



Corpos

Definição

Um corpo é um anel comutativo com elemento identidade em que todo o elemento não nulo é invertível.

Muitas vezes é conveniente pensar em ab^{-1} como sendo $\frac{a}{b}$, quando a e b são elementos de um corpo, com b não nulo.

É fácil ver que um corpo é um domínio de integridade: se a e b forem elementos de um corpo, com $a \neq 0$, e se tiver $ab = 0$, então, multiplicando ambos os membros por a^{-1} , obtemos $b = 0$.

O recíproco não vale, embora não seja difícil verificar que vale no caso finito:

Proposição

Um domínio de integridade finito é um corpo.

Demonstração. Seja D um domínio de integridade com elemento identidade 1 e seja $a \in D \setminus \{0\}$. Vamos mostrar que a é invertível.



Se $a = 1$, então a é o seu próprio inverso, pelo que podemos supor $a \neq 1$. Consideremos agora a sucessão $a, a^2, a^3, \dots$ de elementos de D . Como D é finito, existem inteiros positivos i e j , com $i > j$ tais que $a^i = a^j$. Como num domínio de integridade podemos cancelar factores não nulos, temos $a^{i-j} = 1$. Mas $a \neq 1$ implica $i - j > 1$, donde a^{i-j-1} é o inverso de a . $\square$

Corolário

Para qualquer primo p , o anel $\mathbb{Z}_p$ dos inteiros módulo p é um corpo.

Demonstração. Num dos exemplos anteriores mostra-se que $\mathbb{Z}_p$ é um domínio de integridade. Para concluir a demonstração basta agora usar a proposição anterior. $\square$

Este corolário juntamente com um exemplo dado (que diz que $\mathbb{Z}_n$ não é um domínio de integridade se n não for primo) mostra que $\mathbb{Z}_n$ é um corpo se e só se n for primo.



Exemplo

Seja $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, com as operações

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

e

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

$(a, b, c, d \in \mathbb{Q})$.

É fácil ver que $\mathbb{Q}[\sqrt{2}]$ é um anel comutativo com elemento identidade.

Visto como um número real, o inverso multiplicativo de $a + b\sqrt{2}$ é

$1/(a + b\sqrt{2})$. Para verificar que $\mathbb{Q}[\sqrt{2}]$ é um corpo basta mostrar que $1/(a + b\sqrt{2})$ pode ser escrito na forma $c + d\sqrt{2}$, com $c, d \in \mathbb{Q}$.

Para o conseguir, o que temos a fazer é “racionalizar o denominador”:

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2}.$$

(Note-se que $a + b\sqrt{2} \neq 0$ garante que todos os denominadores são não nulos.)



Ideais e anéis quociente

Definição

Um subanel $\mathcal{I}$ de um anel A diz-se um ideal (bilateral) de A se, para quaisquer $a \in A$ e $i \in \mathcal{I}$, tanto ai como ia pertencem a $\mathcal{I}$.

Assim, um subanel $\mathcal{I}$ de um anel A é um ideal de A se $\mathcal{I}$ “absorver” os elementos de A , isto é, se, para todo o elemento $a \in A$, $a\mathcal{I} = \{ai \mid i \in \mathcal{I}\} = \mathcal{I}$ e $\mathcal{I}a = \{ia \mid i \in \mathcal{I}\} = \mathcal{I}$.

Exemplo

Para qualquer anel A , tanto $\{0\}$ como A são ideais de A .

Exemplo

Para qualquer inteiro positivo n , o conjunto $n\mathbb{Z}$ dos múltiplos de n é um ideal de $\mathbb{Z}$.



Exemplo

Seja A um anel comutativo com elemento unidade e seja $a \in A$. O conjunto $\langle a \rangle = \{ra \mid r \in A\}$ é um ideal de A , dito o *ideal principal* gerado por a .

