Αλγεβρικές Κατασκευές

18-02-2019
1ο διάλειμμα

Ορισμός
Δακτύλιος R είναι ένα σύνολο εφοδιασμένο με δύο (δυαδικές) πράξεις, τη "κανονική" πρόσθεση "$+$" και πολλ/μό "$\cdot$" έτσι ώστε
i) $(R,+)$ αβελιανή ομάδα
ii) $\alpha(\beta\cdot\gamma)=(\alpha\beta)\cdot\gamma \quad \forall \alpha,\beta,\gamma\in R$
iii) $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$ και $(\alpha+\beta)\cdot\gamma=\alpha\gamma+\beta\gamma \quad \forall \alpha,\beta,\gamma\in R$

Ορισμός
Ομάδα G είναι ένα σύνολο εφοδιασμένο με μια δυαδική πράξη $*$
i) $\alpha*(\beta*\gamma)=(\alpha*\beta)*\gamma \quad \forall \alpha,\beta,\gamma\in G$
ii) $\exists\, e\in G \quad x*e=e*x=x \quad \forall x\in G$ (ουδέτερο)
iii) $\forall x\in G \quad \exists\, x'\in G \quad x*x'=x'*x=e$ (αντίστροφο)

Αν επιπλέον ισχύει $a*b=b*a \quad \forall a,b\in G$ $(=)$ G αβελιανή

Ορισμός
Ένας δακτύλιος καλείται μεταθετικός αν $xy=yx \quad \forall x,y\in R$

Θα συμβολίζω με 0_R το προσθετικό ουδέτερο του R.
Θα συμβολίζω με 1_R το πολλαπλασιαστικό ουδέτερο του R (αν υπάρχει)

π.χ. $(2\mathbb{Z},+,\cdot)=\{\dots,-4,-2,0,2,4,\dots\}$

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

Πρόταση:
$1_S=\bar{4}_{12}$ διότι $\bar{0}_{12}\cdot\bar{4}_{12}=\bar{0}_{12}$
$\bar{4}_{12}\cdot\bar{4}_{12}=\bar{4}_{12}$
$\bar{8}_{12}\cdot\bar{4}_{12}=\bar{8}_{12}$

ΜΟΝΟ ΕΓΡΑΨΑ ΟΤΙ $x\cdot 1_S=x$ -1-

Ορισμός
Ένα στοιχείο $a \in R$ λέγεται αντιστρέψιμο αν $\exists\ a' \neq 0_R \in R : a \cdot a' = a' \cdot a = 1_R$
(τα αντιστρέψιμα στοιχεία λέγονται μονάδες του R)

Ορισμός
Ένας δακτύλιος όπου όλα τα στοιχεία του είναι αντιστρέψιμα λέγεται δακτύλιος διαίρεσης

Ορισμός
Σώμα λέγεται ένας μεταθετικός δακτύλιος διαίρεσης

π.χ. Ο $\mathbb{Z}$ με $(\mathbb{Z}, +, \cdot)$ αφού τα μόνα αντίστροφα το ± 1.

Σώμα, $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ για p πρώτα με πράξεις $(+, \cdot)$

(*) $\mathbb{Z}(\sqrt{p}) = \{a + b\sqrt{p},\ a, b \in \mathbb{Z}\}$

Ορισμός
Έστω R δακτύλιος. Ένα πολυώνυμο $\phi(x)$ με συντελεστές από τον R είναι ένα (άπειρο) άθροισμα της μορφής

$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots$ όπου όλα τα $a_i = 0$ εκτός πεπερασμένου πλήθους

Τα a_i λέγονται συντελεστές του $\phi(x)$ και ορίζουμε βαθμό του $\phi(x)$ ($\deg \phi(x) = \max\{i : a_i \neq 0\}$)

Ορισμός (Πολυωνυμικός δακτύλιος)
Έστω R δακτύλιος, ορίζουμε πολυωνυμικό δακτύλιο μεταβλητής x ($συμβ. R[x]$), το σύνολο που έχει ως στοιχεία τα πολυώνυμα ως προς x με συντελεστές στοιχεία $\in R$

Αντίστοιχα, μπορούμε να ορίσουμε τον $R[x,y] = R[y,x]$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ ||

Αντίστοιχα αναφερόμαστε στην έννοια $(R[x])[y]$
του πολ. δακτυλίων ή μεταβλητών
$R[x_1, \dots, x_n]$

