ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ ΙΙ

30/3/2020

Επανάληψη

Θεμελιώδες Θεώρημα Άλγεβρας

Παρατήρηση Το Θεμ. Θεωρ. Άλγεβρας

Βεβαιώνει την ύπαρξη ρίζας αλλά όχι την κατασκευάζει (δεν μας δίνει τύπο).

Τύποι για τις ρίζες πολυωνύμων

16ος αιώνα : (dal Ferro, Cardano, Tartaglia, Ferrari)

Βρήκαν τύπους για την εύρεση πολυωνύμων 3ου και 4ου Βαθμού. Αυτοί οι τύποι εισάγουν τους μιγαδικούς αριθμούς.

Θεώρημα Abel-Ruffini

Δεν υπάρχει τύπος με ριζικά που να επιλύει τα πολυώνυμα βαθμού 5 με πραγματικούς συντελεστές.

Θεώρημα Galois

Τα πολυώνυμα των οποίων οι ρίζες εκφράζονται από κάποιον τύπο που εμπεριέχει πρόσθεση, αφαίρεση, πολλ., διαίρεση και εξαγωγή ριζικών των συντελεστών, είναι ακριβώς εκείνα για τα οποία η αντίστοιχη ομάδα του Galois είναι επιλύσιμη.

Επιλύσιμες Ομάδες

G πεπερ. ομάδα. Κανόνικη σειρά της G λέγεται μια ακολουθία υποομάδων $G_i \leq 0 \leq i \leq s$ της G ως εξής:

$$G = G_0 \triangleright G_1 \ldots \triangleright G_{s-1} \triangleright G_s = \{e\}$$

Ο φυσικός αριθμός αριθμός s λέγεται μήκος της σειράς και οι ομάδες G_i / G_{i+1}, $0 \leq i \leq s-1$ λέγονται παράγοντες της σειράς. Διαίτερα, αν οι παράγοντες της κανονικής σειράς είναι αβελιανές ομάδες τότε η σειρά λέγεται επιλύσιμη. Μια πεπερασμένη ομάδα G που έχει μία επιλύσιμη σειρά λέγεται επιλύσιμη.

Θεμελιώδες Θεώρημα Galois

Έστω F σώμα και $f(x) \in F[x]$. Έστω E το μικρότερο σώμα που περιέχει το F και όλες τις ρίζες του $f(x)$. Υπάρχει μία πλήρης αντιστοιχία ανάμεσα στα υποσώματα που περιέχουν το F και στις υποομάδες της ομ. Galois του $f(x)$.

Θεώρημα 1.2.1 i) F σώμα έστω $f(x), g(x) \in F[x]$, $g(x) \neq 0$. Τότε $\exists$ μοναδικά πολυώνυμα $q(x), r(x) \in F[x]$ τ.ω. $f(x) = g(x)q(x) + r(x)$ με $\deg r(x) < \deg g(x)$ ή $r(x) = 0$

ii) Έστω F σώμα. Τότε ο δακτύλιος $F[x]$ είναι περιοχή κυρίων ιδεωδών (Π.Κ.Ι.).

Ορισμός: $f(x)$ στο $F[x]$ είναι <u>ανάγωγο</u> αν είναι βαθμού τουλάχιστον 1 και δεν γράφεται σαν γινόμενο 2 πολυωνύμων βαθμού ≥ 1.

· Το $f(x)$ είναι ανάγωγο, τότε κάθε φορά που το $f(x)$ διαιρεί το γινόμενο δύο πολυωνύμων. Πρέπει να διαιρεί αναγκαστικά το ένα από τα δύο.

· Πρόκύπτει ότι κάθε πολ. $f(x) \neq 0$ του $F[x]$ αναλύεται μοναδικά ως γινόμενο $f(x) = u p_1^{t_1}(x) \dots p_s^{t_s}(x)$, όπου $u \in F^*$ και τα $p_i(x)$, $1 \leq i \leq s$ είναι κανονικά ανάγωγα πολυώνυμα.

