Λύσεις Θεμάτων Αλγεβρικής Θεωρίας Αριθμών

Μπιζάνος Κωνσταντίνος

23 Αυγούστου 2024

1. Έστω $K \subseteq L$ πεπερασμένη και διαχωρίσιμη επέκταση με $[L : K] = n$ και $\sigma_i \colon L \to N$ οι K - μονομορφισμοί του L στην κανονική θήκη N. Αν $L = K(\vartheta)$ και $f(x) = \mathrm{Irr}(\vartheta, K)$, τότε έχουμε ότι $f(x) = \prod_{i=1}^{n} (x - \vartheta_i)$, όπου $\vartheta_i = \sigma_i(\vartheta)$. Τότε, η $D_{L/K}\left(1, \vartheta, \ldots, \vartheta^{n-1}\right) = \det\left(\vartheta_i^j\right)^2$ είναι μια ορίζουσα Vandermonde και έχουμε ότι

$$D_{L/K}(\vartheta) \coloneqq D_{L/K}\left(1, \vartheta, \ldots, \vartheta^{n-1}\right) = \prod_{1 \le i < j \le n} (\vartheta_i - \vartheta_j) \neq 0.$$

Ισχύει ότι

$$D(\vartheta) = (-1)^{n(n-1)/2} N_{L/K}\left(f'(\vartheta)\right).$$

Απόδειξη. Από την παραπάνω παρατήρηση έχουμε ότι

$$\begin{aligned} D(\vartheta) = \prod_{1 \le i < j \le n} (\vartheta_i - \vartheta_j) &= (-1)^{n(n-1)/2} \prod_{i=1}^{n} \prod_{j \neq i} (\vartheta_i - \vartheta_j) \\ = \quad (-1)^{n(n-1)/2} \prod_{i=1}^{n} \prod_{j \neq i} (x - \vartheta_j) \Big|_{x=\vartheta_i} &= (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\vartheta_i) \\ = \quad (-1)^{n(n-1)/2} N_{L/K}\left(f'(\vartheta)\right) & \end{aligned}$$

□

2. Να δείξετε ότι

$$D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = (-1)^{(p-1)(p-2)/2} \cdot p^{p-2}.$$

Λύση. Αφού $(x-1)f(x) = x^p - 1$, παραγωγίζοντας, έχουμε ότι $f'(\zeta_p) = \frac{p \cdot \zeta_p^{p-1}}{\zeta_p - 1}$. Έχουμε ότι

$$N(p) = p^{p-1},\ N\left(\zeta_p^{p-1}\right) = (-1)^{(p-1)^2} \quad \text{και} \quad N(\zeta_p - 1) = (-1)^{p-1}p.$$

Από το παραπάνω θεώρημα και την πολλαπλασιαστικότητα της νόρμας προκύπτει ότι

$$D_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = (-1)^{(p-1)(p-2)/2} \cdot p^{p-2}.$$

■

3. Βρείτε μια βάση ακεραιότητας του $K = \mathbb{Q}(\sqrt{d})$, όπου d είναι ελεύθερος τετραγώνου.

Λύση. Διακρίνουμε δύο περιπτώσεις.

(α) Αν $d \not\equiv 1 \mod 4$, τότε θ.δ.ο. $\left\{1, \sqrt{d}\right\}$ είναι βάση ακεραιότητας του K. Υπολογίζουμε

$$D_K\left(1, \sqrt{d}\right) = 4d$$

Αν $H = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, τότε έστω $m = [R_K : H]$ και μάλιστα

$$D_K\left(1, \sqrt{d}\right) = 4d = m^2 D_K$$

Αν $m \neq 1$, τότε $m = 2$ και μάλιστα $D_K = d \not\equiv 0, 1 \mod 4$ και καταλήγουμε σε άτοπο.

(β) Αν $d \equiv 1 \mod 4$, θ.δ.ο. $\left\{1, (1+\sqrt{d})/2\right\}$ είναι βάση ακεραιότητητας. Πράγματι,

$$D_K\left(1, (1+\sqrt{d})/2\right) = d$$

όπου η παραπάνω διακρίνουσα είναι ελεύθερη τετραγώνου, συνεπώς το παραπάνω σύνολο είναι βάση ακεραιότητας.

■

4. Ισχύει ότι $D_K \equiv 0, 1 \mod 4$.

