Departamento de Matemática — Universidade do Minho

Álgebra — 2º teste – 13 dez 2019

Lic. em Matemática - 2º ano — duracão: duas horas

Proposta de resolução

1. **Sem justificar**, diga se é verdadeira (V) ou falsa (F) cada uma das seguintes proposições, assinalando a opção conveniente:

   (a) Dados $n \in \mathbb{N}$ e $\sigma \in \mathcal{S}_n$, $o(\sigma) \leq n$. **V** **F**

   Falsa. A permutação τ do exercício 3. deste teste serve como contra exemplo. É uma permutação de $\mathcal{S}_9$ que tem ordem 12.

   (b) Se $\sigma \in \mathcal{S}_8$ tem ordem 5, então, $< \sigma >=< \sigma^4 >$. **V** **F**

   Verdadeira. Se $o(\sigma) = 5$, então $| < \sigma > | = 5$ e $o(\sigma^4) = \frac{5}{\text{m.d.c.}4,5} = 5$. Como $\sigma^4 \in < \sigma >$, temos que $< \sigma >=< \sigma^4 >$ (qualquer elemento de ordem 5 de um grupo de ordem 5 é gerador do grupo).

   (c) Se A é um anel e $a, b \in A$, então, $a^2 - b^2 = (a+b)(a-b)$. **V** **F**

   Falsa. Se A é um anel então, para todos $a, b \in A$, temos que $(a+b)(a-b) = a^2 - ab + ba - b^2$. A igualdade apresentada só se verifica se o anel é comutativo.

   (d) Existe pelo menos um domínio de integridade de característica 10. **V** **F**

   Falsa. Se A é um domínio de integridade de característica 10, temos que $1_A \in A$ e $o(1_A) = 10$. Assim, $10 \cdot 1_A = 0_A$ e, para todo $0 < k < 10$, $k \cdot 1_A \neq 0_A$. Mas,

   $$10 \cdot 1_A = (2 \times 5)(1_A 1_A) = (2 \cdot 1_A)(5 \cdot 1_A),$$

   pelo que, nas condições dadas, A é um domínio de integridade com divisores de zero não nulos, o que é uma contradição.

   (e) Sejam $\varphi : A \to A'$ um morfismo de anéis e I um ideal de A. Então, $\varphi(I)$ é um ideal de A'. **V** **F**

   Falsa. A afirmação só é verdadeira se o morfismo for sobrejtivo (i.e., um epimorfismo).

   (f) O anel $\mathbb{Z}_3 \times \mathbb{Z}_7$ é domínio de integridade. **V** **F**

   Falsa. $([1]_3, [0]_7)$ e $([0]_3, [1]_7)$ são elementos não nulos de $\mathbb{Z}_3 \times \mathbb{Z}_7$ cujo produto é o zero deste anel. Logo, ambos os elementos são divisores de zero não nulos de $\mathbb{Z}_3 \times \mathbb{Z}_7$ e, por essa razão, este anel não é domínio de integridade.

   (g) Nenhum elemento invertível de um anel com identidade é divisor de zero. **V** **F**

   Verdadeira. Se a é um elemento invertível do anel A com identidade e $b \in A$ é tal que $ab = 0_A$ ou $ba = 0_A$, temos que $b = a^{-1}ab = a^{-1}0_A = 0_A$ ou $b = baa^{-1} = 0_A a^{-1} = 0_A$. Estamos em condições de concluir que a não é divisor de zero.

   (h) Dados I e J ideais próprios de um anel A, se $I \cap J$ é ideal maximal de A, então $I = J$. **V** **F**

   Verdadeira. Se $I \cap J$ é um ideal maximal, não existem ideais K de A tais que $I \cap J \subsetneqq K \subsetneqq A$. Mas, $I \cap J \subseteq I \subsetneqq A$ e $I \cap J \subseteq J \subsetneqq A$. Logo, $I = I \cap J = J$.