Πρόταση 1.2.2.

(Οι ρίζες συνδέονται με την παραγοντοποίηση)
Έστω $f(x) \in F[x]$. Το $\alpha \in F$ είναι ρίζα αν-ν $x-\alpha$ διαιρεί το $f(x)$ στο $F[x]$.

Πόρισμα 1.2.3.

$f(x) \in F[x]$ και $\alpha_1, \cdots, \alpha_n \in F$ είναι διακεκριμένες ρίζες του $f(x)$ τότε $f(x) = (x-\alpha_1) \cdots (x-\alpha_n) \cdot p(x)$ όπου $p(x) \in F[x]$.

Ορισμός: Μια **εμφύτευση** σωμάτων (μεταξύ σωμάτων) είναι ένας 1-1 ομομορφισμός δακτυλίων.

Έστω φ εμφ. σωμάτων.
και $\varphi: F \to L$ $\quad \tilde{\varphi}: F[x] \to L[x]$:

$\sum a_i x^i \to \sum \varphi(a_i) x^i$

είναι ο αντίστοιχος ομομ. ανάμεσα στους δακτυλίους πολυων.

Συμβολίζουμε $\tilde{f}(x)$ την εικόνα του $f(x)$ στον $L[x]$. Αν a ρίζα του $f(x)$ τότε $\varphi(a)$ είναι ρίζα του $f(x)$.

Πράγματι

$$\tilde{f}(\varphi(a_1)) = \sum \varphi(c_i)\varphi(a)^i = \sum \varphi(c_i a^i) =$$

$$\varphi\left(\sum c_i a^i\right) = \varphi(f(a)) = \varphi(0) = 0.$$

σελ. 9 Παράδειγμα 1.2.5.

$f(x) = x^3 - 2$. Θα αναλύσουμε το $f(x)$ σε γινόμενο αναγώγων πολυωνύμων του $\mathbb{Q}[x]$, $\mathbb{C}[x]$, $\mathbb{R}[x]$

ρίζες του $f(x)$ στο $\mathbb{C}$:

$b = \sqrt[3]{2}$ ρίζα του $f(x)$

Επομένως, το $x - b \in \mathbb{R}[x]$ διαιρεί το $x^3 - 2$.

Από ευκλ. Αλγ.

$$f(x) = (x-b)(x^2 + bx + b^2).$$

Θέτουμε $p(x) = x^2 + bx + b^2$

Οι άλλες δύο ρίζες του $x^3 - 2$ είναι $\sqrt[3]{2}\left(-\frac{1}{2} \pm \frac{i\sqrt{3}}{2}\right)$.

Θέτουμε τώρα $\omega = -\frac{1}{2} + \frac{i\sqrt{3}}{2} = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$

Παρατηρούμε ότι: $\omega = e^{2\pi i/3}$, $\omega^2 = -\frac{1}{2} - \frac{i\sqrt{3}}{2}$

$\omega^3 = e^{2\pi i} = 1$. Άρα, μπορούμε να βρούμε τις 3 ρίζες του $x^3 - 2$ στο $\mathbb{C}$ ως εξής: $b, \omega b, \omega^2 b$. Επίσης, επισημαίνουμε ότι

i) Καμία από τις ρίζες του $f(x)$ δεν ανήκει στο $\mathbb{Q}[x]$. Δεν υπάρχει πολυώνυμο βαθμού 1 στο $\mathbb{Q}[x]$ που να διαιρεί το $f(x)$. Το f δεν μπορεί να γραφεί ως γινόμενο ~~βαθμού~~ δύο πολυωνύμων ~~το~~ βαθμού μικρότερου του 3. Άρα το $f(x)$ αναγωγό στο $\mathbb{Q}[x]$.

