ΘΕΩΡΙΑ ΣΩΜΑΤΩΝ

Ἐαρινὸ Ἑξάμηνο 2016

Καθηγητὴς Ν. Γ. Τζανάκης

Ἐργαλειοθήκη

Τελευταία ἐνημέρωση 23-4-2016

Στὰ παρακάτω, $K, L, \dots$ εἶναι σώματα. Ἡ ἔκφραση « τὸ πολυώνυμο $f(X) \in K[X]$ εἶναι ἀνάγωγο» ἐννοεῖ ὅτι τὸ $f(X)$ ἔχει συντελεστὲς στὸ K καὶ εἶναι ἀνάγωγο πάνω ἀπὸ τὸ K.

1. Ἂν $p(X), f(X) \in K[X]$ καὶ τὸ $p(X)$ εἶναι ἀνάγωγο, τότε, ἢ $p(X)|f(X)$ ἢ τὰ $p(X), f(X)$ εἶναι πρῶτα μεταξύ τους.

2. Ἂν $d(X)$ εἶναι μκδ τῶν $f(X), g(X) \in K[X]$, τότε ὑπάρχουν $f_1(X), g_1(X) \in K[X]$, τέτοια ὥστε $f_1(X)f(X) + g_1(X)g(X) = d(X)$.

3. Ἂν L εἶναι ἐπέκταση τοῦ K, $f(X), p(X) \in K[X]$ μὲ τὸ $p(X)$ ἀνάγωγο (πάνω ἀπὸ τὸ K) καὶ τὸ $v \in L$ εἶναι κοινὴ ρίζα τῶν $f(X), p(X)$, τότε $p(X)|f(X)$.

4. *Κριτήριο Eisenstein*. Ἔστω $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ καὶ p πρῶτος, τέτοιος ὥστε

   (α′) $p|a_i \ \forall i = 0, 1, \dots, n-1$ (β′) $p \nmid a_n$ (γ′) $p^2 \nmid a_0$.

   Τότε, τὸ $f(X)$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ $\mathbb{Q}$.

5. Ἂν τὸ $f(X) \in K[X]$ εἶναι βαθμοῦ 2 ἢ 3, τότε, τὸ νὰ δείξω ὅτι τὸ $f(X)$ εἶναι ἀνάγωγο πάνω ἀπ' τὸ K ἰσοδυναμεῖ μὲ τὸ νὰ δείξω ὅτι τὸ $f(X)$ δὲν ἔχει ρίζα στὸ K.

6. Ἔστω $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$. Ἂν k/ℓ εἶναι ρίζα τοῦ $f(X)$, ὅπου $k, \ell \in \mathbb{Z}$ καὶ $(k, \ell) = 1$, τότε $k|a_0$ καὶ $\ell|a_n$.

7. Ἔστω ὅτι οἱ a, n εἶναι ἀκέραιοι > 1 καὶ ὁ a δὲν εἶναι n-οστὴ δύναμη ἀκεραίου. Τότε $\sqrt[n]{a} \notin \mathbb{Q}$.

8. (α′) Ἔστω R μεταθετικὸς δακτύλιος μὲ μοναδιαῖο. Κάθε πολυώνυμο γράφεται ὡς ἕνα ἄπειρο ἄθροισμα $\sum_{i=0}^{\infty} a_iX^i$, στὸ ὁποῖο ἐννοεῖται ὅτι, ἀπὸ κάποιον δείκτη i_0 καὶ μετά, ὅλοι οἱ συντελεστὲς a_i εἶναι μηδενικοί. Υἱοθετώντας αὐτὸν τὸν συμβολισμό, μποροῦμε

νὰ ὁρίσομε τὶς πράξεις τῶν πολυωνύμων μὲ ποιό συνοπτικὸ καὶ εὔχρηστο τρόπο: Ἂν $f(X) = \sum_{i=0}^{\infty} a_i X^i$ καὶ $g(X) = \sum_{i=0}^{\infty} b_i X^i$, τότε

$$f(X) + g(X) = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

$$f(X) \cdot g(X) = \sum_{i=0}^{\infty} c_i X^i, \quad c_i = a_0 b_i + a_i b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0 = \sum_{\mu+\nu=i} a_\mu b_\nu.$$

Γιὰ κάθε $r \in R$ ἔχομε τὴν ἀπεικόνιση ἐκτίμησης $\epsilon_r : R[X] \to R$, ποὺ ὁρίζεται ὡς ἑξῆς: Ἂν $f(X) = \sum_{i=0}^{\infty} a_i X^i$, τότε $\epsilon_r(f(X)) = \sum_{i=0}^{\infty} a_i r^i =$ (ἐξ ὁρισμοῦ) $f(r)$. Ἡ ϵ_r εἶναι ὁμομορφισμὸς δακτυλίων – *ὁμομορφισμὸς ἐκτίμησης στὸ r* –, ποὺ σημαίνει ὅτι, γιὰ ὁποιαδήποτε $f(X), g(X) \in R[X]$ καὶ ὁποιοδήποτε $r \in R$, ἰσχύουν οἱ σχέσεις $(f \cdot g)(r) = f(r)g(r)$.