2. Considere os seguintes anéis comutativos com identidade:

   $$A_1 = \mathbb{Z}_{10} \qquad A_2 = \mathbb{Z}_3 \times \mathbb{Z}_7 \qquad A_3 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{Z} \right\}$$

   (a) Indique, **sem justificar**:

   i. a identidade de cada anel:

   $$1_{A_1} = \underline{[1]_{10}} \qquad 1_{A_2} = \underline{([1]_3, [1]_7)} \qquad 1_{A_3} = \underline{I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}$$

ii. a característica de cada anel:
Observação: uma vez que os anéis têm identidade, a caraterística de cada anel é a ordem do seu elemento identidade se e só se esta for finita. Caso contrário, a característica é 0.

$$c(A_1) = \underline{10} \qquad c(A_2) = \underline{\text{m.m.c.}(3,7) = 21} \qquad c(A_3) = \underline{0}$$

iii. um elemento $x \in \mathcal{U}_A \backslash \{1_A\}$ para:

$$A = A_1 : \underline{[9]_{10}} \qquad A = A_2 : \underline{([2]_3, [6]_7)} \qquad A = A_3 : \underline{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}$$

Observação: Em A_1, qualquer elemento da forma $[a]_{10}$, com $a \in \mathbb{Z}$ tal que $\text{m.d.c.}(a, 10) = 1$ e $a \not\equiv 1 (\mod 10)$, é um elemento nas condições pedidas. Em A_2, qualquer elemento da forma $([b]_3, [c]_7)$, com $b, c \in \mathbb{Z}$ tais que $\text{m.d.c.}(b, 3) = \text{m.d.c.}(c, 7) = 1$ e $b \not\equiv 1 (\mod 3)$ e $c \not\equiv 1 (\mod 7)$, é um elemento nas condições pedidas. Em A_3, o elemento apresentado é o único nas condições pedidas.

(b) Quais dos anéis têm divisores de zero não nulos? Indique, caso existam, um divisor de zero não nulo de cada um desses anéis. Justifique.

Os únicos anéis que têm divisores de zero não nulos são A_1 e A_2:

- Em A_1, $[2]_{10}$ e $[5]_{10}$ são dois elementos não nulos tais que $[2]_{10}[5]_{10} = [2 \times 5]_{10} = [10]_{10} = [0]_{10}$.
- Em A_2, $([1]_3, [0]_7)$ e $([0]_3, [1]_7)$ são elementos não nulos de $\mathbb{Z}_3 \times \mathbb{Z}_7$ cujo produto é o zero deste anel. Logo, ambos os elementos são divisores de zero não nulos de $\mathbb{Z}_3 \times \mathbb{Z}_7$.
- Em A_3, como

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Leftrightarrow ab = 0 \Leftrightarrow a = 0 \vee b = 0,$$

não existem divisores de zero não nulos.

3. Considere, em $\mathcal{S}_9$, as permutações

$$\sigma = (1\,2\,3\,4\,5)(2\,6\,7\,9\,5\,1) \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 8 & 7 & 9 & 1 & 2 & 6 \end{pmatrix}.$$

(a) Escreva $\sigma\tau^{-1}$ como produto de ciclos disjuntos.

Temos

$$\begin{aligned} \sigma\tau^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 5 & 2 & 7 & 9 & 8 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 1 & 2 & 3 & 9 & 5 & 4 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 3 & 6 & 4 & 1 & 2 & 5 & 7 \end{pmatrix} = (1\,9\,7\,2\,8\,5\,4\,6) \end{aligned}.$$

(b) Determine $o(\sigma)$.

Escrevendo σ como produto de ciclos disjuntos, obtemos $\sigma = (1\,3\,4\,5\,2\,6\,7\,9)$. Assim, sendo σ um ciclo de comprimento 8, temos que $o(\sigma) = 8$.

(c) Indique, justificando, os elementos de $< \tau^3 >$.

