UNIVERSIDADE FEDERAL DE SANTA CATARINA
UNIVERSIDADE VIRTUAL DO ESTADO DO MARANHÃO
ESPECIALIZAÇÃO EM MATEMÁTICA

JERRY LOPES DOS SANTOS
IANDEJARA ROCHA GALVÃO

QUOCIENTES EM ANÉIS DE POLINÔMIOS

Orientador: Oscar Ricardo Janesch

Barra do Corda - MA
2009

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS FÍSICAS E MATEMÁTICAS
Departamento de Matemática
Curso de Especialização em Matemática-Formação de Professor na modalidade a distância

"Quocientes em Anéis de Polinômios"

Monografia submetida a Comissão de avaliação do Curso de Especialização em Matemática-Formação do professor em cumprimento parcial para a obtenção do título de Especialista em Matemática.

APROVADA PELA COMISSÃO EXAMINADORA em 01/09/2009

Dr. Oscar Ricardo Janesch (CFM/UFSC - Orientador) _____

Dr. Alcides Buss (CFM/UFSC - Examinador) _____

Dr. Roberto Correa da Silva (CFM/UFSC – Examinador) _____

Profª Neri Terezinha Both Carvalho (Drª)
Coordenadora do Curso de Especialização em Matemática-Formação de Professor

Florianópolis, Santa Catarina, setembro de 2009.

Dedicamos a nossos pais pelo apoio e incentivo que sempre nos ofereceram em todos os momentos da nossa vida.

AGRADECIMENTOS

Agradecemos primeiramente a Deus, a nossa família e a todos os colegas e professores que tornaram possível a realização desse sonho, que foi concluir esta Especialização, em especial ao professor Oscar Janesch pela orientação e paciência tida conosco.

"O caminho dos ensinamentos é difícil e obscuro, mas o mais difícil é conduzir os outros de maneira clara e sutil por esse caminho."

SUMÁRIO

1. INTRODUÇÃO

Um resultado clássico da teoria de corpos assegura que se K é um corpo, então sua característica é zero ou é um número primo p. Se K é um corpo de característica zero, então seu corpo primo (menor subcorpo de K) é isomorfo a $\mathbb{Z}$. Portanto, nesse caso, K é infinito. Se K tem característica prima p, então seu corpo primo é isomorfo a Z_p. Pode-se provar que $K \simeq (Z_p)^n$, para algum $n \in \mathbb{N}$, portanto K tem p^n elementos.

O objetivo principal deste trabalho é apresentar uma técnica para construir corpos com p^n elementos, através dos quocientes de anéis de polinômios.

No Capítulo II apresentamos os resultados básicos sobre anéis, domínios e corpos. O Capítulo III é dedicado ao estudo de anéis quocientes e do teorema do isomorfismo. O Capítulo IV trata de anéis de polinômios. Finalmente, no Capítulo V, estudamos irredutibilidade de polinômios e usamos os resultados dos capítulos anteriores para construir corpos com p^n elementos.

2. ANÉIS E IDEAIS

Primeiramente definiremos as estruturas algébricas chamadas anel, anel comutativo, anel com unidade, domínio e corpo, com aplicações e exemplos ilustrativos e em seguida, demonstraremos propriedades aritméticas dos anéis. Trataremos também dos anéis $\mathbb{Z}_n$.

Estudaremos os subanéis com o objetivo de produzir novos exemplos de anéis, e destacaremos os ideais, como classe especial de subanéis.

2.1 Anel, Domínio e Corpo

Seja A um conjunto não vazio, no qual estão definidas duas operações.

$$*: A\times A\to A \qquad \Delta: A\times A\to A$$
$$(a,b)\to a*b \qquad (a,b)\to a\Delta b$$

A notação $(A,*,\Delta)$ indica que consideremos em A as operações $*$ e Δ, chamadas respectivamente de adição e multiplicação.

Definição 2.1.1 Dizemos que $(A,*,\Delta)$ é um anel quando são verificados os axiomas:

i) $a*b=b*a, \forall a,b\in A.$

ii) $a*(b*c)=(a*b)*c, \forall a,b,c\in A.$

iii) Existe $0_A\in A$ tal que $0_A*a=a*0_A=a$, $\forall a\in A$. (0_A é chamado zero de A.)

iv) Dado $a\in A$, existe $(-a)\in A$ tal que $a*(-a)=(-a)*a=0_A$. ($(-a)$ é chamado de simétrico de a).

v) $a\Delta(b\Delta c)=(a\Delta b)\Delta c$, $\forall a,b,c\in A$.

vi) $a\Delta(b*c)=a\Delta b*a\Delta c$

$(a*b)\Delta c=a\Delta c*b\Delta c$, $\forall a,b,c\in A$.

Definição 2.1.2 O anel $(A,*,\Delta)$ é comutativo quando vale o axioma:

vii) $a\Delta b=b\Delta a$, $\forall a,b\in A$.

Definição 2.1.3 O anel $(A,*,\Delta)$ é unitário quando vale o axioma:

viii) Existe $1_A \in A$ tal que $a\Delta 1_A = 1_A \Delta a = a$, $\forall a \in A$.

1_A é chamado de unidade de A.

Definição 2.1.4 O anel $(A,*,\Delta)$ é sem divisores de zero quando satisfaz:

ix) $a,b \in A$ e $a\Delta b = 0_A \Rightarrow a = 0_A$ *ou* $b = 0_A$.

Definição 2.1.5. Um domínio é um anel unitário, comutativo e sem divisores de zero.

Definição 2.1.6 Um corpo é anel unitário e comutativo $(A,*,\Delta)$ que satisfaz:

x) $a \in A$ e $a \neq 0 \Rightarrow \exists a^{-1} \in A$ tal que $a\Delta a^{-1} = a^{-1}\Delta a = 1_A$.

a^{-1} é chamado de inverso de a.

Note: Todo domínio é anel unitário e comutativo. Todo corpo é anel unitário e comutativo.

Exemplo 2.1.7 Com operações usuais de adição e multiplicação: $(\mathbb{Z},+,.)$ é domínio que não é corpo; $(\mathbb{Q},+,.)$ e $(\mathbb{R},+,.)$ são corpos.

Exemplo 2.1.8 Em $\mathbb{R}$ definimos as operações:

$$*: \mathbb{R}X\mathbb{R} \to \mathbb{R}$$
$$a*b = a+b-8$$

$$\Delta: \mathbb{R}X\mathbb{R} \to \mathbb{R}$$
$$a\Delta b = a+b-\frac{ab}{8}$$

$(\mathbb{R},*,\Delta)$ é um anel? Se for determinar sua melhor estrutura algébrica.

Verificar os axiomas:

Sejam $a,b,c \in \mathbb{R}$.

i) $a*b = b*a$?

$a*b = a+b-8 = b+a-8 = b*a$.

ii) $a*(b*c) = (a*b)*c$?

$a*(b*c) = a*(b+c-8) = a+(b+c-8)-8 = (a+b-8)+c-8 = (a*b)*c$.

iii) $\exists 0_a \in \mathbb{R}$ tal que $a*0_a = a, \forall a \in \mathbb{R}$?

$$a+0_a-8=a$$
$$0_a=8$$

Logo, o elemento neutro é 8.

iv) $\forall a \in \mathbb{R}$, existe $(-a) \in \mathbb{R}$ tal que $a*(-a)=8$?

$$a*(-a)=8$$

$$a+(-a)-8=8$$

$$(-a)=16-a$$

Logo, o simétrico de a é $16-a$.

v) $(a\Delta b)\Delta c = a\Delta(b\Delta c)$?

$$(a\Delta b)\Delta c=\left(a+b-\frac{a.b}{8}\right)\Delta c$$

$$(a\Delta b)\Delta c=\left(a+b-\frac{a.b}{8}\right)+c-\left(a+b-\frac{a.b}{8}\right)\frac{c}{8}$$

$$(a\Delta b)\Delta c=a+\left(b+c-\frac{b.c}{8}\right)-\frac{c}{8}\left(b+c-\frac{b.c}{8}\right)$$

Logo, $(a\Delta b)\Delta c = a\Delta(b\Delta c)$.

vi) $a\Delta(b*c)=(a\Delta b)*(a\Delta c)$?

$$a\Delta(b*c)=a\Delta(b+c-8)$$

$$a\Delta(b*c)=a+(b+c-8)-\frac{a.(b+c-8)}{8}$$

$$a\Delta(b*c)=\left(a+b-\frac{a.b}{8}\right)+\left(a+c-\frac{a.c}{8}\right)-8$$

Logo, $a\Delta(b*c)=(a\Delta b)*(a\Delta c)$.

Portanto $(\mathbb{R},*,\Delta)$ é anel.

vii) $a\Delta b = b\Delta a$?

$$a\Delta b = a+b-\frac{a.b}{8} = b+a-\frac{b.a}{8} = b\Delta a\,.$$

Logo, $(\mathbb{R},*,\Delta)$ é anel comutativo.

viii) Existe $1_A\mathbb{R}$ tal que $1_A\Delta a = a, \forall a \in \mathbb{R}$?

$$1_A + a - \frac{1_A.a}{8} = a$$
$$1_A - \frac{1_A.a}{8} = 0$$
$$8.1_A - a.1_A = 0$$
$$(8-a).1_A = 0$$
$$1_A = 0$$

Logo, $(\mathbb{R},*,\Delta)$ é anel comutativo unitário.

ix) O anel não tem ddz?

$a\Delta b = 0_A \Rightarrow a = 0_A \quad ou \quad b = 0_A$?
$a\Delta b = 8 \Rightarrow a = 8 \quad ou \quad b = 8$?

$$a+b-\frac{a.b}{8} = 8$$
$$8.a+8.b-a.b = 64$$
$$8.a+b.(8-a) = 64$$
$$b.(8-a) = 64-8.a$$
$$b.(8-a) = 8.(8-a)$$

1°) Se $a = 8$, Ok!

2°) Suponhamos, $a \neq 8$

$$b = \frac{8.(8-a)}{8-a} \Rightarrow b = 8$$

Portanto se $a\Delta b = 8 \Rightarrow a = 8 \quad ou \quad b = 8$.

Logo, não tem ddz, e portanto $(\mathbb{R},*,\Delta)$ é domínio.

x) $(\mathbb{R},*,\Delta)$ é corpo?

$$0_A = 8 \qquad e \qquad 1_A = 0$$

Seja $a \neq 8$. Existe $a^{-1} \in \mathbb{R}$ tal que $a \Delta a^{-1} = 0$?

$$a + a^{-1} - \frac{a.a^{-1}}{8} = 0$$
$$8.a + 8.a^{-1} - a.a^{-1} = 0$$
$$8.a^{-1} - a.a^{-1} = -8a$$
$$a^{-1}(8-a) = -8a$$
$$a^{-1} = -\frac{8a}{8-a}$$
$$a^{-1} = -\frac{8a}{a-8}$$

Logo, $a^{-1} = \frac{8.a}{a-8}$

Portanto, $(\mathbb{R}, *, \Delta)$ é corpo.

Por comodidade, denotaremos as operações de adição e multiplicação do anel A por $+$ e $.$ respectivamente. Também denotaremos 0_A por 0 e 1_A por 1.

Veremos a seguir algumas propriedades aritméticas dos anéis.

Sejam $(A, +, .)$ um anel e $a, b, c \in A$.

1) o zero é único;

2) o simétrico é único;

3) $a.0 = 0.a = 0$

4) $a + b = a + c \Leftrightarrow b = c$

5) $a = b \Rightarrow a.b = a.c$ e $b.a = c.a$

6) $-(-a) = a$

7) $-(a.b) = (-a).b = a.(-b)$

8) $a.(b-c) = a.b - a.c$

9) $(a-b).c = a.c - b.c$

10) $-(a+b) = -a - b$

11) $(-a)(-b) = a.b$

Quando A tem unidade vale:

12) A unidade é única

13) Se $a \in A, a \neq 0$, e a tem inverso em A então o inverso de a é único.

Demonstração: (1) Sabemos que o anel A tem um zero que denotamos por 0_A. Suponha que exista outro zero em A, que indicaremos por x.

Como 0_A é elemento neutro da adição vale $0_A + x = x$.

Como x é elemento neutro da adição vale $0_A + x = 0_A$.

Das igualdades acima concluímos que $x = 0_A$, e portanto 0_A é único elemento simétrico do anel A.

(2) Seja $a \in A$. Sabemos que a tem um simétrico $-a \in A$. Suponha que $x \in A$ também é simétrico de a.

$x = x + 0$ (0 é elemento neutro para A)

$x = x + (a + (-a))$ ($-a$ é simétrico de a)

$x = (x + a) + (-a)$ (axioma (ii))

$x = 0 + (-a)$ (pois x é simétrico de a)

$x = -a$ (0 é elemento neutro de a)

Logo $x = -a$ e então $-a$ é o único simétrico de a.

(3) Seja $a \in A$. Verificaremos que $a.0 = 0$. A igualdade $0.a = 0$ se prova de forma análoga. Pelo axioma (iii) temos:

$0 = 0 + 0$ (multiplique por a à esquerda)

$a.0 = a.(0 + 0)$ (Use o axioma (vi))

$a.0 = a.0 + a.0$ (Some o simétrico x de $a.0$, que existe pelo axioma (iv))

$a.0 + x = (a.0 + a.0) + x$ (Use o axioma (ii))

$a.0 + x = a.0 + (a.0 + x)$ $(a.0 + x = 0)$

$0 = a.0 + 0$ $(a.0 + 0 = a.0)$

$0 = a.0$

(4) $(\Rightarrow) a+b=a+c$ (Some $-a$ à esquerda)

$-a+(a+b)=-a+(a+c)$ (Use o axioma (ii))

$(-a+a)+b=(-a+a)+c$ $(-a+a=0)$

$0+b=0+c$ (0 é o elemento neutro)

$b=c$

$(\Leftarrow)$ Desde que $+$ é a operação em A, ela associa a cada par de elementos de A um único elemento de A. Como $b=c$ temos que os pares (a,b) e (a,c) são os mesmos em $A\times A$, assim $a+b=a+c$.

(5) É análoga a $(\Leftarrow)$ da propriedade anterior, trocando $+$ por $.$. De fato, como $b=c$ os pares (a,b) e (a,c) coincidem em AXA, e a operação multiplicação associa a cada par de elementos de A um único elemento de A. Portanto, $a.b=a.c$. Da mesma maneira verifica-se que $c.a=b.a$.

(6) Como $-a$ é o simétrico de a valem as igualdades $a+(-a)=(-a)+a=0$. Isso mostra que a é o simétrico de $-a$. Desde que o símbolo $-$ indica o simétrico temos $-(-a)=a$.

(7) $(-a).b+a.b=(-a+a).b$ (axioma (vi))

$(-a).b+a.b=0.b$

$(-a).b+a.b=0$ (Propriedade (3))

Analogamente verifica-se que $a.b+(-a).b=0$. Isso mostra que $(-a).b$ é simétrico de $a.b$. Pela unidade do simétrico vista a propriedade (2) vem que $-(a.b)=(-a).b$.

A igualdade $-(a.b)=a.(-b)$ pode ser verificada da mesma forma.

(8) $a.(b-c)=a(b+(-c))$

$a.(b-c)=a.b+a.(-c)$ (Axioma (vi))

$a.(b-c)=a.b+(-a.c)$ (Propriedade (7))

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

(9) A prova é idêntica à feita acima.

(10) $a+b+(-a)+(-b)=a+(-a)+b+(-b)$ (axiomas (i) e (ii))

$a+b+(-a)+(-b)=0+0$

$a+b+(-a)+(-b)=0$

Analogamente, $(-a)+(-b)+a+b=0$. Segue que o simétrico de $a+b$ é $(-a)+(-b)=-a-b$. Portanto, $-(a+b)=-a-b$.

(11) $(-a).(-b)=-(a.(-b))$ (Propriedade (7))

$(-a).(-b)=-(-a.b)$ (Propriedade (7))

$(-a).(-b)=a.b$ (Propriedade (6))

(12) É idêntica a que fizemos na propriedade (1) trocando 0_A por 1 e trocando $+$ por $.$.

(13) Análoga a demonstração da propriedade (2), trocando $-a$ por a^{-1}, trocando 0 por 1 e trocando $+$ por $.$.

■

Vamos provar que todo corpo é domínio.

Proposição 2.1.9 Se A é corpo, então A é domínio.

Demonstração: Seja A um corpo, então A é anel unitário, comutativo e vale (x).

Precisamos provar que A é sem divisores de zero.

Sejam $a,b \in A$ tais que $a.b=0$. Se $a=0$, acabou.

Assuma $a \neq 0$. Então existe $a^{-1} \in A$ a A. Multiplicando a igualdade $a.b=0$ por a^{-1} teremos:

$a^{-1}.(a.b)=a^{-1}.0$

$(a^{-1}.a).b=0$

$1.b=0$

$b=0$.

Portanto A é domínio.

■

Nosso próximo objetivo é construir os anéis $\mathbb{Z}_n, n \in \mathbb{N}$ e $n>1$, chamados de anéis de classes de restos. Iniciamos com a definição de congruência modulo n.

Definição 2.1.10 Sejam $x, y \in \mathbb{Z}$ e $n \in \mathbb{N}$, $n>1$. Dizemos que x é congruente a y módulo n quando n divide x – y.

Notação: $x \equiv y (\mathrm{mod}\, n)$

Note que: $x \equiv y (\mathrm{mod}\, n) \Leftrightarrow n \backslash (x-y)$

Exemplos 2.1.11 $7 \equiv 2 (\mathrm{mod}\, 5)$, pois $5 \backslash (7-2)$.

Ex.: $-17 \equiv 3 (\mathrm{mod}\, 5)$, pois $5 \backslash (-17-3)$

Ex.: $5 \equiv -1 (\mathrm{mod}\, 6)$, pois $6 \backslash (5-(-1))$

Ex.: $-1 \equiv (n-1).(\mathrm{mod}\, n)$, pois $n \backslash (-1-(n-1))$ isto é, $n \backslash (-n)$.

Lema 2.1.12 A congruência módulo n é uma relação de equivalência em $\mathbb{Z}$. Isto é:

1) $x \equiv x (\mathrm{mod}\, n)$ - Reflexiva

2) $x \equiv y (\mathrm{mod}\, n) \Rightarrow y \equiv x (\mathrm{mod}\, n)$ - Simétrica

3) $x \equiv y (\mathrm{mod}\, n)$ e $x \equiv z (\mathrm{mod}\, n) \Rightarrow x \equiv z (\mathrm{mod}\, n)$ - Transitiva

Demonstração:

(1) $n \backslash x - x \Rightarrow x \equiv x (\mathrm{mod}\, n)$

(2) $x \equiv y (\mathrm{mod}\, n) \Rightarrow n \backslash -(x-y) \Rightarrow n \backslash (y-x) \Rightarrow y \equiv x (\mathrm{mod}\, n)$

(3) $\left.\begin{array}{l} x \equiv y (\mathrm{mod}\, n) \Rightarrow n \backslash (x-y) \\ x \equiv z (\mathrm{mod}\, n) \Rightarrow n \backslash (x-z) \end{array}\right\} \Rightarrow n \backslash (x-y+x-z) \Rightarrow n \backslash (x-z) \Rightarrow x \equiv z (\mathrm{mod}\, n)$

■

Definição 2.1.13 A classe de equivalência de $x \in \mathbb{Z}$ modulo n é o conjunto

$$\bar{x} = \{y \in \mathbb{Z}; y \equiv x (\mathrm{mod}\, n)\}.$$

Notação:

$x+n.\mathbb{Z}=\{x+n.a;a\in\mathbb{Z}\}$.

Note que:

$$y\in\bar{x}\Leftrightarrow y\equiv x(\mathrm{mod}\,n)\Leftrightarrow n\backslash(y-x)\Leftrightarrow y-x=n.a,a\in\mathbb{Z}\Leftrightarrow y=x+n.a\Leftrightarrow y\in x+n.\mathbb{Z}$$

Portanto, $\bar{x}=x+n.\mathbb{Z}$.

O conjunto de todas as classes de equivalência módulo n é denotado por $\mathbb{Z}_n$ isto é, $\mathbb{Z}_n=\{\bar{x},x\in\mathbb{Z}\}$

Outra notação para $\mathbb{Z}_n$ é $\frac{\mathbb{Z}}{n\mathbb{Z}}$, isto é, $\mathbb{Z}_n=\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Lembre que $\bar{x}=x+n.\mathbb{Z}=\{x+na,a\in\mathbb{Z}\}$

Exemplo 2.1.14 $n=2;\mathbb{Z}_2=\{\bar{x};x\in\mathbb{Z}\}$

$\bar{0}=0+2.\mathbb{Z}=\{2.a;a\in\mathbb{Z}\}$ - Números Pares

$\bar{1}=1+2.\mathbb{Z}=\{1+2.a;a\in\mathbb{Z}\}$ - Números Ímpares

$\bar{2}=2+2.\mathbb{Z}=\{2+2.a;a\in\mathbb{Z}\}=\bar{0}=\bar{4}$

$\bar{3}=3+2.\mathbb{Z}=\{3+2.a;a\in\mathbb{Z}\}=\bar{1}=\bar{5}$

$-\bar{1}=-1+2.\mathbb{Z}=\{-1+2.a;a\in\mathbb{Z}\}=\bar{1}$

$-\bar{2}=-2+2.\mathbb{Z}=\{-2+2.a;a\in\mathbb{Z}\}=\bar{0}$

$-\bar{3}=-3+2.\mathbb{Z}=\{-3+2.a;a\in\mathbb{Z}\}=\bar{1}$

$\vdots$

Logo, $\mathbb{Z}_2=\{\bar{0},\bar{1}\}$

Exemplo 2.1.15 $n=3;\mathbb{Z}_3=\{\bar{x};x\in\mathbb{Z}\}$

$\bar{0}=0+3.\mathbb{Z}$ - Múltiplos de 3

$\bar{1} = 1+3.\mathbb{Z}$ - Múltiplos de 3 e somado com 1

$\bar{2} = 2+3.\mathbb{Z}$ - Múltiplos de 3 somado com 2

$\bar{3} = 3+3.\mathbb{Z} = \bar{0}$

$\bar{4} = 4+3.\mathbb{Z} = \bar{1} \ \left(4+3.a = 1+3+3.a = 1+3(a+1)\right)$

$\bar{5} = 5+3.\mathbb{Z} = \bar{2} \ \left(5+3.a = 2+3+3.a = 2+3(a+1)\right)$

$\bar{6} = 6+3.\mathbb{Z} = \bar{0}$

$-\bar{1} = -1+3.\mathbb{Z} = \bar{2} \ \left(-1+3.a = -3+2+3.a = 2+3(a-1)\right)$

$-\bar{2} = -2+3.\mathbb{Z} = \bar{1} \left(-2+3.a = -3+1+3.a = 1+3(a-1)\right)$

$-\bar{3} = -3+3.\mathbb{Z} = \bar{0}$

$\vdots$

Logo, $\mathbb{Z}_3 = \left\{\bar{0}, \bar{1}, \bar{2}\right\}$.

