Επαναληπτικές Ασκήσεις:

ΘΕΩΡΙΑ ΟΜΑΔΩΝ:

Άσκηση 1:

Να αποδείξετε ότι η ομάδα $(\mathbb{Q},+)$ όχι κυκλική. Είναι η ομάδα $(\mathbb{R},+)$ κυκλική;

ΛΥΣΗ

Έστω ότι η ομάδα $(\mathbb{Q},+)$ είναι κυκλική
Τότε $\exists \frac{p}{q} \in \mathbb{Q}$ έτσι ώστε $\mathbb{Q} = <\frac{p}{q}>$ $(q \neq 0)$
Αλλά, $\frac{p}{2q} \in \mathbb{Q} \Rightarrow \frac{p}{2q} \in <\frac{p}{q}>$.
Τότε,

$$\exists k \in \mathbb{Z}: \; k \cdot \frac{p}{q} = \frac{p}{2q} \Rightarrow (k-\tfrac{1}{2})p = 0 \Rightarrow p=0 \text{ ή } k=\frac{1}{2}$$

Έτσι, λοιπόν εάν $p=0 \Rightarrow \mathbb{Q}=\{0\}$ Άτοπο
εαν $k=\frac{1}{2} \Rightarrow k \notin \mathbb{Z}$ Άτοπο
Άρα, πράγματα $(\mathbb{Q},+)$ όχι κυκλική.
Αυτό έχει ως συνέπεια ότι $(\mathbb{R},+)$ όχι κυκλική διότι εαν $(\mathbb{R},+)$ ήταν κυκλική τότε θα έπρεπε (αφού $(\mathbb{Q},+) \leq (\mathbb{R},+)$) η $(\mathbb{Q},+)$ να είναι κυκλική πάω αντίκειται σε αυτό που αποδείξαμε πριν

Άσκηση 2

Να βρείτε το πλήθος των γεννητόρων της κυκλικής ομάδας $\mathbb{Z}_{p \cdot q}$, p,q: πρώτοι, καθώς και το διάγραμμα Hasse των υποομάδων της.

ΛΥΣΗ

Διακρίνουμε δύο περιπτώσεις:
i) Εάν $p \neq q$, τότε $(p,q)=1$
Το πλήθος των γεννητόρων της $\mathbb{Z}_{pq}$, είναι:
$\varphi(pq) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$
Το πλήθος των υποομάδων της $\mathbb{Z}_{pq}$ ούσα κυκλική είναι το πλήθος των διαιρετών του αριθμού $p \cdot q$.
Αυτοί είναι οι εξής τέσσερις: $1, p, q, pq$.

τάξη $p \cdot q$

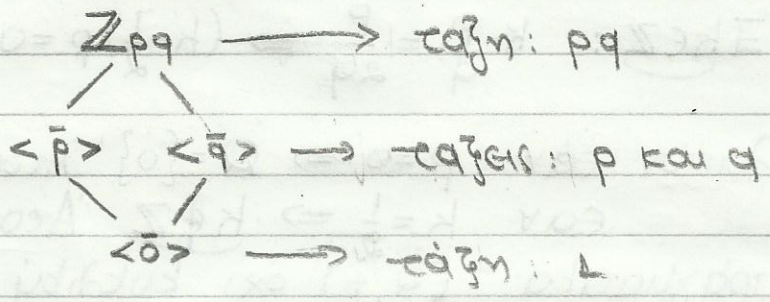
- $H_1 = \langle \bar{1} \cdot \bar{1} \rangle = \langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p \cdot q - 1}\} = \mathbb{Z}_{p \cdot q}$

- $H_2 = \langle \bar{1} \cdot \bar{p} \rangle = \langle \bar{p} \rangle = \mathbb{Z}_p$ ← τάξη p

- $H_3 = \langle \bar{1} \cdot \bar{q} \rangle = \langle \bar{q} \rangle = \mathbb{Z}_q$ ← τάξη q

- $H_4 = \langle \bar{1} \cdot \overline{pq} \rangle = \langle \overline{pq} \rangle = \langle \bar{0} \rangle$ ← τάξη 1

Διάγραμμα Υποομάδων:



ii) Εαν $p = q$ τότε $(p, q) \neq 1$

Το πλήθος των γεννητόρων της $\mathbb{Z}_{pq} = \mathbb{Z}_{p^2}$, είναι:

$\varphi(pq) = \varphi(p^2) = p^{2-1}(p-1) = p(p-1)$

Το πλήθος των υποομάδων της $\mathbb{Z}_{p^2}$, είναι το πλήθος των διαιρετών του p^2.

Αυτοί είναι οι εξής τρεις: $1, p, p^2$

- $H_1 = \langle \bar{1} \cdot \bar{1} \rangle = \langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \ldots, \overline{p^2 - 1}\} = \mathbb{Z}_{p^2}$, τάξη p^2

- $H_2 = \langle \bar{1} \cdot \bar{p} \rangle = \langle \bar{p} \rangle$, τάξη p

- $H_3 = \langle \bar{1} \cdot p^2 \rangle = \langle \overline{p^2} \rangle = \langle \bar{0} \rangle$, τάξη 1

Διάγραμμα Υποομάδων:

$\mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p = \langle \bar{p} \rangle \longrightarrow \langle \bar{0} \rangle$

Άσκηση 3 (Θεωρητική 1)

Έστω $(G,\cdot)$ ομάδα. Να αποδείξετε ότι:

i) Εάν G πεπερασμένη τότε $o(a)=o(a^{-1})$, $\forall a\in G$.

ii) Εάν G άπειρη τότε $o(a)=o(a^{-1})=\infty$, $\forall a\in G$.

ΛΥΣΗ

i) Έστω G πεπερασμένη ομάδα και $a\in G$ τ/ω $o(a)=n \Rightarrow a^n=e$, $n=\min\limits_{k\in\mathbb{N}}\{a\in G: a^k=e\}$

$a^n=e \Rightarrow (a^n)^{-1}=e^{-1}=e \Rightarrow (a^{-1})^n=e \Rightarrow o(a^{-1})\le n=o(a)$

Θα χωρίσουμε τα γνήσια ανισότητα.

Έστω λοιπόν ότι $o(a^{-1})=\lambda<n \Rightarrow (a^{-1})^\lambda=e$ όπου $\lambda=\min\limits_{k\in\mathbb{N}}\{a^{-1}\in G: (a^{-1})^k=e\}$.

Τότε, $\left[(a^{-1})^\lambda\right]^{-1}=e^{-1}=e \overset{G\text{ομαδ.}}{\Longrightarrow} a^\lambda=e$ ενώ $\lambda<n$ πράγμα άτοπο άρα για κάθε $a\in G$ χαρακτηρίζουμε ότι ο ελάχιστος φυσικός με την ιδιότητα $a^k=e$ είναι ο $k=n$. Άρα, αναγκαστικά $o(a^{-1})=o(a)$

ii) Έστω G άπειρη ομάδα και $a\in G$ τ/ω $o(a)=\infty$. Έστω ότι $o(a^{-1})=\lambda \Rightarrow (a^{-1})^\lambda=e \Rightarrow$

$\Rightarrow \left[(a^{-1})^\lambda\right]^{-1}=e^{-1}=e \Rightarrow a^\lambda=e$ άτοπο αφού η υπόθεση δείχνει ότι $o(a)=\infty$, δηλαδή ότι δεν υπάρχει $\lambda\in\mathbb{N}: a^\lambda=e$.

Άσκηση 4 (Θεωρητική 2)

Έστω $(G,\cdot)$ ομάδα πεπερασμένης τάξης και τέτοια ώστε για τυχόν $g\in G$, $o(g)=n$. Τότε, να αποδείξετε ότι $\forall m\in\mathbb{Z}: o(g^k)=\dfrac{n}{(n,k)}$.

ΛΥΣΗ

Έστω $o(g^k)=m \Leftrightarrow (g^k)^m=e$, $m=\min\limits_{\lambda\in\mathbb{Z}}\{g^k\in G:(g^k)^\lambda=e\}$.

Εφόσον, $(g^k)^m=e$ τότε $g^{km}=e$.

Αυτό συνεπάγεται ότι $n\mid km$ όπως $o(g)=n$

Άρα, $\exists\nu\in\mathbb{Z}: km=n\nu$ ① όμως $(n,k)\mid n$ και $(n,k)\mid k \Rightarrow \exists n'$ και k' εν $\mathbb{Z}$: $n'=\dfrac{n}{(n,k)}$ και $k'=\dfrac{k}{(n,k)}$ ώστε $(n',k')=1$.

