Estruturas Algébricas

Aula 6

Fatoração em Anéis

Abramo Hefez

2025

Em um anel nem todo irredutível é primo.

Exemplo no anel de Kummer $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[5i]$

2 é irredutível mas não é primo.

De fato, se $\quad 2 = (a+b\sqrt{-5})(c+d\sqrt{-5}) \Rightarrow$

$$\Rightarrow 4 = (a^2+5b^2)(c^2+5d^2) \Rightarrow$$

$$b = d = 0 \quad e \quad a = \pm 1, \quad c = \pm 1.$$

$$\Rightarrow a+b\sqrt{-5} = \pm 1 \quad ou \quad c+d\sqrt{5} = \pm 1$$

Logo 2 é irredutível

2 não é primo, pois

$$2 = (1+\sqrt{5}i)(1-\sqrt{5}i) = 1+5 = 6$$

e no entanto $2 \nmid (1+\sqrt{5}i)$ e $2 \nmid (1-\sqrt{5}i)$.

Teorema Em um domínio principal todo elemento irredutível é primo.

Dem Seja a um elemento irredutível e suponha que $a|bc$. Suponha que $a \nmid b$, vamos provar que a/c.

A é principal

Considere o ideal $I(a,b) = I(d)$.

$\Rightarrow d/a$ e d/b. Como os únicos divisores de a, então a são as unidades e os associados de a,

ou $d \in A^*$ ou $\underbrace{d = ua}_{\text{não pode ocorrer}}$ com $u \in A^*$ não pode ocorrer pois $\overset{d}{u a}/b \Rightarrow a/b$ absurdo

Portanto, $\quad I(a,b) = I(d) = A$.

Logo $\exists\, \lambda, \mu \in A$ tq $\quad 1 = \lambda a + \mu b$, consequentemente

$$c = \lambda ac + \mu \underbrace{bc}_{a \text{ divide } bc} \Rightarrow a/c$$

Proposição Em um domínio principal A toda cadeia ascendente de ideais

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$$

é estacionária, isto é existe um índice m tal que $I_m = I_{m+1} = \cdots$

Dem É um exercício fácil verificar que

$$I = \bigcup_{j \geq 1} I_j$$

é um ideal.

Como A é domínio principal, temos que

$$I = \bigcup_{j \geq 1} I_j = I(a).$$

Logo para algum m temos que $a \in I_m$.

Assim $I(a) \subset I_m \subset I_{m+1} \subset \cdots \subset \bigcup_{j \geq 1} I_j = I(a)$

Logo $I_m = I_{m+1} = \cdots = I(a)$.

$\square$

Proposição Todo elemento não nulo e não inversível de um domínio principal ou é irredutível, ou possui pelo menos um divisor irredutível.

Dem Seja $a \in A \setminus A^*$, $a \neq 0$. Se a é irredutível, nada temos a provar.

Se $a = a_1 b$ com a_1 e b não associados a $\underline{a}$.

$I(a) \subsetneqq I(a_1)$, pois caso contrário, a_1 e a seriam associados.

Se a_1 é irred. ok.

Se a_1 é redutível, então $a_1 = a_2 b_1$ com a_2 e b_1 não assoc. a $\underline{a_1}$

$$I(a) \subsetneqq I(a_1) \subsetneqq I(a_2).$$

Esse processo tem que parar logo para algum a_m

$I(a) \subsetneqq I(a_m)$ com a_m irredutível e a_m / a.

$\square$

Teorema: Todo elemento a não nulo e não invertível de um domínio principal ou é irredutível, ou se fatora como produto de elem. irredutíveis.

Dem. Se a é irredutível, nada temos a provar.

Suponha que a seja redutível. Logo pela prop. anterior, temos um elemento irredutível a_1 tq $a = a_1 b_1$.

Se b_1 é irredutível, então nada mais temos a provar.

Se b_1 é redutível, então $b_1 = a_2 b_2$, com a_2 irred.

Se b_2 é irredutível, nada mais temos a provar pois $a = a_1 a_2 b_2$, com a_1, a_2, b_2 irredutíveis.

Esse processo tem que terminar pois caso contrário, teríamos uma sequência de elementos b_i tais que $b_{i+1} | b_i$ e b_i não é associado a b_{i+1} com

$$I(b_1) \subsetneq I(b_2) \subsetneq I(b_3) \subsetneq \cdots ,$$

contradição

Proposição Se A é um domínio e $p, p_1, \ldots, p_n$ são elem. primos e se $p | p_1 \cdots p_n$, então p é associado a um p_i.

Dem Por indução sobre n.

$n = 1$ $\quad p | p_1 \Rightarrow p_1 = ap$ como p_1 é irredutível, temos que a é uma unidade, já que p não é unidade.