Lema 2.1.16 Sejam $x, y \in \mathbb{Z}$ e $n \in \mathbb{N}$, $n > 1$. Então:

$$\bar{x} = \bar{y} \Leftrightarrow x \equiv y \pmod{n}$$

Demonstração:

$(\Rightarrow) x \equiv x \pmod{n} \Rightarrow x \in \bar{x} = \bar{y} \Rightarrow x \in \bar{y} \Rightarrow x \equiv y \pmod{n}$

$(\Leftarrow)$ Mostrar $\bar{x} \subseteq \bar{y}$ e $\bar{y} \subseteq \bar{x}$.

$$(\subseteq) \left.\begin{matrix} z \in \bar{x} \Rightarrow z \equiv x \pmod{n} \\ x \equiv y \pmod{n} \end{matrix}\right\} \Rightarrow z \equiv y \pmod{n}$$

$z \equiv y \pmod{n} \Rightarrow z \in \bar{y}$

$$(\supseteq) \left.\begin{matrix} z \in \bar{y} \Rightarrow z \equiv y \pmod{n} \\ y \equiv x \pmod{n} \end{matrix}\right\} \Rightarrow z \equiv x \pmod{n}$$

$z \equiv x \pmod{n} \Rightarrow z \in \bar{x}$.

Note que: $x=y \Rightarrow n \backslash x-y \Rightarrow x \equiv y(\text{mod}\, n) \Rightarrow \bar{x}=\bar{y}$

■

Ex.: $n=3; \mathbb{Z}_3=\{\bar{0},\bar{1},\bar{2}\}$

$\overline{16}=\bar{1}$, pois $16 \equiv 1(\text{mod}\, 3)$

$\overline{-27}=\bar{0}$, pois $-27 \equiv 0(\text{mod}\, 3)$

$\overline{-13}=\bar{2}$, pois $-13 \equiv 2(\text{mod}\, 3)$

Proposição 2.1.17 Se $n \in \mathbb{N}, n>1$, então $\mathbb{Z}_n=\{\bar{0},\bar{1},\bar{2},...,\overline{n-1}\}$ é um conjunto com exatamente n elementos.

Demonstração: Pela definição de $\mathbb{Z}_n$ é claro que $\{\bar{0},\bar{1},\bar{2},...,\overline{n-1}\} \subseteq \mathbb{Z}_n$. Vamos ver a inclusão contrária. Para isso, tome $\bar{a} \subseteq \mathbb{Z}_n$. Como $a \subseteq \mathbb{Z}_n$ e $n \in \mathbb{N}, n \geq 2$, podemos dividir a e n obtendo quociente $q \in \mathbb{Z}$ e resto $n \in \mathbb{N}$.

$$a=nq+r,\ 0 \leq r < n$$

$$a-r=n.q \Rightarrow a \equiv r(\text{mod}\, n)$$

Pelo Lema 2.1.16 vem que $\bar{a} \equiv \bar{r}$.

Mas como $r \in \{0,1,...,n-1\}$ temos $\bar{a} \equiv \bar{r} \in \{\bar{0},\bar{1},...,\overline{n-1}\}$. Para provar que $\mathbb{Z}_n$ tem exatamente n elementos devemos mostrar que os elementos de $\{\bar{0},\bar{1},...,\overline{n-1}\}$ são distintos dois a dois. Suponha que isso não é verdade, isto é, suponha que existem $x, y \in \{0,1,...,n-1\}$ com $x \neq y$ e $\bar{x}=\bar{y}$. Sem perda de generalidade vamos assumir que $x<y$. Como $\bar{x}=\bar{y}$, o Lema 2.1.6 assegura que $x \equiv y(\text{mod}\, n)$ e daí $n \backslash (y-x)$. Mas $0<y-x<n$ e $n \backslash (y-x)$ é impossível. Portanto, nossa suposição não pode ser feita e os elementos de $\{\bar{0},\bar{1},...,\overline{n-1}\}$ são dois a dois distintos.

■

Exemplo 2.1.18 $\mathbb{Z}_2=\{\bar{0},\bar{1}\}$ $\quad \bar{0}=0+2.\mathbb{Z}$ e $\bar{1}=1+2\mathbb{Z}$

Exemplo 2.1.19 $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{3}\}$ $\bar{0} = 0 + 3.\mathbb{Z}$, $\bar{1} = 1 + 3\mathbb{Z}$ e $\bar{2} = 2 + 3\mathbb{Z}$

Objetivo: Mostrar que $\mathbb{Z}_n$ é um anel.

Sejam $\bar{x}, \bar{y} \in \mathbb{Z}_n$. Defina:

$$\bar{x} + \bar{y} = \overline{x+y}$$

$$\bar{x} . \bar{y} = \overline{x.y}$$

$$+ : \mathbb{Z}_n x \mathbb{Z}_n \to \mathbb{Z}_n$$
$$(\bar{x}, \bar{y}) \to \overline{x+y}$$

$$. : \mathbb{Z}_n x \mathbb{Z}_n \to \mathbb{Z}_n$$
$$(\bar{x}, \bar{y}) \to \overline{x.y}$$

Veremos na Proposição 2.1.22 as operações de adição e multiplicação em $\mathbb{Z}_n$ estão bem definidas. Iniciamos com um exemplo.

Exemplo 2.1.20 Em $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$\bar{1} = \overline{15}$ e $\bar{3} = \overline{10}$

$(\bar{1}, \bar{3}) = (\overline{15}, \overline{10})$

$\bar{4} = \overline{25}$, pois $25 \equiv 4 (\text{mod } 7)$ e $\bar{3} = \overline{150}$, pois $150 \equiv 3 (\text{mod } 7)$.

Queremos provar que:

$$(\bar{x}, \bar{y}) = (\bar{a}, \bar{b}) \Rightarrow \begin{cases} \overline{x.y} = \overline{a.b} \\ \overline{x+y} = \overline{a+b} \end{cases} \text{ ou } \bar{x} = \bar{a} \text{ e } \bar{y} = \bar{b} \Rightarrow \begin{cases} \overline{x.y} = \overline{a.b} \\ \overline{x+y} = \overline{a+b} \end{cases}$$

Para provar isso, escreveremos o Lema abaixo.

Lema 2.1.21 Sejam $n \in \mathbb{N}, n > 1$ e $a, b, x, y \in \mathbb{Z}$. Se $x \equiv a (\text{mod } n)$ e $y \equiv b (\text{mod } n)$, então:

1) $x + y \equiv a + b (\text{mod } n)$

2) $x.y \equiv a.b (\text{mod } n)$

Demonstração:

$$(1)\ \left.\begin{array}{l} x\equiv a(\mathrm{mod}\,n)\Rightarrow n\backslash(x-a) \\ y\equiv b(\mathrm{mod}\,n)\Rightarrow n\backslash(y-b) \end{array}\right\}\Rightarrow n\backslash(x-a+y-b)\Rightarrow n\backslash(x+y-(a+b))\Rightarrow x+y\equiv a+b(\mathrm{mod}\,n)$$

$$(2)\ \left.\begin{array}{l} x\equiv a(\mathrm{mod}\,n)\Rightarrow n\backslash(x-a)\Rightarrow n\backslash(xy-ay) \\ y\equiv b(\mathrm{mod}\,n)\Rightarrow n\backslash(y-b)\Rightarrow n\backslash(ay-ab) \end{array}\right\}\Rightarrow n\backslash(xy-ay+ay-ab)\Rightarrow n\backslash(xy-ab)\Rightarrow xy\equiv ab(\mathrm{mod}\,n)$$

■

Proposição 2.1.22 Sejam $n\in\mathbb{N}, n>1$. Se $\bar{x}=\bar{a}$ e $\bar{y}=\bar{b}$, então:

1) $\bar{x}+\bar{y}=\bar{a}+\bar{b}$

2) $\overline{x.y}=\bar{a}.\bar{b}$

Demonstração:

Como $\bar{x}=\bar{a}$ e $\bar{y}=\bar{b}$, pelo Lema 2.1.16 temos $x\equiv a(\mathrm{mod}\,n)$ e $y\equiv b(\mathrm{mod}\,n)$. Pelo Lema 2.1.21 temos $x+y\equiv a+b(\mathrm{mod}\,n)$ e $x.y\equiv a.b(\mathrm{mod}\,n)$, portanto, $\overline{x+y}=\overline{a+b}$ e $\overline{x.y}=\overline{a.b}$ então $\bar{x}+\bar{y}=\bar{a}+\bar{b}$ e $\bar{x}.\bar{y}=\bar{a}.\bar{b}$.

■

Teorema 2.1.23 Sejam $n\in\mathbb{Z}, n\geq 1$. Então $(\mathbb{Z}_n,+,.)$ é anel comutativo com unidade $\bar{1}$. Isto é, os seguintes axiomas são verificados:

i) $\bar{x}+\bar{y}=\bar{y}+\bar{x}$

ii) $\bar{x}+(\bar{y}+\bar{z})=(\bar{x}+\bar{y})+\bar{z}$

iii) $\bar{x}+\bar{0}=\bar{0}+\bar{x}=\bar{x}$

iv) $\bar{x}+(-\bar{x})=(-\bar{x})+\bar{x}=\bar{0}$

v) $\bar{x}.(\bar{y}.\bar{z})=(\bar{x}.\bar{y}).\bar{z}$

vi) $\bar{x}.(\bar{y}+\bar{z})=\bar{x}.\bar{y}+\bar{x}.\bar{z}$

$(\bar{y}+\bar{z}).\bar{x}=\bar{y}.\bar{x}+\bar{z}.\bar{x}$

vii) $\bar{x}.\bar{y}=\bar{y}.\bar{x}$

viii) $\bar{x}.\bar{1} = \bar{1}.\bar{x} = \bar{x}$

Demonstração: Sejam $x, y, z \in \mathbb{Z}$ e $\bar{x}, \bar{y}, \bar{z}, \bar{0}, \bar{1} \in \mathbb{Z}_n$:

i) $\bar{x} + \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} + \bar{x}$

ii) $\bar{x} + (\bar{y} + \bar{z}) = (\bar{x} + \bar{y}) + \bar{z}$

$\bar{x} + (\bar{y} + \bar{z}) = \bar{x} + \overline{(y+z)} = \overline{x + (y+z)}$

Como $x + (x+z) = (x+y) + z$, temos

$\bar{x} + (\bar{y} + \bar{z}) = \overline{x + (y+z)} = \overline{(x+y) + z} = \overline{(x+y)} + \bar{z} = (\bar{x} + \bar{y}) + \bar{z}.$

iii) $\bar{x} + \bar{0} = \bar{0} + \bar{x} = \bar{x}$

$\bar{x} + \bar{0} = \overline{x+0} = \overline{0+x} = \bar{x}$

iv) $\bar{x} + (-\bar{x}) = (-\bar{x}) + \bar{x} = \bar{0}$

$\bar{x} + (-\bar{x}) = \overline{x + (-x)}$

Pela comutatividade vista em (i) temos $\overline{(-x)} + \bar{x} = \bar{x} + \overline{(-x)} = \bar{0}$.

v) $\bar{x}.(\bar{y}.\bar{z}) = (\bar{x}.\bar{y}).\bar{z}$

$\bar{x}.(\bar{y}.\bar{z}) = \bar{x}.\overline{(y.z)} = \overline{x(y.z)} = \overline{(x.y)z} = \overline{(x.y)}.\bar{z} = (\bar{x}.\bar{y}).\bar{z}$

vi) $\bar{x}.(\bar{y} + \bar{z}) = \bar{x}.\bar{y} + \bar{x}.\bar{z}$

$\bar{x}.(\bar{y} + \bar{z}) = \bar{x}.\overline{(y+z)} = \overline{x.(y+z)} = \overline{x.y + x.z} = \bar{x}.\bar{y} + \bar{x}.\bar{z}$

$(\bar{y} + \bar{z}).\bar{x} = \overline{(y+z)}.\bar{x} = \overline{(y+z).x} = \overline{y.x + z.x} = \overline{y.x} + \overline{z.x} = \bar{y}.\bar{x} + \bar{z}.\bar{x}.$

vii) $\bar{x}.\bar{y} = \bar{y}.\bar{x}$

$\bar{x}.\bar{y} = \overline{x.y} = \overline{y.x} = \bar{y}.\bar{x}$.

viii) $\bar{x}.\bar{1} = \bar{1}.\bar{x} = \bar{x}$

$\bar{x}.\bar{1} = \overline{x.1} = \overline{1.x} = \bar{x}.$

■

Veremos agora exemplos de tabelas de operações em $\mathbb{Z}_n$, para n=2,3 e 4.

Exemplo 2.1.24 $n=2, \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

.	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Exemplo 2.1.25 $n=3, \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Exemplo 2.1.26 $n=4, \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Seja $n \in \mathbb{N}, n>1$. Se n não é um número primo podemos escrever $n=a.b$, com $1<a<n$ e $1<b<n$, a, b $\in \mathbb{Z}$.

Segue que $\bar{a}, \bar{b} \in \mathbb{Z}_n, \bar{a} \neq \bar{0}$ e $\bar{b} \neq \bar{0}$.

Assim,

$$\bar{a}.\bar{b} = \overline{a.b} = \bar{n} = \bar{0}, \text{Pois } n \equiv 0 (\text{mod } n).$$

Concluímos que:

$\mathbb{Z}_n$ não é domínio quando n não é primo.

O próximo teorema mostra a recíproca da conclusão acima e também que $\mathbb{Z}_n$ é corpo se, e somente se, n é um numero primo.

Teorema 2.1.27 Seja $n \in \mathbb{Z}, n \geq 1$. As condições abaixo são equivalentes:

a) $\mathbb{Z}_n$ é domínio

b) n é número primo

c) $\mathbb{Z}_n$ é corpo

Demonstração: (a) $\Rightarrow$ (b) Seja $x \in \mathbb{N}$ um divisor de n. Devemos provar que $x=1$ ou $x=n$. Como x divide n, existe $y \in \mathbb{N}$ tal que $n = x.y$. Desde que $\mathbb{Z}_n$ é domínio,

$$\bar{0} = \bar{n} = \overline{x.y} \Rightarrow \bar{x} = \bar{0} \text{ ou } \bar{y} = \bar{0}$$

1° Caso: $\bar{x} = \bar{0}$

$$\bar{x} = \bar{0} \Rightarrow x \equiv 0 (\text{mod } n) \Rightarrow n \backslash x$$

Como $n \backslash x$, $x \backslash n$ e $x, n \in \mathbb{N}$, temos $x = n$.

2° Caso: $\bar{y} = \bar{0}$

$$\bar{y} = \bar{0} \Rightarrow y \equiv 0 (\text{mod } n) \Rightarrow n \backslash y \Rightarrow nt = y \text{ para algum } t \in \mathbb{N}.$$

Substituindo os valores de y em $n = x.y$ vem que $n = x.n.t$. Como $\mathbb{Z}$ é domínio e $n \neq 0$, cancelamos n obtendo $x.t = 1$. Portanto $x = 1$.

(b) $\Rightarrow$ (c) Já sabemos que $\mathbb{Z}_n$ é anel unitário e comutativo. Para ver que é corpo devemos mostrar que todo elemento $\bar{x} \in \mathbb{Z}_n, \bar{x} \neq \bar{0}$, tem inverso em $\mathbb{Z}_n$. Desde que $\bar{x} \neq \bar{0}$ podemos admitir $x = \{1, 2, ..., n-1\}$ e como n é primo temos $mdc(n, x) = 1$. Pela Identidade de Beuzout, existem $r, s \in \mathbb{Z}$ tais que $n.r + x.s = 1$. Tomando classes módulo n vem que

$$\bar{1} = \overline{n.r + s.x} = \overline{n.r} + \overline{s.x} = \overline{n.r} + \overline{x.s} = \bar{0}.r + \overline{x.s} = \bar{0} + \overline{x.s} = \overline{x.s}.$$

Portanto, $\bar{s}$ é o inverso de $\bar{x}$ e $\mathbb{Z}_n$ é corpo.

(c) $\Rightarrow$ (a) Já vimos na Proposição 2.1.9 que todo corpo é domínio.

■

2.2 Subanel e Ideal

Sejam $(A, +, .)$ um anel e $B \subseteq A, B \neq \varnothing$. Dizemos que B é fechado com as operações de A quando:

$x, y \in B \Rightarrow x + y \in B$ e $x.y \in B$.

Isto é, as operações de A também são operações em B.

Exemplo 2.2.1 O conjunto $B = 2.\mathbb{Z} = \{2.x; x \in \mathbb{Z}\}$ é fechado com as operações do anel $(\mathbb{Z}, +, .)$.

$2.x, 2.y \in B \Rightarrow 2.x + 2.y = 2.(x + y) \in B$

$2.x, 2.y \in B \Rightarrow 2.x.2.y = 2.(2x.y) \in B$

Exemplo 2.2.2 O conjunto $B = \{2.x + 1; x \in \mathbb{Z}\} = 1 + 2.\mathbb{Z}$ não é fechado com as operações do anel $(\mathbb{Z}, +, .)$.

$3 \in B, 5 \in B$ porém $3 + 5 \notin B$.

Definição 2.2.3 Se $(B, +, .)$ for um anel com as operações de $(A, +, .)$, dizemos que B é subanel de A.

Sejam $(A, +, .)$ um anel e $(B, +, .)$ um subanel de A. Então os seguintes axiomas são verificados em B:

i) $x + y = y + x, \forall x, y \in B$.

ii) $(x + y) + z = x + (y + z), \forall x, y, z \in B$.

iii) Existe $0_B \in B$ tal que $0_B + x = x + 0_B = x, \forall x \in B.$

Logo, B tem elemento neutro para adição e $0_B = 0_A$.

iv) Dados $x \in B$, existe $(-x) \in B$ tal que $x + (-x) = (-x) + x = 0_B$.

v) $x.(y.z) = (x.y).z, \forall x, y, z \in B$

vi) $x.(y+z) = x.y + x.z, \forall x, y, z \in B$

$(y+z).x = y.x + z.x$

Exemplo 2.2.4 Com as operações usuais, $(\mathbb{Z}, +, .)$ é subanel $(\mathbb{Q}, +, .)$. Porém, $(\mathbb{N}, +, .)$ não é subanel de $(\mathbb{Z}, +, .)$.

De fato , $2 \in \mathbb{N}$, porém $-2 \notin \mathbb{N}$

Proposição 2.2.5 Sejam $(A, +, .)$ um anel e $B \subseteq A, B \neq \varnothing$. São equivalentes:

a) B é subanel de A.

b) $x, y \in B \Rightarrow x - y \in B$ e $x.y \in B.$

Demonstração:

a) $\Rightarrow$ b)

$x, y \in B$ e B é subanel.

$x, y, -y \in B \Rightarrow x.y \in B \ \ e \ \ x - y = x + (-y) \in B$

b) $\Rightarrow$ a)

Por hipótese, a multiplicação de A é fechada em B.

iii) Elemento Neutro.

$B \neq \varnothing \Rightarrow \exists a \in B$

$a, a \in B \Rightarrow 0_A = a - a \in B$

iv) Elemento Simétrico.

$b \in B \Rightarrow b, 0_A \in B \Rightarrow 0_A - b \in B \Rightarrow -b \in B.$

Provar que a adição é fechada em B.

. $x, y \in B$

$x, -y \in B \Rightarrow x-(-x) \in B \Rightarrow x+y \in B$

Os axiomas (i), (ii), (v) e (vi) são hereditários, isto é, valem em B pois valem em A.

■

Observações 2.2.6 Vimos na prova da Proposição 2.2.5 que:

1) Se B é subanel de A, então $0_B = 0_A$.

2) Se B é subanel de A e $b \in B$, então o simétrico de b é o mesmo em A e B.

Notação: Para indicar que B é subanel de A, usa-se a notação $B \leq A$.

Exemplo 2.2.7 Se A é anel então $\{0\}$ e A são subanéis de A. Isto é, $\{0\} \leq A$ e $A \leq A$.

Os subanéis $\{0\}$ e A são chamados subanéis triviais.

Exemplo 2.2.8 O conjunto $\bar{2}\mathbb{Z}_4 = \{\bar{0}, \bar{2}\}$ é subanel de $\mathbb{Z}_4$

$\bar{0}.\bar{0} = \bar{0} \in \{\bar{0}, \bar{2}\}$

$\bar{0}.\bar{2} = \bar{0} \in \{\bar{0}, \bar{2}\}$

$\bar{2}.\bar{2} = \bar{0} \in \{\bar{0}, \bar{2}\}$

$\bar{0} - \bar{2} = \overline{-2} = \bar{2} \in \{\bar{0}, \bar{2}\}$

$\bar{2} - \bar{0} = \bar{2} \in \{\bar{0}, \bar{2}\}$

$\bar{0} - \bar{0} = \bar{0} \in \{\bar{0}, \bar{2}\}$

$\bar{2} - \bar{2} = \bar{0} \in \{\bar{0}, \bar{2}\}$

Estudaremos agora os ideais, que são uma classe especial de subanéis. Os ideais serão necessários para o estudo de um anel quociente que faremos no próximo capitulo.

Exemplo 2.2.9 O conjunto $B = \{\bar{0}, \bar{3}\}$ não é subanel de $\mathbb{Z}_4$.

$\bar{3}.\bar{3} = \bar{1} \notin B$.

Exemplo 2.2.10 Seja $n \in \mathbb{N}, n > 1$. Lembre-se que $n.\mathbb{Z} = \{n.x; x \in \mathbb{Z}\}$. Então $n.\mathbb{Z} \leq \mathbb{Z}$, e $n.\mathbb{Z}$ não tem unidade.

Inicialmente vamos provar que $n.\mathbb{Z} \leq \mathbb{Z}$.

Sejam $u, v \in n.\mathbb{Z}$. Então $u = n.x$ e $v = n.y$, com $x, y \in \mathbb{Z}$.

. $u.v = nx.ny = n(xny) \in n.\mathbb{Z}$.

. $u - v = nx - ny = n(x - y) \in n.\mathbb{Z}$.

Segue da Proposição 2.2.5 que $n.\mathbb{Z} \leq \mathbb{Z}$.

Suponha que $n.\mathbb{Z}$ tem unidade u.

$$u \in n.\mathbb{Z} \Rightarrow u = nx, \ x \in \mathbb{Z}.$$

Como u é unidade, temos que

$$u.n = n \Rightarrow nx.n = n \Rightarrow nx = 1 \Rightarrow n = \pm 1.$$

Absurdo, pois $n \geq 2$.

Portanto, $n.\mathbb{Z}$, $n \geq 2$, é subanel sem unidade.

Em particular.

