Breve referência à Teoria de Anéis

Anéis

Há muitos conjuntos, como é o caso dos inteiros, dos inteiros módulo n ou dos números reais, que consideramos naturalmente munidos de duas operações.

Definição (Anel)

Um anel *A é um conjunto não vazio com duas operações binárias, normalmente designadas por adição e multiplicação e denotadas respectivamente por $+$ e $\cdot$ (ou simplesmente por justaposição) tais que, para quaisquer $a, b, c \in A$:*

1. $a + b = b + a$;
2. $(a + b) + c = a + (b + c)$;
3. *existe um elemento* $0 \in A$ *(dito o* zero *do anel) tal que, para qualquer* $a \in A$, $a + 0 = a$;
4. *existe* $-a \in A$ *tal que* $a + (-a) = 0$;
5. $a(bc) = (ab)c$;
6. $a(b + c) = ab + ac$ *e* $(b + c)a = ba + ca$.

Temos então que um anel é um grupo abeliano com a adição e tem uma multiplicação associativa, a qual é distributiva à esquerda e à direita em relação à adição.

Um anel diz-se *comutativo* se a multiplicação for comutativa.
Se um anel tiver um elemento neutro para a multiplicação, este diz-se o *elemento identidade* (ou o *elemento um*) do anel.
Um elemento não nulo de um anel diz-se *invertível* se tiver inverso multiplicativo.

Exemplo

O conjunto $\mathbb{Z}$ dos inteiros com a adição e multiplicação usuais é um anel comutativo com elemento identidade 1. O conjunto dos elementos invertíveis é $\{1, -1\}$.

Exemplo

O conjunto $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ com a adição e multiplicação módulo n é um anel comutativo com elemento identidade 1. O conjunto dos elementos invertíveis é $U(n)$, o conjunto dos elementos que são primos com n.

Exemplo

O conjunto $2\mathbb{Z}$ dos inteiros pares com a adição e multiplicação usuais é um anel comutativo sem elemento identidade.

Exemplo

Se A e B são anéis, podemos construir o produto directo:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

com as operações componente a componente, isto é,

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

e

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2).$$

Usamos a notação $a - b$ com o significado de $a + (-b)$.

Proposição

Sejam a, b e c elementos de um anel A. Então

1. $a0 = 0a = 0$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$;
4. $a(b-c) = ab - ac$ *e* $(b-c)a = ba - ca$.
   Se A tiver elemento identidade 1, *então*
5. $(-1)a = -a$;
6. $(-1)(-1) = 1$.

Demonstração. 1. Tem-se $0 + a0 = a0 = a(0+0) = a0 + a0$, donde resulta $0 = a0$.
2. Tem-se $a(-b) + ab = a(-b+b) = a0 = 0$, donde resulta $a(-b) = -(ab)$.
Complete a demonstração como exercício. □

Proposição

Se um anel tem elemento identidade, este é único.
Se um elemento de um anel tem um inverso multiplicativo, este é único.

Demonstração. Exercício... (A demonstração é semelhante à de resultados análogos vistos para grupos.) □

Mais um exemplo de anel:

Exemplo

O conjunto

$$M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$$

das matrizes 2×2 com entradas em $\mathbb{Z}$ é um anel com a adição e multiplicação usuais de matrizes. Tem elemento identidade: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Definição (Subanel)

Um subconjunto B de um anel A é um subanel de A se B for um anel com as operações de A.

Proposição (Teste de subanel)

Um subconjunto não vazio B de um anel A é um subanel se for fechado para subtracção e multiplicação, isto é, se $a - b$ e ab pertencem a B, sempre que a e b pertencem a B.

Demonstração. Que B com a adição é um grupo abeliano resulta imediatamente do facto de a adição ser comutativa e de um critério de um dos critérios de subgrupo dados. Como, em A, a multiplicação é associativa e distributiva em relação à adição, tem-se o mesmo considerando a multiplicação e B. Resta ver que a multiplicação é uma operação binária em B, mas isso é dito no enunciado. □

Exemplo

Se A é um anel, $\{0\}$ é um subanel, dito o subanel *trivial* de A. Também A é um subanel de A.

Exemplo

$\{0, 2, 4\}$ é um subanel do anel $\mathbb{Z}_6$ dos inteiros módulo 6.

Exercício

O subanel $\{0, 2, 4\}$ de $\mathbb{Z}_6$ considerado no exemplo anterior tem elemento identidade?

Exemplo

O conjunto

$$M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

é um subanel do anel das matrizes 2×2 com entradas em $\mathbb{Z}$.

Definição

Um elemento não nulo a de um anel comutativo A diz-se um divisor de zero *se existir um elemento não nulo $b \in A$ tal que $ab = 0$.*

Definição

Um domínio de integridade *é um anel comutativo com elemento identidade e sem divisores de zero.*

Resulta da definição que, num domínio de integridade, um produto é 0 se e só se um dos factores for 0.

Exemplo

O anel $\mathbb{Z}$ dos inteiros é um domínio de integridade.

Exemplo

O anel $\mathbb{Z}_6$ dos inteiros módulo 6 não é um domínio de integridade.

Exemplo

Se n for um inteiro não primo, o anel $\mathbb{Z}_n$ dos inteiros módulo n não é um domínio de integridade.

Exemplo

Se p for um número primo, o anel $\mathbb{Z}_p$ dos inteiros módulo p é um domínio de integridade. De facto, suponhamos que $a, b \in \mathbb{Z}_p$ são tais que $ab = 0$ (em $\mathbb{Z}_p$). Então $ab = pk$, para algum inteiro k. Logo, pelo Lema de Euclides, p divide a ou p divide b, donde, em $\mathbb{Z}_p$, $a = 0$ ou $b = 0$.

Exemplo

$\mathbb{Z} \times \mathbb{Z}$ não é um domínio de integridade.

Exemplo

O anel $M_2(\mathbb{Z})$ das matrizes quadradas 2×2 com entradas inteiras não é um domínio de integridade.

Num domínio de integridade podemos usar o cancelamento:

Proposição

Sejam a, b e c elementos de um domínio de integridade. Se $a \neq 0$ e $ab = ac$, então $b = c$.

Demonstração. De $ab = ac$ resulta $a(b - c) = 0$ e, como $a \neq 0$, $b - c = 0$.