \langle m \rangle = \{$για κάποιο $m \in \mathbb{Z}$
$= \{\ldots -2m, -m, m, 2m, 3m, 4m, \ldots\}$

$I$ υποομάδα. Έστω $r \in \mathbb{Z}$ και $a \in \langle m \rangle$
$ar = ra = r(km) = (rk)m \in \langle m \rangle = I \Rightarrow ar = ra \in I$

Άρα το $I = \langle m \rangle$ είναι ιδεώδες. Συνεπώς όλα τα ιδεώδη του $\mathbb{Z}$ είναι τις μορφής $\langle m \rangle$ για κάποιο $m \in \mathbb{Z}$

Date. No.

# Ι ιδεώδες ενός δακτυλίου Β

$(R/I, +, \cdot)$ δακτύλιος πηλίκο

$\{r+I / r\in R\}$ $(r_1+I)+(r_2+I)=(r_1+r_2)+I$

$(r_1+I)(r_2+I)=r_1r_2+I$

$I \lhd (R,+) \Rightarrow$ Η πρόσθεση είναι καλά ορισμένη στον $R/I$ και $R/I$ αβελιανή ομάδα ως προς την πρόσθεση

(Ο πολλαπλασιασμός είναι καλά ορισμένος) ✓

Έστω $r_1+I = r_1'+I$ και $r_2+I = r_2'+I \Rightarrow r_1 = r_1'+i_1$

~~$(r_1+I)(r_2+I)$~~ $\in r_1+I = r_1'+I \Rightarrow \boxed{r_1 = r_1'+i_1}$

$r_2 = r_2+0 \in r_2+I = r_2'+I \Rightarrow r_2 = r_2'+i_2$

$(r_1+I)(r_2+I) = r_1r_2+I = (r_1'+i_1)(r_2'+i_2)+I =$

$= r_1'r_2' + (i_1r_2' + i_1i_2 + r_1'i_2) + I = r_1'r_2'+I = (r_1'+I)(r_2'+I)$

$\in I \quad \in I \quad \in I$

- $((a+I)(b+I))(\gamma+I) = (ab+I)(\gamma+I) = (ab)\gamma + I =$

$(ab\gamma = a(b\gamma))$ $a(b\gamma)+I = (a+I)(b\gamma+I) = (a+I)((b+I)(\gamma+I))$

$a, b, \gamma \in R$

Άρα $R/I$ δακτύλιος.

**Παρατήρηση 1)** Αν $R$ δακτύλιος με μοναδιαίο στοιχείο τότε $R/I$ δακτύλιος με μοναδιαίο στοιχείο για κάθε ιδεώδες του $R$

$1 \in R \Rightarrow 1a = a\cdot 1 = a \quad \forall a \in R$

$(1+I)(a+I) = 1a+I = a+I$

$(a+I)(1+I) = a1+I = a+I$

Το $1+I$ είναι το μοναδιαίο στοιχείο του $R/I$

Date. No.

2) Αν R αντιμεταθετικός δακτύλιος τότε και ο R/I είναι αντιμεταθετικός για κάθε ιδεώδες I του R

$(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I)$

R αντιμεταθετικός

**Θεώρημα:** Έστω I ένα ιδεώδες ενός δακτυλίου R Η απεικόνιση $f: R \to R/I$ με $f(r) = r+I$ είναι ένας ομομορφισμός δακτυλίων με πυρήνα το I

**Απόδ:**

Δείξαμε στο αντίστοιχο θεώρημα στις ομάδες ότι η απεικόνιση f είναι ομομορφισμός ομάδων με πυρήνα το I. Άρα πρέπει να αποδείξουμε ότι:

$f(ab) = f(a) \cdot f(b)$

$f(a)f(b) = (a+I)(b+I) = ab+I = f(ab)$

**Θεώρημα:** (Θεμελιώδες θεώρημα ομομορφισμών δακτυλίων)

Έστω $\varphi: R \to R'$ ένας ομομορφισμός δακτυλίων με πυρήνα $\ker\varphi = I$. Η απεικόνιση $\mu(x+I) = \varphi(x)$ από το R/I στο $\varphi(R)$ είναι ισομορφισμός δακτυλίων. Δηλαδή ισχύει: $R/\ker\varphi \cong \varphi(R)$

**Απόδ:**

$\mu(x+I) = \varphi(x)$ καλά ορισμένη έχει γίνει το θεμελιώδες θεώρημα ομομορφισμού ομάδων

$\mu((x+I)+(y+I)) = \mu(x+I) + \mu(y+I)$ +Η -

μ 1-1

μ επί

$\mu((x+I)(y+I)) = \mu(xy+I) = \varphi(xy) \overset{\varphi \text{ ομομορφισμός δακτυλίων}}{=} \varphi(x)\varphi(y) =$

Date. No.