$2.\mathbb{Z} \leq \mathbb{Z}$

$3.\mathbb{Z} \leq \mathbb{Z}$

$4.\mathbb{Z} \leq \mathbb{Z}$

$5.\mathbb{Z} \leq \mathbb{Z}$

$\vdots$

Note que $4.\mathbb{Z} \leq 2.\mathbb{Z}$, $6.\mathbb{Z} \leq 2.\mathbb{Z}$, $6.\mathbb{Z} \leq 3.\mathbb{Z}$ e $6.\mathbb{Z}$ não é subanel de $4.\mathbb{Z}$(pois $6.\mathbb{Z} \not\leq 4.\mathbb{Z}$).

Proposição 2.2.11 $n.\mathbb{Z} \leq m.\mathbb{Z} \Leftrightarrow m \backslash n$.

Demonstração: $(\Rightarrow)$ Mostrar que $m \backslash n$.

Temos: $n = n.1 \in n.\mathbb{Z} \leq m.\mathbb{Z}$.

$n = m.x$, logo, $m \backslash n$.

($\Leftarrow$) Mostrar que $n.\mathbb{Z} \subseteq m.\mathbb{Z}$.

Seja $n.x \in n.\mathbb{Z}$. Como $m \setminus n$, existe $a \in \mathbb{Z}$ tal que $m.a = n$ e $n.x = \mathrm{m}(ax) \in m.\mathbb{Z}$.

Segue da Proposição acima que para reconhecer os anéis que para conhecer os anéis $m.\mathbb{Z}$ que têm $n.\mathbb{Z}$ como subanel, basta conhecer os divisores de n.

■

Exemplo 2.2.12

$\mathbb{Z}$
|
$2.\mathbb{Z}$
|
$4.\mathbb{Z}$
|
$8.\mathbb{Z}$
|
⋮

Exemplo 2.2.13 Achar anéis $m.\mathbb{Z}$ que tem $6.\mathbb{Z}$ como subanel.

$6 = 2.3 \Rightarrow$ divisores de 6 são 1, 2, 3 e 6.

$6.\mathbb{Z} \leq \mathbb{Z}$, $6.\mathbb{Z} \leq 2.\mathbb{Z}$, $6.\mathbb{Z} \leq 3.\mathbb{Z}$ e $6.\mathbb{Z} \leq 6.\mathbb{Z}$.

Exemplo 2.2.14 $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ não é subanel de $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$, pois $\mathbb{Z}_2 \not\subseteq \mathbb{Z}_3$.

$\bar{0} \in \mathbb{Z}_2 \Rightarrow \bar{0} = 0 + 2.\mathbb{Z} = 2.\mathbb{Z}$

$\bar{0} \in \mathbb{Z}_3 \Rightarrow \bar{0} = 0 + 3.\mathbb{Z} = 3.\mathbb{Z}$

Definição 2.2.15 Seja A um anel. Um subconjunto $I \subseteq A, I \neq \varnothing$, é ideal à esquerda de A quando:

. $a, b \in I \Rightarrow a - b \in I$

. $a \in I \; e \; r \in A \Rightarrow r.a \in I \left(A.I \subseteq I\right)$

Definição 2.2.16 Seja A um anel. Um subconjunto $I \subseteq A, I \neq \varnothing$, é um ideal à direita de A quando:

. $a, b \in I \Rightarrow a - b \in I$

. $a \in I \, e \, r \in A \Rightarrow a.r \in I (I.A \subseteq I)$

Definição 2.2.17 Sejam A um anel e $I \subseteq A, I \neq \varnothing$. Se I é ideal à direita e à esquerda de A, dizemos que I é um ideal (ou ideal bilateral) de A.

Observação 2.2.18 Se A é anel comutativo, as definições de ideal à direita e à esquerda coincidem. Neste caso, falamos apenas de ideal.

Comentário: Note que todo ideal à esquerda, à direita ou bilateral é um subanel.

Portanto, os ideais formam uma classe especial de subanéis.

Seja I um ideal à esquerda de $A.$. Vamos verificar que I é subanel de A.

Sejam $a,b \in I$. Devemos provar que $a-b \in I$ e $a.b \in I$.

. $a.b \in I$ e I é ideal $(\Rightarrow) a-b \in I$.

. $b \in I, a \in I \subseteq A \Rightarrow a.b \in I$.

Agora, seja I um ideal à direita de A. Vamos verificar que I é subanel de A.

Sejam $a.b \in I$. Devemos provar que $a-b \in I$ e $a.b \in I$.

. $a.b \in I$ e I é ideal $\Rightarrow a-b \in I$.

. $a \in I, b \in I \subseteq A \Rightarrow a.b \in I$.

Exemplo 2.2.19 Subanel que não é ideal. Sabemos que $\mathbb{Z}$ é subanel de $\mathbb{Q}$.

No entanto, $\mathbb{Z}$ não é ideal de $\mathbb{Q}$ (nem à direita e nem à esquerda).

$\mathbb{Z} \subseteq \mathbb{Q}$

$\mathbb{Z}$ não é ideal de $\mathbb{Q}$

Tome $x = 1 \in \mathbb{Z}$

$$r = \frac{1}{2} \in \mathbb{Q}$$

$$r.x = \frac{1}{2}.1 = \frac{1}{2} \notin \mathbb{Z}$$

Exemplo 2.2.20 Se A é anel, então $I = \{0\}$ e $I = A$ são ideais de A.

De fato para $I = \{0\}$ temos:

$.0, 0 \in I \Rightarrow 0 - 0 = 0 \in I$

$.r \in A, 0 \in I \Rightarrow r.0 = 0 \in I$

$0.r = 0 \in I$

Para $I = A$ temos:

$. x, y \in I \Rightarrow x - y \in I$

$x \in I \subseteq A, r \in A \Rightarrow x.r \in I \; e \; r.x \in I$

Exemplo 2.2.21 Os ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z}$. Pela Proposição 4.1.1, seja I um subconjunto não vazio de $\mathbb{Z}$. São equivalentes:

(a) $I = n\mathbb{Z} = \{nx; x \in \mathbb{Z}\}$, para algum $n \in \mathbb{N}$.

(b) I é ideal de $\mathbb{Z}$.

(c) I é subanel de $\mathbb{Z}$.

A demonstração dessa Proposição pode ser encontrada em (ver [1], proposição 4.1.1., pg. 104).

2.$\mathbb{Z}$ é ideal de $\mathbb{Z}$.

33.$\mathbb{Z}$ é ideal de $\mathbb{Z}$.

Veremos agora exemplos de ideal à esquerda que não é ideal à direita, e vice-versa.

Exemplo 2.2.22 É fácil ver que com as operações usuais de adição e multiplicação de matrizes que o conjunto $A = M_2(\mathbb{R})$ é anel. Seja $I = \left\{ \begin{pmatrix} u & v \\ 0 & 0 \end{pmatrix} \in A \right\}$.

Então I é ideal à direita de A, mas não é ideal à esquerda.

$. I \neq \varnothing$, pois $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$

. Sejam $X = \begin{pmatrix} u & v \\ 0 & 0 \end{pmatrix} \in I$

$Y = \begin{pmatrix} r & s \\ 0 & 0 \end{pmatrix} \in I$

$$X-Y=\begin{pmatrix} u-r & v-s \\ 0 & 0 \end{pmatrix}\in I$$

. Sejam $X=\begin{pmatrix} u & v \\ 0 & 0 \end{pmatrix}\in I$

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

$$Z.X=\begin{pmatrix} u & v \\ 0 & 0 \end{pmatrix}.\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} u.a+v.c & u.b+vd \\ 0 & 0 \end{pmatrix}, X.Z\in I$$

Logo I é um ideal à direita do anel $A=M_2(\mathbb{R})$. Agora

Tome $X=\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\in I$

$$Z=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\in A$$

$$X.Z=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\notin I$$

Portanto, I não é ideal à esquerda do anel $A=M_2(\mathbb{R})$.

Exemplo 2.2.23 Sejam $A=M_2(\mathbb{R})$ e $J=\left\{\begin{pmatrix} u & 0 \\ v & 0 \end{pmatrix}\in A\right\}$. Então J é ideal à esquerda de A, mas não é ideal à direita.

. $J\neq\varnothing$, pois $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\in J$

. $X=\begin{pmatrix} u & 0 \\ v & 0 \end{pmatrix}\in J$, $Y=\begin{pmatrix} r & 0 \\ s & 0 \end{pmatrix}\in J$

$$X-Y=\begin{pmatrix} u-r & 0 \\ v-s & 0 \end{pmatrix}\in J$$

. $X=\begin{pmatrix} u & 0 \\ v & 0 \end{pmatrix}\in J$, $Z=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in A$

$$Z.X=\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\begin{pmatrix} u & 0 \\ v & 0 \end{pmatrix}=\begin{pmatrix} a.u+b.v & 0 \\ c.u+d.v & 0 \end{pmatrix}\in J$$

Logo J é ideal à esquerda de A.

Agora vamos ver que J não é ideal à direita de A.

$$. X=\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\in J,\ Z=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\in A$$

$$X.Z=\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\notin J$$

J não é ideal à direita de A.

O próximo lema é uma ferramenta para produzir ideais.

Lema 2.2.24 Sejam A um anel e $x_1, x_2, \ldots, x_n \in A$. Então

(1) $A.x_1 + A.x_2 + \ldots + A.x_n = \{a_1.x_1 + a_2.x_2 + \ldots + a_n.x_n ; a_i \in A,\ i \in \{1,\ldots,n\}\}$ é ideal à esquerda de A.

(2) $x_1.A + x_2.A + \ldots + x_n.A = \{x_1.a_1 + x_2.a_2 + \ldots + x_n.a_n ; a_i \in A, i \in \{1,\ldots,n\}\}$ é ideal à direita de A.

Demonstração:

(1) Sejam $u = a_1.x_1 + a_2.x_2 + \ldots + a_n.x_n$, $v = b_1.x_1 + b_2.x_2 + \ldots + b_n.x_n \in A.x_1 + A.x_2 + \ldots + A.x_n$ e $a \in A$. Note que Temos que $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in A$.

$. u - v = (a_1 - b_1).x_1 + (a_2 - b_2).x_2 + \ldots + (a_n - b_n).x_n \in A.x_1 + A.x_2 + \ldots + A.x_n$, pois

$a_i - b_i \in A,\ i = 1,2,\ldots,n$.

$. \alpha.v = (\alpha.a_1).x_1 + (\alpha.a_2).x_2 + \ldots + (\alpha.a_n).x_n \in A.x_1 + A.x_2 + \ldots + A.x_n$, pois $\alpha a_i \in A,\ i = 1,2,\ldots,n$.

Portanto $A.x_1 + A.x_2 + \ldots + A.x_n$ é ideal à esquerda de A.

(2) É análoga à prova de (1).

■

Como conseqüência do Lema 2.2.24, temos:

$Ax = \{a.x ; a \in A\}$ é ideal à esquerda de A.

$xA = \{x.a; a \in A\}$ é ideal à direita de A.

. $A.x$ é chamado ideal principal à esquerda gerado por x.

. $x.A$ é chamado ideal principal à direita gerado por x.

Exemplo 2.2.25 $A = \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$\bar{0}.\mathbb{Z}_4$, $\bar{1}.\mathbb{Z}_4$, $\bar{2}.\mathbb{Z}_4$ e $\bar{3}.\mathbb{Z}_4$ são ideais de $\mathbb{Z}_4$.

$\bar{0}.\mathbb{Z}_4 = \{\bar{0}\}$, $\bar{2}.\mathbb{Z}_4 = \{\bar{0}, \bar{2}\}$

$\bar{1}.\mathbb{Z}_4 = \mathbb{Z}_4$, $\bar{3}.\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}_4$

Definição 2.2.26 Sejam A um anel comutativo e P um ideal de A.

Dizemos que P é ideal primo de A quando $P \neq A$ e $a,b \in A$ e $a.b \in P \Rightarrow a \in P$ *ou* $b \in P$.

Exemplo 2.2.27 $A = \mathbb{Z}, P = 2.\mathbb{Z}$

P é ideal primo de A ?

Se $a,b \in \mathbb{Z}$ e $a,b \in 2.\mathbb{Z}$ então $a \in 2.\mathbb{Z}$ ou $b \in 2.\mathbb{Z}$?

$a.b = 2.k; k \in \mathbb{Z}$

$2 \setminus a.b \Rightarrow 2 \setminus a$ ou $2 \setminus b \Rightarrow a \in 2.\mathbb{Z}$ ou $b \in 2.\mathbb{Z}$.

Logo $2.\mathbb{Z}$ é ideal primo de $\mathbb{Z}$.

Definição 2.2.28 Sejam A um anel comutativo e m um ideal de A. Dizemos que m é ideal maximal de A quando:

i) $m \neq A$;

ii) Se J é ideal de A e $m \subseteq J \subseteq A$, então $J = m$ ou $J = A$.

Exemplo 2.2.29 Se p é um numero primo positivo então $p.\mathbb{Z}$ é ideal maximal de $\mathbb{Z}$. (ver [1], proposição 4.3.4, pg, 117)

$2.\mathbb{Z}$ é ideal maximal de $\mathbb{Z}$

$31.\mathbb{Z}$ é ideal maximal de $\mathbb{Z}$

Exemplo 2.2.30 $4.\mathbb{Z}$ não é ideal maximal de $\mathbb{Z}$

$4.\mathbb{Z} \subseteq 2.\mathbb{Z} \subseteq \mathbb{Z}$

$2.\mathbb{Z} \neq 4.\mathbb{Z}$ e $2\mathbb{Z} \neq \mathbb{Z}$

Exemplo 2.2.31 $\bar{2}.\mathbb{Z}_4$ é ideal maximal de $\mathbb{Z}_4$.

$\bar{2}.\mathbb{Z}_4 = \{\bar{0}, \bar{2}\} \neq \mathbb{Z}_4$

Seja J um ideal de $\mathbb{Z}_4$ tal que $\bar{2}.\mathbb{Z}_4 \subseteq J \subseteq \mathbb{Z}_4$

Se $J = \bar{2}.\mathbb{Z}_4$ acabou!

Se $J \neq \bar{2}.\mathbb{Z}_4$, então $\bar{1} \in J$ ou $\bar{3} \in J$.

. $\bar{1} \in J$; $\bar{2}.\mathbb{Z}_4 \subseteq J \Rightarrow \bar{0}, \bar{2} \in J$

$\bar{1} + \bar{1} + \bar{1} = \bar{3} \in J$

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} \subseteq J \Rightarrow J = \mathbb{Z}_4$

. $\bar{3} \in J$, $\bar{0}, \bar{2} \in J$

$\bar{3} + \bar{3} + \bar{3} = \bar{9} = \bar{1} \in J$

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} \subseteq J \Rightarrow J = \mathbb{Z}_4$

Teorema 2.2.32 Seja $(K, +, .)$ anel comutativo com unidade. São equivalentes:

a) K é corpo;

b) $\{0\}$ é ideal maximal;

c) K só tem ideais triviais.

Demonstração: $a) \Rightarrow b)$ temos:

. $\{0\} \neq K$, por convenção.

. Seja J ideal de K tal que $\{0\} \subseteq J \subseteq K$.

Se $J = \{0\}$, acabou!

Se $J \neq \{0\}$, então existe $x \in J, x \neq 0$.

$0 \neq x \in J \subseteq K$, e K é corpo $\Rightarrow \exists x^{-1} \in K$ tal que $x^{-1}.x = 1$.

Provar que $K \subseteq J$.

Seja $y \in K$. Então $y.x^{-1} \in K$.

$y.x^{-1} \in K, x \in J$ e J é ideal $\Rightarrow y = y.x^{-1}.x \in J$.

Logo, $K \subseteq J$, é portanto $J = K$.

Segue que $\{0\}$ é ideal maximal.

$b) \Rightarrow c)$ Seja J é ideal de K.

$\{0\} \subseteq J \subseteq K$.

Como $\{0\}$ é ideal maximal, temos que $J = \{0\}$ ou $J = K$.

$c) \Rightarrow a)$ Seja $0 \neq x \in K$.

Provar que existe $y \in K$ tal que $x.y = 1$.

O ideal xK é não nulo, pois $x \neq 0$ .Segue-se da hipótese que $xK = K$.

$1 \in K = x.K \Rightarrow 1 = xy$, para algum $y \in K$.

Exemplo 2.2.33 $K = \mathbb{Z}_5$ $n = 5$ primo. Então $\mathbb{Z}_5$ é corpo.

$\{\bar{0}\}$ é ideal maximal, os ideais triviais de $\mathbb{Z}_5$ são $\{\bar{0}\}$ e $\mathbb{Z}_5$.

3. ANEL QUOCIENTE E TEOREMA DO ISOMORFISMO

O objetivo desse capitulo é o estudo de Anéis Quociente, onde a construção se dá através de um subanel especial, chamado ideal.

Estudaremos também as funções entre anéis. Não podemos esquecer que um conjunto pode ou não ser anel, dependendo das operações definidas nesse conjunto. Isso leva a pensar que as funções de interesse sobre os anéis são funções que preservam as operações de anéis, que são denominadas de homomorfismo de anéis.

3.1 Anel Quociente

A partir de um ideal I e do anel A, vamos construir um novo anel, chamado de anel quociente e denotado por $\frac{A}{I}$.

Definição 3.1.1 Sejam $a,b \in A$ e um ideal I do anel A. Dizemos que a é congruente a b módulo I quando a diferença $a-b$ está em I.

Notação: $a \equiv b \pmod{I} \Leftrightarrow a-b \in I.$

Proposição 3.1.2 A relação acima é uma relação de equivalência em A.

1) $a \equiv a \pmod{I}$ - Propriedade Reflexiva.

2) $a \equiv b \pmod{I} \Rightarrow b \equiv a \pmod{I}$ - Propriedade Simétrica.

3) $a \equiv b \pmod{I}$ e $b \equiv c \pmod{I} \Rightarrow a \equiv c \pmod{I}$ - Propriedade Transitiva.

Demonstração: (1) $a-a=0 \in I \Rightarrow a \equiv a \pmod{I}$.

(2) $a \equiv b \pmod{I} \Rightarrow a-b \in I \Rightarrow -(a-b) \in I \Rightarrow b-a \in I \Rightarrow b \equiv a \pmod{I}$.

(3) $\left.\begin{array}{l} a \equiv b \pmod{I} \Rightarrow a-b \in I \\ b \equiv c \pmod{I} \Rightarrow b-c \in I \end{array}\right\} \Rightarrow a-b+b-c \in I \Rightarrow a-c \in I \Rightarrow a \equiv c \pmod{I}.$

■

Definição 3.1.3 A classe de equivalência do elemento $a \in A$ é o conjunto $\bar{a} = \{x \in A; x \equiv a \pmod{I}\}$.

$$x \in \bar{a} \Leftrightarrow x \equiv a \pmod{I}$$

$x \in \bar{a} \Leftrightarrow x - a \in I \left(x - a = u \in I \Rightarrow x = a + u \right)$

$x \in \bar{a} \Leftrightarrow x \in a + I$

$\bar{a} = a + I$

$\frac{A}{I} = \left\{ \bar{a}; a \in A \right\}$ é conjunto quociente de A módulo I.

Proposição 3.1.4 Sejam I um ideal de anel A e $a, b \in A$.

a) $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \left(\operatorname{mod} I \right)$

b) $\bar{a} = \bar{b}$ ou $\bar{a} \cap \bar{b} = \varnothing$.

c) $A = \bigcup_{a \in A} \bar{a}$

Demonstração. (a) $(\Rightarrow) a \in \bar{a} = \bar{b} \Rightarrow a \in \bar{b} \Rightarrow a \equiv b \left(\operatorname{mod} I \right)$

$(\Leftarrow)$ Vamos provar que $\bar{a} \subseteq \bar{b}$.

Seja $u \in \bar{a}$, isto é, $u \equiv a \left(\operatorname{mod} I \right)$ e como congruência módulo I é relação transitiva, temos que $u \equiv b \left(\operatorname{mod} I \right)$.

Portanto $u \in \bar{b}$ e então $\bar{a} \subseteq \bar{b}$.

Para acabar a prova, vamos mostrar $\bar{b} \subseteq \bar{a}$.

Seja $u \in \bar{b}$, isto é, $u \equiv b \left(\operatorname{mod} I \right)$.

Por hipótese, $a \equiv b \left(\operatorname{mod} I \right)$ e como a congruência módulo I é relação transitiva, temos que $u \equiv a \left(\operatorname{mod} I \right)$.

Logo, $u \in \bar{a}$ e então $\bar{b} \subseteq \bar{a}$.

(b) Se $\bar{a} \cap \bar{b} = \varnothing$ nada temos para fazer.

Suponha que existe $z \in \bar{a} \cap \bar{b}$.

Como $z \in \bar{a}$ vemos que $z \equiv a \left(\operatorname{mod} I \right)$. Da mesma forma, $z \in \bar{b}$ implica em $z \equiv b \left(\operatorname{mod} I \right)$.

Pela transitividade da congruência módulo I segue que $a \equiv b \left(\operatorname{mod} I \right)$, e pelo item (a) concluímos que $\bar{a} = \bar{b}$.

(c) Queremos provar que $A = \bigcup_{a \in A} \bar{a}$

Como $\bar{a} \subseteq A$ para todo $a \in A$, é claro que $\bigcup_{a \in A} \bar{a} \subseteq A$. Por outro lado, dado $b \in A$ sabemos que $b \in \bar{b} \subseteq \bigcup_{a \in A} \bar{a}$, pois $\bar{b}$ é um dos conjuntos que estão sendo reunidos.

Logo, $A \subseteq \bigcup_{a \in A} \bar{a}$ e vale $A = \bigcup_{a \in A} \bar{a}$.