Escrevendo τ como produto de ciclos disjuntos, obtemos $\tau = (1\,3\,5\,7)(2\,8\,4)(6\,9)$. Uma vez que os três ciclos são disjuntos podemos concluir que $o(\tau) = \text{m.m.c.}(4, 3, 2) = 12$ e que $\tau^n = (1\,3\,5\,7)^n(2\,8\,4)^n(6\,9)^n$, para todo $n \in \mathbb{Z}$. Da primeira, concluímos que $o(\tau^3) = \frac{12}{\text{m.d.c.}(3,12)} = 4$ e, por isso, $< \tau^3 >= \{\text{id}, \tau^3, (\tau^3)^2, (\tau^3)^3\}$. Da segunda, concluímos que

$$\begin{aligned} \tau^3 &= (1\,3\,5\,7)^3(2\,8\,4)^3(6\,9)^3 = (1\,3\,5\,7)^{-1}\text{id}(6\,9) = (7\,5\,3\,1)(6\,9), \\ \tau^6 &= (1\,3\,5\,7)^6(2\,8\,4)^6(6\,9)^6 = (1\,3\,5\,7)^2 = (1\,5)(3\,7), \\ \tau^9 &= (1\,3\,5\,7)^9(2\,8\,4)^9(6\,9)^9 = (1\,3\,5\,7)(6\,9). \end{aligned}$$

Logo,

$$< \tau^3 >= \{\text{id}, (7\,5\,3\,1)(6\,9), (1\,5)(3\,7), (1\,3\,5\,7)(6\,9)\}.$$

(d) **Sem efetuar cálculos com composição de funções**, mostre que não existe $\delta \in \mathcal{S}_9$ tal que $\delta^2\tau = \sigma$.

Começamos por observar que, por (a),

$$\delta^2\tau = \sigma \Leftrightarrow \delta^2 = \sigma\tau^{-1} = (1\,9\,7\,2\,8\,5\,4\,6).$$

Sendo este um ciclo de comprimento par (8), temos que, existindo δ nas condições dadas, δ^2 é uma permutação ímpar. No entanto, o produto (composta) de qualquer permutação consigo mesma é uma permutação par pois pode ser escrita com o dobro das transposições usadas para escrever essa permutação. Sabemos também que nenhuma permutação pode ser simultaneamente par e ímpar. Logo, não pode existir δ nas condições dadas.

4. (a) Mostre que $\varphi : \mathbb{Z} \to \mathbb{Z}_{10}$ definida por $\varphi(n) = [6n]_{10}$, para todo $n \in \mathbb{Z}$, é um homomorfismo de anéis e determine o seu núcleo.

Sejam $n, m \in \mathbb{Z}$. Então:

1. $\varphi(n+m) = [6(n+m)]_{10} = [6n+6m]_{10} = [6n]_{10} + [6m]_{10} = \varphi(n) + \varphi(m)$;
2. $\varphi(nm) = [6(nm)]_{10} = [36(nm)]_{10} = [(6n)(6m)]_{10} = [6n]_{10}[6m]_{10} = \varphi(n)\varphi(m)$, uma vez que $36 \equiv 6(\mod 10)$.

Tendo em conta os pontos 1. e 2., concluímos que φ é um homomorfismo de anéis.
Mais ainda, tendo em conta que $\mathrm{Nuc}\varphi = \{n \in \mathbb{Z} : \varphi(n) = [0]_{10}\}$ e que

$$\varphi(n) = [0]_{10} \Leftrightarrow [6n]_{10} = [0]_{10} \Leftrightarrow 6n \equiv 0(\mod 10) \Leftrightarrow n \equiv 0(\mod \frac{10}{\text{m.d.c.}(6,10)}) \Leftrightarrow n \equiv 0(\mod 5),$$

concluímos que

$$\mathrm{Nuc}\varphi = 5\mathbb{Z}.$$

(b) Seja A um anel comutativo com identidade tal que

$$\forall x \in A,\ \exists n \in \mathbb{N}\backslash\{1\} : x^n = x.$$

Mostre que todo o ideal primo de A é um ideal maximal de A.