(β′) Ἔστω ὅτι R, R' εἶναι μεταθετικοὶ δακτύλιοι μὲ μοναδιαῖα στοιχεῖα 1_R καὶ $1_{R'}$, ἀντιστοίχως, καὶ $\sigma : R \to R'$ ὁμομορφισμὸς δακτυλίων, τέτοιος ὥστε $\sigma(1_R) = 1_{R'}$. Τότε ὁ σ ἐπεκτείνεται σὲ ὁμομορφισμὸ δακτυλίων, γιὰ τὸν ὁποῖο θὰ χρησιμοποιοῦμε πάλι τὸ ἴδιο σύμβολο,

$$R[X] \ni f = \sum_i r_i X^i \overset{\sigma}{\longmapsto} \sigma f = \sum_i \sigma(r_i) X^i \in R'[X].$$

(γ′) Εἰδικὴ περίπτωση: Ἂν $\sigma : K \to K'$ εἶναι ἐπιμορφισμὸς σωμάτων, τότε ἡ ἀπεικόνιση

$$K[X] \ni f = \sum_i k_i X^i \overset{\sigma}{\longmapsto} \sigma f = \sum_i \sigma(k_i) X^i \in K'[X]$$

εἶναι ἐπιμορφισμὸς δακτυλίων. Ἂν ὁ $\sigma : K \to K'$ εἶναι ἰσομορφισμός σωμάτων, τότε ὁ $\sigma : K[X] \to K'[X]$ εἶναι ἰσομορφισμός δακτυλίων.

9. Ἔστω ὅτι τὰ πεπερασμένα τὸ πλῆθος στοιχεῖα $\alpha, \beta, \gamma, \ldots, \alpha', \beta', \gamma', \ldots$ ἀνήκουν σὲ μία ἐπέκταση ἑνὸς σώματος K. (Τὰ $\alpha, \beta, \gamma, \ldots$ δὲν εἶναι, κατ' ἀνάγκη, ἰσοπληθῆ μὲ τὰ $\alpha', \beta', \gamma', \ldots$). Τότε, ἂν θέλομε ν' ἀποδείξομε ὅτι $K[\alpha, \beta, \gamma, \ldots] = K[\alpha', \beta', \gamma', \ldots]$, ἀρκεῖ νὰ δείξομε ὅτι, καθένα ἐκ τῶν $\alpha, \beta, \gamma, \ldots$ ἀνήκει στὸ δεξιὸ μέλος καὶ καθένα ἐκ τῶν $\alpha', \beta', \gamma', \ldots$ ἀνήκει στὸ ἀριστερὸ μέλος.

10. *Σχέσεις ριζῶν-συντελεστῶν ἑνὸς πολυωνύμου – Τῦποι τοῦ Viète*. Ἔστω τὸ πολυώνυμο μὲ συντελεστὲς ἀπὸ ἕνα σῶμα K:

$$a_n X^n + a_{n-1} X^{n-1} + a_{n-2} X^{n-2} + \cdots + a_1 X + a_0 = a_n (X - r_1)(X - r_2) \cdots (X - r_{n-1})(X - r_n), \quad a_n \neq 0.$$

Τότε

$$\sum_{i=1}^{n} r_i = -\frac{a_{n-1}}{a_n}, \quad \sum_{1 \le i < j \le n} r_i r_j = \frac{a_{n-2}}{a_n}, \quad \sum_{1 \le i < j < k \le n} r_i r_j r_j = -\frac{a_{n-3}}{a_n}, \ldots, (r_1 r_2 \cdots r_n) = (-1)^n \frac{a_0}{a_n}.$$

11. Ἔστω ἀκέραιος $n \geq 2$. Οἱ μιγαδικὲς n-οστὲς ρίζες τῆς μονάδας, οἱ διάφορες τοῦ 1, εἶναι οἱ ρίζες τοῦ πολυωνύμου $X^{n-1} + \cdots + X + 1$. Ἂν $n = p$ πρῶτος, τότε τὸ πολυώνυμο αὐτὸ εἶναι ἀνάγωγο.

Ἡ ἀναλυτικὴ ἔκφραση τῶν n-οστῶν ριζῶν τῆς μονάδος εἶναι

$$\cos\frac{2k\pi}{n} + i\frac{2k\pi}{n}, \quad k = 0, 1, \ldots, n-1.$$

Λόγῳ τῶν τύπων τοῦ De Moivre, εἶναι

$$\cos\frac{2k\pi}{n} + i\frac{2k\pi}{n} = \zeta^k, \text{ ὅπου } \zeta = \frac{2\pi}{n} + i\frac{2\pi}{n}.$$

Μ' ἄλλα λόγια, ἡ πολλαπλασιαστικὴ ὁμάδα τῶν n-οστῶν ριζῶν τῆς μονάδος (ὑποομάδα τῆς $\mathbb{C}^*$) εἶναι κυκλικὴ καὶ ἕνας γεννήτοράς της εἶναι ἡ ζ. Κάθε ζ^k μὲ $(k, n) = 1$ εἶναι γεννήτορας τῆς ὁμάδας τῶν n-οστῶν ριζῶν τῆς μονάδος· καὶ ἀντιστρόφως, κάθε γεννήτορας τῆς ὁμάδας τῶν n-οστῶν ριζῶν τῆς μονάδος εἶναι τῆς μορφῆς ζ^k γιὰ κάποιο k πρῶτο πρὸς n.

Οἱ γεννήτορες τῆς ὁμάδας τῶν n-οστῶν ριζῶν τῆς μονάδος λέγονται ἀλλοιῶς καὶ *πρωταρχικὲς n-οστὲς ρίζες τῆς μονάδος*.

12. Ἂν ὁ $n \geq 2$ εἶναι ἀκέραιος, $a \in \mathbb{C}$ καὶ $\theta \in \mathbb{C}$, τέτοιο ὥστε $\theta^n = a$, τότε ὅλες οἱ ρίζες τοῦ $X^n - a$ εἶναι οἱ $\zeta^k\theta$, $k = 0, 1, \ldots, n-1$, ὅπου ζ εἶναι μία ὁποιαδήποτε πρωταρχικὴ n-οστὴ ρίζα τῆς μονάδος (π.χ. $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$).