24/2/20

Εύδοξος: Μαλιάκας - Ταλέλη

Επανάληψη:

Ορισμός: Ένα σύνολο $(G,*)$ με μία διμελής πράξη $*$

$*: G \times G \to G$ καλείται ομάδα

$(x,y) \longmapsto x*y$

i) η $*$ προσεταιριστική: $(a*\beta)*\gamma = a*(\beta*\gamma)$, $\forall a,\beta,\gamma \in G$

ii) $\exists e \in G$: $x*e = e*x = x$, $\forall x \in G$ (ουδέτερο προσθετικό)

iii) $\forall a \in G$, $\exists \underset{\text{συμβολισμός}}{a^{-1}} \in G$: $a*a^{-1} = a^{-1}*a = e$

Αν επιπλέον $x*y = y*x$, $\forall x,y \in G$, η G καλείται αβελιανή.

Παρατήρηση:

1) Αντίστροφο, ουδέτερο είναι μοναδικά

2) Αν πχ $(\mathbb{Z},+) \Rightarrow 2^4 = 2+2+2+2 = 8$

3) ομάδες: $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{C},+)$, $(\mathbb{Z},+)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$

όχι ομάδες: $(\mathbb{Z}^*,\cdot)$, $(\mathbb{N},+)$ — αν $\mathbb{N} \setminus \{0\} \Rightarrow \nexists e$

(χαλάει η 3η ιδιότ $2 \in \mathbb{Z}$, $\frac{1}{2} \notin \mathbb{Z}$) — πχ $2 \in \mathbb{N}$ αλλά $2^{-1} = -2 \notin \mathbb{N}$

Ορισμός: Δακτύλιος ορίζεται ένα σύνολο R εφοδιασμένο με δύο πράξεις $(R, \underbrace{+,\cdot}_{\text{συμβολισμός}})$ όπου:

i) $(R,+)$ αβελιανή ομάδα

ii) η $\cdot$ να είναι προσεταιριστική: $x\cdot(y\cdot z) = (x\cdot y)\cdot z$, $\forall x,y,z \in R$

iii) $x\cdot(y+z) = x\cdot y + x\cdot z$ (και $(x+y)\cdot z = x\cdot z + y\cdot z$), $\forall x,y,z \in R$

(iv) $\exists 1_R \in R$: $x\cdot 1_R = 1_R \cdot x = x$, $\forall x \in R$)

(*) κανονικά αν ένας δακτ έχει μοναδιαίο, θα λέμε δίνεται R με 1_R

πχ ο $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ δεν έχει μοναδιαίο αν $\exists\, 1_{\mathbb{Z}_2} = 2k \Rightarrow \underset{1_R}{(2k)}\, \underset{x}{2\lambda} = \underset{x}{2\lambda}$, $\forall x \in R$

δηλ $\forall \lambda \in \mathbb{Z}$.

ισχύει $\forall \lambda \Rightarrow$ άρα και για $\lambda = 1 \Rightarrow 2k = 1 \Rightarrow k = \frac{1}{2}$ άτοπο.

$\left\{\begin{array}{l} \text{προσθ. ουδ } 0_R \\ \text{πολλ. ουδ. } 1_R \end{array}\right\}$

(*) Αν ισχύει $x \cdot y = y \cdot x$, $\forall x, y \in R$ ο R καλείται μεταθετικός

πχ $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$

πχ $S = \{\bar{0}_{12}, \bar{4}_{12}, \bar{8}_{12}\} \subseteq \mathbb{Z}_{12} = \{\bar{0}_{12}, \bar{1}_{12}, \ldots, \bar{11}_{12}\}$

$1_S = \bar{4}_{12}$ καθώς $\left.\begin{array}{l} \bar{4}_{12} \cdot \bar{0}_{12} = \bar{0}_{12} \\ \bar{4}_{12} \cdot \bar{4}_{12} = \bar{4}_{12} \\ \bar{4}_{12} \cdot \bar{8}_{12} = \bar{8}_{12} \end{array}\right\}$ $\bar{4}_{12} \cdot x = x$, $\forall x \in S$

