Caderno de Anéis e Corpos

Lourenço Bogo

Sumário

Capítulo 1

Introdução

Nessa matéria, como o nome já diz, vamos tratar sobre dois tipos de estruturas matemáticas: os Anéis e os Corpos. Essas estruturas e suas propriedades vêm sido estudadas há muito tempo por vários matemáticos diferentes.

No começo, muitos matemáticos investiam teempo e trabalho para fazer novas descobertas sobre os anéis, como os números inteiros. Alguns grandes nomes, como Diofantus, Fermat, entre outros, dedicaram boa parte de seu tempo para trabalhar com números inteiros, surgindo com problemas que foram discutidos até recentemente, como o Último Teorema de Fermat: $x^n + y^n = z^n$, com $n \in \mathbb{Z}$

1.1 Introdução

Aneis: Anel é um conjunto A sobre o qal estão definidas duas operações: adição e multiplicação,

$$\forall a, b \in A \begin{cases} + : (a, b) \to a + b \in A \\ \cdot : (a, b) \to a \cdot b \in A \end{cases}$$, que satisfazem as seguintes propriedades:

A1 $(a + b) + c = a + (b + c)$

A2 $a + b = b + a$

A3 $\exists 0 \in A \, t.q. \forall a \in A, \; a + 0 = a$

A4 $\forall a \in A \exists (-a) \, t.q. \; a + (-a) = 0$

$\langle A, + \rangle$ é um grupo abeliano 0 é o elemento neutro e $-a$ é o elemento oposto

AM1 $(a+b).c = a.c + b.c$

AM2 $a.(b+c) = a.b + a.c$

O anel $\langle A, +, \cdot \rangle$ chama-se associativo se:

M1 $(a.b).c = a.(b.c)$

O anel chama-se comutativo se:

M2 $\forall a, b \in A,\ a.b = b.a$

O anel chama-se unitário se $\exists\, 1 \in A\, t.q.\, \forall a \in A\, a.1 = 1.a = a$

1.2 Propriedades

1. O elemento neutro é único:

   Dem: Seja $0'$ outro elemento neutro de A. Consideremos $0+0'$. Como $0'$ é elemento neutro, isso é igual a 0, mas como a soma é comutativa $0 = 0'$■

2. O elemento oposto é único:

   Dem: Seja b outro elemento oposto para a. $a + b = 0 = b + a$. Consideremos $(b+a)+(-a) = 0+(-a) = -a$. Mas $(b+a)+(-a) = b+(a+(-a)) = b+0 = b$. Logo $b = -a$■

3. $\forall a \in A,\ 0.a = a.0 = 0$

4. $\forall a, b \in A,\ (-a).b = -(a.b) = a.(-b)$

1.3 Exemplos de Anéis

1. $\mathbb{Z} = \langle \pm 0, \pm 1, \pm 2, \ldots, n; +, \cdot \rangle$ é um anel associativo, comutativo, unitário.

2. $\langle \mathbb{Q}, +, \cdot \rangle$ - Os números racionais

3. $\langle \mathbb{R}, +, \cdot \rangle$ - Os números reais

4. $\langle \mathbb{C}, +, \cdot \rangle$ - Os números complexos

   são todos anéis comutativos, associativos, unitários e, também, são inversíveis para todos os elementos exceto o zero (0).

5. $2\mathbb{Z}$ é um anel associativo, comutativo mas não é unitário

Seja $\langle A, +, \cdot \rangle$ um anel associativo com 1, $a \in A$, um elemento $b \in A$ chama-se um inverso para a, se $a.b = b.a = 1$. Neste caso o elemento a, chama-se inversível, se denota$a^{-1} := b$

1.4 Corpos

Definição: Seja $\langle A, +, \cdot \rangle$ uum anel comutativo, associativo, com $1 \neq 0 \, t.q. \, \forall a \in A$, se $a \neq 0$, a é inversível. Então chama-se A de corpo.

1.5 Exemplos de Corpos

1. $A = \{0\}$, pois $0 + 0 = 0$ e $0 \cdot 0 = 0$.

   Se A é um anel t.q. $0 = 1$ em A, então $A = 0$ apenas, pois $a = 1 \cdot a = 0 \cdot a = 0$.

   Logo, precisamos da condição $0 \neq 1$.

2. Se $\langle \mathbb{R}^3, \ +, \ \times \rangle$, onde $\times$ é o produto vetorial. Vemos que não temos comutatividade nem associatividade. Pois $i \times (i \times j) = i \times k = -j$ e $(i \times i) \times j = 0$, além de que $a \times b = -b \times a$. Este exemplo é chamado de Anel de Lie, quando tem apenas *anticomutatividade*.

