Departamento de Matemática — Universidade do Minho

Álgebra — 2º teste – 14 jan 2021

Lic. em Ciências de Computação/Lic. em Matemática - 2º ano — duração: duas horas

Nome ______________________________

Curso ____________________ Número ____________

Responda no próprio enunciado, seguindo rigorosamente as instruções dadas em cada um dos grupos

GRUPO I

Em cada uma das questões seguintes, diga se é verdadeira (V) ou falsa (F) a proposição, assinalando a opção conveniente. Cada questão está cotada com 0,8 valores numa escala de 0 a 20.

1. Seja A um anel comutativo com identidade de caraterística 12. Então, A não é um domínio de integridade. V☒ F☐

   Se A tem identidade 1_A e caraterística 12, então, $o(1_A) = 12$. Logo, o elemento $3 \cdot 1_A$ é divisor de zero não nulo de A (ver exercício 1(a) do grupo III). Logo, A não é domínio de integridade.

2. Se I e J são ideais de um anel A tais que $I \cap J = \{0_A\}$, então, para todos $i \in I$ e $j \in J$, $ij = 0_A$. V☒ F☐

   Sabemos que, sendo I e J ideais de A, $IJ \subseteq I \cap J$. O resultado segue de $ij \in IJ$, para todos $i \in I$ e $j \in J$.

3. A soma de dois subanéis de um anel A nunca é um subanel de A. V☐ F☒

   No anel dos inteiros, se considerarmos os subanéis $2\mathbb{Z}$ e $4\mathbb{Z}$, temos que $2\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z}$, que é um subanel de A.

4. Sejam A um anel com identidade e I e J ideais maximais de A. Se $I \neq J$ então $IJ = I \cap J$. V☒ F☐

   Como $I, J \subseteq I + J \subseteq A$ e $I \neq J$, uma vez que I e J são maximais, podemos concluir que $A = I + J$. Como $1_A \in A$ estamos em condições de concluir que $IJ = I \cap J$ (resolução do exercício 65).

5. Sejam A e A' anéis comutativos com identidade e $\varphi : A \to A'$ um morfismo de anéis. Então $\varphi(1_A) = 1_{A'}$. V☐ F☒

   Por exemplo, considerando $A = \mathbb{Z}$, $A' = \mathcal{M}_2(\mathbb{R}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}\}$ e $\varphi : A \to A'$ a aplicação definida por $\varphi(x) = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$, temos que φ é um morfismo de anéis tal que $\varphi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq I_2$.

GRUPO II

Em cada uma das questões seguintes, apresente a sua resposta sem qualquer justificação. Cada questão está cotada com 1,0 valores numa escala de 0 a 20.

1. Indique a ordem da permutação $\alpha = (1\,2\,3)(2\,4\,5\,7)$ de $\mathcal{S}_7$:

   $\alpha = (1\,2\,4\,5\,7\,3)$, pelo que α é um ciclo de comprimento 6, pelo que $o(\alpha) = 6$.

2. Indique os elementos de $< \beta^3 >$, sabendo que $\beta = (1\,2\,3)(4\,5) \in \mathcal{S}_6$:

   A permutação β está escrita como produto de ciclos disjuntos de comprimentos 3 e 2, pelo que $o(\beta) = \text{m.m.c.}(3,2) = 6$. Assim, $o(\beta^3) = 2$. Logo, $< \beta^3 >= \{\text{id}, \beta^3\} = \{\text{id}, (4\,5)\}$, uma vez que $\beta^3 = (1\,2\,3)^3(4\,5)^3 = \text{id}(4\,5) = (4\,5)$.

3. Indique a paridade da permutação $\gamma \in \mathcal{S}_9$, sabendo que $\gamma^5 = (1\,2\,3)(4\,5\,7\,9)$:

   As permutações γ^5 e γ têm a mesma paridade, uma vez que γ^4 é uma permutação par. Como γ^5 é uma permutação ímpar (é produto de uma permutação par por uma ímpar), concluímos que γ é ímpar.

4. Indique duas permutações de $\mathcal{S}_9$, com a mesma ordem mas de paridades diferentes:

   Por exemplo, $\pi_1 = (1\,2\,3\,4)$ e $\pi_2 = (1\,2\,3\,4)(5\,6)$. Ambas as permutações têm ordem 4, π_1 é uma permutação ímpar e π_2 é uma permutação par.

