Terceira Lista de Exercícios: Corpos e Polinômios

MA 673, Elementos de Álgebra, Segundo semestre de 2017, Turma Z

Ex. 1. Quais são os polinômios irredutíveis sobre os corpos dos complexos? E dos reais?

Ex. 2. a) O número e é raiz de algum polinômio com coeficientes reais? E racionais?

b) Seja $a = \sqrt{3} - \sqrt{2}$, encontrar um polinômio com coeficientes racionais tal que a seja uma das raízes deste polinômio.

c) O mesmo como (b) para $a = 2 - i\sqrt{3}$ onde $i^2 = -1$.

Ex. 3. Decompor, sobre $\mathbb{C}$, o polinômio $x^4 + 16$, em produto de polinômios irredutíveis. Decompor o mesmo polinômio em produto de irredutíveis sobre $\mathbb{R}$.

Ex. 4. Decompor o polinômio f em produto de irredutíveis sobre $\mathbb{R}$:

a) $f = x^3 + x + 2$; b) $f = x^5 + x^3 + x^2 + 1$.

Ex. 5. Seja $f(x) = x^4 + 4$. Escrever f como produto de polinômios irredutíveis sobre $\mathbb{C}$ e sobre $\mathbb{R}$. Este polinômio é irredutível sobre $\mathbb{Q}$?

Ex. 6. Seja $f(x) = x^2 + 1 \in \mathbb{Q}[x]$, mostrar que o anel quociente $\mathbb{Q}[x]/(x^2 + 1)$ é um corpo isomorfo ao corpo $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$, onde $i^2 = -1$.

Ex. 7. Sejam $K \subseteq L$ dois corpos, $f \in K[x]$ um polinômio não constante e $\alpha \in L$ uma raiz de f. Mostrar que $K[\alpha] = K(\alpha)$ é um corpo.

Ex. 8. Seja $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ e seja $\alpha \in \mathbb{R}$ uma raiz de f, mostrar que $\mathbb{Q}[\alpha]$ é um corpo. Considerando este corpo como espaço vetorial sobre $\mathbb{Q}$, qual a sua dimensão? Encontrar uma base deste espaço vetorial.

Ex. 9. Seja α uma raiz de $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$ e seja $K = \mathbb{Q}(\alpha)$. Mostrar que K é um espaço vetorial sobre $\mathbb{Q}$ de dimensão 3 e que 1, α, α^2 formam uma base. Apresentar nesta base os elementos α^5, $\alpha^6 - 3\alpha^5 - 2\alpha^4 + \alpha + 1$, $(\alpha^2 - 1)^2$.

Ex. 10. Mostrar que $\mathbb{R}[x]/(x + \sqrt{3}) \cong \mathbb{R}$.

Ex. 11. Usando redução módulo algum número primo adequado, mostrar que o polinômio $f(x)$ é irredutível sobre o corpo dos racionais:

a) $f(x) = 3x^3 + 7x^2 + 10x - 5$. b) $f(x) = 7x^4 - 6x^3 + 8x^2 + 3x + 5$.

c) $f(x) = 9x^4 + 4x^3 - 3x + 7$

Ex. 12. Usando o critério de Eisenstein mostrar que o polinômio $f(x)$ é irredutível sobre os racionais.

a) $f = 5x^{11} - 6x^4 + 12x^3 + 36x^2 - 6$. b) $f = x^4 + 10x - 5$.

c) $f = x^n - 101$ para todo $n \geq 1$. d) $f = 4x^3 - 15x^2 + 60x - 180$.

e) $f = x^5 - 36x^4 + 6x^3 + 30x^2 - 24$. f) $f = x^3 + 3x^2 + 5x + 5$. (Dica: substituir x por $x - 1$.)

g) $f = x^4 + 1$. (Dica: Substituir x por $x + 1$.) h) $f = [(x + 2)^p - 2^p]/x$, onde p é primo.

Ex. 13. Mostrar que o polinômio f é irredutível sobre $\mathbb{Q}$.

a) $f = 2x^5 - 21x^2 + 42x + 63$.

b) $f = x^4 - 8x^3 + 21x^2 - 11x - 11$. (Dica: considerar $f(x + 2)$.)

c) $f = x^p - px + 2p - 1$, onde p é número primo. (Dica: Considerar $f(x + 1)$.)

d) $f = x^p + px^{p-1} + px + 3p + 1$, $p > 2$ é primo. (Dica: Se $p > 3$, considerar $f(x - 1)$.)

Ex. 14. Seja $f \in \mathbb{Z}[x]$. Se $f(0)$ e $f(1)$ são ímpares, mostrar que f não tem raízes inteiras.

Ex. 15. Entre os números abaixo, quais podem ser iguais à característica de um corpo:

0, 1, 2, 3, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 24, 25, 27, 28, 32, 1024.

Quais desses números representam a quantidade de elementos em algum corpo?

Ex. 16. a) Encontrar os polinômios irredutíveis de grau 2 e de grau 3 sobre o corpo de 2 elementos.

b) Construir explícito um corpo de 4 elementos.

Ex. 17. a) Encontrar os polinômios irredutíveis de grau 2 e de grau 3 sobre o corpo de 3 elementos.

b) Construir explícito um corpo de 9 elementos.

Ex. 18. O polinômio $x^4 + 3x^3 + x^2 + 3$ tem raízes no corpo de 5 elementos? Ele é irredutível sobre o mesmo corpo?

Ex. 19. Seja F um corpo com $q = p^n$ elementos onde p é primo. Mostrar que:

a) Se $a \in F$ então $a^q - a = 0$.

b) O corpo F é corpo das raízes do polinômio $f = x^q - x$ sobre $\mathbb{Z}_p$.

c) Se $\phi\colon F \to F$ é definido como $\phi(a) = a^p$ então ϕ é um automorfismo de F (chamado de automorfismo de Frobenius).

d) O grupo F^x é cíclico. Mais geral, se K é corpo e $G \leq H^x$, $|G| < \infty$, então G é cíclico.

e) O corpo de raízes do polinômio $x^{q^m} - x$ sobre F é um corpo com q^m elementos.

f) Para todo p e todo n existe corpo com p^n elementos.

Ex. 20. Se F é um corpo, $|F| = p^n$, onde p é primo, mostrar que para todo k existe um polinômio f, irredutível sobre F tal que o grau de f seja igual a k. (Dica: considerar $g = x^{q^k} - x \in F[x]$, o corpo de raízes de g é um corpo L com q^k elementos. O grupo multiplicativo de L é cíclico por (d), e se a é gerador desse grupo cíclico, mostrar que o polinômio mínimo de a sobre F é irredutível sobre F, e tem grau k.)