Lista de Álgebra - Teoria dos Anéis

1. Seja R anel, $a \in R, n \in \mathbb{Z}$, definimos:

$$n.a = \begin{cases} \underbrace{a + a + \cdots + a}_{n somandos} & \text{se } n > 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{|n| somandos} & \text{se } n < 0 \\ 0.a = 0 \end{cases}$$

2. Esse exercício mostra que todo anel R pode ser imerso (se necessário) num anel S com identidade, possuindo a mesma característica de R. Seja

$$S = \begin{cases} R \times \mathbb{Z} & \text{se } car(R) = 0 \\ ou & \\ R \times \frac{\mathbb{Z}}{n\mathbb{Z}} & \text{se } car(R) = n. \end{cases}$$

   A adição em S é definida componente a componente e a multiplicação é definida por:

$$(r_1, n_1)(r_2, n_2) = (r_1 r_2 + n_1.r_2 + n_2.r_1, n_1 n_2),$$

   onde $n.r$ tem o significado expresso pelo exercício anterior.

   (a) Mostre que S é um anel.

   (b) Mostre que S possui identidade.

   (c) Mostre que S e R possuem a mesma característica.

   (d) Mostre que a aplicação $\phi : R \to S$ definida por $\phi(r) = (r, 0)$ para $r \in R$ mapeia R isomorficamente sobre um subanel de S, isto é, $\phi(R)$ é um subanel de S isomorfo a R.

3. (a) Determine $car(\frac{\mathbb{Z}}{n\mathbb{Z}})$

   (b) Dê exemplo de um domínio de integridade infinito com característica finita.

4. Todo anel com identidade possui um subanel isomorfo a $\mathbb{Z}$ ou a $\frac{\mathbb{Z}}{n\mathbb{Z}}$ para algum $n > 0$. É possível que um anel com identidade possa simultaneamente conter dois subanéis isomorfos a $\frac{\mathbb{Z}}{n\mathbb{Z}}$ e $\frac{\mathbb{Z}}{m\mathbb{Z}}$ para $n \neq m$? Se isso for possível, dê um exemplo. Caso contrário, prove que isso é impossível.

5. É possível para um domínio de integridade conter dois subanéis isomorfos a $\frac{\mathbb{Z}}{p\mathbb{Z}}$ e $\frac{\mathbb{Z}}{q\mathbb{Z}}$, com p e q ambos primos, $p \neq q$? Dê razões ou apresente uma ilustração.

6. Seja $\varphi : R \to S$ homomorfismo de anéis.

   (a) Mostre que se $I \subset R$ é um ideal de R então $\varphi(I)$ é um ideal de $\varphi(R)$. $\varphi(I)$ é um ideal de S?

   (b) Mostre que se $J \subset S$ é ideal de S então $\varphi^{-1}(J) = \{x \in R \mid \varphi(x) \in J\}$ é ideal de R que contém $Ker(\varphi)$.

   (c) Como se correspondem os ideais de R e S, se φ for um epimorfismo?

7. Sejam I, J ideais de um anel R.

   (a) Mostre que J é ideal de $I + J$.

   (b) Mostre que $I \cap J$ é ideal de I.

   (c) Mostre que $\frac{I+J}{J}$ é isomorfo a $\frac{I}{I \cap J}$.

8. Mostre que $15\mathbb{Z}$ é um ideal de $5\mathbb{Z}$ e que $\frac{5\mathbb{Z}}{15\mathbb{Z}}$ é isomorfo a $\frac{\mathbb{Z}}{3\mathbb{Z}}$.

9. Determine todos os homomorfismos de (anéis) de $\mathbb{Z}$ em $\mathbb{Z}$.

10. Determine todos os homomorfismos de (anéis) de $\mathbb{Q}$ em $\mathbb{Q}$.

11. Determine todos os homomorfismos de (anéis) de $\mathbb{R}$ em $\mathbb{R}$.

12. (a) Mostre que os anéis $2\mathbb{Z}$ e $5\mathbb{Z}$ não são isomorfos. (mas $2\mathbb{Z}$ e $5\mathbb{Z}$ são isomorfos como grupos aditivos!!).

    (b) Mostre que os corpos $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ não são isomorfos. Eles são isomorfos como $\mathbb{Q}-$espaços vetoriais?