GRUPO III

Em cada uma das questões seguintes, apresente a sua resposta devidamente justificada. Cada questão está cotada com 4,0 valores numa escala de 0 a 20.

1. Seja A um anel não nulo. Mostre que:

   (a) se $a \in A$ é um elemento de ordem 12, então A tem um divisor de zero.

   Se $a \in A$ é tal que $o(a) = 12$, então, $12a = 0_A$ e $ka \neq 0_A$, para todo $k \in \{1, 2, .., 11\}$. Assim, $4a \neq 0_A$ é tal que

   $$(3a)(4a) = 12a^2 = (12a)a = 0_A a = 0_A.$$

   Logo, $3a$ é divisor de zero de A.

   (b) se, para todos $a \in A \backslash \{0_A\}$ e $b, c \in A$,

   $$ab = ca \Rightarrow b = c,$$

   então A é um anel comutativo.

   Sejam $a, b \in A$. Se $a = 0_A$, temos que $ab = 0_A = ba$. Se $a \neq 0_A$, uma vez que $a(ba) = (ab)a$, aplicando a hipótese, temos que $ba = ab$. Logo, A é comutativo.

2. Sejam A um anel comutativo com identidade, $a, b \in A$ e $I = \{ax + by : x, y \in A\}$.

   (a) Mostre que I é um ideal de A.

   Começamos por observar que $0_A \in A$ e $0_A = a0_A + b0_A$, pelo que $0_A \in I$ e, portanto, $I \neq \emptyset$. Mais ainda, para $i_1, i_2 \in I$, temos que $i_1 = ax_1 + by_1$ e $i_2 = ax_2 + by_2$, com $x_1, y_1, x_2, y_2 \in A$. Então,

   $$i_1 - i_2 = (ax_1 + by_1) - (ax_2 + by_2) = a(x_1 - x_2) + b(y_1 - y_2).$$

   Como $x_1 - x_2, y_1 - y_2 \in A$, temos que $i_1 - i_2 \in I$. Finalmente, se $i \in I$ e $z \in A$, temos que $i = ax + by$, com $x, y \in A$ e, por isso,

   $$zi = iz = (ax + by)z = (ax)z + (by)z = a(xz) + b(yz).$$

Como $xz, yz \in A$, concluimos que $zi = iz \in I$. Estamos em condições de concluir que I é ideal de A.

(b) Para $A = \mathbb{Z}$, dê exemplo, justificando, de elementos a e b para os quais:

i. $I = A$;

Sabemos que $I = A = \mathbb{Z}$ se e só se $1 \in I$. Assim, temos que $I = \mathbb{Z}$ se e só se existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$. Logo, a e b têm de ser tais que $\mathrm{m.d.c.}(a, b) = 1$. Podemos considerar, por exemplo, $a = 2$ e $b = 3$.

ii. I é um ideal maximal de A.

Sabemos que I é ideal maximal de $\mathbb{Z}$ se e só se $I = p\mathbb{Z}$, com p primo. Mas, $I = p\mathbb{Z}$ se e só se existem $x, y \in \mathbb{Z}$ tais que $p = ax + by$ e p é o menor inteiro nestas condições, ou seja, $p = \mathrm{m.d.c.}(a, b)$. Podemos considerar, por exemplo, $a = 10$ e $b = 15$. Neste caso, $I = 5\mathbb{Z}$.

3. Sejam $n \in \mathbb{N}$ e $f_n : \mathbb{Z}_n \to \mathbb{Z}_n$ a aplicação definida por $f_n([x]_n) = ([x]_n)^n$, para todo $[x]_n \in \mathbb{Z}_n$.

(a) Justifique que f_4 não é um endomorfismo de anéis.

Como

$$\begin{aligned} f_4([1]_4 + [1]_4) &= f_4([2]_4) = ([2]_4)^4 \\ &= [16]_4 = [0]_4 \\ &\neq [2]_4 = [1]_4 + [1]_4 \\ &= ([1]_4)^4 + ([1]_4)^4 = f_4([1]_4) + f_4([1]_4), \end{aligned}$$

podemos concluir que f_4 não é compatível com a adição de classes de $\mathbb{Z}_4$, pelo que não é um homomorfismo de anéis. Logo, f_4 não é endomorfismo de anéis.

