Estruturas Algébricas

Aula 5

Divisibilidade e Ideais

Abramo Hefez

2025

Divisibilidade em Anéis

Em um anel A dizemos que um elemento a divide um elemento b se existir um elemento c tal que $b = ac$.

Neste caso, dizemos que b é divisível por a, ou que b é múltiplo de a e escreve-se $a | b$.

Caso contrário, escreve-se $a \nmid b$.

Temos a seguinte proposição, cuja prova é um exercício.

__Proposição__ Sejam $a, b, c, b_1, \ldots, b_n, c_1, \ldots, c_n, v \in A$, $u \in A^*$

1) $a | a$, $a | 0$, $0 | a \Longleftrightarrow a = 0$.
2) $a | b$ e $b | c \Longrightarrow a | c$
3) $a | b$ e $c | d \Longrightarrow a.c | bd$
4) $a | (b+c)$ e $a | b \Longrightarrow a | c$
5) $a | b_1, \ldots, a | b_n \Longrightarrow a | (c_1 b_1 + \cdots + c_n b_n)$
6) $u \in A^* \Longrightarrow u | a$
7) $v | u \Longleftrightarrow v \in A^*$.

__Proposição__ Seja A um domínio de integridade e $a, b \in A$. Tem-se que $a | b$ e $b | a \Longleftrightarrow \exists\, u \in A^*$ tq $a = ub$.

__Dem__

$$\left.\begin{array}{l} a | b \Rightarrow \exists\, c \text{ tq } b = ac \\ b | a \Rightarrow \exists\, d \text{ tq } a = bd \end{array}\right\} \Longrightarrow b = bdc.$$

Se $b \neq 0$, tem-se que $dc = 1$, logo $d \in A^*$ e o resultado segue.

Se $a = 0$, de $a | b$ temos que $b = 0$, logo $a = 1.b$

Reciprocamente, se $a = ub$ com $u \in A^*$, tem-se que $b | a$ e como $b = u^{-1}a$, tem-se que $a | b$. $\square$

Quando existe $u \in A^*$ tq $a = ub$, dizemos que a e b são <u>associados</u>.

Por exemplo, em $\mathbb{Z}$, temos que a e $-a$ são associados, para todo $a \in \mathbb{Z}$.

Em $\mathbb{R}[x]$, o polinômio $2x+1$ é associado a $a(2x+1)$, para todo $a \in \mathbb{R} \setminus \{0\}$.

Em $\mathbb{Z}[i]$, temos que $1+i$ é associado a $-(1+i)$, $i(1+i)$ e $-i(1+i)$.

MDC d é um mdc de $a_1, \ldots, a_s$ se

(i) O elemento d é divisor comum de $a_1, \ldots, a_s$, i.e. $d | a_1, \ldots, d | a_s$

(ii) Para todo divisor comum c de $a_1, \ldots, a_s$, tem-se que $c | d$.

Se d e d' são dois mdc de $a_1, \ldots, a_s$, então $d | d'$ e $d' | d$.

Se A é um domínio, então dois mdc são sempre associados

MMC m é um mmc de $a_1, \ldots, a_s$, se

(i) m é um múltiplo comum de $a_1, \ldots, a_s$,

(ii) Para todo múltiplo comum c de $a_1, \ldots, a_s$, tem-se que $m | c$.

Se m e m' são dois mmc de $a_1, \ldots, a_s$, então $m | m'$ e $m' | m$

Se A é um domínio, então dois mmc são sempre associados.

Em um domínio nem sempre existem mdc e mmc

Exemplo $A = \{ a_0 + a_2 x^2 + \cdots + a_n x^n,\ n \in \mathbb{N},\ a_0, \ldots, a_n \in \mathbb{R} \}$ é um subanel de $\mathbb{R}[x]$.

x^5 e x^6 não possuem mdc em A

a, bx^2, cx^3 são divisores comuns de x^5 e x^6, mas o candidato natural x^3 para mdc, pois $x^2 \nmid x^3$.

