

Κεφάλαιο 1

1.1 1^η Εβδομάδα

Πίνακας 1.1: Αντιστοιχία ιδιοτήτων του $\mathbb{Z}$ και του $K[X]$, με K σώμα

$\mathbb{Z}$	$K[X]$
αντιστρέψιμο στοιχείο: ± 1	αντιστρέψιμο στοιχείο: $c \in K^*$
$p > 1$ πρώτος: $p \nmid ab$ με $a, b > 1$	$p(X) \notin K$ ανάγωγος: $p(X) \nmid a(X)b(X)$ με $a(X), b(X) \notin K$
$d = \text{MK}\Delta(a, b)$ (1) d κ.δ. των a, b (2) αν d' είναι κ.δ. των a, b τότε $d' \mid d$	$d(X) = \text{MK}\Delta(a(X), b(X))$ (1) $d(X)$ κ.δ. των $a(X), b(X)$ (2) αν $d'(X)$ είναι κ.δ. των $a(X), b(X)$ τότε $d'(X) \mid d(X)$ (3) $d(X)$ είναι μονικό
Ανάλυση σε πρώτους: $a > 1$ $a = p_1 \cdots p_n$ $p_1, \dots, p_n$ πρώτοι. Αν $a = q_1 \cdots q_l$, $q_1, \dots, q_l$ πρώτοι, τότε $l = n$ και $(q_1, \dots, q_n)$ είναι μετάθεση των $(p_1, \dots, p_n)$	Ανάλυση σε ανάγωγους: $a(X) \notin K$ $a(X) = p_1(X) \cdots p_n(X)$ $p_1(X), \dots, p_n(X)$ ανάγωγοι. Αν $a(X) = q_1(X) \cdots q_l(X)$, $q_1(X), \dots, q_l(X)$ ανάγωγοι, τότε $l = n$ και υπάρχει μετάθεση $(i_1, \dots, i_n)$ της $(1, \dots, n)$ ώστε $q_k(X) = \text{σταθερά} \cdot p_{i_k}(X)$ για κάθε $k = 1, \dots, n$
Αν $a \in \mathbb{Z}$ και p πρώτος, τότε $p \mid a$ είτε $\text{MK}\Delta(a, p) = 1$	Αν $a(X) \in K[X]$ και $p(X) \in K[X]$ ανάγωγος, τότε $p(X) \mid a(X)$ είτε $\text{MK}\Delta(a(X), p(X)) = 1$
$\text{MK}\Delta(a, b) = d \Rightarrow \exists a', b' :$ $a' \cdot a + b' \cdot b = d$	$\text{MK}\Delta(a(X), b(X)) = d(X) \Rightarrow \exists a'(X), b'(X) \in K[X] :$ $a'(X) \cdot a(X) + b'(X) \cdot b(X) = d(X)$
Ευκλείδεια διαίρεση: $a, b \in \mathbb{Z}, b \neq 0$ $\exists q, r \in \mathbb{Z}, 0 \leq r < b : a = bq + r$	Ευκλείδεια διαίρεση: $a(X), b(X) \in K[X], b(X) \neq 0$ $\exists q(X), r(X) \in K[X], \deg r(X) < \deg b(X) : a(X) = b(X)q(X) + r(X)$ Σύμβαση: $\deg 0 = -\infty$ και $-\infty < m \quad \forall m \in \mathbb{Z}$

Ορισμός 1.1. Έστω R μεταθετικός δακτύλιος με μοναδιαίο στοιχείο 1_R . Συνήθως, αντί για 1_R θα γράφομε, απλούστερα, 1. Ανάλογα, αντί για 0_R (μηδενικό στοιχείο του R), θα γράφομε 0. Το $\emptyset \neq I \subseteq R$ ονομάζεται ιδεώδες αν και μόνον αν

1. $a, b \in I \implies a - b \in I$
2. $a \in I, r \in R \implies ra \in I$

Παράδειγμα 1.2. $\{0\}$ το μηδενικό ιδεώδες και R ολόκληρος ο δακτύλιος

Αν το I είναι ιδεώδες του δακτυλίου R , τότε ορίζω τη σχέση ισοδυναμίας $a \sim b \iff a - b \in I$. Η κλάση ισοδυναμίας του $a \in R$ είναι το σύνολο

$$a + I = \{a + r : r \in R\}$$

Στο σύνολο πηλίκο του ως προς την $\sim$, δηλαδή στο σύνολο των κλάσεων ισοδυναμίας, που συμβολίζεται R/I ορίζω πράξεις

$$\begin{aligned} + : (a + I) + (b + I) &:= (a + b) + I \\ \cdot : (a + I) \cdot (b + I) &:= ab + I \end{aligned}$$

Πρόταση. Οι πράξεις είναι καλά ορισμένες. Δηλαδή, αν $a + I = a' + I$ και $b + I = b' + I$, τότε $(a + I) + (b + I) = (a' + I) + (b' + I)$ και $(a + I) \cdot (b + I) = (a' + I) \cdot (b' + I)$.