$= \mu(x+I)\mu(y+I)$

**Ορισμός:** Ένα ιδεώδες $I \neq R$ σε έναν αντιμεταθετικό δακτύλιο $R$ λέγεται πρώτο ιδεώδες αν ισχύει: αν $ab \in I \Rightarrow a \in I$ ή $b \in I$

**Παράδειγμα 1.** Έστω $p$ πρώτος αριθμός. $\langle p \rangle = pR \neq R$
Έστω $ab \in \langle p \rangle \Rightarrow ab = kp \Rightarrow p \mid ab \Rightarrow p \mid a$ ή $p \mid b$
$\Rightarrow a \in \langle p \rangle$ ή $b \in \langle p \rangle$
Άρα αν $p$ πρώτος τότε: $\langle p \rangle = pZ$ είναι πρώτο ιδεώδες του $Z$
$1 \in R$ $\langle 1 \rangle = 1R = R$ άρα δεν είναι πρώτο ιδεώδες
Έστω $ab$ σύνθετος
$1 < a < ab$ $\langle ab \rangle$ είναι πρώτο? Όχι
$1 < b < ab$ $ab \in \langle ab \rangle$ αλλά $a \notin \langle ab \rangle$ και $b \notin \langle ab \rangle$

**Ορισμός:** Ένα ιδεώδες $I \neq R$ σε έναν αντιμεταθετικό δακτύλιο $R$ λέγεται πρώτο ιδεώδες αν ισχύει: αν $ab \in I \Rightarrow a \in I$ ή $b \in I$

**Θεώρημα:** Έστω $R$ αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $1 \neq 0$. Έστω $I \neq R$ ένα ιδεώδες του $R$. Ο δακτύλιος $R/I$ είναι αμέσως περιοχή αν και μόνο αν $I$ πρώτο ιδεώδες.

**Απόδ.**
($\Rightarrow$) $R/I$ αμέσως περιοχή $I \neq R$. Έστω $ab \in I$
$ab + I = I = 0 + I \Rightarrow 0 + I = ab + I = (a+I)(b+I)$
$\xRightarrow{R/I \text{ αμέσως περιοχή}}$ $a + I = 0 + I$ ή $b + I = 0 + I$

Date. No.

$a+I=0+I$ ή $b+I=0+I \Rightarrow a+0 \in a+I=I$

δηλ $a \in I$ ή $b+0 \in b+I=0+I=I \Rightarrow b \in I \Rightarrow$

$\Rightarrow$ I πρώτο ιδεώδες

($\Leftarrow$) I πρώτο ιδεώδες, R αντιμεταθετικός $\Rightarrow$
$\Rightarrow R/I$ αντιμεταθετικός, R έχει μοναδιαίο στοιχείο $\Rightarrow$
$\Rightarrow R/I$ έχει μοναδιαίο στοιχείο

$I \neq R \Rightarrow R/I \neq \{0+I\} \Rightarrow 0+1 \neq 1+1$

Έστω $(a+I)(b+I)=0+I \Rightarrow ab+I=0+I \Rightarrow$

$\Rightarrow ab=ab+0=ab+I=I \Rightarrow ab \in I$ $\Rightarrow$

I πρώτο ιδεώδες

$\Rightarrow a \in I$ ή $b \in I \Rightarrow \overset{\in I}{a}+I=I=0+I$ ή

$\underset{\in I}{b}+I=I=0+I$

Άρα ο $R/I$ δεν έχει διαιρέτες του μηδενός
οπότε ο $R/I$ ακέραια περιοχή

Ορισμός: Ένα ιδεώδες $M$ του δακτυλίου $R$ λέγεται μεγιστοτικό (μέγιστο) αν

i) $M \neq R$ και

ii) αν $I$ ιδεώδες του $R$ τέτοιο ώστε:
$M \subseteq I \subseteq R$ τότε $I=M$
$I=R$

Θεώρημα: Έστω $R$ αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Το $M$ είναι μεγιστοτικό ιδεώδες του $R$ αν και μόνο αν $R/M$ είναι σώμα

Date. No.

