Soluções de exercícios

Capítulo 1

1*. *Seja D um domínio de integridade. Mostre que:*

(a) *Para cada $d \in D - \{0\}$, a aplicação $\phi_d : D \to D$, definida por $\phi_d(x) = dx$, é injectiva.*

(b) *Se D é finito, então D é um corpo.*

Solução:

(a) Se $d \in D - \{0\}$, então para quaisquer $x, y \in D$,

$$dx = dy \Leftrightarrow dx - dy = 0 \Leftrightarrow d(x-y) = 0 \Rightarrow x - y = 0 \Leftrightarrow x = y,$$

o que mostra que ϕ_d é injectiva.

(b) Se D é finito então, para cada $d \in D - \{0\}$, sendo injectiva, ϕ_d é imediatamente bijectiva. Portanto, existe $c \in D$ tal que $\phi_d(c) = 1$, isto é, $dc = 1$. Isto significa que qualquer $d \in D - \{0\}$ é invertível, e D é um corpo.

2*. *Seja $A = (\mathbb{Q}, +, *)$, onde $+$ denota a adição usual de racionais e $*$ é definida por $a * b = ab/3$.*

(a) *Mostre que A é um corpo.*

(b) *Determine um subanel de A que seja isomorfo ao anel usual $(\mathbb{Z}, +, \cdot)$ dos inteiros, descrevendo o isomorfismo.*

Solução: (a) Uma vez que $+$ é a adição usual, o par $(\mathbb{Q}, +)$ é um grupo comutativo. Bastará então verificar que a operação $*$ é distributiva relativamente à adição, associativa, comutativa e tem elemento neutro e que todo o elemento diferente do zero tem inverso relativamente a esta operação:

<u>Distributividade</u>: Como $*$ é comutativa basta verificar uma das condições de distributividade: para quaisquer $a, b, c \in \mathbb{Q}$,

$$a * (b + c) = \frac{a(b+c)}{3} = \frac{ab + ac}{3} = \frac{ab}{3} + \frac{ac}{3} = (a * b) + (a * c).$$

Associatividade: Para quaisquer $a, b, c \in \mathbb{Q}$, $a * (b * c) = a * \frac{bc}{3} = \frac{abc}{9}$ enquanto $(a * b) * c = \frac{ab}{3} * c = \frac{abc}{9}$, pelo que se confirma a propriedade.

Comutatividade: Para quaisquer $a, b \in \mathbb{Q}$, $a * b = \frac{ab}{3} = \frac{ba}{3} = b * a$.

Elemento neutro: 3 é elemento neutro de $*$ pois, para qualquer $a \in \mathbb{Q}$, $a * 3 = a$.

Existência de inversos: Para cada $a \neq 0$ em $\mathbb{Q}$, $\frac{9}{a}$ é o inverso de a pois $a * \frac{9}{a} = 3$.
(b) Consideremos $S = 3\mathbb{Z} \subseteq \mathbb{Q}$, que é claramente um subanel de A: é não vazio e, para quaisquer $x = 3a, y = 3b \in S$, tem-se $x - y = 3a - 3b = 3(a - b) \in S$ e

$$x * y = \frac{xy}{3} = \frac{3a3b}{3} = 3ab \in S.$$

Também não é difícil ver que $(S, +, *) \cong (\mathbb{Z}, +, \cdot)$: a função

$$\begin{array}{rccc} f: & (S, +, *) & \to & (\mathbb{Z}, +, \cdot) \\ & x & \mapsto & \frac{x}{3} \end{array}$$

é um homomorfismo de anéis: para quaisquer $x, y \in S$ tem-se

$$f(x+y) = \frac{x+y}{3} = \frac{x}{3} + \frac{y}{3} = f(x) + f(y) \quad \text{e} \quad f(x*y) = f(\frac{xy}{3}) = \frac{xy}{9} = f(x)f(y).$$

Além disso, é injectiva, pois

$$f(x) = f(y) \Leftrightarrow \frac{x}{3} = \frac{y}{3} \Leftrightarrow x = y,$$

e é sobrejectiva, pois para cada $a \in \mathbb{Z}$, tomando $x = 3a \in S$, tem-se evidentemente $f(x) = \frac{3a}{3} = a$.

3*. *Prove que se A é um anel, I e J são ideais de A e P é um ideal primo de A, então*

$$IJ \subseteq P \;\Rightarrow\; I \subseteq P \text{ ou } J \subseteq P.$$

Solução: Suponhamos que $IJ \subseteq P$ e $I \nsubseteq P$. Então existe $a \in I$ tal que $a \notin P$. Mas, para qualquer $b \in J$, $ab \in IJ \subseteq P$, o que implica, pela primalidade de P, que $a \in P$ ou $b \in P$. Como $a \notin P$, teremos que ter forçosamente b em P, o que mostra que $J \subseteq P$.