Απόδειξη. Έστω $\omega_1, \ldots, \omega_n$ βάση ακεραιότητας του K. Αν με $\omega_i^{(j)}$ συμβολίζουμε τα συζυγή των ω_i, τότε έχουμε ότι $D_K^{1/2} = \det\left[\omega_i^{(j)}\right]$. Από εναλλακτικό ορισμό της ορίζουσας έχουμε ότι

$$\det\left[\omega_i^{(j)}\right] = \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} \omega_i^{\sigma(i)} = \underbrace{\sum_{\sigma\in A_n} \prod_{i=1}^{n} \omega_i^{\sigma(i)}}_{A} - \underbrace{\sum_{\sigma\in S_n\setminus A_n} \prod_{i=1}^{n} \omega_i^{\sigma(i)}}_{B}$$

Συνεπώς, έχουμε ότι $D_K = (A-B)^2 = (A+B)^2 - 4AB$. Αν δείξουμε ότι $A+B, AB \in \mathbb{Q}$, δεδομένου ότι $A+B, AB$ είναι ακέραιοι αλγεβρικοί πάνω από το $\mathbb{Z}$ σε μια κανονική θήκη N, τότε θα έχουμε ότι $A+B, AB \in \mathbb{Z}$. Δεδομένου αυτού θα έχουμε ότι

$$D_K \equiv (A+B)^2 \equiv 0, 1 \mod 4.$$

Παρατηρήστε ότι $A+B, AB$ παραμένουν αναλλοίωτα στις δράσεις των $\sigma \in \mathrm{Gal}(N, \mathbb{Q})$ και αφού $N/\mathbb{Q}$ είναι επέκταση Galois, τότε έχουμε ότι

$$A+B, AB \in \mathrm{Fix}\left[\mathrm{Gal}(N, \mathbb{Q})\right] = \mathbb{Q}.$$

□

5. Έστω L/K επέκταση Galois και $G = \mathrm{Gal}(L/K)$.

(α) Έστω $\mathfrak{p}$ πρώτο ιδεώδες του K που αδρανεί στην επέκταση. Να δείξετε ότι G είναι κυκλική.

(β) Αν $\mathfrak{p}$ διακλαδίζεται πλήρως σε κάθε ενδιάμεση επέκταση $K \subseteq M \subsetneq L$ και δεν διακλαδίζεται στο L, τότε δείξτε ότι δεν υπάρχει γνήσια ενδιάμεση επέκταση.

(γ) Με τις παραπάνω προϋποθέσεις ότι η G κυκλική τάξης πρώτου αριθμού.

Λύση. (α) Αφού $\mathfrak{p}$ αδρανεί, συνεπώς (αν $\mathfrak{q}$ πάνω από το $\mathfrak{p}$) $e = r = 1$. Όμως,

$$|G_T| = e = 1, \quad r = 1 = [G : G_Z(\mathfrak{q}/\mathfrak{p})], \quad \text{και} \quad G_Z/G_T \cong \mathrm{Gal}\left(R_L/\mathfrak{q}/R_K/\mathfrak{p}\right)$$

Συνδυάζοντας τα παραπάνω με το γεγονός ότι $\mathrm{Gal}\left(R_L/\mathfrak{q}/R_K/\mathfrak{p}\right)$ είναι κυκλική, τότε έχουμε το ζητούμενο.

(β) Αφού $\mathfrak{p}$ δεν διακλαδίζεται στο L, τότε $e = e(\mathfrak{q}/\mathfrak{p}) = 1$. Έστω M ενδιάμεσο σώμα με $M \subsetneq L$. Έχουμε ότι

$$1 = e(\mathfrak{q}/\mathfrak{p}) = e(\mathfrak{q}/\mathfrak{q}_M) \cdot e(\mathfrak{q}_M/\mathfrak{p}) \Rightarrow e(\mathfrak{q}_M/\mathfrak{p}) = 1$$

Αφού $\mathfrak{p}$ διακλαδίζεται πλήρως στο M, τότε έχουμε ότι

$$[M : K] = e(\mathfrak{q}_M/\mathfrak{p}) = 1$$

Άρα, $M = K$.

(γ) Άμεσο από (α) και (β).

■

6. Η norm πρώτου ιδεώδους του K είναι ίση με δύναμη κάποιου πρώτου αριθμού.

Απόδειξη. Έστω $\mathfrak{p} \in \mathrm{Spec}(\mathcal{R}_K)$ μη μηδενικό. Τότε, $\mathfrak{p}$ είναι μέγιστο, άρα το πηλίκο $\mathcal{R}_K/\mathfrak{p}$ είναι ένα πεπερασμένο σώμα, του οποίου το πλήθος ισούται με κάποια δύναμη πρώτου αριθμού. □

7. Έστω $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ και δίνεται ότι ο δακτύλιος των ακεραίων του K είναι ο $R = \mathbb{Z}\left(\sqrt[3]{2}\right)$. Να βρείτε τα ιδεώδη που διαιρούν τα $3, 5$.

