Álgebra — 2º teste/teste global – 19 dez 2016

Licenciatura em Ciências de Computação - 2º ano

Para realizar o TESTE GLOBAL, responda às perguntas 1 - 6
Para realizar o 2º TESTE, responda às perguntas 3 - 8

1. Sejam G um grupo e $H = \{(x, x) : x \in G\}$.

   (a) Mostre que H é subgrupo do produto direto $G \times G$.

   Nas condições do enunciado, temos que:

   i. $(1_G, 1_G) \in H$, pois $1_G \in G$. Logo, $H \neq \emptyset$;

   ii. dados $(x, x), (y, y) \in H$, temos que $x, y \in G$ e, por isso, $xy \in G$. Logo,
   $$(x, x)(y, y) = (xy, xy) \in H;$$

   iii. dado $(x, x) \in H$, temos que que $x \in G$ e, consequentemente, $x^{-1} \in G$. Logo,
   $$(x, x)^{-1} = (x^{-1}, x^{-1}) \in H.$$

   Assim, estamos em condições de concluir que $H < G \times G$.

   (b) Mostre que $H \triangleleft G \times G$ se e só se G é abeliano.

   Suponhamos primeiro que G é abeliano. Então, o produto direto $G \times G$ é também abeliano e, portanto, qualquer seu subgrupo é normal em $G \times G$. Como, por (a), $H < G \times G$, então $H \triangleleft G \times G$.
   Reciprocamente, suponhamos que $H \triangleleft G \times G$. Sejam $a, b \in G$. Então, $(a, a) \in H$ e $(a, b) \in G \times G$. Por hipótese, temos que $(a, b)(a, a)(a, b)^{-1} \in H$, ou seja, $(aaa^{-1}, bab^{-1}) = (a, bab^{-1}) \in H$. Por definição de H, temos que $a = bab^{-1}$. Multiplicando por b à direita, obtemos $ab = ba$. Assim, estamos em condições de concluir que G é abeliano.

   (c) Para $G = \mathbb{Z}_6$, determine um elemento de H que tenha ordem 3.

   Sendo G o grupo aditivo $\mathbb{Z}_6$, temos que $(\overline{2}, \overline{2}) \in H$ é tal que:

   i. $(\overline{2}, \overline{2}) \neq (\overline{0}, \overline{0})$;

   ii. $(\overline{2}, \overline{2}) + (\overline{2}, \overline{2}) = (\overline{4}, \overline{4}) \neq (\overline{0}, \overline{0})$;

   iii. $(\overline{2}, \overline{2}) + (\overline{2}, \overline{2}) + (\overline{2}, \overline{2}) = (\overline{6}, \overline{6}) = (\overline{0}, \overline{0})$.

   Logo, $o((\overline{2}, \overline{2})) = 3$.

   (d) Para $G = \mathbb{Z}_3$, mostre que H é cíclico.

   Sendo G o grupo aditivo $\mathbb{Z}_3$, $H = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{1}), (\overline{2}, \overline{2})\}$. Então, H é um grupo de ordem prima (3), pelo que é um grupo cíclico.

2. Um grupo G diz-se simples se não admite subgrupos diferentes de $\{1_G\}$ e de G.

   Sejam G um grupo simples, G' um grupo e $\varphi : G \to G'$ um morfismo de grupos não constante. Mostre que G' admite um subgrupo isomorfo a G.

Como φ é um morfismo de grupos, temos que $\mathrm{Nuc}\varphi$ é subgrupo de G e $\varphi(G)$ é subgrupo de G'. Como G é um grupo simples, $\mathrm{Nuc}\varphi = \{1_G\}$ ou $\mathrm{Nuc}\varphi = G$. Como φ é não constante, não podemos ter $\mathrm{Nuc}\varphi = G$. Então, temos que $\mathrm{Nuc}\varphi = \{1_G\}$ e, portanto, φ é um monomorfismo. Logo, $G \simeq \varphi(G)$, o que prova o resultado pretendido.

3. Seja $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & a & 1 & 3 & b & c & d \end{pmatrix}$ uma permutação de S_7.

