Anéis e Subanéis

Flávio Ulhoa Coelho

Vimos até agora uma série de conjuntos munidos de estruturas algébricas que, a despeito de diferenças óbvias e significativas, desfrutavam de similaridades. Uma característica comum a todos esses conjuntos era que, neles, estavam definidas duas operações, adição e multiplicação, satisfazendo certas propriedades básicas (associatividade; por vezes comutatividade; existência de elementos neutros, dentre outras).

Nosso próximo objetivo é nomear tais estruturas algébricas levando-se em conta o que elas têm em comum, ou dito de outra forma, os padrões compartilhados. Isso irá facilitar a compreensão dos conjuntos a partir das operações que possam ser ali definidas.

0.1 Definições e propriedades básicas

Definição 0.1 Um **anel** A é um conjunto não vazio munido de duas operações, adição ($+$) e multiplicação ($\cdot$), satisfazendo as seguintes propriedades:

(A1) (associatividade da adição) Para todos a, b, c em A, vale que $(a + b) + c \; = \; a + (b + c)$.

(A2) (comutatividade da adição) Para todos a, b em A, vale que $a + b \; = \; b + a$.

(A3) (existência de elemento neutro da adição) Existe um elemento em A, que denotaremos por 0, tal que para todo a em A, vale $a + 0 \; = \; 0 + a \; = \; a$.

(A4) (existência de elementos opostos) Para cada a em A, existe um elemento em A, que denotaremos por $-a$, tal que $a + (-a) \; = \; (-a) + a \; = \; 0$.

(M1) (associatividade da multiplição) Para todos a, b, c em A, vale que $(a \cdot b) \cdot c \; = \; a \cdot (b \cdot c)$.

(D) (distributividade) Para todos a, b, c em A, vale que $a \cdot (b + c) \; = \; a \cdot b + a \cdot c$ e que $(a + b) \cdot c \; = \; a \cdot c + b \cdot c$.

Observações 0.1 Seja A um anel. (1) O elemento que denotamos por 0 na propriedade (A3) é o único que satisfaz a propriedade requerida. De fato, se $b \in A$ for tal que $a + b = b + a = a$ para todo $a \in A$, seguirá que $0 + b = b$ e $0 + b = 0$. Logo $b = 0$. Devido a essa unicidade, chamamos esse elemento distinguido 0 de **zero de A**.

(2) O elemento que denotamos por $-a$ (na propriedade (A4)) é também único com relação a essa propriedade. De fato, se $b \in A$ for tal que $a + b = 0$, então somando-se $-a$ nos dois lados dessa expressão, teríamos

$$(-a) + (a + b) \ = \ (-a) + 0$$

de onde seguirá que

$$-a \ = \ -a + 0 \ = \ (-a) + (a + b) \ = \ ((-a) + a) + b \ = \ 0 + b \ = \ b \qquad (*)$$

e $-a$ é único elemento, dado a, sarisfazendo (A4) e, por isso, vamos chamar de **oposto de** a. Observe, também, que no cálculo $(*)$ utilizamos as propriedades (A1), (A3) e (A4).

Exemplo 0.1 Observe que os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$, $\mathbb{Z}_m$ ($m \in \mathbb{Z}$), $\mathbb{A}[t]$ (com $\mathbb{A} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$), $\mathbb{M}_n(\mathbb{A})$ (com $\mathbb{A} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$) discutidos nos capítulos anteriores são exemplos de anéis. Mas é fácil ver que eles também satisfazem propriedades adicionais, uns mais do que outros. Vamos especificar isso melhor, nomeando as diferenças e, também, ver novos exemplos.

Definição 0.2 Seja A um anel.

(a) Dizemos que A é um **anel comutativo** se, além das propriedades definidores de anel, A também satisfaz:
(M2) (comutatividade da multiplicação) Para todos a, b em A, vale que $a \cdot b \ = \ b \cdot a$.

(b) Dizemos que A é um **anel com unidade** se, além das propriedades definidores de anel, A também satisfaz:
(M3) (existência de elemento neutro da multiplicação) Existe um elemento em A, que denotaremos por 1, tal que para todo a em A, vale $a \cdot 1 \ = \ 1 \cdot a \ = \ a$.