ii) Αφού το $b \in \mathbb{R}$ όπως και οι συνεπ. του $q(x)$, έπεται ότι $x-b$, $q(x) \in \mathbb{R}[x]$. Στο $\mathbb{R}[x]$ ισχύει ότι $f(x) = (x-b)q(x)$. Επομένως, το $f(x)$ δεν είναι αναγωγό στο $\mathbb{R}[x]$. Το $q(x)$ έχει βαθμό 2, και οι ρίζες του δεν ανήκουν στο σώμα $\mathbb{R}$. Άρα, το $q(x)$ είναι αναγωγό στο $\mathbb{R}$. Η ανάλυση του $f(x)$ σε αναγωγούς παράγοντες στο $\mathbb{R}[x]$ είναι $f(x) = (x-b)(x-\omega b)(x-\omega^2 b)$.

iii) Η ανάλυση του $f(x)$ στο $\mathbb{C}[x]$ είναι $f(x) = (x-b)(x-\omega b)(x-\omega^2 b)$ αφού κάθε πολυώνυμο βαθμού 1 είναι αναγωγό.

Πρόταση 1.2.6. $f(x) \in F[x]$, F σώμα

i) Αν $\deg f(x)$ είναι 2 ή 3 τότε $f(x)$ είναι αναγωγό αν-ν το $f(x)$ δεν έχει ρίζες στο F.

ii) Έστω $F \subset E$, όπου E σώμα. Αν το $f(x)$ είναι αναγωγό στον $E[x]$, τότε το $f(x)$ είναι αναγωγό στον $F[x]$

Ορισμός: Έστω Πολυώνυμο $x^n - 1$

οι αναγωγοί παράγοντές του επί των ρητών λέγονται κυκλοτομικά πολυώνυμα.

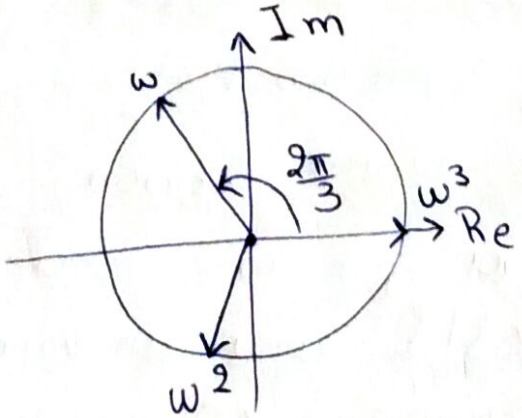
Συμβολίζονται με Φ.

Παράδειγμα 1.2.7. $f(x) = x^3 - 1$

Το πολυώνυμο δεν είναι ανάγωγο στο $\mathbb{Q}[x]$ αφού $f(1) = 0$ και $x^3 - 1 = (x-1)(x^2+x+1)$

Έστω $\Phi_3(x) = x^2 + x + 1$

Οι ρίζες του $\Phi_3(x)$ είναι συζυγείς μιγαδικοί αριθμοί ω, ω^2, όπου $\omega = e^{2\pi i/3}$



Η γρ. παράσταση των ριζών $\omega, \omega^2, \omega^3 = 1$ του πολυωνύμου $x^3 - 1$ στο μιγαδικό επίπεδο.

Οι τρεις ρίζες της μονάδας, δηλαδή οι ρίζες του πολυωνύμου $x^3 - 1$ είναι οι ω, ω^2 και $\omega^3 = 1$, όπου $\omega = e^{2\pi i/3}$. Εύκολα επιβεβαιώνουμε ότι: $(x-\omega)(x-\omega^2) = x^2 + x + 1$. Επομένως,

1. $\omega^2 + \omega + 1 = 0$ και $(\omega^2)^2 + \omega^2 + 1 = 0$

2. $\omega \cdot \omega^2 = 1$.

