

Решения на Домашно задание 3
Специалност Математика, Втори Курс
January 15, 2014

Задача 1. Нека α е корен на полинома $f(x) = x^3 - 2x + 2 \in \mathbb{Q}[x]$ и $K = \mathbb{Q}(\alpha)$. Да се докаже, че $[K : \mathbb{Q}] = 3$ и числата $1, \alpha, \alpha^2$ образуват базис на K над $\mathbb{Q}$. Да се изрази чрез този базис числото $\beta = \frac{\alpha}{1-\alpha}$.

Решение.

- Тъй като полиномът f няма рационални корени, той е неразложим и, следователно, е минималния полином на α . Следователно,

$$[K : \mathbb{Q}] = \deg f = 3.$$

- Числата $1, \alpha, \alpha^2$ са линейно независими, защото, в противен случай, α би задоволявало уравнение $a_0 + a_1\alpha + a_2\alpha^2 = 0$ от степен 2, а това би противоречало на факта, че минималният полином на α е f и е от степен 3. Тъй като това са 3 линейно независими вектора в 3-мерно линейно пространство, те образуват базис.
- Полиномът $g(x) = -x + 1$ е взаимно прост с f , защото f и g нямат общи корени. Следователно, по тъждеството на Безу, съществуват полиноми с рационални коефициенти u и v , задоволяващи

$$u(x)g(x) + v(x)f(x) = 1.$$

Посредством алгоритъма на Евклид получаваме

$$f(x) + g(x)(x^2 + x - 1) = 1.$$

Тъй като $f(\alpha) = 0$, получаваме:

$$\frac{1}{g(\alpha)} = \alpha^2 + \alpha - 1.$$

Следователно,

$$\begin{aligned}\beta &= \frac{\alpha}{1-\alpha} \\ &= \frac{-1+\alpha}{1-\alpha} + \frac{1}{1-\alpha} \\ &= -1 + \frac{1}{g(\alpha)} \\ &= \alpha^2 + \alpha - 2.\end{aligned}$$

Задача 2. Нека K е полето на разлагане над $\mathbb{Q}$ на полинома $x^3 - 7$.

- (а) Да се докаже, че $K = \mathbb{Q}(\alpha, \omega)$, където $\alpha \in \mathbb{R}$, $\alpha^3 = 7$, а ω е примитивен трети корен на единицата и $[K : \mathbb{Q}] = 6$.
- (б) Да се намери примитивен елемент θ на разширението $\mathbb{Q} < K$ и минималният полином на θ над $\mathbb{Q}$.

Решение.

- (а) Корените на полинома

$$f(x) = x^3 - 7 = (x - \alpha)(x - \alpha\omega)(x - \alpha\omega^2)$$

над $\mathbb{C}$ са α , $\alpha\omega$ и $\alpha\omega^2$.

От тук виждаме, че полето на разлагане на f , K , се съдържа в $\mathbb{Q}(\alpha, \omega)$, т.е., $K \leq \mathbb{Q}(\alpha, \omega)$. От друга страна, $\omega = \frac{\alpha\omega}{\alpha}$ и, следователно, $\mathbb{Q}(\alpha, \omega) \leq K$. В резултат, $\mathbb{Q}(\alpha, \omega) = K$.

Разглеждаме редицата от разширения

$$K > \mathbb{Q}(\alpha) > \mathbb{Q}.$$

•

$$\begin{aligned} [\mathbb{Q}(\alpha) : \mathbb{Q}] &= \deg_{\mathbb{Q}} \alpha \\ &= \text{степената на минималния полином на } \alpha \\ &= \deg x^3 - 7 = 3. \end{aligned}$$

•

$$\begin{aligned} [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] &= \deg_{\mathbb{Q}(\alpha)} \omega \\ &= \text{степената на минималния полином на } \omega \text{ над } \mathbb{Q}(\alpha). \end{aligned}$$

