Αλγεβρα I

Καθηγητὴς Ν.Γ. Τζανάκης

Χειμερινὸ ἑξάμηνο 2015-2016

Βασικὴ περιγραφὴ τῶν θεμάτων ποὺ συζητήθηκαν τὴν 7η ἑβδομάδα

(Δὲν πρόκειται γιὰ λεπτομερῆ περιγραφή.)

• **Πρόταση 1.** *Ἔστω δακτύλιος R μὲ μοναδιαῖο. Γιὰ ὅλα τὰ $f(X), g(X) \in R[X]$ ἰσχύουν οἱ σχέσεις:*

$$\begin{aligned} \deg(f(X)+g(X)) &\leq \max\{\deg f(X), \deg g(X)\} \\ \deg(f(X)\cdot g(X)) &\leq \deg f(X) + \deg g(X). \end{aligned}$$

• **Πρόταση 2.** *Ἔστω ἀκέραια περιοχὴ R. Τότε*

1. $\deg(f(X)\cdot g(X) = \deg f(X) + \deg g(X)$ *γιὰ ὅλα τὰ μὴ μηδενικὰ* $f(X), g(X) \in R[X]$.
2. *Ὁ δακτύλιος* $R[X]$ *εἶναι ἀκέραια περιοχή.*
3. $(R[X])^* = R^*$.

• **Πολυωνυμικὴ συνάρτηση**: Ἔστω δακτύλιος R μὲ μοναδιαῖο καὶ $f(X) = \sum_{i=0}^{\infty} r_i X^i \in R[X]$. Ὁρίζομε ὡς *πολυωνυμικὴ συνάρτηση*, ποὺ ἀντιστοιχεῖ στὸ $f(X)$, τὴν ἀπεικόνιση $\overline{f} : R \to R$, ἡ ὁποία ὁρίζεται: $\overline{f}(a) = \sum_{i=0}^{\infty} r_i a^i$ γιὰ κάθε $a \in R$.
Μὴ ταυτίζομε τὴν πολυωνυμικὴ συνάρτηση $\overline{f}$ μὲ τὸ πολυώνυμο $f(X)$! Γιὰ παράδειγμα, τὸ $f(X) = X^3 + [2]X \in \mathbb{Z}_3[X]$, δὲν εἶναι τὸ μηδενικὸ πολυώνυμο, ἐνῶ ἡ ἀντίστοιχη πολυωνυμικὴ συνάρτηση $\overline{f} : \mathbb{Z}_3 \to \mathbb{Z}_3$ εἶναι ἡ μηδενικὴ συνάρτηση, ἀφοῦ $\overline{f}([a]) = [0]$ καὶ γιὰ τὰ τρία $[a] \in \mathbb{Z}_3$.

• **Διαιρετότητα στὰ πολυώνυμα**: Ἔστω μεταθετικὸς δακτύλιος R μὲ μοναδιαῖο. Στὸν δακτύλιο $R[X]$ λέμε ὅτι τὸ μὴ μηδενικὸ πολυώνυμο $f(X)$ διαιρεῖ τὸ πολυώνυμο $g(X)$ (ἰσοδύναμες διατυπώσεις: "$f(X)$ εἶναι διαιρέτης τοῦ $g(X)$", "$g(X)$ εἶναι διαιρετὸ ἀπὸ τὸ (διὰ τοῦ) $g(X)$", "$g(X)$ εἶναι πολλαπλάσιο τοῦ $f(X)$", "$f(X) \mid g(X)$") ἂν ὑπάρχει $h(X) \in R[X]$, τέτοιο ὥστε $g(X) = f(X)\cdot h(X)$.

• **Πρόταση 3.** *Ἔστω μεταθετικὸς δακτύλιος R μὲ μοναδιαῖο. Στὸν δακτύλιο $R[X]$ ἰσχύουν τὰ ἑξῆς:*

1. *Ἂν $f(X) \neq 0_R$ καὶ $f(X)$ διαιρεῖ τὰ $g(X)$ καὶ $h(X)$, τότε τὸ $f(X)$ διαιρεῖ καὶ τὸ $a(X) \cdot g(X) + b(x) \cdot h(X)$, γιὰ ὁποιαδήποτε $a(X), b(X) \in R[X]$.*

2. *Ἂν $f(X), g(X) \neq 0_R$, $f(X) \,|\, g(X)$ καὶ $g(X) \,|\, h(X)$, τότε $f(X) \,|\, h(X)$.*

3. *Κάθε $a \in R^*$ διαιρεῖ κάθε $f(X)$.*

4. ***Ἂν ὁ R εἶναι ἀκέραια περιοχή**, καὶ $f(X) \,|\, g(X)$, μὲ τὰ $f(X), g(X)$ μὴ μηδενικά, τότε* $\deg f(X) \leq \deg g(X)$.