4*. *Seja M um ideal próprio de um anel comutativo com identidade. Prove que M é maximal se e só se*

$$\forall\, a \in A \setminus M \;\; \exists x \in A : \; 1 - ax \in M.$$

Solução: Seja M um ideal maximal de A e $a \in A \setminus M$. Então o ideal

$$\langle M \cup \{a\} \rangle = \{m + ax \mid m \in M, x \in A\}$$

contém M estritamente pelo que terá que coincidir com A. Em particular, $1 \in \langle M \cup \{a\} \rangle$. Logo existem $m \in M$ e $x \in A$ tais que $1 = m + ax$, isto é, $1 - ax = m \in M$.

Reciprocamente, seja M um ideal próprio satisfazendo a condição enunciada e seja J um ideal de A satisfazendo $M \subset J \subseteq A$. Existe pelo menos um elemento $a \in J \setminus M$. Por hipótese existe então $x \in A$ tal que $1 - ax \in M$. Como $1 - ax \in J$ e $ax \in J$ então $1 \in J$ o que é suficiente para concluirmos que $J = A$ (de facto, como qualquer $a \in A$ se escreve na forma $a = a \cdot 1 \in J$, então $A \subseteq J$).

Nota: Com este resultado é possível provarmos que todo o ideal maximal é primo evitando o uso do teorema apresentado nas aulas:

Seja M um ideal maximal de A. Se $ab \in M$ e $b \notin M$ então, usando (a), existe $x \in A$ tal que $1 - bx = m \in M$. Logo $a = a \cdot 1 = a(m + bx) = am + abx \in M$. Isto mostra que

$$ab \in M \Rightarrow a \in M \text{ ou } b \in M,$$

logo M é primo.

5*. *Seja A um anel com identidade no qual todo o elemento a satisfaz $a^2 = a$. Mostre que:*

(a) *$-a = a$, para todo o $a \in A$.*

(b) *A é comutativo.*

(c) *As seguintes condições são equivalentes, para qualquer ideal I de A não nulo:*

(i) *I é primo.* (ii) *$A/I \cong \mathbb{Z}_2$.* (iii) *I é maximal.*

Solução: (a) Provar que $-a = a$ para qualquer $a \in A$ equivale a provar que $a + a = 0$ para qualquer $a \in A$. Como, por hipótese, $(a + a)^2 = a + a$, e

$$\begin{aligned} (a+a)^2 = a + a \quad &\Leftrightarrow \quad a^2 + a^2 + a^2 + a^2 = a + a \\ &\Leftrightarrow \quad a + a + a + a = a + a \\ &\Leftrightarrow \quad a + a = 0, \end{aligned}$$

está provado.

Solução alternativa: Por hipótese, $(-a)^2 = -a$. Por outro lado, $(-a)(-a) = -(-a) = a$. Logo $-a = a$.

(b) Sejam $a, b \in A$. Por hipótese, $(a+b)^2 = a+b$. Além disso,

$$\begin{aligned} (a+b)^2 = a+b \quad &\Leftrightarrow \quad a^2+ab+ba+b^2 = a+b \\ &\Leftrightarrow \quad a+ab+ba+b = a+b \\ &\Leftrightarrow \quad ab+ba = 0. \end{aligned}$$

Portanto, $ab = -ba$. Logo, pela alínea anterior, $ab = ba$, o que mostra que A é comutativo.

(c) (i)$\Rightarrow$(ii): $A/I = \{a+I \mid a \in A\}$. Como I é primo, então $I \neq A$ pelo que $1 \notin I$ e, consequentemente, $1+I \neq 0+I$. Portanto A/I possui pelo menos as classes $0+I$ e $1+I$ e, se queremos mostrar que $A/I \cong \mathbb{Z}_2$, teremos então que mostrar que A/I não possui mais nenhum elemento. Se $a \in I$ então $a+I = 0+I$. Se $a \notin I$ então $a+I \neq 0+I$, pelo que teremos de mostrar neste caso que $a+I = 1+I$. Pela alínea (a), $a+a=0$, isto é, $a(a+1) = 0 \in I$. Logo, como I é primo, $a \in I$ ou $a+1 \in I$. A primeira condição é falsa pelo que necessariamente $a+1 \in I$, ou seja, $a+I = 1+I$ (note que $a-1 = a+1$, pela alínea (a)).