Αρα, η ① γινεται:
$(n,k)\cdot k'm = (n,k)n'\cdot v \Rightarrow k'm = n'\cdot v \Rightarrow$
$\Rightarrow n' \mid k'm \overset{(n',k')=1}{\Longrightarrow} n' \mid m \Rightarrow \frac{n}{(n,k)} \mid m.$
Απο την αλλη μεριά
$(a^k)^{n/(n,k)} = (a^n)^{k/(n,k)} = e^{k/(n,k)} = e$
και αρα, $m \mid \frac{n}{(n,k)}$ αφου m η ταξη του a^k

Επομενως, $m = \frac{n}{(n,k)}$

Ασκηση 5
Να βρειτε τα στοιχεια ταξης 15 στο $\mathbb{Z}_{45}$.
ΛΥΣΗ
$\mathbb{Z}_{45} = \langle \bar{1} \rangle$ αφου $(1,45)=1$
Αρα, η $\mathbb{Z}_{45}$ σιγουρα κυκλικη (πεπερασμενη)
τοτε $\exists \bar{x} \in \mathbb{Z}_{45} : \bar{x} = n\cdot\bar{1}$, $n \in \mathbb{N}$
Αναζητουμε, εκεινα τα $\bar{x} \in \mathbb{Z}_{45}$: $O(\bar{x}) = 15$
$O(\bar{x}) = O(n\cdot\bar{1}) = \frac{O(1)}{(O(1),n)} \Rightarrow 15 = \frac{45}{(45,n)} \Rightarrow (45,n) = 3 \Rightarrow$

$\Rightarrow (3^2\cdot 5, n) = 3$
Μορφη του n σε πρωτογενεις παραγοντες:
$a = \boxed{3}\cdot 2^{l_2}\cdot \cancel{5}\cdot 7^{l_2}\cdot 11^{l_3}\cdot 13^{l_4}$ Ομως θα ισχυει: $n \le 44$
(3: πανω, 5: οχι)

- $a = 3$.
- $a = 3\cdot 2^{l_1}$, $1 \le l_1 \le 3 \Rightarrow \begin{cases} a = 6 \\ a = 12 \\ a = 24 \end{cases}$
- $a = 3\cdot 7 = 21$
- $a = 3\cdot 11 = 33$
- $a = 3\cdot 2\cdot 7 = 42$

Αρα, τα στοιχεια 3, 6, 12, 21, 24, 33, 42 εχουν ταξη ιση με 15 στην ομαδα $(\mathbb{Z}_{45}, \oplus)$

Άσκηση 6 (Θεωρητική-3)

Έστω $(G,\cdot)$ ομάδα.
Για κάθε $x,a \in G$, να δείξετε ότι: $o(a)=o(x^{-1}ax)$.

ΛΥΣΗ

Έστω $o(a)=n \Rightarrow a^n=e$, $n=\min_k\{a\in G: a^k=e\}$

$(x^{-1}ax)^n=(x^{-1}ax)(x^{-1}ax)\dots(x^{-1}ax)=x^{-1}a^nx=$

$=x^{-1}ex=x^{-1}x=e \Rightarrow o(x^{-1}ax)\le n=o(a)$ ①

Αντίστροφα,

Έστω $o(x^{-1}ax)=\ell \Leftrightarrow (x^{-1}ax)^\ell=e \Leftrightarrow$

$\Leftrightarrow (x^{-1}ax)\dots(x^{-1}ax)=e \Leftrightarrow x^{-1}a^\ell x=e \Leftrightarrow$

$\Leftrightarrow a^\ell=x^{-1}ex=e \Leftrightarrow o(a)\le\ell=o(x^{-1}ax)$ ②

Άρα, από τις ① και ② έπεται το ζητούμενο.

Άσκηση 7

Έστω $(\mathbb{Z},\square)$ που είναι εφοδιασμένο με την πράξη

$a\square b=a+b-1$, $\forall a,b\in\mathbb{Z}$

Να εξεταστεί αν $(\mathbb{Z},\square)$ ομάδα. Εάν ναι, τότε να εξεταστεί αν πρόκειται για κυκλική.

ΛΥΣΗ

Προσεταιριστικότητα: Έστω τυχόντα $a,b,\gamma\in\mathbb{Z}$:

$(a\square b)\square\gamma=(a+b-1)\square\gamma=a+b-1+\gamma-1=a+b+\gamma-2$

$a\square(b\square\gamma)=a\square(b+\gamma-1)=a+b+\gamma-1-1=a+b+\gamma-2$.

Μοναδιαίο στοιχείο: Έστω τυχόντα $a,e\in\mathbb{Z}$:

$a\square e=a\,(=e\square a)\Leftrightarrow a+e-1=a\Leftrightarrow e=1\in\mathbb{Z}$

Αντίστροφος (ή Αντίθετος): Έστω τυχόντα $a,b\in\mathbb{Z}$:

$a\square b=e\,(=b\square a)\Leftrightarrow a+b-1=1\Rightarrow b=2-a\in\mathbb{Z}$

Άρα, η $(\mathbb{Z},\square)$ είναι ομάδα.

Ας υποθέσουμε ότι υπάρχει γεννήτορας x

Επομένως, για κάθε $y\in\mathbb{Z}$: $y=x^k$ $k\in\mathbb{N}\Leftrightarrow$

$y=\underbrace{x\square x\square\dots\square x}_{k\text{ φορές}}$ (1)

$x\square x=2x-1$, $x\square(x\square x)=x\square(2x-1)=3x-2$

Επαγωγικά στο k. Λαμβάνουμε σαν σχέση (1)
$y = kx-(k-1) = kx-k+1 = k(x-1)+1 \Rightarrow k = \frac{y-1}{x-1}$
όποτε θα πρέπει:
1) $x \neq 1$ και 2) $x-1 / y-1$ διότι $k \in \mathbb{N}$
Έτσι, εφόσον οι αριθμοί που παίρνουμε διαιρούν έναν ακέραιο είναι οι αριθμοί: 1 και -1
τότε αναγκαστικά:
$x-1=1$ ή $x-1=-1 \Leftrightarrow x=2$ ή $x=0$
Άρα, πράγματι $(\mathbb{Z}, \square)$ κυκλική και μάλιστα $\mathbb{Z} = \langle 0 \rangle = \langle 2 \rangle$ (πραγμα απόλυτα λογικό αφού οι γεννήτορες του $\mathbb{Z}$ είναι το 1 και το -1 ενώ εδώ η πράξη μας δεν είναι το $\alpha+\beta$ αλλά το $\alpha+\beta-1$, δηλαδή "μετακινούμε" το σύνολο $\mathbb{Z}$ αριστερότερα κατά μία μονάδα και άρα ο γεννήτορας $\langle 1 \rangle$ γίνεται $\langle 1-1 \rangle = \langle 0 \rangle$.)

Άσκηση 8

Δείξτε ότι εαν σ είναι ένας κύκλος περιττού μήκους τότε και σ^2 είναι κύκλος

ΛΥΣΗ

Έστω $\sigma = (a_1, a_2, \dots, a_{2k+1})$
Τότε,
$$\sigma^2 = \sigma \circ \sigma = (a_1, a_2, \dots, a_{2k+1})(a_1, a_2, \dots, a_{2k+1}) =$$
$$= \begin{pmatrix} a_1 & a_2 & \cdots & a_{2k-1} & a_{2k} & a_{2k+1} \\ a_3 & a_4 & \cdots & a_{2k+1} & a_1 & a_2 \end{pmatrix} =$$
$$= (a_1, a_3, \dots, a_{2k-1}, a_{2k+1}, a_2, a_4, \dots, a_{2k})$$
Δηλαδή, η σ^2 είναι ένας κύκλος, διότι πρώτα εξαντλούνται τα στοιχεία με περιττούς δείκτες και στη συνέχεια το τελευταίο (a_{2k+1}) συνδέεται με το πρώτο στοιχείο άρτιου δείκτη (το a_2) οπότε εξαντλούνται όλα τα στοιχεία άρτιου δείκτη και τότε το τελευταίο από αυτά (a_{2k}) γυρνά στο a_1
πχ $\rightarrow$ $(1,2,3,4,5)^2 = (1,3,5,2,4)$

Άσκηση 9 (Θεωρητική 4)

Έστω κύκλος $\sigma=(a_1,a_2,\dots,a_k)$. Να δείξετε ότι: για κάθε $f\in S_n$ είναι $f\sigma f^{-1}=(f(a_1),f(a_2),\dots,f(a_k))$ δηλαδή $f\sigma f^{-1}$ κύκλος μήκους $k\le n$

ΛΥΣΗ

Έστω $f=\begin{pmatrix}1 & 2 & 3 & \dots & n\\ f(1) & f(2) & f(3) & \dots & f(n)\end{pmatrix}$.