3. Anel de polinômios.

   Seja R um anel. Denotamos por R[x] um anel de polinômios sobre R:

   $R[x] := \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{R}, \ n \in \mathbb{N}\}$.

   Se $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{m} b_i x^i$, então

   $f(x) + g(x) = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^y i$ e

   $f(x) \cdot g(x) = \sum_{i=0}^{mn} c_i x^i, \ c = \sum_{j+k=i} a_j b_k$

   $R[x] = \{(a_0, a_1, \cdots, a_n, \cdots) \mid a_i \in \mathbb{R}, \text{com um número finito de elementos diferente de } 0\}$.

   $(a_0, a_1, \cdots, a_n, \cdots) + (b_0, b_1, \cdots, b_m, \cdots) = (a_0 + b_0, \cdots)$

   $(a_0, a_1, \cdots, a_n, \cdots) \cdot (b_0, b_1, \cdots, b_m, \cdots) = (c_0, c_1, \cdots)$, onde $c = \sum_{j+k=i} a_j b_k$.

$x = (0, 1, 0, 0, \cdots)$

$1 = (1, 0, 0, 0, \cdots)$

$0 = (0, 0, 0, 0, \cdots)$

4. Um anel de funções (contínuas, deriváveis, etc)

   $\langle \mathbb{F}(\mathbb{R}),\ +,\ \cdot \rangle$ um anel de funções reais é comutativo, associativo e tem 1.

   $\langle \mathbb{F}(\mathbb{R}),\ +,\ \circ \rangle$ não é um anel, pois não há distributiva.

5. Anéis de matrizes

   $M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$ é um anel não comutativo.

   Onde $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ e $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

   Seja R um anel associativo. Definimos $M_n(R) = \left\{ \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \right\} \mid a_{ij} \in R$

   com operações

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} + \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{bmatrix}$$

   e

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{bmatrix} = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mn} \end{bmatrix}$$

   , onde $c_{ij} = a_{i1}b_{1j} + \cdots + a_{in}b + nj$.

6. Um último exemplo é $\mathbb{Z}(\sqrt{2})$ Onde são números da forma $n + m\sqrt{2}$

Capítulo 2

O Anel $\mathbb{Z}_n$

2.1 Introdução

Sendo $\bar{z}$ o resto da divisão de z por n.

$\mathbb{Z}_n = \{\bar{0}, \ldots, n \bar{-} 1\}$

2.2 Propriedades

- $\overline{k} = \overline{m} \Leftrightarrow n|k-m$
- $\overline{k} + \overline{m} = \overline{k+m}$
- $\overline{k}.\overline{m} = \overline{k.m}$
- $-\overline{k} = \overline{n-k}$

$\langle Z_n, +, \cdot \rangle$ é um anel associativo, comutativo, unitário.

Definição: Seja A um anel. Um elemento $a \in A$ chama-se divisor de zero se $a \neq 0$ e $\exists b \in A$ tal que $a.b = 0$.

1. Se a é inversível, a não pode ser um divisor de zero:

   Suponhamos que $a.b = 0 \Rightarrow a^{-1}.(a.b) = 1.b = b$■

2. Qualquer corpo não tem divisores de zero.

Proposição 1 Seja $\overline{m} \in \mathbb{Z}_n$, então

- $\overline{m}$ é um divisor de zero $\Leftrightarrow mdc(m,n) \neq 1$

  Demonstração: $\Rightarrow$: $\exists \overline{k} \neq \overline{0}$ em $\mathbb{Z}_n$ tal que $\overline{m}.\overline{k} = \overline{0}$, ou seja $m.k$ é divisível por n: $\exists l \in \mathbb{Z}$ tal que $m.k = l.n$. Se $mdc(m,n) = 1$ então m é primo com n, logo $n|k$ e $\bar{k} = 0$, um absurdo.

  $\Leftarrow$: Seja $mdc(m,n) = d > 1$. Então $m = m_1.d$, $n = n_1.d$ $1 < m_1, n_1 < n$. Consideremos $\overline{m}.\overline{n_1} = (\overline{m_1}.\overline{d}).\overline{n_1} = \overline{m_1}.(\overline{d}.\overline{n_1}) = \overline{m}.\overline{n} = 0$.

- $\overline{m}$ é inversível $\Leftrightarrow mdc(m,n) = 1$

  Demonstração: $\Rightarrow$: Suponhamos que $\bar{m}$ é inversível. Então $\exists \overline{k} \in \mathbb{Z}_n$ tal que $\overline{m}.\overline{k} = \overline{1}$, ou seja $n|n.k - 1$. Então $\exists l \in \mathbb{Z}$ tal que $m.k - 1 = n.l$, ou seja $m.k + n.l = 1 \Rightarrow mdc(m,n) = 1$.