Το πολυώνυμο $\Phi_3(x)$ είναι ανάγωγο στο $\mathbb{R}[x]$ και στο $\mathbb{Q}[x]$, αφού οι ρίζες του δεν είναι πραγματικοί αριθμοί. Το $\Phi_3(x)$ δεν είναι ανάγωγο στο $\mathbb{C}[x]$. Έτσι, η ανάλυση του x^3-1 σε γινόμενο ανάγωγων πολυωνύμων στους δακτυλίους $\mathbb{R}[x]$ και $\mathbb{Q}[x]$ είναι η ανάλυση της σχέσης

$$x^3-1 = (x-1)(x^2+x+1)$$

ενώ η ανάλυση του x^3-1 σε γινόμενο ανάγωγων πολυωνύμων στον $\mathbb{C}[x]$ είναι

$$x^3-1 = (x-1)(x-\omega)(x-\omega^2).$$

Έστω ένα ανάγωγο πολυώνυμο $p(x) \in F[x]$. $\langle p(x) \rangle$ είναι maximal και ο δακτύλιος $F[x]/\langle p(x) \rangle$ είναι σώμα. Αντίστροφα, τα πρώτα ιδεώδη I του $F[x]$ είναι εκείνα για τα οποία ο δακτύλιος πηλίκο $F[x]/I$ είναι ακέραια περιοχή. Κάθε πρώτο ιδεώδες $I \neq 0$ του $F[x]$ έχει γεννήτορα ένα πρώτο στοιχείο $p(x)$ του $F[x]$. Όμως, το $p(x)$ είναι ανάγωγο στον $F[x]$. Επομένως, κάθε πρώτο μη μηδενικό ιδεώδες του $F[x]$ είναι maximal και έχει γεννήτορα ένα ανάγωγο πολυώνυμο.

Για το ανάγωγο $p(x)$ του $F[x]$ παιτήκαμεν $\phi: F \to F[x]/\langle p(x)\rangle$, $c \mapsto c+\langle p(x)\rangle$, είναι ένας μονομορφισμός σωμάτων. Το σώμα F εμφυτεύται στο σώμα $F[x]/\langle p(x)\rangle$ και το $F[x]/\langle p(x)\rangle$ είναι επέκταση του F μέσω αυτής της εμφύτευσης.

Η $F[x]$ είναι επέκταση του σώματος $\phi(F)$.

Παράδειγμα 1.2.8.

1. Ιδιώδες $I = \langle x^2+1 \rangle$.

Το σώμα $\mathbb{R}[x]/I$ είναι επεκτ. του $\mathbb{R}$ μέσω της εμφύτευσης: $\phi: \mathbb{R} \to \mathbb{R}[x]/I$, $\varphi(r) = r+I$. Τα στοιχεία του $\mathbb{R}[x]/I$ είναι της μορφής $f(x)+I$. Σύμφωνα, όμως, με τον Ευκλ. αλγόριθμο διαίρεσης:

$$f(x) = (x^2+1)\,q(x) + r(x), \quad r(x) \in \mathbb{R}[x], \quad \deg r(x) \leq 1.$$

Επομένως $f(x)+I = r(x)+I$. Άρα, τα στοιχεία του $\mathbb{R}[x]/I$ είναι της μορφής $a+bx+I$, $a,b \in \mathbb{R}$.

Το I είναι ο πυρήνας του επιμορφ. δακτ.

$\mathbb{R}[x] \to \mathbb{C}$, $f(x) \to f(i)$.

Άρα $\varphi : \mathbb{R}[x]/I \to \mathbb{C}$, $f(x)+I \to f(i)$.

είναι ισομορφ. σωμάτων και

$$\varphi(a+bx+I) = a+bi$$

Έτσι, $\varphi \circ \varphi : \mathbb{R} \to \mathbb{C}$, $\varphi \circ \varphi(r) = \varphi(r+I) = r$

είναι εμφύτευση του $\mathbb{R}$ στο $\mathbb{C}$.

2. $I = \langle x^2-3 \rangle$, ιδεώδες του $\mathbb{Q}[x]$. Ο δακτύλιος $E = \mathbb{Q}[x]/I$ είναι σώμα, αφού το πολυώνυμο x^2-3 είναι ανάγωγο στον $\mathbb{Q}[x]$. Τα στοιχεία του E είναι της μορφής $f(x)+I$, όπου $f(x) \in \mathbb{Q}[x]$.