**Απόδ:** i) Το $M$ είναι μεγιστικό $M \neq R$

$R$ αντιμεταθετικός $\Rightarrow R/M$ αντιμεταθετικός
$R$ έχει μοναδιαίο στοιχείο $(1 \in R) \Rightarrow$
$\Rightarrow R/M$ έχει μοναδιαίο στοιχείο $(1+M \in R/M)$
$R/M \neq \{0+M\} \Rightarrow 0+M \neq 1+M$

Έστω $a+M \neq 0+M \Rightarrow a \notin M$
$I_a = \{ra+m \mid r \in R, m \in M\}$ ισχυριζόμαστε ότι $I$ ιδεώδες
i) $0 = 0a + 0^{\in M} \in I_a$
ii) Έστω $r_1a+m_1 \in I$ και $r_2a+m_2 \in I_a$
$(r_1a+m_1) - (r_2a+m_2) = (r_1-r_2)a + \underbrace{m_1-m_2}_{\in M} \in I_a$
iii) Έστω $r \in R$ και $r_1a+m_1 \in I_a$
$(r_1a+m_1)r = r(r_1a+m_1) = rr_1a + \underbrace{rm_1}_{\in M} \in I_a$

Έστω $m \in M \Rightarrow m = 0a + m \in I_a \Rightarrow M \subseteq I_a$
$a \in I_a$, $a \notin M$ $\Rightarrow M \subsetneq I_a \subseteq R$ (μεγιστικό)

$\Rightarrow I_a = R$
$a \in I_a$, $a \notin M$
$1 \in R = I_a \Rightarrow 1 = ra + u$

$(a+M)(r+M) = ar + M = 1 - m + M = 1 + M$ άρα $a+M$ αντιστρέψιμο $\Rightarrow R/M$ είναι αντιμεταθετικός

Αν $R/M$ σώμα $0+M \neq 1+M$ $1 \notin M \Rightarrow M \neq R$
Έστω $I$ ιδεώδες του $R$ τέτοιο ώστε
$M \subsetneq I \subseteq R \Rightarrow$ υπάρχει $a \in I$ και $a \notin M \Rightarrow a+M \neq 0+M$
$R/M$ σώμα άρα $a+M$ αντιστρέψιμο $\Rightarrow$ υπάρχει $b+M \in R/M$ τέτοιο ώστε $(a+M)(b+M) = 1+M$
$ab+M = 1+M \Rightarrow ab = ab+0 \in ab+M = 1+M \Rightarrow$
$\Rightarrow ab = 1+m$ για κάποιο $m \in M$

Date. No.

$ab - u = 1$
$a \in I \quad ab \in I$
$u \in M \subsetneq I$
$\Rightarrow 1 = \underset{\in I}{ab} - \underset{\in I}{u} \in I$

Έστω $r \in R$ και $1 \in I \Rightarrow r = r \cdot \underset{\in I}{1} \in I \Rightarrow R \subseteq I \subseteq R \Rightarrow$
$\Rightarrow I = R$

Άρα το $M$ είναι μεγιστικό

~~Άσκηση Βγάζετε~~

**Θεώρημα:** Δείξτε ότι σε έναν αντιμεταθετικό δακτύλιο με μοναδιαίο στοιχείο κάθε μεγιστικό ιδεώδες είναι πρώτο.

Έστω $M$ μεγιστικό $\Rightarrow R/M$ είναι σώμα $\Rightarrow$
$\Rightarrow R/M$ είναι ακέραια περιοχή $\Rightarrow M$ πρώτο

**Πρόταση:** Έστω $F$ σώμα $\Rightarrow F$ αντιμεταθετικός δακτύλιος,
$F$ έχει μοναδιαίο στοιχείο

Έστω $a, b$ διαιρέτες του μηδενός $\Rightarrow ab = 0$
$a \neq 0$
$b \neq 0$

$a \neq 0$
$a \in I$ σώμα $\Rightarrow a$ αντιστρέψιμο δηλ. $a \cdot a^{-1} = 1$
$ab = 0 \Rightarrow a^{-1}(ab) = a^{-1} \cdot 0 \Rightarrow$
$\Rightarrow (a^{-1}a)b = 0 \Rightarrow 1 \cdot b = 0 \Rightarrow \boxed{b = 0}$

Άρα $F$ ακέραια περιοχή

Date. No.

