Departamento de Matemática da F.C.T.U.C.

Corpos e Equações Algébricas – Teste 1

23/3/2009

Nome (completo): ____

____

Nota: *Justifique resumidamente as suas respostas.*

(1) Diga se as seguintes afirmações são verdadeiras ou falsas. No caso de ser verdadeira, justifique, e, no caso de ser falso, dê um contra-exemplo.
  (a) Num anel com identidade 1, os elementos 1 e -1 são invertíveis.
  (b) Num anel todo o divisor de zero à esquerda também é à direita.
  (c) A função $f : \mathbb{Z}_p \to \mathbb{Z}_p$, com p primo, definida por $f(a) = a^{p^2}$ é um homomorfismo injectivo de anéis.

(2) Seja $A = (\mathbb{Q}, +, *)$ onde $+$ denota a adição usual de racionais e $*$ é definida por $a * b = ab/2$.
  (a) Assuma que $(\mathbb{Q}, +)$ é um grupo comutativo e mostre que A é um corpo.
  (b) Determine um subanel de A que seja isomorfo ao anel usual $(\mathbb{Z}, +, .)$ dos inteiros. Descreva esse isomorfismo.

(3) Considere os polinómios em $\mathbb{Z}_3[x]$ definidos por

$$p(x) = x^4 + 2x + 2,\ q(x) = x^3 + 2x^2 + x.$$

  (a) Determine $mdc(p(x),\, q(x))$.
  (b) Defina ideal I de um anel qualquer.
  (c) Conclua que o ideal $< p(x), q(x) >$ gerado por $p(x)$ e $q(x)$ é principal. Verifique se este ideal é igual a $\mathbb{Z}_3[x]$.

RESOLUÇÃO:

(1) (a) Verdadeira. $a \in A$ diz-se invertível se existe $b \in A$ tal que $ab = ba = 1$. Tem-se $1.1 = 1$ e $(-1)(-1) = 1$. Logo 1 e -1 são invertíveis.

(b) Falsa. Um elemento não nulo a de um anel A é dito divisor de zero à esquerda se existe um elemento b não nulo de A tal que $ab = 0$. Analogamente a é dito divisor de zero à direita se existe um elemento não nulo de A, digamos c, tal que $ca = 0$.
Exemplo de um anel que tem divisores de zero que são apenas de um lado.
Seja $S = \{a = (a_1, a_2, \cdots) : a_i \in \mathbb{Z}\}$ o conjunto das sucessões inteiras. $(S, +)$, com a adição $+$ usual de sucessões, tem a estrutura de grupo abeliano. Seja S^S o conjunto dos homorfismos do grupo S, e $A = (S^S, +, .)$ onde a primeira operação "$+$" significa a adição usual de funções, e a segunda operação "$.$" a composição. A é um anel não comutativo com identidade id (função identidade). (O zero de A é a função nula, denotada por 0.)
Considerem-se λ, τ e ρ homomorfismos não nulos de S, definidos por $\lambda(a_1, a_2, \dots) = (a_2, a_3, \dots)$, $\rho(a_1, a_2, \dots) = (0, a_1, a_2, \dots)$, e $\tau(a_1, a_2, \dots) = (a_1, 0, 0, \dots)$. Em particular, $\tau(0, 0, \dots) = (0, 0, \dots)$. Note-se que $\lambda\rho = id \neq \rho\lambda$ e $\lambda\tau = 0$. Portanto, λ é divisor de zero à esquerda. Se λ fosse um divisor de zero à direita, então existia $f \neq 0$ em A tal que $f\lambda = 0$. Donde $(f\lambda)\rho = 0\rho = 0$, $0 = (f\lambda)\rho = f(\lambda\rho) = f\, id = f$. Portanto, λ é um divisor de zero à esquerda mas não à direita.
Nota: No anel não comutativo $M_n(\mathbb{R})$ das matrizes reais n por n os divisores de zero à esquerda e à direita coincidem. São precisamente todas as matrizes singulares não nulas. Aqui não temos contra-exemplo.