Άρα,

$f\sigma f^{-1}=$

$=\begin{pmatrix}1 & 2 & \dots & a_1 & \dots & a_2 & \dots & a_k & \dots & n\\ f(1) & f(2) & \dots & f(a_1) & \dots & f(a_2) & \dots & f(a_k) & \dots & f(n)\end{pmatrix}(a_1,a_2,\dots,a_k)\begin{pmatrix}f(1) & \dots & f(a_1) & \dots & f(a_n) & \dots & f(n)\\ 1 & \dots & a_1 & \dots & a_n & & n\end{pmatrix}$

$=\begin{pmatrix}f(1) & f(2) & \dots & f(a_1) & \dots & f(a_2) & \dots & f(a_k) & \dots & f(n)\\ f(1) & f(2) & \dots & f(a_2) & \dots & f(a_3) & \dots & f(a_1) & \dots & f(n)\end{pmatrix}=$

$=(f(a_1),f(a_2),\dots,f(a_k))$

Δηλαδή, η $f\sigma f^{-1}$ αφήνει αναλλοίωτα όλα τα $f(i)$ $\forall i=a_1,a_2,\dots,a_k$ ενώ μεταθέτει κυκλικώς τα $\alpha_1,\alpha_2,\dots,\alpha_k$.

Άσκηση 10 (Θεωρητικής)

Εαν $aH=bH$ τότε $Ha^{-1}=Hb^{-1}$, $H\le G$, $\forall a,b\in G$

ΛΥΣΗ

$aH=bH\Rightarrow(\forall h\in H)(\exists h'\in H): ah=bh'$

Έχουμε ότι $(ah)(ah)^{-1}=e\Rightarrow(bh')(ah)^{-1}=e\Rightarrow$

$\Rightarrow(ah)^{-1}=(bh')^{-1}\Rightarrow h^{-1}a^{-1}=h'^{-1}b^{-1}\xrightarrow[h^{-1},h'^{-1}\in H]{H\le G}Ha^{-1}=Hb^{-1}$

Παρατήρηση: Αντιστρόφως:

$Ha^{-1}=Hb^{-1}\Rightarrow(\forall h\in H)(\exists h'\in H): ha^{-1}=h'b^{-1}\Leftrightarrow(ha^{-1})^{-1}=(h'b^{-1})^{-1}\Leftrightarrow$

$\Leftrightarrow ah^{-1}=bh'^{-1}$ και αφού κάθε στοιχείο στην H έχει μοναδικό αντίστροφο επεται ότι $Ha=Hb$.

Άσκηση 11 (Θεωρητική 6).

Έαν $H \leq G$

Να αποδείξετε ότι:

Υπάρχουν τόσα αριστερά σύμπλοκα όσα και τα δεξιά σύμπλοκα της υποομάδας H

ΛΥΣΗ

-Έστω η απεικόνιση φ από το σύνολο των αριστερών συμπλόκων στο σύνολο των δεξιών συμπλόκων ορισμένη ως $\varphi(aH) = Ha^{-1}$, $\forall a \in G$

(Το γεγονός ότι στην εικόνα του aH έχουμε το Ha^{-1}. Δεν μας μάγει να χάνουμε πληροφορία αφού γιαθε α έχει μοναδικό αντίστροφο. Δηλαδή, όπως το τυχαίο α "σαρώνει" όλο το G έτσι και το α^{-1}).

Θα αποδείξουμε ότι φ 1-1 και επί απεικόνιση

$\varphi(aH) = \varphi(bH)$ $\forall a, b \in G \Leftrightarrow Ha^{-1} = Hb^{-1} \overset{\text{Άσκ 10}}{\Leftrightarrow} aH = bH$

άρα η φ 1-1. Τέλος, για το δεξιό σύμπλοκο Hb με $b \in G$, υπάρχει αριστερό σύμπλοκο $b^{-1}H$. τέτοιο ώστε $\varphi(b^{-1}H) = Hb$. Άρα, η φ επί

Άσκηση 12

Έστω το σύνολο $G_H = \{g \in G / gHg^{-1} = H\}$, $H \leq G$

i) Νδο $G_H \leq G$

ii) Νδο $H \trianglelefteq G_H$ και ότι η G_H είναι η μεγαλύτερη υποομάδα της G που περιέχει την H ως κανονική υποομάδα

ΛΥΣΗ

i) $e \in G_H \neq \emptyset$ (αφού $g = e \in G \rightarrow eHe^{-1} = H$)

Έστωσαν g_1 και g_2 εν G_H. και Θδο $g_1 \cdot g_2 \in G_H$.

Δηλαδή Θδο $(g_1 g_2) H (g_1 g_2)^{-1} = H$.

Παίρνουμε το πρώτο μέρος:

$g_1 (g_2 H g_2^{-1}) g_1^{-1} = g_1 H g_1^{-1} = H$.

Αρκεί τώρα νδο για τυχόν $g \in G_H \Rightarrow g^{-1} \in G_H$

δηλαδή $g^{-1}H(g^{-1})^{-1} = H$ πράγμα προφανές αφού
$g^{-1}H(g^{-1})^{-1} = g^{-1}Hg \overset{\circledast}{=} H$. Άρα, $G_H \leq G$.

$\circledast$ $gHg^{-1} = H \Rightarrow H = g^{-1}Hg$.

ii) $G_H = \{g \in G / gHg^{-1} = H\}$.
Έστω $g \in G_H$ και $h \in H$ τότε $ghg^{-1} = h' \in H$
άρα εξασφαλίστηκε η κανονικότητα της H
(ή $G_H = \{g \in G / gH = Hg\}$ αφού H κανονική)
Αλλά θα πρέπει $\forall h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$ ώστε $H \leq G_H$
Αυτό προκύπτει άμεσα εάν όπου $g = e$
Άρα, $(ehe)(eh_2e)^{-1} = eh_1h_2^{-1}e = h_1h_2^{-1} \in H$ ούσα η H κανονική. Άρα, H υποομάδα των G_H.
Τελικά, $H \trianglelefteq G_H$.
Έστω τώρα ότι $\exists F \leq G : H \trianglelefteq G_H$ αλλά $H \trianglelefteq F$ και $G_H \subseteq F$. Έστω λοιπόν $f \in F$: $fHf^{-1} = H$ και $f \in G_H$
$\Rightarrow F \subseteq G_H$. Άρα, αναγκαστικά $F = G_H$. Δηλαδή G_H είναι η μοναδική υποομάδα της G που περιέχει την H ως κανονική υποομάδα.

Άσκηση 13 (Θεωρητική 7)
Εάν G αβελιανή και $H \leq G$ τότε και η G/H αβελιανή

ΛΥΣΗ
Αφού G αβελιανή τότε $H \trianglelefteq G$
Συνεπώς ορίζεται η έννοια του σωλίου G/H
με πράξη για κάθε $a, b \in G$: $aH \odot bH = abH$
G αβελιανή και άρα $abH = baH = bH \odot aH$
Συνεπώς και η G/H είναι αβελιανή

Άσκηση 14

Να αποδείξετε ότι $SL(n,\mathbb{R}) \trianglelefteq GL(n,\mathbb{R})$ με τη βοήθεια των ομομορφισμών.

Λύση

Έστω $\varphi : (GL_n(\mathbb{R}), \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$ με τύπο $\varphi(A) = \det A$, $A \in GL_n(\mathbb{R})$ και $\det A \neq 0$

Τότε για δύο τυχόντες αντιστρέψιμους πίνακες A & B

$\varphi(AB) = \det(AB) = \det A \det B = \varphi(A)\varphi(B)$.

Η φ απεικόνιση είναι ομομορφισμός

$\ker(\varphi) = \{A \in GL_n(\mathbb{R}) : \varphi(A) = 1\} =$

$= \{A \in GL_n(\mathbb{R}) : \det A = 1\} = SL_n(\mathbb{R})$

Οπότε η ομομορφισμός τότε: $\ker(\varphi) \trianglelefteq GL_n(\mathbb{R})$

$\parallel$

$SL_n(\mathbb{R})$.

Άσκηση 15 :

Υπάρχει ισομορφισμός $\varphi : (\mathbb{Q}, +) \longrightarrow (\mathbb{Q}^+, \cdot)$;

Λύση

Έστω ότι υπάρχει ισομορφισμός μεταξύ των ομάδων $(\mathbb{Q}, +)$ και $(\mathbb{Q}^+, \cdot)$, έστω ότι: $\varphi(r) = q$ όπου $r \in \mathbb{Q}$ και $q \in \mathbb{Q}^+$ Τότε η απεικόνιση φ είναι επί

δηλαδή $\exists r' \in \mathbb{Q} : \varphi(r') = 2$. ①

Επειτα, $r' = \frac{r'}{2} + \frac{r'}{2} \Rightarrow \varphi(r') = \varphi\left(\frac{r'}{2} + \frac{r'}{2}\right) \overset{\text{ομομ.}}{=}$

$= \varphi\left(\frac{r'}{2}\right) \cdot \varphi\left(\frac{r'}{2}\right) = \varphi\left(\frac{r'}{2}\right)^2$. ②

Άρα, από τη ② στη ① έχουμε:

$\varphi\left(\frac{r'}{2}\right)^2 = 2 \Rightarrow \varphi\left(\frac{r'}{2}\right) = \sqrt{2} \notin \mathbb{Q}^+$ (Σ)

Συνεπώς, καταλήγουμε ότι δεν υπάρχει φ μεταξύ των $(\mathbb{Q}, +)$ και $(\mathbb{Q}^+, \cdot)$

Άσκηση 16 (Θεωρητική 8)

Έστω $\varphi: G \to H$ ομομορφισμός. Τότε νδο:

1) Εάν $T \leq G \Rightarrow \varphi(T) \leq H$

2) Εάν $K \leq H \Rightarrow \varphi^{-1}(K) \leq G$, με $\varphi^{-1}(K) = \{a \in G / \varphi(a) \in K\}$.