• $M_{n\times n}(\mathbb{K}) = \{$οι $n\times n$ πίνακες με στοιχεία από το $\mathbb{K}\}$

$0_{n\times n} = O$, $1_{n\times n} = I_n$

Ορισμός: Ένα στοιχείο $a \overset{\neq 0_R}{\in} R$ καλείται (αριστερός) διαιρέτης του μηδενός αν

$\exists \underset{\neq 0_R}{\beta \in R}$: $a \cdot \beta = 0_R$ (δεξιός : $\beta \cdot a = 0_R$)

Αν είναι και αριστερός και δεξιός καλείται διαιρέτης του μηδενός.

πχ $\mathbb{Z}_{12}$ $\bar{2}_{12} \cdot \bar{6}_{12} = \bar{0}_{12}$

Ορισμός: Ένας μεταθετικός δακτύλιος, ο οποίος δεν έχει διαιρέτες του μηδενός καλείται (ακέραια) περιοχή.

πχ $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$

όχι ακέραια περιοχή $(\mathbb{Z}_n, +, \cdot)$ όπου n όχι πρώτος

Ορισμός: Ένα στοιχείο $\overset{\neq 0_R}{a} \in R$ καλείται αντιστρέψιμο, αν $\exists \underset{\neq 0_R}{a^{-1}} \in R$ με $a \cdot a^{-1} = \underset{a^{-1} \cdot a}{\overset{\shortparallel}{1_R}}$

Ορισμός: Ένας δακτύλιος ο οποίος κάθε μη-μηδενικό στοιχείο του είναι αντιστρέψιμο καλείται δακτύλιος διαίρεσης.

Ορισμός: Σώμα καλείται ένας μεταθετικός δακτύλιος διαίρεσης.

πχ $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

πχ όχι $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +, \cdot)$; n όχι πρώτος.

(σαν μιγαδικοί)

σώμα: $\mathbb{Q}(\sqrt{p}) = \{ a + \beta\sqrt{p} \;, a, \beta \in \mathbb{Q} \}$, p πρώτος.

Εύρεση αντιστρόφου

Έστω $(a+\beta\sqrt{p})(\gamma+\delta\sqrt{p}) = 1$

$a+\beta\sqrt{p} \neq 0$

$$(A) + (B)\sqrt{p} = 1$$

σύστημα ως προς γ, δ $\Rightarrow \begin{cases} A = 1 \\ B = 0 \end{cases}$

Θεώρημα 1) Κάθε σώμα είναι ακέραια περιοχή.

(Το αντίστροφο δεν ισχύει, πχ $(\mathbb{Z}, +, \cdot)$ είναι ακ. περιοχή, αλλά όχι σώμα)

2) Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

3) Τα ακόλουθα είναι ισοδύναμα. Έστω ο $(\mathbb{Z}_n, +, \cdot)$

a) ο $\mathbb{Z}_n$ σώμα

β) ο $\mathbb{Z}_n$ ακ. περιοχή

γ) ο n πρώτος αριθμός.

- $(\alpha \Leftrightarrow \beta)$ έπονται από τα (1), (2)
- $(\beta \Rightarrow \gamma)$ Έστω $\mathbb{Z}_n$ ακ. περιοχή
  Έστω n όχι πρώτος $\Rightarrow n = k\lambda$, $k, \lambda > 1$
  $\Rightarrow \bar{n}_n = (\overline{k\lambda})_n$
  $\Rightarrow \bar{0}_n = \bar{k}_n \cdot \bar{\lambda}_n$ άτοπο καθώς $\mathbb{Z}_n$ ακ περιοχή
  και $\bar{k}_n, \bar{\lambda}_n \neq \bar{0}_n$ καθώς αν $\bar{k}_n = \bar{0}_n \Leftrightarrow n | k-0$ άτοπο αφού $n > k$.
- $(\gamma \Rightarrow \alpha)$ Έστω n πρώτος και $\underset{\neq \bar{0}_n}{\bar{k}_n} \in \mathbb{Z}_n$
  $\Rightarrow n \nmid k \Rightarrow \mu\kappa\delta(k, n) = 1 \overset{\exists x, y \in \mathbb{Z}}{\Leftrightarrow} 1 = kx + ny$
  $\Rightarrow \bar{1}_n = \bar{k}_n \cdot \bar{x}_n + \cancel{\bar{n}_n \bar{y}_n}^{\,0}$
  $\Rightarrow \bar{1}_n = \bar{k}_n \cdot \bar{x}_n \Rightarrow$ το $\bar{k}_n$ αντιστρ.

