SOLUÇÕES **Teste 1** 24/03/09

---

(1) Basta observar que, por definição de 0, se tem $0+0=0$.

(Outra justificação: como $0+(-0)=0=0+0$ então, pela lei do corte, $-0=0$.)

(2) Se a é invertível então a equação $ax=b$ tem uma solução única: $ax=b \Leftrightarrow x=a^{-1}b$. Caso contrário, pode acontecer tudo, isto é, pode não ter solução (por exemplo, em $\mathbb{Z}_4$, $2x=3$ não tem solução) ou mais do que uma solução (por exemplo, em $\mathbb{Z}_4$, $2x=0$ tem duas soluções: 0 e 2). Podemos dizer um pouco mais: se a tem um inverso à direita a_d^{-1} então a equação tem pelo menos uma solução ($x=a_d^{-1}b$) que é única quando esse inverso também é inverso à esquerda.

(3) aAa é claramente não vazio (contém, por exemplo, os elementos $a0a=0$ e $a1a=a$). Sejam axa e aya dois elementos arbitrários de aAa. Então $axa-aya=a(xa-ya)=a(x-y)a\in aAa$ e $(axa)(aya)=a(xay)a\in aAa$. Isto mostra que aAa é um subanel de A. Além disso, $(a1a)(axa)=aaxa=axa$ e $(axa)(a1a)=axaa=axa$.

(4) É evidente que $0\in R(A)$. Sejam $a,b\in R(A)$ (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 $a-b\in R(A)$) 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 $k\geq m+n-1$, $(a-b)^k=0$.

Finalmente, sejam $a\in A$ e $b\in R(A)$ (com $b^n=0$). Então $(ab)^n=a^nb^n=0$, o que mostra que $ab\in R(A)$.

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

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

(7) Afirmação verdadeira: $a^2 = 1 \Leftrightarrow a^2 - 1 = 0 \Leftrightarrow (a-1)(a+1) = 0$. Como não existem divisores de zero em A então $a - 1 = 0$ ou $a + 1 = 0$, isto é, $a = 1$ ou $a = -1$.

(8) Contra-exemplo: em $\mathbb{Z}_2$, $-1 = 1$ pois $1 + 1 = 0$.

(9) Afirmação verdadeira: $ab = ac \Leftrightarrow a(b - c) = 0$. Como $a \neq 0$ e não existem divisores de zero em A então $b - c = 0$, ou seja, $b = c$.

(10) Pelo algoritmo da divisão em $A[x]$, $\varphi(x) = q(x)x + d$ para algum $q(x) \in A[x]$ e algum $d \in A$. Como φ é sobrejectiva, existem $q_1(x)$ e $p(x)$ em $A[x]$ tais que $\varphi(q_1(x)) = q(x)$ e $\varphi(p(x)) = x$. Portanto, $\varphi(x) = \varphi(q_1(x))\varphi(p(x)) + \varphi(d) = \varphi(q_1(x)p(x) + d)$. Agora, pela injectividade de φ, podemos concluir que $x = q_1(x)p(x) + d$, o que implica que $gr(q_1(x)p(x)) = 1$. Consequentemente, ou $gr(q_1(x)) = 1$ e $gr(p(x)) = 0$, ou $gr(q_1(x)) = 0$ e $gr(p(x)) = 1$. Suponhamos que acontece o primeiro caso. Então $p(x) = a \in A$, o que implica $x = \varphi(p(x)) = \varphi(a) = a$, uma contradição. Logo, ocorre necessariamente o segundo caso: $q_1(x) = c \in A$ e $\varphi(x) = \varphi(q_1(x)p(x) + d) = \varphi(cp(x) + d) = cx + d$.