3) Εάν $\Delta \trianglelefteq H \Rightarrow \varphi^{-1}(\Delta) \trianglelefteq G$

ΛΥΣΗ: Έστω $\varphi: G \to H$ ομομορφισμός

1) $e_G \in T \Rightarrow \varphi(e_G) = e_H \in \varphi(T) \neq \emptyset$

Έστωσαν τυχόντα x και y στο $\varphi(T) \Rightarrow$

$\Rightarrow x = \varphi(a)$ και $y = \varphi(b)$, $\forall a, b \in T$

Τότε $x \cdot y = \varphi(a)\varphi(b) \overset{\text{ομ.}}{=} \varphi(ab)$, $ab \in T \leq G \Rightarrow$

$\Rightarrow x \cdot y = \varphi(a \cdot b) \in \varphi(T)$ (πράξη κλειστή)

Αν είναι x στο $\varphi(T) \Rightarrow x = \varphi(a)$, $\forall a \in T$.

$x^{-1} = (\varphi(a))^{-1} \overset{\text{ομ}}{=} \varphi(a^{-1})$, $a^{-1} \in T \leq G \Rightarrow$

$\Rightarrow x^{-1} = \varphi(a^{-1}) \in \varphi(T)$. Επομένως, $\varphi(T) \leq H$

2) $\varphi(e_G) \in K \Rightarrow e_G \in \varphi^{-1}(K)$.

Έστωσαν τυχόντα a και b στο $\varphi^{-1}(K) \Rightarrow$

$\Rightarrow \varphi(a)$ και $\varphi(b)$ θα ανήκουν στο $K \leq H \Rightarrow$

$\Rightarrow \varphi(a) \cdot \varphi(b) \in K \Rightarrow \varphi(ab) \in K \Rightarrow ab \in \varphi^{-1}(K)$

Αν είναι a στο $\varphi^{-1}(K) \Rightarrow \varphi(a) \in K \leq H \Rightarrow$

$\Rightarrow \varphi(a)^{-1} \in K \Rightarrow \varphi(a^{-1}) \in K \Rightarrow a^{-1} \in \varphi^{-1}(K)$.

Επομένως, $\varphi^{-1}(K) \leq G$.

3) Έστωσαν τυχόντα $a \in \varphi^{-1}(\Delta)$ και $b \in G$

Θδο $bab^{-1} \in \varphi^{-1}(\Delta) \Leftrightarrow \varphi(bab^{-1}) \in \Delta \Leftrightarrow$

$\Leftrightarrow \varphi(b) \cdot \varphi(a) \varphi(b^{-1}) \in \Delta$.

Αφού, $\varphi(a) \in \Delta$ και $\Delta \trianglelefteq H \Rightarrow$

$\Rightarrow \varphi(b)\varphi(a) \cdot \varphi(b)^{-1} \in \Delta \Rightarrow \varphi(b)\varphi(a)\varphi(b^{-1}) \in \Delta$

Άρα, πράγματι $\varphi^{-1}(\Delta) \trianglelefteq G$.

Άσκηση 17

Αν $H \lhd O$ και $a \in O$, τότε να δείξετε ότι η τάξη του στοιχείου Ha στην O/H διαιρεί την τάξη του a.

Λύση

Γνωρίζουμε ότι αν $\varphi: O \to G$ ομομορφισμός τότε $O(\varphi(a)) \mid O(a)$, $\forall a \in O$

Επομένως, αρκεί να ορίσουμε ομομορφισμό $\varphi': O \to O/H$ τέτοιος ώστε $\varphi(a) = Ha$

Αλλά, για τυχόντα a και b στην O, έχουμε:

$\varphi(a \cdot b) = H(ab) = Ha \odot Hb = \varphi(a) \cdot \varphi(b)$, ομομορφισμός

Άσκηση 18

Δίνεται η ομάδα των τεταρτονίων:

$Q_8 = \{I, -I, k, -k, \lambda, -\lambda, J, -J\}$ όπου

$k = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $\lambda = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $J = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ και I ο μοναδιαίος

Επίσης, δίνεται η γνήσια υποομάδα των $\{I, -I\} = H$

Να εξετάσετε με ποια ομάδα είναι ισομορφη η Q_8/H.

Λύση

Από το θεώρημα του Lagrange: $|Q_8/H| = \frac{|Q_8|}{|H|} = 4$

$O(k) = O(\lambda) = O(J) = 4$. Αλλά Q_8 όχι αβελιανή!

Άρα Q_8 όχι κυκλική. Γενικά, η Q_8 έχει δύο γεννήτορες αλλά συγχρόνως και δύο σχέσεις. (πχ $Q_8 = \langle J, \lambda \rangle$ έτσι ώστε $J\lambda = -k \neq k = \lambda J$ και $J^2 = -I = \lambda^2 \Rightarrow J^4 = I = \lambda^4$).

Εύκολα λοιπόν διαπιστώνουμε ότι $Q_8/H \cong$ V-klein με $\varphi(\pm I) = H = e$, $\varphi(\pm k) = Hk = a$, $\varphi(\pm J) = HJ = b$ και $\varphi(\pm \lambda) = H\lambda = \gamma$. ($\Delta\eta\lambda. \exists \varphi: Q_8/H \xrightarrow{\cong} \{e, a, b, \gamma\}$)

Προφανώς τα στοιχεία ανά δεξιά είναι 4, τα εξής:

$HI = H, Hk, HJ, H\lambda$ (όπου πχ $HJ \odot H\lambda = HJ\lambda = -Hk$)

Άσκηση 19.

Να εξετάσετε αν εφαρμόζεται το 1ο Θεώρημα Ισομορφισμών για τον ομομορφισμό $\varphi: \mathbb{Z}_4 \to \mathbb{Z}_8$. Εάν, όχι, τότε μετασχηματίστε τη φ έτσι ώστε να εφαρμόζεται το 1ο Θεώρημα Ισομορφισμών.

ΛΥΣΗ

Παρατηρούμε ότι η φ δεν είναι επί, διότι δεν υπάρχουν αρκετά στοιχεία στο $\mathbb{Z}_4$ ώστε καθένα να απεικονίζεται μονοσήμαντα σε κάθε στοιχείο του $\mathbb{Z}_8$. Άρα, το 1ο Θεώρημα Ισομορφισμών δεν μπορεί να εφαρμοσθεί.

Παρόλα αυτά θα μετασχηματίσουμε την φ έτσι ώστε να εφαρμόζεται το 1ο Θεώρημα Ισομορφισμών

Έστω $\varphi([1]_4) = [2]_8$ τότε

$\varphi([2]_4) = \varphi([1]_4 \oplus [1]_4) \overset{\varphi \text{ ομομ.}}{=\!=} \varphi([1]_4) \oplus \varphi([1]_4) = [4]_8$

και ομοια $\varphi([3]_4) = [6]_8$ και $\varphi([4]_4 = [0]_4) = [8]_8 = [0]_8$.

Επίσης, $\ker(\varphi) = \{[a]_4 / \varphi([a]_4) = [0]_8\} = \{[0]_4\} \Rightarrow \varphi$ 1-1

Έτσι, έχουμε ότι:

$\varphi(\mathbb{Z}_4) = \{\varphi([0]_4) = [0]_8, \varphi([1]_4) = [2]_8, \varphi([2]_4) = [4]_8, \varphi([3]_4) = [6]_8\}$.

Επομένως, αν περιορίσουμε στον ομομορφισμό:

$\varphi: \mathbb{Z}_4 \to \varphi(\mathbb{Z}_4) = \langle [2]_8 \rangle \leq \mathbb{Z}_8$ τότε καλώς είναι επί

Άρα, εφαρμόζοντας το 1ο Θεώρημα Ισομορφισμών

$\exists \bar{\varphi}: \mathbb{Z}_4 / \ker(\varphi) = \mathbb{Z}_4 \overset{\cong}{\Rightarrow} \varphi(\mathbb{Z}_4)$. Άρα, τελικά $\mathbb{Z}_4 \cong \varphi(\mathbb{Z}_4)$.