Suponha válido para $n-1$ e

$$p | p_1 \cdots p_n \Longrightarrow p | p_n \text{ ou } p | p_1 \cdots p_{n-1}$$

Se $p | p_n$ o resultado segue do caso $n = 1$

Se $p | p_1 \cdots p_{n-1}$ o resultado segue da hip. de indução

$\square$

Def. Um domínio A é um domínio de fatoração única (DFU) se todo elemento não nulo e não inversível é irred. ou se fatora como produto de um número finito de elementos irredutíveis e essa fatoração é única a menos da ordem dos fatores e de elementos associados.

Teorema Todo domínio principal é um domínio de fatoração única.

Dem Sabemos que em um domínio principal todo elemento não nulo e não inversível ou é irred. ou se fatora como produto de um nº finito de elem. irredutíveis.
Falta provar a unicidade. Suponha que

$$p_1 \cdots p_n = q_1 \cdots q_m$$

com $n \leq m$ e $p_1, \dots, p_n, q_1, \dots, q_m$ irredutíveis.
Como irredutível é primo e $p_1 \mid q_1 \cdots q_m$, por prop. anterior, temos que p_1 é associado de algum q_i, que após ordenação podemos supor $i = 1$. Portanto, $q_1 = u_1 p_1$, substituindo e simplificando, temos que

$$p_2 \cdots p_n = q_2 \cdots q_m u_1$$

repetindo o argumento temos $q_2 = u_2 p_2, \dots, q_n = u p_n$
se $n = m$, a prova está completa. Se $n < m$, teríamos

$$1 = u_1 u_2 \cdots u_n . q_{n+1} \cdots,$$

o que é um absurdo, pois q_{n+1} é primo, logo não é unidade. $\square$

Exemplos: $\mathbb{Z}$, $K[x]$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{3}]$ são DFU.

Apesar de $\mathbb{Z}$ não ser um corpo, Gauss provou que $\mathbb{Z}[x]$ é um domínio de fatoração única, mesmo não sendo $\mathbb{Z}[x]$ um domínio principal. A prova de Gauss mostra mais geralmente que se um anel A é um domínio de fatoração única, então $A[x]$ é um domínio de Fatoração única.

Anéis quocientes

Dados um anel A e um ideal I, define-se

$$A/_I = \{a+I;\ a\in A\},$$

onde $a+I = \{a+x;\ x\in I\}$.

Os elementos de $A/_I$ são subconjuntos de A.

Obs $\quad a+I = a'+I \iff a-a'\in I$

Em $A/_I$ define-se uma adição e uma multiplicação

$$(a+I)+(b+I) = (a+b)+I$$
$$(a+I)\cdot(b+I) = a\cdot b \in I.$$

- Estas operações são bem definidas, i.e,

Se $a+I = a'+I$ e $b+I = b'+I$, então
$(a+b)+I = (a'+b')+I$ e $(a+I)\cdot(b+I) = (a'+I)\cdot(b'+I)$

Essas duas operações conferem a $A/_I$ uma estrutura de anel comutativo com unidade.

$$\boxed{\begin{array}{c} a+I = 0+I \\ \Updownarrow \\ a\in I \end{array}}$$

$$0 = 0+I \qquad 1 = 1+I$$
$$-(a+I) = -a+I$$

Notação: $a+I = [a]$

Definição Um ideal I de A, $I\neq A$ é dito primo, se
$$a\cdot b\in I \Rightarrow a\in I \text{ ou } b\in I$$

Exemplo Dom. Princ. tem-se que $I(p)$ é um ideal primo se e somente se p é primo.

$ab\in I(p) \iff p/a.b$

Como: p é primo $\iff [p/a.b \Rightarrow p/a$ ou $p/b]$

$$\Updownarrow$$

I(p) é ideal primo $\iff [ab\in I(p) \Rightarrow a\in I(p)$ ou $b\in I(p)]$

Def Um ideal $\mathcal{M}$ de A é maximal, se dado um ideal I tal que

$$\mathcal{M} \subset I \subsetneq A \implies I = \mathcal{M}.$$

{ Equivalentemente: $\mathcal{M} \subsetneq I \subset A \Rightarrow I = A$

Exemplo Em um Dom, P. todo ideal maximal é da forma $I(P)$ com p primo. e vice versa (exercício)

Proposição Seja I um ideal de um anel A, temos que

a) I é um ideal primo se, e somente se, A/I é um domínio

b). I é um ideal maximal se, e somente se, A/I é um corpo.

Dem (a) Se I não é primo, então existem $a, b \in I$ tais que $a.b \in I$. Logo $[a] \neq 0$, $[b] \neq 0$ e $[a].[b] = [ab] = [0]$, logo A/I não é domínio.