**Παράδειγμα**: Υπάρχουν ιδεώδη που είναι πρώτα αλλά δεν είναι μεγιστικά.

$\mathbb{Z}$: ο δακτύλιος των ακεραίων. Το $\{0\}$ είναι πρώτο ιδεώδες του $\mathbb{Z}$

$\{0\} \neq \mathbb{Z}$. Έστω $ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a=0$ ή $b=0$ (ακέραια περιοχή)

$\Rightarrow a \in \{0\}$ ή $b \in \{0\}$ Άρα $\{0\}$ πρώτο

$\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$. Άρα το $\{0\}$ δεν είναι μεγιστικό

**Ιδεώδη του $\mathbb{Z}$**: $\{0\}$ και τα $m\mathbb{Z}$ όπου $m$ μηδενικός

**Πρώτα ιδεώδη**: $\{0\}$ και τα $p\mathbb{Z}$ όπου $p$: πρώτος

**Μεγιστικά ιδεώδη**: $p\mathbb{Z}$ όπου $p$: πρώτος αριθμός

**Άσκηση**: Δείξτε ότι ένα σώμα $F$ έχει ακριβώς δύο ιδεώδη: τα $F$ και $\{0\}$ ($1 \in F$ και $1 \neq 0 \Rightarrow 1 \notin \{0\}$ άρα $1 \in I$ και $I \neq \{0\}$)

Έστω $I \neq \{0\}$ ιδεώδες του $F \Rightarrow$ ~~υπάρχει $I \neq \{0\}$~~

$\Rightarrow$ άρα υπάρχει $a \in I$ με $a \neq 0$ $\Rightarrow$ $a$ αντιστρέψιμο (σώμα)

$a^{-1}a = 1 \in I$

$\uparrow F \quad \uparrow I$

$I = I$

$\Rightarrow$ Έστω $r \in F$ $\quad r = r \cdot 1 \in I \Rightarrow F \subseteq I \subseteq F \Rightarrow I = F$

Date. No.

## Φυλλάδιο (8)

6) Θεωρούμε την υποομάδα $T$ της ομάδας $(\mathbb{C}^*, \cdot)$ όπου $T = \{z \in \mathbb{C} \mid |z| = 1\}$. Δείξτε ότι η υποομάδα $T$ είναι κανονική και ότι $\mathbb{C}^*/T \simeq \mathbb{R}^+$ ✱ Θετικοί πραγματικοί αριθμοί

Λύση: $\mathbb{C}^* \xrightarrow{\varphi} \mathbb{R}^+$ (ομομορφισμός ομάδων)

$\varphi(z) = |z|$. Αν $z \in \mathbb{C}^* \Rightarrow z \neq 0 \Rightarrow |z| \neq 0 \Rightarrow$
$\Rightarrow |z| \in \mathbb{R}^+$ άρα $\varphi$ καλά ορισμένη

$\varphi(z_1 z_2) = |z_1 z_2| = |z_1||z_2| = \varphi(z_1)\varphi(z_2)$
Άρα $\varphi$: ομομορφισμός ομάδων

$\ker\varphi = \{z \in \mathbb{C}^* \mid \varphi(z) = 1\} = \{z \in \mathbb{C}^* \mid |z| = 1\} = T$

Άρα $\ker\varphi = T \Rightarrow T = \ker\varphi$ είναι υποομάδα του $\mathbb{C}^*$ και μάλιστα κανονική

Έστω $r \in \mathbb{R}^+$ $r = |z| = \varphi(r)$ Άρα $\varphi$ επί
$\in \mathbb{C}^*$

Άρα $\mathbb{C}^*/\ker\varphi \simeq \varphi(\mathbb{C}^*) \Rightarrow \mathbb{C}^*/T \simeq \mathbb{R}^+$

Date. No.