Άσκηση 20:

Να δειχθεί ότι η ομάδα πηλίκο $\mathbb{R}/\mathbb{Z} \cong S^1 = \{a+bi / a,b \in \mathbb{R} \text{ και } a^2+b^2=1\}$

ΛΥΣΗ

ΙΔΕΑ: Θα θεωρήσουμε $\varphi: \mathbb{R} \to S^1$ ομομορφισμό και στη συνέχεια θα δείξω $\ker(\varphi) = \mathbb{Z}$ και φ επί

Τότε από 1ο Θεώρημα Ισομορφισμών:

$\exists \bar{\varphi}: \mathbb{R}/\mathbb{Z} = \ker(\varphi) \longrightarrow S^1$ ισομορφισμός

$S^1 = \{a+bi \mid a,b\in\mathbb{Z} \text{ και } a^2+b^2=1\} = \{z\in\mathbb{C} \mid |z|=1\} =$
$= \{\cos 2\pi t + i\sin 2\pi t \mid t\in\mathbb{R}\}$.

Θεωρούμε γνωστον των ακεραίων:

$\varphi: \mathbb{R}\to S^1$ τυπου $\varphi(t) = \cos 2\pi t + i\sin 2\pi t$, $\forall t\in\mathbb{R}$

Εστωσαν $t_1, t_2 \in$ ν $\mathbb{R}$:

$\varphi(t_1+t_2) = \cos 2\pi(t_1+t_2) + i\sin 2\pi(t_1+t_2) =$

$= \cos 2\pi t_1 \cos 2\pi t_2 - \sin 2\pi t_1 \sin 2\pi t_2 + i\sin 2\pi t_1 \cos 2\pi t_2 + i\cos 2\pi t_1 \sin 2\pi t_2 =$

$= (\cos 2\pi t_1 + i\sin 2\pi t_1)\cdot(\cos 2\pi t_2 + i\sin 2\pi t_2) = \varphi(t_1)\cdot\varphi(t_2) \Rightarrow$

$\Rightarrow \varphi$ ομομορφισμος

Η φ επι $\Leftrightarrow (\forall z\in S^1)(\exists t\in\mathbb{R}): \varphi(t) = z$ (ισχυει ς ορισμου)

$\ker(\varphi) = \{t\in\mathbb{R} \mid \varphi(t) = (1,0)\} = \{t\in\mathbb{R} \mid \cos 2\pi t = 1 \ \& \ \sin 2\pi t = 0\}$

$= \{t \mid t\in\mathbb{Z}\} = \mathbb{Z}$. Αρα, απο 1ο Θεωρ. Ισομορφ.

$\exists \bar{\varphi}: \mathbb{R}/\mathbb{Z} \to S^1$ ισομορφια Δηλ. $\mathbb{R}/\mathbb{Z} \cong S^1$.

Ασκηση 21.

Να αποδειξετε οτι:

i) $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$, $\forall n\in\mathbb{N}$

ii) $\mathbb{Z}_{36}/\langle\bar{18}\rangle/\langle\bar{18}\rangle/\langle\bar{36}\rangle \cong \mathbb{Z}_9$

ΛΥΣΗ

i) Εστω: $\varphi: \mathbb{Z}\to\mathbb{Z}_n$ με τυπο $\varphi(k) = k \bmod n$, $k\in\mathbb{Z}$

Η φ προφανως ειναι επι και αφου

$\varphi(k+l) = (k+\lambda) \bmod n = k \bmod n + \lambda \bmod n = \varphi(k)+\varphi(\lambda)$, $\forall k,\lambda\in\mathbb{Z}$

ειναι ομομορφισμος.

Επειτα, $\ker(\varphi) = \{k\in\mathbb{Z} / \varphi(k) = [0]_n\} = \{nk / k\in\mathbb{Z}\} = n\mathbb{Z}$

Αρα, απο το 1ο Θεωρ. Ισομορφισμων:

$\exists \bar{\varphi}: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$, ισομορφισμος

ii) $\mathbb{Z}_{36} \cong \mathbb{Z}/36\mathbb{Z}$, $\langle\bar{18}\rangle = 18\,\mathbb{Z}_{36} \cong {}^{18\mathbb{Z}}/_{36\mathbb{Z}}$

Ετσι, $\mathbb{Z}_{36}/\langle\bar{18}\rangle = \mathbb{Z}/36\mathbb{Z} \,/\, 18\mathbb{Z}/36\mathbb{Z}$. (1)

Επισης, $36\mathbb{Z} \trianglelefteq 18\mathbb{Z} \trianglelefteq \mathbb{Z}$ και $36\mathbb{Z} \trianglelefteq \mathbb{Z}$ (αφου γενικως $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ και αβελιανές).

Τοτε απο το 3ο Θεωρημα Ισομορφισμων

$18\mathbb{Z}/36\mathbb{Z} \trianglelefteq \mathbb{Z}/36\mathbb{Z}$ και μάλιστα στην (1):

$$\frac{\mathbb{Z}/36\mathbb{Z}}{18\mathbb{Z}/36\mathbb{Z}} \cong \mathbb{Z}/18\mathbb{Z} \cong \mathbb{Z}_{18}. \quad (2)$$

Ενας δεύτερος τρόπος να αποδείξουμε την (2) είναι:
$|\mathbb{Z}_{36}/\langle\bar{18}\rangle| = \frac{36}{2} = 18$ συνολικά

$$\mathbb{Z}_{36}/\langle\bar{18}\rangle = \{\langle\bar{18}\rangle, [1]_{36}+\langle\bar{18}\rangle, \ldots, [17]_{36}+\langle\bar{18}\rangle\}$$

όπου:
$([1]_{36}+\langle\bar{18}\rangle)\oplus([1]_{36}+\langle\bar{18}\rangle) = [2]_{36}+\langle\bar{18}\rangle$ Μετά από 17 προσθέσεις
$\Rightarrow \ldots \Rightarrow ([17]_{36}+\langle\bar{18}\rangle)\oplus([1]_{36}+\langle\bar{18}\rangle) = \langle\bar{18}\rangle$
Αφού, $o([1]_{36}+\langle\bar{18}\rangle) = 18 = o([1]_{18})$
Δηλαδή, $[1]_{36}+\langle\bar{18}\rangle \longleftrightarrow [1]_{18}$ ομοια και τα άλλα
Επιπλέον,
$\langle\bar{18}\rangle/\langle\bar{36}\rangle = \langle\bar{0}\rangle = 18\mathbb{Z}_{36}/\langle\bar{0}\rangle$
Αφού, $\langle\bar{0}\rangle \leq 18\mathbb{Z}_{36}$ και $[18\mathbb{Z}_{36} : \langle\bar{0}\rangle] = 2$
τότε $\langle\bar{0}\rangle \trianglelefteq 18\mathbb{Z}_{36}$ και μαλιστα $18\mathbb{Z}_{36}/\langle\bar{0}\rangle \cong \mathbb{Z}_2$
Αλλά, το αρχικό πηλίκο που μας δοθηκε προς αποδειξη τελικα είναι ισομορφο με την $\mathbb{Z}_{18}/\mathbb{Z}_2$ όπου ΠΡΟΣΟΧΗ δεν ορίζεται αφου η $\mathbb{Z}_2 \not\leq \mathbb{Z}_{18}$ (ούτε και $\leq$).
Έτσι, παιρνουμε την ομαδα $9\mathbb{Z}_{18} \leq \mathbb{Z}_8$.
και παράλληλα $9\mathbb{Z}_{18} \cong \mathbb{Z}_2$ αρα τελικα θα προκύψει το πηλίκο:
$\mathbb{Z}_{18}/9\mathbb{Z}_{18}$ το οποίο πραγματι είναι ισομορφο με την ομάδα $\mathbb{Z}_9$.

Άσκηση 22
Να βρείτε όλες τις μη ισόμορφες αβελιανες ομάδες τάξης 900 και να τις συμπτύξετε κατά το δυνατον
ΛΥΣΗ
$|G| = 900 = 2^2 \cdot 3^2 \cdot 5^2$, $n_1 = n_2 = n_3 = 2$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$

Π: πλήθος διαμερίσεων

Το πλήθος είναι: $\Pi(2)\cdot\Pi(2)\cdot\Pi(2) = 2\cdot 2\cdot 2 = 8$

Οπότε:

- $G \cong \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \cong \mathbb{Z}_{900}$
- $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25} \cong \mathbb{Z}_2 \times \mathbb{Z}_{450}$
- $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \cong \mathbb{Z}_3 \times \mathbb{Z}_{300}$
- $G \cong \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \cong \mathbb{Z}_5 \times \mathbb{Z}_{180}$
- $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \cong \mathbb{Z}_6 \times \mathbb{Z}_{150}$
- $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10} \times \mathbb{Z}_{90}$
- $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15} \times \mathbb{Z}_{60}$
- $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \cong \mathbb{Z}_{30} \times \mathbb{Z}_{30}$

ΘΕΩΡΙΑ ΔΑΚΤΥΛΙΩΝ:

Άσκηση 23

Ποια από τα παρακάτω σώματα αποτελούν δακτύλιους;

α) $R = \{\alpha + \beta\sqrt{3} \mid \alpha, \beta \in \mathbb{Z}\}$ πρόσθεση, πολ/μος στο $\mathbb{R}$.