(c) Verdadeira. $\mathbb{Z}_p$, com p primo, é um corpo (em particular, um domínio de integridade) de característica prima. Neste caso, tem-se $(a + b)^{p^2} = a^{p^2} + b^{p^2}$, $(a - b)^{p^2} = a^{p^2} - b^{p^2}$, e, como $\mathbb{Z}_p$ é também um anel comutativo, tem-se $(ab)^{p^2} = a^{p^2} b^{p^2}$. Vem então $f(a + b) = (a + b)^{p^2} = a^{p^2} + b^{p^2} = f(a) + f(b)$ e $f(ab) = (ab)^{p^2} = a^{p^2} b^{p^2} = f(a)f(b)$.
Então, f é um homomorfismo de anéis. Além disso, $f(a) = f(b)$ equivale a escrever $a^{p^2} = b^{p^2} \Leftrightarrow a^{p^2} - b^{p^2} = 0 \Leftrightarrow (a - b)^{p^2} = 0$. Como $\mathbb{Z}_p$ não tem divisores de zero, tem-se $a - b = 0$, isto é, $a = b$. Ou seja f é injectiva.

(2) (a) Como $(\mathbb{Q},+)$ tem estrutura de grupo comutativo, A é também um grupo comutativo com respeito a "+". Em primeiro lugar, $\mathbb{Q}$ é fechado para a operação $*$. A a operação $*$ é comutativa, isto é, para todo o a e b de A, $a*b = ab/2 = ba/2 = b*a$; a operação $*$ é associativa $a*(b*c) = a(bc/2)/2 = (ab/2)c/2 = (a*b)c/2 = (a*b)*c$; a distributividade em A de $*$ relativamente a $+$ é válida, tem-se $a*(b+c) = a(b+c)/2 = (ab+ac)/2 = ab/2+ac/2 = a*b+a*c = b*a+c*a = (b+c)*a$, para todo o a,b,c em A. Portanto, A é anel comutativo com identidade igual a 2 (de facto, $a*2 = a.2/2 = a$ para todo o a em A). Todos os elementos não nulos de A são invertíveis. Dado $a \neq 0$ em A, o inverso de a em A é $4/a$. Concluímos deste modo que A é corpo.

(b) $2\mathbb{Z}$ é um subanel de A: $(2\mathbb{Z},+)$ é grupo comutativo e, além disso, $2\mathbb{Z}$ é fechado para a operação $*$, $2m*2m' = 4mm'/2 = 2mm' \in 2\mathbb{Z}$.
Considere-se $\phi : 2\mathbb{Z} \to \mathbb{Z}$ definida por $\phi(2m) = m$, com $m \in \mathbb{Z}$. ϕ é um homomorfismo de anéis e é bijectivo. De facto, tem-se

$$\begin{gathered}\phi(2m+2m') = \phi(2(m+m')) = m+m' = \phi(2m)+\phi(2m') \\ \phi(2m*2m') = \phi(4(mm')/2) = \phi(2mm') = mm' = \phi(2m)\phi(2m')\end{gathered}$$

e

$$\phi(m) = \phi(m') \Leftrightarrow 2m = 2m' \Leftrightarrow m = m'.$$

Dado $m \in \mathbb{Z}$, tem-se $\phi(2m) = m$.

(3) (a) Sendo $\mathbb{Z}_3$ um corpo, aplicando o algoritmo de Euclides que é válido num anel de polinómios com coeficientes num corpo, tem-se

$$\begin{gathered}x^4+2x+2 = (x+1)(x^3+2x^2+x)+x+2 \\ x^3+2x^2+x = (x^2+1)(x+2)+1\end{gathered}$$

Logo, $mdc(p(x),q(x)) = 1$.

(b) Um subanel I de um anel A diz-se um ideal se, para cada $a \in A$ e cada $x \in I$, ax e xa pertencem a I.

(c) Um ideal principal é um ideal gerado por um só elemento. Tem-se $< p(x), q(x) >= < mdc(p(x),q(x)) >=< 1 >$, portanto, o ideal é principal. Por sua vez, $< 1 >= \{1.p(x) = p(x) : p(x) \in \mathbb{Z}_3[x]\} = \mathbb{Z}_3[x]$.