Exemplo

Seja A um anel comutativo com elemento unidade e sejam $a_1, a_2, \dots, a_n \in A$. O conjunto $\langle a \rangle = \{r_1a_1 + r_2a_2 + \dots + r_na_n \mid r \in A\}$ é um ideal de A , dito o ideal gerado por $a_1, a_2, \dots, a_n$.



Anéis quociente

Sejam A um anel e $\mathcal{I}$ um ideal de A . Atendendo a que A , com a adição, é um grupo e $\mathcal{I}$ é um subgrupo normal, podemos formar o grupo quociente: $A/\mathcal{I} = \{a + \mathcal{I} \mid a \in A\}$. Poderemos definir (de forma natural) uma multiplicação por forma a obter um anel? Vamos ver que sim, desde que $\mathcal{I}$ seja um ideal e não apenas um subanel.

Proposição

Sejam A um anel e $\mathcal{I}$ um subanel de A . O conjunto das classes laterais $\{a + \mathcal{I} \mid a \in A\}$ é um anel com as operações

$$(r + \mathcal{I}) + (s + \mathcal{I}) = (r + s) + \mathcal{I} \text{ e } (r + \mathcal{I})(s + \mathcal{I}) = (rs) + \mathcal{I}$$

se e só se $\mathcal{I}$ for um ideal de A .

Demonstração. Vejamos que se $\mathcal{I}$ for um ideal, então a multiplicação está bem definida. Suponhamos que $a + \mathcal{I} = a' + \mathcal{I}$ e que $b + \mathcal{I} = b' + \mathcal{I}$. Devemos mostrar que $ab + \mathcal{I} = a'b' + \mathcal{I}$.



Por definição, existem $i, j \in \mathcal{I}$ tais que $a = a' + i$ e $b = b' + j$. Então

$$ab = (a' + i)(b' + j) = a'b' + ib' + a'j + ij,$$

logo

$$ab + \mathcal{I} = a'b' + ib' + a'j + ij + \mathcal{I} = a'b' + \mathcal{I},$$

pois $\mathcal{I}$ absorve $ib' + a'j + ij$.

Suponhamos que $\mathcal{I}$ é um subanel que não é um ideal de A . Então existem $a \in A$ e $i \in \mathcal{I}$ tais que $ai \notin \mathcal{I}$ ou $ia \notin \mathcal{I}$. Admitamos que $ia \notin \mathcal{I}$. Consideremos os elementos $i + \mathcal{I} = 0 + \mathcal{I}$ e $a + \mathcal{I}$. Claro que $(i + \mathcal{I})(a + \mathcal{I}) = ia + \mathcal{I}$, mas $(0 + \mathcal{I})(a + \mathcal{I}) = 0 \cdot a + \mathcal{I} = \mathcal{I}$. Como $ia + \mathcal{I} \neq \mathcal{I}$, a multiplicação não está bem definida e, portanto, o conjunto das classes laterais com estas operações não forma um anel.

Os detalhes restantes são simples e ficam como exercício. □

Exemplo

Consideremos o anel quociente $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$. Vejamos como se adicionam e multiplicam $2 + 4\mathbb{Z}$ e $3 + 4\mathbb{Z}$.

$$(2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4 + 4\mathbb{Z} = 1 + 4\mathbb{Z},$$

$$(2 + 4\mathbb{Z})(3 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4 + 4\mathbb{Z} = 2 + 4\mathbb{Z}.$$



Exercício

Sejam $A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ e $\mathcal{I}$ o subconjunto de A das matrizes cujas entradas são inteiros pares.

1. Mostre que $\mathcal{I}$ é um ideal de A .
2. Quantos elementos tem o anel quociente $A/\mathcal{I}$?

A resposta à segunda alínea é: 16. (Exemplo:

$$\begin{pmatrix} 3 & 17 \\ 0 & -11 \end{pmatrix} + \mathcal{I} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 16 \\ 0 & -12 \end{pmatrix} + \mathcal{I} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \mathcal{I}.)$$