

1 Anéis

Esta semana discutiremos o conceito de anéis. Eles são fundamentais em diversas áreas da matemática, e também são o primeiro passo para entendermos a tecnologia que permite classificar grupos (abelianos) de ordem infinita.

Definição 1. Um **anel** é um conjunto R munido de duas operações $+$ e $\cdot$, que satisfaz as seguintes propriedades:

- 1) $(R, +)$ é um grupo abeliano.
- 2) Vale a associatividade para a multiplicação:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

- 3) Vale a distributividade com respeito a soma:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Se, além disso, valerem as seguintes propriedades:

- 4) $a \cdot b = b \cdot a$, para todo $a, b \in R$, diremos que R é **comutativo**.
- 4) Se existir $1 \in R$, talque $1 \cdot a = a \cdot 1 = a$, para todo $a \in R$, diremos que R é **anel com identidade**.

Omitiremos frequentemente a notação " $\cdot$ " para denotar a multiplicação em um anel. Isto é, escreveremos ab para denotar $a \cdot b$. Quando quisermos enfatizar as operações do anel R , escreveremos o anel como $(R, +, \cdot)$.

Exemplo 1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ com a soma e produto usuais são exemplos de anéis comutativos com identidade.

Exemplo 2. O conjunto dos restos módulo n , $\mathbb{Z}_n$, com a soma e produto usuais é um anel comutativo com identidade.

Exemplo 3. O conjunto das matrizes de ordem n sobre com coeficientes em um anel comutativo R , denotado por $M(n, R)$ é um anel com identidade, quando consideramos a soma e produto usual de matrizes, mas não é comutativo.

Exemplo 4. Seja R um anel comutativo com identidade. O conjunto dos polinômios com coeficientes em R , dado por:

$$R[x] := \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n; a_i \in R\},$$

com a soma e produto usual de polinômios é um anel comutativo com identidade.

Exemplo 5. O conjunto dado por:

$$\mathbb{Z}[i] := \{a + bi; a, b \in \mathbb{Z}\},$$

é um anel, conhecido como **anel dos inteiros de Gauss**.

Definição 2. Seja $(R, +, \cdot)$ um anel. $a \in R$ é dito **divisor de zero à esquerda**, se $a \neq 0$ e existe $b \in R$ tal que $ab = 0$. Analogamente definimos divisores de zero a direita. $a \in R$ é dito **invertível à esquerda**, ou se $a \neq 0$ e existe $b \in R$ tal que $ba = 1$. Analogamente definimos invertíveis à direita. Um elemento que é invertível a esquerda e a direita é dito **unidade** do anel R . O conjunto de todas as unidades de R é denotado por R^* .

Exemplo 6. O elemento $A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, é um divisor de zero à esquerda em $M(2, \mathbb{Z})$.

Definição 3. Um **domínio**, ou **domínio de integridade** ou ainda **anel de integridade** é um anel comutativo com identidade e sem divisores de zero. Um anel R é dito **anel de divisão**, se $(R \setminus \{0\}, \cdot)$ for um grupo. Um **corpo** é um anel de divisão comutativo.

Exemplo 7. $\mathbb{Z}$ é um domínio, mas não é corpo. $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.

O próximo teorema é de fácil verificação.

Teorema 1. *Seja $(R, +, \cdot)$ um anel. Então valem as seguintes propriedades:*

1. *Se R é anel com identidade então 1 é único.*
2. *Se R tem mais de um elemento, e R possui identidade então $1 \neq 0$.*
3. *Se R é um anel que vale a lei do cancelamento a esquerda, então R não tem divisores de zero a esquerda. Analogamente para divisores de zero a direita.*

Podemos agora definir os homomorfismos de anéis, que são funções entre anéis que preservam sua estrutura.

Definição 4. Sejam $(R, +_R, \cdot_R), (S, +_S, \cdot_S)$ anéis e $f : R \rightarrow S$ uma função. Diremos que f é um **homomorfismo de anéis**, se f satisfizer:

- 1) $f(a +_R b) = f(a) +_S f(b), \forall a, b \in R.$
- 2) $f(a \cdot_R b) = f(a) \cdot_S f(b), \forall a, b \in R.$

Monomorfismos, epimorfismos e automorfismos são definidos de maneira análoga a de grupos. Alguns autores chamam um monomorfismo $R \rightarrow S$ de **mergulho**.

Exemplo 8. Seja $f : \mathbb{Z} \rightarrow M(2, \mathbb{Z})$ dada por $f(a) = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, é um mergulho.