Ορισμός: Ένας $\mathbb{K}$ διανυσματικός χώρος (ή ένας δ. χ. υπεράνω σωμ. $\mathbb{K}$) είναι μία τριάδα $(V, +, \cdot)$ όπου το $(V, +)$ είναι αβελιανή ομάδα (τα στοιχεία της οποίας καλούνται διανύσματα) εφοδιασμένο με μια εξωτερική πράξη "$*$" έτσι ώστε
$* : \mathbb{K} \times V \to V$
$(k, \bar{v}) \mapsto k * \bar{v}$

1) $(k+\lambda) * \bar{x} = k * \bar{x} + \lambda * \bar{x}$, $\forall k, \lambda \in \mathbb{K}$, $\bar{x} \in V$
2) $k * (\bar{x} + \bar{y}) = k * \bar{x} + k * \bar{y}$, $\forall k \in \mathbb{K}$, $\bar{x}, \bar{y} \in V$
3) $(k\lambda) * \bar{x} = k(\lambda * \bar{x})$, $\forall k, \lambda \in \mathbb{K}$, $\bar{x} \in V$
4) $1 * \bar{x} = \bar{x}$, $\forall \bar{x} \in V$

πχ $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

Ορισμός. Ιδεώδες ενός δακτυλίου R είναι ένα σύνολο
1) $I \neq \emptyset$ $(0_R \in I)$
2) $\alpha - \beta \in I$, $\forall \alpha, \beta \in I$ $(\overset{(=)}{\alpha + \beta} \in I)$
3) $r \cdot \alpha \in I$, $\alpha \cdot r \in I$, $\forall \alpha \in I$, $r \in R$ $(I \triangleleft R)$
δεξιό + αριστερό → ιδεώδες

Πχ 1) $R = (\mathbb{Z}, +, \cdot)$ Τα ιδεώδη του είναι η $n\mathbb{Z} = \langle n \rangle$

2) αν $I, J \trianglelefteq R \Rightarrow I \cap J \trianglelefteq R$

α) $\left.\begin{array}{l} I \trianglelefteq R \Rightarrow 0_R \in I \\ J \trianglelefteq R \Rightarrow 0_R \in J \end{array}\right\} \Rightarrow 0_R \in I \cap J$

β) $a, \beta \in I \cap J \Rightarrow \left\{\begin{array}{l} a \in I \cap J \Rightarrow \begin{cases} a \in I \\ a \in J \end{cases} \\ \beta \in I \cap J \Rightarrow \begin{cases} \beta \in I \\ \beta \in J \end{cases} \end{array}\right.$ $\left.\begin{array}{l} a, \beta \in I \trianglelefteq R \Rightarrow a - \beta \in I \\ a, \beta \in J \trianglelefteq R \Rightarrow a - \beta \in J \end{array}\right\} a - \beta \in I \cap J$

γ) $\begin{array}{l} r \in R \\ a \in I \cap J \end{array} \Rightarrow \left.\begin{array}{l} \left.\begin{array}{l} r \in R \\ a \in I \end{array}\right\} \xRightarrow{I \trianglelefteq R} ra, ar \in I \\ a \in J \rightarrow ra, ar \in J \end{array}\right\} ar, ra \in I \cap J.$

Πχ ($I \cup J$ όχι πάντα ιδεώδες)

$2\mathbb{Z}, 3\mathbb{Z} \trianglelefteq \mathbb{Z}$

$2\mathbb{Z} \cup 3\mathbb{Z} \ntrianglelefteq \mathbb{Z}$

$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$

$3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

$2\mathbb{Z} \cup 3\mathbb{Z} = \{\ldots, -6, -4, -3, -2, 0, 2, 3, 4, 6 \ldots\}$