■

Exemplo 3.1.5 $A = \mathbb{Z}$, $I = 4.\mathbb{Z}$

$$\frac{A}{I} = ? \quad \frac{\mathbb{Z}}{4.\mathbb{Z}} = ?$$

$$\frac{\mathbb{Z}}{4.\mathbb{Z}} = \left\{\bar{x}; x \in \mathbb{Z}\right\}, \quad \bar{x} = x + 4\mathbb{Z}$$

$$\bar{0} = 0 + 4.\mathbb{Z}, \ \bar{1} = 1 + 4.\mathbb{Z}$$

$$\bar{2} = 2 + 4.\mathbb{Z}, \ \bar{3} = 3 + 4.\mathbb{Z}$$

$$\frac{\mathbb{Z}}{4.\mathbb{Z}} = \left\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\right\} = \mathbb{Z}_4$$

Exemplo 3.1.6 $A = \mathbb{Z}$, $I = n.\mathbb{Z}$

$$\frac{A}{I} = \frac{\mathbb{Z}}{n.\mathbb{Z}} = \left\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\right\}$$

Exemplo 3.1.7 $A = \mathbb{Z}_6$, $I = \bar{3}.\mathbb{Z}_6 = \left\{\bar{0}, \bar{3}\right\}$

Determinar $\frac{A}{I}$

$$\frac{A}{I} = \frac{\mathbb{Z}_6}{\bar{3}.\mathbb{Z}_6} = \left\{\bar{x}; x \in \mathbb{Z}_6\right\}, \quad \bar{x} = x + \bar{3}.\mathbb{Z}_6$$

$$\bar{\bar{0}} = \bar{0} + \left\{\bar{0}, \bar{3}\right\} = \left\{\bar{0}, \bar{3}\right\}$$

$$\bar{\bar{1}} = \bar{1} + \left\{\bar{0}, \bar{3}\right\} = \left\{\bar{1}, \bar{4}\right\}$$

$$\bar{\bar{2}} = \bar{2} + \left\{\bar{0}, \bar{3}\right\} = \left\{\bar{2}, \bar{5}\right\}$$

$$\frac{A}{I} = \frac{\mathbb{Z}_6}{\bar{3}.\mathbb{Z}_6} = \left\{\bar{x}; x \in \mathbb{Z}_6\right\} = \left\{\bar{\bar{0}}, \bar{\bar{1}}, \bar{\bar{2}}\right\}$$

Objetivo: Definir operações dentro desses conjuntos quocientes de maneira conveniente para que esse conjunto quociente seja um anel.

Vamos definir uma adição $+$ e uma multiplicação $.$ em $\frac{A}{I}$, de forma que $\left(\frac{A}{I},+,.\right)$ seja um anel.

Sejam $\bar{a}=a+I$ e $\bar{b}=b+I$ elementos de $\frac{A}{I}$. Defina:

i) $\bar{a}+\bar{b}=\overline{a+b}$

ii) $\bar{a}.\bar{b}=\overline{a.b}$

Usando a notação para $\bar{a}=a+I$ e $\bar{b}=b+I$, temos:

. $(a+I)+(b+I)=(a+b)+I$

. $(a+I).(b+I)=a.b+I$

Vamos verificar as operações de adição e multiplicação em $\frac{A}{I}$ estão bem definidas.

Observamos que se trata de uma generalização do que fizemos para os anéis $\mathbb{Z}_n=\frac{\mathbb{Z}}{n.\mathbb{Z}}$.

Proposição 3.1.8 Sejam I um ideal de anel A e $a,b,x,y\in A$. Se $a\equiv x(\text{mod}\, I)$ e $b\equiv y(\text{mod}\, I)$, então:

a) $a+b\equiv x+y(\text{mod}\, I)$

b) $a.b\equiv x.y(\text{mod}\, I)$

Demonstração. (a) Devemos provar que $a+b\equiv x+y(\text{mod}\, I)$, então:

$$\left.\begin{array}{l} a=x(\text{mod}\, I)\Rightarrow a-x\in I \\ b=y(\text{mod}\, I)\Rightarrow b-y\in I \end{array}\right\}\Rightarrow a-x+b-y\in I\Rightarrow a+b-(x+y)\in I\Rightarrow a+b\equiv x+y(\text{mod}\, I).$$

(b) Devemos mostrar que $a.b\equiv x.y(\text{mod}\, I)$, então:

$$a\equiv x(\text{mod}\, I)\Rightarrow a-x\in I\Rightarrow (a-x)b\in I\Rightarrow ab-xb\in I(*)$$

$$b\equiv y(\text{mod}\, I)\Rightarrow b-y\in I\Rightarrow x(b-y)\in I\Rightarrow xb-xy\in I(**)$$

Agora de $(*)$ e $(**)$ temos:

$$ab-xb+xb-xy\in I\Rightarrow ab-xy\in I\Rightarrow ab\equiv xy(\text{mod}\, I).$$

■

Proposição 3.1.9 Sejam $\bar{a},\bar{b},\bar{x},\bar{y} \in \frac{A}{I}$ tais que $\bar{a}=\bar{x}$ e $\bar{b}=\bar{y}$. Então $\bar{a}+\bar{b}=\bar{x}+\bar{y}$ e $\bar{a}.\bar{b}=\bar{x}.\bar{y}$.

Demonstração: Como $\bar{a}=\bar{x}$ e $\bar{b}=\bar{y}$ pelo item (a) da Proposição 2.1.4., temos:

$a \equiv x(\text{mod } I)$

$b \equiv y(\text{mod } I)$

Pela Proposição 3.1.8, temos:

$a+b=x+y(\text{mod } I)$

$a.b=x.y(\text{mod } I)$

Pelo item (a) da Proposição 3.1.4, temos:

$\overline{a+b}=\overline{x+y}$ e $\overline{a.b}=\overline{x.y}$

$\bar{a}+\bar{b}=\bar{x}+\bar{y}$ e $\bar{a}.\bar{b}=\bar{x}.\bar{y}$

■

Teorema 3.1.10 Seja I um ideal do anel A. Então $\left(\frac{A}{I},+,.\right)$ é um anel.

Demonstração:

i) $\bar{x}+\bar{y}=\bar{y}+\bar{x}$

$\bar{x}+\bar{y}=\overline{x+y}$

$\bar{x}+\bar{y}=\overline{y+x}$

$\bar{x}+\bar{y}=\bar{y}+\bar{x}$

ii) $\bar{x}+(\bar{y}+\bar{z})=(\bar{x}+\bar{y})+\bar{z}$

$\bar{x}+(\bar{y}+\bar{z})=\bar{x}+\overline{(y+z)}$

$\bar{x}+(\bar{y}+\bar{z})=\overline{x+(y+z)}$

$\bar{x}+(\bar{y}+\bar{z})=\overline{(x+y)+z}$

$\bar{x}+(\bar{y}+\bar{z})=\overline{(x+y)}+\bar{z}$

$\bar{x}+(\bar{y}+\bar{z})=(\bar{x}+\bar{y})+\bar{z}$

iii) $\bar{0}+\bar{x}=\bar{x}$

$\bar{0}+\bar{x}=\overline{0+x}=\bar{x}+\bar{0}=\bar{x}+\bar{0}=\bar{x}$

$0+x=x+0 \Rightarrow \overline{0+x}=\overline{x+0}$

$\bar{0}$ é o elemento neutro da adição.

iv) $\bar{x}+\left(\overline{-x}\right)=\left(-\bar{x}\right)+\bar{x}=\bar{0}$

$\bar{x}+\left(\overline{-x}\right)=\overline{x+(-x)}=\overline{(-x)+x}=\left(\overline{-x}\right)+\bar{x}=0$

$x+(-x)=(-x)+x \Rightarrow \overline{x+(-x)}=\overline{(-x)+x}$

$\left(\overline{-x}\right)$ é o simétrico de $\bar{x}$.

v) $\bar{x}.\left(\bar{y}.\bar{x}\right)=\left(\bar{x}.\bar{y}\right).\bar{z}$

$\bar{x}.\left(\bar{y}.\bar{x}\right)=\overline{x.(y.z)}$

$\bar{x}.\left(\bar{y}.\bar{x}\right)=\overline{(x.y).z}=$

$x.(y.z)=(x.y).z \Rightarrow \overline{x.(y.z)}=\overline{(x.y).z}$

$\overline{(x.y)}.\bar{z}=\left(\bar{x}.\bar{y}\right).\bar{z}$

vi) $\bar{x}.\left(\bar{y}+\bar{z}\right)=\bar{x}.\bar{y}+\bar{x}.\bar{z}$ e $\left(\bar{y}+\bar{z}\right).\bar{x}=\bar{y}.\bar{x}+\bar{x}.\bar{z}$

$\bar{x}.\left(\bar{y}+\bar{z}\right)=\bar{x}.\left(\overline{y+z}\right)=x.(y+z)=x.y+x.z \Rightarrow \overline{x.(y+z)}=\overline{x.y+x.z}$

$\overline{x.y+x.z}=\overline{x.y}+\overline{x.z}=\bar{x}.\bar{y}+\bar{x}.\bar{z}$

a outra é:

$\left(\bar{y}+\bar{z}\right).\bar{x}=\bar{y}.\bar{x}+\bar{z}.\bar{x}$

$\left(\bar{y}+\bar{z}\right).\bar{x}=\left(\overline{y+z}\right).\bar{x}=\left(\overline{y+z}\right).\bar{x}=\overline{(y+z).x}=y.x+z.x \Rightarrow (y+z).x=\overline{y.x+zx}$

$\overline{y.x+z.x}=\overline{y.x}+\overline{z.x}=\bar{y}.\bar{x}+\bar{z}.\bar{x}$

■

Definição 3.1.11 O anel $\left(\frac{A}{I},+,.\right)$ é chamado anel quociente de A por I.

Exemplos de Construção de Anel Quociente:

Exemplo 3.1.12 $A=\mathbb{Z}, I=4.\mathbb{Z}$

$$\frac{A}{I}=\frac{\mathbb{Z}}{4.\mathbb{Z}}=\left\{\bar{0},\bar{1},\bar{2},\bar{3}\right\}=\mathbb{Z}_4$$

$$\frac{\mathbb{Z}}{4.\mathbb{Z}}=\left\{\bar{x};x\in\mathbb{Z}\right\},\quad \bar{x}=x+4.\mathbb{Z}$$

$\bar{0} = 0 + 4.\mathbb{Z}$, $\bar{1} = 1 + 4.\mathbb{Z}$

$\bar{2} = 2 + 4.\mathbb{Z}$, $\bar{3} = 3 + 4.\mathbb{Z}$

$$\frac{\mathbb{Z}}{4.\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}_4$$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Exemplo 3.1.13 $A = \mathbb{Z}_6$, $I = \bar{3}.\mathbb{Z}_6 = \{\bar{0}, \bar{3}\}$

Determinar $\frac{A}{I}$

$$\frac{A}{I} = \frac{\mathbb{Z}_6}{\bar{3}.\mathbb{Z}_6}\{\bar{x}; x \in \mathbb{Z}_6\}, \quad \bar{x} = x + \bar{3}.\mathbb{Z}_6$$

$$\bar{\bar{0}} = \bar{0} + \{\bar{0}, \bar{3}\} = \{\bar{0}, \bar{3}\}$$

$$\bar{\bar{1}} = \bar{1} + \{\bar{0}, \bar{3}\} = \{\bar{1}, \bar{4}\}$$

$$\bar{\bar{2}} = \bar{2} + \{\bar{0}, \bar{3}\} = \{\bar{2}, \bar{5}\}$$

$$\frac{A}{I} = \frac{\mathbb{Z}_6}{\bar{3}.\mathbb{Z}_6} = \{\bar{x}; x \in \mathbb{Z}_6\} = \{\bar{\bar{0}}, \bar{\bar{1}}, \bar{\bar{2}}\}$$

+	$\bar{\bar{0}}$	$\bar{\bar{1}}$	$\bar{\bar{2}}$
$\bar{\bar{0}}$	$\bar{\bar{0}}$	$\bar{\bar{1}}$	$\bar{\bar{2}}$
$\bar{\bar{1}}$	$\bar{\bar{1}}$	$\bar{\bar{2}}$	$\bar{\bar{0}}$
$\bar{\bar{2}}$	$\bar{\bar{2}}$	$\bar{\bar{0}}$	$\bar{\bar{1}}$

·	$\bar{\bar{0}}$	$\bar{\bar{1}}$	$\bar{\bar{2}}$
$\bar{\bar{0}}$	$\bar{\bar{0}}$	$\bar{\bar{0}}$	$\bar{\bar{0}}$
$\bar{\bar{1}}$	$\bar{\bar{0}}$	$\bar{\bar{1}}$	$\bar{\bar{2}}$
$\bar{\bar{2}}$	$\bar{\bar{0}}$	$\bar{\bar{2}}$	$\bar{\bar{1}}$

Corolário 3.1.14 Sejam A um anel e I um ideal de A.

1) Se A tem unidade 1 então o anel $\frac{A}{I}$ tem unidade $\bar{1}$.

2) Se A é anel comutativo então o anel $\frac{A}{I}$ também é comutativo.

Demonstração: (1) Devemos provar que $\bar{x}.\bar{1} = \bar{1}.\bar{x} = \bar{x}$, $\forall x \in A$.

$$\bar{x}.\bar{1} = \overline{x.1} = \overline{1.x} = \bar{1}.\bar{x} = \bar{x}$$

(2) Sejam $x, y \in A$. Mostrar que $\bar{x}.\bar{y} = \bar{y}.\bar{x}$

$$\bar{x}.\bar{y} = \overline{x.y} = \overline{y.x} = \bar{y}.\bar{x}$$

Logo $\frac{A}{I}$ também é comutativo.

■

Exemplo 3.1.15 Não vale a recíproca do item (1) do Corolário 3.1.14, isto é, existe anel sem unidade A e ideal I de A tal que $\frac{A}{I}$ tem unidade. Tomando

$$A = 2.\mathbb{Z}, I = 6.\mathbb{Z}, \frac{A}{I} = \frac{2.\mathbb{Z}}{6.\mathbb{Z}} = \{\bar{0}, \bar{2}, \bar{4}\}.$$

Logo, $\frac{2.\mathbb{Z}}{6.\mathbb{Z}}$ é anel com unidade $\bar{4}$, apesar de $2.\mathbb{Z}$ não ter unidade.

Exemplo 3.1.16 A recíproca do item (2) do Corolário 3.1.14 anterior também não vale. Por exemplo, $A = M_2(\mathbb{R})$ não é comutativo e $I = A$ temos que $\frac{A}{I} = \{\bar{0}\}$. Logo, $\frac{A}{I}$ é comutativo apesar de A não ser comutativo.

Teorema 3.1.17 Sejam A um anel comutativo com unidade e I um ideal de A, $I \neq A$. Então:

a) $\frac{A}{I}$ é domínio $\Leftrightarrow$ I é ideal primo de A.

b) $\frac{A}{I}$ é corpo $\Leftrightarrow$ I é ideal maximal de A.

Demonstração: (a) $(\Rightarrow)$ Sejam $a, b \in A$ tais que $a.b \in I$.

Como $0 - a.b \in I$ vem que $0 \equiv a.b \pmod{I}$ e então $\bar{0} = \overline{a.b} = \bar{a}.\bar{b}$. Como $\frac{A}{I}$ é domínio devemos ter $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$.

Fazendo $\bar{a} = \bar{0}$, temos:

$$\bar{a}=\bar{0}\Rightarrow a\equiv 0(\text{mod}\, I)\Rightarrow a-0\in I\Rightarrow a\in I$$

Fazendo $\bar{b}=\bar{0}$, temos:

$$\bar{b}=\bar{0}\Rightarrow b\equiv 0(\text{mod}\, I)\Rightarrow b-0\in I\Rightarrow b\in I$$

Portanto $a\in I$ ou $b\in I$, isto é, I é ideal primo de A.

$(\Leftarrow)$ Como A é anel comutativo com unidade, segue do Corolário 3.1.14 parte (2) que $\frac{A}{I}$ é anel comutativo com unidade. Falta provar que $\frac{A}{I}$ não tem divisores de zero.

Sejam $a,b\in\frac{A}{I}$ tais que $\bar{a}.\bar{b}=\bar{0}$. Como $\bar{0}=\bar{a}.\bar{b}$ temos $a.b\in I$, mas I é ideal primo e então $a\in I$ ou $b\in I$.

Fazendo $a\in I$, temos:

$$a\in I\Rightarrow a-0\in I\Rightarrow a\equiv 0(\text{mod}\, I)\Rightarrow \bar{a}=\bar{0}.$$

Fazendo $b\in I$, temos:

$$b\in I\Rightarrow b-0\in I\Rightarrow b\equiv 0(\text{mod}\, I)\Rightarrow \bar{b}=\bar{0}.$$

Portanto $\bar{a}=\bar{0}$ ou $\bar{b}=\bar{0}$, isto é, $\frac{A}{I}$ é domínio.

(b) $(\Rightarrow)$ Sejam J um ideal de A tal que $I\subsetneq J\subseteq A$. Então existe $a\in J$ tal que $a\notin I$. Segue que $\bar{a}\neq\bar{0}$, e como $\frac{A}{I}$ é corpo, existe $\bar{b}\in\frac{A}{I}$ tal que $\bar{a}.\bar{b}=\bar{1}$. Isso leva a $a.b-1\in I$, isto é, $1=a.b+i$, $i\in I\subseteq J$. Note que $a.b\in J$ pois $a\in J$. Como $i,a.b\in J$ temos $1=a.b+i\in J$. Portanto $J=A$ e I é ideal máxima de A.

$(\Leftarrow)$ Como A é anel comutativo com unidade, segue do Corolário 3.1.14 parte (1) que $\frac{A}{I}$ é anel comutativo com unidade. Falta provar que todo elemento não nulo de $\frac{A}{I}$ tem inverso em $\frac{A}{I}$.

Seja $\bar{a}\in\frac{A}{I},\bar{a}\neq\bar{0}$. Segue que $a\notin I$ e então $I\subsetneq I+a.A\subseteq A$. Note que $I+a.A$ é ideal de A. Desde que I é ideal maximal devemos ter $I+a.A=A$. Em particular $1\in A=I+a.A$ e daí, $1=i+a.b$ para $i\in I$ e $b\in A$. Tomando classes módulo I na igualdade $1=i+a.b$ temos

$\bar{1} = \bar{i} + \bar{a}.\bar{b}$. Mas $i \in I$ e então $\bar{i} = \bar{0}$. Logo $\bar{a}.\bar{b} = 1$, isto é, $\bar{b}$ é o inverso de $\bar{a}$. Portanto $\frac{A}{I}$ é corpo.

■

Exemplo 3.1.18 Sabemos que se p é um numero primo então $p.\mathbb{Z}$ é ideal maximal de $\mathbb{Z}$. Logo $\mathbb{Z}_p = \frac{\mathbb{Z}}{p.\mathbb{Z}}$ é corpo.

Exemplo 3.1.19 Sabemos que se n não é um número primo então $n.\mathbb{Z}$ não é ideal primo de $\mathbb{Z}$. Logo $\mathbb{Z}_n = \frac{\mathbb{Z}}{n.\mathbb{Z}}$ não é domínio.

3.2 Homomorfismos e Isomorfismos

Definição 3.2.1 Sejam $(A,+,.)$ e $(B,*,\Delta)$ anéis. Um homomorfismo de A em B é uma função $f: A \to B$ tal que:

i) $f(a+b) = f(a) * f(b), \forall a,b \in A.$

ii) $f(a,b) = f(a) \Delta f(b), \forall a,b \in A.$

Definição 3.2.2 Um homomorfismo $f: A \to A$ é chamado de endomorfismo.

$$End(A) = \{f: A \to A; f \text{ é homomorfismo}\}.$$

Definição 3.2.3 Um isomorfismo $f: A \to A$ é chamado de automorfismo.

$$Aut(A) = \{f: A \to A; f \text{ é isomorfismo}\}$$

Exemplo 3.2.4 Sejam A e B anéis. Então $f: A \to B$, $f(x) = 0$, é homomorfismo, chamado de homomorfismo nulo.

Temos $a,b \in A$, então:

$f(a+b) = 0 = 0+0 = f(a) + f(b)$

$f(a.b) = 0 = 0.0 = f(a).f(b)$

Exemplo 3.2.5

. $f: \mathbb{Z} \to \mathbb{R}, f(x) = 0$

. $f: \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}_3, f(x) = \bar{0}$

. $f: n\mathbb{Z} \to M_{2X2}(\mathbb{R}), f(x) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Exemplo 3.2.6 Se A é um anel, então $f:A\to A, f(x)=x$, é um homomorfismo, chamado de homomorfismo identidade.

Note que f é isomorfismo e, portanto, é automorfismo de A.

Temos $x,y\in A$, então:

$f(x+y)=x+y=f(x)+f(y)$

$f(x.y)=x.y=f(x).f(y)$

Exemplo 3.2.7

$Id:\mathbb{Z}_4\to\mathbb{Z}_4$

$Id(\bar{x})=\bar{x}$

$Id(\bar{0})=\bar{0}$

$Id(\bar{1})=\bar{1}$

$Id(\bar{2})=\bar{2}$

$Id(\bar{3})=\bar{3}$

Exemplo 3.2.8 $Id:\mathbb{Z}_2\to\mathbb{Z}_2, Id(\bar{x})=\bar{x}$

$Id(\bar{0})=\bar{0}$

$Id(\bar{1})=\bar{1}$

Exemplo 3.2.9 Se A é subanel de B, então $f:A\to B, f(x)=x$, é um homomorfismo, chamado homomorfismo inclusão.

Exemplo 3.2.10

. $f:\mathbb{Z}\to\mathbb{Q}, f(x)=x$

. $f:\mathbb{Z}\to\mathbb{Z}[\sqrt{p}], f(x)=x$

Exemplo 3.2.11 $f:\mathbb{Z}\to\mathbb{Z}, f(x)=-x$, não é homomorfismo.

. $a,b\in\mathbb{Z}$

. $f(a+b)=-(a+b)=-a-b=f(a)+f(b)$

. $f(a.b)=-(a.b)\neq(-a).(-b)=f(a).f(b)$

$a=1$ e $b=2$

$f(a.b) = -(1.2) = -2$

$f(a).f(b) = f(1).f(2) = (-1).(-2) = 2$

Como $f(a.b) \neq f(a).f(b)$, então f não é homomorfismo.

Exemplo 3.2.12 $f: \mathbb{Z}_2 \to \mathbb{Z}_2, f(\bar{x}) = -\bar{x}$ é homomorfismo.

$f(\bar{x}) = -\bar{x} = \bar{x}$ f é a função identidade, pois $-\bar{0} = \bar{0}$ e $-\bar{1} = \bar{1}$

Exemplo 3.2.13 $f: \mathbb{Z}_3 \to \mathbb{Z}_3, f(\bar{x}) = -\bar{x}$, não é homomorfismo.

$\bar{x} = \bar{1}$ e $\bar{y} = \bar{2}$ $(\bar{2} + \bar{1} = \bar{0})$

$f(\bar{1}.\bar{2}) = f(\bar{2}) = -\bar{2} = \bar{1}$

$f(\bar{1}).f(\bar{2}) = (-\bar{1}).(-\bar{2}) = \bar{2}$

Logo $f(\bar{1}.\bar{2}) \neq f(\bar{1}).f(\bar{2})$

Exemplo 3.2.14 $f: \mathbb{Z}[\sqrt{p}] \to \mathbb{Z}[\sqrt{p}], f(a + b\sqrt{p}) = a - b\sqrt{p}$ é homomorfismo. Mais que isso,

$f \in Aut(\mathbb{Z}[\sqrt{p}])$.