Exemplo 9. Seja $f : \mathbb{Z} \rightarrow \mathbb{Z}_m$ dada por $f(a) = \bar{a}$, é um epimorfismo.

As seguintes propriedades são fácil verificação.

Teorema 2. *Seja $f : R \rightarrow S$ um homomorfismo de anéis. Então temos:*

- a) $f(0_R) = 0_S$
- b) $f(-a) = -f(a)$

c) Se R tem identidade, então $f(1_R) = -f(1_S)$.

d) Se a é uma unidade de R então $f(a^{-1}) = f(a)^{-1}$.

Analogamente ao caso do kernel de homomorfismos de grupos, se $f : R \rightarrow S$ é um homomorfismo de anéis, dizemos que o conjunto $\ker f := \{a \in R; f(a) = 0_S\}$ é dito kernel (ou núcleo) de f .

Análogo ao estudo de subgrupos e subgrupos normais, veremos a seguir o conceito de subanel e de ideal de um dado anel.

Definição 5. Sejam R um anel, $S \subset R$ um subconjunto de R . Diremos que S é **subanel** de R se S for um anel com as operações induzidas de R e também for fechado para as operações de soma e produto de R .

Definição 6. Sejam R um anel, $S \subset R$ um subconjunto de R . Diremos que S é **ideal à esquerda** de R , denotado por $S \triangleleft_e R$ se S for um subanel, e além disso, para todo $r \in R$ e todo $s \in S$ temos $rs \in S$. Analogamente, S será ideal à direita se S for subanel e $sr \in S$ para todo $r \in R$ e todo $s \in S$. I é dito **ideal bilateral**, ou simplesmente ideal de R se I for um ideal a esquerda e a direita.

Exemplo 10. É fácil ver 0 e R são ideais de R . 0 é dito **ideal trivial** de R .

Exemplo 11. É fácil ver que para todo $n \in \mathbb{Z}$, o grupo cíclico $\langle n \rangle$ é um ideal de $\mathbb{Z}$.

Exemplo 12. Não é difícil ver que para todo se $f : R \rightarrow S$ é um homomorfismo de anéis, então $\ker f$ é um ideal de R . Podemos ver que $\text{Im} f$ é um subanel de S .

Exemplo 13. Note que $\mathbb{Z} \subset \mathbb{Q}$ é um subanel, mas não um ideal.

Exemplo 14. Sejam R um anel, e considere o conjunto $Z(R) := \{a \in R; ax = xa \forall x \in R\}$, dito centro de R . É fácil ver que o centro sempre é um subanel de R , mas podemos construir exemplos onde $Z(R)$ não é ideal.

A seguinte caracterização de ideal será muito importante no que se segue. Sua verificação é imediata.

Teorema 3. *Seja R um anel, e $I \subset R$ um subconjunto. Então I é um ideal de R se, e somente se, satisfaz as seguintes propriedades:*

1. *Para todos $a, b \in I$, tem-se que $a - b \in I$.*
2. *Para todo $a \in I$ e $r \in R$, tem-se que $ra \in I$.*

Para tornar o estudo de anéis e ideais mais concretos, muitas vezes recorreremos ao conceito de conjunto gerador de um anel. Para defini-lo, precisamos do seguinte lema técnico:

Lema 1. *Seja R um anel, e I_λ , uma família de ideais indexada por um conjunto Λ qualquer. Então $\bigcap_{\lambda \in \Lambda} I_\lambda$ é um ideal à esquerda.*

Definição 7. *Seja R um anel e X um subconjunto de R . O ideal gerado por X é o ideal dado pela intersecção de todos os ideais que contém X , e denotado por (X) . Os elementos de X são ditos os **geradores** do ideal (X) . Se um ideal I de R puder ser gerado por um número finito de elementos $\{a_1, \dots, a_n\}$ diremos que I é **finitamente gerado**, e escrevemos $I = (a_1, \dots, a_n)$. Se $I \triangleleft R$ puder ser gerado por um único elemento a , diremos que $I = (a)$ é um **ideal principal**. Um anel A onde TODOS os ideais são principais é dito **anel de ideais principais**. Se ademais A for domínio diremos que A é **domínio de ideais principais**.*

Voltaremos mais tarde nesse curso ao estudo desses anéis.