Provamos que A/I domínio $\Rightarrow$ I é primo.

Suponha I primo

$[a] \neq 0, [b] \neq 0 \Rightarrow a \notin I, b \notin I \overset{I \text{ primo}}{\Longrightarrow} a.b \notin I \Rightarrow [a].[b] \neq 0,$

logo A/I é domínio.

(b) Precisamos mostrar que I é maximal se, e somente se, todo $[a] \neq 0$ possui um inverso.

- I maximal. Se $[a] \neq 0$, então $a \notin I$ e $I \subsetneq I + I(a) = A$.

logo $\exists\, b \in I$, $c \in A$ tq

$$1 = b + c.a$$

Assim, $[1] = [b + ca] = \underset{0}{\underset{\|}{[b]}} + [c][a] = [c][a].$

- A/I corpo. Seja

$$I \subsetneq J \subset A$$

Como $J \neq I$, então existe $a \in J$ tal que $a \notin I$.

Como $[a] \neq [0]$, então $\exists\, b \in A$ tq $[a][b] = [1]$ $\Rightarrow$ $\underset{J}{\underset{\cap}{ab}} + \underset{J}{\underset{\cap}{c}} = 1$ $c \in I$ $\Rightarrow \boxed{1 \in J}$

Anéis quocientes de $\mathbb{Z}$ $\qquad n \in \mathbb{Z}$, $n \geq 2$.

$\mathbb{Z}_n := \mathbb{Z}/I(n)$

Alg. da divisão $a \in \mathbb{Z}$, $\exists\, q, r \in \mathbb{Z}$, $0 \leq r < n$ tq.

$$a = qn + r$$

Logo $[a] = [qn] + [r] = [0] + [r] = [r]$. Assim,

$$\mathbb{Z}_n = \{[0], \dots, [n-1]\}$$

. $[a] + [b] = [a+b]$ $\qquad [a]\cdot[b] = [a.b]$.

Obs $\qquad [a] = [b] \iff a - b \in I(n) \iff a \equiv b \mod n$.

$\mathbb{Z}_2$ já conhecemos

$\mathbb{Z}_3$:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

.	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$\mathbb{Z}_4$ já conhecemos

$\mathbb{Z}_n$ é corpo $\iff$ n é primo. (Exercício)

Quocientes de $K[x]$ por um ideal

Seja $I = I(p(x)) \neq 0$ com $\text{grau}(p(x)) = n$.

Dado $f(x) \in K[x]$ — $p(x)$ mônico (pomo supor)

$$f(x) = p(x) \cdot q(x) + r(x) \quad \text{com } r(x) = 0 \text{ ou } \text{grau}(r) < \underset{\overset{\|}{n}}{\text{grau}(p(x))}$$

Portanto, em $K[x]/I(p(x))$

$$[f(x)] = [p(x) \cdot q(x)] + [r(x)] = [r(x)]$$

com $r(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$

Assim,

$$[f(x)] = a_0[1] + a_1[x] + \dots + a_{n-1}[x^{n-1}]$$

Segue-se que $K[x]/I(p(x))$ é um <u>K-espaço vet.</u>

com base $[1], [x], \dots, [x^{n-1}]$. $\left\{ K[x]/I(p(x)) = \{\text{classes de polin de grau} \leq n-1\} \right.$

Sabemos que $K[x]/I(p(x))$ é um corpo $\Longleftrightarrow$

$p(x)$ é um polinômio irredutível.

<u>Exemplo</u> $K = \mathbb{Z}_2$ e $p(x) = x^2 + x + 1$ é irred em $\mathbb{Z}_2[x]$

$$\mathbb{F}_4 = \mathbb{Z}_2[x]/I(x^2+x+1) \quad \text{é um corpo}$$

Como é espaço vet. de dimensão 2 sobre $\mathbb{Z}_2$, gerado por $[1]$ e $[x]$, tem 4 elementos.

Tabela a seguir

$$\mathbb{F}_4 = K[X]/I(P(X)) = \{[0],[1],[X],[1+X]\}$$

$+$	$[0]$	$[1]$	$[X]$	$[1+X]$
$[0]$	$[0]$	$[1]$	$[X]$	$[1+X]$
$[1]$	$[1]$	$[0]$	$[1+X]$	$[X]$
$[X]$	$[X]$	$[1+X]$	$[0]$	$[1]$
$[1+X]$	$[1+X]$	$[X]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[X]$	$[1+X]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[X]$	$[1+X]$
$[X]$	$[0]$	$[X]$	$[1+X]$	$[1]$
$[1+X]$	$[0]$	$[1+X]$	$[1]$	$[X]$