Exemplo 0.2 (a) De todos os conjuntos listados no Exemplo 0.1, apenas $\mathbb{H}$ e os conjuntos de matrizes não são comutativos. Por outro lado, todos eles são exemplos de anéis com unidade.

(b) Vamos construir um anel sem unidade. Podemos começar nossa discussão olhando para o anel $\mathbb{Z}$. É claro que $\mathbb{Z}$ possui unidade 1. Nossa ideia é considerar um subconjunto de $\mathbb{Z}$ que não contenha o elemento 1 mas que ainda preservem as características de ser um anel: as duas operações e suas propriedades. Não basta, por isso, tirar apenas o elemento 1 de $\mathbb{Z}$ e considerar o conjunto $\tilde{\mathbb{Z}} = \mathbb{Z} \setminus \{1\}$, pois nesse caso a adição de $\mathbb{Z}$ não estaria bem definida nesse subconjunto (por exemplo, a soma de dois elementos $3, -2 \in \tilde{\mathbb{Z}}$ seria igual a um elmento que não pertence a $\tilde{\mathbb{Z}}$). É necessário retirar, além do 1, outros elementos que possam, ao somarmos, produzirem o 1. Uma ideia nessa direção poderia ser retirar todos os números ímpares e, portanto, considerarmos o conjunto

$$2\mathbb{Z} \ = \ \{\cdots, -4, \ -2, \ 0, \ 2, \ 4, \ 6, \cdots\}$$

formado pelos inteiros pares. De outra forma, $2\mathbb{Z} = \{a \in \mathbb{Z} : a = 2b \text{ para algum } b \in \mathbb{Z}\}$. Vamos mostrar que esse é um anel sem unidade.

Nossa primeira preocupação é saber se as operações de adição e multiplicação de $\mathbb{Z}$ estão bem definidas em $2\mathbb{Z}$ (no sentido de que a adição e a multiplicação de dois elementos de $2\mathbb{Z}$ estão também em $2\mathbb{Z}$; aliás, outra maneira de se dizer isso é dizer que o subconjunto $2\mathbb{Z}$ é fechado para somas e produtos de inteiros). De fato, dados $a, a' \in 2\mathbb{Z}$, então $a = 2b$ e $a' = 2b'$ para alguns $b, b' \in \mathbb{Z}$. Daí

$$a + a' = 2b + 2b' = 2(b + b') \in 2\mathbb{Z} \quad \text{e} \quad a \cdot a' = 2b \cdot 2b' = 2(2b \cdot b') \in 2\mathbb{Z}$$

e as operações de adição e multiplicação de $\mathbb{Z}$ estão bem definidas em $2\mathbb{Z}$.

Agora, se observarmos as propriedades que definem um anel, vemos que elas são de dois tipos: as de caráter geral em que uma determinada propriedade é descrita para todos os elementos do anel (por exemplo, associatividade, comutatividade, distributividade) e, por outro lado, as que determinam a existência de elementos com características próprias (o zero, o um, existência de opostos ou de inversos).

No caso de $\mathbb{Z}$ (levando-se em conta o fato de $\mathbb{Z}$ ser um anel comutativo com unidade) , as de primeiro tipo serão (A1), (A2), (M1), (M2) e (D) e, por conta de seu caráter geral, também valerão para os elementos de qualquer subconjunto de $\mathbb{Z}$. Tais propriedades, dizemos, são herdadas por $2\mathbb{Z}$ porque consideramos aqui as mesmas operações definidas para $\mathbb{Z}$.

Por outro lado, precisamos verificar as propriedades que estabelecam a existência de certos elementos para o subconjunto considerado. Por exemplo, o elemento neutro 0 pertence a $2\mathbb{Z}$ e, portanto, podemos concluir que a propriedade (A3) é válida para $2\mathbb{Z}$.