Минималният полином на ω над $\mathbb{Q}$ е циклотомичният полином $\Phi_3(x) = x^2 + x + 1$, който е неразложим в полето $\mathbb{Q}(\alpha)$ и, следователно остава минимален и над $\mathbb{Q}(\alpha)$. Затова,

$$[K : \mathbb{Q}(\alpha) = \deg \Phi_3 = 2.]$$

•

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

- (б) Имитирайки доказателството на теоремата за примитивния елемент, означаваме с $\alpha_1 = \alpha$, $\alpha_2 = \alpha\omega$, $\alpha_3 = \alpha\omega^2$, $\beta_1 = \omega$ и $\beta_2 = \omega^2$ корените на f и Φ_3 , съответно. Разглеждаме множеството

$$\begin{aligned} M &= \left\{ -\frac{\alpha_i - \alpha_1}{\beta_j - \beta_1} \mid i = 1, 2, 3, j = 2 \right\} \\ &= \left\{ 0, -\frac{\alpha\omega - \alpha}{\omega^2 - \omega}, -\frac{\alpha\omega^2 - \alpha}{\omega^2 - \omega} \right\} \\ &= \left\{ 0, -\frac{\alpha}{\omega}, -\frac{\alpha(\omega - 1)}{\omega} \right\} \end{aligned}$$

Избираме $c = 1 \in \mathbb{Q} \setminus M$. Конструираме $\theta = \alpha + c\beta = \sqrt{7} + \omega$. По построение, минималният полином на θ дели $h(x)$,

$$\begin{aligned} h(x) &= f(x - c\beta_1)f(x - c\beta_2) = f(x - \omega)(x - \omega^2) \\ &= ((x - \omega)^3 - 7)((x - \omega^2)^3 - 7) \\ &= (x^3 - 3\omega x^2 + 3\omega^2 x - 8)(x^3 - 3\omega^2 x^2 + 3\omega x - 8) \\ &= x^6 - 3(\omega + \omega^2)x^5 + (3\omega + 3\omega^2 + 9)x^4 - (9\omega^2 + 9\omega + 8 + 8)x^3 \\ &\quad - (24\omega + 24\omega^2 - 9)x^2 - 24(\omega + \omega^2)x + 64 \\ &= x^6 + 3x^5 + 6x^4 - 7x^3 + 15x^2 + 24x + 64 \end{aligned}$$

(В тези изчисления използваме многократно факта, че ω и ω^2 са корените на полинома $x^2 + x + 1$ и, по формулите на Виет, $\omega + \omega^2 = -1$ и $\omega^3 = 1$.)

Тъй като $\deg h = 6 = \deg_{\mathbb{Q}} \theta$, минималният полином на θ е h .

Задача 3. Нека $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.

- (а) Да се докаже, че $[K : \mathbb{Q}] = 4$ и числата $1, \sqrt{5}, \sqrt{7}, \sqrt{35}$ образуват базис на K над $\mathbb{Q}$.
- (б) Да се намери примитивен елемент θ на разширението $\mathbb{Q} < K$ и минималният полином на θ над $\mathbb{Q}$. Да се изразят числата $1, \sqrt{5}, \sqrt{7}, \sqrt{35}$ чрез базиса $1, \theta, \theta^2, \theta^3$

Решение.

- (а) • Разглеждаме редицата от разширения

$$K > \mathbb{Q}(\sqrt{5}) > \mathbb{Q}.$$

Степента на разширението $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$ е 2, защото $\sqrt{5}$ е ирационално число с минимален полином $f(x) = x^2 - 5$. Числото $\sqrt{7}$ е корен на полинома $g(x) = x^2 - 7$ и следователно степента му задоволява неравенството: $\deg_{\mathbb{Q}(\sqrt{5})} \sqrt{7} \leq \deg g = 2$ Тъй като не е елемент на полето $\mathbb{Q}(\sqrt{5})$, имаме:

