UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

ANTÔNIO MÁRIO ALVES DO NASCIMENTO

CORPOS FINITOS E DOIS PROBLEMAS OLÍMPICOS

FORTALEZA

2019

ANTÔNIO MÁRIO ALVES DO NASCIMENTO

CORPOS FINITOS E DOIS PROBLEMAS OLÍMPICOS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em rede nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matematica. Área de Concentração: Ensino de Matematica

Orientador: Prof. Dr. Esdras Soares de Medeiros Filho

FORTALEZA

2019

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

N193c Nascimento, Antonio Mário Alves do.
Corpos finitos e dois problemas olímpicos / Antonio Mário Alves do Nascimento. – 2019.
85 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2019.
Orientação: Prof. Dr. Esdras Soares de Medeiros Filho.

1. Grupos. 2. Anéis. 3. Anéis de polinômios. 4. Corpo finito. I. Título.

CDD 510

ANTÔNIO MÁRIO ALVES DO NASCIMENTO

CORPOS FINITOS E DOIS PROBLEMAS OLÍMPICOS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em rede nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matematica. Área de Concentração: Ensino de Matematica

Aprovada em: 28 de Setembro de 2019

BANCA EXAMINADORA

Prof. Dr. Esdras Soares de Medeiros
Filho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. José Othon Dantas Lopes
Universidade Federal do Ceará (UFC)

Prof. Dr. Ângelo Papa Neto
Instituto Federal de Educação, Ciência e Tecnologia
do Ceará (IFCE)

À minha família. Irmãos, esposa e filha pela capacidade de acreditar em mim e investir em mim. Mãe, seu cuidado e dedicação foi que deram , a esperança e inspiração para sempre seguir. Pai, sua presença significou segurança e certeza de que não estou sozinho nessa caminhada.

AGRADECIMENTOS

Agradeço a Deus em primeiro lugar, pela força, coragem, proteção nessa caminhada, e em todas as viagens necessárias.

À minha família por sempre acreditar em mim e pelo apoio incondicional. E em especial a minha mãe Neide e meu pai Mário por me ensinar a persistir, a ter coragem e fé nessa e em todas as outras conquistas.

À minha esposa Jonieli e minha filha Maria Júlia pela compreensão, amor e apoio todos os dias e em todas as ausências.

À todos os professores do curso. Mas principalmente ao meu orientador Prof. Dr. Esdras Soares de Medeiros Filho que foi muito importante na realização deste trabalho.

Aos colegas do curso pelos momentos de descontração, troca de ideias e companhia nos almoços.

"A álgebra é generosa: frequentemente ela dá mais do que se lhe pediu."

(Jean Le Rond d'Alembert)

RESUMO

Nesta dissertação apresentamos um estudo sobre álgebra abstrata, mais precisamente sobre corpos finitos. O objetivo deste trabalho é apresentar a solução dos problemas "Seja a inteiro positivo e p um divisor primo de $a^3 - 3a + 1$ com $p \neq 3$. Prove que p é da forma $9k+1$ ou $9k-1$, sendo k inteiro."proposto no OBM em 2017 nível 3 e "Demonstrar que, para cada número inteiro $a > 1$, os divisores primos do número $5a^4 - 5a^2 + 1$ são da forma $20k \pm 1, k \in \mathbb{Z}$."proposto na 13ª olimpíada de Matemática Ibero-Americana. Nesse sentido, começamos com a introdução da teoria de grupos e apresentamos conceitos básicos e teoremas importantes como o teorema de Lagrange. Em seguida, introduzimos a teoria dos anéis, apresentamos definições importantes como quociente de anel e destacamos o anel polinomial. Mais adiante, começamos o estudo de corpos. Estudaremos a construção de corpo a partir de um polinômio irredutível, extensão de corpo, corpo de decomposição e caracterização de corpo finito. Finalmente, fornecemos as soluções dos problemas mencionados acima.

Palavras-chave: Grupos. Anéis. Anéis de polinômios. Corpo Finito.

ABSTRACT

In this dissertation we present a study about abstract algebra, more precisely, about fields finite. The goal of this work is to present the solution of the problems "Let a positive integer and p be a prime divisor in $a^3 - 3a + 1$ with $p \neq 3$. Prove that p is of the form $9k + 1$ ou $9k - 1$, where k is integer."proposed at OBM in 2017 level 3 and "Demonstrate that for every integer $a > 1$, the prime divisors of $5a^4 - 5a^2 + 1$ have the form $20k \pm 1$, $k \in \mathbb{Z}$."proposed at the 13th olympic Ibero-American Mathematics. In this sense, we begin with the introduction of group theory and we present basic concepts and important theorems like Lagrange's theorem. Then we introduce the theory of rings, we present important definitions as ring quotient and highlight the polynomial ring. Further on, we begin the study of fields. We will study field construction from an irreducible polynomial, field extension, field of decomposition and characterization of finite field. Finally, we provide the solutions of the problems mentioned above.

Keywords: Groups. Rings. Polynomial rings. Finite Field.

SUMÁRIO

1 INTRODUÇÃO

Álgebra abstrata é a sub-área da matemática que estuda as estruturas algébricas como grupos, anéis, corpos, espaços vetoriais entre outros. Corpo é um conjunto que, a grosso modo, estão bem definidas as operações de soma, subtração, multiplicação e divisão e corpo finito é um corpo que contém um número finito de elementos, que também podem ser chamados de corpos de Galois em homenagem ao matemático francês Évariste Galois. Algumas aplicações de corpos finitos incluem códigos corretores de erros, criptografia, Álgebra de computação e geradores pseudo-aleatório de números.

Usaremos essas estruturas algébricas na solução de dois problemas propostos em olimpíadas de matemática.

(1) Seja a inteiro positivo e p um divisor primo de $a^3 - 3a + 1$ com $p \neq 3$. Prove que p é da forma $9k + 1$ ou $9k - 1$, sendo k inteiro. Proposto na OBM em 2017 nível 3 (problema 6)

(2) Demonstrar que, para cada número inteiro $a > 1$, os divisores primos do número $5a^4 - 5a^2 + 1$ são da forma $20k \pm 1, k \in \mathbb{Z}$. Proposto em 2010 na *XIII* Olimpíada Ibero-americana de matemática universitária (problema 6).

Ambos os problemas foram propostos pelo matemático húngaro Géza Kós, nome bem conhecido por fazer parte de vários comitês olímpicos internacionais de matemática. Surpreendentemente, nenhum estudante alcançou a nota máxima para o problema (1). Isso nos motivou a escrever um material que abordasse um conteúdo autocontido que conduzisse o leitor compreender bem uma solução algébrica encontrada no AoPs Online (veja em https://artofproblemsolving.com/community/c6h1556461p9495218) . Esse trabalho visa não somente esgotar esse tipos de problema, mas visa também servir de material de estudo complementar para estudantes olímpicos e estudantes de graduação em matemática.

Aparentemente são apenas problemas de divisibilidade, mas a teoria dos números não tem ferramentas suficientes para a solução de ambos os problemas, sendo assim necessário recorrer a corpos finitos . Mas antes, precisamos entender como os elementos dessas estruturas algébricas se comportam, como ocorrem as operações nesses conjuntos. Neste contexto este trabalho traz ferramentas suficientes para tal compreensão.

Este trabalho está organizado da seguinte maneira. No capitulo 2 será feita uma breve introdução à teoria dos grupos, introduzindo as definições de grupos, grupo abeliano, ordem de um grupo, subgrupos, subgrupos gerados, ordem de um elemento de um grupo e homomorfismo de grupos e destacando o teorema de Lagrange e seus corolários que são fundamentais na solução

dos problemas mencionados acima.

No capitulo 3, será feita a introdução a teoria dos anéis apresentando a definição de anel, subanel, ideais, anéis quocientes e homomorfismo de anéis. Apresentamos também alguns tipos de anéis, tais como anel comutativo, domínio de integridade, anel com divisão e corpo, e abordamos o anel $\mathbb{Z}_n$ que é o conjunto das classes residuais modulo n, mostraremos que se n é um número primo então $\mathbb{Z}_n$ é um corpo finito com n elementos.

No capitulo 4, destacamos um tipo especial de anel que são os anéis de polinômios em uma indeterminada x. Apresentamos o algoritmo da divisão para polinômios, raízes de um polinômio, polinômios irredutíveis, critério de Eisenstein e ideais principais.

No capitulo 5, apresentamos primeiro a construção de corpos finitos a partir de um polinômio irredutível, extensão de corpo, elemento algébrico e transcendente, corpo de decomposição. Em seguida fazemos a caracterização de corpos finitos, definindo a característica de um corpo e o corpo de Galois $\mathbb{F}_p$. Em seguida mostramos que todo corpo finito tem ordem potência de primo,e mostramos também que a reciproca é verdadeira, para todo $n \in \mathbb{N}$ e todo p primo existe um único corpo com ordem p^n. Destacamos também as raízes de polinômios com coeficientes em corpos finitos, que dado um polinômio irredutível em um corpo finito, então suas raízes são simples e da forma $\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}$ onde m é o grau do polinômio.

Finalmente, no capitulo 6, apresentamos a solução dos dois problemas mencionados acima.

2 GRUPOS, SUBGRUPOS E HOMOMORFISMO DE GRUPOS

2.1 Grupos

Nesta seção apresentaremos a definição de grupo e suas propriedades básicas e mostraremos alguns exemplos de grupo.

Uma operação $*$ em um conjunto não vazio G é uma função

$$\begin{array}{rccc} * & : & G\times G & \longrightarrow & \mathrm{G} \\ & & (a,b) & \longrightarrow & a*b \end{array}$$

Portanto, uma operação em G associa a cada par de elementos (a,b) de G um único elemento $a*b$ em G.

Definição 2.1. *Um grupo é um par $(G,*)$, constituído de um conjunto G e uma operação binária $(*)$ em G, que satisfaz os seguintes axiomas:*

(i) Associatividade: se x,y,z são elementos de G então $x*(y*z)=(x*y)*z$

(ii) Elemento neutro: existe um elemento e em G tal que $x*e=e*x=x$.

(iii) Inversos: para todo elemento x de G existe um elemento x' em G tal que $x*x'=x'*x=e$

Além disso em alguns grupos verifica-se a comutatividade.

Definição 2.2. *Dizemos que um Grupo $(G,*)$ é abeliano ou comutativo se, e somente se, $*$ é uma operação comutativa.*

(iv) $x*y=y*x$ para todos $x,y\in G$

Se a operação for uma adição conhecida o grupo é chamado de grupo aditivo e denotado por $(G,+)$ e se for uma multiplicação conhecida será chamado de grupo multiplicativo e denotado por $(G,\cdot)$. Se o grupo é aditivo denominamos o inverso por simétrico.

Definição 2.3. *A ordem de um grupo G é definida como sendo o número de elementos em G e é denotada por $|G|$.*

Com a definição de ordem de um grupo podemos caracterizar os grupos como infinitos ou finitos. Um grupo G será denominado finito quando a ordem de G for finita, ou seja, $|G|=n$ com $n\in\mathbb{N}^*$. Caso contrário o grupo G será denominado de grupo infinito.

Exemplo 2.1. $(\mathbb{Z},+)$

(i) A soma é associativa nos inteiros,

(ii) O elemento neutro para a soma dos inteiros é o 0

(iii) Para cada $x \in \mathbb{Z}$,existe $-x \in \mathbb{Z}$, tal que $x+(-x)=0$.

(iv) Além disso a soma de inteiros é comutativa.

Então $(\mathbb{Z},+)$ é um grupo abeliano infinito e o denotamos por grupo aditivo dos inteiros.

Exemplo 2.2. *$(\mathbb{Z},\cdot)$ não é grupo.Pois o axioma (iii) não é satisfeito, ou seja, para cada $x \in \mathbb{Z}$, não existe $y \in \mathbb{Z}$ tal que $x \cdot y = 1$*

Exemplo 2.3. $(\mathbb{Q}^*,\cdot)$

(i) O produto é associativo nos racionais,

(ii) O elemento neutro é o 1,

(iii) para todo $x \in \mathbb{Q}^*$ existe $\frac{1}{x} \in \mathbb{Q}^*$ tal que $x \cdot \frac{1}{x} = 1$

(iv) Além disso $(\cdot)$ é comutativo.

Portanto $(\mathbb{Q}^*,\cdot)$ é um grupo abeliano infinito. e denotamos por grupo multiplicativo dos racionais.

Antes de prosseguirmos com exemplos de grupos definiremos congruências e o conjunto $\mathbb{Z}_n$.

Definição 2.4. *Diremos que dois números inteiros a e b são congruentes módulo n se os restos de sua divisão euclidiana por n são iguais. E escrevemos $a \equiv b\ mod(n)$*

Proposição 2.1. *Se $a,b,m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b\ mod(n)$ se, e somente se, $n|b-a$.*

Demonstração. Sejam $a = nq + r$, com $0 \leq r < n$ e $b = nq' + r'$, com $0 \leq r' < n$, as divisões euclidianas de a e b por n, respectivamente. Logo, $b - a = n(q' - q) + (r' - r)$.

Portanto, $a \equiv b \bmod(n)$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $n|b-a$, já que $|r - r'| < n$. □

Proposição 2.2. *sejam $a,b,c,d,n \in \mathbb{Z}$, com $n > 1$.*

(i) Se $a \equiv b\ mod(n)$ e $c \equiv d\ mod(n)$, então $a + c \equiv b + d\ mod(n)$.

(ii) Se $a \equiv b\ mod(n)$ e $c \equiv d\ mod(n)$, então $ac \equiv bd\ mod(n)$.

Demonstração. Suponhamos que $a \equiv b \bmod(n)$ e $c \equiv d \bmod(n)$. Logo, temos que $n|b-a$ e $n|d-c$.

(i) Basta observarmos que $n|(b-a)+(d-c)$ e, portanto $n|(b+d)-(a+c)$, o que prova essa parte do resultado.

(ii) Basta observarmos que $bd-ac = d(b-a)+a(d-c)$ e concluir que $n|bd-ac$.

□

Definição 2.5. *A classe de equivalência de $x \in \mathbb{Z}$ modulo n è o conjunto*

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

.

Note que $x + n \cdot \mathbb{Z} = x + n \cdot a; a \in \mathbb{Z}$

Assim temos que se $y \in \overline{x} \iff y \equiv x \bmod(n) \iff n|(y-x) \iff (y-x) = n \cdot a, a \in \mathbb{Z} \iff y = x + n \cdot a \iff y \in x + n \cdot \mathbb{Z}$

Portanto $\overline{x} = x + n \cdot \mathbb{Z}$ Denotaremos por $\mathbb{Z}_n$ o conjunto de todas as classes de equivalência modulo n, isto é, $\mathbb{Z}_n = \{\overline{x}; x \in \mathbb{Z}\}$. outra notação para $\mathbb{Z}_n$ é $\frac{\mathbb{Z}}{n\mathbb{Z}}$

Lema 2.1. *Sejam x,y $\in \mathbb{Z}$ e n$\in \mathbb{N}$,n ≥ 1. Então:*

$$\overline{x} = \overline{y} \iff x \equiv y\, mod(n)$$

Demonstração. ($\Longrightarrow$) Suponha $\overline{x} = \overline{y}$. Como $x \equiv x \bmod(n) \Longrightarrow x \in \overline{x} = \overline{y} \Longrightarrow x \in \overline{y} \Longrightarrow x \equiv y \bmod(n)$

($\Longleftarrow$) Suponha $x \equiv y \bmod(n)$, e tome $z \in \overline{x}$, temos que $z \equiv x \bmod(n) \Longrightarrow z \equiv y \bmod(n) \Longrightarrow z \in \overline{y} \Longrightarrow \overline{x} \subseteq \overline{y}$.

Seja agora $w \in \overline{y} \Longrightarrow w \equiv y \bmod(n) \Longrightarrow z \equiv x \bmod(n) \Longrightarrow z \in \overline{x} \Longrightarrow \overline{y} \subseteq \overline{x}$ e portanto $\overline{x} = \overline{y}$. □

Proposição 2.3. *Se $n \in \mathbb{N}$, $n \geq 1$, então $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ é um conjunto com exatamente n elementos.*

Demonstração. Pela definição de $\mathbb{Z}_n$, temos que o conjunto $\{\overline{1}, \overline{2}, \ldots, \overline{n-1}\} \subseteq \mathbb{Z}_n$, Devemos mostrar a inclusão contrária.

Seja $\overline{x} \in \mathbb{Z}_n$ então $x = pn + q$ *com* $0 \leq q \leq n-1$, Assim $q \in \{\overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ como $x = pn + q \Longrightarrow x - q = pn \Longrightarrow n \mid (x-q) \Longrightarrow x \equiv q \bmod(n) \Longrightarrow \overline{x} = \overline{q} \Longrightarrow \overline{x} \in \{\overline{1}, \overline{2}, \ldots, \overline{n-1}\}$.

Devemos mostrar que os elementos de $\{\overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. São dois a dois distintos. Suponha $x, y \in \{1, 2, \ldots, n-1\}$ com $x \neq y$ e $\overline{x} = \overline{y}$. Como $\overline{x} = \overline{y} \Longrightarrow x \equiv y \bmod(n) \Longrightarrow n \mid (x-y)$.

Assumindo, sem perda de generalidade, que $x > y$. Como $0 \leq x, y < n-1$ temos que $x-y < n-1$ e como $n \mid (x-y)$ temos que $x-y = 0$ *ou seja*, $x = y$. Contradição pois $x \neq y$. Assim concluímos que os elementos de $\mathbf{Z}_n$ são dois a dois distintos, e portanto $\mathbb{Z}_n = \{\overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ tem exatamente n elementos. □

Sejam $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Definiremos adição e multiplicação, respectivamente por:

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

(ii) $\overline{a}\overline{b} = \overline{ab}$

Proposição 2.4. *Sejam $n \in \mathbb{N}, n \geq 1$. Se $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$, então:*

(i) $\overline{x} + \overline{y} = \overline{a} + \overline{b}$

(ii) $\overline{x} \cdot \overline{y} = \overline{a} \cdot \overline{b}$

Demonstração. (i) Se $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$, pelo lema 2.1 temos que $x \equiv a \bmod(n)$ e $y \equiv b \bmod(n)$ e assim temos que $x + y \equiv a + b \bmod(n)$.

(ii) A demonstração segue de maneira análoga a (i).

□

Exemplo 2.4. $(\mathbb{Z}_n, +)$

(i) É associativa, pois a soma de inteiros é associativa,

(ii) O elemento neutro é $\overline{0}$,

(iii) Para todo $\overline{x}$, existe $\overline{y}$, tal que $\overline{x} + \overline{y} = \overline{0}$, basta tomar $\overline{y} = \overline{n-x}$,

(iv) Note também que $\overline{x} + \overline{y} = \overline{y} + \overline{x}$.

Portanto $(\mathbb{Z}_n, +)$ é um grupo abeliano finito, pois a ordem de $\mathbb{Z}_n$ é n.

2.1.1 Tabela de Cayley para grupos finitos

Seja $(G, *)$ um grupo finito. Suponha que $G = \{e, a_1, \ldots, a_{n-1}\}$ onde e é o elemento neutro de G. A operação binaria $*$ pode ser representada pela tabela

$*$	e	a_1	$\cdots$	a_{n-1}
e	e	a_1	$\cdots$	a_{n-1}
a_1	a_1	$a_1 * a_1$	$\cdots$	$a_1 * a_{n-1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_{n-1}	a_{n-1}	$a_{n-1} * a_1$	$\cdots$	$a_{n-1} * a_{n-1}$

Essa é tabela de Cayley para o grupo $(G,*)$.

Exemplo 2.5. *Construa a tabela de Cayley para o grupo* $(G,\cdot)$ *onde* $G=\{-1,1\}$

$\cdot$	*-1*	*1*
-1	*1*	*-1*
1	*-1*	*1*

note que o elemento neutro de G é 1, e o inverso de 1 é 1, e o inverso de -1 é -1.

Exemplo 2.6. *Construa a tabela de Cayley para* $(\mathbb{Z}_5,+)$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Exemplo 2.7. *Construa a tabela de Cayley para* $\mathbb{Z}_5^*=\{\overline{1},\overline{2},\overline{3},\overline{4}\}$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Com a proposição abaixo vamos assegurar propriedades básicas dos grupos , que dentre elas estão a unicidade do elemento neutro e que cada elemento de um grupo possui um único elemento inverso.

Proposição 2.5. *Seja* $(G,*)$ *um grupo:*

(i) Existe um único elemento neutro em G.

(ii) Para cada $a\in G$ *existe um único inverso em G*

(iii) Se $a\in G$ *e* $a'\in G$ *é o inverso de a, então o inverso de a' é a, isto é* $(a')'=a$.

(iv) Se $a,b\in G$ *e* $a',b'\in G$ *são os inversos de a e b, respectivamente, então o inverso de* $a*b$ *é* $b'*a'$

Demonstração. Assumindo as hipóteses.

(i) suponha que existam e e $f \in G$ tal que $a*e = e*a = a$ e $a*f = f*a = a$ para todo $a \in G$, em particular $f*e = e*f = f$ e $e*f = f*e = e$, assim $f*e = f$ e $f*e = e$ logo, $e = f$.

(ii) Suponha que a' e a"são inverso de a,ou seja $a*a' = a'*a = e$ e $a*a" = a"*a = e$ então temos que

$$a' = e*a'$$

onde e é o elemento neutro de G,

$$a' = (a"*a)*a'$$

$$a' = a"*(a*a')$$

$$a' = a"*e = a"$$

(iii) Suponha a' o inverso de a, ou seja $a'*a = a*a' = e$, assim

$$(a')' = (a')'*e$$

$$(a')' = (a')'*(a'*a)$$

$$(a')' = ((a')'*a')*a$$

$$(a')' = e*a = a$$

(iv) Devemos mostrar que $(a*b)*(b'*a') = e$ onde a' e b' são os inversos de a e b, respectivamente. $(a*b)*(b'*a') = a*(b*b'*a') = a*(b*b')*a' = a*(e*a') = a*a' = e$ assim provamos que $(a*b)' = b'*a'$

□

Proposição 2.6. *Dados $a,b \in G$ então as equações $a*x = b$ e $a*y = b$ tem soluções únicas para x e para y em G. Em particular,vale a lei do cancelamento.*

$$a*u = a*w \text{ , então } u = w$$

e

$$u*a = w*a \text{ , então } u = w$$

Demonstração. Temos que $a*x=b$ e $a*y=b$, então:

$$a*x=a*y$$

Operando em ambos os lados da igualdade por a', onde $a'*a=a*a'=e$,ou seja a' é o inverso de a, e e é o elemento neutro de G. Assim:

$$a'*(a*x)=a'*(a*y)$$

$$(a'*a)*x=(a'*a)*y$$

$$e*x=e*y$$

$$x=y$$

Em particular, se

$$a*u=a*w,$$ Basta fazer u=x e w=y, daí temos que u=w

e

$$u*a=w*a$$

$$(u*a)*a'=(w*a)*a'$$

$$u*(a*a')=w*(a*a')$$

$$u*e=w*e$$

$$u=w$$

□

2.1.2 Potências de um elemento em um grupo

Seja G um grupo multiplicativo e $x \in G$, então definimos as potências de x por

$$x^n = \begin{cases} e & \text{se } n = 0 \\ \underbrace{x \cdot x \cdots x}_{n \text{ vezes}} & \text{se } n > 0 \\ (x^{-1})^{|n|} & \text{se } n < 0 \end{cases}$$

Seja G m grupo aditivo e $x \in G$, então definimos as potências de x por

$$nx = \begin{cases} e & \text{se } n = 0 \\ \underbrace{x + x + \cdots + x}_{n \text{ vezes}} & \text{se } n > 0 \\ |n|(-x) & \text{se } n < 0 \end{cases}$$

Exemplo 2.8. *Seja o grupo aditivo* $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ *assim as potências do elemento* $\overline{4}$ *são:*

$$\begin{array}{rcccl} 1 \cdot \overline{4} & = & & = & \overline{4} \\ 2 \cdot \overline{4} & = & \overline{4} + \overline{4} & = & \overline{2} \\ 3 \cdot \overline{4} & = & \overline{4} + \overline{4} + \overline{4} & = & \overline{0} \\ 4 \cdot \overline{4} & = & \overline{4} + \overline{4} + \overline{4} + \overline{4} & = & \overline{4} \\ 5 \cdot \overline{4} & = & \overline{4} + \overline{4} + \overline{4} + \overline{4} + \overline{4} & = & \overline{2} \end{array}$$

e assim por diante.

Exemplo 2.9. *Seja o grupo multiplicativo* $\mathbb{U}_5 = \{\overline{x} \in \mathbb{Z}_5; (x,5) = 1\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$*, assim as potências do elemento* $\overline{3}$ *são:*

$$\begin{array}{rcccl} \overline{3}^1 & = & & = & \overline{3} \\ \overline{3}^2 & = & \overline{3} \cdot \overline{3} & = & \overline{4} \\ \overline{3}^3 & = & \overline{3} \cdot \overline{3} \cdot \overline{3} & = & \overline{2} \\ \overline{3}^4 & = & \overline{3} \cdot \overline{3} \cdot \overline{3} \cdot \overline{3} & = & \overline{1} \\ \overline{3}^5 & = & \overline{3} \cdot \overline{3} \cdot \overline{3} \cdot \overline{3} \cdot \overline{3} & = & \overline{3} \end{array}$$

e assim por diante.

