MA 553 A, Segundo Semestre 2019, Lista 1

Todos anéis aqui são comutativos e com 1.

Ex. 1. Os números inteiros $\mathbb{Z}$ com a soma e o produto usual formam um anel. Este anel tem divisores de zero?

Ex. 2. Seja $I = (m) = m\mathbb{Z}$ o conjunto de todos múltiplos de $m \in \mathbb{Z}$, mostrar que $\lhd\mathbb{Z}$. Mostrar que se $J \lhd \mathbb{Z}$ então $J = (m)$ para algum $m \in BZ$.

Ex. 3. Denotamos $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ os restos na divisão por m em $\mathbb{Z}$, mostrar que $\mathbb{Z}_m$ é um anel com as operações módulo m. Quais são os números m tais que $\mathbb{Z}_m$ não tem divisores de zero? Quais são os divisores de 0 em $\mathbb{Z}_{12}$ e em $\mathbb{Z}_{100}$? E em $\mathbb{Z}_{101}$?

Ex. 4. Seja $d \in \mathbb{Z}$ um inteiro que é produto de primos distintos em $\mathbb{Z}$, consideramos o conjunto $\mathbb{Z}[\sqrt{d} = \{a+b\sqrt{d} \mid a, b \in \mathbb{Z}\}$, mostrar que ele é um subanel de $\mathbb{C}$. Mostrar que $\mathbb{Q}(\sqrt{d} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ é um subcorpo dos complexos.

Ex. 5. Mostrar que se A é um anel finito com 1 e sem divisores de 0, então A é corpo. (Obs.: Aqui nem precisa A comutativo.)

Ex. 6. Quais dos seguintes são subanéis de $\mathbb{Q}$:

a) Os números racionais com denominador ímpar (escritos como frações irredutíveis);

b) Os números racionais com denominador par (escritos como frações irredutíveis);

c) Os racionais não negativos;

d) Os racionais que são quadrados de números racionais;

e) Os racionais com numeradores pares (escritos como frações irredutíveis);

f) Os racionais com numeradores ímpares (escritos como frações irredutíveis).

Ex. 7. Mostrar que num domínio A, se $a \in A$ e $a^2 = 1$ então $a = \pm 1$.

Ex. 8. Um elemento $a \in A$ do anel A é *nilpotente* se $a^m = 0$ para algum $m \in \mathbb{N}$. Mostrar que se $n = a^k b$, a, k, $b \in \mathbb{N}$, então $ab \in \mathbb{Z}_n$ é nilpotente. Quais são todos os elementos nilpotentes em $\mathbb{Z}_n$?

Ex. 9. Sejam A um anel e $I \lhd A$, mostrar que $I = A$ se e somente se I contém elementos invertíveis de A. Deduzir que A é corpo se e somente se os dois únicos ideais de A são A e 0.

Ex. 10. Seja A um domínio e sejam a, $b \in A$. Mostrar que $(a) = (b)$ se e somente se $a \sum b$ (isto é, $a = ub$ onde u é invertível em A.)

Ex. 11. Se $a \in A$ é nilpotente, mostrar que $1 - ax$ é invertível para todo $x \in A$.

Ex. 12. Se A é corpo, o corpo de frações de A coincide com A. Demonstrar!

Ex. 13. Seja $A = \mathbb{Q}[x]$ o anel dos polinômios na variável x, com coeficientes racionais, mostrar que ele é:

a) domínio;

b) anel euclidiano;

c) o seu corpo de frações é $\mathbb{Q}(x)$, as funções racionais.

Ex. 14. Seja $A = \mathbb{Z}[x]$ o anel dos polinômios com coeficientes inteiros na variável x. Este anel é um domínio? Mostrar que o ideal gerado pelos polinômios 2 e x não é principal. Este anel pode ser euclidiano?

Ex. 15. O mesmo como no exercício anterior para o anel $A = K[x, y]$, o anel dos polinômios com coeficientes no corpo K e variáveis x e y, e o ideal gerado por x e y.

Ex. 16. Se A é anel, e a, $b \in A$ são não nulos, denotamos por d um MDC de a e b. Se A é euclidiano e d e d_1 são dois MDC para a e b, mostrar que a e b são associados. Esta afirmação vale para anéis principais? E para anéis fatoriais?

Ex. 17. Encontrar o MDC d dos elementos a e b do respectivo anel A, e escrever $d = xa + yb$, x, $y \in A$ (este último para os exemplos (a), (b) (f), (g)):

a) $a = 2210$, $b = 1131$, $A = \mathbb{Z}$.

b) $a = 11391$, $b = 5673$, $A = \mathbb{Z}$.

c) $a = 91442056588823$, $b = 779086434385541$, $A = \mathbb{Z}$.

d) $a = 85$, $b = 1 + 13i$, $A = \mathbb{Z}[i]$.

e) $a = 47 - 13i$, $b = 53 + 56i$, $A = \mathbb{Z}[i]$.

f) $a = x^5 - 2x^3 + x^2 - 3x + 1$, $b = x^3 - 3x + 1$, $A = \mathbb{Q}[x]$.

g) $a = x^4 - 2x^3 + 2x - 4$, $b = x^3 - 2x^2 + 4x - 8$, $A = \mathbb{Q}[x]$.