$x = a + b\sqrt{p}, y = c + d\sqrt{p}$

. $f(x+y) = f((a+c) + (b+d).\sqrt{p})$

$f(x+y) = (a+c) - (b+d).\sqrt{p}$

$f(x+y) = (a - b\sqrt{p}) + (c - d\sqrt{p})$

$f(x+y) = f(a + b\sqrt{p}) + f(c + d\sqrt{p})$

$f(x+y) = f(x) + f(y)$

. $f(x.y) = f((a.c + pbd) + (ad + bc).\sqrt{p})$

$f(x.y) = (ac + pbd) - (ad + bc).\sqrt{p}$

$f(x.y) = (a - b\sqrt{p}).(c - d\sqrt{p})$

$f(x.y) = f(a + b\sqrt{p}).f(c + d\sqrt{p})$

$f(x.y) = f(x).f(y)$

Proposição 3.2.15 Seja $f:A\to B$ um homomorfismo. Então:

a) $f(0)=0$;

b) $f(-a)=-f(a)$;

c) $f(a-b)=f(a)-f(b)$;

d) Se A e B são domínios, então f é o homomorfismo nulo ou $f(1)=1$.

e) Se A e B são corpos, então f é nula ou f é injetiva.

Demonstração:(a) $0=0+0$

$f(0)=f(0+0)$

$f(0)=f(0)+f(0)$

$f(0)-f(0)=f(0)+f(0)-f(0)$

$0=f(0)+0$

$0=f(0)$

$f(0)=0.$

(b) $0=a+(-a)$

$f(0)=f(a+(-a))$

Pelo item (a) temos:

$0=f(a)+f(-a)$

$f(-a)=-f(a)$

(c) $f(a-b)=f(a+(-b))$

$f(a-b)=f(a)+f(-b)$

Pelo item (b), temos:

$f(a-b)=f(a)-f(b)$

(d) $1=1.1$

$f(1)=f(1.1)$

$f(1)=f(1).f(1)$

$f(1)-f(1).f(1)=0$

Sabendo que B é domínio, então:

$f(1)=0$ ou $f(1)=1$

Se $f(1)=1$, acabou!

Assuma que $f(1)=0$. Devemos provar que f é homomorfismo nulo.

Seja $a \in A$, então:

$a=a.1$

$f(a)=f(a.1)$

$f(a)=f(a).f(1)$

$f(a)=f(a).0$

$f(a)=0$

Logo, f é homomorfismo nulo.

(e) Sejam A e B corpos e suponhamos que f não é a função constante zero. Assim, pelo item anterior sabemos que $f(1)=1$. Vamos provar que f é injetiva. De fato, se, $x,y \in A$ e $f(x)=f(y)$ teremos, $f(x-y)=0$. Suponhamos por absurdo que $x \neq y$, então $x-y \neq 0$ e A corpo, isso nos diz que existe $b \in A$ tal que $b.(x-y)=1$ e daí segue que $1=f(1)=f(b(x-y))=f(b).f(x-y)=f(b).0=0$ que é uma contradição.

■

Observação 3.2.16

$f: A \to B$ homomorfismo $\Rightarrow f(0_A)=0_B$

$f(0_A) \neq 0_B \Rightarrow f$ não é homomorfismo.

Exemplo 3.2.17 Verifique se $f: \mathbb{Z} \to \mathbb{Z}$, $f(x)=x+1$, é homomorfismo.

$f(0)=1 \neq 0$

Logo f não é homomorfismo.

Observação 3.2.18

$f(0)=0 \not\Rightarrow f$ é homomorfismo.

Exemplo 3.2.19 $f: \mathbb{Z} \to \mathbb{Z}$, $f(x)=2.x$

$f(0)=0$

Porém, f não é homomorfismo

$f(1.2)=f(2)=4 \neq 8=2.4=f(1).f(2)$

Proposição 3.2.20 Seja $f: A \to B$ um homomorfismo de anéis.

1) Se J é subanel de A então $f(J)$ é subanel de B.

2) Se I é ideal de A então $f(I)$ é ideal de $f(A)=\text{Im}(f)$.

Demonstração: (1) Temos $0 \in J \Rightarrow f(0) \in f(J) \Rightarrow f(J) \neq \varnothing$.

Sejam $x, y \in f(J)$. Devemos mostrar que $x.y \in f(J)$ e $x-y \in f(J)$.

Como $x, y \in f(J)$, existem, $a, b \in J$ tais que $f(a)=x$ e $f(b)=y$.

Mas J é subanel e então $ab, a-b \in J$.

Aplicando f temos $f(a.b), f(a-b) \in f(J)$.

Segue que

$x.y = f(a).f(b) = f(a.b) \in f(J)$ e $x-y = f(a)-f(b) = f(a-b) \in f(J)$.

Portanto $f(J)$ é subanel de B.

(2) $0 \in I \Rightarrow f(0) \in f(I) \Rightarrow f(I) \neq \varnothing$.

Sejam $x, y \in f(I)$ e $z \in f(A)$. Devemos provar que $x-y \in f(I), zx \in f(I)$ e $xz \in f(I)$.

Como I é ideal, então I é subanel, segue de (1) que $f(I)$ é subanel. Isso garante que $x-y \in f(I)$.

Vamos mostrar apenas que $xz \in f(I)$, pois de forma análoga se prova que $zx \in f(I)$.

Como $x \in f(I)$ e $z \in f(A)$, existem $a \in I$ e $c \in A$ tais que $f(a)=x$ e $f(c)=z$. Mas I é ideal de A e então $a.c \in I$.

Aplicando f temos $f(a.c) \in f(I)$.

Segue que $x.z = f(a).f(c) = f(a.c) \in f(I)$.

Portanto $f(I)$ é ideal de $f(A)$.

3.3 Núcleo e Imagem

Seja $f : A \to B$ um homomorfismo de anéis. Definimos:

. núcleo (ou kernel) de f por $N(f) = \{a \in A; f(a) = 0\}$

. imagem de f por $\text{Im}(f) = \{ f(a); a \in A\}$

Teorema 3.3.1 Seja $f : A \to B$ um homomorfismo. Então:

a) $\text{Im}(f)$ é subanel de B.

b) $N(f)$ é ideal de A.

c) f é injetora $\Leftrightarrow N(f) = \{0\}$.

Demonstração: (a) Como A é subanel de A e $f(A) = \text{Im}(f)$ então, pela Proposição 3.2.20 (1), temos que $\text{Im}(f)$ é subanel de B.

(b) Sejam $x, y \in N(f)$ e $z \in A$.

Devemos provar que:

. $x-y \in N(f)$;

. $zx \in N(f)$;

. $xz \in N(f)$

Como $f(x)=0$ e $f(y)=0$, a Proposição 3.2.20 assegura que:

. $f(x-y)=f(x)-f(y)$

$f(x-y)=0-0$

$f(x-y)=0 \Rightarrow x-y \in N(f)$.

. $f(zx)=f(z).f(x)$

$f(zx)=f(z).0$

$f(zx)=0 \Rightarrow zx \in N(f)$.

. $f(xz)=f(x).f(z)$

$f(xz)=0.f(z)$

$f(xz)=0 \Rightarrow xz \in N(f)$.

c) $(\Rightarrow)$ Pela Proposição 3.2.20 (a), temos:

$x \in N(f) \Leftrightarrow f(x)=0$

$x \in N(f) \Leftrightarrow f(x)=f(0)$

$x \in N(f) \Leftrightarrow x=0$

$(\Leftarrow)$ $f(x)=f(y) \Rightarrow f(x)-f(y)=0$

Pela Proposição 3.2.20 (c), temos:

$f(x)=f(y) \Rightarrow f(x-y)=0$

$f(x)=f(y) \Rightarrow x-y \in N(f)=\{0\}$

$f(x)=f(y) \Rightarrow x-y=0 \Rightarrow x=y$

Logo, f é injetora.

■

Exemplo 3.3.2

$f: A \to B, f(x)=0$

$N(f)=A$ e $\text{Im}(f)=\{0\}$

Exemplo 3.3.3

$f: A \to A, f(x)=x$

$N(f)=\{0\}$ e $\text{Im}(f)=A$

Exemplo 3.3.4

$f:\mathbb{Z}\left[\sqrt{p}\right]\to\mathbb{Z}\left[\sqrt{p}\right], f\left(a+b\sqrt{p}\right)=a-b\sqrt{p}$

$N(f)=\{0\}$ e $\text{Im}(f)=\mathbb{Z}\left[\sqrt{p}\right]$

Exemplo 3.3.5

$f:AXA\to M_2(A), f(a,b)=\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$

$\text{Im}(f)=\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}; a,b\in A\right\}\subseteq M_2(A)$

$N(f)=?$

$(a,b)\in N(f)\Leftrightarrow f(a,b)=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$(a,b)\in N(f)\Leftrightarrow \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$(a,b)\in N(f)\Leftrightarrow a=0 \quad e \quad b=0$

$(a,b)\in N(f)\Leftrightarrow (a,b)=(0,0)$

$N(f)=\{(0,0)\}\Rightarrow f$ é injetora.

Exemplo 3.3.6

$f:\mathbb{Z}\to\mathbb{Z}_n, f(x)=\bar{x}$

$N(f)=?$

$x\in N(f)\Leftrightarrow f(x)=\bar{0}$

$x\in N(f)\Leftrightarrow \bar{x}=\bar{0}$

$x\in N(f)\Leftrightarrow x\equiv 0(\text{mod}\, n)$

$x\in N(f)\Leftrightarrow n\backslash x$

$x\in N(f)\Leftrightarrow x\in n\mathbb{Z}$

$N(f)=n\mathbb{Z}$

3.4 Teorema do Isomorfismo

Seja $f:A\to B$ um homomorfismo. Então $\frac{A}{N(f)}\simeq Im(f)$.

Demonstração: Já vimos no Teorema 3.3.1 que a Im(f) é subanel de B e que $N(f)$ é ideal A. Desde que Im(f) é subanel de B, temos em particular que Im(f) é um anel.

Portanto, $\varphi:\frac{A}{N(f)}\to\simeq Im(f),\varphi(\bar{a})=f(a)$, é uma correspondência entre anéis.

No entanto, os elementos de $\frac{A}{N(f)}$ são classes de equivalência, e então devemos propor que φ não depende da escolha dos representantes das classes. Isto é, devemos mostrar que se $\bar{a}=\bar{b}$ em $\frac{A}{N(f)}$ então $\varphi(\bar{a})=\varphi(\bar{b})$.

Temos que $\bar{a}=\bar{b}$ é o mesmo que $a-b\in N(f)$, e daí $0=f(a-b)=f(a)-f(b)=\varphi(\bar{a})-\varphi(\bar{b})$.

Logo $\varphi(\bar{a})=\varphi(\bar{b})$ e φ está bem definida. Agora vamos ver que φ é homomorfismo.

Sejam $\bar{a},\bar{b}\in\frac{A}{N(f)}$ e lembre que $a,b\in A$ e f é homomorfismo.

Então, temos:

$\varphi(\bar{a}+\bar{b})=\varphi(\overline{a+b})$

$\varphi(\bar{a}+\bar{b})=f(a+b)$

$\varphi(\bar{a}+\bar{b})=f(a)+f(b)$

$\varphi(\bar{a}+\bar{b})=\varphi(\bar{a})+\varphi(\bar{b})$ e

$\varphi(\bar{a}.\bar{b})=\varphi(\overline{a.b})$

$\varphi(\bar{a}.\bar{b})=f(a.b)$

$\varphi(\bar{a}.\bar{b})=f(a).f(b)$

$\varphi(\bar{a}.\bar{b})=\varphi(\bar{a}).\varphi(\bar{b})$

Segue que φ é homomorfismo.

Para ver que φ é sobrejetor, tome $y\in\text{Im}(\varphi)$. Então $y=f(\varphi)$, para $x\in A$.

Desde que $\bar{x} \in \frac{A}{N(f)}$ e $\varphi(\bar{x}) = f(x) = y$, concluímos que φ é sobrejetora.

Falta ver que φ é injetora. Faremos isso mostrando que $N(\varphi) = \{\bar{0}\}$.

Temos:

$\bar{u} \in N(\varphi) \Leftrightarrow \varphi(\bar{u}) = 0 \Leftrightarrow f(u) = 0 \Leftrightarrow$

$u \in N(f) \Leftrightarrow u - 0 \in N(f) \Leftrightarrow \bar{u} = \bar{0}.$

Portanto $\varphi : \frac{A}{N(f)} \to \text{Im}(f), \varphi(\bar{a}) = f(a)$ é isomorfismo de anéis.

■

Exemplo 3.4.1 $f : \mathbb{Z} X \mathbb{Z} \to \mathbb{Z}, f(x,y) = x$

f é homomorfismo.

. $f((x_1,y_1)+(x_2,y_2)) = f(x_1+x_2, y_1+y_2)$

$f((x_1,y_1)+(x_2,y_2)) = x_1 + x_2$

$f((x_1,y_1)+(x_2,y_2)) = f(x_1,y_1) + f(x_2,y_2)$

. $f((x_1,y_1).(x_2,y_2)) = f(x_1.x_2, y_1.y_2)$

$f((x_1,y_1).(x_2,y_2)) = x_1.x_2$

$f((x_1,y_1).(x_2,y_2)) = f(x_1,y_1).f(x_2,y_2)$

. $\text{Im}(f) = \mathbb{Z}$ e

. $N(f) = ?$

$(x,y) \in N(f) \Leftrightarrow f(x,y) = 0$

$(x,y) \in N(f) \Leftrightarrow x = 0$

$N(f) = \{0\} X \mathbb{Z}$

$\frac{\mathbb{Z} X \mathbb{Z}}{\{0\} X \mathbb{Z}} \simeq \mathbb{Z}$

Exemplo 3.4.2 $f : 4.\mathbb{Z} \to \mathbb{Z}_6, f(x) = \bar{x}$

É fácil ver que f é homomorfismo: $a = 4.x, b = 4.y, x, y \in \mathbb{Z}.$

. $f(a+b) = f(4.x + 4.y)$

$f(a+b) = \overline{4.x + 4.y}$

$f(a+b)=\overline{4.x}+\overline{4.y}$

$f(a+b)=f(4.x)+f(4.y)$

$f(a+b)=f(a)+f(b)$

. $f(a.b)=f(4.x.4.y)$

$f(a.b)=\overline{4.x.4.y}$

$f(a.b)=\overline{4.x}.\overline{4.y}$

$f(a.b)=f(4.x).f(4.y)$

$f(a.b)=f(a).f(b)$

Vamos provar que $Im(f)=\{\bar{0},\bar{2},\bar{4}\}$ $u\in Im(\varphi)\Leftrightarrow u=f(4x), x\in\mathbb{Z}$.

Temos 3 possibilidades: $x=3.k, x=3k+1$ ou $x=3.k+2$.

. $x=3k\Rightarrow u=f(4.x)=f(12.k)=\overline{12.k}=\bar{0}$

. $x=3k+1\Rightarrow u=f(4.x)=f(12.k+4)=\overline{12.k+4}=\bar{4}$

. $x=3k+2\Rightarrow u=f(4.x)=f(12.k+8)=\overline{12.k+8}=\bar{2}$

Portanto, $u\in Im(f)$ se, e somente se, $u\in\{\bar{0},\bar{2},\bar{4}\}$.

Vamos provar que $N(f)=12.\mathbb{Z}$.

$4.k\in N(f)\Leftrightarrow f(4.k)=\bar{0}$

$4.k\in N(f)\Leftrightarrow \overline{4.k}=\bar{0}$

$4.k\in N(f)\Leftrightarrow 4.k\equiv 0(\mathrm{mod}\,6)$

$4.k\in N(f)\Leftrightarrow 6\setminus 4.k$

$4.k\in N(f)\Leftrightarrow 3\setminus 2.k$

$4.k\in N(f)\Leftrightarrow 3\setminus k$

$4.k\in N(f)\Leftrightarrow k=3.u$

$v=4k\in N(f)\Leftrightarrow v=12.u\Leftrightarrow v\in 12.\mathbb{Z}$

Pelo Teorema do Isomorfismo temos:

$$\frac{4.\mathbb{Z}}{12.\mathbb{Z}}\simeq\{\bar{0},\bar{2},\bar{4}\}$$

4 ANEL DE POLINOMIOS E ALGORITMO DA DIVISÃO

Estudamos anteriormente alguns anéis especiais, entre os quais os anéis $\mathbb{Z}_n$. Agora estudaremos anéis de polinômios, onde a partir do anel A definiremos o anel $A[x]$, formado pelos polinômios na indeterminada x, com coeficientes em A. Observaremos que a melhor estrutura algébrica para $A[x]$ é domínio, e que isso ocorre exatamente quando A é domínio ou corpo. Trabalharemos o algoritmo de Euclides e sua relação com raízes de polinômios.

4.1 Anel de Polinômios

Definição 4.1.1 Seja A um anel. Um polinômio sobre A na indeterminada (ou variável) x, é uma expressão da forma:

$a_0 + a_1.x + a_2.x^2 + \ldots$ onde $a_i \in A, \forall i \in \mathbb{N}$, e existe $n \in \mathbb{N}$ tal que $a_i = 0$, para $j > n$.

Notação: $p(x) = a_0 + a_1.x + a_2.x^2 + \ldots + a_n.x^n$

Quando $a_n \neq 0$ dizemos que $p(x)$ tem grau n, e denotamos isso por:

$\partial(p(x)) = n$

Neste caso, a_n é o coeficiente dominante de $p(x)$.

Um polinômio $p(x) = a_0 + a_1.x + \ldots + a_{n-1}.x^{n-1} + x^n$ é chamado polinômio mônico.

Notação: Seja A um anel. O conjunto de todos os polinômios em x, sobre A, é denotado por $A[x]$.

$A[x] = \{a_0 + a_1.x + \ldots + a_n x^n ; n \in \mathbb{N}, a_i \in A\}$

Note que $A \subseteq A[x]$.

Exemplos 4.1.2

. $p(x) = 1 + 5.x^3 + 2.x^4 \in \mathbb{Z}[x]$

$\partial(p(x)) = 4$

. $p(x) = 1 + x \in \mathbb{Z}[x]$

$\partial(p(x)) = 1$

. $p(x) = 7 \in \mathbb{Z}[x]$

$\partial(p(x)) = 0$

. $p(x) = 0$ não tem grau.

. $p(x) = 1 + 5.x^3 + 2.x^4 + 0.x^5$

$\partial(p(x)) = 4$

. $p(x) = 5 - 3.x + 2.x^2 + 0.x^3 + 3.x^4 + 0.x^5 + \ldots$

$p(x) = 5 - 3.x + 2.x^2 + 3.x^4$

$\partial(p(x)) = 4$, coeficiente dominante é 3.

. $p(x) = 1$ é mônico

. $p(x) = 7$ não é mônico.

Sejam $p(x) = a_0 + a_1.x + \ldots \in A[x]$ e $q(x) = b_0 + b_1.x + \ldots \in A[x]$.

$p(x) = q(x) \Leftrightarrow a_i = b_i, \forall i \in \mathbb{N}$.

Em $A[x]$, definimos as operações:

. $p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1).x + \ldots \in A[x]$

. $p(x).q(x) = c_0 + c_1.x + c_2.x + \ldots \in A[x]$

Com

$c_0 = a_0.b_0$

$c_1 = a_0.b_1 + a_1.b_0$

$c_2 = a_0.b_2 + a_1.b_1 + a_2.b_0$

$c_3 = a_0.b_3 + a_1.b_2 + a_2.b_1 + a_3.b_0$

$\vdots$

$c_k = a_0.b_k + a_1.b_{k-1} + \ldots + a_k.b_0 = \sum_{i+j=k} a_i.b_j$

Note que estes são as operações usuais de adição e multiplicação de polinômios.

Exemplo 4.1.3

. $p(x) = 2 + x + 2.x^2, q(x) = 1 + 3.x + x^2$

. $p(x).q(x) = 2 + (6+1).x + (2+3+2).x^2 + (1+6).x^3 + 2.x^4$

$p(x).q(x) = 2 + 7.x + 7.x^2 + 7.x^3 + 2.x^4$

Teorema 4.1.4 Seja A um anel. Então:

1) $A[x]$ é um anel.

2) Se A é comutativo, então $A[x]$ é comutativo.

3) Se A tem unidade 1, então $A[x]$ tem unidade $g(x)=1$.

4) Se A é domínio então $A[x]$ é domínio.

Demonstração: (1) Sejam

$p(x)=a_0+a_1.x+a_2.x^2+... \in A[x]$

$q(x)=b_0+b_1.x+b_2.x^2+... \in A[x]$

$r(x)=c_0+c_1.x+c_2.x^2+... \in A[x]$

Vamos verificar os 6 axiomas de anel.

i) $p(x)+q(x)=q(x)+p(x)$

$p(x)+q(x)=(a_0+b_0)+(a_1+b_1).x+(a_2+b_2).x^2+...$

$p(x)+q(x)=(b_0+a_0)+(b_1+a_1).x+(b_2+a_2).x^2+...$

$p(x)+q(x)=q(x)+p(x)$

ii) $(p(x)+q(x))+r(x)=p(x)+(q(x)+r(x))$

$(p(x)+q(x))+r(x)=((a_0+b_0)+(a_1+b_1).x+...)+c_0+c_1.x+...$

$(p(x)+q(x))+r(x)=((a_0+b_0)+c_0)+((a_1+b_1)+c_1).x+...$

$(p(x)+q(x))+r(x)=(a_0+(b_0+c_0))+(a_1+(b_1+c_1)).x+...$

$(p(x)+q(x))+r(x)=(a_0+a_1.x+...)+(b_0+c_0)+(b_1+c_1).x+...$

$(p(x)+q(x))+r(x)=p(x)+(q(x)+r(x))$

iii) $p(x)+t(x)=t(x)+p(x)=p(x)$, para algum $t(x)\in A[x]$, $t(x)=0$ é o elemento neutro.

De fato,

$t(x)=0+0.x+0.x^2+...$

$p(x)+t(x)=(a_0+0)+(a_1+0).x+(a_2+0).x^2+...$

$p(x)+t(x)=(0+a_0)+(0+a_1).x+(0+a_2).x^2+...$

$p(x)+t(x)=a_0+a_1.x+a_2.x^2+...$

$p(x)+t(x)=p(x)$

iv) $p(x)+(-p(x))=(-p(x))+p(x)=0$

$-p(x) = -a_0 - a_1.x - a_2.x^2 - ...$ é simétrico de $p(x)$

. $p(x)+(-p(x)) = (a_0 - a_0)+(a_1 - a_1).x+(a_2 - a_2).x^2 + ...$

$p(x)+(-p(x)) = (-a_0 + a_0)+(-a_1 + a_1).x+(-a_2 + a_2).x^2 + ...$

$p(x)+(-p(x)) = 0+0.x+0.x^2 + ... = 0$

v) $p(x)(q(x).r(x)) = (p(x).q(x)).r(x)$

$q(x).r(x) = d_0 + d_1.x + d_2.x^2 + ..., d_1 = \sum_{j+t=i} b_j.c_t$

$p(x)(q(x).r(x)) = e_0 + e_1.x + e_2.x^2 + ...$

$e_i = \sum_{j+t=i} a_j.d_t$

$p(x).q(x) = l_0 + l_1.x + l_2.x^2 + ...$

$l_i = \sum_{j+t=i} a_j.b_t$

$(p(x).q(x)).r(x) = m_0 + m_1.x + m_2.x^2 + ...$

$m_i = \sum_{j+t=i} l_j.c_t$

Provar que $e_i = m_i, \forall i \in \mathbb{N}$.

