3^a Lista de Exercícios de Anéis e Corpos - MAT0264

1^a parte: Polynômios

1. Mostre que:
   (a) $x^2 + x + 1$ é irredutível em $\mathbb{Z}_2[x]$;
   (b) $x^2 + 1$ é irredutível em $\mathbb{Z}_7[x]$;
   (c) $x^3 - 9$ é irredutível em $\mathbb{Z}_{31}[x]$;
   (d) $x^3 - 9$ é redutível em $\mathbb{Z}_{11}[x]$.

2. Seja $f \in \mathbb{Q}[x]$, $f \neq 0$. Mostre que f é divisível pelo quadrado de um polinômio se e só se $\text{mdc}(f, f') \neq 1$.

3. (a) Mostre que se p é um primo, então o polinômio $f(x) = x^n - p$ é irredutível sobre $\mathbb{Q}$, $\forall n \geq 1$.
   (b) Mostre que o polinômio $f(x) = 1 + x + ... + x^{p-1}$, ($p$ primo), é irredutível sobre $\mathbb{Q}$.

4. (a) Decomponha $f(x) = x^4 + 4$ em fatores irredutíveis de $\mathbb{Z}_5[x]$.
   (b) Faça o mesmo para $f(x) = x^3 + 2x + 3$ em $\mathbb{Z}_5[x]$.
   (c) $f(x) = x^2 + 6x + 12$ é irredutível em $\mathbb{Q}[x]$? E em $\mathbb{R}[x]$? E em $\mathbb{C}[x]$?
   (d) Repita o item (c) para $g(x) = x^2 + 8x - 2$.

5. Verificar se cada um dos polinômios abaixo é irredutível em $\mathbb{Q}[x]$:
   (a) $2x^4 - 8x^2 + 1$
   (b) $x^4 + 3x + 5$
   (c) $3x^4 + 2x^3 + 4x^2 + 5x + 1$
   (d) $10x^{11} + 6x^3 + 6$
   (e) $x^3 - 3n^2x + n^3$, onde $n \in \mathbb{Z}$
   (f) $2x^4 + 4x^2 - 2$
   (g) $x^3 - 15x^2 + 10x - 84$
   (h) $x^4 + 4x^3 + 6x^2 + 2x + 1$

6. Mostre que $f(x) = x^4 + x^3 + x + 1$ não é irredutível sobre F para qualquer corpo F.

7. Mostrar que existe número infinito de inteiros a tais que $f(x) = x^7 + 15x^2 - 30x + a$ seja irredutível em $\mathbb{Q}$.

2^a parte: Extensão de corpos

1. (a) Prove que o conjunto dos automorfismos de um corpo E é um grupo com respeito à composição. (Denotado por Aut E).
   (b) Seja $F \subset E$ e defina G_F o subgrupo de todos os automorfismos $\tau : E \to E$ tais que $\tau(a) = a$ para todo $a \in F$. Mostre que G_F é um subgrupo de $\text{Aut}\, E$. (Chamado grupo de Galois de E sobre F).

2. Seja F uma extensão algébrica de $\mathbb{R}$. Mostre que $F = \mathbb{R}$ ou $F = \mathbb{C}$.

3. Calcule $[E : F]$ e encontre uma base de E como F-espaço vetorial, nos seguintes casos. Determine também $u \in E$ tal que $E = F(u)$.
   (a) $E = \mathbb{Q}(\sqrt{2})$, $F = \mathbb{Q}$
   (b) $E = \mathbb{Q}(\sqrt{3}, i)$, $F = \mathbb{Q}$
   (c) $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{18})$, $F = \mathbb{Q}$
   (d) $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$, $F = \mathbb{Q}$
   (e) $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[3]{24})$, $F = \mathbb{Q}$
   (f) $E = \mathbb{Q}(\sqrt{2}, \sqrt{6})$, $F = \mathbb{Q}(\sqrt{3})$
   (g) $E = \mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10})$, $F = \mathbb{Q}(\sqrt{3} + \sqrt{5})$
   (h) $E = \mathbb{Q}(\sqrt[3]{2}, u)$, $F = \mathbb{Q}$, onde $u^2 + 6u + 2 = 0$.

4. Mostre que $\alpha \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$, determinando $irr(\alpha, \mathbb{Q})$, nos seguintes casos:

(a) $\alpha = 1 + \sqrt{2}$ (b) $\alpha = \sqrt{5} + \sqrt{7}$ (c) $\alpha = 1 + i$
(d) $\alpha = \sqrt{1 + \sqrt[3]{3}}$ (e) $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$ (f) $\alpha = \sqrt{\sqrt[3]{2} - i}$
(g) $\alpha = \sqrt{2} + i$

5. Decida se os elementos $\alpha \in \mathbb{C}$ abaixo so algébricos ou transcendentes sobre F. No caso dos algébricos, calcule grau$(irr(\alpha, F))$.
(a) $\alpha = i, \quad F = \mathbb{Q}$ (b) $\alpha = 1 + i, \quad F = \mathbb{R}$
(c) $\alpha = \sqrt{\pi}, \quad F = \mathbb{Q}$ (d) $\alpha = \sqrt{\pi}, \quad F = \mathbb{R}$
(e) $\alpha = \sqrt{\pi}, \quad F = \mathbb{Q}(\pi)$ (f) $\alpha = \pi^2, \quad F = \mathbb{Q}(\pi^3)$

6. Mostre que se $\alpha \in \mathbb{C}$ é transcendente sobre $\mathbb{Q}$ então $\sqrt{\alpha}$ é transcendente sobre $\mathbb{Q}$.