β) $R = \{\frac{p}{q} \mid q \in \mathbb{Q} \mid q : \text{περιττός}\}$ -//- , -//- στο $\mathbb{Q}$

γ) $R = \{A \in M(2,\mathbb{R}) / \det A = 0\}$ -//- , -//- στο $M(2,\mathbb{R})$.

ΛΥΣΗ

Γνωρίζουμε ότι $(R,+,\cdot)$ είναι δακτύλιος εαν

1) $(R,+)$ αβελιανή ομάδα, 2) $(R,\cdot)$ ημιομάδα

3) Ισχύει ο επιμεριστικός νόμος

Λόγω ότι με τον ορισμό αυτό η μεθοδος είναι χρονοβόρα έχουμε διατυπώσει το θεώρημα:

$R \leq \mathcal{O}_2$, $\mathcal{O}_2$: δακτύλιος αν, ν $\forall r_1, r_2 \in R$: $r_1 - r_2 \in R$ & $r_1 \cdot r_2 \in R$

α) Έστωσαν, $r_1, r_2 \in R$.

$$r_1 - r_2 = (\alpha_1 + \beta_1\sqrt{3}) - (\alpha_2 + \beta_2\sqrt{3}) = \underbrace{(\alpha_1 - \alpha_2)}_{\in \mathbb{R}} + \underbrace{(\beta_1 - \beta_2)}_{\in \mathbb{R}}\sqrt{3} \in R$$

$$r_1 \cdot r_2 = (\alpha_1 + \beta_1\sqrt{3})\cdot(\alpha_2 + \beta_2\sqrt{3}) = \alpha_1\alpha_2 + 3\beta_1\beta_2 + (\alpha_1\beta_2 + \alpha_2\beta_1)\sqrt{3} \in R$$

Και όπως $(\mathbb{R},+,\cdot)$ δακτύλιος (και μάλιστα σώμα)

Το R θα είναι υποδακτύλιος του $\mathbb{R}$ $\Rightarrow$

$\Rightarrow R$ θα είναι και δακτύλιος

β) Έστωσαν $r_1, r_2 \in R \rightsquigarrow r_1 = \frac{p_1}{q_1}$, q_1: περ. $r_2 = \frac{p_2}{q_2}$, q_2: περ.

$r_1 - r_2 = \frac{p_1}{q_1} - \frac{p_2}{q_2} = \frac{p_1 q_2 - q_1 p_2}{q_1 q_2} \in R$ (αφού $q_1 \cdot q_2$: περιττός)

$r_1 \cdot r_2 = \frac{p_1}{q_1} \cdot \frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2} \in R$ (αφού $q_1 q_2$: περιττός)

Οπότε $(\mathbb{Q}, +, \cdot)$ δακτύλιος (και μάλιστα σώμα)
τότε $R \leq \mathbb{Q}$. $\Rightarrow R$ δακτύλιος

γ) Έστωσαν $A, B \in R \rightsquigarrow \det A = 0$ και $\det B = 0$, $A, B \in M(2, R)$
Έαν $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ και $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ τότε

$A + B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ όπου $\det(A+B) = 1 \neq 0$, $A+B \notin R$

άρα η πράξη δεν είναι καλά ορισμένη
συνεπώς το R σε τούτη την περίπτωση δεν
αποτελεί δακτύλιο (ούτε υποδακτύλιο του $M(2,R)$)

Άσκηση 24

Στο δακτύλιο $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ να βρείτε όλες τις μονάδες
τους μηδενοδιαιρέτες, τα μηδενοδύναμα στοιχεία. Επειτα
να βρείτε όλα τα πρώτα και μεγιστα ιδεώδη.

ΛΥΣΗ

$\mathbb{Z}_2 \oplus \mathbb{Z}_4 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{0},\bar{3}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2}), (\bar{1},\bar{3})\}$

ΜΟΝΑΔΕΣ: Για τυχόν $(\alpha, \beta) \in \mathbb{Z}_2^* \oplus \mathbb{Z}_4^*$, αναζητούμε
στοιχείο $(\alpha', \beta') \in \mathbb{Z}_2 \oplus \mathbb{Z}_4$: $(\alpha, \beta) \cdot (\alpha', \beta') = (1,1)$
($\mathbb{Z}_2 \oplus \mathbb{Z}_4$ πραφανώς μοναδιαίος δακτύλιος με $(\bar{1},\bar{1})$ μοναδιαίο)
$\Rightarrow (\alpha\alpha', \beta\beta') = (1,1) \Rightarrow \alpha\alpha' = 1$ και $\beta\beta' = 1$, $\forall \alpha, \alpha' \in \mathbb{Z}_2, \beta, \beta' \in \mathbb{Z}_4$
$\Rightarrow (\alpha = 1 \ \& \ \alpha' = 1)$ και $[(\beta = 1 \ \& \ \beta' = 1) \text{ ή } (\beta = 3 \ \& \ \beta' = 3)]$
Άρα, οι μοναδιτές μοναδες είναι τα στοιχεία:
$(\bar{1},\bar{1})$ και $(\bar{1},\bar{3})$.

ΜΗΔΕΝΟΔΙΑΙΡΕΤΕΣ: Για τυχόν $(a,b)\in \mathbb{Z}_2\oplus\mathbb{Z}_4-\{(0,0)\}$, αναζητούμε στοιχείο $(a',b')\in \mathbb{Z}_2\oplus\mathbb{Z}_4-\{(0,0)\}$: $(a,b)(a',b')=(0,0) \Rightarrow$
$\Rightarrow (aa', bb')=(0,0) \Rightarrow aa'=0$ & $bb'=0 \Rightarrow$ ($b,b'\in\mathbb{Z}_4$)
$\Rightarrow (a,a'\in\mathbb{Z}_2 : a=0$ ή $a'=0)$ & $(b=0$ ή $b'=0$ και $2\cdot 2=0)$
Επομένως, έχουμε τους μηδενοδιαιρέτες:
$(0,b)$, $b\in\mathbb{Z}_4$, $(a,0)$, $a\in\mathbb{Z}_2$ και το στοιχείο $(1,2)$.

ΜΗΔΕΝΟΔΥΝΑΜΑ: Για τυχόν $(a,b)\in(\mathbb{Z}_2\oplus\mathbb{Z}_4)-\{(0,0)\}$ αναζητούμε
$n\in\mathbb{N}$: $(a,b)^n=(0,0) \Rightarrow a^n=0$ και $b^n=0$
Μοναδική περίπτωση το στοιχείο : $(0,2)$ τέτοιο ώστε
$(0,2)\cdot(0,2)=(0,4)\equiv(0,0)$
Μηδενοδύναμο στοιχείο το $(0,2)$.

Επειτα, αναζητούμε όλα τα ιδεώδη του $\mathbb{Z}_2\oplus\mathbb{Z}_4$ (Αντιμεταθετικού Μοναδιαίου)
Εύκολα βλέπουμε ότι αυτά είναι:
$\{[0]_2\}\oplus\{[0]_4\}$, $\{[0]_2\}\oplus 2\mathbb{Z}_4$, $\{[0]_2\}\oplus\mathbb{Z}_4$, $\mathbb{Z}_2\oplus\{[0]_4\}$,
$\mathbb{Z}_2\oplus 2\mathbb{Z}_4$, $\mathbb{Z}_2\oplus\mathbb{Z}_4$.