13. Seja R anel comutativo com identidade e seja $\mathbb{H}_R = \{a + bi + cj + dk \mid a, b, c, d \in R, i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j\}$ o anel dos quatérnions sobre R. Defina: $\overline{a + bi + cj + dk} = a - bi - cj - dk$, o conjugado de $a + bi + cj + dk$. Mostre que:

    (a) $\overline{\overline{\alpha}} = \alpha$ e que $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$, para todo $\alpha \in \mathbb{H}$.

    (b) $||\alpha\beta|| = ||\alpha||||\beta||$, para todo $\alpha, \beta \in \mathbb{H}$.

14. Considere $C([0,1],\mathbb{R})$ o anel das funções contínuas de $[0,1]$ em $\mathbb{R}$.

    (a) Mostre que M é um ideal maximal de $C([0,1],\mathbb{R})$ se e somente se existe $\alpha \in [0,1]$ tal que $M = M_\alpha = \{f \in C([0,1],\mathbb{R}) \mid f(\alpha) = 0\}$.

    (b) Mostre que $I = \{f \in C([0,1],\mathbb{R}) \mid f(\frac{1}{2}) = f(\frac{1}{3}) = 0\}$ é um ideal de $C([0,1],\mathbb{R})$ que não é primo.

15. Sejam m, n inteiros relativamente primos ($i.e. mdc(m,n) = 1$). Mostre que $\frac{\mathbb{Z}}{mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$.

16. Seja R anel com a propriedade que $a^2 = a$, para todo $a \in R$. Mostre que R é comutativo. O anel R com a propriedade anterior é chamado de anel de Boole. Adicionalmente, mostre que se R é um anel de Boole então a característica de R é dois.

17. Seja R anel com a propriedade que $a^3 = a$, para todo $a \in R$. Mostre que R é comutativo. (De modo mais geral, é possível demonstrar que se R anel tal que para todo elemento $a \in R$, $a^n = a$, para algum $n = n(a)$, então R é comutativo).

18. Seja R anel comutativo com identidade. Mostre que:

    (a) M é ideal maximal de R se e somente se, o quociente R/M é corpo.

    (b) P é ideal primo de R se e somente se, o quociente R/P é domínio de integridade.

19. Seja R anel e M ideal de R. Então R/M é simples, se e somente se, M é ideal maximal.

20. Descreva todas as estruturas de anéis não comutativos não isomorfas que podem ser definidas num conjunto com quatro elementos.

21. Sejam F corpo e R anel. Seja $\varphi : F \to R$ homomorfismo de anéis, não nulo. Mostre que φ é monomorfismo de anéis.

22. Seja R anel e sejam $f, g : \mathbb{Q} \to R$ homomorfismos de anéis tais que $f(n) = g(n)$ para todo $n \in \mathbb{Z}$. Mostre que $f = g$.

    Seja R anel. Um elemento $a \in R$ é dito ser nilpotente, se existir um inteiro positivo n tal que $a^n = 0$. Um elemento $e \in R$ é idempotente,

se $e^2 = e$. Num anel com identidade, os elementos 0 e 1 são chamados de idempotentes triviais.

23. Seja $n = p_1^{n_1} \cdots p_k^{n_k} \in \mathbb{N}^*$. Prove que $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ é nilpotente se e somente se $p_1 \cdots p_k$ divide m.

24. Determine os elementos idempotentes do anel $\mathbb{Z}/n\mathbb{Z}$. Mostre a seguir que o anel $\mathbb{Z}/n\mathbb{Z}$ não possui elementos idempotentes não triviais se e somente se n é um potência de um número primo.

25. Seja R anel, $e \in R$, idempotente de R. Mostre que o conjunto $eRe = \{ere \mid r \in R\}$ é um subanel de R com identidade e.

26. Sejam n, m inteiros positivos $n \geq 2, m \geq 2$. Determine os homomorfismos de anéis $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

27. Existe um anel comutativo R com identidade tal que $R[X] \cong (\mathbb{Z}, +, .)$?

28. Sejam D_1, D_2 anéis de divisão e suponha que para $n, m \in \mathbb{N}^*$ exista um isomorfismo $M_n(D_1) \cong M_m(D_2)$. Mostre que $n = m$ e que $D_1 \cong D_2$.

29. Dê exemplos de anéis R e subanéis S de R satisfazendo:

    (a) R possui identidade 1_R, S não possui identidade 1_S.

    (b) R não possui identidade 1_R, S possui identidade 1_S.