Também x^5 e x^6 não possuem mmc, pois os candidatos são os associados de $x^8, x^9, \ldots$ são múltiplos comuns, mas $x^8 \nmid x^9$.

Ideais

Um subconjunto I de um anel A é um ideal se

(i) $I \neq \emptyset$

(ii) $\forall a, b \in I$, $a+b \in I$

(iii) $\forall b \in A$, $\forall a \in I$, $a.b \in I$.

Exemplos:

a) $\{0\}$ e A são ideais de A. Se $a \in I$, então

$-a = (-1)a \in I$.

b) Para $a \in I$, é um ideal o conjunto

$I(a) = \{xa \,;\, x \in A\}$.

A relação entre ideais e divisibilidade é a seguinte

$$\boxed{a|b \iff I(b) \subset I(a)}$$

Portanto, $I(b) = I(a) \iff a|b$ e $b|a$

e se A é um domínio, então $I(b) = I(a) \iff$ a e b são associados.

c) Se $a_1, \dots, a_n \in A$, temos que

$I(a_1, \dots, a_n) = \{x_1 a_1 + \dots + x_s a_s \,;\, a_1, \dots, a_s \in A\}$

é um ideal de A.

<u>Obs</u>: A é um corpo, se, e somente se, os únicos ideais de A são $\{0\}$ e A.

<u>Proposição</u> Seja A um anel e $a_1, \dots, a_s \in A$.

a) Se $d \in A$ é tal que $I(d) = I(a_1, \dots, a_s)$, então d é um mdc de $a_1, \dots, a_s$.

b) Se $m \in A$ é tal que $I(m) = I(a_1) \cap \dots \cap I(a_s)$, então m é um mmc de $a_1, \dots, a_s$.

<u>Dem</u> a) Como $a_1, \dots, a_s \in I(d)$, temos que $d|a_1, \dots, d|a_s$.

Se $c|a_1, \dots, c|a_s$, então

$I(d) = I(a_1, \dots, a_s) \subset I(c)$

$\Rightarrow c|d$.

b) Como $m \in I(d) = I(a_1) \cap \dots \cap I(a_s)$, temos de m é múltiplo de $a_1, \dots,$ de a_s.

Se c é um mmc de $a_1, \dots, a_s$, temos que

$$I(c) \subset I(a_i) \quad \forall i;$$

então

$$c \in I(c) \subset I(a_1) \cap \dots \cap I(a_s) = I(m),$$

logo

$$c = bm, \text{ ou seja } m \mid c.$$

Depois dos corpos, os anéis que possuem uma estrutura de ideais mais simples são os anéis para os quais todo ideal é da forma é $I(a)$ para algum elemento a do anel.

Esses anéis são chamados de <u>anéis principais</u>. Pelo o que provamos anteriormente, em anéis principais existem mdc e mmc e muitas outras propriedades que mostraremos mais adiante.

<u>Teorema</u> Todo domínio euclidiano é um domínio principal

<u>Dem</u> Seja $(D, +, \cdot, \varphi)$ um domínio euclidiano e seja $I \subset D$ um ideal.

Se $I = \{0\}$, então $I = I(0)$ é principal.

Suponha que $I \neq \{0\}$ e seja $a \in I \setminus \{0\}$ tal que $\varphi(a)$ tenha o menor valor. Vamos mostrar que $I = I(a)$.

De fato, como $a \in I$, temos que $I(a) \subset I$. Por outro lado, seja $b \in I \setminus \{0\}$, dividindo b por a temos que existem $q, r \in A$ tq

$$b = aq + r \quad , \quad \text{com } r = 0 \text{ ou } \varphi(r) < \varphi(a).$$

Como $b, a \in I$, temos que $r = b - aq \in I$ e como a é o elemento de I cujo valor por φ é mínimo, temos que $r = 0$, o que implica que

$$b = aq \in I(a). \qquad \square$$

<u>Corolário</u> São domínios principais $\mathbb{Z}$, $K[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-3}]$.