7. (a) Sejam $E \supset F$ uma extensão e $\alpha, \beta \in E$. Suponha que α é transcendente sobre F mas algébrico sobre $F(\beta)$. Mostre que β é algébrico sobre $F(\alpha)$.
(b) Seja $E \supset F$ uma extensão e seja $\alpha \in E$ transcendente sobre F. Mostre que todo elemento $\beta \in F(\alpha)$ é transcendente sobre F.

8. Considere o polinômio $f(x) = x^4 - 2x^2 + 9 \in \mathbb{Q}[x]$.
(a) Mostre que f é irredutível sobre $\mathbb{Q}$.
(b) Verifique que f se fatora sobre $\mathbb{Q}(i)$ da seguinte maneira:

$$f(x) = (x^2 + 2ix - 3)(x^2 - 2ix - 3).$$

(c) Mostre que $i + \sqrt{2} \in \mathbb{Q}(i, \sqrt{2})$ é uma raiz de f. Calcule $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}]$.

9. Seja $\epsilon \in \mathbb{C}$, $\epsilon^3 = 1$. Calcule $[\,\mathbb{Q}(\epsilon) : \mathbb{Q}]$.

10. Sejam $E \supset F$ uma extensão e $\alpha \in E$ algébrico sobre F de grau ímpar. Prove que α^2 é algébrico sobre F de grau ímpar e que $F(\alpha) = F(\alpha^2)$.

11. Seja F um corpo e seja K uma extensão de F. Sejam α, $\beta \in K$ elementos algébricos sobre F com $[F(\alpha) : F] = n$ e $[F(\beta) : F] = m$. Mostre que se $mdc(m, n) = 1$, então $[F(\alpha, \beta) : F] = mn$.

12. Considere o seguinte polinômio $f(x) = x^3 - 6x^2 + 9x + 3 \in \mathbb{Q}[x]$.
(a) Mostre que f é irredutível sobre $\mathbb{Q}$.
(b) Seja $u \in \mathbb{C}$ uma raiz de f. Calcule $[\mathbb{Q}(u) : \mathbb{Q}]$. Expresse cada um dos seguintes elementos de $\mathbb{Q}(u)$ como combinação linear de 1, u e u^2 sobre $\mathbb{Q}$: u^5, $3u^5 - u^4 + 2$, $(u+1)^{-1}$, $(u^2 - 6u + 8)^{-1}$.

13. Em cada um dos itens abaixo, decida se $f \in F[x]$ é irredutível sobre F:
(a) $f(x) = x^2 + 3$, $F = \mathbb{Q}(\sqrt{5})$;
(b) $f(x) = x^3 + 8x - 2$, $F = \mathbb{Q}\sqrt{2}$.

14. Seja F um corpo e seja E uma extensão de F tal que $[E : F] = p$, onde p é um número primo. Mostre que $E = F(\alpha)$, para qualquer $\alpha \in E \setminus F$.

15. Seja E uma extensão de um corpo finito F, $|F| = q$. Seja $\alpha \in E$ algébrico sobre F de grau n. Quantos elementos tem o corpo $F(\alpha)$?

16. Dê exemplo de um corpo com 9 elementos.

17. (a) Mostre que existe $p(x) \in \mathbb{Z}_3[x]$, de grau 3, irredutível sobre $\mathbb{Z}_3$.
(b) Use (a) para provar que existe um corpo F com 27 elementos. Qual a característica de F?

18. Seja F um corpo finito de característica p. Mostre que todo elemento de F algébrico sobre $\mathbb{Z}_p \subset F$.

19. (a) Mostre que se F é um corpo finito então existem $n \in \mathbb{Z},\ n \geq 1$, e p um primo positivo tais que $|F| = p^n$.

(b) Dados $n \in \mathbb{Z}, n \geq 1$ e p um primo positivo, existe um corpo finito F com p^n elementos?

20. (a) Prove que para todo corpo finito F, existe um polinômio de grau 2 com coeficientes em F que é irredutível sobre F.

(b) Mostre que dados um natural n, e um primo natural p existe um corpo com p^{2^n} elementos.

3^a parte: Construções com régua e compasso

1. Prove que o pentágono regular é construtível.

2. Prove que o polígono regular de 9 lados não é construtível.

3. Prove que um polígono regular de n lados é construtível se e somente se o ponto $P = (\cos \frac{2\pi}{n}, \sin \frac{2\pi}{n})$ é construtível.

4. O polígono regular de 15 lados é construtível?

5. Mostre que se os polígonos regulares de m e de n lados são construtíveis e $mdc(m,n) = 1$, então o polígono regular de mn lados é construtível.
Sugestão: Escreva $\frac{2\pi}{mn} = a\frac{2\pi}{m} + b\frac{2\pi}{n}$, com $a, b \in \mathbb{Z}$ e calcule $\cos \frac{2\pi}{mn}$.

6. Prove que é possível trissectar o ângulo de $72°$.