   (a) Considere $a = 2$, $b = 7$, $c = 5$ e $d = 6$.

      i. Mostre que σ é uma permutação par.

         Como
         $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 3 & 7 & 5 & 6 \end{pmatrix} = (1\,4\,3)(5\,7\,6) = (1\,3)(1\,4)(5\,6)(5\,7),$$
         concluímos que, escrevendo σ como um produto de um determinado número de transposições, esse número tem de ser par. Logo, σ é uma permutação par.

      ii. Determine σ^{16}.

         Como $\sigma = (1\,4\,3)(5\,7\,6)$ e estes dois ciclos são disjuntos e têm comprimento 3, temos que $o(\sigma) = \mathrm{m.m.c.}(3,3) = 3$. Assim, $\sigma^3 = \mathrm{id}$. Como $16 = 3 \times 5 + 1$, temos que
         $$\sigma^{16} = \sigma^{3\times5+1} = (\sigma^3)^5\sigma^1 = (\mathrm{id})^5\sigma = \mathrm{id}\sigma = \sigma.$$

      iii. Existe $\tau \in S_7$ tal que $o(\tau\sigma) = 8$? Justifique.

         Nenhuma permutação de S_7 tem ordem 8. De facto, como, em S_7, um ciclo tem, no máximo, ordem 7, para poder ter ordem maior ou igual a 8, a permutação terá de ser escrita como produto de ciclos disjuntos, sendo a sua ordem, neste caso, o mínimo múltiplo comum dos comprimentos desses ciclos. Como 8 não é mínimo múltiplo comum de números menores que 8, essa permutação não existe. Se não existe qualquer permutação com ordem 8, também não existe τ de tal modo que $\tau\sigma$ tenha ordem 8.

   (b) Dê exemplo, ou justifique que não é possível, de valores de a, b, c e d de tal modo que σ tenha ordem 12.

   Se considerarmos $a = 5$, $b = 6$, $c = 7$ e $d = 2$, temos que
   $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 1 & 3 & 6 & 7 & 2 \end{pmatrix} = (1\,4\,3)(2\,5\,7\,6).$$
   Como σ se escreve como produto de dois ciclos disjuntos de comprimentos 3 e 4, temos que $o(\sigma) = 3 \times 4 = 12$.

4. Sejam A um anel comutativo com identidade e $a \in A$.

   (a) Mostre que $R_a = \{x \in A : xa = 0_A\}$ é um ideal de A.

   Nas condições do enunciado, temos:

      i. $0_A \in A$ é tal que $0_A a = 0_A$. Logo, $0_A \in R_a$ e, portanto, $R_a \neq \emptyset$;

      ii. dados $x, y \in R_a$, $x, y \in A$, $xa = 0_A$ e $ya = 0_A$, pelo que $x - y \in A$ é tal que
         $$(x - y)a = xa - ya = 0_A - 0_A = 0_A.$$
         Logo, $x - y \in R_a$;

iii. dado $x \in R_a$ e $y \in A$, $x, y \in A$ e $xa = 0_A$. Assim, $yx \in A$ e

$$(yx)a = y(xa) = y0_A = 0_A.$$

Assim, $yx \in R_a$. Como A é comutativo, podemos também concluir que $xy \in R_a$.

Logo, R_a é um ideal de A.

(b) Mostre que o ideal é próprio se e só se $a \neq 0_A$.

Como

$$R_a = A \Leftrightarrow 1_A \in R_a \Leftrightarrow 1_A a = 0_A \Leftrightarrow a = 0_A,$$

temos que

$$R_a \neq A \Leftrightarrow a \neq 0_A,$$

o que prova o resultado pretendido.

(c) Determine R_a se:

i. A é domínio de integridade e $a \neq 0_A$;

Se A é domínio de integridade, o único divisor de zero é o elemento 0_A. Se $a \neq 0_A$, afirmar que $x \in R_a$ é equivalente a afirmar que x é divisor de zero. Logo, $R_a = \{0_A\}$.

ii. $A = \mathbb{Z}_{12}$ e $a = [2]_{12}$.