(b) Mostre que f_3 é um endomorfismo de anéis e determine o seu núcleo.

Sejam $[x]_4, [y]_4 \in \mathbb{Z}_3$. Então, como $\mathbb{Z}_3$ é um anel comutativo e de caraterística 3,

$$\begin{aligned} f([x]_3 + [y]_3) &= f_3([x + y]_3) = ([x + y]_3)^3 \\ &= [(x + y)^3]_3 = [x^3 + 3x^2y + 3xy^2 + y^3]_3 \\ &= [x^3 + y^3]_3 = ([x]_3)^3 + ([y]_3)^3 \\ &= f_3([x]_3) + f_3([y]_3) \end{aligned}$$

e

$$\begin{aligned} f([x]_3[y]_3) &= f_3([xy]_3) = ([xy]_3)^3 \\ &= [(xy)^3]_3 = [x^3y^3]_3 \\ &= ([x]_3)^3([y]_3)^3 \\ &= f_3([x]_3) + f_3([y]_3). \end{aligned}$$

Estamos em condições de concluir que f_3 é um morfismo de anéis.

Mais ainda, como $f_3([0]_3) = [0]_3$, $f_3([1]_3) = [1]_3$ e $f_3([2]_3) = [8]_3 = [2]_3$, concluímos que $\mathrm{Nuc} f_3 = \{[0]_3\}$.

(c) Para que valores de n f_n é um endomorfismo de anéis?

Uma vez que, independentemente de $n \in \mathbb{N}$, $(xy)^n = x^n y^n$, para todos $x, y \in \mathbb{Z}$, f_n é morfismo de anéis se e só se f_n for compatível com a adição de classes em $\mathbb{Z}_n$ e isso só é possível se no desenvolvimento da expressão $(x + y)^n$, os coeficientes de todos os termos, com a exceção de x^n e y^n, forem divisível por n. Para isso acontecer, n tem de ser um número primo (recordar que esses coeficientes são ${}^nC_k$, com $1 \leq k \leq n - 1$). Assim, f_n é um endomorfismo se e só se n é um número primo.

GRUPO IV

Esta questão é facultativa. Caso opte por responder, apresente a sua resposta devidamente justificada. A questão está cotada com 2,0 valores extra escala.

1. Considere o subconjunto $X = \{2+\sqrt{-5}, 3+\sqrt{-5}\}$ do domínio de integridade $D = \mathbb{Z}[\sqrt{-5}]$. Mostre que

$$\exists^1 x \in X : (x) \text{ é maximal na classe dos ideais principais de } D.$$

Sabemos que (x) é maximal na classe dos ideais principais de D se e só se (x) é irredutível em D. Vejamos que $7+\sqrt{-5}$ é redutível e que $3+\sqrt{-5}$ é irredutível em D:

- $7+\sqrt{-5}$ é redutível pois $7+\sqrt{-5} = (2-\sqrt{-5})(1+\sqrt{-5})$ e $2-\sqrt{-5}, 1+\sqrt{-5} \notin \mathcal{U}_{\mathbb{Z}[\sqrt{-5}]} = \{-1, 1\}$.
- Claramente, $3+\sqrt{-5}$ não é o zero nem uma unidade do anel.
  Sejam $a+b\sqrt{-5}, c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tais que
  $$3+\sqrt{-5} = (a+b\sqrt{-5})(c+d\sqrt{-5}).$$
  Sendo estes dois complexos iguais, então, também o são os quadrados dos seus módulos. Logo, temos que
  $$14 = (a^2+5b^2)(c^2+5d^2).$$
  Tendo em conta que os fatores são não negativos, as únicas fatorizações possíveis são, a menos da ordem dos fatores, 2×7 e 1×14. Como a primeira é impossível (pois $a^2+5b^2 \neq 2$, para quaisquer inteiros a e b), concluímos que $a^2+5b^2 = 1$ ou $c^2+5d^2 = 1$. Como $a, b, c, d \in \mathbb{Z}$, concluímos que só podemos ter $a = \pm 1$ e $b = 0$ ou $c = \pm 1$ e $d = 0$, i.e., concluímos que $a+b\sqrt{-5}$ é uma unidade ou $c+d\sqrt{-5}$ é uma unidade. Logo $3+\sqrt{-5}$ é irredutível.