2.2 Subgrupos

Nesta seção estudaremos os subgrupos, que são grupos contidos em grupos, estudaremos subgrupos gerados por elementos e ordem de elementos de um grupo.

A partir de agora usaremos preferencialmente a notação de grupo multiplicativo $(G,\cdot)$ para um grupo qualquer $(G,*)$. Assim evitaremos usar $*$ entre os elementos e $a*b$ será escrito como $a\cdot b$ ou somente ab, e também iremos denotar o elemento inverso a' por a^{-1}. Quando formos tratar de grupos aditivos, as ressalvas serão feitas quando necessárias.

Definição 2.6. *Seja $(G,\cdot)$ um grupo e H um subconjunto não vazio de G. Dizemos que H é subgrupo de G, se $(H,\cdot)$ é um grupo, e escrevemos $H \leq G$.*

Como a operação $\cdot$ é associativa para os elementos de G, então ela também é associativa para os elementos de H, assim para verificar se um subconjunto H, é subgrupo de G, devemos verificar os seguintes axiomas em relação a operação que define G.

(i) $a\cdot b \in H$ para todos $a,b \in H$

(ii) Existe $e_H \in H$ onde e_H é o elemento neutro de H.

(iii) Se $a \in H$ então $a^{-1} \in H$ tal que $a\cdot a^{-1} = a^{-1}\cdot a = e_H$

Se H é subgrupo G, então existem e_H e e_G em H e G respectivamente. Também para cada $a \in H$ existem os inversos a_H^{-1} e a_G^{-1} em H e G respectivamente. Na proposição abaixo iremos provar que $e_H = e_G$ e $a_H^{-1} = a_G^{-1}$.

Proposição 2.7. *Sejam $(G,\cdot)$ um grupo, $H \leq G$ e $a \in H$ então*

(i) $e_H = e_G$

(ii) $a_H^{-1} = a_G^{-1}$

Demonstração. De fato.

(i) temos que $e_H\cdot e_H = e_H$, como $e_H \in G$ temos que $e_H\cdot e_G = e_H$, e portanto $e_H\cdot e_G = e_H\cdot e_H$ se tomarmos o inverso u de e_H em G.

$$u\cdot(e_H\cdot e_G) = u\cdot(e_H\cdot e_H)$$

$$(u\cdot e_H)\cdot e_G = (u\cdot e_H)\cdot e_H$$

$$e_G\cdot e_G = e_G\cdot e_H$$

$$e_G = e_H$$

(ii) Temos que $e_G = e_H = e$, assim $a_H^{-1}\cdot a = a\cdot a_H^{-1} = e$ e $a_G^{-1}\cdot a = a\cdot a_G^{-1} = e$. Portanto $a_H^{-1}\cdot a = a_G^{-1}\cdot a$ e pela unicidade do elemento inverso temos que $a_H^{-1} = a_G^{-1}$

□

Exemplo 2.10. *Verifique se* $(n\mathbb{Z},+)$ *é subgrupo de* $(\mathbb{Z},+)$

Solução

(i) *Para todos* $x,y \in n\mathbb{Z}$*, temos que* $x+y \in n\mathbb{Z}$

(ii) $0 \in n\mathbb{Z}$

(iii) *para todo* $x \in n\mathbb{Z}$*, existe* $x^{-1} \in n\mathbb{Z}$ *tal que* $x+x^{-1} = x^{-1}+x = 0$*,se* $x = n\cdot a$ *com* $a \in \mathbb{Z}$*, basta tomar* $x^{-1} = n\cdot(-a)$.

Exemplo 2.11. *Verifique se* $H = \{\overline{0},\overline{3},\overline{6},\overline{9},\overline{12}\}$ *é subgrupo de* $(\mathbb{Z}_{15},+)$

Iremos fazer essa verificação por meio da tabela de Cayley.

+	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$
$\overline{0}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{12}$	$\overline{0}$
$\overline{6}$	$\overline{6}$	$\overline{9}$	$\overline{12}$	$\overline{0}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{12}$	$\overline{0}$	$\overline{3}$	$\overline{6}$
$\overline{12}$	$\overline{12}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$

Note que a soma é fechada para H, que o elemento neutro de $\mathbb{Z}_{15}$ *é o* $\overline{0} \in H$ *e que para cada* $a \in H$ *existe* $a^{-1} \in H$*. Assim H é subgrupo de* $\mathbb{Z}_{15}$*, ou seja,* $H \leq \mathbb{Z}_{15}$.

Note que todo grupo G possui pelo menos dois subgrupos, $\{e\}$ e G, e são ditos **subgrupos triviais** de G, e qualquer outro subgrupo H de G chamaremos de **subgrupo próprio** de G e denotaremos por $H < G$

Proposição 2.8. *Seja H um subconjunto não vazio do grupo G. São equivalentes.*

(i) $H \leq G$

(ii) $a,b \in H \Longrightarrow a\cdot b^{-1} \in H$

Demonstração. É claro que se $H \leq G$ então $a\cdot b^{-1} \in H$, pois $a,b \in H \Longrightarrow b^{-1} \in H$ e então $a\cdot b^{-1} \in H$. Devemos mostrar agora que a reciproca é verdadeira, se $a\cdot b^{-1} \in H$, com $a,b \in H$ então $H \leq G$. Inicialmente , como a operação em H é a mesma que em G e G é um grupo, então a associatividade em H está garantida.

Vamos verificar agora que o elemento neutro está em H. De (ii) temos que $b\cdot b^{-1} \in H$ como $b \in G$ e G é um grupo, então $b\cdot b^{-1} = e$ e portanto $e \in H$.

Vamos verificar agora o elemento inverso. Como $e, b \in H$ então $e \cdot b^{-1} \in H \Longrightarrow b^{-1} \in H$ para todo $b \in H$.

Temos que para $a, b \in H \Longrightarrow a, b^{-1} \in H \Longrightarrow a \cdot (b^{-1})^{-1} \in H \Longrightarrow a \cdot b \in H$ e portanto a operação é fechada para H. □

Exemplo 2.12. *Verifique se* $X = \{\overline{1}, \overline{4}\}$ *é subgrupo do grupo* $(\mathbb{Z}_5^*, \cdot)$

Note que sendo $a = \overline{1}$ *e* $b = \overline{4}$*, temos que* $\overline{4}^{-1} = \overline{4}$ *pois* $\overline{4} \cdot \overline{4} = \overline{1}$*, assim* $ab^{-1} = \overline{1} \cdot \overline{4} = \overline{4} \in \mathbb{Z}_5^*$.

Assim $X \leq \mathbb{Z}_5^*$

2.2.1 Subgrupos gerados por um elemento

Iremos apresentar agora uma maneira de produzir subgrupos a partir de um elemento de um grupo G.

Definiremos o conjunto

$$\langle x \rangle = \{x^m; m \in \mathbb{Z}\}$$

Proposição 2.9. *Sejam G um grupo e* $x \in G$*. Então* $\langle x \rangle$ *é subgrupo abeliano de G, que denotamos* $\langle x \rangle$*, e chamamos de subgrupo gerado por x.*

Demonstração. Sejam $a, b \in \langle x \rangle$, para $\langle x \rangle$ ser subgrupo de G, temos que mostrar que $ab^{-1} \in \langle x \rangle$.

Note que $a = x^m$ e $b = x^n$ para $m, n \in \mathbb{Z}$, assim $b^{-1} = (x^n)^{-1} = x^{-n}$, logo $ab^{-1} = x^m \cdot x^{-n} = x^{m-n} \in \langle x \rangle$, portanto $\langle x \rangle \leq G$.

Iremos mostrar agora a comutatividade, $ab = x^m \cdot x^n = x^{m+n} = x^{n+m} = x^n \cdot x^m = ba$, assim $\langle x \rangle$ é subgrupo abeliano. □

2.2.2 Ordem de um elemento de um grupo

Definição 2.7. *Sejam G, um grupo, e* $x \in G$*. A ordem de x é a ordem do subgrupo gerado por x, isto é,* $|\langle x \rangle|$.

A ordem de x será indicada por $o(x)$ ou por $|x|$

Proposição 2.10. *Sejam G um grupo e* $x \in G$*. São equivalentes:*

(i) $o(x) = n < \infty$

(ii) $\exists\, r \in \mathbb{N}^*$ *tal que* $x^r = e$, $\langle x \rangle = \{e, x, x^2, \ldots x^{n-1}\}$, $n = min\{r \in \mathbb{N}^*; x^r = e\}$ *e* $n|r$.

Demonstração. $(i) \Longrightarrow (ii)$. Se $o(x) = n$, então $\langle x \rangle = \{x^k; k \in \mathbb{Z}\}$ é um subgrupo finito com n elementos. Sejam $p, q \in \mathbb{Z}$, com $p \neq q$ tais que $x^p = x^q$ assim $x^p x^{-q} = x^q x^{-q}$. Segue que $x^{p-q} = e$, sem perda de generalidade podemos assumir que $p > q$. Basta tomar $r = p - q$, daí $x^r = e$.

Afirmamos que $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$

Note que a inclusão $\{e, x, x^2, \ldots, x^{n-1}\} \subseteq \langle x \rangle$ é obvia, pois existe $r \in \mathbb{N}^*$, tal que $x^r = e$. Iremos provar a inclusão contraria agora. Seja $a = x^t \in \langle x \rangle$, pelo algorítimo da divisão euclidiana, $t = cn + b$ onde $0 \leq b < n$, assim $x^t = x^{cn+b} = x^{cn} x^b = (x^n)^c x^b = e x^b = x^b$, como $0 \leq b < n$, isso implica que $a \in \{e, x, x^2, \ldots, x^{n-1}\}$, ou seja $\langle x \rangle \subseteq \{e, x, x^2, \ldots, x^{n-1}\}$, portanto $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$.

Vamos mostrar que $n = min\{r \in \mathbb{N}^*; x^r = e\}$. Suponha que que não, então existe $n - k \in \{r \in \mathbb{N}^* \,;\, x^r = e\}$, ou seja, $x^{n-k} = e$, assim $x^{n-k} x = x$, segue que $x^{n-k+1} = x$ daí $n = k$, absurdo, pois $n - k \in \mathbb{N}^*$.

Vamos provar agora que se $x^r = e$ com $r \in \mathbb{N}^*$ então $n|r$. Dividindo r por n, existem $a, b \in \mathbb{Z}$ tais que $r = an + b$ com $0 \leq b < n$, temos que $x^r = x^{an+b} = x^{an} x^b = (x^n)^a x^b = e x^b = x^b = e$, se $b \neq 0$ isso contradiz a minimalidade de n, portanto $b = 0$ e $r = an$ portanto $n|r$.

$(i) \Longleftarrow (ii)$. Basta mostrarmos que os elementos de $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$ são dois a dois distintos. Suponha que não, então existem $u, w \in \mathbb{Z}$ com $0 < u, w < n$ tais que $x^u = x^w$ e $u \neq w$, sem perda de generalidade, tomamos $u - w > 0$ e $x^{u-w} = e$. Absurdo, pois fere a minimalidade de n, então $o(x) = n = min\{r \in \mathbb{N}^* \,; x^r = e\}$ e $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$.

□

Exemplo 2.13. *Qual a ordem de* $\overline{7} \in \mathbb{Z}_{11}^*$

Solução

Temos que pelo pequeno teorema de Fermat:

$7^{10} \equiv 1$ *mod* 11 *ou seja,* $\overline{7}^{10} = 1$ *em* $\mathbb{Z}_{11}^*$

Pela proposição acima a $o(\overline{7})|10$*, logo* $o(\overline{7}) \in \{1, 2, 5, 10\}$*, verificando cada caso:*

$\overline{7}^1 = \overline{7}$

$\overline{7}^2 = \overline{5}$

$\overline{7}^5 = \overline{7}^2 \cdot \overline{7}^2 \cdot \overline{7} = \overline{5} \cdot \overline{5} \cdot \overline{7} = \overline{10}$

$\overline{7}^{10} = \overline{7}^5 \cdot \overline{7}^5 = \overline{10} \cdot \overline{10} = \overline{1}$.

Portanto em $\mathbb{Z}_{11}^*$ *a* $o(\overline{7}) = 10$.

Definição 2.8. *Um grupo G será chamado de grupo cíclico se* $G = \langle x \rangle$ *para algum* $x \in G$ *ou seja G é gerado por um elemento.*

Exemplo 2.14. *Considere o grupo aditivo* $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

Usando a definição de potencias de um elemento no grupo aditivo temos que:

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

$\langle 2 \rangle = \{\overline{0}, \overline{2}, \overline{4}\}$

$\langle 3 \rangle = \{\overline{0}, \overline{3}\}$

$\langle 4 \rangle = \{\overline{0}, \overline{4}, \overline{2}\}$

$\langle 5 \rangle = \{\overline{0}, \overline{5}, \overline{4}, \overline{3}, \overline{2}, \overline{1}\}$

Assim o grupo aditivo $\mathbb{Z}_6$ *é cíclico e seus geradores são* $\overline{1}$ *e* $\overline{5}$

Proposição 2.11. *Seja* $G = \langle a \rangle$ *um grupo cíclico de ordem n. Os geradores de G são da forma* a^r*, onde* $(r,n) = 1$

Demonstração. $(\Longrightarrow)$ Seja $a^r \in G$ um gerador de G. E suponha que $(n,r) = k$, assim $n = xk$ e $r = yk$

$(a^r)^x = a^{rx} = a^{ykx} = a^{xky} = (a^{xk})^y = (a^n)^y = e^y = e$. Temos que $o(a^r) = y < n$, absurdo. Pois contradiz a minimalidade de n. Portanto o mdc $(r,n) = 1$.

$(\Longleftarrow)$ Queremos mostrar que se r e n são coprimos, então a^r gera o grupo G, ou seja, $o(a^r) = n$ e se $(a^r)^k = e$, então $k = xn$. Observe que $o(a) = n$, e suponha que $(a^r)^k = e$, $a^{rk} = e$ logo a $o(a)|rk$, ou seja, $n|rk$ como $(r,n) = 1$, isso implica que $n|k \Longrightarrow k = xn$. Portanto a^r gera G. □

2.2.3 Classes Laterais e o Teorema de Lagrange

Para fazermos o estudo sobre o teorema de Lagrange, devemos primeiro definir classes laterais e estudar algumas propriedades básicas das classes laterais.

Proposição 2.12. *Sejam G um grupo, H um subgrupo de G e* $x, y \in H$*. A relação R sobre G definida por*

$$xRy \Longleftrightarrow x^{-1}y \in H$$

é uma relação de equivalência.

Demonstração. Devemos mostrar que essa relação é reflexiva, simétrica e transitiva.

(i) Reflexiva: Seja $x \in G$, então existe $x^{-1} \in G$, tal que $x^{-1}x = e$ como $e \in H$ temos que xRx é uma relação reflexiva.

(ii) Simétrica: Seja $x, y \in G$. Se yRx, então $x^{-1}y \in H$ e portanto $(x^{-1}y)^{-1} = y^{-1}x \in H$. Logo xRy e a relação é simétrica.

(iii) Transitiva:Sejam $x, y, z \in G$ e yRx e xRz temos que $x^{-1}y \in H$ e $z^{-1}x \in H$. Logo $(z^{-1}x)(x^{-1}y) = z^{-1}(xx^{-1}y) = z^{-1}(ey) = z^{-1}y \in H \Longrightarrow yRz$. Portanto a relação R é transitiva.

□

De maneira análoga, se G é um grupo e H é subgrupo de G, a relação R definida por $xR^*y \Longleftrightarrow yx^{-1} \in H$ é uma relação de equivalência.

Observe que se $yRx \Longleftrightarrow x^{-1}y \in H$, então existe $h \in H$ tal que $x^{-1}y = h \Longrightarrow y = xh$, ou seja, $y \in xH = \{xh\ ; h \in H\}$. Logo a classe de equivalência de $x \in G$, definida pela relação R é $\{y \in G | yRx\} = xH$. De maneira análoga, quando a relação é $yR^*x \Longleftrightarrow yx^{-1}$, a classe de equivalência de $x \in G$ é $\{y \in G | yR^*x\} = Hx$

Definição 2.9. *A classe de equivalência $xH = \{xh\ , tal\ que\ h \in H\}$ é chamada de* ***Classe lateral de x à esquerda*** *de H em G. De maneira análoga, $Hx = \{hx\ , tal\ que\ h \in H\}$ é chamada de* ***classe lateral de x a direita*** *de H em G.*

Observação 1: Se G é um grupo aditivo, denotamos as classes gH e Hg, por:

$$g + H = \{g + h | h \in H\}$$

e

$$H + g = \{h + g | h \in H\}$$

Respectivamente.

Observação 2: Se o grupo G é abeliano e H é subgrupo de G, então

$$gH = Hg \text{ para todo } g \in G$$

Neste caso H é chamado de subgrupo normal de G.

Exemplo 2.15. *Determine as classes laterais a esquerda e a direita do subgrupo* $H = \{\overline{0}, \overline{3}\}$ *no grupo aditivo* $(\mathbb{Z}_6, +)$.

Solução

Como $\mathbb{Z}_6$ *é um grupo aditivo abeliano, então as classes laterais a esquerda e a direita coincidem e se escrevem com notação aditiva.* $x+H = \{x+h | h \in H\}$ *e* $H+x = \{h+x | h \in H\}$

$0+H = H+0 = \{0,3\} = \overline{0} = \overline{3}$

$1+H = H+1 = \{1,4\} = \overline{1} = \overline{4}$

$2+H = H+2 = \{2,5\} = \overline{2} = \overline{5}$

Note que $0+H = 3+H, 1+H = 4+H$ *e assim por diante.*

Logo $(0+H) \cap (1+H) = \varnothing$, $(0+H) \cap (2+H) = \varnothing$ *e* $(1+H) \cap (2+H) = \varnothing$, *ou seja, são dois a dois disjuntos e portanto* $\mathbb{Z}_6 = (0+H) \cup (1+H) \cup (2+H)$

Lema 2.2. *Seja G um grupo, H um subgrupo de G e* $x, y \in G$

(i) $y \in xH \iff xH = yH$

(ii) $y \in Hx \iff Hx = Hy$

Demonstração. .

(i) $(\Longrightarrow)$ Suponha que $y \in xH$, então por definição yRx e pela propriedade simétrica xRy, vamos mostrar agora que $xH \subset yH$. seja $u \in xH$, assim uRx, e pela transitividade uRy,ou seja, $u \in yH$.

vamos mostrar agora a inclusão contraria $xH \supset yH$. Seja $w \in yH$, assim wRy pela transitividade wRx, assim temos que $xH \supset yH$ e portanto $xH = yH$.

$(\Longleftarrow)$ Suponha agora $xH = yH$, é claro que $y \in yH$ pois $e \in H$ e $y = ye \in yH$, como $xH = yH$, temos que $y \in xH$.

(ii) A demonstração do item (ii) é análoga a demonstração do item (i). Basta trocar a lateralidade e R por $R*$.

□

Corolário 2.1. *Sejam G um grupo e* $H \leq G$, *então*

(i) Duas classes laterais à esquerda (ou à direita) são iguais ou disjuntas.

(ii) A união das classes laterais à esquerda (ou à direita) é G.

Demonstração. (i) Sejam duas classes laterais a esquerda xH e yH tal que $xH \cap yH \neq \varnothing$, ou seja, existe $z \in xH$ e $z \in yH$,pelo lema 2.2 temos que $zH = xH$, como $z \in yH$ também pelo lema 2.2 temos que $zH = yH$ e portanto $xH \cap yH = \varnothing$ ou $xH = yH$.

(ii) Seja $X = \{x_1H, x_2H, \ldots, x_rH\}$ com $x_i \in G$ para todo $i \in \{1,2,\ldots,r\}$ O conjunto das classes laterais a esquerda de H em G que são disjuntas.Devemos mostrar que $G = \bigcup x_iH$.
Note que $x_iH \subset G \, \forall i \in \{1,2,\ldots r\}$, logo a inclusão $\bigcup x_iH \subset G$ é obvia.
Seja agora $z \in G$, temos que a classe lateral $zH \in X$. Como $z \in zH \subseteq \bigcup x_iH$, então $G \subseteq \bigcup x_iH$.

□

Proposição 2.13. *Sejam G um grupo, H um subgrupo de G e x ∈ G, então*

(i) Toda classe lateral de H em G tem |H| elementos.

(ii) A cardinalidade da classe lateral xH é igual a cardinalidade da classe lateral Hx.

Demonstração. .

(i) Temos que mostrar que $|xH| = |Hx| = |H|$.
Considere as funções

$$\begin{array}{ccccccccc} \text{f} & : & \text{H} & \longrightarrow & \text{xH} & \quad \text{g} & : & \text{H} & \longrightarrow & \text{Hx} \\ & & \text{h} & \longmapsto & \text{xh} & \text{e} & & \text{h} & \longmapsto & \text{hx} \end{array}$$

temos que mostrar que f e g são bijeções. Iremos mostrar para f e segue de maneira análoga para g. Seja $f(h) = f(k), \Longrightarrow xh = xk, \Longrightarrow x^{-1}xh = x^{-1}xk \Longrightarrow h = k$, logo f é injetiva. Iremos mostrar agora que f é sobrejetora, seja $w \in xH$, temos que $u = xh$ para $h \in H$ assim $f(h) = xh = u$ logo f é sobrejetora e portanto é uma bijeção, e de maneira análoga g também é uma bijeção.

(ii) Temos que mostrar a função abaixo é uma bijeção.

$$\begin{array}{ccccc} \text{f} & : & \{xH\,; x \in G\} & \longrightarrow & \{Hx\,; x \in G\} \\ & & \text{xH} & \longmapsto & Hx^{-1} \end{array}$$

Vamos verificar a injetividade. $f(xH) = f(yH) \Longrightarrow Hx^{-1} = Hy^{-1} \Longrightarrow x^{-1} \in Hy^{-1} \Longrightarrow x^{-1} = hy^{-1}$, *com* $h \in H \Longrightarrow x^{-1}y = h$, *com* $h \in H \Longrightarrow y = xh$, *com* $h \in H \Longrightarrow y \in xH \Longrightarrow xH = yH$ logo fé injetiva.
Agora iremos verificar a sobrejetividade de f, Seja $Hy \in \{Hx\,; x \in G\}$, note que existe $y^{-1}H \in \{xH\,; x \in G\}$ tal que $f(y^{-1}H) = Hy$. Assim f é sobrejetiva e portanto bijetiva

□

Definição 2.10. *Seja $H \leq G$, o índice de H em G é o numero de classes laterais a esquerda de H em G. O índice de um subgrupo pode ser finito ou infinito, e é indicado por $(G : H)$.*

Exemplo 2.16. *Seja o grupo* $(\mathbb{Z}_8,+)$ *e* $H=\{\overline{0},\overline{4}\}$. *Calcule* $(\mathbb{Z}_8:H)$*:*

Solução

Note que:

$\overline{0}+H=\{\overline{0},\overline{4}\}$

$\overline{1}+H=\{\overline{1},\overline{5}\}$

$\overline{2}+H=\{\overline{2},\overline{6}\}$

$\overline{3}+H=\{\overline{3},\overline{7}\}$

Assim, o conjunto de classes laterais a esquerda de H é $\{\overline{0}+H,\overline{1}+H,\overline{2}+H,\overline{3}+H\}$ e Portanto $(\mathbb{Z}_8:H)=4$

Teorema 2.1 (Lagrange)**.** *Seja G um grupo finito e seja* $H\leq G$. *Então* $(G:H)=\frac{|G|}{|H|}$, *em particular* $|H|$ *divide* $|G|$.

Demonstração. Se G é um grupo finito, então $(G:H)=n$.

Seja $\{x_iH\ ;x_i\in G\}$ o conjunto das classes laterais distintas à esquerda de H em G. Pelo corolário 2.1 temos que $x_iH\cap x_jH=\varnothing$ para todo $i\neq j$ e $G=x_1H\cup x_2H\cup\cdots\cup x_nH$ e pela proposição 2.13, temos que $|x_iH|=|H|$. Logo $|G|=\underbrace{|H|+|H|+\cdots+|H|}_{n\ vezes}\Longrightarrow|G|=|H|\cdot n$ e portanto $(G:H)=\frac{|G|}{|H|}$.

Note que $(G:H)$ é um numero inteiro, e em particular $|H|$ divide $|G|$. □

Corolário 2.2. *Seja G um grupo finito e* $g\in G$. *Então* $o(g)$ *divide* $|G|$.

Demonstração. Da definição de ordem, temos que $o(g)=|\langle g\rangle|$, da proposição 2.9 temos que $\langle g\rangle$ é um subgrupo de G e pelo teorema 2.1, isso mostra que $o(g)=|\langle g\rangle|$ divide $|G|$. □

Corolário 2.3. *Seja* $(G,\cdot)$ *um grupo finito então, para todo* $a\in G$, *temos que* $a^{|G|}=e$.

