

Álgebra

Andrey

Definição 1. α e β são conjugados quando, se $P \in \mathbb{Q}[x]$, então $P(\alpha) = 0 \iff P(\beta) = 0$.

Definição 2. Seja $I_\alpha = \{P \in \mathbb{Q}[x] : P(\alpha) = 0\}$. O elemento mônico de menor grau em I_α é o polinômio minimal de α , P_α .

Definição 3. Podemos redefinir α e β conjugados como $P_\alpha(\beta) = 0$.

Lema 1. P_α é irredutível.

Lema 2. $Q(\alpha) = 0$ e Q irredutível $\implies Q = c \cdot P_\alpha$.

Definição 4. $P \in \mathbb{Q}[x_1, x_2, \dots, x_n]$ é simétrico se $P(x_1, x_2, \dots, x_n) = P(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)})$, para toda permutação π de $\{1, 2, \dots, n\}$.

Teorema 1. x_1, x_2, \dots, x_n . $\sigma_k := \sum_{i \in \text{kelem}} x_i$. P é simétrico \iff existe $Q \in \mathbb{Q}[y_1, y_2, \dots, y_n]$ $P(x_1, x_2, \dots, x_n) = Q(\sigma_1, \sigma_2, \dots, \sigma_n)$.

Corolário 1. $\alpha_1, \alpha_2, \dots, \alpha_n$ são conjugados, então $\sigma_i \in \mathbb{Q}$.

Teorema 2. α e β são algébricos, então $\alpha + \beta$, $\alpha\beta$, α^{-1} e α^2 são algébricos.

Tem muitos jeitos de provar.

Definição 5. (Extensão de Corpo)

Definição 6. (Grau de uma Extensão) Dimensão de K , visto como espaço vetorial em \mathbb{R}

Problema 1 (OBM 2017, 6). Seja a inteiro positivo e p um divisor primo de $a^3 - 3a + 1$, com $p \neq 3$. Prove que p é da forma $9k + 1$ ou $9k - 1$, sendo k um inteiro.

Teorema 3. Φ_n é irredutível.

Lema 3. Φ_p é irredutível.

Lema 4. (Critério de Eisenstein)

Lema 5. Φ_{2^n} é irredutível.

Demonstração. Vamos mostrar que, se ω é raiz de $x^{2^{n-1}} + 1$, então $P_\omega = P_{\omega^3} = P_{\omega^5} = P_{\omega^7}$.

Lema 6. Seja $a \in \mathbb{Z}_{2^n}^\times$, existe m tal que $a \equiv 3^m$ ou $a \equiv 5^m$ ou $a \equiv 7^m$.

Problema 2. Seja $f \in \mathbb{Q}[x]$ não constante. Se $\alpha^3 - 3\alpha + 1 = f(\alpha)^3 - 3f(\alpha) + 1 = 0$. Prove que $(f^n(\alpha))^3 - 3f^n(\alpha) + 1 = 0$.

Problema 3. Seja n ímpar e $a_1, a_2, \dots, a_n \in \mathbb{Z}$ distintos. Prove que $(x - a_1)(x - a_2) \cdots (x - a_n) - 1$ é irredutível em $\mathbb{Q}[x]$.

Lema 7. (Lema de Gauss)

Problema 4 (IMO 1993, 1). Let $n > 1$ be an integer and let $f(x) = x^n + 5 \cdot x^{n-1} + 3$. Prove that there do not exist polynomials $g(x), h(x)$, each having integer coefficients and degree at least one, such that $f(x) = g(x) \cdot h(x)$.

Problema 5. Existe $P \in \mathbb{Z}[x]$, irredutível em $\mathbb{Z}[x]$, mas redutível em $\mathbb{Z}_q[x]$, para todo q primo.

Solução. $P(x) = x^4 - 10x^2 + 1$.

Problema 6. Prove que, para todo n , existe $f \in \mathbb{Z}_p[x]$ irredutível tal que o grau de f é n .

Problema 7. Prove que, se d divide $a^4 + a^3 + 2a^2 - 4a + 3$, então $d \equiv x^4 \pmod{13}$.