Λύση. Ενδεικτικά θα βρούμε τα ιδεώδη που διαιρούν το 3. Αν $\vartheta = \sqrt[3]{2}$, εχουμε ότι $f(x) = x^3 - 2 = \mathrm{Irr}(\vartheta, \mathbb{Q})$ και μάλιστα

$$f(x) = x^3 - 2 = x^3 - 8 = (x-2)^3 \mod \mathbb{F}_3[x]$$

Συνεπώς, έχουμε ότι

$$3R = \langle 3, \vartheta - 2\rangle^3$$

από την παραπάνω ανάλυση σε πρώτα ιδεώδη προκύπτει άμεσα οι ζητούμενοι διαιρέτες. ■

8. (α) Να ορισθεί η ομάδα κλάσεων.

(β) Έστω A ακέραιο ιδεώδες του K, για το οποίο υπάρχει m φυσικός αριθμός ώστε A^m να είναι κύριο με $(m, \mathfrak{h}_K) = 1$. Τότε, το A είναι κύριο.

Λύση. (α) Έστω K αλγεβρικό σώμα αριθμών με $[K : \mathbb{Q}] = n$, $\mathcal{I}_K$ η ομάδα κλασματικών ιδεωδών του K (χωρίς το 0) και $\mathcal{H}_K = \{a\mathcal{R}_K \mid a \in K \setminus \{0\}\}$. Θα ονομάζουμε ομάδα κλάσεων ιδεωδών την ομάδα πηλίκο

$$\mathcal{C}_K = \mathcal{I}_K/\mathcal{H}_K.$$

Με $\mathfrak{h}_k$ συμβολίζουμε την τάξη της ομάδας $\mathcal{C}_K$

(β) Υπάρχει $x, y \in \mathbb{Z}$ ώστε $1 = xm + y\mathfrak{h}_K$. Τότε, ισχύει ότι

$$A\mathcal{H}_K = A^1\mathcal{H}_K = \left[\left(A^{\mathfrak{h}_K}\right)\right]^y \mathcal{H}_K \cdot [(A^m)]^x \mathcal{H}_K = \mathcal{H}_K.$$

■

9. (α) Έστω L/K επέκταση Galois, $\mathfrak{p}$ πρώτο του K και $\mathfrak{q}$ πάνω από το $\mathfrak{p}$. Να ορισθεί η ομάδα ανάλυσης $G_Z(\mathfrak{q}/\mathfrak{p})$ του $\mathfrak{q}$ πάνω από το $\mathfrak{p}$.

(β) Έστω $\mathfrak{q}_1, \mathfrak{q}_2$ πρώτα ιδεώδη του L. Αν $\mathfrak{p} = \mathfrak{q}_1 \cap R_K = \mathfrak{q}_2 \cap R_K$, δείξτε ότι $G_Z(\mathfrak{q}_1, \mathfrak{p})$ και $G_Z(\mathfrak{q}_2, \mathfrak{p})$ είναι συζυγείς.

(α)

(β) Έχουμε ότι $\mathfrak{p} = \mathfrak{q}_1 \cap R_K = \mathfrak{q}_2 \cap R_K$ είναι πρώτο και $\mathfrak{q}_1, \mathfrak{q}_2$ πάνω από το $\mathfrak{p}$. Αφού η $G = \mathrm{Gal}(L/K)$ δρά μεταβατικά στο σύνολο των πρώτων ιδεωδών που βρίσκονται στην ανάλυση του $\mathfrak{p}R_L$, τότε υπάρχει $\sigma \in G$ τ.ω. $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. Δείξτε ότι

$$\sigma G_Z(\mathfrak{q}_1, \mathfrak{p})\sigma^{-1} = G_Z(\sigma(\mathfrak{q}_1), \mathfrak{p}) = G_Z(\mathfrak{q}_2, \mathfrak{p})$$

10. (α) Έστω K αλγεβρικό σώμα αριθμών και R ο δακτύλιος των αλγεβρικών αριθμών. Να αποδειχθεί ότι η ομάδα των μονάδων $E(R) = \{\epsilon \in R \mid N(\epsilon) = \pm 1\}$.

(β) Να υπολογιστεί η ομάδα των μονάδων του $\mathbb{Q}(\sqrt{d})$, όπου $d < 0$.