Ex. 18. Se a, $b \in A$ são ambos $\neq 0$, um MMC de a e b é um elemento m de A tal que a e b dividem m e se $t \in A$, a e b dividem t, então m divide t. Notação: $m = [a, b]$.

a) Mostrar que se $m = [a, b]$ existe então m gera o maior ideal principal contido em $(a) \cap (b)$ em A.

b) Se A é euclidiano, então $[a, b]$ existe para quaisquer a e b, e os MMC's de a e b são associados.

c) Mostrar que se A é euclidiano e $a, b \in A$ são não nulos, então $(a, b)[a, b] \sim ab$.

Ex. 19. Mostrar que num domínio principal o enunciado do exercício 16 continua valendo, bem como o do exercício 18.

Ex. 20. Seja A domínio de fatoração única e sejam $a, b, c \in A$. Mostrar que:

a) Se $c|a$ e $c|b$ então $cMDC(a/c, b/c) = MDC(a, b)$.

b) Se m e n são números naturais e $(a, b) = 1$ então $(a^m, b^n) = 1$.

c) Se a^n divide b^n então a divide b.

Ex. 21. Mostrar que num domínio, todo elemento primo é irredutível.

Ex. 22. Mostrar que se A é euclidiano então todo irredutível é primo. O mesmo vale para anéis principais? E para fatoriais?

Ex. 23. Seja A um anel euclidiano, mostrar que o grupo $A^\times$ dos elementos invertíveis de A coincide com o conjunto $\{a \in A \mid d(a) = d(1)\}$.

(Observação: Em $\mathbb{Z}$ com o d usual, temos $d(1) = |1| = 1$. Se $A = K[x]$, o anel dos polinômios na variável x com coeficientes no corpo K, temos $d(1) = \deg(1) = 0$).

Ex. 24. a) Quais são os elementos invertíveis em $\mathbb{Z}[i]$?

b) Quais dos seguintes elementos são irredutíveis em $\mathbb{Z}[i]$: 2, 3, 5, 7, 11, 13, 17, 19, $1 - 2i$, $2 + 3i$, $3 - 4i$?

Ex. 25. Seja $\omega \in \mathbb{C}$, $\omega \neq 1$ e $\omega^3 = 1$.

a) Mostrar que $A = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ é um anel. (Dica: Usar que $\omega^2 + \omega + 1 = 0$.)

b) Se $\overline{\alpha}$ denota o conjugado de α, defina $N(\alpha) = \alpha\overline{\alpha}$. Mostrar que se $\alpha, \beta \in A$ então $N(\alpha)N(\beta) = N(\alpha\beta)$. Deduzir daqui que se $N(\alpha)$ é primo em $\mathbb{Z}$ então α é irredutível em A.

c) Mostrar que $1 - \omega$ é primo em A.

d) Mostrar que A é euclidiano.

Ex. 26. Seja A um anel euclidiano com a respectiva função d. Suponha $a \in A$, $a \neq 0$.

a) Mostrar que se $d(a) = 0$ então a é invertível em A.

b) Se $0 \neq b \in A$ e $d(ab) = d(b)$, então a é invertível.

c) Se $d(a) = 1$, mostrar que a é ou invertível ou irredutível em A.

Ex. 27. a) Mostrar que $A = \mathbb{Z}[\sqrt{-2}]$ é um anel euclidiano.

b) Mostrar que $A = \mathbb{Z}[\sqrt{2}]$ é euclidiano.

(Dica: a) Se $a = m + n\sqrt{-2} \in A$, defina $d(a) = m^2 + 2n^2$, e denota por $b^{-1} = u + v\sqrt{-2}$ a inversa de $b \neq 0$, $b \in A$, em $\mathbb{Q}[\sqrt{-2}]$. Escrevendo $ab^{-1} = u + v\sqrt{-2}$, $u, v \in \mathbb{Q}$, escolha inteiros M e N mais próximos a u e a v, respectivamente. Verifique que $M + N\sqrt{-2}\ a = (M + N\sqrt{-2}b + c$ onde $d(c) < d(a)$ ou $c = 0$. b) Defina $d(a) = |m^2 - 2n^2|$ e prossiga como em item (a).)

Ex. 28. Sejam $a, b, c \in A$, A domínio de fatoração única. Suponha $(a, b) = 1$ e a divide c, bem como b divide c. Mostrar que ab divide c.

Ex. 29. Mostrar que $A = \mathbb{Z}[\sqrt{5}]$ não é domínio de fatoração única.