Exemplo de um domínio que não é principal:

Em $\mathbb{Z}[x]$ o ideal $I(2,x)$ não é principal.

De fato, se $I(2,x) = I(p(x))$ para algum $p(x) \in \mathbb{Z}[x]$, então $2 = p(x) \cdot q_1(x)$ e $x = p(x) q_2(x)$

Da primeira igualdade, temos que $p(x) = \pm 1$ ou $p(x) = \pm 2$.

- Se $p(x) = \pm 1$, então $I(2,x) = I(\pm 1) = \mathbb{Z}[x]$, o que é uma contradição, pois os elementos de $I(2,x)$ têm coeficientes constantes pares, o que não ocorre para todos os elementos de $\mathbb{Z}[x]$.

- Se $p(x) = \pm 2$, então $I(p(x)) = I(\pm 2)$, o que implica que todos os coeficientes dos polinômios em $I(p(x))$ são pares, o que é uma contradição, pois $x \in I(p(x))$.

Fatoração em Anéis

O modêlo aqui é o Teorema Fundamental da Aritmética:
Em $\mathbb{Z}$ todo elemento diferente de 0 e de ± 1, ou é primo ou se fatora como produto de números primos (irred.) de modo único a menos da ordem e do sinal dos fatores

Ex $\quad 6 = 2\times 3 = 3\times 2 = (-2)\times(-3) = (-3)\times(-2)$.

Nesse resultado há duas afirmações

a) Todo número $\neq 0, \pm 1$ ou irredutível ou se fatora como produto de um nº finito de elem. irred.

b) A fatoração é única a menos de ordem e de associados.

Nessa questão de fatoração há dois conceitos envolvidos.

Elementos irredutíveis: Um elemento a de um anel A é irredutível se toda vez que se escreve $a = bc$, tem-se que ou b ou c é uma unidade.

Ex. Em $\mathbb{Z}$, 2 é irredutível, pois se

$$2 = b.c$$

então $|b||c| = 2$, logo $|b| = 1$ ou $|c| = 1$, pois caso contrário $|b| \geq 2$ e $|c| \geq 2 \Rightarrow |b||c| \geq 4$

- Em $k[x]$, x é irredutível, pois se

$$x = p(x)\cdot q(x),$$

logo $gr(p(x)) + g(q(x)) = 1 \Rightarrow gr(p(x)) = 0, 1$
se $gr(p(x)) = 0$, tem-se que $p(x)$ é uma unidade
se $gr(p(x)) = 1$, então $gr(q(x)) = 0$ logo $q(x)$ é uma unidade.

Elementos primos: Um elemento a de um anel é primo se toda vez que a/bc, então a/b ou a/c.

Esta é a definição de Euclides 300 aC.

Exemplo $2 \in \mathbb{Z}$ é primo

$2/bc$, então bc é par, logo b ou c é par, ou seja, $2/b$ ou $2/c$

$x \in K[x]$ é primo

$x/p(x) \cdot q(x)$. Se $x \nmid p(x)$ e $x \nmid q(x)$

então $p(x) = a_0 + a_1 x + \cdots \quad a_0 \neq 0$

$q(x) = b_0 + b_1 x + \cdots \quad b_0 \neq 0$

logo $p(x) q(x) = a_0 b_0 + \cdots \quad a_0 b_0 \neq 0$, logo

$x \nmid p(x) q(x)$ absurdo

Note que o argumento usado para provar irred. e primalid. é distinto.

Esses dois conceitos são em geral distintos.

Proposição Todo elemento primo é irredutível.

Dem Seja $p \in A$ primo e suponha que

$$p = a \cdot b,$$

logo p/a ou p/b.

Suponha p/a, logo $a = bp$ e portanto, $p = ab = bpb$

logo $b^2 = 1$ e, portanto, b é inversível $\square$