Para verificarmos (A4), seja $a \in 2\mathbb{Z}$, isto é, $a = 2b$ para algum $b \in \mathbb{Z}$. É fácil ver, então, que $-a = -2b = 2(-b) \in 2\mathbb{Z}$ o que nos garante a validade dessa propriedade. Com isso, mostramos que $2\mathbb{Z}$ é um anel comutativo. E quanto à unidade? Como $1 \notin 2\mathbb{Z}$, a unidade que serve ao conjunto $\mathbb{Z}$ não pertence a $2\mathbb{Z}$. Isso resolve parte dessa questão pois, em princípio, poderia haver algum outro elemento de $2\mathbb{Z}$ que cumprisse a propriedade (M3) nesse conjunto (mesmo sem cumprí-la em $\mathbb{Z}$). Aliás, veremos mais adiante um exemplo em que isso pode acontecer sob certas condições. No entanto, veremos que isso não ocorre nesse exemplo específico. De fato, suponha que exista um elemento $\overline{a} \in 2\mathbb{Z}$ tal que

$$\overline{a} \cdot b = b \quad \text{para todo} \quad b \in 2\mathbb{Z}$$

(é isso que requer a propriedade (M3)). Mas $\overline{a} \in 2\mathbb{Z}$ implica que $\overline{a} = 2c$ para algum $c \in \mathbb{Z}$. Por outro lado, como a relação $\overline{a} \cdot b = b$ tem que ser verdadeira para todo $b \in 2\mathbb{Z}$, ela o será por exemplo, para $b = 2$. Com isso, teremos

$$2 = \overline{a} \cdot 2 = 2 \cdot c \cdot 2 = 4 \cdot c$$

o que é uma contradição, pois 2 não é múltiplo de 4. Concluímos então que $2\mathbb{Z}$ é um anel sem unidade.

Uma observação antes de terminarmos esse exemplo. Não há nada de muito especial no número 2, poderíamos ter escolhido qualquer número m distinto de $-1, 0, 1$ que o conjunto $m\mathbb{Z}$ formado pelos múltiplos de m seria um anel (comutativo) sem unidade.

(c) Vamos considerar o seguinte conjunto de funções

$$\mathbb{F}([0,1], \mathbb{R}) \;=\; \{f\colon [0,1] \longrightarrow \mathbb{R}\}$$

munido das seguintes operações. Dados $f, g \in \mathbb{F}([0,1], \mathbb{R})$, definimos $f + g\colon [0,1] \longrightarrow \mathbb{R}$ e $f \cdot g\colon [0,1] \longrightarrow \mathbb{R}$ dados por $(f+g)(x) = f(x) + g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$, respectivamente. Deixamos ao leitor verificar as propriedades que fazem esse conjunto ser um anel comutativo com unidade.

Quando discutimos o conjunto dos inteiros $\mathbb{Z}$, observamos que, apesar de serem só dois os seus elementos com inversos (no caso, 1 e -1), esse conjunto satisfazia uma propriedade que se mostrou importante: *o produto de dois inteiros não nulos é um elemento não nulo.* Esse fato, por exemplo, foi essencial, para que mostrássemos a Lei do Cancelamento da Multiplicação para $\mathbb{Z}$. Com isso em mente, vamos fazer a próxima definição.

Definição 0.3 Seja A um anel.

(a) Dizemos que um elemento não nulo $a \in A$ é um **divisor de zero de** A se existir $b \in A$ também não nulo tal que ou $a \cdot b = 0$ ou $b \cdot a = 0$.

(b) Dizemos que A é um **domínio de integridade** se A for um anel comutativo com unidade e sem divisores de zero.

Observação 0.1 Observe que se $a \neq 0$ for um divisor de zero em um anel e se $b \neq 0$ for tal que $a \cdot b = 0$, não é sempre verdade que $b \cdot a = 0$ (há um exemplo de matrizes 2×2 no arquivo *Estruturas não comutativas* onde isso ocorre). É claro que, se A for comutativo, então isso valerá. A rigor, poderíamos usar uma terminologia como *divisor de zero à direita* ou *à esquerda* dependendo de qual produto daria zero, mas não entraremos em tais nuances. A definição acima será suficiente para o que propomos.

É claro que $\mathbb{Z}$ é um domínio de integridade. Outros exemplos incluem os conjuntos de polinômios estudados. Por outro lado, vimos que conjuntos como $\mathbb{Z}_m$ (com m não primo) ou conjuntos de matrizes quadradas possuem elementos divisores de zero e portanto não serão domínios. O conjunto $\mathbb{Z}_4$, por exemplo, é um anel comutativo com unidade mas com divisores de zero (por exemplo, $\overline{2}$). Vimos também que o conjunto de matrizes $n \times n$ (com $n \geq 2$) possui divisores de zero.