Έστω $S = R[x_1, \dots, x_n]$ κάθε στοιχείο του μορφής

$\alpha x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$, $\alpha \in R$, $a_i \in \mathbb{N}$ καλείται μονώνυμο
($συμβ. x^a$, όπου $a \in \mathbb{N}^n$)

(Ένα πολυώνυμο είναι άθροισμα μονωνύμων)

π.χ. $R[x_1, x_2, x_3, x_4]$, $\phi = x_1 x_3 - 2x_1 x_3^2$

$x^a, a = (1,0,1,0)$ $\qquad$ $x^\beta, \beta = (1,0,2,1)$

πράξεις (στον πολ/κό δακτύλιο)

Έστω $f = \sum_{u \in \mathbb{N}^n} c_u x^u$ $\qquad$ $g = \sum_{u \in \mathbb{N}^n} d_u x^u$

→ (ίδιοι έχουμε προσθέσει μηδενικά
→ πχ. το πλήθος c_u, d_u, ούτε ένα μηδέν)

Ορίζουμε "+" $f+g = \sum_{u \in \mathbb{N}^n} (a_u + d_u) x^u$

"·" $f \cdot g = \sum_{k \in \mathbb{N}^n} \left(\sum_{\alpha+\beta=k} a_\alpha d_\beta \right) x^k$

} δίνεται δομή δακτυλίου στο $R[x_1, \ldots, x_n]$

Περιοχές Μοναδιαίων Διαίρεσης

Ορισμός

Έστω R μεταθετικός δακτύλιος με μοναδιαίο στοιχείο, ο R λέγεται **ακέραια περιοχή** (ή περιοχή) αν $ab = 0_R \Rightarrow$ αναγκαστικά $a = 0_R$ ή $b = 0_R$

(αν a, b με $ab = 0_R \Rightarrow$ καλούνται μηδενοδιαιρέτες)

* 0_R ακέραια περιοχή αν δεν έχει μηδενοδιαιρέτες)

πχ ο $\mathbb{Z}_6$ δεν είναι ακέραια περιοχή.

Θεώρημα

1) Κάθε σώμα είναι ακέραια περιοχή

(Το αντίστροφο δεν ισχύει το $\mathbb{Z}$ είναι ΑΠ αλλά όχι Σώμα)

2) Κάθε πεπερασμένη ακ. περιοχή είναι σώμα.

Πρόταση

Αν ο R είναι ακέραια περιοχή τότε και ο $R[x]$ είναι ακέραια

Απόδειξη

Έστω ο $R[x]$ όχι ακέραια περιοχή $\Rightarrow$

$\exists\ \varphi_1, \varphi_2 \in R[x]$ με $\varphi_1, \varphi_2 \neq 0$ και $\varphi_1 \cdot \varphi_2 = 0$

$\Leftrightarrow \deg(\varphi_1 \cdot \varphi_2) = 0 \Rightarrow \underbrace{\deg \varphi_1}_{\in \mathbb{N}} + \underbrace{\deg \varphi_2}_{\in \mathbb{N}} = 0$

$\deg \varphi_1 = \deg \varphi_2 = 0 \Rightarrow \varphi_1, \varphi_2 \in R$ άρα, ο R έχει διαιρέτες του μηδενός, δηλ. ότι ο R είναι ακέραια περιοχή

$\varphi_1, \varphi_2 \neq 0$ με $\varphi_1 \cdot \varphi_2 = 0$

Θεώρημα (Ευκλείδιου Αλγόριθμου)

Έστω $f(x), g(x) \in R[x]$, R ακέραια περιοχή και $g(x) \neq 0$. Τότε υπάρχουν μοναδικά πολυώνυμα $u(x), \pi(x)$ τ.ω. $f(x) = \pi(x) \cdot g(x) + u(x)$ $\deg(u(x)) < \deg(g(x))$ ή $u(x) = 0$

Αν $u(x) = 0$ τότε $g(x) \mid f(x)$

($\alpha \mid \beta$, αν $\exists\ \gamma : \beta = \alpha\gamma$)

Ιδιότητες (διαιρετότητα σε πολυώνυμα)