# Φυλλάδιο 9

(4), (5) Βρείτε όλους τους διαιρέτες του μηδενός και όλα τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_2 \times \mathbb{Z}_4$

Λύση:

$([0]_2, [0]_4)$, $([0]_2, [1]_4)$, $([0]_2, [2]_4)$, $([0]_2, [3]_4)$, $([1]_2, [0]_4)$, $([1]_2, [1]_4)$, $([1]_2, [2]_4)$, $([1]_2, [3]_4)$ : ο αντίστροφος ο ίδιος ο εαυτός του

αντιστρέψιμο: ο εαυτός του είναι αντίστροφος εαυτός του

□ : διαιρέτες του μηδενός

○ : αντιστρέψιμα

Θέμα εξετ:

→ Δείξτε ότι η $H = \langle [2]_6, [3]_6 \rangle$ είναι κανονική υποομάδα της $\mathbb{Z}_6 \times \mathbb{Z}_6$ και βρείτε με ποια γνωστή σας ομάδα είναι ισόμορφη η $\mathbb{Z}_6 \times \mathbb{Z}_6 = H$

Λύση: Η είναι η κυκλική ομάδα που παράγεται από το $\langle [2]_6, [3]_6 \rangle$ συνεπώς είναι υποομάδα της αβελιανής $\mathbb{Z}_6 \times \mathbb{Z}_6$ άρα είναι κανονική.

προσθέτω το 2 και το 3

$H = \{([0]_6, [0]_6), ([2]_6, [3]_6), ([4]_6, [0]_6), ([0]_6, [3]_6), ([2]_6, [0]_6), ([4]_6, [3]_6)\}$

Άρα $|\mathbb{Z}_6 \times \mathbb{Z}_6 / H| = \frac{|\mathbb{Z}_6 \times \mathbb{Z}_6|}{|H|} = \frac{36}{6} = 6$

$\mathbb{Z}_6 \times \mathbb{Z}_6 / H = \{([a]_6, [b]_6) + H\}$, $o(([1], [1]) + H) = ?$

1. $(([1], [1]) + H) = (([1], [1]) + H) \neq ([0], [0]) + H$

2 $(([1], [1]) + H) = (([2], [2]) + H) \neq ([0], [0]) + H$

όμοια για 3, 4, 5 θα είναι $\neq ([0], [0]) + H$

$o(([1], [1]) + H) \mid 6 \Rightarrow o(([1], [1]) + H) \in \{1, 3, 3, 6\}$ (× × ×)

Άρα: $o(([1]_6, [1]_6) + H) = 6$ Lagrange

και $\mathbb{Z}_6 \times \mathbb{Z}_6 / H = \langle ([1]_6, [1]_6) + H \rangle$ ⑥

Άρα $Z_6 \times Z_6 / H$ κυκλική $\Rightarrow Z_6 \times Z_6 / H \simeq Z_6$

## Φυλλάδιο 9

5) Έστω $D_1, D_2$ αμέσως περιοχές με: $1_{D_1} \neq 0_{D_1}$ και $1_{D_2} \neq 0_{D_2}$. Δείξτε ότι $D_1 \times D_2$ δεν είναι αμέσως περιοχής.

Λύση:

$$(1_{D_1}, 0_{D_2})(0_{D_1}, 1_{D_2}) = (0_{D_1}, 0_{D_2})$$

$$\neq (0,0)$$

## Φυλλάδιο 7

5) Να δείξετε ότι κάθε στοιχείο $\sigma \in A_n$ $(n \geq 3)$ μπορεί να γραφεί σαν γινόμενο 3-κύκλων

Λύση: $\sigma \in A_n \Rightarrow \sigma = (\tau_1 \tau_2)(\tau_3 \tau_4) \cdots (\tau_{2k-1} \tau_{2k})(\tau_{2k+1} \tau_{2k+2})$

1) $\tau_{2k-1} \tau_{2k} = (i,j)(i,j) = (1,2,3)(1,3,2)$

2) $\tau_{2k-1} \tau_{2k} = (i,j)(i,u) = (i,u,j)$

3) $\tau_{2k-1} \tau_{2k} = (i,j)(u,\ell) = (i,j)(u,\ell)$

$(a,b,t)(a,b,\delta) = (a,t)(b,\delta)$

Άρα το $\tau_{2k-1} \tau_{2k}$ είναι γινόμενο 3-κύκλων.

Συνεπώς το $\sigma = \tau_1 \tau_2 \cdots \tau_{2n-1} \tau_{2n}$ είναι γινόμενο 3-κύκλων.