Para referência futura, vamos enunciar as Leis do Cancelamento e deixar o detalhamento das demonstrações aos leitores (compare com o que fizemos para $\mathbb{Z}$).

Proposição 0.1 Sejam A um anel e $a, b, c \in A$.

(LCA) Se $a + b = a + c$, então $b = c$.

(LCM) Assuma que A não tenha divisores de zero e que $a \neq 0$. Se $a \cdot b = a \cdot c$, então $b = c$ e se $b \cdot a = c \cdot a$, então $b = c$.

Vamos terminar nossa discussão inicial nomeando conjuntos que têm a propriedade de que todo elemento não nulo possui inverso. É o caso dos conjuntos $\mathbb{Q}\,, \mathbb{R}\,, \mathbb{C}\,, \mathbb{Z}_p$ (com p primo) ou $\mathbb{H}$.

Definição 0.4 Sejam A um anel com unidade e $a \in A$ não nulo.

(a) Dizemos que a é **invertível** se existir um elemento $a^{-1} \in A$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

(b) A é chamado de **anel com divisão** se
(M4) todo elemento não nulo de A for invertível.

(c) A é chamado de **corpo** se for comutativo e valer
(M4) todo elemento não nulo de A for invertível.

Pelo que vimos até agora, os conjuntos $\mathbb{Q}\,, \mathbb{R}\,, \mathbb{C}\,, \mathbb{Z}_p$ (com p primo) são exemplos de corpos enquanto que $\mathbb{H}$ é um anel com divisão (não comutativo). Iremos voltar à questão do estudo de elementos invertíveis em um outro texto. Mas antes, vamos estudar dois tipos de subestruturas de anéis, os subanéis e os ideais.

Exercício 0.1 Prove que se $(A, +, \cdot)$ é um anel qualquer e se $a, b, c \in A$, então as seguintes propriedades são válidas
(a) $0 \cdot a = a \cdot 0 = 0$. (b) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$.
(c) $(-a) \cdot (-b) = a \cdot b$ (d) $a \cdot (b - c) = a \cdot b - a \cdot c$.
(e) $(b - c) \cdot a = b \cdot a - c \cdot a$.
Se A tiver elemento neutro da multiplicação 1, mostre que
(f) $(-1) \cdot a = -a$ (g) $(-1) \cdot (-1) = 1$ (h) $(-1) \cdot (-a) = a$.

Exercício 0.2 Exiba um anel não comutativo e sem unidade.

Exercício 0.3 Seja $A \subset \mathbb{Z}$ um subconjunto de $\mathbb{Z}$ que tenha a estrutura de anel com relação às operações de adição e multiplicação de $\mathbb{Z}$. Mostre que existe $m \in \mathbb{Z}$ tal que $A = m\mathbb{Z}$. Mostre também que, se $1 \in A$, então $A = \mathbb{Z}$.

Exercício 0.4 Mostre a Proposição 0.1.

Exercício 0.5 Mostre que o anel $\mathbb{F}\,([0, 1], \mathbb{R}\,)$ definido no Exemplo 0.2 (c) possui divisores de zero.

Exercício 0.6 Calcule os divisores de zero dos aneis: $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$ e $\mathbb{Z}_{24}$.

Exercício 0.7 Considere o anel $\mathbb{Z}_m$ e seja a com $0 \leq a < m$. Mostre que $\overline{a} \in \mathbb{Z}_m$ é um divisor de zero se e somente se $\mathrm{mdc}(a, m) \neq 1$

Exercício 0.8 Seja D um domínio de integridade finito e seja $a \in D$, $a \neq 0$.

(a) Mostre que se $ax = ay$ então $x = y$.

(b) Mostre que D é um corpo.

Exercício 0.9 Considere o conjunto $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}$ com operações:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

(a) Mostre que $\mathbb{Q}[\sqrt{2}]$ é um anel comutativo com unidade.