    (c) R possui identidade 1_R, S possui identidade 1_S e $1_R = 1_S$.

    (d) R possui identidade 1_R, S possui identidade 1_S e $1_R \neq 1_S$.

0.1 Anéis de polinômios

30. Seja K corpo, $f(x) \in K[x]$. Mostre que são equivalentes:

    (a) $f(x)$ é irredutível sobre K.

    (b) $< f(x) >$ é ideal maximal de $K[x]$.

    (c) $\frac{K[x]}{<f(x)>}$ é corpo.

31. (a) Seja D domínio. Descreva os inversíveis de $D[x]$.

    (b) Encontre os inversíveis de $\mathbb{Z}[x]$ e de $\mathbb{Z}_7[x]$.

32. Considere $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ e $g(x) = x^2 + 2x - 3$, em $\mathbb{Z}_7[x]$. Encontre $q, r \in \mathbb{Z}_7[x]$ tais que $f = g \cdot q + r$, com $r = 0$ ou $gr(r) < 2$.

33. (a) Decomponha o polinômio $f(x) = x^4 + 4$ 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) O polinômio $f(x) = x^2 + 6x + 12$ é irredutível em $\mathbb{Q}[x]$? E em $\mathbb{R}[x]$? E em $\mathbb{C}[x]$?
    (d) Repita o ítem (c) para $g(x) = x^2 + 8x - 2$.

34. Encontre o mmc e o mdc entre os seguintes polinômios sobre o corpo $\mathbb{Q}$:
    (a) $f(x) = x^3 - 6x^2 + x + 4$ e $g(x) = x^5 - 6x + 1$
    (b) $f(x) = x^2 + 1$ e $g(x) = x^6 + x^3 + x + 1$

35. 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 irredutível em $\mathbb{Z}_{11}[x]$

36. (a) Mostre que $x^2 + 1$ é irredutível em $\mathbb{Z}_{11}[x]$ e prove diretamente que $\frac{\mathbb{Z}_{11}[x]}{<x^2+1>}$ é um corpo com 121 elementos.
    (b) Mostre que $x^2 + x + 4$ é irredutível sobre $\mathbb{Z}_{11}$ e prove diretamente que $\frac{\mathbb{Z}_{11}[x]}{<x^2+x+4>}$ é um corpo com 121 elementos.
    (c) Os corpos $\frac{\mathbb{Z}_{11}[x]}{<x^2+1>}$ e $\frac{\mathbb{Z}_{11}[x]}{<x^2+x+4>}$ são isomorfos? Justifique.

37. Mostre que $\frac{\mathbb{R}[x]}{<x^2+1>} \cong \mathbb{C}$.

38. Sejam K corpo e $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x], f \neq 0$. A derivada $f'(x)$ de $f(x)$ é o polinômio

$$f'(x) = a_1 + \cdots + (i \cdot 1)a_ix^{i-1} + \cdots + (n \cdot 1)a_nx^{n-1},$$

onde $i \cdot 1$ possui o seu sentido usual para $i \in \mathbb{Z}^+$ e $1 \in K$.

Mostre que f é divisível pelo quadrado de um polinômio não constante se e somente se $mdc(f, f') = 1$.

39. Se $f \in \mathbb{Z}_p[x]$ é irredutível sobre $\mathbb{Z}_p$, (p primo), de grau n. Mostre que $\frac{\mathbb{Z}_p[x]}{<f>}$ é um corpo com p^n elementos.

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

41. Verifique-se cada um dos polinômios $f \in \mathbb{Z}[x]$ abaixo é irredutível sobre $\mathbb{Q}$ e, se for o caso, decomponha-o como produto de irredutíveis em $\mathbb{Q}[x]$.

    (a) $f(x) = x^5 + 2x^3 + 2x^2 + 2x + 2$

    (b) $f(x) = x^3 + 6x^2 + 5x + 25$

    (c) $f(x) = x^4 + 8x^3 + x^2 + 2x + 5$

    (d) $f(x) = x^8 + 10x^3 + 20x^2 + 30x + 22$

    (e) $f(x) = x^3 - 2x^2 + x + 15$

    (f) $f(x) = x^4 - 2$

    (g) $f(x) = x^4 - x + 1$

42. Considere o polinômio $f = x^4 + 15x^3 + 7 \in \mathbb{Z}[x]$. Use redução módulo 5 para concluir que f é irredutível sobre $\mathbb{Q}$. Mostre que f, considerado como um elemento de $\mathbb{Z}_3[x]$, é redutível.