Demonstração. Do corolário 2.2 segue que $o(g)||G|$, e da proposição 2.10 $a^{o(g)}=e$. Se $o(g)=n\Longrightarrow|G|=kn$, logo $a^{|G|}=a^{kn}=(a^n)^k=e^k=e$ □

Corolário 2.4. *Todo grupo de ordem prima é cíclico e só tem subgrupos triviais.*

Demonstração. Se $|G|=p$ com p primo, então para $x\neq e$ temos que $|\langle x\rangle|\neq 1$ e como $\langle x\rangle$ é subgrupo de G, temos que $|\langle x\rangle|$ divide $|G|$, isto é $|\langle x\rangle|=p=|G|$. Logo concluímos que $\langle x\rangle=G$, ou seja G é cíclico.

Seja agora H um subgrupo de G, pelo teorema de Lagrange segue que $|H|$ divide $|G|$, assim temos que $|H| \mid p \Longrightarrow |H| = 1 ou |H| = p$.

Se $|H| = 1 \Longrightarrow H = \{e\}$ e se $|H| = p \Longrightarrow H = G$

□

Exemplo 2.17. *Determine todos os subgrupos de* $(\mathbb{Z}_6, +)$

Solução

Seja $H \leq \mathbb{Z}_6$*, Então* $|H| = 1, 2, 3$ *ou* 6.

Se $|H| = 1$*, então* $H = \{\overline{0}\}$.

Se $|H| = 6$*, então* $H = \mathbb{Z}_6$

Se $|H| = 2$ *ou* $|H| = 3$ *os subgrupos são cíclicos.*

Temos que $\overline{1}$ *e* $\overline{5}$ *geram* $\mathbb{Z}_6$*. Logo*

$\langle\overline{2}\rangle = \{\overline{0}, \overline{2}, \overline{4}\} = \langle\overline{4}\rangle$ *e* $\langle\overline{3}\rangle = \{\overline{0}, \overline{3}\}$

Portanto os subgrupos de $\mathbb{Z}_6$ *são*

$\{\overline{0}\}, \{\overline{0}, \overline{2}, \overline{4}\}, \{\overline{0}, \overline{3}\}$ *e* $\mathbb{Z}_6$

2.3 Homomorfismo e isomorfismo

Definição 2.11. *Uma função* $\varphi : (G, *) \longrightarrow (G', \triangle)$ *de um grupo noutro diz-se um homomorfismo de anéis se* $\varphi(x * y) = \varphi(x) \triangle \varphi(y)$*, para todo elemento x,y de G. Um isomorfismo é um homomorfismo bijetivo.*

Exemplo 2.18. $f : (\mathbb{R}^*, \cdot) \longrightarrow (\mathbb{R}^*, \cdot)$ *dada por* $f(x) = |x|$*,* $(\mathbb{R}^*, \cdot)$ *sendo o grupo multiplicativo dos números reais não nulos, é homomorfismo.*

De fato, pois seja $x_1, x_2 \in \mathbb{R}^*$, temos que $f(x_1 x_2) = |x_1 x_2| = |x_1||x_2| = f(x_1) f(x_2)$

Exemplo 2.19. *Mostraremos que* $f : (\mathbb{R}_+^*, \cdot) \longrightarrow (\mathbb{R}, +)$ *dada por* $f(x) = log(x)$ *para todo* $x \in \mathbb{R}_+^*$ *é um isomorfismo.*

Solução

Devemos mostrar que f é um homomorfismo e que f é bijetiva.

(i) Homomorfismo: sejam $x_1, x_2 \in \mathbb{R}_+^*$, então $f(x_1 x_2) = \log(x_1 x_2) = \log(x_1) + \log(x_2) = f(x_1) + f(x_2)$

(ii) Bijetiva:

(1) Injetividade: sejam $x_1, x_2 \in \mathbb{R}_+^*$ tal que $f(x_1) = f(x_2) \Longrightarrow \log(x_1) = \log(x_2) \Longrightarrow x_1 = x_2$ e portanto f é injetiva.

(2) Sobrejetividade: Seja $z \in \mathbb{R}$, tal que $z = \log(x) \Longrightarrow x = e^z$, portanto $x \in \mathbb{R}_+^*$ e f é sobrejetiva.

Iremos apresentar agora algumas propriedades básicas dos homomorfismos.

Proposição 2.14. *Sejam G e H grupos e $f : G \longrightarrow H$ um homomorfismo de grupos. Assim temos que*

(1) $f(e_G) = e_H$, onde e_G, e_H são os elementos neutros de G e H, respectivamente.

(2) $f(x^{-1}) = f(x)^{-1}$, para todo $x \in G$

(3) $f(x^n) = f(x)^n$, para todo $n \in \mathbb{Z}$

Demonstração. .

(1) $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$. Temos que
$f(e_G)f(e_G)^{-1} = f(e_G)f(e_G)f(e_G)^{-1} \Longrightarrow e_H = f(e_G)$.

(2) Temos que $f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H = f(x)f(x)^{-1}$.
Segue que $f(x^{-1}) = f(x)^{-1}$.

(3) $f(a^n) = f(\underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ vezes}}) = \underbrace{f(a) \cdot f(a) \cdot \cdots \cdot f(a)}_{n \text{ vezes}} = f(a)^n$.

□

De maneira geral, um homomorfismo entre grupos G e H enviam subgrupos de G em subgrupos H, é isso que vamos mostrar no lema a seguir. Devemos lembrar que o conjunto imagem de uma aplicação de G em H é dada pelo conjunto $\text{Im}(f) = \{y \in H \ : \ y = f(x) \text{ para algum } x \in G\}$. E para $S \subseteq G$ temos que a imagem de S por f é dada por $f(S) = \{f(x) \ : \ x \in S\}$.

Lema 2.3. *Sejam G e H grupos, S um subgrupo de G, e $f : G \longrightarrow H$ um homomorfismo. Então $f(S)$ é um subgrupo de H. Em particular, $Im(f) = f(G)$ é um subgrupo de H.*

Demonstração. Considere o conjunto $f(S) = \{f(x) \ ; \ x \in S\}$, note que $f(S)$ é não vazio, pois $e_G \in S$ e $f(e_G) = e_H$ pois f é um homomorfismo. Para todos $x, y \in f(S)$ existem $a, b \in S$, tais que $f(a) = x$ e $f(b) = y$, então $x, y \in f(S)$, Usando o critério de subgrupo, devemos mostrar que $xy^{-1} \in f(S)$. Ora, note que S é subgrupo de G, então temos que $ab^{-1} \in S$ e assim $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = xy^{-1} \in f(S)$. Portanto $f(S)$ é subgrupo de H.

Em particular G é subgrupo trivial de G, e portanto $f(G) = \text{Im}(f)$ é subgrupo de H. □

De maneira geral os algebristas não se preocupam com a natureza dos elementos de um grupo, se preocupam como esses elementos se operam, por isso não fazem distinção de grupos isomorfos, ou seja quando existe um isomorfismo entre eles. É neste sentido que apresentaremos as proposições abaixo.

Proposição 2.15. *Todo grupo cíclico de ondem infinita é isomorfo ao grupo aditivo dos inteiros.*

Demonstração. Seja G um grupo infinito, $a \in G$ tal que $G = \langle a \rangle$ e $f : \mathbb{Z} \longrightarrow G$ definida por $f(n) = a^n$. Devemos mostrar que f é um isomorfismo.

A aplicação f é um homomorfismo pois dados $m,n \in \mathbb{Z}$ temos que $f(m+n) = a^{m+n} = a^m a^n = f(m)f(n)$

por outro lado, se $f(m) = f(n) \Longrightarrow a^m = a^n$, como G é infinito, temos que as potências de a são todas distintas, portanto se $a^m = a^n \Longrightarrow m = n$. Logo f é injetiva.

Para todo $x \in G$, existe $n \in \mathbb{Z}$ tal que $x = a^n$, assim f é sobrejetiva, e portanto é bijetiva mostrando que f é um isomorfismo. □

Proposição 2.16. *Seja G um grupo cíclico finito de ordem n, então G é isomorfo ao grupo aditivo* $\mathbb{Z}_n$

Demonstração. Seja $G = \{e, a, a^2, \ldots, a^{n-1}\}$ gerado por a. Considere $g : \mathbb{Z}_n \longrightarrow G$ definida por $g(\overline{k}) = a^k$. g é um isomorfismo.

Note que g é um homomorfismo pois dados $\overline{m}, \overline{k} \in \mathbb{Z}_n$ temos que $g(\overline{m} + \overline{k}) = g(\overline{m+k}) = a^{m+k} = a^m a^k = g(\overline{m})g(\overline{k})$.

Por outro lado se $g(\overline{m}) = g(\overline{k}) \Longrightarrow a^m = a^k \Longrightarrow a^{m-k} = e$ ou seja, $n \mid (m-k) \Longrightarrow m \equiv k \bmod n$, isto é, $\overline{m} = \overline{k}$. A sobrejetividade é óbvia, pois para cada $x \in G$ existe um $\overline{k} \in \mathbb{Z}_n$, tal que $x = a^k$, é claro, pois G é cíclico gerado por a.

Portanto g é um isomorfismo. □

Proposição 2.17. *Se $f : G \longrightarrow H$ é um isomorfismo, então $f^{-1} : H \longrightarrow G$ também é um isomorfismo.*

Demonstração. Seja $f : G \longrightarrow H$ é um isomorfismo, como f é bijetora, então f admite inversa f^{-1} que também é bijetora. Portanto só nos resta provar que f^{-1} é um homomorfismo.

Dados $x, y \in H$ existem $a, b \in G$ tais que $x = f(a)$ *e* $y = f(b)$, temos que $f^{-1}(x) = a$ *e* $f^{-1}(y) = b$. Assim

$$f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)f^{-1}(y).$$

Portanto f^{-1} é um isomorfismo. □

Seja o homomorfismo $f : G \longrightarrow H$ Definiremos agora o **núcleo** de f, e denotaremos por $\text{Ker}(f)$ da seguinte maneira $\text{Ker}(f) = \{x \in G : f(x) = e_H\}$.

Proposição 2.18. *Seja $f : G \longrightarrow H$ um homomorfismo, então*

(i) $Ker(f)$ é subgrupo de G.

(ii) f é injetivo se, e somente se, $Ker(f) = \{e_G\}$

Demonstração. .

(i) Note que $\text{Ker}(f) \neq \varnothing$ pois f é um homomorfismo e $f(e_G) = e_H$. Assim $e_G \in \text{Ker}(f)$ Sejam $a, b \in \text{Ker}(f)$, temos que $f(a) = e_H$ e $f(b) = e_H$. Note que $f(b)^{-1}f(b) = e_H = f(b) \Longrightarrow f(b)^{-1} = f(b^{-1}) = e_H$ Assim $f(ab^{-1}) = f(a)f(b^{-1}) = e_H e_H = e_H \Longrightarrow ab^{-1} \in \text{Ker}(f)$. Isso mostra que $\text{Ker}(f)$ é subgrupo de G

(ii) ($\Longrightarrow$) Suponha que f é injetora. Para todo $a \in \text{Ker}(f)$ temos que $f(a) = e_H$, como $f(e_G) = e_H$ e f é injetiva então $a = e_G$ para todo $a \in \text{Ker}(f)$ logo $\text{Ker}(f) = \{e_G\}$
($\Longleftarrow$) Suponha agora que $\text{Ker}(f) = \{e_G\}$ e seja $f(a) = f(b)$, temos que $f(a)f(b)^{-1} = f(b)f(b)^{-1} \Longrightarrow f(a)f(b^{-1}) = e_H \Longrightarrow f(ab^{-1}) = e_H \Longrightarrow ab^{-1} \in \text{Ker}(f)$. Mas como $\text{Ker}(f) = \{e_G\} \Longrightarrow ab^{-1} = e_G \Longrightarrow a = b$ e portanto f é injetiva.

□

3 ANÉIS

Definição 3.1. *Dizemos que $(A,+,\cdot)$ é um anel, se A é um conjunto não vazio que possui duas operações, as quais chamaremos de adição (+) e multiplicação ($\cdot$), definidas da seguinte maneira:*

$$\begin{array}{rcccl} + & : & A\,X\,A & \to & A \\ & & (x,y) & \mapsto & x+y \end{array} \qquad \begin{array}{rcccl} \cdot & : & A\,X\,A & \to & A \\ & & (x,y) & \mapsto & x\cdot y \end{array}$$

e que satisfazem os seguintes axiomas para todos $x,y,z \in A$

A1) $(x+y)+z = x+(y+z)$ *((Associatividade da soma)*

A2) $\exists 0 \in A$ *tal que ,* $0+x = x$ *e* $x+0 = x$ *para todo* $x \in A$ *(Elemento neutro da soma)*

A3) $\forall x \in A$, $\exists -x \in A$, *tal que,* $x+(-x) = 0$ *e* $(-x)+x = 0$ *(Existência do inverso aditivo),*

A4) $x+y = y+x$ *(Comutatividade da soma),*

A5) $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ *(Associatividade do produto),*

A6) $x\cdot(y+z) = x\cdot y + x\cdot z$ *e* $(x+y)\cdot z = x\cdot z + y\cdot z$ *(Distributividade da multiplicação em relação a adição à direita e à esquerda)*

Os axiomas de $A1$ a $A4$ afirmam que $(A,+)$ é um grupo abeliano, o axioma $A5$ afirma que em A a operação $(\cdot)$ é associativa e o axioma $A6$ afirma que a operação $(\cdot)$ é distributiva em relação a operação $(+)$.

Definição 3.2. *Dizemos que o anel $(A,+,\cdot)$ é um anel comutativo se $\forall x,y \in A$, temos que $x\cdot y = y\cdot x$*

Definição 3.3. *Dizemos que o anel $(A,+,\cdot)$ é um anel com unidade se $\forall x \in A, \exists 1 \in A$ tal que $1\cdot x = x\cdot 1 = x$*

Exemplo 3.1. $(\mathbb{Z},+,\cdot)$ *é um anel comutativo com unidade 1.*

Solução

A1) A soma é fechada para os inteiros.

A2) A soma é associativa para os inteiros

A3) Existe $0 \in \mathbb{Z}$, tal que $x+0 = x$ para todo $x \in \mathbb{Z}$

A4) para todo $x \in \mathbb{Z}$, existe $-x \in \mathbb{Z}$ tal que $x+(-x) = 0$

A5) A soma é comutativa nos inteiros.

A6) A multiplicação é fechada para os inteiros,

A7) A multiplicação é associativa nos inteiros.

A8) A multiplicação é distributiva em relação a soma nos inteiros tanto pela direita , quanto pela esquerda.

Assim $(\mathbb{Z},+,\cdot)$ com suas operações de adição e multiplicação sera chamado de anel dos inteiros.

Exemplo 3.2.
- $(\mathbb{Q},+,\cdot)$*, o conjunto dos racionais com a operação de adição e multiplicação usuais.*
- $(\mathbb{R},+,\cdot)$*, o conjunto dos reais com a operação de adição e multiplicação usuais.*
- $(\mathbb{C},+,\cdot)$*, o conjunto dos números complexos com a operação de adição e multiplicação usuais.*

Definição 3.4. *Dizemos que o anel* $(A,+,\cdot)$ *é um anel sem divisores de zero se* $\forall x,y \in A$*, temos que* $x \cdot y = 0 \Rightarrow x = 0$ *ou* $y = 0$

Vimos do exemplo anterior que $\mathbb{Z}_n$ com as operações $+$ *e* $\cdot$ é um anel. para $n = 8$ temos que $(\mathbb{Z}_8,+,\cdot)$ é um anel com **divisores de zero** pois $\overline{2} \cdot \overline{4} = \overline{0}$.

Definição 3.5. *Dizemos que o anel* $(A,+,\cdot)$ *é um domínio de integridade ou simplesmente domínio se* $(A,+\cdot)$ *é um anel comutativo, com unidade e sem divisores de zero.*

Do exemplo 3.1 temos que $(\mathbb{Z},+,\cdot)$ é um anel comutativo e com unidade, da definição 3.4 temos que $\mathbb{Z}$ não tem divisores de zero, portanto o anel $(\mathbb{Z},+,\cdot)$ é um domínio de integridade, ou simplesmente domínio.

Definição 3.6. *Um anel* $(A,+,\cdot)$ *é dito um anel com divisão ou quase corpo se para* $a \in A$*,* $a \neq 0$ *existe* $b \in A$ *tal que* $ab = ba = 1$

Finalmente chegamos a definição de corpo.

Definição 3.7. *Dizemos que o anel* $(A,+,\cdot)$ *é um corpo se* $(A,+,\cdot)$ *é um anel comutativo com unidade e com divisão.*

Com as operações usuais de adição e multiplicação temos que $\mathbb{Z}$ não é corpo, e $\mathbb{Q},\mathbb{R}$ *e* $\mathbb{C}$ são corpos.

Proposição 3.1. *Se A é um anel, então para todos* $a,b \in A$

(i) O zero é único

(ii) *O simétrico é único*

(iii) $a0 = 0a = 0$

(iv) $a+b = a+c \iff b = c$

(v) $b = c \implies ab = ac$ *e* $ba = ca$

(vi) $-(-a) = a$

(vii) $a(-b) = (-a)b = -ab$

(viii) $a(b-c) = ab-ac$

(ix) $(a-b)c = ac-bc$

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

(xi) $(-a)(-b) = ab$

Se, além disso, A possui unidade, então.

(xii) *A unidade é única*

(xiii) *Se* $a \in A$, $a \neq 0$ *e a possui inverso em A, então o inverso é único.*

Demonstração. (i) Suponha que 0_1 e 0_2 são zeros de A.

Como 0_2 é elemento neutro da adição temos que $0_1 + 0_2 = 0_1$.

Como 0_1 é elemento neutro da adição então temos que $0_1 + 0_2 = 0_2$

Daí concluímos que $0_1 = 0_2$ e denotaremos apenas por 0.

(ii) Suponha que a_1 *e* a_2 são simétricos de a $a_1 = a_1 + 0$ (0 é o elemento neutro de A)

$a_1 = a_1 + (a + a_2)$ (a_2 é simétrico de a em A.

$a_1 = (a_1 + a) + a_2$ (A soma é associativa em A)

$a_1 = 0 + a_2$ (a_1 é elemento simétrico de a em A.)

$a_1 = a_2$

E o simétrico de a será denotado por $-a$.

(iii) $a0 = a(0+0) = a0 + a0 \implies a0 = 0$ de maneira análoga fazemos para $0a = (0+0)a = 0a + 0a \implies 0a = 0$ e portanto $a0 = 0a = 0$.

(iv) $(\implies)$ $a+b = a+c$ se somarmos $-a$ a ambos lados da igualdade pela esquerda temos que $-a+(a+b) = -a+(a+c) \implies (-a+a)+b = (-a+a)+c \implies 0+b = 0+c \implies b = c$.

$(\impliedby)$ Se $b = c$. Como a operação soma associa a um par de elementos em A a um único elemento em A, Como $b = c$ então os pares (a,b) *e* (a,c) são os mesmos e portanto $a+b = a+c$.

(v) Como a operação $\cdot$ em A associa a cada par de elementos de A a um único elemento de A. como $b = c$ então os pares (a,b) *e* (a,c) são os mesmos e portanto $ab = ac$ e de mesma

maneira verificamos para $ba = ca$.

(vi) Como o simétrico de a é $-a$ então valem as igualdades $a+(-a) = (-a)+a = 0$. Isso mostra que o simétrico de $-a$ é a e assim $-(-a) = a$ onde $-$ significa o simétrico.

(vii) $a(-b)+ab = a((-b)+b) = a0 = 0 \Longrightarrow a(-b) = -ab$ e $(-a)b+ab = ((-a)+a)b = 0b = 0 \Longrightarrow (-a)b = -ab$ e portanto $a(-b) = (-a)b = -ab$

(viii) $a(b-c) = a(b+(-c)) = ab+a(-c) = ab-ac$

(ix) $(a-b)c = (a+(-b))c = ac+(-b)c = ac-bc$

(x) $(a+b)+(-a)+(-b) = a+b+(-a)+(-b) = a+(-a)+b+(-b) = (a+(-a))+(b+(-b)) = 0+0 = 0$ assim o simétrico de $(a+b)$ é $(-a)+(-b)$ Portanto $(-(a+b) = (-a)+(-b) = -a-b$

(x) $(-a)(-b) = -(a(-b) = -(-ab) = ab$

(iv) Suponha que 1_x e 1_y sejam unidades de A.

Como 1_x é unidade temos que $1_x 1_y = 1_y$.

Como 1_y é unidade de A, temos que $1_x 1_y = 1_x$.

Daí concluímos que $1_x = 1_y$. E denotaremos a unidade por 1.

(iv) Suponha a' e a" inversos de a em A. Temos que $a' = a'1$ (1 é a unidade de A)

$a' = a'(aa$") (a" é inverso de a em A)

$a' = (a'a)a$" (O produto é associativo)

$a' = 1a$" (a' é inverso de a em A)

Portanto $a' = a$". O inverso de a será denotado por a^{-1}.

□

Proposição 3.2. *Um domínio de integridade finito é um corpo.*

Demonstração. Se A um domínio de integridade finito, então A é um anel comutativo, com unidade tal que se $ab = 0 \Longrightarrow a = 0$ *ou* $b = 0$. Como por hipótese A é finito, então sejam $a_1, a_2, \ldots, a_n$ os elementos de A. tome $x \in A$ tal que $x \neq 0$ assim $a_1x, a_2x, \ldots, a_nx$ todos são elementos de A, pois caso contrário, se $a_ix = a_jx$ para $i \neq j$ então $(a_i - a_j)x = 0$ como $x \neq 0$ isso implica que $a_i - a_j = 0$ ou seja $a_i = a_j$ contradizendo $i \neq j$. Assim $a_1x, a_2x, \ldots, a_nx$ são elementos distintos em A, e são exatamente n elementos. Seja $y \in A$ então y pode ser escrito da forma a_ix, em particular $x = a_{i_0}x = xa_{i_0}$ pois A é um anel comutativo. Propomos mostrar que a_{i_0} é o elemento neutro de cada elemento em A. Como mencionado anteriormente $y = a_ix$ para algum $a_i \in A$ e temos que $ya_{i_0} = (a_ix)a_{i_0} = a_i(xa_{i_0}) = a_ix = y$ portanto a_{i_0} é o elemento neutro

de A e escrevemos como 1. Temos que $1 \in A$ assim pelo argumento anterior 1 pode ser escrito como um múltiplo de a, ou seja existe $b \in A$ tal que $ab = ba = 1$. □

Proposição 3.3. *Se A é corpo então A é domínio*

Demonstração. Suponha que A seja um corpo, então A é um anel com unidade e comutativo. precisamos mostrar que A não tem divisores de zero.

Suponha que $ab = 0$, se $a = 0$, acabou. Assuma então $a \neq 0$, então existe $a^{-1} \in A$ tal que $aa^{-1} = a^{-1}a = 1 \Longrightarrow a^{-1}ab = 1b \Longrightarrow a^{-1}0 = b \Longrightarrow b = 0$.

Portanto A é domínio. □

Teorema 3.1. *Sejam* $n \in \mathbb{Z}$, $n \geq 1$. *Então* $(\mathbb{Z}_n, +, \cdot)$ *é um anel comutativo com unidade* $\overline{1}$.

Demonstração. Sejam $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_n$, vamos verificar os axiomas da definição de anel.

A1) $\overline{a} + \overline{b} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} = \overline{a + b} \in \mathbb{Z}_n$

A2) $(\overline{x} + \overline{y}) + \overline{z} = \overline{(x + y)} + \overline{z} = \overline{(x + y) + z} = \overline{x + (y + z)} = \overline{x} + \overline{(y + z)} = \overline{x} + (\overline{y} + \overline{Z}$

A3) $\exists\, \overline{0} \in \mathbb{Z}_n$ tal que $\overline{x} + \overline{0} = \overline{x + 0} = \overline{x}$ e $\overline{0} + \overline{x} = \overline{0 + x} = \overline{x}$.

A4) $\exists\, -\overline{x} \in \mathbb{Z}_n$ tal que $\overline{x} + (-\overline{x}) = \overline{x + (-x)} = \overline{0}$ e $(-\overline{x}) + \overline{x} = \overline{(-x) + x} = \overline{0}$.

A5) $\overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x}$.

A6) $\overline{a}\overline{b} = (a + n\mathbb{Z})(b + n\mathbb{Z}) = (ab) + n\mathbb{Z} = \overline{ab} \in \mathbb{Z}$.

A7) $(\overline{xy})\overline{z} = \overline{(xy)}\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\overline{(yz)} = \overline{x}(\overline{yz})$.

A8) $\overline{x}(\overline{y} + \overline{z}) = \overline{x}\overline{(y + z)} = \overline{x(y + z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \overline{xy} + \overline{xz}$. e $(\overline{x} + \overline{y})\overline{z} = \overline{(x + y)}\overline{z} = \overline{(x + y)z} = \overline{xz + yz} = \overline{xz} + \overline{yz} = \overline{xz} + \overline{yz}$. Assim $(\mathbb{Z}_n, +, \cdot)$ é um anel, e além disso:

A9) $\overline{xy} = \overline{xy} = \overline{yx} = \overline{yx}$, é um anel comutativo.