(ii)$\Rightarrow$(iii): A condição (ii) diz-nos, em particular, que A/I é um corpo, pelo que I é imediatamente maximal (resultado teórico das aulas).

(iii)$\Rightarrow$ (i): Resultado provado nas aulas que assegura que todo o ideal maximal é primo.

6*. *Seja $(A, +, \cdot)$ um anel comutativo. Considere o conjunto*

$$\mathcal{N}(A) = \{a \in A \mid \exists n \in \mathbb{N}, a^n = 0\}.$$

(a) *Calcule $\mathcal{N}(\mathbb{Z})$ e $\mathcal{N}(\mathbb{Z}_{16})$.*

(b) *Mostre que:*

 (i) *$\mathcal{N}(A)$ é um ideal de A.*

 (ii) *Para qualquer ideal primo I de A, $\mathcal{N}(A) \subseteq I$.*

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

Solução: (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)(i) 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 $k \geq m + n - 1$, $(a-b)^k = 0$.

(ii) Seja I um ideal primo de A. Se $a \in \mathcal{N}(A)$ então $a^n = 0$ para algum natural n. Mas $aa^{n-1} = a^n = 0 \in I$ 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.

(iii) $A/\mathcal{N}(A) = \{a + \mathcal{N}(A) \mid a \in A\}$ pelo que

$$\begin{aligned}
a + \mathcal{N}(A) \in \mathcal{N}(A/\mathcal{N}(A)) \quad &\Leftrightarrow \quad \exists n \in \mathbb{N} :\ (a + \mathcal{N}(A))^n = \mathcal{N}(A) \\
&\Leftrightarrow \quad \exists n \in \mathbb{N} :\ a^n + \mathcal{N}(A) = \mathcal{N}(A) \\
&\Leftrightarrow \quad \exists n \in \mathbb{N} :\ a^n \in \mathcal{N}(A) \\
&\Leftrightarrow \quad \exists n \in \mathbb{N},\, \exists m \in \mathbb{N} :\ (a^n)^m = 0 \\
&\Leftrightarrow \quad \exists n, m \in \mathbb{N} : a^{nm} = 0 \\
&\Leftrightarrow \quad a \in \mathcal{N}(A) \\
&\Leftrightarrow \quad a + \mathcal{N}(A) = \mathcal{N}(A).
\end{aligned}$$

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

7*. *Seja D um domínio de integridade e considere no conjunto $S = D \times (D \setminus \{0\})$ a relação*

$$(a, b) \sim (c, d) \equiv ad = bc.$$

(a) *Mostre que $\sim$ é uma relação de equivalência em S.*

(b) *Denote a classe de equivalência $\{(c, d) \in S \mid (c, d) \sim (a, b)\}$ por a/b (ou $\frac{a}{b}$) e o conjunto de todas as classes de equivalência $\{a/b \mid (a, b) \in S\}$ por K. Prove que*

$$a/b + c/d = (ad + bc)/bd \quad \text{ e } \quad a/b \cdot c/d = ac/bd$$

definem operações em K que lhe dão uma estrutura de corpo (o chamado corpo das fracções *ou* quocientes *de D).*

(c) *No caso $D = \mathbb{Z}$ que corpo é K ?*

(d) *Mostre que $D' = \{a/1 \mid a \in D\}$ é um subanel de K isomorfo a D e que para cada $x \in K$ existem $a, b \in D'$ com $b \neq 0$ tais que $x = ab^{-1}$.*

(e) *Seja D' um domínio de integridade contido num corpo L e*

$$K' = \{a'(b')^{-1} \mid a', b' \in D', b' \neq 0\}.$$

Prove que K' é o menor subcorpo de L que contém D' e qualquer isomorfismo de D em D' tem uma extensão única a um isomorfismo de K em K'.

(f) *Conclua que o corpo dos quocientes K de um domínio de integridade D é o menor corpo (a menos de isomorfismo) contendo D (no sentido de que não existe nenhum corpo L tal que $D \subset L \subset K$).*

Solução:

(a) As propriedades reflexiva e simétrica são imediatas. Suponhamos $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$. Então $ad = bc$ e $cf = de$. Isto implica $adf = bcf$ e $bcf = bde$ e portanto $adf = bde$. Cancelando d obtemos $af = be$, isto é, $(a, b) \sim (e, f)$. Assim, $\sim$ é transitiva.

