Departamento de Matemática da Universidade de Coimbra **Corpos e Equações Algébricas**

SOLUÇÕES **Teste 1** 11/03/2011

1.(a) Determinemos $0_{\mathcal{A}}$: como $a + 0_{\mathcal{A}} = a \Leftrightarrow a +_6 0_{\mathcal{A}} +_6 1 = a \Leftrightarrow 0_{\mathcal{A}} +_6 1 = 0$, então $0_{\mathcal{A}} = 5$. Isso, bem como o cálculo de todos os simétricos, pode ser feito mais rapidamente calculando a tabela da operação + em $0_{\mathcal{A}}$:

+	0	1	2	3	4	$\boxed{5}$
0	1	2	3	4	$\boxed{5}$	0
1	2	3	4	$\boxed{5}$	0	1
2	3	4	$\boxed{5}$	0	1	2
3	4	$\boxed{5}$	0	1	2	3
4	$\boxed{5}$	0	1	2	3	4
$\boxed{5}$	0	1	2	3	4	$\boxed{5}$

Portanto, o neutro é o 5 e $-0 = 4, -1 = 3, -2 = 2, -3 = 1, -4 = 0$ e $-5 = 5$.

Quanto à identidade e os elementos invertíveis basta determinarmos a tabela de $\cdot$:

$\cdot$	$\boxed{0}$	1	2	3	4	5
$\boxed{0}$	$\boxed{0}$	1	2	3	4	5
1	1	3	5	1	3	5
2	2	5	2	5	2	5
3	3	1	5	3	1	5
4	4	3	2	1	$\boxed{0}$	5
5	5	5	5	5	5	5

Em conclusão:

$0_{\mathcal{A}}$	$1_{\mathcal{A}}$	-0	-1	-2	-3	-4	-5	0^{-1}	1^{-1}	2^{-1}	3^{-1}	4^{-1}	5^{-1}
5	0	4	3	2	1	0	5	0	×	×	×	4	×

(b) Elementos invertíveis: 0, 4; divisores de zero: 1, 2, 3 (pois $1 \cdot 2 = 5 = 0_{\mathcal{A}}$ e $2 \cdot 3 = 5 = 0_{\mathcal{A}}$).

2. São todas falsas pelo que não precisamos de provar nada!

3.(a) $\mathcal{N}(\mathbb{Z}) = \{0\}$ pois $\mathbb{Z}$ não possui divisores de zero ($a^n = 0$ num domínio de integridade implica sempre $a = 0$).

Por outro lado, $a^n = 0$ em $\mathbb{Z}_{16}$ significa $a^n \equiv 0 \pmod{16}$ em $\mathbb{Z}$, isto é, $16 = 2^4 \mid a^n$. Assim, necessariamente, $2 \mid a$ e a é obrigatoriamente par. Como esta condição é também claramente suficiente, então

$$\mathcal{N}(\mathbb{Z}_{16}) = \{0, 2, 4, 6, 8, 10, 12, 14\}.$$

(b) É evidente que $0 \in \mathcal{N}(A)$. É também evidente que para quaisquer $a \in \mathcal{N}(A)$ e $b \in A$, $ab \in \mathcal{N}(A)$, uma vez que $(ab)^n = a^n b^n$ para qualquer n.

Sejam $a, b \in \mathcal{N}(A)$ (suponhamos $a^n = 0$ e $b^m = 0$). Então $a^t = 0$ para qualquer $t \geq n$ e $b^s = 0$ para qualquer $s \geq m$. Portanto, para $k \geq n$ e usando a fórmula binomial $(a-b)^k = \sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}a^i\, b^{k-i}$, válida em qualquer anel comutativo, temos:

i	$k-i$	$a^i\, b^{k-i}$
0	k	b^k
1	$k-1$	$a\, b^{k-1}$
2	$k-2$	$a^2\, b^{k-2}$
$\vdots$	$\vdots$	$\vdots$
$n-1$	$k-n+1$	$a^{n-1}\, b^{k-n+1}$
n	$k-n$	$a^n\, b^{k-n} = 0$
$n+1$	$k-n-1$	$a^{n+1}\, b^{k-n-1} = 0$
$\vdots$	$\vdots$	$\vdots$
k	0	$a^k = 0$

Assim, como os a^i são nulos a partir de $i = n$, para garantirmos que todas as parcelas no somatório são nulas (e assim garantirmos que $(a-b)^k = 0$, mostrando que $a - b \in \mathcal{N}(A)$) basta exigir que $k - n + 1 \geq m$ (para que tenhamos $b^{k-i} = 0$ para $i = 0, 1, 2, \ldots, n-1$). Portanto, para $k \geq m + n - 1$, $(a-b)^k = 0$.