Πρώτα-Μεγιστα ιδεώδη
Προφανώς (Ε} οριόμου) το $\{[0]_2\}\oplus\{[0]_4\}$ όχι πρώτο αλλά, ούτε και μεγιστο (αφού δεν είναι κύριο)
Επισης το $\mathbb{Z}_2\oplus\mathbb{Z}_4$ δεν είναι μεγιστο (αφου δεν είναι κύριο) και ούτε πρώτο (Ε} οριόμου του)
Για τα ιδεώδη $I=\{[0]_2\}\oplus\mathbb{Z}_4$ και $J=\mathbb{Z}_2\oplus\{[0]_4\}$
παρατηρούμε ότι είναι κύρια ομως, το J όχι μεγιστο αφού $J\leq\mathbb{Z}_2\oplus 2\mathbb{Z}_4\leq\mathbb{Z}_2\oplus\mathbb{Z}_4$, ενώ το I είναι μεγιστο αφου το μεσως επομενο του είναι το $\mathbb{Z}_2\oplus\mathbb{Z}_4$. Αυτό, έχει ως συνέπεια το I να είναι πρώτο ιδεώδες (αφού $\mathbb{Z}_2\oplus\mathbb{Z}_4$ αντιμεταθετικός μοναδιαίος δακτύλιος). Όσο για το J δεν είναι πρώτο διότι επιλέγοντας το στοιχείο $([1]_2,[2]_4)\in\mathbb{Z}_2\oplus\mathbb{Z}_4$ παρατηρούμε ότι:
$([1]_2,[2]_4)\cdot([1]_2,[2]_4)=([1]_2,[0]_4)\in\mathbb{Z}_2\oplus\{[0]_4\}$ αλλά

$([1]_2, [2]_4) \notin \mathbb{Z}_2 \oplus \{[0]_4\}$.
Για το ιδεώδες $\{[0]_2\} \oplus 2\mathbb{Z}_4$ δεν είναι μέγιστο διότι
$\{[0]_2\} \oplus 2\mathbb{Z}_4 \leq \{[0]_2\} \oplus \mathbb{Z}_4 \leq \mathbb{Z}_2 \oplus \mathbb{Z}_4$.
Επίσης, όχι πρώτο αφού:
$([0]_2, [3]_4) \cdot ([1]_2, [2]_4) = ([0]_2, [2]_4) \in \{[0]_2\} \oplus 2\mathbb{Z}_4$
αλλά αριστερά δεν ανήκουν στο $\{[0]_2\} \oplus 2\mathbb{Z}_4$
Έπειτα, το σώμα $\mathbb{Z}_2 \oplus 2\mathbb{Z}_4$ είναι προφανώς μέγιστο αφού είναι μικρό και το αμέσως επόμενο που το περιέχει ως ιδεώδες είναι το $\mathbb{Z}_2 \oplus \mathbb{Z}_4$. Το γεγονός αυτό συνεπάγεται ότι το $\mathbb{Z}_2 \oplus 2\mathbb{Z}_4$ είναι πρώτο ιδεώδες

Άσκηση 25:
Να αποδείξετε ότι το σώμα
$R = \{q \in \mathbb{Q} : q = \frac{m}{2n+1}, m, n \in \mathbb{Z}\}$ είναι αντιμεταθετικός και μοναδιαίος δακτύλιος με τις συνήθεις πράξεις προσθέσεως και πολ/μου ρητών.
Έπειτα να βρείτε ένα μέγιστο ιδεώδες του σώματος R.

Λύση
Καταρχάς $R \subseteq \mathbb{Q}$ (αφού $\frac{1}{2} \notin R$)
Εφόσον, για τυχόντα $q_1, q_2 \in R$:
- $q_1 + q_2 = \frac{m_1}{2n_1+1} + \frac{m_2}{2n_2+1} = \frac{m_1(2n_2+1) + m_2(2n_1+1)}{(2n_1+1)(2n_2+1)} \in R$
- $q_1 \cdot q_2 = \frac{m_1}{2n_1+1} \cdot \frac{m_2}{2n_2+1} = \frac{m_1 \cdot m_2}{(2n_1+1)(2n_2+1)} \in R$

Τότε, $(R, +, \cdot) \leq (\mathbb{Q}, +, \cdot) \Rightarrow (R, +, \cdot)$ δακτύλιος
Η αντιμεταθετικότητα ισχύει στους ρητούς
Υπάρχει μοναδιαίο στοιχείο (το 1 προφανώς)
Έστω το ιδεώδες $I \lhd R$
$I = \{\frac{3k}{2n+1}, k, n \in \mathbb{Z}\} \lhd R$ με πράξη κλειστή και επίσης ιδεώδες διότι:

για τυχόν $q \in R$ και $q' \in I \Rightarrow$

$$\Rightarrow \frac{m}{2n+1} \cdot \frac{3k}{2n'+1} = 3\frac{mk}{(2n+1)(2n'+1)} \in I$$

Ας υποθέσουμε ότι το I όχι μέγιστο

Τότε $\exists J : I \subsetneq J \subsetneq R$

Άρα, $I \subsetneq J \Rightarrow \exists a \in J$ και $a \notin I \Rightarrow \exists \frac{m}{2n+1} \in J - I \Rightarrow$

$\Rightarrow m \notin 3\mathbb{Z} \Rightarrow m \in \mathbb{Z} - 3\mathbb{Z} \Rightarrow m \neq 3k, k \in \mathbb{Z}$

$\Rightarrow m = 3k+1$ ή $m = 3k+2$, $k \in \mathbb{Z}$

- $m = 3k+1 \rightarrow \frac{3k+1}{2n+1} \in J$ } J ιδεωδ. $\Rightarrow \frac{3k+1}{2n+1} - \frac{3k}{2n+1} \in J$

αλλά $I \subsetneq J \Rightarrow \frac{3k}{2n+1} \in J$

$\Rightarrow \frac{1}{2n+1} \in J \xrightarrow{J \text{ ιδεωδ.}} (2n+1)\frac{1}{2n+1} = 1 \in J \Rightarrow$

$\Rightarrow \forall r \in R: r = r \cdot 1 \in J \Rightarrow r \in J \Rightarrow R \subseteq J \xrightarrow{J \subseteq R} J = R$

πράγμα άτοπο άρα υποθέσαμε ότι I όχι μέγιστο

Άσκηση 26

Ν.δ.ο $\varphi : \mathbb{Z} \oplus \mathbb{Z} / \{0\} \oplus \mathbb{Z} \rightarrow \mathbb{Z}$ είναι ισομορφισμός δακτυλίων.

ΛΥΣΗ

Έστω $f : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}$ τ.ω.τ. $f(n,m) = n$

Για τυχόντα (n,m) & $(k,l) \in \mathbb{Z} \oplus \mathbb{Z}$

- $f((n,m)+(k,l)) = f(n+k, m+l) = n+k =$
$= f(n,m) + f(k,l)$
- $f((n,m)\cdot(k,l)) = f(nk, ml) = nk =$
$= f(n,m) \cdot f(k,l)$

Άρα, f ομομορφισμός μεταξύ των $\mathbb{Z} \oplus \mathbb{Z}$ και $\mathbb{Z}$

Επίσης, f επιμορφισμός (εξ ορισμού του)

$\ker(f) = \{(n,m) \in \mathbb{Z} \oplus \mathbb{Z} / f(n,m) = 0_{\mathbb{Z}}\} =$
$= \{(0,m) / m \in \mathbb{Z}\} = \{0\} \oplus \mathbb{Z}$. Άρα, από το 1ο Θ. ισομ.

των δακτυλίων $\exists \varphi: \mathbb{Z}\oplus\mathbb{Z}/\ker(f)=\{0\}\oplus\mathbb{Z} \to \mathbb{Z}$ ισομορφισμός δακτυλίων.

Παρατήρηση: Δηλαδή, $\mathbb{Z}\oplus\mathbb{Z}/\{0\}\oplus\mathbb{Z} \cong \mathbb{Z}$
Ο $\mathbb{Z}$ δακτύλιος είναι ακέραια περιοχή αλλά όχι σώμα. Άρα, το ιδεώδες $\{0\}\oplus\mathbb{Z}$ είναι πρώτο αλλά όχι μέγιστο.

Άσκηση 27:
Να βρείτε ένα μη τετριμμένο γνήσιο (δηλ. κύριο) ιδεώδες του δακτυλίου $\mathbb{Z}\oplus\mathbb{Z}$ το οποίο δεν είναι πρώτο.