A10) $\exists\, \overline{1} \in \mathbb{Z}_n$ tal que $\overline{x}\overline{1} = \overline{x1} = \overline{x}$. De acordo com $A9$) $\overline{x}\overline{1} = \overline{1}\overline{x} = \overline{x}$. Ou seja $(\mathbb{Z}_n, +, \cdot)$ tem unidade $\overline{1}$.

□

Teorema 3.2. *Seja* $n \in \mathbb{Z}$, $n \geq 1$. *As condições abaixo são equivalentes:*

(i) $\mathbb{Z}_n$ *é domínio.*

(ii) n é um numero primo.

(iii) $\mathbb{Z}_n$ *é corpo.*

Demonstração. $(i) \Longrightarrow (ii)$ Suponha $\mathbb{Z}_n$ um domínio. Devemos mostrar que se a divide n, então $a = 1$ *ou* $a = n$.

Como a divide n, existe $b \in \mathbb{Z}$ tal que $n = ab$, mas por hipótese $\mathbb{Z}_n$ é um domínio. então:

$$\overline{0} = \overline{n} = \overline{a}\overline{b} \Longrightarrow \overline{a} = \overline{0} \; ou \; \overline{b} = \overline{0}$$

1^o caso: $\overline{a} = \overline{0}$

temos que se $\overline{a} = \overline{0} \Longrightarrow a \equiv 0 \bmod n$ então concluímos que $a \mid n$ e $n \mid a$ logo $a = n$.

2^o Caso: $\overline{b} = \overline{0}$

temos que se $\overline{b} = \overline{0} \Longrightarrow b \equiv 0 \bmod(n)$ assim $n \mid b$ ou seja $b = kn$. Substituindo b em $n = ab$, tem-se $n = akn$ como $\mathbb{Z}_n$ é domínio e $n \neq 0$, vale a lei do cancelamento. Daí $ak = 1$ como $a, k \in \mathbb{Z}$ isso implica que $a = 1$.

$(ii) \Longrightarrow (iii)$ Suponha agora n um número primo. Considere o anel $\mathbb{Z}_n$ munido das operações soma e produto. Já sabemos que $\mathbb{Z}_n$ é comutativo e unitário. Devemos mostra que todo $\overline{a} \in \mathbb{Z}_n$ tem inverso, ou seja, existe $\overline{x} \in \mathbb{Z}_n$ tal que $\overline{ax} = \overline{1}$. Como $\text{mdc}(a,n) = 1$, pois n é primo, então pelo teorema de Bachet-Bézout (Este teorema se encontra em (MARTINEZ; et al, 2011) na pagina 14 teorema 1.7) existem $p, q \in \mathbb{Z}$ tal que $ap + nq = 1$, tomando essa identidade modulo n, tem-se $\overline{ap} + \overline{nq} = \overline{1} \Longrightarrow \overline{ap} + \overline{0}\overline{q} = \overline{1} \Longrightarrow \overline{ap} = \overline{1}$.

Assim o inverso de $\overline{a}$ é $\overline{p}$, e portanto $\mathbb{Z}_n$ é corpo.

$(iii) \Longrightarrow (i)$ Já foi provado na proposição 3.3. □

3.1 Subanel e ideais

Definição 3.8. *Sejam $(A, +, \cdot)$ um anel. Um subconjunto não vazio $B \subseteq A$ é subanel de A quando:*

(i) As operações de A são operações em B, isto é,

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

(ii) $(B, +, \cdot)$ é um anel.

Os axiomas da definição 3.1 são facilmente verificados. Note que a associatividade, o elemento neutro, a comutatividade da soma são herdadas.

Exemplo 3.3. *Com as operações usais $(\mathbb{Z}, +, \cdot)$ é subanel de $(\mathbb{Q}, +, \cdot)$, mas $(\mathbb{N}, +, \cdot)$ não é subanel de $(\mathbb{Z}, +, \cdot)$, pois temos que $2 \in \mathbb{N}$ mas $-2 \notin \mathbb{N}$*

Com a proposição abaixo iremos apresentar um critério para subanel.

Proposição 3.4. *Sejam $(A,+,\cdot)$ um anel e $B \subseteq A, B \neq \varnothing$. São equivalentes:*

(i) *B é subanel*

(II) $x,y \in B \Rightarrow x-y \in B$ *e* $x \cdot y \in B$

Demonstração. $(i) \Longrightarrow (ii)$ Se B é subanel, então as operações $+$ e $\cdot$ são fechadas em B, e além disso se $x,y \in B \Longrightarrow x,y,-y \in B$ pois os elementos de B possuem elemento simétrico em B, assim $x+(-y) = x-y \in B$ e $xy \in B$

$(ii) \Longrightarrow (i)$ Devemos mostrar que os axiomas da definição 3.1 são válidos

(1) Por hipótese a multiplicação de A é fechada em B.

(2) O elemento neutro da soma de A pertence a B, pois como $x \in B \Longrightarrow x-x = 0 \in B$.

(3) Os elementos de B possuem simétrico, pois como $x, 0 \in B \Longrightarrow 0-x = -x \in B$.

Com esses elementos vamos provar que a soma é fechada para B. De fato, se $x,y \in B \Longrightarrow x,-y \in B \Longrightarrow x-(-y) = x+y \in B$.

Os outros axiomas são herdados de A, ou seja, valem em B, pois valem em A.

□

Exemplo 3.4. *O conjunto $B = \{\overline{0}, \overline{2}\}$ é subanel de $\mathbb{Z}_4$.*

Devemos mostrar que se $a,b \in B$ então $a-b$ e $ab \in B$

$\overline{0} \cdot \overline{0} = \overline{0} \in B$

$\overline{0} \cdot \overline{2} = \overline{2} \cdot \overline{0} = \overline{0} \in B$

$\overline{2} \cdot \overline{2} = \overline{0} \in B$

$\overline{0} - \overline{0} = \overline{0} \in B$

$\overline{2} - \overline{0} = \overline{2} \in B$

$\overline{0} - \overline{2} = -\overline{0} = \overline{2} \in B$

$\overline{2} - \overline{2} = \overline{0} \in B$

Exemplo 3.5. *Seja $n \in \mathbb{N}, n > 1$. Lembre-se que $n\mathbb{Z} = \{nx\,;\, x \in \mathbb{Z}\}$. Então $n\mathbb{Z}$ é subanel de $\mathbb{Z}$, e $n\mathbb{Z}$ não tem unidade.*

Inicialmente vamos mostrar que $n\mathbb{Z}$ é subanel de $\mathbb{Z}$.

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

(·) $uw = nx \cdot ny = n(xny) \in n\mathbb{Z}$.

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

Segue da proposição 3.4 que $n\mathbb{Z}$ é subanel de $\mathbb{Z}$.

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

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

Como u é a unidade, temos que

$$un = n \Longrightarrow (nx)n = n \Longrightarrow nx = 1 \Longrightarrow n \pm 1.$$

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

Proposição 3.5. *$n \cdot \mathbb{Z}$ é subanel de $m \cdot \mathbb{Z} \Longleftrightarrow m|n$.*

Demonstração. ($\Longrightarrow$) Suponha $n\mathbb{Z}$ subanel de $m\mathbb{Z}$. Então $n \in n\mathbb{Z} \subseteq m\mathbb{Z}$, ou seja , $n = m \cdot x$ com $x \in m\mathbb{Z}$, portanto $m|n$.

($\Longleftarrow$) Suponha agora que $m \mid n$, do exemplo 3.5 temos que $n\mathbb{Z}$ e $m\mathbb{Z}$ são anéis com as operações usuais de adição e multiplicação de inteiros. Basta mostrar que $n\mathbb{Z} \subseteq m\mathbb{Z}$. De fato, seja $nx \in n\mathbb{Z}$. Como $m \mid n$ temos que $n = ma, a \in \mathbb{Z}$. Assim $nx = (ma)x = m(ax) \in m\mathbb{Z}$ e portanto $n\mathbb{Z}$ é subanel de $m\mathbb{Z}$. □

Com esta proposição, para conhecer os anéis $m\mathbb{Z}$ que tem subanéis $n\mathbb{Z}$, devemos conhecer os divisores de n

Exemplo 3.6. *$8\mathbb{Z}$ é subanel de $\mathbb{Z}$,$2\mathbb{Z}$,$4\mathbb{Z}$ e $8\mathbb{Z}$.*

Vamos ver agora uma classe de subanéis chamada de ideais de um anel.

Definição 3.9. *Seja A um anel. Um subanel I do anel A é ideal á esquerda de A quando:*

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

Definição 3.10. *Seja A um anel. Um subanel I do anel A é ideal á direita de A quando:*

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

Definição 3.11. *Sejam A um anel e I subanel de A. Se I é ideal à direita e à esquerda de A, Dizemos que I é um ideal (ou ideal bilateral) de A.*

Observação

Dado um anel A, então A e $\{0\}$ são ideais de A e são chamados de ideais triviais.

Exemplo 3.7. *Os ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z}$*

Definição 3.12. *Sejam A um anel comutativo e P um ideal de A. Dizemos que P é ideal primo de A quando* $P \neq A$, $a,b \in A$ *com* $a \cdot b \in P \Rightarrow a \in P$ *ou* $b \in P$

Exemplo 3.8. *Se* $A = Z$ *e* $P = 2\mathbb{Z}$, *Temos que P é um ideal primo, pois* $P \neq A$ *e seja* $a,b \in A$ *com* $ab \in P$. *Logo* $ab = 2k \Longrightarrow 2|ab \Longrightarrow 2|a$ *ou* $2|b$ *ou seja* $a \in P$ *ou* $b \in P$

Definição 3.13. *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* $J = A$.

Proposição 3.6. *Seja* $n \in \mathbb{N}$, $n \geq 2$. *São equivalentes:*

(i) n é um número primo.

(ii) $n\mathbb{Z}$ *é ideal maximal de* $\mathbb{Z}$.

(iii) $n\mathbb{Z}$ *é ideal primo de* $\mathbb{Z}$.

Demonstração. A demonstração desta proposição se em encontra em (JANESCH; TANEJA, 2011) pagina 117 proposição 4.3.4 □

Teorema 3.3. *Seja* $(K,+,\cdot)$ *um anel comutativo com unidade. São equivalentes:*

(i) K é corpo

(ii) $\{0\}$ *é ideal maximal;*

(iii) K só tem ideais triviais.

Demonstração. $(i) \Longrightarrow (ii)$ Devemos mostrar que $\{0\}$ é ideal maximal. Note que $\{0\} \neq K$, e seja J um ideal de K tal que $\{0\} \leq J \leq K$. Se $J = \{0\}$, está provado. Suponha então que $J \neq \{0\}$, então existe $x \neq 0 \in J$, Como K é corpo, existe $x^{-1} \in K$ tal que $x^{-1}x = 1$. vamos provar que $K \subseteq J$,

Seja $y \in K \Longrightarrow yx^{-1} \in K$, como $x \in J$ e J é ideal então pela definição de ideal $yx^{-1} \in J$ e portanto $K \subseteq J$

$(ii) \Longrightarrow (iii)$ Seja J ideal de K, tal que $\{0\} \supseteq J \supseteq K$, Como $\{0\}$ é ideal maximal temos que $J = \{0\}$ ou $J = K$.

$(iii) \Longrightarrow (i)$ Devemos mostrar que K possui inverso multiplicativo. Considere o ideal $xK \neq \{0\}$, pois $x \neq 0$, que por hipótese $xK = K$. Logo $1 \in K = xK$, Assim existe $y \in K$ tal que $xy = 1$. ou seja , todo elemento não nulo de K, possui inverso. □

Exemplo 3.9. *$\mathbb{Z}_7$ é corpo, pois 7 é primo. $\{0\}$ é ideal maximal e $\{0\}$ e $\mathbb{Z}_7$ são os únicos ideais de $\mathbb{Z}_7$.*

3.2 Anéis quocientes

Definição 3.14. *Sejam $a,b \in A$ e um ideal I do anel A. Dizemos que a é congruente a b modulo I quando a diferença $a-b$ está em I.*

Em símbolos temos que $a \equiv b \bmod I \iff a-b \in I$

Proposição 3.7. *Se I é um ideal do anel A então a relação $x \equiv y$ mod I é uma relação de equivalência em A. Isto é, para todos $a,b,c \in A$ vale:*

(i) $a \equiv a$ *mod* I *(reflexiva)*

(ii) Se $a \equiv b$ *mod* I*, então* $b \equiv a$ *mod* I *(Simétrica)*

(iii) Se $a \equiv b$ *mod* I *e* $b \equiv c$ *mod* I*, então* $a \equiv c$ *mod* I*.*

Demonstração. (i) temos que $0 = a-a \in I \longrightarrow a \equiv a \bmod I$

(ii) Se $a \equiv b \bmod I \Longrightarrow a-b \in I \Longrightarrow -(a-b) = b-a \in I$ e portanto $b \equiv b \bmod I$

(iii) Se Se $a \equiv b \bmod I$ e $b \equiv c \bmod I$, temos que $a-b, b-c \in I \Longrightarrow (a-b)+(b-c) = a-b+b-c = a-c \in I$ e portanto $a \equiv c \bmod I$.

□

Definição 3.15. *Seja I um ideal do anel A. Dado $a \in A$, chamamos de classe de equivalência de a módulo I, ao conjunto de todos os elementos de A que são congruentes à a módulo I*

$$\overline{a} = \{x; x \equiv a \ mod \ I\}$$

Note que se

$$x \in \overline{a} \iff x-a \in I \iff x-a = b \ com \ b \in I$$

$$x = a+b \iff x \in a+I$$

Assim concluímos que $\overline{a} = a+I$.

Denotaremos por $\frac{A}{I} = \{\overline{a}; a \in A\}$ o conjunto quociente de A modulo I.

Proposição 3.8. *Sejam I um ideal do anel A e $a,b \in A$*

(i) $\overline{a} = \overline{b} \iff a \equiv b \ mod \ I$

(ii) $\overline{a} = \overline{b}$ *ou* $\overline{a} \cap \overline{b} = \varnothing$

(iii) $A = \bigcup_{a \in A} \overline{a}$

Demonstração. (i) $(\Longrightarrow)$ se $a \in \overline{a} = \overline{b} \Longrightarrow a \in \overline{b} \Longrightarrow a \equiv b \bmod I$.

$(\Longleftarrow)$ Temos que mostrar que $\overline{a} \supset \overline{b}$ e $\overline{b} \subset \overline{a}$. Seja $x \in \overline{a} \Longrightarrow x \equiv a \bmod I$ e como $a \equiv b \bmod I$ então $x \equiv b \bmod I$ e portanto $x \in \overline{b}$.

Suponha agora que $x \in \overline{b} \Longrightarrow x \equiv b \bmod I$ e como $a \equiv b \bmod I \Longrightarrow b \equiv a \bmod I$ então $x \equiv a \bmod I$ e portanto $x \in \overline{a}$.

(ii) Suponha $\overline{a} \neq \overline{b}$, e seja $x \in \overline{a} \cap \overline{b} \Longrightarrow x \in \overline{a}$ *e* $x \in \overline{b}$ ou seja $x \equiv a \bmod I$ e $x \equiv b \bmod I$, pela simetria e transitividade, temos que $a \equiv b \bmod I$ e portanto $\overline{a} = \overline{b}$. Absurdo, pois por hipótese $\overline{a} \neq \overline{b}$. e assim $\overline{a} \cap \overline{b} = \varnothing$.

(iii) Como $\overline{a} \subseteq A$ para todo $a \in A$, é claro que $\bigcup_{a \in A} \overline{a} \subseteq A$. Por outro lado, dado $b \in A$, sabemos que $b \in \overline{b} \subset \bigcup_{a \in A} \overline{a}$ e assim $A \subset \bigcup_{a \in A} \overline{a}$ e portanto $A = \bigcup_{a \in A} \overline{a}$

□

Exemplo 3.10. *Seja* $A = \mathbb{Z}$ *e* $I = 6\mathbb{Z}$ *Temos que* $\frac{A}{I} = \frac{\mathbb{Z}}{6\mathbb{Z}} = \{\overline{x}; x \in \mathbb{Z}\}$,*onde* $\overline{x} = x + 6\mathbb{Z}$

$\overline{0} = 0 + 6\mathbb{Z}$; $\overline{1} = 1 + 6\mathbb{Z}$; $\overline{2} = 2 + 6\mathbb{Z}$

$\overline{3} = 3 + 6\mathbb{Z}$; $\overline{4} = 4 + 6\mathbb{Z}$; $\overline{5} = 5 + 6\mathbb{Z}$

$\frac{\mathbb{Z}}{6\mathbb{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\} = \mathbb{Z}_6$

De maneira geral $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}$ Devemos definir operações no conjunto $\frac{A}{I}$ de modo que este seja um anel.

Seja $\overline{a} = a + I$ e $\overline{b} = b + I$, definiremos a soma e o produto da seguinte maneira:

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

(ii) $\overline{a} \cdot \overline{b} = \overline{ab}$

As operações nesse anel quociente são bem definidas.

Proposição 3.9. *Seja I um ideal de um anel A, e* $a, b, x, y \in A$. *Se* $a \equiv x \bmod I$ *e* $b \equiv y \bmod I$ *então:*

(i) $a + b \equiv x + y \bmod I$

(ii) $ab \equiv xy \bmod I$

Demonstração. (i) $a \equiv x \bmod I \Longrightarrow a - x \in I$ e $b \equiv y \bmod I \Longrightarrow b - y \in I$, então $(a - x) + (b - y) \in I \Longrightarrow a - x + b - y = (a + b) - (x - y) \in I$ e portanto $a + b \equiv x + y \bmod I$.

(ii) $a \equiv x \bmod I \Longrightarrow a - x \in I$ como $b \in A$ e I é ideal, então $(a-x)b \in I$. De maneira análoga, $b \equiv y \bmod I \Longrightarrow b - y \in I$ e $x(b-y) \in I$. Então, $(a-x)b + x(b-y) = ab - xb + xb - xy = ab - xy \in I$ e portanto $ab \equiv xy \bmod I$.

□

Teorema 3.4. *Seja I um ideal do anel A. Então* $\left(\frac{A}{I}, +, \cdot\right)$ *é um anel.*

Demonstração. Devemos mostrar que todos os axiomas da definição de anel, são válidos. Dados $\overline{a}, \overline{b}, \overline{c} \in \frac{A}{I}$, então:

A1) $\overline{a} + \overline{b} = \overline{a+b} \in \frac{A}{I}$

A2) $(\overline{a} + \overline{b}) + \overline{c} = \overline{(a+b)} + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \overline{(b+c)} = \overline{a} + (\overline{b} + \overline{c})$.

A3) $\exists \overline{0}$, tal que $\overline{0} + \overline{a} = \overline{0+a} = \overline{a}$ e $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$.

A4) $\exists \overline{-a}$ tal que $\overline{-a} + \overline{a} = \overline{-a+a} = \overline{0}$ e $\overline{a} + \overline{-a} = \overline{a+(-a)} = \overline{0}$.

A5) $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}$.

A6) $\overline{a} \cdot \overline{b} = \overline{a \cdot b} \in \frac{A}{I}$.

A7) $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{(a \cdot b)} \cdot \overline{c} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot (b \cdot c)} = \overline{a} \cdot \overline{(b \cdot c)} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$.

A8) $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{(b+c)} = \overline{a \cdot (b+c)} = \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} + \overline{a \cdot c} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$. e $(\overline{b} + \overline{c}) \cdot \overline{a} = \overline{(b+c)} \cdot \overline{a} = \overline{(b+c) \cdot a} = \overline{b \cdot a + c \cdot a} = \overline{b \cdot a} + \overline{c \cdot a} = \overline{b} \cdot \overline{a} + \overline{c} \cdot \overline{a}$.

□

Definição 3.16. *O anel* $\left(\frac{A}{I}, +, \cdot\right)$ *é chamado de anel quociente de A por I.*

Voltando ao exemplo 3.10. temos que $\frac{\mathbb{Z}}{6\mathbb{Z}}$ é um anel.

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

e

·	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Corolário 3.1. *Sejam A um anel e I um ideal de A.*

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

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

Demonstração. (1) Devemos mostrar que para todo $\overline{x} \in \frac{A}{I}$, $\overline{x}\overline{1} = \overline{1}\overline{x} = \overline{x}$.

De fato, pois $\overline{x}\overline{1} = \overline{x1} = \overline{x}$ e $\overline{1}\overline{x} = \overline{1x} = \overline{x}$.

(2) Temos que mostrar que para todos $\overline{x}, \overline{y} \in \frac{A}{I}$, $\overline{xy} = \overline{yx}$.

De fato, pois $\overline{x} \cdot \overline{y} = \overline{xy} = \overline{yx} = \overline{y} \cdot \overline{x}$.

□

Teorema 3.5. *Sejam A um anel comutativo com unidade e I um ideal de A, $I \neq A$. Então:*

(i) $\frac{A}{I}$ *é domínio* $\Longleftrightarrow$ *I é ideal primo de A.*

(ii) $\frac{A}{I}$ *é corpo* $\Longleftrightarrow$ *I é ideal maximal de A.*

Demonstração. (i) $(\Longrightarrow)$ Sejam $a, b \in A$ e $ab \in I$, isso implica que $0 - ab \in I \Longrightarrow 0 \equiv ab \bmod I$, mas como $\frac{A}{I}$ é domínio, então $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$.

Se $\overline{a} = \overline{0} \Longrightarrow a \equiv 0 \bmod I \Longrightarrow a - 0 \in I \Longrightarrow a \in I$.

Se $\overline{b} = \overline{0} \Longrightarrow b \equiv 0 \bmod I \Longrightarrow b - 0 \in I \Longrightarrow b \in I$.

$(\Longleftarrow)$ Como A é um anel comutativo com unidade, então pelo corolário anterior temos que $\frac{A}{I}$ é um anel comutativo com unidade. Falta mostrar que $\frac{A}{I}$ não tem divisores de zero. Sejam $\overline{a}, \overline{b} \in \frac{A}{I}$, tal que $\overline{a}\overline{b} = \overline{0} \Longrightarrow ab \equiv 0 \bmod I$, ou seja, $ab - 0 \in I \Longrightarrow ab \in I$ como I é ideal primo, então temos que

$a \in I$ ou $b \in I$.

Se $a \in I \Longrightarrow a - 0 \in I \Longrightarrow a \equiv 0 \bmod I$ e portanto $\overline{a} = \overline{0}$.

Se $b \in I \Longrightarrow b - 0 \in I \Longrightarrow b \equiv 0 \bmod I$ e portanto $\overline{b} = \overline{0}$

(ii) $(\Longrightarrow)$ Queremos mostrar que I é ideal maximal. Por hipótese $I \neq A$, falta mostrar que se J é ideal de A e $I \subseteq J \subseteq A$, então $J = I$ ou $J = A$.

Suponha J ideal de A e $I \subsetneq J \subseteq A$. Então existe $a \in J$ tal que $a \notin I$, e segue que $\overline{a} \neq \overline{0}$, e consequentemente $\overline{a} \in \frac{A}{I}$, como $\frac{A}{I}$ é corpo, então existe $\overline{b} \in \frac{A}{I}$, tal que $\overline{a}\overline{b} = \overline{1}$, ou seja, $ab \equiv 1 \bmod I$, isso implica que; $ab - 1 \in I \Longrightarrow ab - 1 = i \; com \; i \in I$.

Como $a \in J$ isso implica que $ab \in J$, e como $i \in I \Longrightarrow i \in J$ pois $I \subset J$. e portanto $1 = ab - i \in J$, e concluímos que $1 \in J \supseteq A$ e portanto A é corpo e possui apenas ideais triviais, como $J \neq \{0\}$ temos que $J = A$.

$(\Longleftarrow)$ Suponha agora que I é ideal maximal de A. Como A é um anel comutativo com unidade, então pelo corolário anterior temos que $\frac{A}{I}$ é um anel comutativo com unidade. Falta mostrarmos que $\frac{A}{I}$ tem inverso multiplicativo. Seja $\overline{a} \in \frac{A}{I}$, com $\overline{a} \neq \overline{0}$, segue que $a \notin I$, pois se $a \in I \Longrightarrow \overline{a} = \overline{0}$, contradição pois $\overline{a} \neq \overline{0}$. Seja $aA = \{ax; x \in A\}$ o ideal principal gerado por a. Assim temos que $I + aA = \{u + v \; ; \; v \in I, u \in aA\}$ é ideal de

A. de forma que $I \supsetneq I + aA \subset A$, como I é ideal maximal, temos que $I + aA = A$ e daí vem que $1 \in I + aA \Longrightarrow 1 = u + v$, como $v \in aA \Longrightarrow v = ax$, *com* $x \in A$, Logo $1 = u + ax \Longrightarrow 1 - ax = u \Longrightarrow 1 - ax \in I \Longrightarrow 1 \equiv ax \bmod I$ e portanto $\overline{1} = \overline{ax} = \overline{xa}$, ou seja, o inverso de $\overline{a}$ é $\overline{b}$

□

Exemplo 3.11. *Seja p primo, então* $p\mathbb{Z}$ *é ideal maximal* $\frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{Z}_p$ *é corpo. Por outro lado, seja n um número não primo, então* $n\mathbb{Z}$ *não é ideal maximal e portanto* $\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$ *não é domínio.*

3.3 Homomorfismo e isomorfismo de anéis

Definição 3.17. *Sejam* $(A, +, \cdot)$ *e* $(B, *, \triangle)$ *anéis. Um homomorfismo de A em B é uma função* $f : A \longrightarrow B$ *tal que:*

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

(ii) $f(a \cdot b) = f(a) \triangle f(b).$

Observação

Quando estamos falando de homomorfismo entre os anéis A e B, é comum denotarmos as mesmas operações. Ou seja $(A, +, \cdot)$ e $(B, +, \cdot)$, mas não podemos esquecer que $+$ e $\cdot$ podem representar operações diferentes em A e B.