Λύση. 1. Έστω $\epsilon \in E(R)$, τότε υπάρχει ϵ' με $\epsilon\epsilon' = 1 \Rightarrow N(\epsilon\epsilon') = N(\epsilon)N(\epsilon') = 1$. Όμως $N(\epsilon), N(\epsilon') \in \mathbb{Z}$, συνεπώς $N(\epsilon) = \pm 1$.

Αντίστροφα, έστω $\epsilon \in R$ με $N(\epsilon) = \pm 1$, τότε αν $f(x) = \chi_{A(a)}(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$, όπου

$$N(\epsilon) = (-1)^n a_0 = \pm 1$$

Συνεπώς

$$\epsilon \left(\epsilon^{n-1} + \sum_{i=1}^{n-1} a_i x^i \right) = \pm 1$$

και έχουμε το ζητούμενο.

(β) Συμβολίζουμε με

$$\omega_m = \begin{cases} \sqrt{m}, & m \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{m}}{2}, & \text{αν } m \equiv 1 \mod 4 \end{cases}$$

Συνεπώς, αν $\varepsilon = a + b\omega_n$ με $a, b \in \mathbb{Z}$ αντιστρέψιμο, τότε έχουμε ότι

$$N_K(\varepsilon) = \begin{cases} a^2 - mb^2, & m \equiv 2, 3 \mod 4 \\ a^2 + ab + \frac{1-m}{4}b^2, & \text{αν } m \equiv 1 \mod 4 \end{cases} = \pm 1.$$

Διακρίνουμε περιπτώσεις :

(α) Υποθέτουμε ότι $m < 0$.

- Αν $m \equiv 2, 3 \mod 4$, τότε $a^2 + |m|b^2 = 1$.
  - Αν $|m| > 1$, τότε έχουμε ότι $a = \pm 1$ και $b = 0$, άρα $\varepsilon = \pm 1$.
  - Αν $m = -1$, τότε $a^2 + b^2 = 1$, συνεπώς έχουμε τέσσερεις λύσεις $a = \pm 1$ και $b = 0$ και $a = 0$ και $b = \pm 1$. Δηλαδή $\varepsilon = \pm 1$ ή $\pm i$
- Αν $m \equiv 1 \mod 4$, έχουμε ότι

$$a^2 + ab + \frac{1-m}{4}b^2 = \left(a + \frac{b}{2}\right)^2 + \frac{|m|}{4}b^2 = 1.$$

  - Αν $|m| > 4$, τότε όμοια έχουμε ότι $b = 0$ και $a = \pm 1$.
  - Αν $|m| \leq 4$ και $m \equiv 1$, τότε $m = -3$. Παρατηρήστε ότι για $|b| \geq 2$ δεν υπάρχουν λύσεις. Για $b = 1$, προκύπτει ότι $a^2 + a + 1 = 1$, άρα $a = 0$ ή $a = -1$. Τέλος, αν $b = 0$, έχουμε ότι $a = \pm 1$ και για $b = -1$ έχουμε $a = 0$.

■

11. Να υπολογιστεί ο αριθμός κλάσεων του αλγεβρικού σώματος αριθμών $\mathbb{Q}(\sqrt[3]{2})$. Δίνεται ο δακτύλιος ακέραιων αλγεβρικών $\mathbb{Z}(\sqrt[3]{2})$.

Λύση. Υπολογίζουμε τη σταθερά του Minkowski $M_K = 2,34$. Συνεπώς σε κάθε κλάση $c \in \mathcal{C}_K$ υπάρχει ένα ακέραιο ιδεώδες A τ.ω. $N_K(A) < M_K$, άρα $N_K(A) = 1$ ή $N_K = 2$.

- Αν $N_K(A) = 1$ έχουμε ότι $1 \in A$, δηλαδή $A = R_K$.
- Αν $N_K(A) = 2$, τότε A είναι πρώτο και μάλιστα $2 \in A$, δηλαδή $A | 2R_K$. Άρα, αρκεί να αναλύσουμε το $2R_K$ σε ανάλυση πρώτων ιδεωδών. Έχουμε ότι

$$x^3 - 2 = x^3 \mod \mathbb{F}_2[X]$$

άρα

$$2R_K = \left\langle 2, \sqrt[3]{2} \right\rangle^3$$

Συνεπώς $A = \langle 2, \sqrt[3]{2} \rangle = \sqrt[3]{2}R_K$, και αφού A είναι κύριο συμπεραίνουμε ότι $\mathfrak{h}_K = 1$.

■