0.2 Anéis Euclidianos, Principais e Fatoriais

43. Determine o grupo de unidades de $\mathbb{Z}_6, \mathbb{Z}_7, \mathbb{Z}_8$.

44. Determine todos os homomorfismos de $\mathbb{Q}(\sqrt{2})$ em $\mathbb{Q}(\sqrt{2})$.

45. Mostre que $\varphi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$ definida por $\varphi(f(x)) = f(\sqrt{2})$ é um homomorfismo de anéis. Determine $Ker(\varphi)$. $Ker(\varphi)$ é um ideal maximal de $\mathbb{Q}[x]$?

46. Seja R domínio de integridade de característica $p > 0$.

    (a) Seja p primo positivo. Mostre que $p \mid \binom{p}{i}$, para todo i, $1 \leq i < p$; onde $\binom{p}{i} = \frac{p!}{i!(p-i)!}$.

    (b) Mostre que $(x + y)^p = x^p + y^p$, para todo $x, y \in R$.

(c) Mostre que a aplicação $\phi : R \to R$, definida por $\phi(a) = a^p$, é um homomorfismo de anéis (denominado homomorfismo de Frobenius).

(d) Mostre que se R for um domínio de integridade finito de característica $p > 0$ então o homomorfismo de Frobenius é um automorfismo de R.

(e) Dado $p \in \mathbb{Z}$, primo, provar que o único automorfismo de $\mathbb{Z}_p$ em $\mathbb{Z}_p$ é o automorfismo idêntico. Deduza daí que $a^p \equiv a \pmod{p}$, para todo $a \in \mathbb{Z}$.

(f) Provar que se p não divide a então $a^{p-1} \equiv 1 \pmod{p}$. Este último resultado é conhecido como Pequeno Teorema de Fermat.

47. Seja K corpo de característica $p > 0$ e $n \in \mathbb{N} \setminus \{0\}$. Mostre que $L = \{x \in K \mid x^{p^n} = x\}$ é um subcorpo de K.

48. (a) Determine os inversíveis de $\mathbb{Z}[i]$.

(b) Mostre que se $\alpha = a + bi \in \mathbb{Z}[i]$ não é inversível, então $a^2 + b^2 > 1$.

49. Determine o máximo divisor comum em $\mathbb{Z}[i]$, entre os seguintes elementos:

(a) $\alpha = 3 + 4i$ e $\beta = 4 - 3i$.

(b) $\alpha = 11 + 7i$ e $\beta = 18 - i$.

50. (a) Mostre que as únicas unidades de $\mathbb{Z}[\sqrt{-5}]$ são ± 1.

(b) Mostre que $(1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = 3 \cdot 7$.

(c) Mostre que $(1 - 2\sqrt{-5})$ e 3 são irredutíveis em $\mathbb{Z}[\sqrt{-5}]$.

(d) Mostre que 3 não é primo em $\mathbb{Z}[\sqrt{-5}]$.

51. Mostre que $(\mathbb{Z}[\sqrt{-2}], +, ., \varphi)$ é um domínio euclidiano, onde φ é dada por $\varphi(a + b\sqrt{-2}) = a^2 + 2b^2$.

52. Dados $\alpha = 1 + 2i, \beta = 3 + 4i$, $\alpha, \beta \in \mathbb{Z}[i]$. Achar $q, r \in \mathbb{Z}[i]$ tais que $\alpha = \beta q + r$, onde $r = 0$ ou $\varphi(r) < \varphi(\beta)$. Tais q, r são únicos?

53. Considere $\mathbb{Z}[x]$ o anel de polinômios com coeficientes inteiros.

(a) $\mathbb{Z}[x]$ é um domínio de fatorização única?

(b) Mostre que $I = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$ é um ideal de $\mathbb{Z}[x]$. O ideal I é maximal?

(c) $\mathbb{Z}[x]$ é um domínio principal?

(d) $\mathbb{Z}[x]$ é um domínio euclidiano?

54. Verifique se cada uma das afirmações abaixo é verdadeira ou falsa, provando-a ou exibindo um contra-exemplo:

(a) Todo domínio euclidiano é principal.

(b) Todo domínio principal é euclidiano.

(c) Todo domínio de fatorização única é euclidiano.