Quando apresentamos:

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

(ii) $f(ab) = f(a)f(b)$

Deve ficar claro que $a+b$ e ab são operações em A e que $f(a) + f(b)$ e $f(a)f(b)$ são operações em B.

Se $f : A \longrightarrow B$ é bijetivo, então é um **isomorfismo**. Neste caso dizemos A e B são isomorfos e escrevemos $A \simeq B$.

Os homomorfismos $f : A \longrightarrow A$ são chamados de endomorfismos, e os isomorfismos $f : A \longrightarrow A$ são chamados de **automorfismos**.

Exemplo 3.12. *Sejam A e B anéis. Então* $f : A \longrightarrow B$, $f(x) = 0$*, é homomorfismo, chamado homomorfismo nulo.*

Temos que:

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

(ii) $f(ab) = 0 = 0 \cdot 0 = f(0)f(0)$.

Proposição 3.10. *Sejam f $A \to B$ um homomorfismo. Então:*

(i) $f(0) = 0'$.

(ii) $f(-a) = -f(a)$.

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

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

(v) Se A se B são corpos, então f é nula ou f é injetiva.

Demonstração. (i) $f(0) = f(0+0) = f(0) + f(0) \Longrightarrow f(0) = 0'$

(ii) Se $a + (-a) = 0$ e $f(0) = 0'$ segue que $f(0) = f(a + (-a)) = f(a) + f(-a) = 0' \Longrightarrow f(-a) = -f(a)$

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

(iv) Temos que $1 \cdot 1 = 1 \Longrightarrow f(1 \cdot 1) = f(1) \Longrightarrow f(1)f(1) = f(1) \Longrightarrow f(1)f(1) - f(1) = 0' \Longrightarrow f(1)\,(f(1) - 1') = 0'$ como A e B, são domínios, segue que: $f(1) = 0'$ ou $f(1) - 1' = 0' \Longrightarrow f(1) = 1'$.

Se $f(1) = 0'$, temos que $f(x) = f(x \cdot 1) = f(x)f(1) = f(x) \cdot 0' = 0'$, ou seja, f é a função constante nula.

(vi) Suponha que A e B são corpos e que f não é o homomorfismo nulo. Como A e B são corpos,e portanto domínios, então $f(1) = 1'$. vamos mostrar que f é injetiva. Seja $f(a) = f(b) \Longrightarrow f(a) - f(b) = 0' \Longrightarrow f(a-b) = 0'$. Suponha por absurdo que $a - b \neq 0$, então existe $x \in A$ tal que $x \cdot (a-b) = 1$, pois A é corpo, e daí segue que $f(x)f(a-b) = f(x) \cdot 0' = 1'$. contradição, pois B é corpo.

□

Note que se $f : A \longrightarrow B$ é homomorfismo, então $f(0) = 0'$ e que se $f(0) \neq 0'$ então $f : A \longrightarrow B$ não é homomorfismo.

Proposição 3.11. *Seja $f : A \longrightarrow B$ é um homomorfismo de anéis, então:*

(i) Se S é subanel de A, então $f(S)$ é subanel de B.

(ii) Se I é ideal de A, então $f(I)$ é ideal de $f(A) = Im(f)$.

Demonstração. (i) sejam $a, b \in S$, assim temos que $f(a), f(b) \in f(S)$..

$f(a) - f(b) = f(a-b)$ como $a - b \in S$ então $f(a) - (b) \in f(S)$.

$f(a)f(b) = f(ab)$, como $ab \in S$ então $f(a)f(b) \in f(S)$.

Portanto, $f(S)$ é subanel de B.

(ii) Sejam $a, b \in I$ e $r \in A$. Do item anterior, vimos que $f(a) - f(b) \in f(I)$.

Temos que $f(a) \in f(I)$ e $f(r) \in f(A)$. Note que $f(a)f(r) = f(ar)$, como $ar \in I$ pois I é ideal de A, então $f(a)f(r) \in f(I)$, e portanto $f(I)$ é ideal de $f(A) = Im(f)$.

□

Seja o homomorfismo $f : A \Longrightarrow B$, definiremos:

· **Núcleo (ou Kernel)** de f por $N(f) = \{x \in A \; ; \; f(x) = 0\}$

· **Imagem** de f por $Im(f) = \{f(x) \; ; \; x \in A\}$

Com essas definições de núcleo e imagem, apresentaremos o primeiro teorema do homomorfismo.

Teorema 3.6. *(i) $Im(f)$ é subanel de B.*

(ii) $N(f)$ é ideal de A

(iii) f é injetiva $\Longleftrightarrow N(f) = \{0\}$.

(iv) Os anéis $\frac{A}{N(f)}$ e $Im(f)$ são isomorfos.

Demonstração. (i) Sejam $x, y \in Im(f)$, então existem $a, b \in A$ tal que $f(a) = x$ e $f(b) = y$

$x - y = f(a) - f(b) = f(a-b) \in Im(f)$

$xy = f(a)f(b) = f(ab) \in Im(f)$.

Portanto $Im(f)$ é subanel de B.

(ii) Sejam $a, b \in N(f)$ e $r \in A$

$f(a-b) = f(a) - f(b) = 0' - 0' = 0' \Longrightarrow a - b \in N(f)$.

$f(ar) = f(a)f(r) = 0' \cdot f(r) = 0' \Longrightarrow ar \in N(f)$.

Portanto $N(f)$ é ideal de A.

(iii) ($\Longrightarrow$) Suponha f injetora. Seja $a \in N(f)$, assim $f(a) = 0' \Longrightarrow f(a) = f(0) \Longrightarrow$, como f é injetiva, então $a = 0$

($\Longleftarrow$) Suponha agora que $N(f) = \{0\}$.

Sejam $a, b \in A$ tais que $f(a) = f(b)$. Logo:

$$f(a) = f(b) \Longrightarrow f(a) - f(b) = 0' \Longrightarrow f(a-b) = 0'$$

Como $N(f) = \{0\}$, isso implica que $a - b = 0 \longrightarrow a = b$, e portanto f é injetiva.

(iv) Temos que provar que

$$\begin{array}{ccccc} \mathrm{g} & ; & \frac{A}{N(f)} & \longrightarrow & Im(f) \\ & & \overline{a} & \longrightarrow & f(a) \end{array}$$

é um isomorfismo.

Note que$g(\overline{a}) = f(a)$ então temos que:

$g(\overline{a}+\overline{b}) = f(a+b) = f(a)+f(b) = g(\overline{a})+g(\overline{b})$

$g(\overline{a}\cdot\overline{b}) = f(a\cdot b) = f(a)\cdot f(b) = g(\overline{a})\cdot g(\overline{b})$

Logo g é homomorfismo. Falta mostrar que é bijetivo.

Injetividade: $g(\overline{a}) = g(\overline{b}) \Longrightarrow f(a) = f(b) \Longrightarrow f(a-b) = 0' \Longrightarrow a-b \in N(f) \Longrightarrow a \equiv b \bmod(N(f))$ e portanto $\overline{a} = \overline{b}$.

Sobrejetividade: Seja $Im(g) = \{g(\overline{a})\ ;\ \overline{a} \in \frac{A}{N(f)}$, mas como $g(\overline{a}) = f(a)$, temos que $Im(g) = \{g(\overline{a})\ ;\ \overline{a} \in \frac{A}{N(f)} = \{f(a)\ ;\ a \in A\} = Im(f)$.

Concluímos que g é bijetivo e portanto $\frac{A}{N(f)}$ e $Im(f)$ são isomorfos ($\frac{A}{N(f)} \simeq Im(f)$).

□

4 ANÉIS DE POLINÔMIOS

Estudamos anteriormente alguns tipos de anéis, estudaremos agora os anéis de polinômios, onde a partir do anel A definiremos $A[x]$ que é formado pelos polinômios na indeterminada x e coeficientes em A

4.1 Anéis de polinômios e o algoritmo da divisão

Definição 4.1. *Seja $(A,+,\cdot)$ um anel. Então*

$$A[x] = \{a_0 + a_1x + \ldots + a_nx^n; n \in \mathbb{N}, a_i \in A, \forall i \in \{1,2,\ldots,n\}\}$$

Os elementos de $A[x]$ são chamados de polinômios.

Definição 4.2. *Seja A um anel. Um polinômio sobre A na indeterminada (ou variável) x, é uma expressão da forma: $a_0 + a_1x + a_2x^2 + \ldots$ onde $a_i \in A$, e existe $n \in \mathbb{N}$ tal que $a_j = 0$ para cada $j \geq n$.*

Seja o polinômio $p(x) = a_0 + a_1x + a_2x^2 + \ldots a_nx^n$. Quando $a_n \neq 0$, dizemos que n é o grau de $p(x)$ e denotamos por $\partial(p(x))$. Neste caso a_n é o coeficiente dominante de $p(x)$. Se $a_n = 1$, $p(x)$ será chamado de polinômio mônico.

Notação: O conjunto de todos os polinômios na indeterminada x e coeficientes no anel A, será denotado por $A[x] = \{a_0 + a_1x + a_2x^2 \ldots + a_nx^n \ ; \ n \in \mathbb{N}, a_i \in A\}$. Note que para cada $a_i \in A$ com $i \in \{1,2,\ldots,n\}$ poderá ser identificado como um polinômio constante $p(x) = a_i$, com $i \in \{1,2,\ldots,n\}$. Deste modo $A \subseteq A[x]$.

Exemplo 4.1. *Seja o polinômio $p(x) = 3 + 4x^3 + x^4 \in \mathbb{Z}[x]$*

- $\partial(p(x)) = 4$
- $a_n = 1$

Definição 4.3. *Sejam $p(x) = a_0 + a_1x + \ldots \in A[x]$ e $q(x) = b_0 + b_1x + \ldots A[x]$. Dizemos que $p(x) = q(x)$ quando $a_i = b_i$ para todo $i \in \mathbb{N}$*

Agora vamos definir as operações de adição e multiplicação em $A[x]$.

1) $p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots \in A[x]$
2) $p(x)q(x) = c_0 + c_1x + \ldots \in A[x]$. $c_0 = a_0b_0$

   $c_1 = a_0b_1 + a_1b_0$

$c_2 = a_0b_2 + a_1b_1 + a_2b_0$

$\vdots$

$c_k = a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \ldots + a_{k-1}b_1 + a_kb_0 = \sum_{i+j=k} a_ib_j$

Estas são as operações usuais dos polinômios

Exemplo 4.2. *Seja* $p(x) = 3 + 2x + 4x^2$ *e* $q(x) = 4 + 5x + 2x^2$

1) $p(x) + q(x) = (3+4) + (2+5)x + (4+2)x^2 = 7 + 7x + 6x^2$

2) $p(x)q(x) = c_0 + c_1x + \ldots\ c_0 = 3 \cdot 4 = 12$

$c_1 = 3 \cdot 5 + 2 \cdot 4 = 15 + 8 = 23$

$c_2 = 3 \cdot 2 + 2 \cdot 5 + 4 \cdot 4 = 6 + 10 + 16 = 32$

$c_3 = 2 \cdot 2 + 4 \cdot 5 = 4 + 20 = 24$

$c_4 = 4 \cdot 2 = 8$

$p(x)q(x) = 12 + 23x + 32x^2 + 16x^3 + 8x^4$

Teorema 4.1. *Seja A um anel. Então:*

(i) $A[x]$ *é um anel.*

(ii) A é comutativo, então $A[x]$ *é comutativo.*

(iii) Se A tem unidade 1, então $A[x]$ *tem unidade* $g(x) = 1$.

(iv) Se A é domínio, então $A[x]$ *é domínio.*

Demonstração. (i) sejam $p(x) = a_0 + a_1x + \ldots \in A[x]$, $q(x) = b_0 + b_1x + \ldots \in A[x]$ e $r(x) = c_0 + c_1x + \ldots \in A[x]$. Devemos mostrar que os axiomas da definição de anel são válidos.

A1) $p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots$, como $a_i + b_i \in A$, então $p(x) + q(x) \in A[x]$

A2) $(p(x) + q(x)) + r(x) = ((a_0 + b_0) + (a_1 + b_1)x + \ldots) + c_0 + c_1x + \ldots = (a_0 + b_0 + c_0) + (a_1 + b_1 + c_1)x + \ldots = a_0 + a_1x + \ldots + ((b_0 + c_0) + (b_1 + c_1)x + \ldots) = p(x) + (q(x) + r(x))$.

A3) Existe um $t(x) \in A[x]$ tal que $p(x)t(x) = t(x)p(x) = p(x)$

assim teremos que $a_i + t_i = t_i + a_i = a_i \Longrightarrow t_i = 0$ e portanto $t(x) = 0 + 0x + \ldots = 0$.

A4) Existe $-p(x) \in A[x]$ tal que $p(x) + (-p(x) = (-p(x)) + p(x) = 0$.

De fato. $-p(x) = -a_0 - a_1x - \ldots \in A[x]$ e $p(x) + (-p(x)) = (a_0 + (-a_0)) + (a_1 + (-a_1)) + \ldots = 0 + 0x + \ldots = 0$.

De maneira análoga fazemos para $(-p(x)) + p(x) = 0$.

A5) $p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots = (b_0 + a_0) + (b_1 + a_1)x + \ldots = q(x) + p(x)$.

A6) Já vimos que $p(x)q(x) = c_0 + c_1x + \ldots$ onde $c_k = \sum_{i+j=k} a_i b_j \in A$, Portanto $p(x)q(x) \in A[x]$.

A7) Queremos mostrar que $(p(x)q(x))r(x) = p(x)(q(x)r(x))$

$p(x)q(x) = d_0 + d_1x + \ldots$, com $d_k = \sum_{i+j=k} a_i b_j$

$(p(x)q(x))r(x) = e_0 + e_1x + \ldots$, com $e_K = \sum_{i+j=k} d_i c_j$

$q(x)r(x) = f_0 + f_1x + \ldots$, com $f_k = \sum_{i+j=k} b_i c_j$

$p(x)(q(x)r(x)) = l_0 + l_1x + \ldots$, com $l_k = \sum_{i+j=k} a_i f_j$.

Temos que mostrar que $l_k = e_k$ para todo $k \in \mathbb{N}$.

Seja $l_k = \sum_{i+j=k} a_i f_j$.

$$l_k = \sum_{i+j=k} a_i \left(\sum_{l+t=j} b_l c_t \right).$$
$$l_k = \sum_{i+l+t=k} a_i (b_l c_t).$$
$$l_k = \sum_{i+l+t=k} (a_i b_l) c_t.$$
$$l_k = \sum_{n+t=k} \left(\sum_{i+l=n} a_i b_l \right) c_t$$
$$l_k = \sum_{n+t=k} d_n c_t = e_k.$$

A8) Faremos a distributividade à esquerda. Queremos mostrar que $p(x)(q(x) + r(x)) = p(x)q(x) + p(x)r(x)$.

Escrevendo $p(x)(q(x) + r(x)) = u_0 + u_1x + \ldots$ com $u_i = \sum_{j+t=i} a_j (b_t + c_t)$

$p(x)q(x) = l_0 + l_1x + \ldots$ com $l_i = \sum_{j+t=i} a_j b_t$

$p(x)r(x) = v_0 + v_1x + \ldots$ com $v_i = \sum_{j+t=i} a_j c_t$

Devemos mostrar que $u_i = l_i + v_i$ para todo $\in \mathbb{N}$.

Para $i \in \mathbb{N}$ temos que:

$$u_i = \sum_{j+t=i} a_j (b_t + c_t)$$
$$u_i = \sum_{j+t=i} a_j b_t + a_j c_t$$
$$u_i = \sum_{j+t=i} a_j b_t + \sum_{j+t} a_j c_t$$
$$u_i = l_i + v_i$$

Agora falta mostrarmos que $((q(x) + r(x))p(x) = q(x)p(x) + r(x) + p(x)$.

$((q(x) + r(x))p(x) = m_0 + m_1x + \ldots$, com $m_k = \sum_{i+j=k} (b_i + c_i) a_j$

$q(x)p(x) = n_0 + n_1x + \ldots$, com $n_k = \sum_{i+j=k} b_i a_j$

$r(x)p(x) = t_0 + t_1x + \ldots$, com $t_k = \sum_{i+j=k} c_i a_j$.

Para terminar a demonstração, devemos mostrar que $m_k = n_k + t_k$ para todo $k \in \mathbb{N}$.

Seja $k \in \mathbb{N}$, de forma que

$$m_k = \sum_{i+j=k} (b_i + c_i)\, a_j$$
$$m_k = \sum_{i+j=k} b_i a_j + c_i a_j$$
$$m_k = \sum_{i+j=k} b_i a_j + \sum_{i+j=k} c_i a_j$$
$$m_k = n_k + t_k$$

Como $A[x]$ satisfaz todos os axiomas acima, $A[x]$ é um anel.

(ii) Sejam $p(x) = a_0 + a_1 x + \ldots \in A[x]$ e $q(x) = b_0 + b_1 x + \ldots \in A[x]$.

Temos que $p(x)q(x) = c_0 + c_1 x + \ldots \in A[x]$, com $c_i = \sum_{j+t=i} a_j b_t$,

$q(x)p(x) = l_0 + l_1 x + \ldots \in A[x]$, com $l_i = \sum_{j+t=k} b_t a_j$.

Mas por hipótese A é um anel comutativo, então para cada $i \in \mathbb{N}$ temos que

$$c_i == \sum_{j+t=i} a_j b_t = \sum_{j+t=k} b_t a_j = l_i$$

(iii) Seja $p(x) = a_0 + a_1 x + \ldots \in A[x]$ e escreva $g(x) = 1$ como $g(x) = b_0 + b_1 x + \ldots$ onde $b_0 = 1$ e $b_t = 0$ para todo $t \geq 1$.

$p(x)g(x) = c_0 + c_1 x + \ldots$, com $c_i = \sum_{j+t=i} a_j b_t$.

Devemos provar que $c_i = a_i$, para todo $i \in \mathbb{N}$, aí teremos $p(x)q(x) = p(x)$.

Para $i \in \mathbb{N}$, a única maneira 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 maneira análoga, prova-se que $g(x)p(x) = p(x)$.

E portanto $g(x) = 1$ é unidade de $A[x]$

(iv) Como A é domínio, então A é um anel comutativo, com unidade e sem divisores de zero.

Segue de $(i), (ii)$ *e* (iii) que $A[x]$ é um anel comutativo e com unidade, faltando provar que $A[x]$ não tem divisores de zero.

Sejam $p(x) = a_0 + a_1 x + \ldots \in A[x]$, e $q(x) = b_0 + b_1 x + \ldots \in A[x]$ tais que $p(x)q(x) = 0$.

Iremos fazer a demonstração por absurdo. Suponha que $p(x) \neq 0$,$q(x)neq0$,ou seja, existem $m, n \in \mathbb{N}$, tais que $p(x) = a_0 + a_1 x + \ldots + a_m x^m$, com $a_m \neq 0$ e $q(x) = b_0 + b_1 x + \ldots + b_n x^n$, com $b_n \neq 0$ que $p(x)q(x) = 0$

$0 = p(x)q(x) = c_0 + c_1 x + \ldots$, com $c_i = \sum_{j+t=i} a_j b_t$

Temos que $c_i = 0$ para todo $i \in \mathbb{N}$. Em particular $c_{m+n} = 0$

$0 = c_{m+n} = \sum_{j+t=m+n} a_j b_t$. Como $\sum_{j+t=m+n} a_j b_t = a_0 b_{m+n} + a_1 b_{m+n-1} + \ldots + a_{m-1} bn + 1 + a_m b_n + a_{m+1} b_{n-1} \ldots + a_{m+n} b_0$, temos que:

$c_{m+n} = a_0 b_{m+n} + a_1 b_{m+n-1} + \ldots + a_{m-1} bn + 1 + a_m b_n + a_{m+1} b_{n-1} \ldots + a_{m+n} b_0$. $(*)$

Note que se $i > m$, temos que $a_i = 0$ e se $j > n$, temos que $b_j = 0$. Assim em $(*)$, concluímos que $0 = a_m b_n$, Contradição. pois a_m e b_n são não nulos e por hipótese A é domínio. Então $A[x]$ é domínio

□

Observação: A é subanel de $A[x]$.

De fato, já vimos que $A \subseteq A[x]$ e como A é um anel com as restrições do anel $A[x]$, então A é subanel de $A[x]$.

Exemplo 4.3.

- $\mathbb{Z}[x]$ *é domínio, pois* $\mathbb{Z}$ *é domínio.*
- $n\mathbb{Z}[x]$ *é anel comutativo, pois* $n\mathbb{Z}$ *é anel comutativo.*
- $\mathbb{Z}_n[x]$ *é anel comutativo com unidade, pois* $\mathbb{Z}_n$ *é anel comutativo com unidade.*
- $\mathbb{Z}_p[x]$ *é domínio para todo p positivo primo, pois* $\mathbb{Z}_p$ *é domínio para todo p positivo primo.*

Veremos agora que $A[x]$ nunca é corpo, pois $p(x) = x \in A[x]$ não é inversível. De fato. Suponha que existe $q(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in A[x]$, tal que $1 = p(x)q(x)$.

$1 = x(a_0 + a_1 x + a_2 x^2 + \ldots + a_x^n)$

$1 = a_0 x + a_1 x^2 + \ldots + a_n x^{n+1}$

$1 = 0$. Absurdo.

Proposição 4.1. *Sejam A um anel e* $p(x), q(x) \in A[x]$ *com* $p(x) \neq 0, q(x) \neq 0$

(i) Se $p(x) + q(x) \neq 0$ *então* $\partial(p(x) + q(x)) \leq max\{\partial(p(x)), \partial(q(x))\}$

(ii) Se $\partial(p(x)) \neq \partial(q(x))$ *e* $p(x) + q(x) \neq 0$ *então* $\partial(p(x) + q(x)) = max\{\partial(p(x)), \partial(q(x))\}$.

(iii) Se $p(x)q(x) \neq 0$ *então* $\partial(p(x)q(x)) \leq \partial(p(x)) + \partial(q(x))$.

(iv) Se A é domínio, então $\partial(p(x)q(x)) = \partial(p(x)) + \partial(q(x))$.

Demonstração. Sejam $p(x) = a_0 + a_1 x + \ldots a_n x^n$ de $\partial(p(x)) = n$ e $q(x) = b_0 + b_1 x + \ldots + b_m x^m$ de $\partial(q(x)) = m$. Sem perda de generalidade assuma que $n \geq m$.

(i) $p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x \ldots + (a_m + b_m)x^m + \ldots + (a_n + b_n)x^n$, onde acrescentamos coeficientes $b_j = 0$ para $j > m$, se for necessário. Se $a_n + b_n \neq 0$ então $\partial(p(x) + q(x)) = n$, caso contrário $\partial(p(x) + q(x)) < n$ e portanto $\partial(p(x) + q(x)) \leq max\{\partial(p(x)), \partial(q(x))\}$

(ii) Por hipótese $\partial(p(x)) \neq \partial(q(x))$, então $n \neq m$, vamos assumir que $n > m$. Então $p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x \ldots + (a_m + b_m)x^m + (a_{m+1} + b_{m+1})^{m+1} \ldots + (a_n + b_n)x^n$, desde que $a_n \neq 0$ temos que $p(x)+q(x) \neq 0$, e também $\partial(p(x)+q(x)) = n = max\{\partial(p(x)), \partial(q(x))\}$.

(iii) Escrevendo $p(x)q(x) = c_0 + c_1x + \ldots c_kx^k = \sum_{i+j=k} a_ib_j$, e lembrando que $a_i = 0$ para $i > n$, pois $\partial(p(x)) = n$ e $b_j = 0$ para $j > m$,pois $\partial(q(x)) = m$. Vemos que $c_k = 0$ para $k > n+m$. De fato, quando $k > n+m$ cada uma das parcelas do somatório $\sum_{i+j=k} a_ib_j$ envolve a_i com $i > n$ ou b_j com $j > m$ portanto todas as parcelas são nulas. Consequentemente, $c_k = 0$ para $k > n+m$. Segue que $p(x)q(x) = c_0 + c_1x + \ldots + c_{n+m}x^{n+m}$.