Tome então $i \in \mathbb{N}$, daí

$e_i = \sum_{j+t=i} a_j.d_t$

$e_i = \sum_{j+t=i} a_j.\left(\sum_{\alpha+\beta=t} b_\alpha.c_\beta \right)$

$e_i = \sum_{j+\alpha+\beta=i} a_j.(b_\alpha.c_\beta)$

$e_i = \sum_{j+\alpha+\beta=i} (a_j.b_\alpha).c_\beta$

$e_i = \sum_{n+\beta=i} \left(\sum_{j+\alpha=n} a_j.b_\alpha \right).c_\beta$

$e_i = \sum_{n+\beta=i} l_n.c_\beta$

$e_i = m_i$

vi) Faremos a distributividade à esquerda. Queremos mostrar que $p(x)(q(x)+r(x)) = p(x).q(x)+p(x).r(x)$.

Escrevendo $p(x)\big(q(x)+r(x)\big)=u_0+u_1.x+u_2.x^2+...$

$$u_i=\sum_{j+t=i} a_i.\big(b_t+c_t\big)$$

$$p(x).q(x)=l_0+l_1.x+l_2.x^2+...$$

$$l_i=\sum_{j+t=i} a_i.b_t$$

$$p(x).r(x)=v_0+v_1.x+v_2.x^2+...$$

$$v_i=\sum_{j+t=i} a_i.c_t$$

Devemos mostrar que $u_i=l_i+v_i, \forall i\in\mathbb{N}$.

Para $i\in\mathbb{N}$ temos:

$$u_i=\sum_{j+t=i} a_j.\big(b_t+c_t\big)$$

$$u_i=\sum_{j+t=i}\big(a_j.b_t+a_j.c_t\big)$$

$$u_i=\sum_{j+t=i} a_j.b_t+\sum_{j+t=i} a_j.c_t$$

$$u_i=l_i+v_i$$

Agora falta mostrar que $\big(q(x)+r(x)\big).p(x)=q(x).p(x)+r(x).p(x)$.

$$\big(q(x)+r(x)\big).p(x)=m_0+m_1.x+m_2.x^2+...$$

$$m_k=\sum_{i+j=k}\big(b_j+c_j\big).a_i$$

$$q(x).p(x)=n_0+n_1.x+n_2.x^2+...$$

$$n_k=\sum_{i+j=k} b_j.a_i$$

$$r(x).p(x)=t_0+t_1.x+t_2.x^2+...$$

$$t_k=\sum_{i+j=k} c_j.a_i$$

Para acabar devemos provar que $m_k=n_k+t_k, \forall k\in\mathbb{N}$.

$$m_k=\sum_{i+j=k}\big(b_j+c_j\big).a_i$$

$$m_k=\sum_{i+j=k}\big(b_j.a_i+c_j.a_i\big)$$

$$m_k=\sum_{i+j=k} b_j.a_i+\sum_{i+j=k} c_j.a_i$$

$m_k = n_k + t_k$

Como $A[x]$ satisfaz os 6 axiomas de anel , temos que $A[x]$é um anel.

(2) Sejam $p(x) = a_0 + a_1.x + ... \in A[x]$ e $q(x) = b_0 + b_1.x + ... \in A[x]$. Escrevendo

$p(x).q(x) = l_0 + l_1.x + l_2.x^2 + ...$

$l_i = \sum_{j+t=i} a_j.b_t$

$q(x).p(x) = w_0 + w_1.x + w_2.x^2 + ...$

$w_i = \sum_{j+t=i} b_t.a_j$

Devemos provar que $l_1 = w_1, \forall i \in \mathbb{N}$. Por hipótese, o anel A é comutativo, e então para cada $i \in \mathbb{N}$ temos $l_i = \sum_{j+t=i} a_j.b_t = \sum_{j+t=i} b_t.a_j = w_1$.

(3) Seja $p(x) = a_0 + a_1.x + a_2.x^2 + ... \in A[x]$. Escreva $g(x) = 1$ como $g(x) = b_0 + b_1.x + b_2.x^2 + ...$, onde $b_0 = 1$ e $b_t = 0$ para $t \geq 1$.

Escrevendo $p(x).g(x) = c_0 + c_1.x + c_2.x^2 + ...$

$c_i = \sum_{j+t=i} a_j.b_t$, devemos provar que $c_i = a_i, \forall i \in \mathbb{N}$, então teremos $p(x).g(x) = p(x)$.

Para $i \in \mathbb{N}$, note que a única forma das parcelas do somatório $\sum_{j+t=i} a_j.b_t$ serem não nulas é quando $t = 0$. Assim,

$c_i = \sum_{j+t=i} a_j.b_t$

$c_i = \sum_{j+0=i} a_j.b_0$

$c_i = \sum_{j=i} a_j$

$c_i = a_i$

De forma análoga prova-se que $g(x).p(x) = p(x)$. Portanto, $g(x) = 1$ é a unidade do anel $A[x]$.

(4) Como A é domínio, temos que A é anel comutativo, com unidade e sem divisores de zero. Segue dos itens (2) e (3), que $A[x]$também é anel comutativo com unidade. Falta provar que $A[x]$não tem divisores de zero. Faremos esta prova por absurdo, isto é, vamos supor que

$A[x]$ tenha divisores de zero. Então existem $p(x), q(x) \in A[x]$, $p(x) \neq 0$, $q(x) \neq 0$, tais que $p(x).q(x) = 0$. Escrevendo $p(x) = a_0 + a_1.x + a_2.x^2 + \ldots$, $q(x) = b_0 + b_1.x + b_2.x^2 + \ldots$, e lembrando que estes polinômios são não nulos, existem $m, n \in \mathbb{N}$ tais que $p(x) = a_0 + a_1.x + \ldots + a_m.x^m, a_m \neq 0$ e $q(x) = b_0 + b_1.x + \ldots + b_n.x^n, b_n \neq 0$. Desde que:

$0 = p(x).q(x) = c_0 + c_1.x + c_2.x^2 + \ldots$

$c_i = \sum_{j+t=i} a_j.b_t$

temos que $c_i = 0, \forall i \in \mathbb{N}$. Em particular, $c_{n+m} = 0$. Mas

$0 = c_{n+m}$

$0 = \sum_{j+t=n+m} a_i.b_t$

$0 = a_0.b_{n+m} + a_1.b_{n+m-1} + \ldots + a_{m-1}.b_{n+1} + a_m.b_n + a_{m+1}.b_{n-1} + \ldots + a_{n+m}.b_0$

$0 = a_m.b_n$ (pois $b_i = 0$ para $j > n$ e $a_j = 0$ para $j > m$).

Isso contradiz o fato de A ser domínio. Portanto, $A[x]$ não tem divisores de zero.

■

Observação 4.1.5 A é subanel de $A[x]$.

$A \subseteq A[x]$

$a \in A \Rightarrow a = p(x) \in A[x]$.

Exemplos 4.1.6

$\mathbb{Z}[x]$ é domínio, pois $\mathbb{Z}$ é domínio.

. $n.\mathbb{Z}[x]$ é anel comutativo, pois $n.\mathbb{Z}$ é anel comutativo,

$A = 2.\mathbb{Z}$

$A = 2.\mathbb{Z}[x]$

$1 + 4.x \notin 2.\mathbb{Z}[x]$

$6 + 4.x \in 2.\mathbb{Z}[x]$

. $\left(\mathbb{Q}\left[\sqrt{p}\right]\right)[x]$ é domínio, pois $\mathbb{Q}\left[\sqrt{p}\right]$ é domínio

. $\mathbb{Z}_p[x]$ é domínio

. $\mathbb{Z}_n[x]$ é anel comutativo com unidade

. $\mathbb{R}[x]$ é domínio

. $\mathbb{C}[x]$ é domínio

Exemplo 4.1.7

. $p(x)=\bar{2}x^3+x^2-x+\bar{3}\in\mathbb{Z}_4[x]$ e $q(x)=\bar{2}x^3+\bar{3}.x^2+\bar{1}\in\mathbb{Z}_4[x]$

$p(x)+q(x)=(\bar{2}+\bar{2}).x^3+(\bar{1}+\bar{3}).x^2+(-\bar{1}+\bar{0}).x+(\bar{3}+\bar{1})$

$p(x)+q(x)=-\bar{1}.x$

$p(x)+q(x)=\bar{3}.x$

Exemplo 4.1.8

$p(x)=\bar{2}.x^6\in\mathbb{Z}_8[x]$ e $q(x)=\bar{4}.x^3\in\mathbb{Z}_8[x]$

$p(x).q(x)=(\bar{2}.\bar{4}).x^9$

$p(x).q(x)=\bar{0}$

A melhor estrutura algébrica para $A[x]$ é domínio. De fato, $A[x]$ nunca é corpo, pois o polinômio $p(x)=x\in A[x]$ não é inversível.

Se $p(x)=x$ fosse inversível, existiria $q(x)=a_0+a_1.x+...+a_n.x^n\in A[x]$ tal que $1=p(x).q(x)$

$1=a_0.x+a_1.x^2+...+a_n.x^{n+1}$

$1=0$. Absurdo.

Proposição 4.1.9 Se A é domínio então os elementos inversíveis de A e de $A[x]$ coincidem, isto é, $U(A)=U(A[x])$.

Demonstração: (Ver [2], Proposição 1.1.2, pg 27).

■

Exemplo 4.1.10

$U(\mathbb{Z}[x])=U(\mathbb{Z})=\{\pm 1\}$

$U(\mathbb{R}[x])=U(\mathbb{R})=\mathbb{R}^*$

$U(\mathbb{Z}_p[x])=U(\mathbb{Z}_p)=\mathbb{Z}_p^*$

4.2 Algoritmo da Divisão

Teorema 4.2.1 Sejam K um corpo, $f(x), g(x) \in K[x]$ e $g(x) \neq 0$. Então existem únicos $f(x), r(x) \in K[x]$ tais que $f(x) = g(x).q(x) + r(x)$, com $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x))$.

Demonstração: Se $f(x) = 0$ tome $q(x) = r(x) = 0$.

Podemos admitir $f(x) \neq 0$, e como $g(x) \neq 0$, escrevemos

$f(x) = a_0 + a_1.x + ... + a_n.x^n$, $\partial(f(x)) = n$

$g(x) = b_0 + b_1.x + ... + b_m.x^m$, $\partial(g(x)) = m$

1° Caso: $\partial(f(x)) < \partial(g(x))$

Tome $q(x) = 0$ e $r(x) = f(x)$.

2° Caso: $\partial(f(x)) \geq \partial(g(x))$

Vamos usar o Segundo Princípio de Indução sobre $n = \partial(f(x))$.

Se $n = 0$, então $f(x) = a_0 \in K$

$0 = n$

$0 = \partial(f(x)) \geq \partial(g(x)) \Rightarrow$

$\Rightarrow \partial(g(x)) = 0 \Rightarrow$

$\Rightarrow g(x) = b_0 \in K$

Como $0 \neq g(x) = b_0 \in K$, temos que $b_0^{-1} \in K$.

Tome $q(x) = b_0^{-1}.a_0$ e $r(x) = 0$. É claro que

$f(x) = a_0 = b_0(b_0^{-1}.a_0) + 0$

$f(x) = g(x).q(x) + r(x)$, com $r(x) = 0$.

Agora consideramos $n \geq 1$ e nossa hipótese de indução é: "Se $h(x) \in K[x]$, $h(x) \neq 0$ e $\partial(h(x)) < n$, existem $q_1(x)$, $r_1(x) \in K[x]$ tais que $h(x) = g(x).q_1(x) + r_1(x)$, com $r_1(x) = 0$ ou $\partial(r_1(x)) < \partial(g(x))$".

Agora considere o polinômio $h(x) = f(x) - (a_n.b_m^{-1}.x^{n-m})g(x)$. (*)

Se $h(x) = 0$, então $f(x) = g(x).q(x) + r(x)$, com $r(x) = 0$ e $q(x) = a_n b_m^{-1} x^{n-m}$.

Se $h(x) \neq 0$, podemos calcular seu grau. E pela escolha de $h(x)$ temos $\partial(h(x)) < n$. Usando a hipótese de indução obtemos $q_1(x)$, $r_1(x) \in K[x]$ tais que $h(x) = g(x).q_1(x) + r_1(x)$, com $r_1(x) = 0$ ou $\partial(r_1(x)) < \partial(g(x))$.

Substituindo em (*) e isolando $f(x)$, vem que

$f(x) = g(x)\left(q_1(x) + a_n.b_m^{-1}.x^{n-m}\right) + r_1(x)$.

Chame $q(x) = g(x).q(x) + r(x)$, com $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x))$.

Isso prova a existência de $q(x)$ e $r(x)$ como enunciado. Resta verificar a unicidade.

Sejam $q(x)$, $\tilde{q}(x)$, $r(x)$, $\tilde{r} \in K[x]$ tais que

$f(x) = g(x).q(x) + r(x)$, com $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x))$

$f(x) = g(x).\tilde{q}(x) + \tilde{r}(x)$, com $\tilde{r}(x) = 0$ ou $\partial(\tilde{r}(x)) < \partial(g(x))$.

Temos agora a igualdade $g(x).\left(\tilde{q}(x) - \tilde{q}(x)\right) = \tilde{r}(x) - r(x)$

Suponha $q(x) \neq \tilde{q}(x)$. Então $q(x) - \tilde{q}(x) \neq 0$ e $\tilde{r}(x) - r(x) \neq 0$ .Logo,

$\partial(g(x)) \leq \partial\left(\left(q(x) - \tilde{q}(x)\right).g(x)\right) = \partial\left(\tilde{r}(x) - r(x)\right) < \partial(g(x))$.

Essa contradição diz que não podemos supor $q(x) \neq \tilde{q}(x)$. Portanto, $q(x) = \tilde{q}(x)$. A igualdade $g(x).\left(\tilde{q}(x) - \tilde{q}(x)\right) = \tilde{r}(x) - r(x)$ fica $0 = \tilde{r}(x) - r(x)$.

Isso assegura que $\tilde{r}(x) = r(x)$.

■

Teorema 4.2.2 Seja A um anel comutativo com unidade. Dados $f(x), g(x) \in A[x], g(x) = b_0 + b_1.x + ... + b_m.x^m$ com $b_m \in U(A)$, existem únicos $q(x)$, $r(x) \in A[x]$ tais que $f(x) = g(x).q(x) + r(x)$, com $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x))$.

Demonstração: Para provar a existência de $q(x)$, $r(x) \in A[x]$, procedemos da mesma maneira como fizemos na prova do Teorema 4.2.1.

Vamos mostrar a unicidade.

Sejam $q(x)$, $\tilde{q}(x)$, $r(x)$, $\tilde{r}(x) \in A[x]$ tais que

$f(x) = g(x).q(x) + r(x)$, com $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x))$

$f(x)=g(x).\tilde{q}(x)+\tilde{r}(x)$, com $\tilde{r}(x)=0$ ou $\partial(\tilde{r}(x))<\partial(g(x))$.

Isso fornece a igualdade

$g(x).(q(x)-\tilde{q}(x))=\tilde{r}(x)-r(x)$.

Suponha $q(x)-\tilde{q}(x)\neq 0$.

Afirmação: $g(x).(q(x)-\tilde{q}(x))\neq 0$ e $\partial(g(x).(q(x)-\tilde{q}(x)))\geq\partial(g(x))$.

Escreva $q(x)-\tilde{q}(x)=c_0+c_1.x+...+c_t.x^t$, com $c_t\neq 0$.

Se $g(x).(q(x)-\tilde{q}(x))=0$ vem que $b_m.c_t=0$, daí, $b_m^{-1}.b_m.c_t=0$, que leva à contradição $c_t=0$. Logo, $g(x).(q(x)-\tilde{q}(x))\neq 0$.

Desde que $b_m.c_t\neq 0$, temos:

$\partial(g(x).(q(x)-\tilde{q}(x)))=m+t\geq\partial(g(x))$.

Da afirmação acima podemos concluir que $r(x)\neq 0$ e $\tilde{r}(x)\neq 0$.

De fato, se $r(x)=0$, então $g(x).(q(x)-\tilde{q}(x))=\tilde{r}(x)$. Olhando para o grau, chegamos ao absurdo $\partial(g(x))\leq\partial(g(x).(q(x)-\tilde{q}(x)))=\partial(\tilde{r}(x))<\partial(g(x))$.

Assim, $r(x)\neq 0$, e analogamente $\tilde{r}(x)\neq 0$. Isso garante que podemos falar em $\partial(r(x))$ e $\partial(\tilde{r}(x))$.

Finalmente,

$\partial(g(x))\leq\partial(g(x).(q(x)-\tilde{q}(x)))=\partial(\tilde{r}(x)-r(x))\leq máx\{\partial(\tilde{r}(x)),\partial(r(x))\}<\partial(g(x))$ A

contradição acima mostra que não podemos ter $q(x)-\tilde{q}(x)\neq 0$.

Portanto, $q(x)=\tilde{q}(x)$ e conseqüentemente $r(x)=\tilde{r}(x)$.

■

Exemplo 4.2.3 $f(x)=4.x^3+6.x^2+4.x+3\in\mathbb{R}[x]$ $\quad g(x)=2.x^2+x+1\in\mathbb{R}[x]$

$$\begin{array}{rl} 4.x^3+6.x^2+4.x+3 & \underline{\left|2.x^2+x+1\right.} \\ \underline{-\left(4.x^3+2.x^2+2.x\right)} & 2.x+2 \\ 4.x^2+4.x+3 & \\ \underline{-\left(4.x^2+4.x+3\right)} & \\ 1 & \end{array}$$

$q(x)=2.x+2$ e $r(x)=1$

$4.x^3+6.x^2+4.x+3=\left(2.x^2+x+1\right).(2.x+1)+1$

$\partial(r(x))=0<\partial(g(x))=2$

Exemplo 4.2.4 $f(x)=4.x^3+6.x^2+4.x+3\in\mathbb{Z}[x]$, $g(x)=3.x+7\in\mathbb{Z}[x]$ e 3 não é inversível em $\mathbb{Z}$.

$$\begin{array}{l} 4.x^3+6.x^2+4.x+3\,\underline{\left|3.x+7\right.} \\ \qquad\qquad\qquad \left(4.\frac{1}{3}\right).x^2 \\ \qquad\qquad\qquad \frac{4}{3}.x^2\in\mathbb{Z}[x] \end{array}$$

Não é possível dividir $f(x)$ por $g(x)$ em $\mathbb{Z}[x]$.

Exemplo 4.2.5 $f(x)=4.x^3+6.x^2+4.x+3\in\mathbb{Z}[x]$ $g(x)=x^2+x+2\in\mathbb{Z}[x]$

$$\begin{array}{rl} 4.x^3+6.x^2+4.x+3 & \underline{\left|x^2+x+2\right.} \\ \underline{-\left(4.x^3+2.x^2+8.x\right)} & 4.x+2 \\ 4.x^2+4.x+3 & \\ \underline{-\left(4.x^2+4.x+3\right)} & \\ -6.x-1 & \end{array}$$

$q(x)=4.x+2$ $r(x)=-6.x-1$

$4.x^3+6.x^2+4.x+3=\left(x^2+x+2\right).(4.x+2)+(-6.x-1)$

$\partial(r(x))=1<\partial(g(x))=2$

Proposição 4.2.6 Sejam A um anel comutativo com unidade, $\alpha\in A$ e $f(x)\in A[x]$. Então existe $q(x)\in A[x]$ tal que

$f(x)=(x-\alpha).q(x)+f(\alpha)$

Demonstração:

$f(x) \in A[x]$

$g(x) = x - \alpha$

$f(x) = (x-\alpha).q(x) + r(x)$

$r(x) = 0$ ou $\partial(r(x)) < 1$. Logo $r(x) = b \in A$.

$f(x) = (x-\alpha).q(x) + b$

$f(x) = (x-\alpha).q(\alpha) + b \Rightarrow b = f(\alpha)$

$f(x) = (x-\alpha).q(x) + f(\alpha)$

■

Corolário (D'Alembert) 4.2.7 Sejam A um anel comutativo com unidade, $\alpha \in A$ e $f(x) \in A[x]$. São equivalentes:

i) α é raiz de $f(x)$.

ii) $(x-\alpha) \setminus f(x)$

Demonstração: (i) $\Rightarrow$(ii) De acordo com a Proposição 4.2.6, existe $q(x) \in A[x]$ tal que $f(x) = (x-\alpha).q(x) + f(\alpha)$.

Como α é raiz de $f(x)$, temos $f(\alpha) = 0$. Segue que $(x-\alpha) \setminus f(x)$.

(ii) $\Rightarrow$(i) Por hipótese, existe $q(x) \in A[x]$ tal que $f(x) = (x-\alpha).q(x)$. Avaliando $f(x)$ em α, temos $f(\alpha) = (\alpha - \alpha).q(\alpha) = 0$.

Logo α é raiz de $f(x)$.

■

Exemplo 4.2.8

Determine o resto da divisão de $f(x) = 2.x^4 - x^3 + x^2 - 2.x - 3$ por $g(x) = (x-1)$, em $\mathbb{Z}[x]$.

$f(x) = (x-1).q(x) + f(1)$ o resto é $f(1) = -3$.

Exemplo 4.2.9

Determine $k \in \mathbb{Z}$ tal que $f(x) = x^4 + k.x^2 + 2.x - 8$ seja divisível por $g(x) = x + 2$, em $\mathbb{Z}[x]$.

-2 deve ser raiz de $f(x)$

$0 = f(-2)$

$0 = 16 + 4.k - 4 - 8$

$0 = 4 + 4.k \Rightarrow$

$k = -1$

Exemplo 4.2.10

Determinar $a, b \in \mathbb{Z}$ tais que $g_1(x) = x+1$ e $g_2(x) = x+2$ dividam

$f(x) = 2.x^3 + a.x^2 + b.x + 2$

$g_1(x) \setminus f(x) \Leftrightarrow f(-1) = 0 \Rightarrow -2 + a - b + 2 = 0$

$g_2(x) \setminus f(x) \Leftrightarrow f(-2) = 0 \Rightarrow -16 + 4.a - 2.b + 2 = 0$

$$\begin{cases} a - b = 0 \Rightarrow a = b \\ 4a. - 2.b = 14 \Rightarrow 4.a - 2.a = 14 \Rightarrow a = 7 \; e \; b = 7 \end{cases}$$

Exemplo 4.2.11

Dividindo $f(x)$ por $(x-3)$ temos resto 6.

Dividindo $f(x)$ por $(x-5)$ temos resto 8.