Απόδειξη.

$$\begin{aligned} a + I = a' + I &: \iff a' = a + \iota_1, & \iota_1 \in I \\ b + I = b' + I &: \iff b' = b + \iota_2, & \iota_2 \in I \end{aligned}$$

άρα $a'b' = ab + a\iota_2 + b\iota_1 + \iota_1\iota_2$ και συνεπώς $a'b' - ab \in I$, δηλαδή $a'b' + I = ab + I$. $\square$

Παράδειγμα 1.3 (όχι καλά ορισμένων “πράξεων”). $R = \mathbb{Z}, I = 7\mathbb{Z}$ άρα $R/I = \{0 + I, \dots, 6 + I\}$. Ορίζω την “πράξη” $(a + 7\mathbb{Z}) \star (b + 7\mathbb{Z}) = c + 7\mathbb{Z}$ όπου c το υπόλοιπο της διαίρεσης του ab διά 5.

Ελέγχω το αποτέλεσμα στην εξής περίπτωση:

$$\begin{aligned}(4 + 7\mathbb{Z}) \star (3 + 7\mathbb{Z}) &= 2 + 7\mathbb{Z} \\ (11 + 7\mathbb{Z}) \star (10 + 7\mathbb{Z}) &= 1 + 7\mathbb{Z}\end{aligned}$$

Δηλαδή, ενώ $4 + 7\mathbb{Z} = 11 + 7\mathbb{Z}$ και $3 + 7\mathbb{Z} = 10 + 7\mathbb{Z}$, οι αντίστοιχοι πολλαπλασιασμοί δίνουν διαφορετικά αποτελέσματα, άρα η φαινομενική “πράξη” δεν είναι πράξη.

Ιδεώδες που παράγεται από κάποια στοιχεία $\alpha, \beta, \gamma, \dots \in R$. Συμβολίζεται με $\langle \alpha, \beta, \gamma, \dots \rangle$ και ορίζεται ως το σύνολο

$$\{r_1\alpha + r_2\beta + \dots : r_1, r_2, \dots \in R\}$$

Αν τα στοιχεία $\alpha, \beta, \gamma, \dots$ είναι άπειρα στο πλήθος, τότε εννοείται ότι μόνο πεπερασμένο το πλήθος $r_1, r_2, r_3, \dots$ είναι $\neq 0$. Σημαντική ειδική περίπτωση: Ιδεώδες που παράγεται από ένα μόνο στοιχείο. Ένα τέτοιο ιδεώδες λέγεται *κύριο*. Η τυπική του μορφή είναι

$$\langle a \rangle = \{ra : r \in R\}$$

Ορισμός 1.4. Ένας δακτύλιος του οποίου όλα τα ιδεώδη είναι κύρια ονομάζεται *δακτύλιος κυρίων ιδεωδών* (Δ.Κ.Ι. ή στ’ αγγλικά P.I.D. principal ideal domain)

Παράδειγμα 1.5. Ο δακτύλιος $\mathbb{Z}$ καθώς και οι πολυωνυμικοί δακτύλιοι $K[X]$, όπου K σώμα, είναι Δ.Κ.Ι. Αυτό ισχύει γιατί και στους δύο υπάρχει ευκλείδεια διαίρεση.

Παράδειγμα 1.6 (Δακτύλιος που δεν είναι Δ.Κ.Ι.). Έστω ο υποδακτύλιος R του $\mathbb{C}$, που ορίζεται ως εξής: $R = \{a + bi\sqrt{5} : a, b \in \mathbb{Z}\}$. Θεωρώ το ιδεώδες $I = \{2x + (1 + i\sqrt{5})y : x, y \in \mathbb{Z}\}$. Αν ήταν το I κύριο ιδεώδες, τότε θα υπήρχαν $a_0, b_0 \in \mathbb{Z}$ ώστε $I = \langle a_0 + b_0i\sqrt{5} \rangle$, δηλαδή

$$\{2x + (1 + i\sqrt{5})y : x, y \in \mathbb{Z}\} = \{(a_0 + b_0i\sqrt{5})(r + si\sqrt{5}) : r, s \in \mathbb{Z}\} \quad (1.1)$$

Για $x = 1, y = 0$ παίρνω το 2. Άρα το 2 ανήκει στο αριστερό μέρος της (1.1), οπότε θα πρέπει να υπάρχουν $r_1, s_1 \in \mathbb{Z}$ ώστε

$$2 = (a_0 + b_0i\sqrt{5})(r + si\sqrt{5})$$

Παίρνω τη συζήγη μιγαδική

$$2 = (a_0 - b_0i\sqrt{5})(r - si\sqrt{5})$$

Πολλαπλασιάζοντας $4 = (a_0^2 + 5b_0^2)(r_1^2 + 5s_1^2)$. Επειδή οι παράγοντες είναι ακέραιοι, $a_0^2 + 5b_0^2 = 1$ ή 2 ή 4.