(iv) Novamente escreva $p(x)q(x) = c_0 + c_1x + \ldots c_kx^k = \sum_{i+j=k} a_ib_j$, lembre se que $a_n \neq 0, b_m \neq 0$ pois $\partial(p(x)) = n$ e $\partial(q(x)) = m$. Vimos na demonstração anterior que $c_k = 0$ se $k > n+m$. Além disso note que $C_{n+m} = a_0b_{n+m} + a_1b_{n+m-1} + \ldots + a_{n-1}b_{m+1} + a_nb_m + \ldots + a_{n+m}b_0 = a_nb_m$, pois $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$. Como A é domínio e $a_n \neq 0, b_m \neq 0$ então $c_{n+m} \neq 0$. Portanto

$$\partial(p(x)q(x)) = \partial(p(x)) + \partial(q(x)) = n+m$$

□

Proposição 4.2. *Se A é domínio então os elementos invertíveis de A e de $A[x]$ coincidem, isto é, $U(A) = U(A[x])$.*

Demonstração. A inclusão $U(A) \subseteq U(A[x])$ é imediata pois $A \subseteq A[x]$.

Tome $f(x) \in A[x]$ então existe $g(x) \in A[x]$ tal que $f(x)g(x) = 1$. Assim $f(x) \neq 0$ e $g(x) \neq 0$. Como $A[x]$ é domínio, pois A é domínio, segue da proposição 4.1 que $0 == \partial(1) = \partial(f(x)) = \partial(g(x))$.

Portanto $\partial(f(x)) = \partial(g(x)) = 0$, isto é, $f(x) = a, a \in A$ *e* $g(x) = b, b \in A$ e $ab = 1$, logo $f(x) = a \in U(A)$ □

Corolário 4.1. *Nenhum anel de polinômios é corpo.*

Demonstração. Seja A um anel, e suponha que $U(A[x]) = A[x]^*$. Como A é subanel de $A[x]$, temos que A é domínio. Pela proposição 4.2 temos que $U(A) = U(A[x]) = A[x]^*$, que é um absurdo. □

Exemplo 4.4.
- $U(\mathbb{Z}) = U(\mathbb{Z}[x]) = \{-1, +1\}$
- $U(\mathbb{Q}) = U(\mathbb{Q}[x]) = \mathbb{Q}^*$

- $U(\mathbb{R}) = U(\mathbb{R}[x]) = \mathbb{R}^*$
- $U(\mathbb{Z}_p) = U(\mathbb{Z}_p[x]) = \mathbb{Z}_p^*$

Teorema 4.2 (Algoritmo da divisão)**.** *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* $f(x) = g(x) \cdot q(x) + r(x)$*, com* $r(x) = 0$ *ou* $\partial(r(x)) < \partial(g(x))$.

Demonstração. Se $f(x) = 0$, acabou. Basta toma $q(x) = r(x) = 0$.

Suponha que $f(x) \neq 0$, e como $g(x) \neq 0$, escrevemos: $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $\partial(p(x)) = n$ e $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$, $\partial(g(x)) = m$

Temos dois casos a analisar:

1º caso $\partial(p(x)) = n < \partial(g(x)) = m$. Tome $q(x) = 0$ e $r(x) = f(x)$

2º caso $\partial(p(x)) = n \geq \partial(g(x)) = m$.

Vamos usar o segundo princípio de indução sobre $n = \partial(p(x))$. Se $n = 0$, então $f(x) = a_0$. Assim temos que $0 = n = \partial(p(x)) \geq \partial(g(x)) \Longrightarrow \partial(g(x)) = 0 \Longrightarrow g(x) = b_0 \in K$. Como $0 \neq g(x) = b_0 \in K$, temos que , existe $b_0^{-1} \in K$. Tome $q(x) = b_0^{-1}a_0$ e $r(x) = 0$. É claro que $f(x) = g(x)q(x) + r(x) = b_0(b_0^{-1}a_0 + 0 = a_0$.

Agora consideramos $n \geq 1$, e nossa hipótese de indução é: "Se $h(x) \in K[x], h(x0 \neq 0$ *e* $\partial(h(x)) < n$. Então 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

$$h(x) = f(x) - \left(a_nb_m^{-1}x^{n-m}\right)g(x). \quad (*)$$

Se $h(x) = 0$, então $f(x) = g(x)q(x) + r(x)$, com $r(x) = 0$ e $q(x) = \left(a_nb_m^{-1}x^{n-m}\right)$. Se $h(x) \neq 0$, podemos calcular o seu grau. E pela escolha de $h(x)$ temos $\partial(h(x)) < n$. Usando a hipótese de indução obtemos que $q_1(x), r_1(x) \in K[x]$, 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

$$f(x) = g(x)\left(q_1(x) + a_nb_m^{-1}x^{n-m}\right) + r_1(x).$$

Chame $q(x) = \left(q_1(x) + a_nb_m^{-1}x^{n-m}\right)$ e $r(x) = r_1(x)$. Então $f(x) = g(x)q(x) + r(x)$, com $r(x) = 0$ ou $\partial(r(x)) < \partial(g(x))$. Isso mostra a existência $q(x)$ e $r(x)$.

Resta mostrar a unicidade. Sejam $q(x), q'(x), r(x), r'(x) \in K[x]$ tais que :

$$f(x) = g(x)q(x) + r(x),\ com\ r(x) = 0\ ou\ \partial(r(x)) < \partial(g(x)).$$

$$f(x) = g(x)q'(x) + r'(x),\ com\ r'(x) = 0\ ou\ \partial\left(r'(x)\right) < \partial\left(g(x)\right).$$

Teremos agora a igualdade

$$g(x)\left(q(x) - q'(x)\right) = r(x) - r'(x).$$

Suponha $q(x) \neq q'(x)$, então $q(x) - q'(x) \neq 0$ e $r(x) - r'(x) \neq 0$. Logo,

$$\partial\left(g(x)\right) \leq \partial\left(\left(q(x) - q'(x)\right)g(x)\right) = \partial\left(r(x) - r'(x)\right) < \partial\left(g(x)\right).$$

Essa contradição diz que não podemos supor que $q(x) \neq q'(x)$. Portanto $q(x) = q'(x)$ e a igualdade $g(x) \cdot (q(x) - q'(x)) = r(x) - r'(x)$ nos diz que $0 = r(x) - r'(x)$ e portanto $r(x) = r'(x)$. □

Teorema 4.3. *Sejam A um anel comutativo com unidade. Dados* $f(x), g(x) \in A[x]$ *e* $g(x) = b_0 + b_1x + b_2x^2 + \ldots b_mx^m$ *com* $b_m \in U(A)$. *Existem únicos* $f(x), r(x) \in A[x]$ *tais que* $f(x) = g(x) \cdot q(x) + r(x)$, *com* $r(x) = 0$ *ou* $\partial\left(r(x)\right) < \partial\left(g(x)\right)$.

Demonstração. Para mostrar a existência procedemos da mesma maneira da prova do teorema 4.2.

Falta mostrarmos a unicidade.

Sejam $q(x),' q(x), r(x), r'(x) \in A[x]$

$$f(x) = g(x)q'(x) + r'(x),\ com\ r'(x) = 0\ ou\ \partial\left(r'(x)\right) < \partial\left(g(x)\right)$$

Teremos agora a igualdade

$$g(x)\left(q(x) - q'(x)\right) = r(x) - r'(x)$$

Suponha $q(x) - q'(x) \neq 0$

Afirmação: $g(x)\left(q(x) - q'(x)\right) \neq 0$ e $\partial\left(g(x)\left(q(x) - q'(x)\right)\right) \geq \partial\left(g(x)\right)$.

Escreva $q(x) - q'(x) = c_0 + c_1x + c_2x^2 + \ldots + c_tx^t$ com $c_t \neq 0$

Se $g(x)\left(q(x) - q'(x)\right) = 0$ vem que $b_mc_t = 0$, e daí, $b_m^{-1}b_mc_t = 0$, que leva a contradição $c_t = 0$. Logo $g(x)\left(q(x) - q'(x)\right) \neq 0$, desde que $b_mc_t \neq 0$, temos:

$$\partial\left(g(x)\left(q(x) - q'(x)\right)\right) = m + t \geq m = \partial\left(g(x)\right)$$

Da afirmação acima podemos concluir que $r(x) \neq 0$ e $r'(x) \neq 0$. De fato, se $r(x) = 0$, então $g(x)\left(q(x) - q'(x)\right) = r'(x)$. Olhando para o grau, chegamos a um absurdo.

$$\partial\left(g(x)\right) = \partial\left(g(x)\left(q(x) - q'(x)\right)\right) = \partial\left(r'(x)\right) < \partial\left(g(x)\right)$$

Assim $r(x) \neq 0$, e analogamente $r'(x) \neq 0$. Isso garante que podemos falar em $\partial\left(r(x)\right)$ e $\partial\left(r'(x)\right)$.

Finalmente,

$$\partial\left(g(x)\right) \leq \partial\left(g(x)\left(q(x) - q'(x)\right)\right) = \partial\left(r(x) - r'(x)\right) \leq max\{\partial\left(r(x)\right), \partial\left(r'(x)\right)\} < \partial\left(g(x)\right).$$

A contradição acima mostra que não podemos ter $q(x) - q'(x) \neq 0$. Portanto $q(x) = q'(x)$ e consequentemente $r(x) = r'(x)$.

□

Definição 4.4. *Sejam A um anel, $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in A[x]$ e $\alpha \in A$. Chamaremos de **valor** de $f(x)$ em α o elemento*

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots a_n\alpha^n.$$

Como A é anel e $\alpha, a_0, a_1, \ldots, a_n \in A$, então $f(\alpha) \in A$

Se $f(\alpha) = 0$ dizemos que α é raiz de $f(x)$.

Proposição 4.3. *Sejam A um anel comutativo com unidade e $\alpha \in A$. Para $f(x) \in A[x]$ existe $q(x) \in A[x]$ tal que $f(x) = (x - \alpha)q(x) + f(\alpha)$.*

Demonstração. Como $\alpha \in A$ temos que $x - \alpha \in A[x]$ de acordo com o teorema 4.3 existem $q(x), r(x) \in A[x]$ tais que $f(x) = (x - \alpha)q(x) + r(x)$, com $r(x) = 0$ ou $\partial\left(r(x)\right) < \partial\left(x - \alpha\right)) = 1$.

Isso assegura que $r(x)$ é constante.

Avaliando $f(x)$ no ponto α, temos que

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) \Longrightarrow f(\alpha) = r(\alpha)$$

Como $r(x)$ é constante, então $r(x) = f(\alpha)$ e com isso temos que

$$f(x) = (x - \alpha)q(x) + f(\alpha).$$

□

Corolário 4.2 (D'Alembert)**.** *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) $(x-\alpha)$ *divide* $f(x)$.

Demonstração. $(i) \Longrightarrow (ii)$ Segue da proposição 4.3 que existe $q(x) \in A[x]$ tal que $f(x) = (x-\alpha)q(x) + f(\alpha)$, mas como α é raiz temos que $f(\alpha) = 0$ e portanto $(x-\alpha)|f(x)$.

$(ii) \Longrightarrow (i)$ Por hipótese existe $q(x) \in A[x]$ tal que $f(x) = (x-\alpha)q(x)$. Analisando $f(x)$ no ponto α temos que

$$f(\alpha) = (\alpha-\alpha)q(\alpha) = 0.$$

Portanto α é raiz de $f(x)$. □

Definição 4.5. *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 raiz de multiplicidade r ,* $r \in \mathbb{N}^*$ *quando*

$$f(x) = (x-\alpha)^r q(x) \text{ , com } q(x) \in A[x] \text{ e } q(\alpha) \neq 0$$

Observação:

Dizer que α é uma raiz de multiplicidade r de $f(x)$, significa dizer que Dizer que α é uma raiz de multiplicidade r de $f(x)$, significa dizer que $(x-\alpha)^r|f(x)$ e $(x-\alpha)^{r+1} \nmid f(x)$.

Exemplo 4.5. *Determinar a multiplicidade da raiz 2 do polinômio*

$$f(x) = x^4 + x^3 - 3x^2 - 5x - 2.$$

Dividindo $f(x)$ *por* $(x-2)$*, temos que*

$$f(x) = (x-2)(x^3 + 3x^2 + 3x + 1)$$

Como 2 não é raiz de $q(x) = x^3 + 3x^2 + 3x + 1$*, pois* $q(2) \neq 0$*, temos que 2 é raiz simples de* $f(x)$*, ou seja, multiplicidade 1.*

Proposição 4.4. *Sejam A um domínio,* $f(x) \in A[x], f(x) \neq 0$ *e* $\alpha_1, \alpha_2, \ldots, \alpha_t$*, com* $t \in \mathbb{N}$ *as raízes distintas de* $f(x)$ *com multiplicidade* $r_1, r_2, \ldots, r_t$ *respectivamente. Então* $r_1 + r_2 + \ldots + r_t \leq \partial(f(x))$ *.*

Demonstração. Como α_1 é raiz de multiplicidade r_1, então $f(x) = (x-\alpha_1)^{r_1} q_1(x)$, 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

$$f(x) = (x-\alpha_1)^{r_1}(x-\alpha_2)^{r_2}q_2(x), q(x) \in A[x] \text{ e } q_2(\alpha_2) \neq 0$$

Seguindo o processo,

$$f(x) = (x-\alpha_1)^{r_1}(x-\alpha_2)^{r_2}q_2(x)\cdots(x-\alpha_t)^{r_t}q_t(x), q_t(x) \in A[x]$$

Usando a propriedade do grau de polinômios em domínios, vem que

$$\partial(f(x)) = \partial((x-\alpha_1)^{r_1}) + \partial(x-\alpha_2)^{r_2}) + \ldots + \partial((x-\alpha_t)^{r_t}) + \partial(q_t(x))$$

$$= r_1 + r_2 + \ldots + r_t + \partial(q_t(x))$$

$$\geq r_1 + r_2 + \ldots + r_t.$$

□

Exemplo 4.6. *$f(x) = (x-1)^2(x^2-2)(x^2+1) \in \mathbb{Z}[x]$. 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.

Em $\mathbb{R}$,
- *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*

Em **C**,
- *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 $1 = r_5$*

$r_1 + r_2 + r_3 + r_4 + r_5 = 6 = \partial(f(x))$

Definição 4.6. *Se $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in F[x]$ então a derivada de $f'(x)$ de $f(x)$ é definida por $f'(x) = a_1 + a_2x + a_3x^2 + \ldots + a_nx^{n-1} \in F[x]$.*

Se $f(x), g(x) \in F[x]$ segue imediatamente as regras de derivação

(i) $(f(x)+g(x))' = f(x)' + g(x)'$

(ii) $(a \cdot f(x))' = a \cdot f(x)'$

(iii) $(f(x)g(x))' = f(x)'g(x) + f(x)g(x)'$

Teorema 4.4. *Um elemento $\alpha \in F$ é uma raiz múltipla de $f(x) \in F[x]$ se e somente se é uma raiz de $f(x)$ e de $f'(x)$.*

Demonstração. Suponhamos que $\alpha \in F$ seja uma raiz de multiplicidade $m \geq 2$, ou seja, $f(x) = (x-\alpha)^m g(x)$,onde $g(x) \in F[x]$ e $g(\alpha) \neq 0$. Então

$$f'(x) = ((x-\alpha)^m g(x))' = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g(x)' \ \ com\, m-1 \geq 1$$

Portanto $f'(\alpha) = 0$ e α é raiz de $f'(x)$.

Suponhamos agora que $\alpha \in F$ seja raiz de $f(x)$ e de $f'(x)$. Então $f(x) = (x-\alpha)q(x)$ onde $q(x) \in F[x]$ e assim

$$f'(x) = q(x) + (x-\alpha)g(x)' \Longrightarrow f'(\alpha) = q(\alpha) = 0$$

Logo α é raiz de $q(x)$ e portanto $(x-\alpha)$ divide $q(x)$ e então $q(x) = (x-\alpha)h(x)$ com $h(x) \in F[x]$ e assim $f(x) = (x-\alpha)^2 h(x)$ e portanto α é raiz com múltipla de $f(x)$. □

4.2 Irredutibilidade de Polinômios

Polinômios irredutíveis são aqueles que não podem ser decompostos como produto de outros polinômios não invertíveis. De acordo com a proposição 4.2, os polinômios invertíveis de um domínio $A[x]$ coincidem com os elementos invertíveis do domínio A.

Definição 4.7. *Sejam D um domínio e $p(x) \in D[x]$ um polinômio não nulo e não invertível. Dizemos que $p(x)$ é irredutível quando $p(x) = f(x)g(x)$, com $f(x), g(x) \in D[x]$, então $f(x)$ ou $g(x)$ é invertível em $D[x]$.*

Por outro lado dizemos que $p(x)$ é redutível quando existem $f(x), g(x) \in D[x]$,não inversíveis, tais que $p(x) = f(x)g(x)$.

Proposição 4.5. *Sejam K um corpo e $p(x) \in K[x]$.*

(i) Se $p(x)$ é constante, então $p(x)$ não é redutível e nem irredutível em $K[x]$.

(ii) Se $\partial(p(x)) = 1$, então $p(x)$ é irredutível em $K[x]$.

Demonstração. (i) É claro que o polinômio $p(x) = 0$ não é redutível nem irredutível. Se $p(x) = a, a \neq 0$, então $p(x)$ é inversível em $K[x]$ e portanto, não é redutível nem irredutível. (ii) Como $\partial(p(x)) = 1$ temos que $p(x)$ é não nula e não inversível em $K[x]$. Escrevendo

$p(x) = f(x)g(x)$, com $f(x), g(x) \in K[x]$ e usando os resultados sobre grau de polinômios, temos: $1 = \partial(p(x)) = \partial(f(x)) + \partial(g(x))$, segue que $\partial(f(x)) = 0$ ou $\partial(g(x)) = 0$. Assim $f(x)$ ou $g(x)$ é um 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 4.5 (Teorema Fundamental da Álgebra)**.** *Todo polinômio não constante de* $\mathbb{C}[x]$ *tem todas as suas raízes em* $\mathbb{C}$

Demonstração. A demonstração deste teorema pode ser encontrado em (JANESCH, 2008) na página 51 teorema 1.3.1 □

Teorema 4.6. *Seja* $p(x)$ *em* $\mathbb{C}[x]$*. São equivalentes:*

(i) $\partial(p(x)) = 1$

(ii) $p(x)$ *é irredutível em* $\mathbb{C}[x]$.

Demonstração. $(i) \Longrightarrow (ii)$ Como $\mathbb{C}$ é corpo, o resultado segue do item (ii) proposição 4.5

$(ii) \Longrightarrow (i)$ Como $p(x)$ é irredutível, segue do item (i) proposição 4.5 que $p(x)$ não é constante.Logo $\partial(p(x)) \geq 1$. Suponha $\partial(p(x)) > 1$, então pelo teorema 4.5 $p(x)$ possui raiz $\alpha \in \mathbb{C}$ e então $p(x) = (x-\alpha)q(x)$, com $q(x) \in \mathbb{C}[x]$. Segue que $\partial(g(x)) + 1 = \partial(p(x)) > 1$. Assim $\partial(g(x)) > 0$ e $p(x)$ é decomposto em polinômios não nulos e não inversíveis em $\mathbb{C}[x]$, contradizendo a irredutibilidade de $p(x)$. Portanto $\partial(p(x)) = 1$. □

Proposição 4.6. *(a) Sejam D um domínio,* $p(x) \in D[x]$ *e* $\partial(p(x)) > 1$*. Se* $p(x)$ *tem uma raiz em D em* $p(x)$ *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* $p(x)$ *é redutível em* $K[x] \Longleftrightarrow p(x)$ *tem raiz em K.*

Demonstração. (a) Seja $\alpha \in D$ uma raiz de $p(x)$. Segue que $p(x) = (x-\alpha)q(x)$, com $q(x) \in D[x]$.

Como $\partial(x-\alpha)) = 1$ e $\partial(q(x)) \geq 1$. Assim $(x-\alpha)$ e $q(x)$ são elementos não nulos e não inversíveis de $D[x]$, portanto $p(x)$ é redutível em $D[x]$.

(b) $(\Longleftarrow)$ segue do item (a)

$(\Longrightarrow)$ Desde que $p(x)$ seja redutível em $K[x]$, existem $f(x), g(x) \in K[x]$ não inversíveis e não nulos tais que $p(x) = f(x)g(x)$.

Como $p(x)$ tem grau 2 ou 3, e $f(x)$ e $g(x)$ são não constantes, vem que $\partial(f(x)) = 1$ ou $\partial(g(x)) = 1$. Sem perda de generalidade, assumimos $\partial(f(x)) = 1$ e escrevemos $f(x) = ax + b$, $a \neq 0$. Assim $p(x) = (ax+b)g(x)$ Portanto $-a^{-1}b \in K$ é raiz de $p(x)$.

□

Teorema 4.7. *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. $(i) \Longrightarrow (ii)$ Como $p(x)$ é irredutível em $\mathbb{R}[x]$, temos que $p(x)$ não é constante, e pelo teorema 4.5 , existe $\alpha \in \mathbb{C}$ tal que α é raiz de $p(x)$

1º caso:$\alpha \in \mathbb{R}$

Desde que $(x-\alpha) \in \mathbb{R}[x]$ e $(x-\alpha)$ divida $p(x)$ existe $q(x) \in \mathbb{R}[x]$ tal que $p(x) = (x-\alpha)q(x)$. No entanto $p(x)$ é polinômio irredutível em $\mathbb{R}[x]$, então $q(x)$ é um polinômio constante não nulo e portanto $\partial(p(x)) = 1$

2º caso: $\alpha \notin \mathbb{R}$.

Escreva $\alpha = a + bi$, com $a, b \in \mathbb{R}$ 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 $\mathbb{C}[x]$.

$p(x) = (x-\alpha)(x-\overline{\alpha})q(X)$, Com $p(x) \in \mathbb{C}[x]$ $p(x) = (x-(a+bi)(x-(a-bi))q(x)$.

$p(x) = (x-a-bi)(x-a+bi)q(x)$

$p(x) = (x^2 - 2ax + a^2 + b^2)q(x)$.

Como $p(x)$ e $(x^2 - 2ax + a^2 + b^2)$ estão em $\mathbb{R}[x]$, então o algoritmo de Euclides garante a existência de $q_1(x)$ e $r_1(x)$ tais que $p(x) = ((x^2 - 2ax + a^2 + b^2)q_1(x) + r_1(x)$, com $r_1(x) = 0$ ou $\partial(r_1(x)) < 2$

Por outro lado, se $q_1(x)$ e $r_1(x) \in \mathbb{C}[x]$, então temos em $\mathbb{C}[x]$ as igualdades $p(x) = (x^2 - 2ax + a^2 + b^2)q(x)$ e $p(x) = (x^2 - 2ax + a^2 + b^2)q_1(x) + r_1(x)$. Pela unicidade do quociente e do resto, obtidos pelo algoritmo de Euclides para polinômios em $\mathbb{C}[x]$, vem que $q(x) = q_1(x)$ e $r_1(x) = 0$. Segue que $q(x) \in \mathbb{R}[x]$, pois $q_1(x) \in \mathbb{C}[x]$.

Como $p(x) = (x^2 - 2ax + a^2 + b^2)q(x)$ é irredutível em $\mathbb{R}[x]$, temos que $q(x)$ é constante não nulo $q(x) = c$, com $c \in \mathbb{R}^*$.

$$p(x) = (cx^2 - 2cax + ca^2 + cb^2) = cx^2 - 2cax + c(a^2 + b^2)$$

Logo $\partial(p(x)) = 2$ e o discriminante será dado por $\triangle = (-2ca)^2 - 4c(c(a^2 + b^2))$

$\triangle = 4c^2a^2 - 4c^2a^2 - 4c^2b^2$

$\triangle = -4c^2b^2 < 0$pois $b, c \neq 0$.

$(ii) \Longrightarrow (i)$ Se $\partial(p(x)) = 1$, então $p(x)$ é irredutível em $\mathbb{R}[x]$ pela proposição 4.5. Se $\partial(p(x)) = 2$ e o discriminante for negativo, então $p(x)$ não tem raízes em $\mathbb{R}$ e pela proposição 4.6 $p(x)$ é irredutível em $\mathbb{R}[x]$. □

Proposição 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. A demonstração desta proposição se encontra em (GONÇALVES, 2007) pagina 82 proposição 2 □

Definição 4.8. *O polinômio $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ é dito primitivo quando $mmc = (a_0, a_1, a_2, \ldots, a_n) = 1$*

Proposição 4.8. *Seja $p(x) \in \mathbb{Z}[x]$ tal que $\partial(p(x)) \geq 1$ e $p(x)$ primitivo, então são equivalentes:*

(i) $p(x)$ é irredutível em $\mathbb{Z}[x]$.

(ii) $p(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração. $(i) \Longrightarrow (ii)$ Segue do lema de Gauss.

$(ii) \longrightarrow (i)$É claro que $p(x) \in \mathbb{Z}[x]^*/U(\mathbb{Z})$, pois $\partial(p(x)) \geq 1$

Como $f(x), g(x) \in \mathbb{Q}[x]$ e $p(x)$ é irredutível em $\mathbb{Q}[x]$ segue que $f(x)$ *ou* $g(x)$ é polinômio constante não nulo. Sem perda de generalidade, seja $f(x) = a \neq 0$, vem que $p(x) = ag(x)$. Assim a divide todos os coeficientes de $p(x)$, mas $p(x)$ é primitivo e então $a = \pm 1$. Segue que $f(x) = \pm 1$ é inversível em $\mathbb{Z}[x]$ e portanto $p(x)$ é irredutível em $\mathbb{Z}[x]$.