Calcule o resto da divisão de $f(x)$ por $(x-3).(x-5)$

$f(3) = 6, f(5) = 8$

$f(x) = (x-3).q(x) + r(x), r(x) = 0$ ou $\partial(r(x)) < 2$

$r(x) = a.x + b$

$f(x) = (x-3).(x-5).q(x) + (a.x + b)$

$$\begin{matrix} 6 = f(3) = 3.a + b \\ 8 = f(5) = 5.a + b \end{matrix} \Rightarrow \begin{cases} 3.a + b = 6 \\ 5.a + b = 8 \end{cases} \Rightarrow \begin{cases} 3.a + b = 6.(-1) \\ 5.a + b = 8 \end{cases} \Rightarrow$$

$$2.a = 2 \Rightarrow a = 1$$

$\Rightarrow 3 + b = 6 \Rightarrow b = 3$. Portanto $r(x) = x + 3$.

Definição 4.2.12 Sejam A um anel comutativo com unidade e $\alpha \in A$ uma raiz de $f(x) \in A[x], f(x) \neq 0$. Dizemos que α é uma raiz de multiplicidade $r, r \in \mathbb{N}^*$, quando

$f(x) = (x-\alpha)^r q(x)$, com $q(x) \in A[x], q(\alpha) \neq 0$.

Note que α é raiz de multiplicidade r quando $(x-\alpha)^r \setminus f(x)$ e $(x-\alpha)^{r+1} \not\setminus f(x)$.

Exemplo 4.2.13

Determinar a multiplicidade da raiz 2 do polinômio $f(x) = x^4 + x^3 - 3.x^2 - 5.x - 2$.

$f(x) = (x-2).(x^3 + 3.x^2 + 3.x + 1)$ e $q(x) = x^3 + 3.x^2 + 3.x + 1$

$q(2)=8+12+6+1\neq 0$

2 é raiz de multiplicidade 1

2 é raiz simples.

Exemplo 4.2.14

Determinar a multiplicidade da raiz -1 do polinômio $f(x)=x^4+x^3-3.x^2-5.x-2$

$f(x)=(x+1).(x^3-3.x-2)$

$q_1(x)=x^3-3.x-2$

$q_1(-1)=-1+3-2=0\Rightarrow(x+1)\backslash q_1(x)$

$q_1(x)=(x+1).(x^2-x-2)$

$q_2(x)=x^2-x-2$

$q_2(-1)=1+1-2=0\Rightarrow(x+1)\backslash q_2(x)$

$q_2(x)=(x+1).(x-2)$

$q_3(x)=x-2$

$q_3(-1)=-1-2\neq 0$

$f(x)=(x+1).q(x)$

$f(x)=(x+1).(x+1).q_2(x)$

$f(x)=(x+1).(x+1).(x+1).(x-2)$

-1 é raiz de multiplicidade 3 de $f(x)$.

Proposição 4.2.15 Sejam A um domínio, $f(x)\in A[x], f(x)\neq 0$ e $\alpha_1,\alpha_2,...,\alpha_t\in A$ as raízes distintas de $f(x)$ com multiplicidade $r_1,r_2,...,r_t$ respectivamente. Então $r_1+r_2+...+r_t\leq\partial(f(x))$.

Demonstração: Como α_1 é raiz de multiplicidade r_1, temos $f(x)=(x-\alpha_1)^{r_1}.q_1(x)$, com $q_1(x)\in A[x]$ e $q_1(\alpha_1)\neq 0$.

Como α_2 é raiz de $f(x), \alpha_2\neq\alpha_1$ e $A[x]$ é domínio, segue que α_2 é raiz de $q_1(x)$. Levando em consideração a multiplicidade de α_2, escrevemos $f(x)=(x-\alpha_1)^{r_1}.(x-\alpha_2)^{r_2}.q_2(x)$, com $q_2(x)\in A[x]$ e $q_2(\alpha_2)\neq 0$.

Seguindo o processo, $f(x)=(x-\alpha_1)^{r_1}.(x-\alpha_2)^{r_2}.....(x-\alpha_t)^{r_t}.q_t(x)$ com $q_t(x)\in A[x]$.

Usando a propriedade do grau de polinômio em domínio, vem que:

$$\partial(f(x))=\partial(x-\alpha_1)^{r_1}+\partial(x-\alpha_2)^{r_2}+...+\partial(x-\alpha_t)^{r_t}+\partial(q_t(x))$$

$$\partial(f(x))=r_1+r_2+...+r_t+\partial(q_t(x))$$

$$\partial(f(x))\geq r_1+r_2+...+r_t.$$

■

Observação 4.2.16 Em particular, a proposição acima diz que o número de raízes não excede o grau do polinômio.

Exemplo 4.2.17

Seja $f(x)=(x-1)^2.(x+3)^4.\left(x-\sqrt{2}\right)^2.q(x)\in\mathbb{C}[x]$, tal que $q(x)$ não tem raiz real.

1 é raiz de multiplicidade $2=r_1$

-3 é raiz de multiplicidade $4=r_2$

$\sqrt{2}$ é raiz de multiplicidade $2=r_3$

$f(x)$ tem 3 raízes reais $r_1+r_2+r_3=8\leq\partial(f(x))$

Exemplo 4.2.18

$f(x)=(x-1)^2.(x^2-2).(x^2+1)\in\mathbb{Z}[x]$. As raízes de $f(x)$ são $1,\sqrt{2},-\sqrt{2},i,-i$.

Em $\mathbb{Z}$, $f(x)$ tem raiz 1 de multiplicidade 2

Em $\mathbb{Q}$, $f(x)$ tem raiz 1 de multiplicidade 2

$$\text{Em } \mathbb{R},\begin{cases} f(x)\ tem\ raiz\ 1\ de\ multiplicidade\ 2 \\ f(x)\ tem\ raiz\ \sqrt{2}\ de\ multiplicidade\ 1 \\ f(x)\ tem\ raiz\ -\sqrt{2}\ de\ multiplicidade\ 1 \end{cases}$$

$$\text{Em } \mathbb{C},\begin{cases} f(x)\ tem\ raiz\ 1\ de\ multiplicidade\ 2=r_1 \\ f(x)\ tem\ raiz\ \sqrt{2}\ de\ multiplicidade\ 1=r_2 \\ f(x)\ tem\ raiz\ -\sqrt{2}\ de\ multiplicidade\ 1=r_3 \\ f(x)\ tem\ raiz\ i\ de\ multiplicidade\ 1=r_4 \\ f(x)\ tem\ raiz\ -i\ de\ multiplicidade\ 1=r_5 \end{cases}$$

$$r_1+r_2+r_3+r_4+r_5=6=\partial(f(x))$$

O próximo exemplo mostra que a hipótese de A ser domínio é essencial para a Proposição 4.2.15.

Exemplo 4.2.19

$f(x)=x^2+x\in\mathbb{Z}_6[x]$

$f(\bar{0})=\bar{0}, f(\bar{1})=\bar{2}, f(\bar{2})=\bar{0}$

$f(\bar{3})=\bar{0}, f(\bar{4})=\bar{2}, f(\bar{5})=\bar{0}$

$$\left.\begin{array}{l}\bar{0}\ \text{é raiz}\\ \bar{2}\ \text{é raiz}\\ \bar{3}\ \text{é raiz}\\ \bar{5}\ \text{é raiz}\end{array}\right\} 4>\partial(f(x))=2$$

$r_1+r_2+r_3+r_4=4>2=\partial(f(x))$

5. POLINÔMIOS IRREDUTÍVEIS E CORPOS COM p^n ELEMENTOS

Neste capítulo estudaremos irredutibilidade de polinômios com suas demonstrações e exemplos. Faremos também a construção de corpos com p^n elementos a partir de polinômios irredutíveis e ideais maximais com exemplificação de construção de corpos com p^n elementos a partir de $\mathbb{Z}_p[x]$.

5.1 Irredutibilidade de Polinômios

Definição 5.1.1 Sejam D um domínio e $p(x) \in D[x]$ um polinômio não nulo e não inversível.

.Dizemos que $p(x)$ é irredutível quando:

$p(x) = f(x).g(x) \in D[x] \Rightarrow f(x)$ ou $g(x)$ é inversível em $D[x]$.

.Dizemos que $p(x)$ é redutível quando:

Existem $f(x), g(x) \in D[x]$ não inversíveis tais que $p(x) = f(x).g(x)$.

Observação 5.1.2 Polinômios constantes em $K[x]$, K um corpo, não são redutíveis nem irredutíveis.

Exemplo 5.1.3

$f(x) = 2.x + 2 \in \mathbb{Z}[x]$ é redutível em $\mathbb{Z}[x]$.

. $f(x) = 2.(x+1), p(x) = 2$ e $g(x) = x+1$ não são inversíveis em $\mathbb{Z}[x]$.

Exemplo 5.1.4

. $f(x) = 2.x + 2 \in \mathbb{Q}[x]$ é irredutível em $\mathbb{Q}[x]$.

$f(x) = g(x).h(x) \Rightarrow g(x)$ ou $h(x)$ constante.

Assuma $g(x) = a \in \mathbb{Q}^*$

Logo $g(x)$ é inversível

Portanto $f(x)$ irredutível.

Exemplo 5.1.5

. $p(x)=2\in\mathbb{Z}[x]$ é irredutível em $\mathbb{Z}[x]$.

. $p(x)=2\in\mathbb{Q}[x]$ não é redutível nem irredutível em $\mathbb{Q}[x]$.

5.2 Polinômios Irredutíveis em $\mathbb{C}[x]$.

Proposição 5.2.1 Sejam K um corpo e $p(x)\in K[x]$.

a) Se $p(x)$é polinômio constante, então $p(x)$não é redutível e nem irredutível em $K[x]$.

b) Se $\partial(p(x))=1$, então $p(x)$é irredutível em $K[x]$.

Demonstração: (a) É claro que o polinômio $p(x)=0$não é redutível e nem irredutível. Se $p(x)=a, a\neq 0$, então $p(x)$é polinômio inversível de $K[x]$e, portanto, não é redutível nem irredutível em $K[x]$.

(b) Como $\partial(p(x))=1$, temos que $p(x)$é não nulo e não inversível. Escrevendo $p(x)=f(x).g(x)$com $f(x),g(x)\in K[x]$e usando os resultados sobre grau de polinômios, temos:

$1=\partial(f(x))+\partial(g(x))$.

Segue que $\partial(f(x))=0$ou $\partial(g(x))=0$. Assim, $f(x)$ou $g(x)$é polinômio constante não nulo. Logo, $f(x)\in K^*=U(K)$ ou $g(x)\in K^*=U(K)$.

Portanto, $p(x)$ é irredutível em $K[x]$.

■

Teorema 5.2.2 Teorema Fundamental da Álgebra.

Todo polinômio não constante de $\mathbb{C}[x]$ tem todas as suas raízes em $\mathbb{C}$.

[MONTEIRO, L.H.J.-Elementos de Álgebra. Rio de Janeiro: LTC, 1978.]

■

Teorema 5.2.3 Seja $p(x)\in\mathbb{C}[x]$. São equivalentes.

i) $\partial(p(x))=1$.

ii) $p(x)$ é irredutível em$\mathbb{C}[x]$.

Demonstração: (i) $\Rightarrow$(ii). Segue do item b) da Proposição 5.2.1.

(ii) $\Rightarrow$(i) Como $p(x)$é irredutível em $\mathbb{C}[x]$, segue da Proposição 5.2.1. a) que $p(x)$não é constante. Logo, $\partial(p(x)) \geq 1$. Suponha $\partial(p(x)) > 1$. Pelo Teorema 5.2.2., $p(x)$possui raiz $\alpha \in \mathbb{C}$, e então $p(x) = (x-\alpha).q(x) \in \mathbb{C}[x]$. Segue que $\partial(q(x))+1 = \partial(p(x)) > 1$.

Assim, $\partial(q(x)) > 0$. Desta forma, obtivemos uma decomposição de $p(x)$como produto de dois polinômios não inversíveis de $\mathbb{C}[x]$ contradizendo a irredutibilidade de $p(x)$. Portanto, $\partial(p(x)) = 1$.

■

Exemplo 5.2.4 Em $\mathbb{C}[x]$:

. $f(x) = 3.i - \sqrt{3}$, não é redutível nem irredutível.

. $f(x) = x - (i+1)$é irredutível.

. $f(x) = 3.x^4 - 8.x^3 - 6.x^2 + 24.x + 19$é redutível. Pois

$$f(x) = 3.(x+1).(x+1).\left(x - \frac{7+2.\sqrt{2}.i}{3}\right).\left(\frac{x-7-2.\sqrt{2}.i}{3}\right)$$

5.3 Polinômios Irredutíveis em $\mathbb{R}[x]$.

Teorema 5.3.1 Seja $p(x) \in \mathbb{R}[x]$. São equivalentes:

i) $p(x)$é irredutível em $\mathbb{R}[x]$.

ii) $p(x)$tem grau 1 ou $p(x)$tem grau 2 e discriminante negativo.

Demonstração: (i) $\Rightarrow$(ii) Como $p(x)$é irredutível em $\mathbb{R}[x]$ temos que $p(x)$não é constante. Pelo Teorema 5.2.2, existe $\alpha \in \mathbb{C}$ tal que α é raiz de $p(x)$.

1° Caso: $\alpha \in \mathbb{R}$.

Desde que $(x-\alpha) \in \mathbb{R}[x]$ e $(x-\alpha)$ divide $p(x)$, existe $q(x) \in \mathbb{R}[x]$ tal que $p(x) = (x-\alpha).q(x)$. No entanto, $p(x)$é irredutível em $\mathbb{R}[x]$, e então $q(x)$é polinômio constante não nulo. Logo, $\partial(p(x)) = 1$.

2° Caso: $\alpha \notin \mathbb{R}$.

Escreva $\alpha = a + b.i, a, b \in \mathbb{R}$ e $b \neq 0$.

Sabemos que $\overline{\alpha}$ também é raiz de $p(x)$e que $\overline{\alpha} \neq \alpha$. Assim, $(x-\alpha).(x-\overline{\alpha})$divide $p(x)$em $\mathbb{C}[x]$.

$p(x)=(x-\alpha).(x-\overline{\alpha}).q(x); \quad q(x) \in \mathbb{C}[x]$

$p(x)=(x-(a+b.i)).(x-(a-b.i)).q(x);$

$p(x)=(x^2-2.a.x+a^2+b^2).q(x).$

Como $p(x)$ e $(x^2-2.a.x+a^2+b^2)$estão em $\mathbb{R}[x]$, o algoritmo de Euclides em $\mathbb{R}[x]$garante a existência de $q_1(x), r_1(x) \in \mathbb{R}[x]$ tais que $p(x)=(x^2-2.a.x+a^2+b^2).q_1(x)+r_1(x)$, com $r_1(x)=0$ou $\partial(r_1(x))<2$.

Por outro lado, $q_1(x)$ e $r_1(x) \in \mathbb{C}[x]$, então temos $\mathbb{C}[x]$as igualdades $p(x)=(x^2-2.a.x+a^2+b^2).q(x)+0$

$p(x)=(x^2-2.a.x+a^2+b^2).q_1(x)+r_1(x)$. Pela unicidade do quociente e do resto, obtidos pelo algoritmo de Euclides para polinômios em $\mathbb{C}[x]$, vem $q(x)=q_1(x)$. Segue que $q(x) \in \mathbb{R}[x]$, pois $q_1(x) \in \mathbb{R}[x]$.

Como $p(x)=(x^2-2.a.x+a^2+b^2).q(x)$e $p(x)$é irredutível em $\mathbb{R}[x]$, devemos ter $q(x)$constante não nulo.

Seja $q(x)=c \in \mathbb{R}$. Então $p(x)=c.x^2-2.a.c.x+c.(a^2+b^2)$. Logo, $\partial(p(x))=2$, e o descriminante é:

$\Delta=4.a^2.c^2-4.c^2.(a^2+b^2)$

$\Delta=-4.c^2.b^2<0$ pois b, $c \neq 0$.

(ii) $\Rightarrow$(ii) Se $\partial(p(x))=1$, então $p(x)$é irredutível em $\mathbb{R}[x]$, pela Proposição 5.2.1.

Se $\partial(p(x))=2$e $p(x)$tem discriminante negativo, então $p(x)$não tem raiz em $\mathbb{R}$. Segue da Proposição 5.2.1.(b), que $p(x)$é irredutível em $\mathbb{R}[x]$.

■

Exemplo 5.3.2 Em $\mathbb{R}[x]$,

. $p(x)=\sqrt[3]{7}$ não é redutível nem irredutível.

. $p(x)=3.x+\ln 19$é irredutível.

. $p(x)=5.x^2-7.x+3$ é irredutível, pois $\Delta=49-60<0$

$p(x)=\sqrt{3}.x^{13}+19.x^7-\sqrt{5}.x^3+2.x+4$ é redutível.

5.4 Polinômios Irredutíveis em $\mathbb{Q}[x]$ e $\mathbb{Z}[x]$.

Proposição 5.4.1

a) Sejam D um domínio, $p(x)\in D[x]$ e $\partial(p(x))>1$. Se $p(x)$ tem raiz em D então $p(x)$ é redutível em $D[x]$.

b) Sejam K um corpo, $p(x)\in K[x]$ e $\partial(p(x))=2$ ou $\partial(p(x))=3$. Então:

$p(x)$ tem raiz em $K \Leftrightarrow p(x)$ é redutível em $K[x]$.

Demonstração: (a) Seja $\alpha\in D$ uma raiz de $p(x)$. Segue que $p(x)=(x-\alpha).q(x)$, com $(x-\alpha)$, $q(x)\in D[x]$.

Como $\partial(p(x))>1$, temos que $\partial.(x-\alpha)=1$ e $\partial(q(x))\geq 1$. Assim, $x-\alpha$ e $q(x)$ são polinômios não inversíveis de $D[x]$.

Logo, $p(x)$ é redutível em $D[x]$.

(b) $(\Rightarrow)$ Segue do item (a).

$(\Leftarrow)$ Desde que $p(x)$ seja redutível em $K[x]$, existem $f(x)$, $g(x)\in K[x], f(x)$ e $g(x)$ não inversíveis, tais que $p(x)=f(x).g(x)$.

Como $p(x)$ tem grau 2 ou 3 e $f(x)$ e $g(x)$ não são constantes, vem $\partial(f(x))=1$ e $\partial(g(x))=1$. Sem perda de generalidade admitimos que $\partial(f(x))=1$, e escrevemos $f(x)=a.x+b, a\neq 0$.

Assim, $p(x)=(a.x+b).g(x)$. Portanto, $-a^{-1}.b\in K$ é raiz de $p(x)$.

■

Proposição 5.4.2 Sejam $p(x)$ e $\mathbb{Q}[x]$ e $d\in\mathbb{Q}^*$. São equivalentes:

i) $p(x)$ é irredutível em $\mathbb{Q}[x]$.

ii) $dp(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração: (i) $\Rightarrow$(ii) Como $p(x)$ é irredutível, temos que $p(x)$ é não nulo e não inversível. Em particular, $p(x)$ não é polinômio constante. É claro que $dp(x)\neq 0$, pois

$d \neq 0, p(x) \neq 0$ e $\mathbb{Q}[x]$é domínio. Além disso, $dp(x)$não é inversível, pois não é polinômio constante.

Suponha $f(x), g(x) \in \mathbb{Q}[x]$ tais que $dp(x) = f(x).g(x)$. Multiplicando por d^{-1}, temos $p(x) = (d^{-1} f(x)).g(x)$.

Por hipótese, $p(x)$é irredutível, e então $d^{-1}.f(x)$ou $g(x)$é inversível. Segue que $f(x)$ ou $g(x)$é inversível, e, portanto, $dp(x)$é irredutível.

(ii) $\Rightarrow$(i) Já provamos que multiplicar polinômios irredutíveis por constante não nula resulta em polinômio irredutível. Por hipótese, $dp(x)$ é irredutível, e então, multiplicando por d^{-1}, concluímos que $p(x)$ é irredutível.

Exemplo 5.4.3

$p(x) = \frac{5}{3}.x^4 + x^3 + \frac{1}{2}.x^2 + \frac{1}{6}.x + \frac{2}{3} \in \mathbb{Q}[x]$.

Tome $d = mmc(2,3,6) = 6$.

$p(x)$é irredutível em $\mathbb{Q}[x]$ se e somente se,

$6.p(x) = 10.x^4 + 6.x^3 + 3.x^2 + x + 4 \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Q}[x]$.

Observação 5.4.4 A proposição anterior diz para estudar a irredutibilidade em $\mathbb{Q}[x]$, basta estudar a irredutibilidade de $p(x) \in \mathbb{Z}[x]$ em $\mathbb{Q}[x]$.

Definição 5.4.5 O polinômio $p(x) = a_0 + a_1.x + ..., a_n.x^n \in \mathbb{Z}[x]$ é primitivo quando $mdc = (a_0, a_1, ..., a_n) = 1$.

Exemplos 5.4.6

. $p(x) = 5.x^5 - 20.x^3 + 10$ não é primitivo, pois $p(x) = 5.(x^5 - 4.x^3 + 2)$.

. $p(x) = 5.x^5 - 20.x^3 + 3.x + 10$é primitivo.

Proposição 5.4.7 Lema de Gauss

Seja $p(x) \in \mathbb{Z}[x], \partial(p(x)) \geq 1$. Se $p(x)$é irredutível em $\mathbb{Z}[x]$, então $p(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração: Já vimos na proposição 5.4.7. que todo polinômio de grau 1 em $\mathbb{Q}[x]$ é irredutível em $\mathbb{Q}[x]$. Assim, podemos assumir que $\partial(p(x)) > 1$.

Segue que $p(x)$não é nulo e não inversível em $\mathbb{Q}[x]$.

Supondo que $p(x)$não é irredutível em $\mathbb{Q}[x]$, vem que $p(x)$é redutível em $\mathbb{Q}[x]$. Então existem $f(x), g(x) \in \mathbb{Q}[x]$, polinômios não inversíveis, tais que $p(x) = f(x).g(x)$. Note que $\partial(f(x)) \geq 1$ e $\partial(g(x)) \geq 1$.

Usando a propriedade do grau de polinômios, temos $1 \leq \partial(f(x)), \partial(g(x)) < \partial(p(x))$.

Também existem $\alpha, \beta \in \mathbb{Z}^*$, tais que $\alpha.f(x) = f_1(x) \in \mathbb{Z}[x]$ e $\beta.g(x) = g_1(x) \in \mathbb{Z}[x]$. É claro que $\partial(f_1(x)) = \partial(f(x))$ e $\partial(g_1(x)) = \partial(g(x))$. Assim, $1 \leq \partial(f_1(x)), \partial(g_1(x)) < \partial(p(x))$. Para $m = \alpha.\beta \in \mathbb{Z}^*$, podemos escrever $m.p(x) = f_1(x).g_1(x)$.