(Dica: $x = a + b\sqrt{5} \in A$, defina a norma $N(x) = a^2 - 5b^2$ e mostre que $N(x)N(y) = N(xy)$ para quaisquer x, $y \in A$. Para $a = 3$, $b = 1$, temos $(3 + \sqrt{5})(3 - \sqrt{5}) = 2 \cdot 2 = 4$. Mas $3 \pm \sqrt{5}$ e 2 têm norma 4. Mostraremos que se $\alpha \in A$ tem norma 4 ele é irredutível. Por absurdo, se $\alpha = \beta\gamma$ em A, teremos $N(\beta) = \pm 1, \pm 2, \pm 4$. Se $N(\beta) = \pm 1$ então β é invertível em A. Se $N(\beta) = \pm 4$ então γ será invertível. Se $N(\beta) = \pm 2$, teremos, para $\beta = u + v\sqrt{5}$, que $u^2 - 5v^2 = 2$. Dividindo por 5, a^2 terá resto ± 2, o que é impossível. Assim temos duas decomposições de 4, logo A não é domínio fatorial.)

Ex. 30. Seja $A = \mathbb{Z}[i]$ o anel dos inteiros de Gauss.

a) Calcular as normas de $2 \pm i$ e de $1 \pm 2i$.

b) Mostrar que $5 \in A$ não é primo.

c) Por que a igualdade $5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$ em A não contradiz a fatoração única em A?

* * *

Ex. 31. a) Escrever os números 241, 649, 520 (dados no sistema decimal) nos sistemas binário, octal e hexadecimal.

b) Escrever os números 101100101 e 111001 do sistema binário para o sistema octal. Escrever os mesmos números no sistema hexadecimal.

c) Escrever o número ABC do sistema hexadecimal para o sistema decimal.

Ex. 32. Mostrar que o produto de três inteiros consecutivos é divisível por 6. É verdade que o produto de 4 inteiros consecutivos é divisível por 24?

Ex. 33. a) Quais são os possíveis restos na divisão de um quadrado perfeito por 4?

b) Se $n \in \mathbb{Z}$ mostrar que 4 não divide $n^2 + 2$.

c) Calcular o resto na divisão por 4 de um números escrito no sistema decimal com n algarismos todos iguais a 1: $111\ldots11$ (n vezes).

d) Mostrar que os números de (c) não são quadrados perfeitos se $n > 1$.

Ex. 34. a) Determinar quais são os restos dos cubos de inteiros na divisão por 9.

b) Se 9 divide a soma $a^3 + b^3 + c^3$, a, b, $c \in \mathbb{Z}$, mostrar que 3 divide pelo menos um entre a, b, c.

c) Mostrar que existe uma infinidade de números inteiros que não são soma de três cubos de inteiros.

Ex. 35. a) Encontrar um par de números naturais a e b tais que $(a, b) = 10$, $[a, b] = 100$.

b) Encontrar todos os números naturais a e b com essa propriedade.

Ex. 36. a) Se $m > n$ e $a > 2$, mostrar que $a^{2^n} + 1$ divide $a^{2^m} - 1$.

b) Mostrar que $(a^{2^n} + 1, a^{2^m} + 1) = 1$ se a é par, e é igual a 2 se a é ímpar.

Ex. 37. a) Seja $F_n = 2^{2^n} + 1$, $n \geq 0$. Mostrar que se $m \neq n$ então $(F_m, F_n) = 1$.

b) Deduzir de (a) que existem infinitos números primos.

Ex. 38. a) Mostrar que existem infinitos primos da forma $4k + 3$, $k \in \mathbb{N}$.

b) Mostrar que existem infinitos primos da forma $6k + 5$, $k \in \mathbb{N}$.

Ex. 39. Seja a um inteiro ímpar, mostrar que o número 4 divide $a^2 - 1$. O número 8 divide $a^2 - 1$?

Ex. 40. Seja $n > 1$, mostrar que os números $n! + 2$, $n! + 3$, $\ldots$, $n! + n$ são todos compostos.

Ex. 41. Sejam $f_0 = 0$, $f_1 = 1$ e $f_{n+1} = f_n + f_{n-1}$, $n \geq 1$, os números de Fibonacci.

a) Mostrar que $(f_n, f_{n+1}) = 1$ para todo n.

b) Mostrar que $(f_n, f_k) = f_d$ onde $d = (n, k)$. (Dica: Primeiro mostrar que se k divide n então f_k divide f_n. Depois mostrar que se $n = kq + r$, $0 \leq r \leq k - 1$, tem-se $(f_n, f_k) = (f_k, f_r)$.)

Ex. 42. O famoso cometa de Halley passa perto da Terra (de modo que seja visível a olho nú), aproximadamente a cada 75 anos. A última vez que ele passoiu perto da Terra foi em 1986. Em que ano(s) entre 3000 e 3100 ele passará perto da Terra?

Ex. 43. a) Mostrar que se $n > 1$ então $n - 1$ divide $n^2 - 1$.

b) Encontrar todos $n \in \mathbb{N}$ tais que $n - 1$ divide $n^2 * 1$.

Ex. 44. Mostrar que para todo $n \in \mathbb{Z}$ tem-se $(2n + 1, 9n + 4) = 1$.

Ex. 45. Mostrar que se $n > 6$ então n pode ser apresentado como soma de dois números naturais a e b tais que $(a, b) = 1$. (Dica: Considere separadamente os casos n par e n ímpar.)