  $\Leftarrow$: Suponhamos que $mdc(m,n) = 1$ pela Identidade de Bizout, $\exists r, s \in \mathbb{Z}$ tal que $m.r + n.s = 1 \Rightarrow \overline{m}.\overline{r} + \overline{n}.\overline{s} = \overline{1} \Rightarrow \overline{m}.\overline{r} = 1$ (pois $\overline{n}.\overline{s} = \overline{0}$).

Um anel A, chama-se de domínio de integridade se A não tiver divisores de zero. Cada corpo é um domínio de integridade no qual cada elemento não nulo é inversível.

Em cada domínio de integridade se verifica a lei de cancelamento: se $a.b = a.c$ e $a \neq 0$ entãoy $b = c$.

Teorema 1: Seja $D = \{a_1, \ldots, a_n\}$ um domínio de integridade. Seja $0 \neq a \in D$, consideremos $\{a_1.a, \ldots, a_n.a\} \subseteq D$. Observemmos que se $i \neq j$ então $a_i.a \neq a_j.a$. Então $D = \{a_1.a, \ldots, a_n.a\}$. Em particular existe i tal que $a_i.a = a$. Denotemos $e = a_i$ e provemos que $\forall b \in D$ $e.b = b.e = b$ $(e = 1)$.

$e.a = a \Rightarrow e.(e.a) = e.a \Rightarrow e^2.a = a$, $(a.e - a).e = (a.e).e - a.e = a.e^2 - a.e = a.(e^2 - e) = 0 \Rightarrow a.e = a = e.a$.

Seja $b \in D$ arbitrário, então $b \in \{a_1.a, dots, a_n.a\}$,portanto, $\exists j$ tal que $b = a_j.a$. Agora $b.e = (a_j.a).e = a_j.(a.e) = a_j.a = b$. Como antes, temos também que $e.b = b$. Como b é arbitrário, e é um elemento neutro $(e = 1)$, temos $1 \in \{a_1.a, \ldots, a_n.a\}$, então $\exists k$ tal que $1 = a_k.a$. Consideremos $(a.a_k - 1) \Rightarrow a_k.(a.a_k - 1) = 1.a_k - a_k = 0$.

Pela lei do cancelamento, $a.a_k = 1$, então $a_k = a^{-1}$.

2.3 Sub-anel e Sub-corpo

Seja A um anel. Um subconjunto $B \subseteq A$ chama-se $sub - anel$ se:

1. $0 \in B$

2. $\forall a, b \in B,\ a + b,\ a.b \in B$

3. $\forall b \in B,\ -b \in B$

Se A é um corpo e um sub-anel B forma um corpo também, então B chama-se sub-corpo de A.

Os únicos dois corpos sem sub-corpos próprios são $\mathbb{Z}_p$ (p primo) e $\mathbb{Q}$.

2.4 Soma Direta de Anéis

A, B anéis:

$A \oplus B = \{(a, b) | a \in A, b \in B\}$

$(a, b) + (c, b) = (a + c, b + d)$, o mesmo para o produto.

2.5 Ideiais

Seja A um anel. Um subanel $I \subset A$ chama-se **ideal** (à direita (esquerda)) se $\forall a \in A$, $\forall i \in I$, $i.a(a.i) \in I$.

Caso I seja um ideal à direta e à esquerda, ele é chamado ideal bilateral.

Os ideais triviais para qualquer anel A são o (0) e o próprio anel A.

Exemplos:

1. Seja A um anel comutativo unitário, $a \in A$. Então $a.A = \{a.x | x \in A\}$ é um ideal de A.

   aA é um subanel de A $\begin{cases} ax + ay = a(x + y) \in aA \\ (ax)(ay) = a(xy) = \in aA \\ -(ax) = a(-x) \in aA \\ 0 = 0a \in aA \end{cases}$ y $\forall y \in A$, $(ax)y = a(xy) \in aA \Rightarrow aA$ é um ideal de A.

   Esse ideal é cahamado também de ideal principal de A e pode ser denotado como (a).

Proposição 1: Em $\mathbb{Z}$, todo ideal tem forma $n\mathbb{Z}$ para algum $n \geq 0$. Provemos que todo subanel S de $\mathbb{Z}$ tem essa forma para algum $n \geq 0$.

$s \neq$, pois $0 \in S$. Se $s = (0)$ então $S = 0.\mathbb{Z}(n = 0)$.

Suponhamos que $S \neq (0)$, então existe $s \in S$, $s \neq 0$. Se $s < 0$, consideremos $-s \in S$, $-s > 0$.

Então $S_+ = m \in S|m > 0 \neq$, $S_+ \subseteq$