Λύση
Ουσιαστικά αναζητούμε ιδεώδες $I \lhd \mathbb{Z}\oplus\mathbb{Z}$ έτσι ώστε ο δακτύλιος πηλίκο $\mathbb{Z}\oplus\mathbb{Z}/I$ να μην είναι ακέραια περιοχή, δηλ. να έχει μηδενοδιαιρέτες. Για αυτό το σκοπό θεωρούμε το σύνολο $2\mathbb{Z}\oplus 3\mathbb{Z} = \{(2k,3l) \in \mathbb{Z}\oplus\mathbb{Z} \mid k,l\in\mathbb{Z}\}$ το οποίο από τον ορισμό είναι ιδεώδες του $\mathbb{Z}\oplus\mathbb{Z}$
Ορίζουμε την απεικόνιση
$\varphi: \mathbb{Z}\oplus\mathbb{Z} \to \mathbb{Z}_2\oplus\mathbb{Z}_3$ τύπου $\varphi(n,m)=([n]_2,[m]_3)$
η οποία είναι ομομορφισμός (ορισμός) και επί
Επίσης, $\ker(\varphi)=\{(n,m)\in\mathbb{Z}\oplus\mathbb{Z} / \varphi(n,m)=([0]_2,[0]_3)\} =$
$= \{(n,m)\in\mathbb{Z}\oplus\mathbb{Z} / ([n]_2,[m]_3)=([0]_2,[0]_3)\} =$
$= \{(n,m)\in\mathbb{Z}\oplus\mathbb{Z} / [n]_2=[0]_2 \ \& \ [m]_3=[0]_3\} =$
$= \{(n,m)\in\mathbb{Z}\oplus\mathbb{Z} / 2/n \text{ και } 3/m\} = 2\mathbb{Z}\oplus 3\mathbb{Z}$
Έτσι, από το 1ο Θεώρημα Ισομορφισμών
$\exists \bar{\varphi}: \mathbb{Z}\oplus\mathbb{Z}/\ker(\varphi)=2\mathbb{Z}\oplus 3\mathbb{Z} \longrightarrow \mathbb{Z}_2\oplus\mathbb{Z}_3$ ισομορφισμός
Δηλαδή,

$$\mathbb{Z}_2\oplus\mathbb{Z}_3 \cong \mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus 3\mathbb{Z}$$

$(\bar{1},\bar{0})(\bar{0},\bar{1})=(\bar{0},\bar{0})$

Άρου, $\mathbb{Z}_2\oplus\mathbb{Z}_3$ όχι ακέραια περιοχή τότε $2\mathbb{Z}\oplus 3\mathbb{Z}$ όχι πρώτο αλλά μόνο ιδεώδες του $\mathbb{Z}\oplus\mathbb{Z}$

Άσκηση 28 (Θεωρητική)

Να αποδείξετε ότι:

R/I δεν έχει μηδενοδιαιρέτες αν. ν I πρώτο ιδεώδες

ΛΥΣΗ

($\Rightarrow$): Έστω R/I δεν έχει μηδενοδιαιρέτες και ας υποθέσουμε ότι I όχι πρώτο ιδεώδες του R

τότε $\forall r_1, r_2 \in R$ με $r_1 \cdot r_2 \in I \Rightarrow r_1 \notin I$ και $r_2 \notin I \Rightarrow$

$\Rightarrow (r_1 + I) \neq I \neq (r_2 + I)$.

Όμως, $(I+r_1)\cdot(I+r_2) = I + r_1 r_2 \overset{r_1 r_2 \in I}{=} I$ πραγμα

άτοπο αφού R/I δεν έχει μηδενοδιαιρέτες

($\Leftarrow$): Έστω I πρώτο ιδεώδες του R και ας υποθέσουμε ότι R/I έχει μηδενοδιαιρέτες

τότε $(\forall I + r_1 \overset{\neq I}{\in} R/I)\ (\exists I + r_2 \overset{\neq I}{\in} R/I) : (I+r_1)(I+r_2) = I$

$\Rightarrow I + r_1 r_2 = I \overset{\text{πρώτο}}{\Rightarrow} r_1 \in I$ ή $r_2 \in I \Rightarrow I + r_1 = I$ ή

$I + r_2 = I$ άτοπο αφού και οι δύο είναι $\neq I$ από την υπόθεση

Άσκηση 29

Έστω $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R} \right\}$

i) Να δείξετε ότι R με την πρόσθεση και τον πολ/μο των πινάκων αποτελεί δακτύλιο

ii) Να δείξετε ότι $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a,b \in \mathbb{R} \right\}$ είναι πρώτο και μεγιστο ιδεώδες του δακτυλίου R.

ΛΥΣΗ

i) $R \subseteq M(2,\mathbb{R})$ καθώς $M(2,\mathbb{R})$ δακτύλιος

Με έναν απλό έλεγχο οι πράξεις $(+,\cdot)$ είναι καλά ορισμένες στο R οπότε $R \leq M(2,R) \Rightarrow R$ δακτύλιος

ii) Εξετάζουμε εαν $I \lhd R$. Εύκολα, φαίνεται ότι

$\forall A_{2\times 2} \in I$ και $B_{2\times 2} \in R$: $A_{2\times 2} \cdot B_{2\times 2}$ και $B_{2\times 2} \cdot A_{2\times 2}$ ανήκουν στο $I \Rightarrow I \lhd R$

Θδο I μεγιστο ⇔ πρωτο ιδεώδες του R

α' τρόπος:

Έστω $\varphi: R \to \mathbb{R}$ τύπου $\varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = c$ ο που προφανώς είναι ένας επιμορφισμός.

Επίσης, $\ker(\varphi) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R \,/\, \varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = 0 = c \right\} = I$

Ταυτόσημα, από το πρώτο θεώρημα ισομορφισμών $\exists \bar{\varphi}: R/I \xrightarrow{\cong} \mathbb{R}$. Δηλαδή, $R/I \cong \mathbb{R}$ σώμα και R ένας αντιμεταθετικός-Μοναδιαίος δακτύλιος. Τότε, επεται ότι το I μεγιστο $\Rightarrow$ I πρωτο

β' τρόπος

Έστω ότι I όχι μεγιστο ιδεώδες του R

άρα $\exists J: I \subsetneq J \subsetneq R \Rightarrow \exists X: X \in J - I \Rightarrow$

$\Rightarrow X = \begin{pmatrix} \alpha & b \\ 0 & c \neq 0 \end{pmatrix}$ αλλά το στοιχείο $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in J$.

Τότε, όντας J ιδεώδες έχουμε

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in J \Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} \in J.$$

Το J ιδεώδες και άρα

$$\begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{c} \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in J$$

$\in J$

Το J ιδεώδες και άρα

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in J$$

Αλλα, τότε είχαμε δει πριν ότι $J = R$ πραγμα άτοπο αφού υποθέσαμε ότι I όχι μεγιστο

Άρα, I μεγιστο του R.

Το ότι I πρωτο ελέγχεται αμέσως εξ ορισμού:

Θυμίζουμε: I πρωτο $\Leftrightarrow (\forall r_1, r_2 \in R): r_1 \cdot r_2 \in I \Rightarrow r_1 \in I$ ή $r_2 \in I$

Άσκηση 30

Να εξεταστεί εάν τα πολυώνυμα

i. $p(x) = x^3+2x^2+2x+1 \in \mathbb{Z}_3[x]$

ii. $q(x) = x^4+1 \in \mathbb{Q}[x]$ και στον $\mathbb{R}[x]$

είναι ανάγωγα. Να αναλυθούν πλήρως.

ΛΥΣΗ

i. $p(x) = x^3+2x^2+2x+1 \equiv x^3-x^2-x+1 =$

$= x^2(x-1)-(x-1) = (x-1)(x^2-1) \equiv$

$\equiv (x+2)(x^2+2) \equiv (x+2)(x^2-1) =$

$= (x+2)(x-1)(x+1) \equiv (x+2)(x+2)(x+1) =$

$= (x+2)^2(x+1)$. Άρα, το $p(x) \in \mathbb{Z}_3[x]$ μη ανάγωγο

ii. Το κριτήριο Eisenstein μας αναφέρει ότι αν $q(x) = a_0+a_1x+\dots+a_nx^n \in \mathbb{Z}[x]$ και p πρώτος τ/ω $p \mid a_i$, $i=1,2,\dots,n-1$ αλλά $p \nmid a_n$, $p^2 \nmid a_0$ τότε το $q(x)$ ανάγωγο.

Εδώ δεν μπορούμε να το χρησιμοποιήσουμε το συγκεκριμένο κριτήριο.

Έστω λοιπόν ότι δεν είναι ανάγωγο $\Rightarrow$

$\Rightarrow q(x) = g(x) \cdot h(x)$.

Για $x = x+1$

$q(x+1) = g(x+1)h(x+1) \Rightarrow q(x+1) = (x+1)^4+1 \Rightarrow$

$\Rightarrow q(x+1) = x^4+\binom{4}{1}x^3 \cdot 1 + \binom{4}{2}x^2 \cdot 1^2 + \binom{4}{3}x \cdot 1^3 + 1^4 + 1 \Rightarrow$

$\Rightarrow q(x+1) = x^4+4x^3+6x^2+4x+2$

Παρατηρούμε ότι για $p=2$ πληρείται το παραπάνω κριτήρια άρα το $q(x+1)$ ανάγωγο, άρα και το $q(x)$ ανάγωγο.

iii. Ανάγωγα πολυώνυμα στον $\mathbb{R}[x]$ είναι τα πρωτοβάθμια και τα δευτεροβάθμια μόνο! Μελετώντας το:

Έστω ότι δεν είναι ανάγωγο: $q(x) = (x^2+ax+\beta)(x^2+a'x+\beta') \Rightarrow$

$\Rightarrow x^4+1 = x^4+(\alpha+\alpha')x^3+(\beta'+\beta+\alpha\alpha')x^2+(\alpha\beta'+\alpha'\beta)x+\beta\beta'$

$\Rightarrow \dots \Rightarrow$ τελικά $x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$