Από Ευκλείδιο Αλγόριθμο Διαίρεσης:

$f(x) = (x^2-3)q(x) + r(x)$, όπου $r(x) \in \mathbb{Q}[x]$, $\deg r(x) < 1$.

Επομένως, $E = \{ax+b+I : a,b \in \mathbb{Q}\}$

Το σώμα E είναι επέκταση του $\mathbb{Q}$ μέσω της εμφύτευσης $c \mapsto c+I$.

Θα υπολογίσουμε το αντίστροφο του x^2+1 στο E. Αφού $x^2+I = 3+I$ έπεται ότι

$$\frac{1}{3}(x^2+1) = \frac{1}{3}x^2 + I = 1+I \Rightarrow (x+I)\left(\frac{1}{3}x+I\right)$$

$= 1+I$, άρα $(x+I)^{-1} = \frac{1}{3}x+I$.

Συμπέρασμα: $(x+1+I)(x+1) = (x^2+x)+I = (x+3)+I$ στο E.

Στην γενική περίπτωση, παρατηρούμε ότι αν $r(x), g(x) \in \mathbb{Q}(x)$ έτσι ώστε $f(x)r(x)+g(x)(x^2-3)=1$, τότε $f(x)r(x)+I = 1+I$ και άρα $(r(x)+I)^{-1} = f(x)+I$.

Έχουμε $r(x)+I$ μη μηδενικό στοιχείο του E, αν-ν $r(x)$ δεν είναι στοιχείο του ιδεώδους I, αν-ν $ΜΚΔ(r(x), x^2-3) = 1$. Σε αυτήν την περίπτωση, από ευκλείδια διαίρεση υπάρχουν $f(x), g(x)$ με $f(x)\cdot r(x) + g(x)(x^2-3) = 1$.

Άρα στο E, $(f(x)+I)(r(x)+I) = 1+I$.

Συνεπώς, το αντίστροφο του $r(x)+I$ στο E είναι το $f(x)+I$.

Η εύρεση αντιστρόφου γίνεται με Ευκ. Αλγόριθμο. Αν για δοθέν $r(x)$ ισχύει ότι $r(x)+I \neq I$, τότε τα πολυώνυμα $f(x), g(x)$ υπάρχουν. Θα εφαρμόσουμε τα παραπάνω για να υπολογίσουμε το $(r(x)+I)^{-1}$, όπου $r(x) = x+2$. Από Ευκ. Διαίρεση του x^2-3 με το $x-2$ βρίσκουμε:

$x^2-3 = (x-2)(x+2)+1 \Rightarrow (2-x)(x+2)+(x^2-3) = 1 \Rightarrow$

$(x+2+I)^{-1} = -x+2+I$.

Επαλήθευση: $(x+2+I)(-x+2+I) = (-x^2+4)+I$.

Αλλά, $x^2+I = 3+I$. Συνεπώς, $(x^2+I)(-x^2+2+I) = (-x^2+4)+I = (-3+4)+I = 1+I$, που είναι το ουδέτερο του E ως προς τον πολλαπλασιασμό.

Πρόταση 1.2.9: Έστω $f(x) \in F[x]$, όπου F σώμα και $\deg f(x) = n < \infty$. Τότε το $f(x)$ έχει το πολύ n ρίζες στο F.

ΠΡΟΣΟΧΗ Το πολυώνυμο $x^2 - 1$ στο $\mathbb{Z}_8[x]$ έχει 4 ρίζες!! τις $[1]_8, [3]_8, [5]_8, [7]_8$.

Απόδειξη Αν $f(x)$ έχει s ρίζες, έστω $a_1, \ldots, a_s$, από Προτ. 1.2.2. έπεται ότι $f(x) = (x-a_1)\cdots(x-a_s)g(x)$, $g(x) \in F[x]$. Συγκρίνοντας τους βαθμούς των πολυωνύμων των δύο μελών προκύπτει ότι $s \leq n$.