□

4.2.1 Critério de irredutibilidade de Eisenstein

Proposição 4.9. *Seja $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \mathbb{Z}[x]$. Se existir um número p tal que $p|a_0, p|a_1, \ldots, p|a_{n-1}, p \nmid a_n e p^2 \nmid a_0$ então $f(x)$ é irredutível sobre $\mathbb{Q}$*

Demonstração. A demostração se encontra em (GONÇALVES, 2007) teorema 6 pagina 83 □

Exemplo 4.7. *Seja $f(x) = x^3 + 2x + 10$. O critério de Eisenstein se aplica para o primo $p = 2$, logo $f(x)$ é irredutível sobre $\mathbb{Q}$.*

4.3 Ideais principais

Seja K um corpo. Um ideal principal de $K[x]$ é o conjunto dos múltiplos de um elemento $p(x) \in K[x]$. $J = p(x) \cdot K[x] = \{p(x) \cdot f(x) \; ; \; f(x) \in K[x]\}$

Teorema 4.8. *Todo ideal de $K[x]$ é principal.*

Demonstração. Seja J um ideal de $K[x]$. Se $j = \{0\}$, então J é gerado por 0. Suponhamos que $J \neq \{0\}$ e escolhemos $0 \neq p(x) \in J$ tal que $\partial(p(x))$ seja o menor possível. Se $p(x) = a$ constante não nulo, então $1 = a^{-1}a \in J$ e assim segue imediatamente que $J = K[x]$ é gerado por $1 \in K[x]$.

Suponhamos então que $\partial(p(x)) > 0$. Como $p(x) \in J$ claramente temos que $K[x] \cdot p(x) \subset J$. Agora vamos provar que $J \subset K[x] \cdot p(x)$.

De fato, seja $f(x) \in J$. Pelo algoritmo de Euclides existem $q(x), r(x) \in K[x]$ tais que $f(x) = q(x)p(x) + r(x)$, com $r(x) = 0$ ou $\partial(r(x)) < \partial(p(x))$.

Agora como $p(x), f(x) \in K[x]$. Segue que $r(x) = f(x) - q(x)p(x) \in J$, pela minimalidade de nossa escolha para $p(x)$ temos que $r(x) = 0$ e portanto $f(x) = q(x)p(x) \in K[x] \cdot p(x)$, ou seja, $j \subset K[x] \cdot p(x)$. □

5 CORPOS FINITOS

5.1 Construção de corpos a partir de um polinômio irredutível

Teorema 5.1. *sejam K um corpo e p(x) ∈ K[x]. Então as seguintes condições são equivalentes:*

(i) p(x) é irredutível sobre K.

(ii) $J = K[x] \cdot p(x)$ é um ideal maximal em K[x].

(iii) $\frac{K[x]}{J}$ é corpo, onde $J = K[x] \cdot p(x)$.

Demonstração. $(i) \Longleftrightarrow (ii)$

$(\Longrightarrow)$ Suponhamos $p(x) \in K[x]$, $p(x)$ irredutível sobre K. Como $\partial(p(x)) > 1$ segue imediatamente que $J \neq K[x]$.

Seja $I = K[x] \cdot h(x)$ um ideal de $K[x]$ tal que $I \supset J$. Vamos provar que $I = J$ ou $I = K[x]$.

Assim $p(x) \in K[x] \cdot p(x) = J \subset I = K[x] \cdot h(x) \Longrightarrow p(x) \subset K[x] \cdot h(x)$, isso nos diz que $p(x) = g(x)h(x)$ para algum $g(x) \in K[x]$. Como $p(x)$ é irredutível temos que $g(x) = a$ constante não nulo, ou $h(x) = b$ constante não nulo.

Se $g(x) = a$ temos que $h(x) = a^{-1}p(x)$ e assim $I = K[x] \cdot h(x) \subset K[x] \cdot p(x) = J$ e portanto $I = J$.

Se $h(x) = b$ temos que $I = K[x] \cdot h(x) = K[x]$.

$(\Longleftarrow)$ Seja $J = K[x] \cdot p(x)$ um ideal maximal em $K[x]$. Assim $J \neq K[x]$ nos diz que $\partial(p(x)) \geq 1$. Suponhamos $g(x), h(x) \in K[x]$ tais que $p(x) = g(x)h(x)$. assim segue imediatamente que $J \subset I = K[x] \cdot h(x)$ e como J é ideal maximal temos que $I = J$ ou $I = K[x]$.

Se $I = J$ segue que $h(x) \in J = K[x] \cdot p(x)$ e $p(x) = g(x)f(x)p(x)$, com $f(x) \in K[x]$, Como $p(x) \neq 0$ e $K[x]$ é um domínio, temos $1 = g(x)f(x)$, ou seja, $g(x) \in K[x]$ é inversível e então $g(x) = a \neq 0$ é um polinômio constante e $p(x)$ é irredutível sobre K.

Se $I = K$, então $h(x) = b \neq 0$ um polinômio constante e portanto $p(x)$ é um polinômio irredutível sobre K.

$(ii) \Longleftrightarrow (iii)$ é consequência do teorema 3.5 □

Exemplo 5.1. *Vamos provar que se $A = \mathbb{R}$ e $I = A(x^2+1)$ então $\frac{A}{I} \simeq \mathbb{C}$.*

Solução: *De fato, como x^2+1 é um polinômio irredutível em $\mathbb{R}[x]$ então temos que $L = \frac{A}{I}$ é um corpo.*

Se $p(x) \in \mathbb{R}$ então pelo algoritmo de Euclides existem $q(x), r(x) \in \mathbb{R}[x]$ tais que $p(x) = (x^2+1)q(x) + r(x)$, com $r(x) = ax + b$, $a, b \in \mathbb{R}$. Passando a barra (modulo I) e tendo em vista que $\overline{x^2+1)} = \overline{0}$, temos que $\overline{p(x)} = \overline{(x^2+1)q(x)+r(x)} = \overline{r(x)} = \overline{ax+b} = \overline{a}\overline{x} + \overline{b}$. Assim $L = \{\overline{a}\overline{x} + \overline{b}\ ;\ a, b \in \mathbb{R}\}$. Observe também que se denotarmos $\overline{\mathbb{R}} = \{\overline{a}\ ;\ a \in \mathbb{R}\}$ então a função barra $\begin{array}{rccc} - & : & \mathbb{R} & \longrightarrow & \overline{\mathbb{R}} \\ & & a & \mapsto & \overline{a} \end{array}$ *preserva soma e produto e de fato isomorfismo, ou seja $\mathbb{R} \simeq \overline{\mathbb{R}}$.*

Agora, como em L, $\overline{x}$ satisfaz a equação $z^2 + \overline{1}$, pois $z^2 + \overline{1} = \overline{z^2+1} = \overline{0}$, Podemos construir um isomorfismo ψ de $\mathbb{C}$ sobre L como segue:

$$\begin{array}{rccc} \psi & : & \mathbb{C} & \longrightarrow & L \\ & & i & \mapsto & \overline{x} \\ & & a & \mapsto & \overline{a} \end{array}$$

Teorema 5.2. *Sejam p um numero primo e p(x)$\in \mathbb{Z}_p[x]$ um polinômio irredutível em $\mathbb{Z}_p$ e de grau n. Se $J = p(x) \cdot \mathbb{Z}_p[x]$, 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 do teorema 5.1 que $\frac{\mathbb{Z}_p[x]}{J}$ é corpo. Falta mostrar que $\frac{\mathbb{Z}_p[x]}{J}$ tem p^n elementos.

Seja $f(x) \in \mathbb{Z}_p[x]$, aplicando o algoritmo de Euclides, existem $q(x), r(x) \in \mathbb{Z}_p[x]$ tais que $f(x) = p(x)q(x) + r(x)$, com $r(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$. Passando a barra (modulo J) e tendo em vista que $\overline{p(x)} = \overline{0}$. temos que $\overline{f(x)} = \overline{r(x)}$. Isso mostra que $\frac{\mathbb{Z}_p[x]}{J} \subset T = \{\overline{r(x)}\ ;\ r(x) \in \mathbb{Z}_p[x]\}$. A inclusão $T \subset \frac{\mathbb{Z}_p[x]}{J}$ é óbvia. Portanto $\frac{\mathbb{Z}_p[x]}{J} = T$.

Agora basta provar que T tem exatamente p^n elementos. Primeiro vamos mostrar que todos os elementos de T são distintos.

$$\partial\left(p(x)h(x)\right) = \partial\left(r(x) - s(x)\right) < n$$

$$n + \partial\left(h(x)\right) < n.\ \textit{Absurdo}.$$

Portanto $\overline{r(x)} \neq \overline{s(x)}$. Agora note que $r(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n_1}x^{n-1}$ tem exatamente n coeficientes, e para cada coeficiente temos p escolhas, pois $a_i \in \mathbb{Z}_p$ e portanto T tem p^2 elementos. □

Exemplo 5.2. *Tome $p(x) = x^2 + x + \overline{1}$ que é irredutível em $\mathbb{Z}_2[x]$ segue do teorema 5.2 que $\frac{\mathbb{Z}_2[x]}{p(x)\mathbb{Z}_2[x]}$ é um corpo com 4 elementos.*

De acordo com a demonstração do teorema 5.2, estes elementos são: $\overline{r(x)} = \overline{\overline{0}}$

$\overline{r(x)} = \overline{\overline{1}}$

$\overline{r(x)} = \overline{x}$

$\overline{r(x)} = \overline{\overline{1}+x} = \overline{\overline{1}}+\overline{x}$

5.2 extensão de corpos

Definição 5.1. *Seja F um corpo e $K \subseteq F$, tal que K é um corpo com as operações de F. Dizemos que K é subcorpo de F. Se $K \neq F$, então K é dito subcorpo próprio de F. Nesse contexto, F é chamado de extensão de (corpos) de K*

Exemplo 5.3. *O corpo $\mathbb{R}$ é extensão do corpo $\mathbb{Q}$, e o corpo $\mathbb{C}$ é extensão do corpo $\mathbb{R}$.*

Definição 5.2. *Um corpo que não contém subcorpo próprio é chamado de subcorpo primo.*

Para definir o grau de uma de uma extensão necessitamos de algumas noções básicas de álgebra linear como espaço vetorial e base. Seja K um corpo qualquer e V um conjunto não vazio onde está definida uma operação soma. Suponhamos também que esteja definida uma operação de elementos de K sobre V. Assim estão definidas:

$$\begin{array}{rcccl} + & : & \mathrm{L}\times L & \longrightarrow & \mathrm{L} \\ & & (\mathrm{u},\mathrm{v}) & \longrightarrow & \mathrm{u+v} \end{array} \quad e \quad \begin{array}{rcccl} \cdot & : & \mathrm{K}\times L & \longrightarrow & \mathrm{L} \\ & & (\lambda,\mathrm{u}) & \longrightarrow & \lambda\ \mathrm{u} \end{array}$$

Dizemos que V munido dessas operações é um espaço vetorial sobre K e as seguintes propriedades são verificadas para quaisquer $u, v, w \in V$ e $\lambda, \mu \in K$

(i) $u+(v+w) = (u+v)+w$ (associatividade da soma)

(ii) $\exists\, 0 \in V$ tal que $u+0 = 0+u = u$ (existência de elemento neutro para a soma)

(iii) Para todo $x \in V$ existe $y \in V$ tal que $x+y = y+x = 0$ (existência de elemento inverso para a soma)

(iv) $u+v = v+u$ (comutatividade da soma)

(v) $1v = v$ onde 1 é unidade do corpo K.

(vi) $\lambda(u+v) = \lambda u+\lambda v$ e $(\mu+\lambda)u = \mu u+\lambda u$

(vii) $\lambda(\mu u) = (\lambda\mu)u = \mu(\lambda u)$

Observação: Se L é uma extensão de corpo K então L pode ser visto como espaço vetorial sobre K. De fato, as operações

$$\begin{array}{rcccc} + & : & \mathrm{L}\times L & \longrightarrow & \mathrm{L} \\ & & (\mathrm{u},\mathrm{v}) & \longrightarrow & \mathrm{u+v} \end{array} \qquad e \qquad \begin{array}{rcccc} \cdot & : & \mathrm{K}\times L & \longrightarrow & \mathrm{L} \\ & & (\lambda,\mathrm{u}) & \longrightarrow & \lambda\ \mathrm{u} \end{array}$$

Um subconjunto não vazio W de V diz-se um subespaço vetorial de V se as seguintes condições são satisfeitas:

(a) $w_1, w_2 \in W \Longrightarrow w_1 + w_2 \in W$

(b) $\lambda \in K, w \in W \Longrightarrow \lambda w \in W$

Se $v_1, v_2, \ldots v_n \in V$ dizemos que $v_1, v_2, \ldots v_n$ são linearmente independentes se equação $\sum_{i=1}^{n} \alpha_i v_i = 0$, com $\alpha_i \in K$ é satisfeita apenas para $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$ caso contrário dizemos que $v_1, v_2, \ldots v_n$ são linearmente dependentes.

Se V é um espaço vetorial e $u_1, u_2, \ldots u_r \in V$ então é de fácil verificação que

$$W = \left\{ \sum_{i=1}^{r} \alpha_i u_i; \alpha_i \in K, i = 1, 2, \ldots, r \right\}$$

é um subespaço vetorial de V, o qual chamaremos de subespaço gerado por $u_1, u_2, \ldots, u_r$. Denotaremos esse espaço por $W = \langle u_1, u_2, \ldots, u_r \rangle$.

Se um conjunto (ordenado) $v_1, v_2, \ldots v_n \in V$ for linearmente independente e tal que $\langle v_1, v_2, \ldots v_n \rangle = V$ dizemos que $v_1, v_2, \ldots v_n$ é uma base de V.

Teorema 5.3. .

(a) Todo espaço vetorial V sobre um corpo K possui uma base.

(b) Se um espaço vetorial V sobre um corpo K possui uma base com n elementos então toda base de Vpossui n elementos.

Se um espaço vetorial sobre um corpo K possui uma base com n elementos, chamamos ao número n de dimensão de V sobre K e denotamos por $[V : K] = n$

Definição 5.3. *A dimensão de F como espaço vetorial sobre K é chamada grau da extensão e é denotada por $[F : K]$. F é dito uma extensão finita de K se $[F : K] < \infty$. Caso contrário dizemos que F é uma extensão infinita.*

Teorema 5.4. *Sejam K um corpo, F uma extensão finita de K e L uma extensão finita de F. Então L é uma extensão finita de K e*

$$[L : K] = [L : F][F : K]$$

Demonstração. Sejam $[L:F]=m$ e $[F:K]=n$. Sejam $\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$ e $\{\beta_1,\beta_2,\ldots,\beta_n\}$ bases de L sobre F e de F sobre K, respectivamente. Então cada elemento $\alpha\in L$ se escreve como $\alpha=a_1\alpha_1+a_2\alpha_2+\ldots+a_m\alpha_m$ com $a_i\in F$, para todo $i=,1,2,\ldots,m$. Além disso, cada $a_i\in F$ pode ser escrito como $a_i=b_{i1}\beta_1+b_{i2}\beta_2+\ldots+b_{in}\beta_n$, onde $b_{ij}\in K$ para todos $i=1,2,\ldots,m$ e $j=1,2,\ldots,n$. Assim obtemos a seguinte expressão

$$\alpha=\sum_{i=1}^{m}a_i\alpha_i=\sum_{i=1}^{m}\left(\sum_{j=1}^{n}b_{ij}\beta_j\right)\alpha_i=\sum_{i=1}^{m}\sum_{j=1}^{n}b_{ij}\beta_j\alpha_i.$$

Assim basta mostrar que que os elementos $\beta_j\alpha_i$, com $1\leq j\leq n$, $1\leq i\leq m$ são linearmente independentes sobre K. Suponhamos que

$$\sum_{i=1}^{m}\sum_{j=1}^{n}b_{ij}\beta_j\alpha_i=0$$

então

$$\sum_{i=1}^{m}\left(\sum_{j=1}^{n}b_{ij}\beta_j\right)\alpha_i=0$$

Pela independência linear dos α_i sobre F temos que

$$\sum_{j=1}^{n}b_{ij}\beta_j=0,\ \ \textit{para todo } i\in\{1,2,\ldots,m\}$$

E pela independência dos β_j sobre K temos que $b_{ij}=0$ para todo $i=1,2,\ldots,m$ e para $j=1,2,\ldots,n$. Logo $\{\beta_j\alpha_i\mid i\in\{1,2,\ldots,m\},j\in\{1,2,\ldots,n\}$ é uma base de L sobre K com mn elementos, isto é, $[L:K]=mn=[L:F][F:K]$. □

Definição 5.4. *Sejam K um subcorpo de F e M um subconjunto de F. Então o corpo $K(M)$ é definido pela interseção de todos os subcorpos de F que contém K e M e é chamado de extensão de corpo obtido de K adjuntando M*

(i) Se M for finito, digamos $M=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ escrevemos $K(M)=K(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

(i) Se M consistir de um único elemento $\alpha\in F$, então $L=K(\alpha)$ é dita uma extensão simples de K e α é dito um elemento definidor de L sobre K.

Definição 5.5. *Seja F uma extensão do corpo K. Dizemos que $\alpha\in F$ é algébrico sobre K quando existe um polinômio não nulo $p(x)\in K[x]$ tal que $p(\alpha)=0$. Caso contrário dizemos que α é transcendente sobre K.*

Exemplo 5.4. *O corpo $\mathbb{R}$ é uma extensão do corpo $\mathbb{Q}$. Como $\sqrt{2}$ é raiz do polinômio $p(x)=x^2-2$ então $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$. De maneira análoga $i\in\mathbb{C}$ é algébrico sobre $\mathbb{Q}$, pois i é raiz do polinômio x^2+1.*

Definição 5.6. *Dizemos que o corpo F é uma extensão algébrica sobre K se todo elemento de F for algébrico sobre K. Se pelo menos um elemento de F for transcendente sobre K a extensão é dita transcendental (ou transcendente).*

Definição 5.7. *Sejam $\alpha \in F$ algébrico sobre K e $p(x)$ um polinômio em $K[x]$, mônico e de menor grau tal que $p(\alpha) = 0$, $p(x)$ é o polinômio minimal (ou mínimo) de α sobre K e denotaremos por $p(x) = m_\alpha(x)$.*

Lema 5.1. *O polinômio minimal $m_\alpha(x) \in F[x]$ de um elemento $\alpha \in K$ divide todos os outros polinômios $p(x) \in F[x]$ tais que $p(\alpha) = 0$.*

Demonstração. Sejam $p(x), m_\alpha(x) \in F[x]$, então pelo algoritmo de Euclides existem $q(x), r(x) \in F[x]$ tais que $p(x) = m_\alpha(x)q(x) + r(x)$.

Como $p(\alpha) = 0$, temos que $p(\alpha) = m_\alpha(\alpha)q(\alpha) + r(\alpha) = 0$, como $m_\alpha(\alpha) = 0$, segue que $r(\alpha) = 0$. Se $r(x) \neq 0$ temos que $\partial(r(x)) < \partial(m_\alpha(x))$, absurdo pois $m_\alpha(x)$ é o polinômio de menor grau que tem α como raiz. Portanto $p(x) = m_\alpha(x)q(x)$.

□

Lema 5.2. *Sejam L uma extensão do corpo K e $\alpha \in L$ algébrico sobre K, então o polinomio minimal $m_\alpha(x)$ é irredutível sobre K.*

Demonstração. Seja $m_\alpha(x)$ o polinômio minimal de $\alpha \in L$. Suponha que $m_\alpha(x)$ seja redutível, então existem $p(x), q(x) \in K[x]$, com $p(x), q(x) \neq 0$ e não constantes tais que $m_\alpha(x) = p(x)q(x)$. Aplicando α, temos que $0 = m_\alpha(\alpha) = p(\alpha)q(\alpha)$, mas como $K[x]$ é domínio então $p(\alpha) = 0$ ou $q(\alpha) = 0$. Se $p(\alpha) = 0$, pelo lema anterior temos que $\partial(m_\alpha(x)) \leq \partial(p(x))$ pela propriedade de grau do polinômio temos que $\partial(p(x)) \leq \partial(m_\alpha(x))$ o que nos diz que $m_\alpha(x) = ap(x)$ e de maneira análoga se $q(\alpha) = 0$ então $m_\alpha(x) = bq(x)$. Absurdo. pois $p(x), q(x)$ são não constantes. □

Corolário 5.1. *Todo elemento $\alpha \in L$ que é algébrico sobre o corpo K possui um único polinômio minimal em $K[x]$*

Demonstração. Sejam $m_1(x), m_2(x) \in K[x]$tais que ambos são polinômios mínimos do elemento $\alpha \in L$ pelo Lema 5.1 temos que $m_1(x) = m_2(x)p(x)$ para algum $p(x) \in K[x]$ e que $m_2(x) = m_1(x)q(x)$ para algum $q(x) \in K[x]$. Assim temos que $\partial(m_1(x)) = \partial(m_2(x)) + \partial(p(x))$ e $\partial(m_2(x)) = \partial(m_1(x)) + \partial(q(x))$ segue que $\partial(m_1(x)) = \partial(m_1(x)) + \partial(p(x)) + \partial(q(x))$ daí

$\partial(p(x)) = \partial(q(x)) = 0$ e com isso $p(x)$ e $q(x)$ são polinômios constantes, ou seja, $m_1(x) = m_2(x) \cdot c$, para algum $c \in K$. Como $m_1(x)$ e $m_2(x)$ são mônicos então $c = 1$ e $m_1(x) = m_2(x)$ $\square$

5.3 Corpo de decomposição

Definição 5.8. *Seja K um corpo e $f(x) \in K[x]$. Dizemos que $f(x)$ se fatora em $K[x]$ se $f(x)$ pode ser escrito como produto de fatores lineares.*

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

Com $c, \alpha_1, \alpha_2, \ldots \alpha_n \in K$.

Definição 5.9. *Seja K um corpo e F uma extensão de K. Então F é um corpo de decomposição para um polinômio $f(x) \in K[x]$ se*

(i) $f(x)$ se fatora em $F[x]$

(ii) Se existir um corpo F' tal que $K \subset F' \subset F$ e $f(x)$ se fatora em $F'[x]$, então $F' = F$. Ou seja, F é o menor corpo que contém K e todas as raízes de $f(x)$.

Teorema 5.5. *Seja K um corpo e $f(x) \in K[x]$ um polinômio irredutível. Então, existem um corpo F e $\alpha \in F$ tais que $K \subset F$ e $f(\alpha) = 0$. Além disso $[F : K] = \partial(f(x))$*

Demonstração. Consideremos $F = \frac{K[x]}{f(x)\cdot K[x]}$ que é um corpo, pois $f(x)$ é irredutível. Os elementos de F são as classes $h(x) + f(x) \cdot K[x]$, com $h(x) \in K[x]$. Para todo $a \in K \subset K[x]$ podemos construir as classes $\overline{a}$ determinada pelo polinômio constante a e se $a, b \in K$ são distintos, então $\overline{a} \neq \overline{b}$, pois f possui grau positivo por não ser invertível. A aplicação $a \longrightarrow \overline{a}$ nos fornece um isomorfismo de K sobre um subcorpo K' de F, portanto, F pode ser visto como uma extensão de K. Para todo $h(x) = a_0 + a_1x + a_2x^2 + \ldots + a_mx^m \in K[x]$ e, usando as operações com classes residuais e a identificação $\overline{a_i} = a_i$, temos que

$$\begin{aligned}\overline{h(x)} &= \overline{a_0 + a_1x + a_2x^2 + \ldots + a_mx^m} \\ &= \overline{a_0} + \overline{a_1x} + \ldots + \overline{x_mx^m} \\ &= a_0 + a_1\overline{x} + \ldots + a_m\overline{x}^m\end{aligned}$$

Portanto todo elemento de F pode ser escrito como um polinômio em $\overline{x}$ com coeficientes em K. Como todo corpo que contém K e $\overline{x}$ deve conter os elementos da forma $h(\overline{x})$, onde $h(x) \in K[x]$,

temos que F é um extensão K obtida por adjunção de $\overline{x}$. Se $f(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$ então

$$f(\overline{x}) = b_0 + b_1\overline{x} + \ldots + b_n\overline{x}^n = \overline{f(x)} = 0$$

Portanto $\overline{x}$ é uma raiz em F.

Falta mostrar que $[F : K] = \partial(f(x))$. Seja $c \in F$, vimos c pode ser escrito como um polinômio em $\overline{x}$ com coeficientes em K. Assim $c = h(\overline{x})$, $h(x) \in K[x]$. Pelo algoritmo da divisão existem $q(x), r(x) \in K[x]$ tais que $h(x) = q(x)f(x) + r(x)$ com $\partial(r(x)) < n$. Assim temos que $c = h(\overline{x}) = q(\overline{x})f(\overline{x}) + r(\overline{x}) = r(\overline{x}) = a_0 + a_1\overline{x} + a_2\overline{x}^2 + \ldots + a_{n-1}\overline{x}^{n-1}$, pois $f(\overline{x}) = 0$, portanto $\{a_0, a_1, \ldots, a_{n-1}\}$ é uma base de F sobre K daí $[F : K] = \partial(f(x))$. □

Teorema 5.6. *Se $f(x) \in K[x]$, então existe uma extensão F de K que é um corpo de decomposição para $f(x)$.*

Demonstração. Vamos mostrar que existe uma extensão L de K sobre a qual $f(x)$ se decompõe completamente em fatores lineares. Faremos a prova por indução sobre o grau n de $f(x)$.