(b) Encontre o elemento inverso de um elemento não nulo $a + b\sqrt{2}$ de $\mathbb{Q}[\sqrt{2}]$. Conclua que $\mathbb{Q}[\sqrt{2}]$ é um corpo.

0.2 Subanéis

Ao longo desse texto, temos visto exemplos de anéis que contém subconjuntos que são eles próprios anéis se considerarmos as mesmas operações do conjunto maior restritas ao menor. É o caso dos anéis nas inclusões (de conjuntos) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ por exemplo, ou mesmo nas inclusões $\mathbb{Z}[t] \subset \mathbb{Q}[t] \subset \mathbb{R}[t] \subset \mathbb{C}[t]$. Isso ocorre mesmo que nem todas as propriedades de um anel se mantenham em algum subconjunto: por exemplo, $\mathbb{Q}$ satisfaz a propriedade de existência de inversos para todos os seus elementos não nulos, mas $\mathbb{Z}$ (anel contido em $\mathbb{Q}$) não a satisfaz.

Vamos formalizar melhor esse tipo de relações.

Definição 0.5 Sejam A um anel e $B \subset A$ um subconjunto não vazio de A. Dizemos que B é um **subanel de** A se for ele mesmo um anel se considerarmos as mesmas operações de A em B.

Exemplo 0.3 (a) Como já mencionado acima, as inclusões

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \quad \text{e} \quad \mathbb{Z}[t] \subset \mathbb{Q}[t] \subset \mathbb{R}[t] \subset \mathbb{C}[t]$$

definem *torres de subanéis.*

(b) O conjunto $2\mathbb{Z}$ construído no Exemplo 0.2 (b) é um exemplo de subanel de $\mathbb{Z}$.

(c) Considere o conjunto

$$\mathbf{Cont}([0,1], \mathbb{R}) = \{f \colon [0,1] \longrightarrow \mathbb{R} \text{ contínua}\}$$

das funções contínuas de $[0,1]$ em $\mathbb{R}$. É claro que esse conjunto está contido em $\mathbb{F}([0,1],\mathbb{R})$ e se considerarmos as mesmas operações do conjunto maior, podemos ver que $\mathbf{Cont}([0,1],\mathbb{R})$ é também um anel. Logo, será um subanel de $\mathbb{F}([0,1],\mathbb{R})$. Observe que a soma e o produto de funções contínuas são também contínuas (isso é essencial para que as operações de $\mathbb{F}([0,1],\mathbb{R})$ estejam bem definidas em $\mathbf{Cont}([0,1],\mathbb{R})$).

Ao construírmos, no Exemplo 0.2(b) um anel sem unidade, vimos que certas propriedades operatórias de um anel A são naturalmente herdadas por qualquer subconjunto B de A se utilizarmos as mesmas operações nesses conjuntos. O próximo lema formaliza essa observação.

Lema 0.1 Sejam A um anel com operações $+, \cdot$ e $B \subset A$ um subconjunto de A tal que se $b, b' \in B$, então tanto $b + b'$ quanto $b \cdot b'$ também pertencem a B. Então as propriedades listadas como (A1), (A2), (M1) e (D) na definição de anel também estão satisfeitas em B se levarmos em conta essas mesmas operações. Além disso, se A for comutativo, então a propriedade (M2) também será válida em B.

DEMONSTRAÇÃO. Deixado como exercício. $\mathbf{\Lambda}$

Decorre desse lema que, para se verificar se um subconjunto B de um anel A é um subanel, devemos nos concentrar em dois pontos: (i) que as operações de A estejamo definidas em B, isto é, que dados $b, b' \in B$, então tanto $b + b'$ quanto $b \cdot b'$ também pertençam a B (dizemos, nesse caso, que esse subconjunto está fechado para essas operações); e (ii) nas propriedades que envolvam existência, isto é, nas propriedades (A3) e (A4) (no caso de anel), pois os elementos que sabemos existir em A podem não estar no subconjunto B.

O seguinte resultado nos dá então um critério para quando um subconjunto de um anel é um subanel.

Proposição 0.2 Sejam A um anel com operações $+, \cdot$ e $B \subset A$ um subconjunto não vazio de A. Então B é um subanel de A se as seguintes propriedades são válidas:

(a) Dados $b, b' \in B$, então $b + b' \in B$.