Em $A = \mathbb{Z}_{12}$, temos que $[0]_{12}[2]_{12} = [0]_{12}$, $[6]_{12}[2]_{12} = [0]_{12}$ e $[x]_{12}[2]_{12} \neq [0]_{12}$, para todo $x \in \{1, 2, 3, 4, 5, 7, 8, 9, 10, 11\}$. Logo, $R_a = \{[0]_{12}, [6]_{12}\}$.

5. Sejam A um anel não nulo com identidade 1_A e $\varphi : \mathbb{Z} \to A$ a aplicação definida por $\varphi(n) = n1_A$, para todo $n \in \mathbb{Z}$.

(a) Mostre que φ é um morfismo de anéis.

Sejam $n, m \in \mathbb{Z}$. Então:

$$\begin{aligned}\varphi(n+m) &= (n+m)1_A \\ &= n1_A + m1_A && \text{[pelas propriedades dos múltiplos]} \\ &= \varphi n + \varphi m\end{aligned}$$

e

$$\begin{aligned}\varphi(nm) &= (nm)1_A \\ &= (nm)(1_A 1_A) && \text{[por definição de } 1_A\text{]} \\ &= (n1_A)(m1_A) && \text{[pelas propriedades dos múltiplos]} \\ &= \varphi n \varphi m\end{aligned}$$

Logo, φ é um morfismo de anéis.

(b) Determine $\mathrm{Nuc}\varphi$ se:

i. $o(1_A) = \infty$;

Se $o(1_A) = \infty$, temos que $n1_A = 0_A$ se e só se $n = 0$, pelo que $\mathrm{Nuc}\varphi = \{0\}$.

ii. $A = \mathbb{Z}_6$.

Se $A = \mathbb{Z}_6$, $n1_A = 0_A$ se e só se $n[1]_6 = [0]_6$. Como $n[1]_6 = [n]_6$, temos que

$$n \in \mathrm{Nuc}\varphi \Leftrightarrow [n]_6 = [0]_6 \Leftrightarrow n \in 6\mathbb{Z}.$$

Logo, $\mathrm{Nuc}\varphi = 6\mathbb{Z}$.

6. Considere o domínio de integridade $\mathbb{Z}[\sqrt{-7}]$.

   (a) Determine o conjunto das unidades de $\mathbb{Z}[\sqrt{-7}]$.

   (b) Seja $a+b\sqrt{-7}$ uma unidade de $\mathbb{Z}[\sqrt{-7}]$. Então, existe $c+d\sqrt{-7}\in\mathbb{Z}[\sqrt{-7}]$ tal que

   $$(A) \qquad (a+b\sqrt{-7})(c+d\sqrt{-7})=1.$$

   Sendo dois números complexos iguais, também são iguais os quadrados dos seus módulos. Assim, temos que

   $$(a^2+7b^2)(c^2+7d^2)=1.$$

   Como $a,b,c,d\in\mathbb{Z}$, concluímos que só podemos ter $a=\pm1$,$c=\pm1$ e $b=d=0$. Substituindo em (A), concluímos que só podemos ter $a=c=\pm1$ e $b=d=0$. Assim, as únicas unidades de $\mathbb{Z}[\sqrt{-7}]$ são 1 e -1. Logo $\mathcal{U}_{\mathbb{Z}[\sqrt{-7}]}=\{-1,1\}$.

   (c) Mostre que $1+\sqrt{-7}$ é irredutível em $\mathbb{Z}[\sqrt{-7}]$.

   Sejam $a+b\sqrt{-7}, c+d\sqrt{-7}\in\mathbb{Z}[\sqrt{-7}]$ tais que

   $$1+\sqrt{-7}=(a+b\sqrt{-7})(c+d\sqrt{-7}).$$

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

   $$8=(a^2+7b^2)(c^2+7d^2).$$

   Tendo em conta que os fatores são não negativos, as únicas fatorizações possíveis são, a menos da ordem dos fatores, 2×4 e 1×8. Como a primeira é impossível (pois $a^2+7b^2\neq2$, para quaisquer inteiros a e b), concluímos que $a^2+7b^2=1$ ou $c^2+7d^2=1$. Aplicando agora o raciocínio usado anteriormente, concluímos que $a+b\sqrt{-7}$ é uma unidade ou $c+d\sqrt{-7}$ é uma unidade. Logo $1+\sqrt{-7}$ é irredutível.