$$\deg_{\mathbb{Q}(\sqrt{5})} \sqrt{7} = 2$$

Следователно, $[K : \mathbb{Q}(\sqrt{5})] = 2$. От тук имаме

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 4.$$

Твърдим, че числата $1, \sqrt{5}, \sqrt{7}, \sqrt{35}$ са линейно независими над $\mathbb{Q}$. За целта, разглеждаме произволна линейна комбинация над $\mathbb{Q}$

$$a_0 + a_1\sqrt{5} + a_2\sqrt{7} + a_3\sqrt{35} = 0$$

От тук, в случай, че $a_2 \neq 0$ и $a_3 \neq 0$ едновременно, бихме могли да изразим $\sqrt{7} = -\frac{a_0+a_1\sqrt{5}}{a_2+a_3\sqrt{5}}$, което противоречи на $\sqrt{7} \notin \mathbb{Q}$. Следователно $a_2 = a_3 = 0$ и, следователно, $a_0 + a_1\sqrt{5} = 0$. Поради ирационалността на $\sqrt{5}$, това е единствено възможно за $a_0 = a_1 = 0$. Следователно, $1, \sqrt{5}, \sqrt{7}, \sqrt{35}$ са линейно независими. Поради това, че размерността на K като линейно пространство над $\mathbb{Q}$ е точно 4, това означава, че тези числа образуват базис.

- (б) Означаваме с $\alpha_1 = \sqrt{5}$, $\alpha_2 = -\sqrt{5}$, $\beta_1 = \sqrt{7}$ и $\beta_2 = -\sqrt{7}$ корените на f и g , съответно. Конструираме множеството

$$M = \left\{ -\frac{\alpha_i - \alpha_1}{\beta_j - \beta_1} \mid i = 1, 2 \ j = 2 \right\} = \left\{ 0, -\sqrt{\frac{5}{7}} \right\}$$

Избираме $c = 1 \in \mathbb{Q} \setminus M$ и разглеждаме $\theta = \alpha + c\beta = \sqrt{5} + \sqrt{7}$. Съгласно Теоремата за примитивния елемент, θ е примитивен елемент на разширението $K > \mathbb{Q}$, т. е., $K = \mathbb{Q}(\theta)$. Минималният полином на θ е полином от степен $\deg_{\mathbb{Q}} K$ и дели полинома h .

$$\begin{aligned} h(x) &= f(x - c\beta_1)f(x - c\beta_2) = f(x - \sqrt{7})f(x + \sqrt{7}) \\ &= (x^2 - \sqrt{7}x + 2)(x^2 + \sqrt{7}x + 2) = x^4 - 24x^2 + 4. \end{aligned}$$

Поради това, че h има степен 4 това означава, че h е минималният полином на θ . Лесно се намира, че

$$\begin{aligned} \theta &= \sqrt{5} + \sqrt{7} \\ \theta^2 &= 12 + 2\sqrt{35} \\ \theta^3 &= 26\sqrt{5} + 22\sqrt{7}. \end{aligned}$$

Следователно,

$$\begin{aligned} \sqrt{35} &= \frac{1}{2}\theta^2 - 6 \\ \sqrt{5} &= -\frac{1}{4}\theta^3 + \frac{13}{2}\theta \\ \sqrt{7} &= \frac{1}{4}\theta^3 - \frac{11}{2}\theta. \end{aligned}$$

Задача 4. Да се намери циклотомичния полином Φ_{35} .

Решение. Съгласно теорема доказана на лекции,

$$\begin{aligned}\Phi_{35}(x) &= \prod_{d|35} (x^d - 1)^{\mu(\frac{35}{d})} \\&= \frac{(x-1)(x^{35}-1)}{(x^5-1)(x^7-1)} \\&= \frac{x^{28} + x^{21} + x^{14} + x^7 + 1}{x^4 + x^3 + x^2 + x + 1} \\&= x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} \\&\quad + x^{12} - x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1.\end{aligned}$$