(b) Dados $b, b' \in B$, então $b \cdot b' \in B$.

(a) Dado $b \in B$, então $-b \in B$.

DEMONSTRAÇÃO.
Os itens (a) e (b) do enunciado garantem que o subconjunto B é fechado para as operações de adição e multiplicação definidas em A. Usando-se Lema 0.1, já temos então garantida a validade das propriedades (A1), (A2), (M1) e (D) faltando portanto verificarmos (A3) e (A4). Observe que o item (c) do enunciado garante exatamente a validade de (A4). Agora, como B é não vazio,

segue que ele possui um elemento b. Por (c), temos que $-b \in B$. Agora, usando-se o item (a) (com $b' = -b$), teremos

$$0 \; = \; b + (-b) \in B$$

e a propriedade (A3) é assim verificada. Logo B é um subanel de A. Λ

Terminamos essa seção com um exemplo.

Exemplo 0.4 Considere o seguinte subconjunto B do anel $A = \mathbb{M}_2(\mathbb{R})$:

$$B \; = \; \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$$

É claro que $B \subset A$. Vamos mostrar que B é um subanel de A e, para tal, utilizaremos a Proposição 0.2. Dadas duas matrizes $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a' & 0 \\ 0 & 0 \end{pmatrix} \in B$, é fácil ver que

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a' & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a + a' & 0 \\ 0 & 0 \end{pmatrix} \in B \quad \text{e} \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a' & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a \cdot a' & 0 \\ 0 & 0 \end{pmatrix} \in B$$

e, com isso, B é fechado para as operações de adição e multiplicação de A. Para o item (c), basta obaservar que, dada $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in B$,

$$-\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \; = \; \begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix} \in B.$$

Logo, B é um subanel de A.

Antes de prosseguirmos, gostaríamos de fazer um comentário. Sabemos que $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é a unidade do anel $\mathbb{M}_2(\mathbb{R})$. No entanto, esse elemento não pertence a B. Isso significa que B não tem unidade?

Observe, no entanto, que o elemento $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in B$ é tal que para todo $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in B$, temos

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \; = \; \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \; = \; \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

ou, em outras palavras, $1_B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in B$ é a unidade no (sub)anel B. Em outras palavras, tanto A quanto B possuem unidades, mas elas diferem como elementos.

Esse último exemplo mostra-nos que um subanel pode ter uma unidade distinta da do anel em que está contido. Isso, no entanto, não irá ocorrer sempre. O Exercício 0.16 abaixo nos diz que se A for um anel com unidade e sem divisores de zero e se B for um subanel de A com unidade, então essas unidades devem coincidir.

Exercício 0.10 Mostre o Lema 0.1.

Exercício 0.11 Calcule todos os subanéis de $\mathbb{Z}_{12}$ e de $\mathbb{Z}_7$.

Exercício 0.12 Mostre que a intersecção de subanéis de um anel é também um subanel. Vale que a união de subanéis é também um subanel?

Exercício 0.13 Sejam A um anel e $a \in A$. Mostre que os conjuntos $\{x \in A \colon xa = 0\}$ e $\{x \in A \colon xa = ax\}$ são subanéis de A.

Exercício 0.14 Seja A um anel.

(a) Mostre que $Z(A) = \{x \in A \colon xy = yx, \text{ para todo } y \in A\}$ é um subanel de A ($Z(A)$ é chamado de **centro de** A).

(b) Mostre que se A for um anel com divisão (isto é, um anel com unidade e tal que todo elemento não nulo é invertível), então $Z(A)$ é um corpo.

(c) Mostre que o centro do anel dos quatérnios é $\mathbb{R}$.

Exercício 0.15 Considere o anel $A = \mathbb{M}_2(\mathbb{R})$ e seu subanel $B = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$. Mostre que B é um corpo (e portanto tem uma estrutura algébrica mais restritiva do que A, que não é comutativo e possui elementos não nulos não invertíveis).

Exercício 0.16 Sejam A um anel com unidade 1_A e sem divisores de zero e $B \subset A$ um subanel de A com unidade 1_B. Mostre que $1_A = 1_B$.