Ideais desempenham um papel semelhante ao de subgrupos normais em grupos. Com eles podemos definir a noção de anel quociente. De fato sejam R um anel, e I um ideal. Como $(R, +)$ é um grupo abeliano, e I é um subgrupo e portanto normal, segue que R/I é um grupo abeliano. O que podemos provar é que de fato R/I é um anel, dito **anel quociente** de R por I .

Teorema 4. *Sejam R um anel e I um ideal (bilateral). Então R/I definido acima é um anel.*

Demonstração. De fato, temos que $(R/I, +)$ é um grupo abeliano. Falta provar que a operação do produto induzida pelo produto de R é bem definida, uma vez que como elas verificam as propriedades de distributividade e associatividade para R , também vão verificar para R/I . Sendo assim, suponha que $a_1 + I = a_2 + I$ e que $b_1 + I = b_2 + I$, temos que mostrar que $a_1a_2 + I = b_1b_2 + I$. De fato, como $a_1 + I = a_2 + I$ segue que $a_1 \in a_2 + I$ e assim, existe $i \in I$ tal que $a_1 = a_2 + i$. Analogamente, existe $j \in I$ tal que $b_1 = b_2 + j$. Assim, $a_1b_1 = a_2b_2 + a_2j + ib_2 + ij$. Assim, $a_1b_1 - a_2b_2 = a_2j + ib_2 + ij$. Como I é ideal segue que $a_2j + ib_2 + ij \in I$, e portanto $a_1b_1 - a_2b_2 \in I$, de onde segue que $a_1b_1 + I = a_2b_2 + I$. Logo a operação de multiplicação está bem definida. $\square$

Não será surpresa para nenhum leitor que os teoremas de isomorfismos que demonstramos para grupos, também valem para anéis. Temos claro que tomar cuidado com a operação de multiplicação, mas é possível mostrar que tudo se encaixa bem. De fato temos os seguintes;

Teorema 5 (Primeiro Teorema do isomorfismo). *Seja $f : R \rightarrow S$ um homomorfismo de anéis. Então existe um isomorfismo entre $R/\ker f$ e $\text{Im} f$.*

Teorema 6 (Segundo Teorema do isomorfismo). *Sejam R um anel e I, J ideais de R . Então existe um isomorfismo entre $I/I \cap J$ e $I + J/J$.*

Teorema 7 (Terceiro Teorema do isomorfismo). *Sejam R um anel e I, J ideais de R tais que $I \subset J$. Então J/I é um ideal de R/I e existe um isomorfismo entre $(R/I)/(J/I)$ e R/J .*

Por fim, também temos o Teorema da correspondência.

Teorema 8 (Terceiro da correspondência). *Sejam R um anel e I um ideal de R . Então existe uma correspondência biunívoca entre ideais de R/I e ideais de R que contém I .*

A seguir, estudaremos dois tipos especiais de ideais, que são importantes no estudo das estruturas dos anéis: Ideais primos e maximais.

Definição 8. Sejam R um anel e I um ideal. Diremos que I é um **ideal primo**, se $I \neq R$ para todos $J, K \subset R$ com $JK \subset I$, temos que $J \subset I$ ou $K \subset I$.

A seguinte caracterização é de fácil verificação e muito útil.

Teorema 9. *Sejam R um anel e I um ideal tal que $I \neq R$. Se para quaisquer $a, b \in R$ tal que $ab \in I$ temos que $a \in I$ ou $b \in I$, então I é primo. Ademais, se R é comutativo vale a recíproca. Isto é, se I é primo então para quaisquer $a, b \in R$ tal que $ab \in I$ temos que $a \in I$ ou $b \in I$,*

Exemplo 15. Se R é um domínio, então o ideal gerado por (0) é um domínio.

Exemplo 16. Os únicos ideais de um corpo F são o 0 e o próprio F .

O seguinte teorema nos ajuda a encontrar muitos exemplos de ideais primos.

Teorema 10. *Seja R um anel comutativo com identidade, então um ideal $I \triangleleft R$ é primo se, e somente se R/I é domínio.*

Demonstração. Suponha que $I \triangleleft R$ é primo, e sejam $a + I, b + I \in R/I$ tais que $(a + I)(b + I) = \bar{0} = I$. Assim $ab + I = I$, e portanto $ab \in I$. Assim como I é primo, segue que $a \in I$ ou $b \in I$. Portanto $a + I = I$ ou $b + I = I$, logo R/I é domínio. Por outro lado suponha que R/I seja domínio. Sejam $a, b \in I$ tais que $ab \in I$. Assim $ab + I = I$ e portanto $(a + I)(b + I) = I$ e assim $a + I = I$ ou $b + I = I$, isto é $a \in I$ ou $b \in I$. $\square$

Definição 9. Seja R um anel. Um ideal I é dito maximal se $I \neq R$ e se para todo ideal J de R tal que $I \subset J$, então $J = I$ ou $J = R$.