(b) A operação $+$ está bem definida: sejam $a/b, c/d, a'/b', c'/f' \in K$ e suponhamos $a/b = a'/b'$ e $c/d = c'/d'$. Então $ab' = ba'$ e $cd' = dc'$, pelo que $ab'dd' = ba'dd'$ e $cd'bb' = dc'bb'$. Portanto $ab'dd' + cd'bb' = ba'dd' + dc'bb'$ e consequentemente $(ad + bc)b'd' = bd(a'd' + b'c')$. Isto significa que

$$(ad + bc, bd) \sim (a'd' + b'c', b'd')$$

donde $(ad + bc)/bd = (a'd' + b'c')/b'd'$.

Uma prova análoga mostra que $\cdot$ também está bem definida.

As propriedades associativa,comutativa e distributiva são simples de verificar. O elemento neutro de $+$ é $0/b$ e o elemento neutro de $\cdot$ é b/b (onde $b \neq 0$). Para cada $a/b \in K$, o respectivo simétrico é a fracção $(-a)/b = a/(-b)$ e o inverso, quando $a/b \neq 0$ (isto é, $a \neq 0$), é a fracção b/a. Portanto, K é um corpo.

(c) É evidente que o caso $D = \mathbb{Z}$ nos dá $K = \mathbb{Q}$. Assim, a construção de K a partir de D é uma generalização da construção clássica dos racionais como fracções de inteiros.

(d) O facto de que D' é um subanel de K é evidente: $0 = 0/1 \in D'$ e para quaisquer $a/1, b/1 \in D'$, $a/1 - b/1 = (a-b)/1 \in D'$ e $a/1 \cdot b/1 = ab/1 \in D'$.

Definindo $f : D \to D'$ por $f(a) = a/1$ para qualquer $a \in D$, temos

$$f(a+b) = (a+b)/1 = (a \cdot 1 + b \cdot 1)/1 \cdot 1 = a/1 + b/1 = f(a) + f(b)$$

e

$$f(ab) = ab/1 = a/1 \cdot b/1 = f(a) \cdot f(b).$$

Da definição de f, f é claramente sobrejectiva. Quanto à injectividade, basta observar que

$$a = b \Leftrightarrow a \cdot 1 = 1 \cdot b \Leftrightarrow a/1 = b/1 \Leftrightarrow f(a) = f(b).$$

Portanto, f é um isomorfismo de D em $D' \subseteq K$. O resto é óbvio: para cada $x = a/b \in K$, $b \neq 0$ (pelo que $b/1 \neq 0$) e

$$a/b = a/1 \cdot 1/b = a/1 \cdot (b/1)^{-1}.$$

(e) É fácil verificar que K' é um subcorpo de L. É óbvio que se trata então do menor subcorpo de L que contém D'. Seja f um isomorfismo de D em D' e $a/b \in K$. Consideremos a função $g : K \to K'$ definida por $g(a/b) = f(a)f(b)^{-1}$. Identificando o domínio D com o conjunto $\{a/1 \mid a \in D\}$, é claro que $f = g_{|D}$. Além disso,

$$a/b = c/d \Leftrightarrow ad = bc \Leftrightarrow f(ad) = f(bc) \Leftrightarrow f(a)f(d) = f(b)f(c) \Leftrightarrow$$

$$\Leftrightarrow f(a)f(b)^{-1} = f(c)f(d)^{-1} \Leftrightarrow g(a/b) = g(c/d).$$

Portanto, g é injectiva. Da definição de g, segue também que g é sobrejectiva. Além disso,

$$\begin{aligned} g(a/b + c/d) &= g((ad+bc)/bd) \\ &= f(ad+bc)(f(bd))^{-1} \\ &= [f(a)f(d) + f(b)f(c)][f(b)^{-1}f(d)^{-1}] \\ &= f(a)f(b)^{-1} + f(c)f(d)^{-1} \\ &= g(a/b) + g(c/d) \end{aligned}$$

e

$$\begin{aligned} g(a/b \cdot c/d) &= g(ac/bd) \\ &= f(ac)(f(bd))^{-1} \\ &= [f(a)f(c)][f(b)^{-1}f(d)^{-1}] \\ &= f(a)f(b)^{-1}f(c)f(d)^{-1} \\ &= g(a/b)g(c/d) \end{aligned}$$

para quaisquer $a/b, c/d \in K$. Logo, g é um isomorfismo.

Seja g' outro isomorfismo de K em K' tal que $f = g'_{|D}$. Então, para qualquer $a/b \in K$,

$$\begin{aligned} g'(a/b) &= g'(a/1 \cdot (b/1)^{-1}) \\ &= g'(a/1)g'((b/1)^{-1}) \\ &= g'(a/1)g'(b/1)^{-1} \\ &= f(a)f(b)^{-1} \\ &= g(a/b). \end{aligned}$$

(f) A conclusão é imediata da alínea anterior.