   (d) Mostre que $1+\sqrt{-7}$ não é um elemento primo em $\mathbb{Z}[\sqrt{-7}]$.

   $1+\sqrt{-7}$ não é primo pois divide $(1+\sqrt{-7})(1-\sqrt{-7})=8=2\times4$ e não divide nem 2 nem 4. De facto, se $1+\sqrt{-7}\mid 2$, existiria $a+b\sqrt{-7}\in\mathbb{Z}[\sqrt{-7}]$ tal que

   $$2=(1+\sqrt{-7})(a+b\sqrt{-7})=(a-7b)+(b+a)\sqrt{-7},$$

   ou seja, existiria $b\in\mathbb{Z}$ tal que $2=-8b$, o que é impossível em $\mathbb{Z}$. Do mesmo modo, se $1+\sqrt{-7}\mid 4$, existiria $a+b\sqrt{-7}\in\mathbb{Z}[\sqrt{-7}]$ tal que

   $$4=(1+\sqrt{-7})(a+b\sqrt{-7})=(a-7b)+(b+a)\sqrt{-7},$$

   ou seja, existiria $b\in\mathbb{Z}$ tal que $4=-8b$, o que também é impossível em $\mathbb{Z}$.

   (e) Determine $[1+\sqrt{-7},4]$.

   Por (b), temos que $1+\sqrt{-7}$ é irredutível em $\mathbb{Z}[\sqrt{-7}]$, pelo que existe sempre máximo divisor comum entre este elemento e qualquer outro. Além disso, em (c), vimos que $1+\sqrt{-7}$ não divide 4. Assim, os únicos divisores comuns entre os dois elementos são as unidades, pelo que $[1+\sqrt{-7},4]=\mathcal{U}_{\mathbb{Z}[\sqrt{-7}]}=\{-1,1\}$.

7. Sejam K um corpo, A um anel não nulo com identidade e $\alpha: K\to A$ um homomorfismo de anéis tal que $\alpha(1_K)=1_A$. Mostre que existe um subanel de A isomorfo a K.

Como α é um homomorfismo de anéis, temos que $\mathrm{Nuc}\alpha$ é ideal de K e $\alpha(K)$ é subanel de A. Como K é um corpo, os seus únicos ideais são $\{0_K\}$ e K, pelo que $\mathrm{Nuc}\alpha = \{0_K\}$ ou $\mathrm{Nuc}\alpha = K$. Como $1_K \notin \mathrm{Nuc}\alpha$, não podemos ter $\mathrm{Nuc}\alpha = K$. Então, temos que $\mathrm{Nuc}\alpha = \{0_K\}$ e, portanto, α é um monomorfismo. Logo, $K \simeq \alpha(K)$, o que prova o resultado pretendido.

8. Seja A um anel comutativo com característica 3. Mostre que:

   (a) $(a+b)^3 = a^3 + b^3$;

   Como A é um anel comutativo, temos que $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$. Mais ainda, como A tem característica 3, temos que, para todo $x \in A$, $3x = 0_A$. Em particular, $3a^2b = 3ab^2 = 0_A$. Logo, $(a+b)^3 = a^3 + b^3$.

   (b) $B = \{a \in A : a^3 = a\}$ é um subanel de A.

   Como $0_A^3 = 0_A$, temos que $0_A \in B$ e, portanto, $B \neq \emptyset$. Mais ainda, para $x, y \in B$, temos que $x, y \in A$, $x^3 = x$ e $y^3 = y$, pelo que $x - y, xy \in A$ e

$$\begin{aligned} (x-y)^3 &= x^3 + (-y)^3 && \text{[por (a)]} \\ &= x^3 - y^3 = x - y \end{aligned}$$

   e

$$\begin{aligned} (xy)^3 &= x^3y^3 && \text{[porque o anel é comutativo]} \\ &= xy. \end{aligned}$$

   Logo, B é subanel de A.