Έστω $\varphi_1(x), \varphi_2(x), \varphi_3(x), \varphi_4(x) \in R[x]$

1) $\varphi_1(x) \mid \varphi_1(x)$ και $\varphi_1(x) \mid 0$
2) $\varphi_1(x) \mid \varphi_2(x)$ και $\varphi_2(x) \mid \varphi_3(x) \Rightarrow \varphi_1(x) \mid \varphi_3(x)$
3) $\varphi_1(x) \mid \varphi_2(x)$ και $\varphi_1(x) \mid \varphi_3(x) \Rightarrow \varphi_1(x) \mid \alpha\varphi_2(x) + \beta\varphi_3(x)$
4) $\varphi_1(x) \mid \varphi_2(x)$ και $\varphi_3(x) \mid \varphi_4(x) \Rightarrow \varphi_1(x)\varphi_3(x) \mid \varphi_2(x)\varphi_4(x)$

Ορισμός (ανάγωγο)

Έστω R ακέραιο περιοχή. Ένα στοιχείο $p \in R$ που δεν είναι αντιστρέψιμο λέγεται ανάγωγο αν όποτε είναι $p = ab$, $a, b \in R$ $\Rightarrow$ a αντιστρέψιμο ή b αντιστρέψιμο.

Π.χ. στο $\mathbb{Z}$ τα ανάγωγα είναι οι πρώτοι αριθμοί $\pm p$

$p = p \cdot 1$ ή $p = (-p)(-1)$ (± 1 αντιστρέψιμα)

Ορισμός (ανάγωγο πολυώνυμο)

Ένα πολυώνυμο $\phi(x) \in R[x]$ με $\deg \phi(x) > 0$ λέγεται ανάγωγο αν (δεν) μπορεί να γραφεί ως $\phi(x) = \phi_1(x)\phi_2(x)$ με $\phi_1(x), \phi_2(x) \in R[x]$ και $\deg \phi_1(x), \deg \phi_2(x) > 0$

Παρατήρηση

1) Σημαντικό ρόλο διαδραματίζει ο δακτύλιος R στον οποίο βρισκόμαστε (κάτι είναι ανάγωγο στον $R_1[x]$ αλλά όχι στον $R_2[x]$)

Π.χ. → $\mathbb{R}[x]$ το x^2+1 είναι ανάγωγο

→ $\mathbb{C}[x]$ το x^2+1 όχι ανάγωγο, αφού $x^2+1 = (x-i)(x+i)$

2) Δεν αναζητάμε ιδιαίτερη ρίζων ενός πολυωνύμου με το χαρακτηριστικό ως ανάγωγο.

Π.χ. $x^4+2x^2+1 \in \mathbb{R}[x]$ δεν έχει ρίζες

αλλά $x^4+2x^2+1 = (x^2+1)(x^2+1)$ δεν είναι ανάγωγο

$R = \mathbb{Z}$ το 5 ανήκει

$R = \mathbb{Q}$ το 5 όπ. ανήκει αφού $5 = \frac{5}{3} \cdot 3$

Ορισμός ΠΜΑ

Θεωρούμε αυτεπαίο περιοχή R. Ο R καλείται ΠΜΑ αν

i) κάθε στοιχείο του είναι αναλύσιμο: είτε βρίσκεται ως πεπερασμένο γινόμενο αναγώγων στοιχείων του R

ii) Αν $a \in R$ με $a = p_1, \dots, p_t = a_1, \dots, a_2$ (γινόμενο αναγ. στοιχείων του R)

υποχρεωτικά $t = 2$ και κάθε p_i είναι ισοδύναμο με κάποιο a_j

Π.χ. Το $\mathbb{Z}$: οι αριθμοί είναι είτε ± 1 (αντιστρέψιμοι) είτε έχει ΜΟΝΑΔΙΚΗ ΠΡΩΤΑΡΧΙΚΗ ΑΝΑΛΥΣΗ

($a, b \in R$ λέγονται ισοδύναμα αν $\exists\, \varepsilon \in R$ αντιστρέψιμο με $a = b\varepsilon$)

Π.χ. • στο $\mathbb{Z}$ τα ισοδύναμα είναι τα $\{\pm k\}$

• στο $\mathbb{R}[x]$: $x^3 - x^2 + x - 1 = (x-1)(x^2+1)(2x-2)\left(\frac{1}{5}x^2 + \frac{1}{5}\right)$

δύο διασπάσεις λόγω αναγώγων

$\mathbb{R}[x]$ είναι ΠΜΑ : $2x - 2 = 2(x-1)$ } ΙΣΟΔΥΝΑΜΑ
και 2 αντιστρ.

Θεώρημα

Αν ο R είναι ΠΜΑ και ο $R[x]$ ΠΜΑ

Π.Χ.

αν $R = \mathbb{K}$ σώμα τότε έχω ΠΜΑ

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