**Άσκ:** Να εξετάσετε αν η απεικόνιση $\varphi: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}_{21}$ με τύπο $\varphi(u,v) = [7u+15v]_{21}$ είναι ομομορφισμός δακτυλίων. Αν ναι, δείξτε ότι $\ker\varphi = \{(3a,7b) \mid a,b\in\mathbb{Z}\}$

**Λύση:** $\varphi((u_1,v_1)+(u_2,v_2)) = \varphi((u_1+u_2, v_1+v_2)) =$
$= [7(u_1+u_2)+15(v_1+v_2)]_{21} = [7u_1+15v_1]_{21} + [7u_2+15v_2]_{21}$
$= \varphi((u_1,v_1)) + \varphi((u_2,v_2))$

$\varphi((u_1,v_1)\cdot(u_2,v_2)) = \varphi((u_1u_2, v_1v_2)) = [7u_1u_2+15v_1v_2]_{21}$

$\varphi((u_1,v_1))\cdot\varphi((u_2,v_2)) = [7u_1+15v_1]_{21}\cdot[7u_2+15v_2]_{21} =$
$= [49u_1u_2 + 105u_1v_2 + 105v_1u_2 + 225v_1v_2]_{21} = [7u_1u_2+15v_1v_2]_{21}$
$105u_1v_2 \equiv 0 \pmod{21}$, $105v_1u_2 \equiv 0 \pmod{21}$

Άρα $\varphi$ ομομορφισμός δακτυλίων

**Άσκ:** Να εξετάσετε αν η απεικόνιση $\varphi: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}_{21}$ με τύπο $\varphi(u,v) = [7u+15v]_{21}$. Είναι ομομορφισμός δακτυλίων? Αν ναι, δείξτε ότι $\ker\varphi = \{(3a,7b) \mid a,b\in\mathbb{Z}\}$

**Λύση:** (⊃) Έστω $(3a,7b)\in\{(3a,7b)\mid a,b\in\mathbb{Z}\} \Rightarrow \varphi(3a,7b) =$
$= [7\cdot 3a + 15\cdot 7b]_{21}$
Άρα $\{(3a,7b)\mid a,b\in\mathbb{Z}\} \subseteq \ker\varphi = [21a+105b]_{21} = [0]_{21}$

(⊂) Έστω $(u,v)\in\ker\varphi \Rightarrow \varphi(u,v) = [0]_{21} \Rightarrow$
$\Rightarrow [7u+15v]_{21} = [0]_{21} \Rightarrow 7u+15v \equiv 0 \pmod{21} \Rightarrow$
$\Rightarrow 21 \mid 7u+15v$
$3\mid 21$, $21\mid 7u+15v \Rightarrow 3\mid 7u+15v$, $3\mid 15v$ $\Rightarrow 3\mid 7u$
$3\mid 7$ και $3\mid u$ $\Rightarrow$ $\mu\kappa\delta(3,7)=1$ $\Rightarrow 3\mid u$

NO

Date

$7|21 \quad 21|7m+15n \Rightarrow 7|7m+15n$ } $\Rightarrow$
$7|7m$

$\Rightarrow 7|15n$ } $\rightarrow \boxed{7|n}$
$\mu\kappa\delta(7,15)=1$

Άρα $\text{Ker}\, g \subseteq \{(3a,7b) \mid a,b \in \mathbb{Z}\}$

Συνεπώς $\text{Ker}\, g = \{(3a,7b) \mid a,b \in \mathbb{Z}\}$

Άσκ: Βρείτε μια υποομάδα της $S_{11}$ τάξης 28 και δείξτε ότι η $S_{11}$ **δεν** έχει υποομάδα τάξης 17

Λύση: $H = \langle (1,2,3,4)(5,6,7,8,9,10,11) \rangle$

$o((1,2,3,4)(5,6,7,8,9,10,11)) = \text{ελκ}(4,7) = 28$

$(3,8)=1$

- Βρείτε μια υποομάδα της $S_{11}$ τάξης $24 : \not{3} \cdot 8$
-//- -//- $21 : 3 \cdot 7 \cdot 1$

Έστω $H \leq S_{11}$ με $|H| = 17 \xrightarrow{\text{Lagrange}} |H| \,||S_{11}| \Rightarrow$
$\Rightarrow 17 \,|\, 11! = 1 \cdot 2 \cdot 3 \cdots 11$ άτοπο άρα δεν $\exists$ υποομάδα της $S_{11}$ τάξης 17

τάξης 56? $17 \nmid 56$ $7 \cdot 8$ (αλλά $7+8 \neq 11$)
άρα δεν έχει