5. ***Ἂν ὁ R εἶναι ἀκέραια περιοχή**, τὰ $f(X), g(X)$ εἶναι μὴ μηδενικά, $f(X) \,|\, g(X)$ καὶ $g(X) \,|\, f(X)$, τότε ὑπάρχει $a \in R^*$, τέτοιο ὥστε $g(X) = a \cdot f(X)$.*

• **Ἀνάγωγα πολυώνυμα**: Ἔστω μεταθετικὸς δακτύλιος R μὲ μοναδιαῖο. Τὸ *μὴ σταθερὸ* πολυώνυμο $f(X) \in R[X]$ χαρακτηρίζεται ἀνάγωγο στὸ $R[X]$ ἂν δὲν μπορεῖ ν' ἀναλυθεῖ σὲ γινόμενο $f(X) = g(X) \cdot h(X)$ μὲ τὰ $g(X), h(X) \in R[X]$ μὴ σταθερά (δηλαδή, βαθμοῦ ≥ 1).

• **Πρόταση 4.** *Ἂν R εἶναι ἀκέραια περιοχή, τότε, στὸ $R[X]$, κάθε πολυώνυμο πρώτου βαθμοῦ εἶναι ἀνάγωγο.*

Προσοχή! Ἡ πρόταση δὲν ἰσχύει, κατ' ἀνάγκη, ἂν ὁ R δὲν εἶναι ἀκέραια περιοχή. Παραδείγματος χάριν, τὸ $[5]X + [1] \in \mathbb{Z}_6[X]$ δὲν εἶναι ἀνάγωγο (!) διότι $[5]X + [1] = ([2]X + [1]) \cdot ([3]X + [1])$.

• **Θεώρημα 5** (Τῆς εὐκλείδειας διαίρεσης)**.** *Ἔστω ἀκέραια περιοχὴ R, $f(X), g(X) \in R[X]$, $g(X) \neq 0_R$ καὶ ὁ συντελεστὴς μεγιστοβαθμίου ὅρου τοῦ $g(X)$ εἶναι μονάδα (ἀντιστρέψιμο στοιχεῖο) τοῦ R. Τότε ὑπάρχει ἕνα μοναδικὸ ζεῦγος πολυωνύμων $q(X), r(X) \in R[X]$, τέτοιων ὥστε*

$$f(X) = g(X) \cdot q(X) + r(X) \quad \text{καὶ } \deg r(X) < \deg g(X).$$

Τὰ $q(X), r(X)$ λέγονται *πηλίκο* καὶ *ὑπόλοιπο*, ἀντιστοίχως, τῆς διαίρεσης $f(X)$ διὰ $g(X)$.

• **Μονικὸ (ἢ κανονικὸ) πολυώνυμο**: Ἔστω σῶμα F καὶ μὴ μηδενικὸ $f(X) \in F[X]$. Λέμε ὅτι τὸ $f(X)$ εἶναι *μονικὸ* (ἢ *κανονικὸ*) πολυώνυμο ἂν ὁ συντελεστὴς τοῦ μεγιστοβαθμίου ὅρου του εἶναι 1_F.
Παρατήρηση: Ἂν $f(X) = a_n X^n + \cdots + a_1 X + a_0$, μὲ $a_n \neq 0_F$, τότε τὸ πολυώνυμο $a_n^{-1} f(X)$ εἶναι μονικό, ἄρα, γιὰ κάθε μὴ μηδενικὸ $f(X) \in F[x]$ ὑπάρχει $c \in F$, τέτοιο ὥστε τὸ $c \cdot f(X)$ νὰ εἶναι μονικὸ πολυώνυμο.

• **Μέγιστος Κοινὸς Διαιρέτης Πολυωνύμων**.

• **Θεώρημα 6.** *Ἔστω σῶμα F καὶ $f(X), g(X) \in F[X]$ ὄχι καὶ τὰ δύο μηδενικά. Ὑπάρχει πολυώνυμο $d(X) \in F[X]$, ποὺ ἱκανοποιεῖ τὶς ἑξῆς ἀπαιτήσεις:*

1. *$d(X) \mid f(X)$ καὶ $d(X) \mid g(X)$, δηλαδή, τὸ $d(X)$ εἶναι κοινὸς διαιρέτης τῶν $f(X), g(X)$.*
2. *Τὸ $d(X)$ διαιρεῖται ἀπὸ κάθε κοινὸ διαιρέτη τῶν $f(X), g(X)$.*
3. *Τὸ $d(X)$ εἶναι μονικό.*
4. *Ὑπάρχουν $a(X), b(X) \in F[X]$, τέτοια ὥστε, $d(X) = a(X)f(X) + b(X)g(X)$.*

Πρόταση-Ὁρισμός 7. *Τὸ πολυώνυμο $d(X)$ τοῦ Θεωρήματος 6 εἶναι μοναδικὸ καὶ καλεῖται* μέγιστος κοινὸς διαιρέτης *τῶν $f(X), g(X)$. Χρησιμοποιοῦμε τὸν συμβολισμὸ $d(X) = \text{ΜΚΔ}(f(X), g(X))$ ἢ, ἁπλούστερα, $d(X) = (f(X), g(X))$. Ἂν $\text{ΜΚΔ}(f(X), g(X)) = 1_F$, τότε λέμε ὅτι τὰ $f(X), g(X)$ εἶναι* πρῶτα μεταξύ τους.

Ἀναφορὲς

[1] Δ. Βάρσος, Δ. Δεριζιώτης, Γ. Εμμανουήλ, Μ. Μαλιάκας, Ο. Ταλέλλη, *Μια Εισαγωγή στην Άλγεβρα*, Γ΄ έκδοση, Εκδόσεις ΣΟΦΙΑ, Αθήνα 2012.