$2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ αλλά $3 - 2 = 1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

* Αν $I, J \trianglelefteq R \Rightarrow I \cup J \trianglelefteq R \Leftrightarrow I \subseteq J$ ή $J \subseteq I$

Βασικά Ιδεώδη

· $I, J \trianglelefteq R \Rightarrow$ ορίζω το $I + J = \{a + \beta, a \in I, \beta \in J\}$

$I \cdot J = \{\sum a\beta, a \in I, \beta \in J\}$

Περιοχή κύριων Ιδεωδών (Π.Κ.Ι.)

Ορισμός Ένα ιδεώδες $I \trianglelefteq R$ καλείται κύριο αν $\exists a \in R$: $I = \langle a \rangle$.

Πχ $(\mathbb{Z}, +, \cdot)$ ένα ιδεώδες του $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, \ldots\} = \langle 2 \rangle$

Όλα του τα ιδεώδη η $\mathbb{Z} = \langle n \rangle$

<u>Ορισμός</u>. Ένας μεταθετικός δακτύλιος, ακ. περιοχή για την οποία κάθε ιδεώδες είναι κύριο καλείται περιοχή κύριων ιδεωδών (ΠΚΙ)

<u>Πχ</u> ΠΚΙ: Κάθε σώμα είναι ΠΚΙ

Ένα σώμα $\mathbb{K}$ έχει δύο ιδεώδη: – το $\{0_R\} = \langle 0_R \rangle$
\ το $\mathbb{K} = \langle 1_{\mathbb{K}} \rangle$ είναι κύρια

$\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}_p, \mathbb{Q}(\sqrt{p})$

<u>Θεώρημα</u>: αν $\mathbb{K}$ σώμα $\Rightarrow$ ο $\mathbb{K}[x]$ είναι ΠΚΙ

$\mathbb{K}[x] = \{a_0 + a_1x + \dots + a_nx^n, \ a_i \in \mathbb{K}\}$

Έστω I ιδεώδες του $\mathbb{K}[x]$ – αν $I = \{0_{\mathbb{K}}\} = \langle 0_{\mathbb{K}} \rangle$ κύριο
\ αν $I = \mathbb{K}[x] \Leftrightarrow 1_{\mathbb{K}} \in I = \langle 1_{\mathbb{K}} \rangle$

άρα $I \subsetneq \mathbb{K}[x]$

Στο I υπάρχουν πολυώνυμα βαθμού ≥ 1.

$I \triangleleft R \quad I = R \Leftrightarrow 1_R \in I$

Αν όχι $\Rightarrow$ το I θα περιείχε στοιχεία 0 βαθμού, δηλ. στοιχεία του $\mathbb{K}$, πχ το $\lambda \in \mathbb{K}$

$\left.\begin{array}{l} \lambda \in I \\ \lambda^{-1} \in \mathbb{K} \end{array}\right\} \begin{array}{l} \lambda\lambda^{-1} \in I \\ 1 \in I \end{array}$

$I = \mathbb{K}[x]$ άτοπο

Έστω $q(x)$ το πολυώνυμο με τον μικρότερο βαθμό $q(x) \in I$

δο $I = \langle q(x) \rangle$ (Προφανώς $\langle q(x) \rangle \subseteq I$)

Έστω $p(x) \neq 0 \in I$. δο $p(x) \in \langle q(x) \rangle$

Εκτελώ τη διαίρεση $p(x) : q(x) \Rightarrow p(x) = \pi(x)q(x) + u(x)$,

όπου $u(x) = 0$ ή βαθμός$(u(x)) <$ βαθμός$(q(x))$

1) $u(x) = 0 \Rightarrow p(x) = \pi(x)q(x)$ ✓

2) $\beta(u(x)) < \beta(q(x)) \Rightarrow u(x) = p(x) - \pi(x)q(x) \in I$ άρα $u(x) \in I$
άτοπο αφού $q(x)$ έχει το μικρότερο βαθμό.