(c) Seja $a + \mathcal{N}(A) \in \mathcal{N}(A/\mathcal{N}(A))$. Então existe $n \in \mathbb{N}$ tal que $(a + \mathcal{N}(A))^n = 0 + \mathcal{N}(A)$. Isto significa que $a^n + \mathcal{N}(A) = 0 + \mathcal{N}(A)$, isto é, $a^n \in \mathcal{N}(A)$. Portanto, existe um $m \in \mathbb{N}$ tal que $(a^n)^m = 0$, ou seja $a^{nm} = 0$. Logo $a \in \mathcal{N}(A)$ e, consequentemente, $a + \mathcal{N}(A) = 0 + \mathcal{N}(A)$. Em conclusão,

$$\mathcal{N}(A/\mathcal{N}(A)) = \{\mathcal{N}(A)\}.$$

(d) Seja P um ideal primo de A. Se $a \in \mathcal{N}(A)$ então $a^n = 0$ para algum natural n. Mas $aa^{n-1} = a^n = 0 \in P$ e P é primo, o que implica $a \in P$ ou $a^{n-1} \in P$. No primeiro caso concluímos logo o que desejávamos. No segundo caso, aplicando o mesmo raciocínio, podemos concluir que $a \in P$ ou $a^{n-2} \in P$. Repetindo o raciocínio indutivamente chegaremos, ao cabo de um número finito de passos, à conclusão de que $a \in P$ sempre.

Aprofundando a questão 2:

(a) só é verdadeira em anéis comutativos (nesse caso, de facto, $(a+b)(a-b) = (a+b)a + (a+b)(-b) = a^2 + ba - ab - b^2 = a^2 + ab - ab - b^2 = a^2 - b^2$). Num anel onde existam elementos a e b tais que $ab \neq ba$ tem-se $ba - ab \neq 0$ pelo que $(a+b)(a-b) = a^2 + ba - ab - b^2 \neq a^2 - b^2$. Por exemplo, no anel das matrizes quadradas de ordem 2 com coeficientes inteiros, para

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

(b) não é verdadeira: basta atentarmos no exemplo do anel $\mathbb{Z}$.

(c) não é verdadeira, falha para a adição do anel:

$h(a+b) = (a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4 = a^4+2a^2b^2+b^4$ enquanto que $h(a)+h(b) = a^4+b^4$ e $2a^2b^2$ nem sempre é zero em $\mathbb{Z}_4$ (por exemplo: para $a=b=1$).

Resolução alternativa: como $h(0)=0, h(1)=1, h(2)=0$ e $h(3)=1$, indo à tabela da operação $+$ em $\mathbb{Z}_4$ obtemos imediatamente a tabela dos diversos valores de $h(a+b)$:

$$\begin{array}{c|cccc} a\backslash b & 0 & 1 & 2 & 3 \\ \hline 0 & & & & \\ 1 & & & & \\ 2 & & & & \\ 3 & & & & \end{array} \quad \xrightarrow{+_4} \quad \begin{array}{c|cccc} a+b & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array} \quad \xrightarrow{h} \quad \begin{array}{c|cccc} & & & & \\ \hline & 0 & 1 & 0 & 1 \\ & 1 & 0 & 1 & 0 \\ & 0 & 1 & 0 & 1 \\ & 1 & 0 & 1 & 0 \end{array}$$

Por outro lado, a tabela dos valores de $h(a)+h(b)$ obtem-se fazendo

$$\begin{array}{c|cccc} a\backslash b & 0 & 1 & 2 & 3 \\ \hline 0 & & & & \\ 1 & & & & \\ 2 & & & & \\ 3 & & & & \end{array} \quad \xrightarrow{h} \quad \begin{array}{c|cccc} h(a)\backslash h(b) & 0 & 1 & 0 & 1 \\ \hline 0 & & & & \\ 1 & & & & \\ 0 & & & & \\ 1 & & & & \end{array} \quad \xrightarrow{+_4} \quad \begin{array}{c|cccc} & & & & \\ \hline & 0 & 1 & 0 & 1 \\ & 1 & \boxed{2} & 1 & \boxed{2} \\ & 0 & 1 & 0 & 1 \\ & 1 & \boxed{2} & 1 & \boxed{2} \end{array}$$