55. Verifique se os elementos α abaixo são irredutíveis nos domínios D indicados. Nos casos em que couber, decomponha α como produto de irredutíveis:

(a) $\alpha = 14$ em $D = \mathbb{Z}$.

(b) $\alpha = 2x - 10$ em $D = \mathbb{Z}[x]$.

(c) $\alpha = 2x - 10$ em $D = \mathbb{Z}_{11}[x]$.

(d) $\alpha = 5$ em $D = \mathbb{Z}[i]$.

(e) $\alpha = 7$ em $D = \mathbb{Z}[i]$.

(f) $\alpha = 4 + 3i$ em $D = \mathbb{Z}[i]$.

56. Mostre que $\frac{\mathbb{Z}[i]}{3\cdot\mathbb{Z}[i]}$ é um corpo, mas $\frac{\mathbb{Z}[i]}{2\cdot\mathbb{Z}[i]}$ não é corpo.

57. Mostre que $\mathbb{Q}[x, y]$ não é um anel principal.

0.3 Extensões finitas e algébricas

58. 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) $E = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}), F = \mathbb{Q}$;

(f) $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{6}, \sqrt[3]{24}), F = \mathbb{Q}$;

(g) $E = \mathbb{Q}(\sqrt{2}, \sqrt{6}), F = \mathbb{Q}(\sqrt{3})$;

(h) $E = \mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10}), F = \mathbb{Q}(\sqrt{3} + \sqrt{5})$;

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

60. Prove que $f(x) = x^2 - 3$ é irredutível sobre $\mathbb{Q}(\sqrt[3]{2})$.

61. Prove que $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3} + \sqrt{7})$.

62. Generalize o resultado do exercício anterior.

63. Seja $L = K(u)$, onde $u \in L$ é algébrico sobre K e $[L : K]$ é ímpar. Mostre que $L = K(u^2)$.

64. Mostre que se L/K é uma extensão finita de corpos tal que $[L : K]$ seja um número primo, então $L = K(\alpha)$, para qualquer $\alpha \in L \setminus K$.

65. (Um exemplo de extensão algébrica que não é finita) Seja $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \cdots, \sqrt{p}, \cdots)$ o subcorpo de $\mathbb{R}$ gerado por $\mathbb{Q}$ e pelas raízes quadradas de todos os números primos positivos.

    (a) Mostre que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \cdots$ é uma cadeia ascendente própria de subcorpos de $\mathbb{R}$ e, portanto, $E/\mathbb{Q}$ não é extensão finita. (Sugestão: Mostre que se $p_1, \cdots, p_n, p_{n+1}$ são os primeiros $n+1$ primos então $\sqrt{p_{n+1}} \notin \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$, usando indução em n.)

    (b) Mostre que $E/\mathbb{Q}$ é uma extensão algébrica.

66. Para cada $n \geq 1$, seja $L_n = \mathbb{Q}(\sqrt[n]{2})$.

    (a) Mostre que $[L_n : \mathbb{Q}] = n$;

    (b) Se $m \geq 1$ divide n, mostre que $L_m \subseteq L_n$ e, determine $[L_m : L_n]$.

    (c) Se $mdc(m, n) = 1$, mostre que $L_{mn} = \mathbb{Q}(\sqrt[m]{2}, \sqrt[n]{2})$.

67. Seja L/K uma extensão de corpos e sejam $u, v \in L$ elementos algébricos sobre K tais que $[K(u) : K] = n$ e $[K(v) : K] = m$.

(a) Mostre que se $mdc(n, m) = 1$ então $Irr(v, K)$ é irredutível sobre $K(u)$.

(b) Mostre que se $mdc(n, m) = 1$ então $[K(u, v) : K] = nm$.

(c) Calcule $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) : \mathbb{Q}]$.

0.4 Corpos Finitos

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

69. Dê exemplo de um corpo com 9 elementos.

70. (a) Mostre que existe $p(x) \in \mathbb{Z}_3[x]$, de grau 3, irredutivel sobre $\mathbb{Z}_3$.

    (b) Use o ítem (a) para provar que existe um corpo F com 27 elementos. Qual a característica de F?

71. Seja F corpo finito de característica $p > 0$. Mostre que todo elemento de F é algébrico sobre $\mathbb{Z}_p \subseteq F$.

72. Prove que toda extensão finita de um corpo finito é simples.

73. (a) Mostre que 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?