Suponhamos que I é um ideal primo de A, i.e., que:
(i) $A\backslash I \neq \emptyset$;
(ii) se $ab \in I$ então $a \in I$ ou $b \in I$.
Queremos provar que I é um ideal maximal de A, i.e., que não existe K ideal de A tal que $I \subsetneq K \subsetneq A$. Seja K um ideal de A tal que $I \subsetneq K$. Pretendemos provar que $K = A$. Para tal, basta provar que $1_A \in K$. De $I \subsetneq K$ sabemos que existe $x \in K$ tal que $x \notin I$. Mas, se $x \in K$, então, $x \in A$ e, por hipótese, existe um natural $n \geq 2$ tal que $x^n = x$. Mas,

$$x^n = x \Leftrightarrow x^n - x = 0_A \Leftrightarrow x(x^{n-1} - 1_A) = 0_A.$$

Como I é um ideal primo, $0_A \in I$ e $x \notin I$, temos, por (ii), que $x^{n-1} - 1_A \in I$. Então, $x^{n-1} - 1_A \in K$. Juntamente com o facto de que se $x \in K$, então, $x^{n-1} \in K$, concluímos que

$$1_A = x^{n-1} - (x^{n-1} - 1_A) \in K.$$

5. Considere o domínio de integridade $\mathbb{Z}[\sqrt{-5}]$. Recorde que $\mathcal{U}_{\mathbb{Z}[\sqrt{-5}]} = \{-1, 1\}$.

(a) Mostre que $1 + \sqrt{-5}$ é irredutível em $\mathbb{Z}[\sqrt{-5}]$.

Claramente, $1 + \sqrt{-5}$ 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

$$1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5}).$$

Sendo estes dois complexos iguais, então, também o são os quadrados dos seus módulos. Logo, temos que

$$6 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Tendo em conta que os fatores são não negativos, as únicas fatorizações possíveis são, a menos da ordem dos fatores, 2×3 e 1×6. 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 $1 + \sqrt{-5}$ é irredutível.

(b) Mostre que $1+\sqrt{-5}$ não é um elemento primo em $\mathbb{Z}[\sqrt{-5}]$.

$1+\sqrt{-5}$ não é primo pois divide $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2\times 3$ e não divide nem 2 nem 3. De facto, se $1+\sqrt{-5} \mid 2$, existiria $a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tal que

$$2 = (1+\sqrt{-5})(a+b\sqrt{-5}) = (a-5b)+(b+a)\sqrt{-5},$$

ou seja, existiria $b \in \mathbb{Z}$ tal que $2 = -6b$, o que é impossível em $\mathbb{Z}$. Do mesmo modo, se $1+\sqrt{-5} \mid 3$, existiria $a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tal que

$$3 = (1+\sqrt{-5})(a+b\sqrt{-5}) = (a-5b)+(b+a)\sqrt{-5},$$

ou seja, existiria $b \in \mathbb{Z}$ tal que $3 = -6b$, o que também é impossível em $\mathbb{Z}$.

(c) Determine $[1+\sqrt{-5}, 12]$.

Por (a), temos que $1+\sqrt{-5}$ é irredutível em $\mathbb{Z}[\sqrt{-5}]$, pelo que existe sempre máximo divisor comum entre este elemento e qualquer outro elemento de $\mathbb{Z}[\sqrt{-5}]$. Mais ainda, sabemos que, para todo $x \in \mathbb{Z}[\sqrt{-5}]$,

$$[1+\sqrt{-5}, x] = \begin{cases} (1+\sqrt{-5})\mathcal{U}_{\mathbb{Z}[\sqrt{-5}]} & \text{se } 1+\sqrt{-5} \mid x \\ \mathcal{U}_{\mathbb{Z}[\sqrt{-5}]} & \text{caso contrário} \end{cases}$$

Em (b), vimos que $1+\sqrt{-5}$ divide 6. Como $6 \mid 12$, temos que $1+\sqrt{-5}$ divide 12. Assim, $[1+\sqrt{-5}, 12] = (1+\sqrt{-5})\mathcal{U}_{\mathbb{Z}[\sqrt{-7}]} = \{1+\sqrt{-5}, -1-\sqrt{-5}\}$.

Cotação: **1.** 6 valores; **2.** 4 valores; **3.** 3 valores; **4.** 4 valores; **5.** 3 valores