Note que $m \neq \pm 1$. De fato, se $m \neq \pm 1$, a igualdade acima diz que $p(x)$é redutível em $\mathbb{Z}[x]$. Isso contradiz nossa hipótese.

Sejam $f_1(x) = a_0 + a_1.x + ... + a_r.x^r \in \mathbb{Z}[x], a_r \neq 0$;

$g_1(x) = b_0 + b_1.x + ... + b_s.x^s \in \mathbb{Z}[x], b_s \neq 0$;

Então $r + s = \partial(p(x))$.

Como $m \in \mathbb{Z}, m \neq 0, \pm 1$, existe um numero primo q que divide m.

Afirmação: $q \backslash a_i, \forall i \in \{0,1,...,r\}$ ou $q \backslash b_j, \forall j \in \{0,1,...,s\}$.

Vamos provar esta afirmação por redução ao absurdo.

Suponha que a afirmação não seja verdadeira, isto é, existe $i \in \{0,1,...,r\}$ tal que $q \not\backslash a_i$ e existe $j \in \{0,1,...,s\}$ tal que $q \not\backslash b_i$. Podemos considerar i e j os menores possíveis com tal propriedade.

Sabemos que q divide m em $\mathbb{Z}$ assim, q divide $mp(x)$ em $\mathbb{Z}[x]$, e então q divide $f_1(x)g_1(x)$ em $\mathbb{Z}[x]$. Segue que q divide em $\mathbb{Z}$ o coeficiente de x^{i+j} do polinômio $f_1(x)g_1(x)$. De outra forma:

$$q \backslash a_0.b_{i+j} + a_1.b_{i+j-1} + ... + a_{i-1}.b_{i+j} + a_i.b_i + a_{i+1}.b_{j-1} + ... + a_{i+j}.b_0$$

Pela escolha de i e j, sabemos que $q \backslash a_0.b_{i+j}, ..., q \backslash a_{i-1}.b_{j+1}$, pois $q \backslash a_0, ..., q \backslash a_{i-1}$;

$q \backslash a_{i+1}.b_{j-i}, ..., q \backslash a_{i+j}.b_0$, pois $q \backslash b_{j-1}, ..., q \backslash b_0$.

Concluímos que $q \backslash a_i.b_j$, e desde que q seja primo, $q \backslash a_i$ e $q \backslash b_j$.

Este absurdo prova a afirmação verdadeira, vamos admitir sem perda de generalidade que $q \setminus a_i, \forall i \in \{0,1,...,r\}$. Isto garante que q divide $f_1(x)$ em $\mathbb{Z}[x]$, isto é, existe $f_2(x) \in \mathbb{Z}[x]$ tal que $f_1(x) = q.f_2(x)$.

Escrevendo $m = q.m_1$ com $m_1 \in \mathbb{Z}$, temos:

$m.p(x) = f_1(x).g_1(x)$

$q.m_1.p(x) = q.f_2(x).g_1(x)$

$m_1.p(x) = f_2(x).g_1(x)$

Novamente $m_1 \neq 0, \pm 1$ e então m_1 tem um divisor primo.

Seguindo o processo, que é finito, pois o número de fatores primos de m é finito, obtemos $p(x) = f^*(x).g^*(x)$, com $f^*(x), g^*(x) \in \mathbb{Z}[x]$.

Mas $\partial(f^*(x)) = \partial(f_1(x)) \geq 1$ e $\partial(g^*(x)) = \partial(g_1(x)) \geq 1$, logo $f^*(x)$ e $g^*(x)$ são inversíveis em $\mathbb{Z}[x]$.

Isto contradiz a irredutibilidade de $p(x)$ em $\mathbb{Z}[x]$. Portanto $p(x)$ deve ser irredutível em $\mathbb{Q}[x]$.

■

O exemplo abaixo mostra que não vale a recíproca do Lema de Gauss.

Exemplo 5.4.8

$p(x) = 2.x + 2 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$

$p(x)$ é irredutível em $\mathbb{Q}[x]$

$p(x)$ é redutível em $\mathbb{Z}[x]$, pois $p(x) = 2.(x+1)$

Proposição 5.4.9 Seja $p(x) \in \mathbb{Z}[x]$ tal que $\partial(p(x)) \geq 1$ e $p(x)$ primitivo. São equivalentes:

i) $p(x)$ é irredutível em $\mathbb{Z}[x]$.

ii) $p(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração: (i) $\Rightarrow$ (ii) É o Lema de Gauss.

(ii) $\Rightarrow$ (i) É claro que $p(x) \in \mathbb{Z}[x]^* / U(\mathbb{Z})$, pois $\partial(p(x)) \geq 1$.

Sejam $f(x), g(x) \in \mathbb{Z}[x]$, tais que $p(x) = f(x).g(x)$.

Como $f(x), g(x) \in \mathbb{Q}[x]$ e $p(x) = f(x).g(x)$ é irredutível em $\mathbb{Q}[x]$, devemos ter $f(x)$ ou $g(x)$ inversíveis em $\mathbb{Q}[x]$. Logo, $f(x)$ ou $g(x)$ é polinômio constante.

Assuma $f(x) = a \in \mathbb{Z}$. De $p(x) = f(x).g(x)$, vem que $p(x) = a.g(x)$.

Assim, a divide todos os coeficientes de $p(x)$, mas $p(x)$ é primitivo, e então $a = \pm 1$. Segue que $f(x) = a = \pm 1$ é inversível em $\mathbb{Z}[x]$.

Portanto, $p(x)$ é irredutível em $\mathbb{Z}[x]$.

■

5.5 Critérios de Irredutibilidade de Eisenstein

Seja $p(x) = a_0 + a_1.x + ... + a_n.x^n \in \mathbb{Z}[x]$.

Se existir um número primo p tal que $p \setminus a_0, p \setminus a_1, ..., p \setminus a_{n-1}, p \not\setminus a_n$ e $p^2 \not\setminus a_0$, então $p(x)$ é irredutível em $\mathbb{Q}[x]$.

A demonstração do critério de irredutibilidade de Eisenstein pode ser encontrado em ([3], Teorema 6, pg 83).

Exemplos 5.5.1

. $p(x) = \frac{1}{7}.x^6 + 2.x + 1$

$q(x) = 7.p(x) = x^6 + 14.x + 7$

Usando Eisenstein com $p = 7$, temos $q(x)$ é irredutível em $\mathbb{Q}[x]$. Logo, $p(x)$ é irredutível em $\mathbb{Q}[x]$.

. $p(x) = 2.x^7 + 3.x^5 + 3 \in \mathbb{Z}[x]$.

Usando Eisenstein com $p = 3$, vemos que $p(x)$ é irredutível em $\mathbb{Q}[x]$.

$p(x)$ é primitivo $\Rightarrow p(x)$ é irredutível em $\mathbb{Z}[x]$.

. $p(x) = 10.x^{11} + 6.x^3 + 6$

$p = 3, p(x)$ é irredutível em $\mathbb{Q}[x]$.

$p(x)$ é redutível em $\mathbb{Z}[x]$, pois

$p(x) = 2.(5.x^{11} + 3.x^3 + 3)$.

5.6 Construção de Corpos com p^n Elementos

Na demonstração do próximo teorema usamos o fato seguinte: "Se K é corpo então todo ideal de $K[x]$ é da forma $f(x).K[x]$, para algum $f(x) \in K[x]$. A demonstração desse fato pode ser vista em ([3], pg 72, teorema 2).

Teorema 5.6.1 Sejam K um corpo e $p(x) \in K[x]$.

Então as seguintes condições são equivalentes:

a) $p(x)$ é irredutível sobre K.

b) $J = K[x].p(x)$ é um ideal maximal em $K[x]$.

c) $\frac{K[x]}{J}$ é um corpo, onde $J = K[x].p(x)$.

Demonstração: (a) $\Leftrightarrow$ (b)

$(\Rightarrow)$ Suponhamos $p(x) \in K[x]$, $p(x)$ irredutível sobre K, e seja $J = K[x].p(x) = \{g(x).p(x) : g(x) \in K[x]\}$. Como grau $p(x) \geq 1$ temos imediatamente que $J \neq K[x]$.

Se $I = K[x].h(x)$ é um ideal de $K[x]$ tal que $I \supset J$ vamos provar que $I = J$ ou $I = K[x]$. Assim, $p(x) \in K[x].p(x) \subset K[x].h(x)$ nos diz que, $p(x) = g(x).h(x)$ para algum $g(x) \in K[x]$. Como $p(x)$ é irredutível temos que $g(x) = a \in K - \{0\}$ constante ou $h(x) = b \in K - \{0\}$ constante. Se $g(x) = a \neq 0$ constante temos que $h(x) = a^{-1}.p(x)$ e, portanto $I = K[x].h(x) \subset K[x].p(x) = J$ e isto nos dá $I = J$.

Se $h(x) \neq b \neq 0$ constante temos $I = K[x].h(x) = K[x]$ isto termina a implicação (a) $\Rightarrow$(b).

$(\Leftarrow)$ Seja $J = K[x].p(x)$ um ideal maximal em $K[x]$. Assim $J \neq K[x]$ nos diz que $\partial.p(x) \geq 1$. Suponhamos $g(x), h(x) \in K[x]$ e $p(x) = g(x).h(x)$. Assim segue imediatamente que $J \subset I = K[x].h(x)$ e como J é maximal temos que $J = I$ ou $I = K[x]$. Se $J = I$ segue que $h(x) \in J = K[x].p(x)$ isto nos diz que $p(x) = g(x).f(x).p(x)$. Como $p(x) \neq 0$ e $K[x]$ é um domínio de integridade teremos $1 = g(x).f(x)$, isto é, $g(x) \in K[x]$ é um polinômio invisível em $K[x]$. Portanto temos imediatamente que $g(x) = a \neq 0$ é um polinômio constante.

Se $I = K[x]$ segue imediatamente que $h(x) = b \neq 0$ constante ou seja $p(x)$ é irredutível sobre K.

(b) $\Leftrightarrow$ (c) é conseqüência do Teorema 3.1.17 (b) ■

Exemplo 5.6.2 Vamos provar que se $A = \mathbb{R}[x]$ e $I = A.(x^2+1)$, então $\frac{A}{I} \simeq \mathbb{C}$. De fato, como (x^2+1) é um polinômio irredutível em $\mathbb{R}[x]$ segue que $L = \frac{A}{I}$ é um corpo.

Se $p(x) \in A$ então pelo algoritmo da divisão existem polinômios $q(x), r(x) \in A$ tais que:

$p(x) = q(x)(x^2+1) + r(x)$, onde $r(x) = b.x + a$, $a, b \in \mathbb{R}$.

Passando a barra (congruência módulo I) e tendo em vista que $\overline{(x^2+1)} = \bar{0}$ temos:

$\overline{p(x)} = \overline{q(x)(x^2+1)} + \overline{r(x)} = \overline{b.x+a} = \bar{b}.\bar{x} + \bar{a}$. Assim, $L = \{\bar{b}.\bar{x} + \bar{a}; \bar{a}, \bar{b} \in \mathbb{R}\}$.

Observe que se denotarmos $\overline{\mathbb{R}} = \{\bar{a}; a \in \mathbb{R}\}$ então a função barra $\begin{matrix} \bar{}: \mathbb{R} \to \overline{\mathbb{R}} \\ a \to \bar{a} \end{matrix}$ preserva soma e produto e de fato é isomorfismo, ou seja, $\mathbb{R} \simeq \overline{\mathbb{R}}$.

Agora, como em L, $\bar{x}$ satisfaz a equação $z^2 + \bar{1} = 0$, pois $\overline{z^2} + \bar{1} = \overline{z^2+1} = \bar{0}$ podemos construir um isomorfismo $\alpha \in \mathbb{C}$ sobre L como segue:

$\varphi: \mathbb{C} \to L$.

$a + b.i \to \bar{a} + \bar{b}.\bar{x}$

$a \to \bar{x}$

$a \to \bar{a}$

Portanto $C \simeq L$.

Exemplo 5.6.3 Seja $A = \mathbb{Q}[x]$ e $I = A.(x^2 - p)$ onde p é um número primo positivo. É de fácil verificação que $K = \{a + b.\sqrt{p}; a, b \in \mathbb{Q}\}$ é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$ e $\sqrt{p}$.

Vamos mostrar nesse exemplo que $\frac{A}{I} \simeq K$.

De fato, seja $L = \frac{A}{I} = \{\overline{p(x)}; p(x) \in A\}$, onde a barra é relativa a congruência módulo I.

Como $\sqrt{p} \notin \mathbb{Q}$ sabemos que $x^2 - p$ é polinômio irredutível em $\mathbb{Q}[x]$ e, portanto L é um corpo.

Se $p(x) \in A$ então pelo algoritmo de divisão existe $q(x), r(x)$ em $\mathbb{Q}[x]$ tais que: $p(x) = q(x).(x^2 - p) + r(x)$, onde $r(x) = b.x + a$, $a, b \in \mathbb{R}$.

Como no exemplo anterior segue imediatamente que $\overline{p(x)} = \overline{q(x).(x^2 - p)} + \overline{r(x)} = \overline{b.x + a} = \bar{b}.\bar{x} + \bar{a}$ e, portanto $L = \{\bar{b}.\bar{x} + \bar{a}; \bar{a}, \bar{b} \in \mathbb{R}\}$. De modo inteiramente análogo ao exemplo anterior chegamos que a função barra: $\bar{} : \mathbb{Q} \to \overline{\mathbb{Q}}$ é um isomorfismo, ou seja, $\mathbb{Q} \simeq \overline{\mathbb{Q}} = \{\bar{a}; a \in \mathbb{Q}\}$ e também $\bar{x}$ satisfaz em L a equação $z^2 - p = 0$ pois $\overline{z^2} - \bar{p} = \overline{x^2 - p} = \bar{0}$. Assim podemos construir um isomorfismo $\varphi : K \to L$ como segue:

$\varphi : K \to L$

$a + b.\sqrt{p} \to \bar{a} + \bar{b}.\bar{x}$

$a \to \bar{a}$

$x \to \sqrt{p}$

5.7 Exemplos de Polinômios Irredutíveis em $\mathbb{Z}_p$

Exemplo 5.7.1 $p(x) = x^3 + x + \bar{1} \in \mathbb{Z}_5[x]$ é irredutível em $\mathbb{Z}_5$ e $I = p(x).\mathbb{Z}_5[x]$ é ideal maximal. Logo, $\frac{\mathbb{Z}_5[x]}{I}$ é corpo.

Exemplo 5.7.2 $p(x) = x^2 - \bar{3} \in \mathbb{Z}_5[x]$ é irredutível em $\mathbb{Z}_5$. Logo, $\frac{\mathbb{Z}_5[x]}{p(x).\mathbb{Z}_5[x]}$ é corpo.

Exemplo 5.7.3 $p(x) = x^2 + \bar{1} \in \mathbb{Z}_7[x]$ é irredutível em $\mathbb{Z}_7$. Logo, $\frac{\mathbb{Z}_7[x]}{p(x).\mathbb{Z}_7[x]}$ é corpo.

Exemplo 5.7.4 $p(x) = x^2 + x + \bar{1} \in \mathbb{Z}_3[x]$ é redutível em $\mathbb{Z}_3$. Pois $p(x) = (x + \bar{2})^2$ é sua forma reduzida.

O próximo teorema é uma ferramenta para construir corpos com p^n elementos, para p = primo e $n \in \mathbb{N}$.

Teorema 5.7.5 Sejam p um número primo e $p(x) \in \mathbb{Z}_p[x]$ um polinômio irredutível em $\mathbb{Z}_p$ e de grau n. Se $J = p(x).\mathbb{Z}_p[x]$, então $\frac{\mathbb{Z}_p[x]}{J}$ é corpo com exatamente p^n elementos.

Demonstração: Como $p(x)$é irredutível em $\mathbb{Z}_p[x]$, segue o teorema 5.6.1 que $\frac{\mathbb{Z}_p[x]}{J}$é corpo. Resta provar que $\frac{\mathbb{Z}_p[x]}{J}$ tem p^n elementos.

Seja $f(x)\in\mathbb{Z}_p[x]$ aplicando o algoritmo de Euclides podemos escrever $f(x)=p(x).q(x)+r(x)$, $r(x)=a_0+a_1.x_1+...+a_{n-1}.x^{n-1}\in\mathbb{Z}_p[x]$ e $f(x)\in\mathbb{Z}_p[x]$.

Segue que $\frac{\mathbb{Z}_p[x]}{J}$ temos $\overline{f(x)}=\overline{r(x)}$. Isso mostra que $\frac{\mathbb{Z}_p[x]}{J}\subseteq T=\left\{\overline{r(x)};r(x)=a_0+a_1.x+...+a_{n-1}.x^{n-1}\in\mathbb{Z}_p[x]\right\}$.

A inclusão $T\subseteq\frac{\mathbb{Z}_p[x]}{J}$ é obvia. Portanto, $\frac{\mathbb{Z}_p[x]}{J}=T$.

Agora vamos mostrar que T tem exatamente p^n elementos. Para isso basta verificar que se $r(x)=a_0+a_1.x+...+a_{n-1}.x^{n-1}$, $s(x)=b_0+b_1.x+...+b_{n-1}.x^{n-1}\in\mathbb{Z}_p[x]$ então $\overline{r(x)}\neq\overline{s(x)}$.

Supondo que $\overline{r(x)}=\overline{s(x)}$vem que $r(x)-s(x)\in J$, isto é, $r(x)-s(x)=p(x).f(x)$. Note que $r(x)-s(x)\neq 0$ e, portanto o grau de $r(x)-s(x)$está definido. Assim:

$$p(x).f(x)=r(x)-s(x)\Rightarrow\partial(p(x).f(x))=\partial(r(x)-s(x))<n$$
$$\Rightarrow\partial(p(x))+\partial(f(x))<n$$
$$\Rightarrow n+\partial(f(x))<n\text{. Absurdo.}$$

■

Agora para ilustrar o Teorema 5.7.5 com um exemplo.

Exemplo 5.7.6 Como $p(x)=x^3+x^2+x+\bar{2}\in\mathbb{Z}_3[x]$é irredutível em $\mathbb{Z}_3$, segue do Teorema 5.7.5 que $\frac{\mathbb{Z}_3[x]}{p(x).\mathbb{Z}_3[x]}$ é corpo com 27 elementos. De acordo com a demonstração do Teorema 5.7.5, estes elementos são:

$\overline{r_1(x)}=\bar{\bar{0}}$ $\quad\overline{r_2(x)}=\overline{x^2}$ $\quad\overline{r_3(x)}=\overline{\bar{2}.x^2}$

$\overline{r_4(x)}=\bar{\bar{1}}$ $\quad\overline{r_5(x)}=\overline{\bar{1}+x^2}$ $\quad\overline{r_6(x)}=\overline{\bar{1}+\bar{2}.x^2}$

$\overline{r_7(x)}=\bar{\bar{2}}$ $\quad\overline{r_8(x)}=\overline{\bar{2}+x^2}$ $\quad\overline{r_9(x)}=\overline{\bar{2}+\bar{2}.x^2}$

$$\overline{r_{10}(x)} = \bar{x} \qquad \overline{r_{11}(x)} = \overline{x + x^2} \qquad \overline{r_{12}(x)} = \overline{x + \bar{2}.x^2}$$
$$\overline{r_{13}(x)} = \overline{\bar{1} + x} \qquad \overline{r_{14}(x)} = \overline{\bar{1} + x + x^2} \qquad \overline{r_{15}(x)} = \overline{\bar{1} + x + \bar{2}.x^2}$$
$$\overline{r_{16}(x)} = \overline{\bar{2} + x} \qquad \overline{r_{17}(x)} = \overline{\bar{2} + x + x^2} \qquad \overline{r_{18}(x)} = \overline{\bar{2} + x + \bar{2}.x^2}$$

$$\overline{r_{19}(x)} = \overline{\bar{2}x} \qquad \overline{r_{20}(x)} = \overline{\bar{2}.x + x^2} \qquad \overline{r_{21}(x)} = \overline{\bar{2}.x + \bar{2}.x^2}$$
$$\overline{r_{22}(x)} = \overline{\bar{1} + \bar{2}.x} \qquad \overline{r_{23}(x)} = \overline{\bar{1} + \bar{2}.x + x^2} \qquad \overline{r_{24}(x)} = \overline{\bar{1} + \bar{2}.x + \bar{2}.x^2}$$
$$\overline{r_{25}(x)} = \overline{\bar{2} + \bar{2}.x} \qquad \overline{r_{26}(x)} = \overline{\bar{2} + \bar{2}.x + x^2} \qquad \overline{r_{27}(x)} = \overline{\bar{2} + \bar{2}.x + \bar{2}.x^2}.$$

Exemplo 5.7.7 Tome $p(x) = x^2 + x + \bar{1}$ que é irredutível em $\mathbb{Z}_2$, então $I = p(x).\mathbb{Z}_2[x]$ é ideal maximal de $\mathbb{Z}_2[x]$.

Como $p(x) = x^2 + x + \bar{1} \in \mathbb{Z}_2[x]$ é irredutível em $\mathbb{Z}_2$, segue do Teorema 5.7.5 que $\dfrac{\mathbb{Z}_2[x]}{p(x).\mathbb{Z}_2[x]}$ é corpo com 4 elementos. De acordo com a demonstração do Teorema 5.7.5, estes elementos são:

$$\overline{r_1(x)} = \bar{\bar{0}} \qquad \overline{r_2(x)} = \bar{x}$$
$$\overline{r_3(x)} = \bar{\bar{1}} \qquad \overline{r_4(x)} = \overline{\bar{1} + x}.$$

6 CONSIDERAÇÕES FINAIS

Mediante aos estudos aqui demonstrados, tivemos um grande avanço em nossa carreira docente. Este trabalho veio a engrandecer nossa gama de saberes. Nele pudemos constatar as diversas características inerentes aos anéis de polinômios, especificamente ao estudo de seus quocientes.

Com esse estudo conseguimos generalizar ainda mais do que foi oferecido no curso de álgebra, como uma proposta pós-moderna destinada à estudante de nível de pós-graduação já com uma base de nível superior na disciplina. Esse é o grande marco da nossa aprendizagem em quocientes de anéis de polinômios.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] JANESCH, O.R.; TANEJA, I.J. **Álgebra I**. Florianópolis: UFSC/EAD/CED/CFM,2008.

[2] JANESCH, O. R.; **Álgebra II**. Florianópolis: UFSC/EAD/CED/CFM,2008.

[3] GONÇALVES, A. **Introdução a álgebra**. 5ª. Ed. Rio de Janeiro:2007.

[4] VÍDEOS DA ESPECIALIZAÇÃO EM MATEMÁTICA MARANHÃO. UFSC 2009. Disponível em:<htth://www.prolicen.ufsc.br/maespec/course/view.php?id=5> Acesso em : Maio 2009.