$$\begin{aligned}a_0^2 + 5b_0^2 = 1 &\implies a_0 = \pm 1, b_0 = 0 \\ a_0^2 + 5b_0^2 = 2 &\text{ προφανώς αδύνατη} \\ a_0^2 + 5b_0^2 = 4 &\implies a_0 = \pm 2, b_0 = 0\end{aligned}$$

άρα $a_0 + b_0i\sqrt{5} = \pm 1$ ή ± 2 . Στο αριστερό μέλος της (1.1) ανήκει το $1 + i\sqrt{5}$ (πάρε $x = 0, y = 1$) άρα πρέπει να ανήκει και στο δεξιό μέλος της (1.1), δηλαδή

$$1 + i\sqrt{5} = \pm 1(r_2 + s_2i\sqrt{5}) \quad \text{ή} \quad \pm 2(r_2 + s_2i\sqrt{5})$$

Το δευτερό προφανώς αποκλείεται, οπότε καταλήγω στο συμπέρασμα ότι $a_0 + b_0i\sqrt{5} = \pm 1$. Άρα το $I = \langle \pm 1 \rangle = R$ και συμπεραίνω ότι $\{2x + (1 + i\sqrt{5})y : x, y \in \mathbb{Z}\} = R$. Αλλά $1 \in R$, άρα πρέπει να υπάρχουν $x, y \in \mathbb{Z}$, ώστε $2x + (1 + i\sqrt{5})y = 1$. Αυτό συνεπάγεται ότι $2x + y = 1$ και $y = 0$, οπότε $2x = 1$, άτοπο αφού $x \in \mathbb{Z}$.

Ορισμός 1.7. Έστω δακτύλιος R και ιδεώδες $I \neq \{0\}$, R του R . Λέω ότι το I είναι maximal (μεγιστικό) αν δεν υπάρχει γνήσιο μεγαλύτερο από το I ιδεώδες του R , εκτός από τον ίδιο τον R , δηλ. είναι αδύνατον να βρω ιδεώδες J του R με $I \subsetneq J \subsetneq R$.

- Ισοδύναμη διατύπωση: Αν το J είναι ιδεώδες του R και $I \subseteq J$, τότε $J = I$ ή $J = R$.
- Ισοδύναμη διατύπωση: Αν το J είναι ιδεώδες του R και $I \subsetneq J$, τότε $J = R$.

Παράδειγμα. Στάνταρ παραδείγματα.

1. $R = \mathbb{Z}$. Εδώ όλα τα ιδεώδη είναι κύρια, δηλαδή της μορφής $\langle m \rangle$.
Ισχύει το εξής: Το $\langle m \rangle$ είναι maximal $\iff m$ πρώτος.
2. $R = K[X]$ με K σώμα. Όλα τα ιδεώδη είναι κύρια, δηλαδή, της μορφής $I = \langle f(X) \rangle$.
Ισχύει το εξής: Τό $\langle f(X) \rangle$ είναι maximal $\iff f(X)$ ανάγωγο στο $K[X]$.

Πρόταση 1.8. Ο δακτύλιος πηλίκο R/I είναι σώμα $\iff I$ είναι maximal ιδεώδες του R .

Έστω K σώμα και $f(X) \in K[X]$ μη μηδενικό, $I = \langle f(X) \rangle$.

Πόρισμα 1.9. Αν το K είναι σώμα και $p(x) \in K[X]$ ανάγωγο, τότε ο δακτύλιος πηλίκο $K/\langle p(X) \rangle$ είναι σώμα.

Ασκήσεις

Άσκηση 1.10. Έστω $p(X) = X^2 + 2 \in \mathbb{Q}[X]$ και $I = \langle p(X) \rangle$. Σύμφωνα με το Πόρισμα 1.9, ο δακτύλιος $K[X]/I$ είναι σώμα. Υπολογίστε το αντίστροφο στοιχείο του $X + I$.

Άσκηση 1.11. Έστω $p(X) = X^2 + X + 1 \in \mathbb{Q}[X]$ και $I = \langle p(X) \rangle$. Σύμφωνα με το Πόρισμα 1.9, ο δακτύλιος $K[X]/I$ είναι σώμα. Υπολογίστε το αντίστροφο στοιχείο του $(X^3 + 3X^2 + 4X + 3) + I$.

Άσκηση 1.12. Έστω ο υποδακτύλιος δακτύλιος $R = \{x + yi : x, y \in \mathbb{Z}\}$ του $\mathbb{C}$. Αποδείξτε ότι το σύνολο $S = \{10x + (1 - 3i)y : x, y \in \mathbb{Z}\} \subseteq R$ δεν είναι ιδεώδες του R .

Άσκηση 1.13. Έστω ο υποδακτύλιος δακτύλιος $R = \{x + yi : x, y \in \mathbb{Z}\}$ του $\mathbb{C}$ και $I = \langle 10, 3 - i \rangle$. Αποδείξτε τα εξής:

- (i) $I = \{10x + (3 - i)y : x, y \in \mathbb{Z}\}$.
- (ii) $I = \langle 3 - i \rangle$.
- (iii) $3 + i \notin I$.