Exemplo 17. Os ideais $\langle p \rangle \subset \mathbb{Z}$ são maximais em $\mathbb{Z}$.

Exemplo 18. Os ideais $M(2, \langle p \rangle)$ são maximais em $M(2, \mathbb{Z})$. Sempre que p for um número primo.

Provaremos o seguinte resultado.

Teorema 11. *Sejam R um anel e M um ideal. São equivalentes:*

1) M é maximal.

2) R/M não possui ideais bilaterais não triviais.

3) Para todo $x \in R \setminus M$, temos que $(x) + M = R$.

Demonstração. 1) $\implies$ 2). Seja I/M um ideal de R/M . Pelo Teorema da correspondência temos que $M \subset I$. Por definição de ideal maximal temos $R = I$ ou $M = I$. Assim I/M é trivial.

2) $\implies$ 3). Para todo $x \in R \setminus M$, temos que $I = (x) + M$ é ideal de R que contém M e é diferente de M . Assim, I/M ideal não nulo de R/M , pois $x \notin M$ e $x \in I$. Assim por 2) segue que $R/M = (x) + M/M$, e portanto $R = (x) + M$.

3) $\implies$ 1). Seja I um ideal tal que $M \subset I$. Suponha $x \in I \setminus M$. Temos como $(x) \subset I$ e também $M \subset I$ temos $(x) + M \subset I$, mas por 3) temos que $(x) + M = R$, e portanto $R = I$, e então M é maximal. $\square$

De posse desse Teorema, podemos provar seguinte resultado que usaremos extensivamente no futuro.

Corolário 1. *Seja R um anel comutativo com identidade. Então um ideal M é maximal se, e somente se R/M é corpo.*

Demonstração. Se R/M é corpo seus únicos ideais são 0 e R/M , segue que M é maximal da equivalência com o item 2) do teorema anterior.

Suponha que M seja maximal. E considere $a + M \in R/M$. Queremos provar que $a + M$ admite inverso. Como $a \notin M$ temos pelo item 3) do teorema anterior que $(a) + M = R$. Assim, existem $b \in R$ e $m \in M$ tal que $1 = ba + m$, o que implica que $1 - ba \in M$, e logo $1 + M = ba + M$ e portanto $1 = (b + M)(a + M)$. Como queríamos. $\square$

Análogo a definição de grupos podemos definir anéis simples.

Definição 10. Um anel R é dito **simples** se não possui nenhum ideal bilateral não-trivial.

Qualquer anel de divisão é simples.

O seguinte resultado é importante no estudo de anéis não comutativos. Deixaremos a demonstração (que não é fácil) como exercício ao leitor.

Teorema 12. *Sejam R um anel e $n > 1$ um inteiro. Então os ideais de $M(n, R)$ são da forma $M(n, I)$ com I ideal de R .*

Esse resultado tem como corolário imediato o seguinte importante teorema.

Teorema 13. *Sejam R um anel e $n > 1$ um inteiro. Se R é simples então $M(n, R)$ é simples.*

2 Exercícios

1. Mostre que os conjuntos dados nos exemplos 1-5 são de fato anéis.
2. Mostre que $\mathbb{Z}_n$ é corpo se, e somente se n é primo.
3. Dê exemplo de um anel de divisão que não seja corpo.
4. Mostre que a hipótese de R possuir identidade no Teorema 2-d) é indispensável. Isto é, prove que existe um homomorfismo de anéis $f : R \rightarrow S$ tal que $f(1_R) = 1_S$.
5. Seja F um corpo. Prove que $Z(M(2, F)) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in F \right\}$ e conclua que $Z(M(2, F))$ não é ideal de $M(2, F)$.
6. Seja R um anel com identidade e I um ideal. Mostre que se $1 \in I$, então $I = R$.
7. Mostre que se $I \subset \mathbb{Z}$ é um ideal maximal então $I = \langle p \rangle$ para algum primo p .
8. Sejam R um anel e $n > 1$ um inteiro. Prove que os ideais de $M(n, R)$ são da forma $M(n, I)$ com I ideal de R .

9. Sejam R um anel e F um corpo. Prove que $f : R \rightarrow F$ é um homomorfismo de anéis, então f é monomorfismo.