Se $n = 1$ então $L = K$.

Suponhamos $n > 1$. Se os fatores se os fatores irredutíveis de $f(x)$ forem de grau 1, então K é um corpo de decomposição para $f(x)$ e $L = K$. Caso contrário, pelo menos um dos fatores irredutíveis, suponha $p(x)$, tem grau ≥ 2. Pelo teorema 5.5 , existe uma extensão L_1 de K contendo uma raiz α de $f(x)$. Logo, sobre L_1 o polinômio possui o fator linear $x - \alpha$. O grau do fator restante f_1 é $n - 1$. Então por indução existe uma extensão L de L_1 contendo todas as raízes de $f_1(x)$. Como $\alpha \in L$, L é uma extensão de K contendo todas as raízes de $f(x)$

Finalmente, tome F a interseção de todos os subcorpos de L contendo K e também todas as raízes de $f(x)$. Então F é o corpo de decomposição de $f(x)$. □

5.4 Caracterização dos corpos finitos

Definição 5.10. *A característica de um corpo K é o menor número inteiro positivo tal que $ma = \underbrace{a + a + a + \ldots + a}_{m \text{ vezes}} = 0$. Se m não existir, dizemos que a característica do corpo é zero.*

Teorema 5.7. *A característica de um domínio de integridade é um número primo ou zero.*

Demonstração. Seja D um domínio, e suponhamos que sua característica seja $n \neq 0$. Se n não é primo, então $n = ab$ onde $1 < a < n$ e $1 < b < n$. Assim, $0 = 1.n = 1(ab) = (1a)(1b)$. Como

não há divisores de zero em D, então $1a = 0$ ou $1b = 0$. Segue que $ar = (1a)r = 0$ para todo $r \in D$ ou $br = (1b)r = 0$ para todo $r \in D$, o que contradiz a definição de característica n. □

Teorema 5.8. *Se F é um corpo finito, então F tem característica $p > 0$, onde p é um número primo.*

Demonstração. Pelo teorema 5.7, basta mostrar que todo corpo finito possui característica positiva. Assim consideremos K um corpo finito e sejam $1, 2 \cdot 1, 3 \cdot 1, \ldots$ os múltiplos inteiros da unidade de K. Como K possui somente um número finito de elementos distintos, temos então que existem inteiros $m, n \in \mathbb{Z}$ tais que $1 < m < n$ e $n1 = m1$, ou seja, $n1 - m1 = 0 \Longrightarrow (n-m)1 = 0$ e assim K possui característica positiva. □

Para um primo p, seja $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$. Consideremos a aplicação $\phi : \mathbb{Z}_p \longrightarrow \mathbb{F}_p$ definida por $\phi(\overline{a}) = a$, para $a \in \{1, 2, 3, \ldots, p-1\}$. Notemos que se $\overline{a} = \overline{b} \in \mathbb{Z}_p$, existe $k \in \mathbb{Z}$ tal que $a - b = pk$. Assim $\phi(\overline{a-b}) = \phi(\overline{pk}) \Longrightarrow a - b = 0 \Longrightarrow \phi(a) - \phi(b) = 0 \Longrightarrow \phi(a) = \phi(b)$.

Portanto ϕ está bem definida. Além disso, ϕ é um homomorfismo sobrejetor. De fato, para todos $\overline{a}, \overline{b} \in \mathbb{Z}_p$, temos que:

$$\phi(\overline{a} + \overline{b}) = \phi(\overline{a+b}) = a + b = \phi(\overline{a}) + \phi(\overline{b}).$$

$$\phi(\overline{a}\overline{b}) = \phi(\overline{ab}) = ab = \phi(\overline{a})\phi(\overline{b}).$$

E ainda para todo $a \in \mathbb{F}_p$ existe $\overline{a} \in \mathbb{Z}_p$ tal que $\phi(\overline{a}) = a$

Assim , pelo teorema do isomorfismo ,$\mathbb{F}_p$ é isomorfo a $\mathbb{Z}_p$, ou seja, $\mathbb{F}_p$ tem a mesma estrutura que $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

Então $\mathbb{F}_p$ dotado da estrutura de corpo induzida por ϕ é um corpo finito, chamado de Corpo de Galois de ordem p

Proposição 5.1. *Seja p um número primo. O subcorpo primo de um corpo F de característica p é isomorfo a $\mathbb{F}_p$*

Demonstração. Consideremos a aplicação $\phi : \mathbb{Z}_p \longrightarrow F$ dada por $\phi(\overline{a}) = a \cdot 1$. Temos que a aplicação está bem definida. De fato, se $\overline{a} = \overline{b}$ em $\mathbb{Z}_p$, com a, b inteiros, então existe $k \in \mathbb{Z}$ tal que $a = b + pk$ de modo que

$$a1 = (b + pk)1 = b1 + pk1 = b1$$

Além disso ϕ é homomorfismo. De fato, para todos $\overline{a},\overline{b} \in \mathbb{Z}_p$, temos que

$$\phi(\overline{a}+\overline{b}) = (a+b)\cdot 1 = a1 + b1 = \phi(\overline{a}) + \phi(\overline{b}).$$

$$\phi(\overline{a}\cdot\overline{b}) = (ab)\cdot 1 = a1 \cdot b1 = \phi(\overline{a})\cdot\phi(\overline{b}).$$

Logo, sendo $\mathbb{Z}_p$ e F corpos, temos que ϕ é um homomorfismo injetor e assim $\phi(\mathbb{Z}_p)$ é um subcorpo de F isomorfo a $\mathbb{Z}_p$. Como qualquer subcorpo de F contém 0 e 1, temos que qualquer subcorpo também irá conter $\phi(\mathbb{Z}_p)$. Logo $\phi(\mathbb{Z}_p)$ é o subcorpo primo de F e é isomorfo a $\mathbb{F}_p$. □

Lema 5.3. *Sejam p um número primo e F um corpo finito de característica p. Então*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

para todo inteiro positivo n.

Demonstração. Vamos provar por indução em n.

Para $n = 1$, Usando o teorema binomial, temos que

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \quad (*)$$

Se $0 < k < p$, então

$$\binom{p}{k} = \frac{p!}{(p-k)!k!}$$

Deve ser divisível por p, uma vez que p não divide $(p-k)!k!$. Como F é um corpo finito de característica p, então todos, exceto o primeiro e o ultimo termo de $(*)$ devem ser zero. Portanto $(a+b)^p = a^p + b^p$. Agora suponhamos que o resultado seja válido para todo h, onde $1 \leq h \leq n$. Pela hipótese de indução,

$$(a+b)^{p^{n+1}} = ((a+b)^p)^{p^n} = (a^p + b^p)^{p^n} = (a^p)^{p^n} + (b^p)^{p^n} = a^{p^{n+1}} + b^{p^{n+1}}.$$

Logo o resultado é válido para $n+1$ e , então , a prova está completa. □

Lema 5.4. *Seja F um corpo finito contendo um subcorpo K com q elementos. Então , F tem q^m elementos onde $m = [F : K]$*

Demonstração. Temos que F é um espaço vetorial sobre K, então a dimensão do espaço vetorial de F sobre K é finita, pois F é finito. Se $m = [F : K]$, então F possui uma base sobre K com m elementos, digamos que sejam $b_1, b_2, \ldots, b_m$. Portanto, todo elemento de F se escreve de modo único da forma $a_1b_1 + a_2b_2 + \ldots a_mb_m$ onde $a_1, a_2 \ldots a_m \in K$, mas como K possui q elementos então F possui exatamente q^m elementos. □

Teorema 5.9. *Seja F um corpo finito. Então F possui p^n elementos onde p é a característica de F e n é a dimensão de F sobre seu corpo primo.*

Demonstração. Como F é finito então a característica de F é p um número primo. Portanto o subcorpo primo K de F é isomorfo a $\mathbb{F}_p$ e, assim, possui p elementos. Então , pelo lema 5.4, F tem p^n elementos e $n = [F : K]$. □

Lema 5.5. *Se F é um corpo finito com q elementos, então $a^q = a$ para todo $a \in F$*

Demonstração. Se $a = 0$ segue a igualdade. Por outro lado, temos que os elementos não nulos de F formam um grupo de ordem $q-1$ com a operação produto. Então, $a^{q-1} = 1$, para todo $a \in F$, com $a \neq 0$. Logo $a^{q-1} \cdot a = 1 \cdot a$, ou seja, $a^q = a$ para todo $a \in F^*$ □

Proposição 5.2. *Se F é um corpo finito com q elementos e K é um subcorpo de F, então o polinômio $x^q - x \in K[x]$ é fatorado em $F[x]$ na forma $x^q - x = \prod_{a \in F} (x - a)$ e F é um corpo de decomposição de $x^q - x$ sobre K.*

Demonstração. O polinômio $x^q - x$ de grau q possui no máximo q raízes em F. Ainda pelo lema 5.5 temos que todos os elementos de F são raízes de $x^q - x$. Logo $x^q - x$ se fatora em F e não pode fatorar-se em nenhum outro corpo menor que F. Portanto F é um corpo de decomposição para o polinômio $x^q - x$ sobre K. □

Teorema 5.10 (Existência e unicidade de corpos finitos)**.** *Para todo primo p e todo inteiro positivo n existe um corpo finito com p^n elementos. Além disso, corpos finitos com $q = p^n$ elementos são isomorfos a corpo de decomposição do polinômio $x^q - x$ sobre $\mathbb{F}_p$*

Demonstração. Para $q = p^n$ consideremos $x^q - x \in \mathbb{F}_p[x]$. Seja F o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Esse polinômio possui q raízes distintas em F, já que sua derivada é $qx^{q-1} - 1 = -1$ em $\mathbb{F}_p[x]$. Seja $S = \{a \in F \ : \ a^q - a = 0\}$ então S é um subcorpo de F, pois:

- S contém os elementos 0 e 1.
- $a, b \in S$ implica que $(a-b)^q = a^q - b^q = a - b \in S$

$*$ Dados $a, b \in S$ com $b \neq 0$ temos $(ab^{-1})^q = a^q b^{-q} = ab^{-1} \in S$

Por outro lado $x^q - x$ deve decompor-se em S já que S contém todas as suas raízes. Portanto $F = S$ e, como S contém q elementos, F é um corpo com q elementos.

$(Unicidade)$ A proposição 5.2 mostra que dois corpos de ordem p^n são corpos de decomposição de $x^{p^n} - x$ sobre $\mathbb{F}_p$, portanto o resultado segue do teorema da extensão do isomorfismo (Ver (MORANDI, 1996)), teorema 3.20) □

Teorema 5.11 (Critério de subcorpo)**.** *Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos. Então, todo subcorpo de $\mathbb{F}_q$ tem ordem p^m, onde m é um inteiro positivo tal que m divide n. Por outro lado, se m divide n, então há um único subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração. Seja F um subcorpo de $\mathbb{F}_q$. Vamos assumir que F tem p^m elementos. Então pelo lema 5.4, temos $q = p^n = (p^m)^k = p^{mk}$ onde $k = [\mathbb{F}_q : F]$. Logo $n = mk$ e, portanto m divide n. Por outro lado suponha que m divide n para algum $m > 0$. Então $p^m - 1$ divide $p^n - 1$. Consequentemente, $x^{p^m} - 1$ divide $x^{p^n} - 1$. Portanto $x^{p^m} - x$ divide $x^{p^n} - x$ e toda raiz de $x^{p^m} - x$ também é raiz de $x^{p^n} - x = x^q - x$. Logo $\mathbb{F}_q$ deve conter como subcorpo o corpo de decomposição de $x^{p^m} - x$ sobre $\mathbb{F}_q$, e pelo teorema 5.10 , tal corpo de decomposição deve ter ordem p^m. Agora suponhamos que existem dois subcorpos F e K de ordem p^m em $\mathbb{F}_q$. Então existe pelo menos um elemento de K que é diferente de todos os elementos de F e, como F possui todas as raízes de $x^{p^m} - x$ esses subcorpos juntos possuem mais de p^m raízes de $x^{p^m} - x$ em $\mathbb{F}_q$ que é um absurdo. □

Teorema 5.12. *O grupo multiplicativo $\mathbb{F}_q^*$ formado por todos os elementos não nulos de $\mathbb{F}_q$ é cíclico.*

Demonstração. Podemos assumir $q \geq 3$. Sejam $h = q - 1$ a ordem do grupo $\mathbb{F}_q^*$ e $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ a decomposição de h em fatores primos. Para todo i com $1 \leq i \leq m$, o polinômio $x^{h/p_i} - 1$ tem no máximo h/p_i raízes em $\mathbb{F}_q$. Como $h/p_i < h$ segue que existem elementos não nulos em $\mathbb{F}_q$ que não são raízes desse polinômio. Seja a_i um tal elemento e $b_i = a_i^{h/p_i^{r_i}}$. Assim $b_i^{p_i^{r_i}} = 1$ e , então, a ordem de b_i é um divisor de $p_i^{r_i}$. Logo a ordem de b_i é da forma $p_i^{s_i}$ com $0 \leq s_i \leq r_i$. por outro lado temos que $(a_i^{h/p_i^{r_i}})^{p_i^{r_i}} = a^h = 1$ e portanto,

$$b_i^{p_i^{r_i - 1}} = (a_i^{h/p_i^{r_i}})^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1$$

e então a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b = b_1 b_2 \cdots b_m$ tem ordem h. Suponhamos que a ordem de h seja um divisor próprio de h, e portanto um divisor de pelo

menos um dos m inteiros h_i, $1 \leq i \leq m$. Digamos que este inteiro seja h_1. Então temos que

$$1 = b^{h_1} = b_1^{h_1} b_2^{h_1} \cdots b_m^{h_1}$$

Agora se $2 \leq i \leq m$, então $p_i^{r_i}$ divide h_1 e , assim $b_i^{h_1} = 1$. Portanto $b_1^{h_1} = 1$. Isto implica que a ordem b_1 deve dividir h_1, que é impossível, pois a ordem de b_1 é $p_1^{r_1}$. Portanto $\mathbb{F}_q^*$ é um grupo cíclico com gerador b. □

Definição 5.11. *Um elemento $\alpha \in \mathbb{F}_q$ é dito um elemento primitivo, se α é um gerador do grupo $\mathbb{F}_q^*$, ou seja $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$.*

Teorema 5.13. *Seja $\mathbb{F}_r$ uma extensão e $\mathbb{F}_q$. Então, $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$ e todo elemento primitivo de $\mathbb{F}_r$ é um gerador e $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Demonstração. Seja α um elemento primitivo de $\mathbb{F}_r$. Temos que $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_r$. Por outro lado $\mathbb{F}_q(\alpha)$ contém 0 e todas as potências de α e, portanto todos os elementos de $\mathbb{F}_r$. Logo $\mathbb{F}_q(\alpha) = \mathbb{F}_r$. □

Corolário 5.2. *Para todo corpo finito $\mathbb{F}_q$ e todo inteiro positivo n existe um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n.*

Demonstração. Seja $\mathbb{F}_r$ uma extensão de $\mathbb{F}_q$ de ordem q^n. de modo que $[\mathbb{F}_r : \mathbb{F}_q] = n$, pelo teorema 5.13, $\mathbb{F}_r = \mathbb{F}_q(\alpha)$ para algum $\alpha \in \mathbb{F}_q$. Então o polinômio minimal de α sobre $\mathbb{F}_q$ é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n. □

Lema 5.6. *Seja $f(x) \in \mathbb{F}_q[x]$um polinômio irredutível sobre $\mathbb{F}_q$ e α uma raiz de $f(x)$ em uma extensão de $\mathbb{F}_q$. Então para um polinômio $h(x) \in \mathbb{F}_q[x]$ temos que $h(\alpha) = 0$ se, e somente se $f(x)$ divide $h(x)$*

Demonstração. Seja a o coeficiente líder de $f(x)$ e $g(x) = a^{-1} f(x)$. Então $g(x)$ é um polinômio mônico irredutível em $\mathbb{F}_q[x]$ com $g(\alpha) = 0$ e, portanto é o polinômio minimal de α sobre $\mathbb{F}_q$. Como $h(\alpha) = 0$, pela definição de polinômio minimal vem que $g(x)$ divide $h(x)$ e portanto $f(x)$ divide $h(x)$. □

Lema 5.7. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então $f(x)$ divide $x^{q^n} - x$ se e somente se m divide n*

Demonstração. Suponhamos que $f(x)$ divide $x^{q^n} - x$ e seja α uma raiz de $f(x)$ no corpo de decomposição de $f(x)$ sobre $\mathbb{F}_q$. Então $\alpha^{q^n} = \alpha$ de modo que $\alpha \in \mathbb{F}_{q^n}$. Logo $\mathbb{F}_q(\alpha)$ é subcorpo

de $\mathbb{F}_{q^n}$. Mas como $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=m$ e pelo lema 5.4 $[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$, então pelo teorema 5.4 segue que m divide n.

Por outro lado, se m divide n então pelo teorema 5.11 temos que $\mathbb{F}_{q^n}$ tem $\mathbb{F}_{q^m}$ como subcorpo. Se α é raiz de $f(x)$ no corpo de decomposição de $f(x)$ sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=m$ e então $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^m}$. Assim $\alpha\in\mathbb{F}_{q^m}$ e , então $\alpha^{q^n}=\alpha$, portanto α é raiz de $x^{q^n}-x\in\mathbb{F}_q[x]$ e pelo lema 5.6 $f(x)$ divide $x^{q^n}-x$. □

Teorema 5.14. *Se $f(x)$ é um polinômio irredutível de $\mathbb{F}_q[x]$ de grau m, então $f(x)$ possui uma raiz α em $\mathbb{F}_{q^m}$. Além disso, todas as raízes de $f(x)$ são simples e são os m elementos distintos $\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{m-1}}$.*

Demonstração. Seja α um raiz de $f(x)$ no corpo de decomposição de $f(x)$ sobre o $\mathbb{F}_q$. então $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=m$ e $\mathbb{F}_q(\alpha)=\mathbb{F}_{q^m}$. Em particular $\alpha\in\mathbb{F}_{q^m}$. Agora mostremos que se β é uma raiz de $f(x)$ então β^q também é raiz de $f(x)$. Escrevendo $f(x)=a_mx^m+a_{m-1}x^{m-1}+\ldots+a_1x+a_0$ com $a_i\in\mathbb{F}_q$, para todo $i=0,1,2,\ldots,m$, então usando o lema 5.3 e o lema 5.5 temos que

$$f(\beta^q)=a_m(\beta^q)^m+\ldots+a_1\beta^q+a_0$$

$$=a_m^q(\beta^q)^m+\ldots+a_1^q\beta^q+a_0^q$$

$$=(a_m\beta^m+\ldots+a_1\beta+a_0)^q$$

$$=f(\beta)^q=0$$

Portanto os elementos $\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{m-1}}$ são raízes de $f(x)$. Resta mostrar que esses elementos são distintos. Suponhamos o contrário: que $\alpha^{q^j}=\alpha^{q^k}$ para alguns j,k inteiros com $0\leq j<k\leq m-1$. Ao elevar ambos os lados dessa igualdade à potência q^{m-k}, temos

$$(\alpha^{q^j})^{q^{m-k}}=(\alpha^{q^k})^{q^{m-k}}\Longrightarrow\alpha^{q^{m-k+j}}=\alpha^{q^m}=\alpha$$

Assim segue do lema 5.6 que $f(x)$ divide $x^{q^{m-k+j}}-x$. Mas pelo lema 5.7 , isto só é possível se m divide $m-k+j$. Como $0\leq m-k+j<m$ chegamos a uma contradição, Portanto $\alpha,\alpha^q,\alpha^{q^2},\ldots,\alpha^{q^{m-1}}$. são elementos distintos.

□

6 DOIS PROBLEMAS OLÍMPICOS

6.1 Problema 1

O problema a seguir foi um problema proposto na OBM 2017 nível 3.

Seja a inteiro positivo e p um divisor primo de a^3-3a+1 *com* $p \neq 3$. *Prove que p é da forma* $9k+1$ *ou* $9k-1$, *sendo k inteiro.*

6.1.1 Solução

Se $p \mid a^3-3a+1$ então $a^3-3a+1=0$ em $\mathbb{F}_p$. Seja $a \in \mathbb{F}_p$ tal que $x^2-ax+1=0$. Como $a=z+\frac{1}{z}$ onde z e $\frac{1}{z}$ são as raízes de $p(x)=x^2-a^{-1}x+1$.

temos que:

$$a^3-3a+1=\left(z+\frac{1}{z}\right)^3-3\cdot\left(z+\frac{1}{z}\right)+1$$

$$=z^3+3\cdot z^2\cdot\frac{1}{z}+3\cdot z\cdot\left(\frac{1}{z}\right)^2+\left(\frac{1}{z}\right)^3-3\cdot z-3\cdot\frac{1}{z}+1$$

$$=z^3+\frac{1}{z^3}+1$$

$$=\frac{z^6+1+z^3}{z^3}\cdot\frac{(z^3-1)}{(z^3-1)}$$

$$=\frac{z^9+z^3+z^6-z^6-1-z^3}{z^3\cdot(z^3-1)}$$

$$=\frac{z^9-1}{z^3\cdot(z^3-1)}=0 \ \ em\ \mathbb{F}_p$$

Isso implica que $z^9-1=0 \Longrightarrow z^9=1$. Pela proposição 2.10 temos que $o(z)$ divide 9 ,ou seja,$o(z) \in \{1,3,9\}$. Note que se $o(z)=1$ ou $o(z)=3$ temos que $a^3-3a+1=z^3+\frac{1}{z^3}+1=3=0$, portanto $p=3$. Absurdo, pois $p \neq 3$. Assim a $o(z)=9$. Faremos a analise de dois casos:

Se $z \in \mathbb{F}_p$ e Como $z \neq 0$, $z \in \mathbb{F}_p^*$ que é um grupo multiplicativo com ordem $p-1$, então pelo corolário 2.2 temos que $9 \mid p-1$ ou seja $p=9k+1$.

Suponha agora $z \notin \mathbb{F}_p$.

Como z e $\frac{1}{z}$ são raízes do polinômio $p(x) = x^2 - ax + 1$, ou seja

$$p(x) = (x-z)(x-\frac{1}{z})$$

Mas como $z \notin \mathbb{F}_p$, pela proposição 4.6 temos que $p(x)$ é irredutível em $\mathbb{F}_p[x]$ e assim pelo teorema 5.14 $p(x)$ possui uma raiz z em $\mathbb{F}_{p^2}$ e ainda pelo teorema 5.14 as raízes de $p(x)$ são simples e são os elementos distintos z, z^p, daí temos que $\frac{1}{z} = z^p$ e portanto também temos $z^{p+1} = 1$ e consequentemente pela proposição 2.10 temos que $9 \mid p+1$ e portanto $p = 9k-1$

6.2 Problema 2

O problema a seguir foi proposto na *XIII* Olimpíada Ibero-americana de matemática universitária em novembro de 2010, problema 6.

Demonstrar que, para cada número inteiro $a > 1$, os divisores primos do número $5a^4 - 5a^2 + 1$ são da forma $20k \pm 1, k \in \mathbb{Z}$.

6.2.1 Solução

Se $p \mid 5a^4 - 5a^2 + 1$ então $5a^4 - 5a^2 + 1 = 0$ em $\mathbb{F}_p$. Seja $a \in \mathbb{F}_p$ e note que se $5a^4 - 5a^2 + 1 = 0$ então $5 - 5(a^{-1})^2 + (a^{-1})^4 = 0$. De fato, pois como $a \in \mathbb{F}_p \Longrightarrow a^{-1} \in \mathbb{F}_p$ e multiplicando ambos os lados da expressão $5a^4 - 5a^2 + 1 = 0$ por $(a^{-1})^4 = a^{-4}$ temos

$$a^{-4}(5a^4 - 5a^2 + 1) = a^{-4} \cdot 0$$

$$5 - 5a^{-2} + a^{-4} = 0$$

$$5 - 5(a^{-1})^2 + (a^{-1})^4 = 0$$

Seja $a^{-1} \in \mathbb{F}_p$ tal que $x^2 - a^{-1}x + 1 = 0$. Como $a^{-1} = z + \frac{1}{z}$ onde z e $\frac{1}{z}$ são as raízes de $p(x) = x^2 - a^{-1}x + 1$.

Temos que:

$$5 - 5(a^{-1})^2 + (a^{-1})^4 = 5 - 5\left(z + \frac{1}{z}\right)^2 + \left(z + \frac{1}{z}\right)^4$$

$$= 5 - 5\left(z^2 + 2 + \frac{1}{z^2}\right) + \left(z^4 + \frac{1}{z^4} + 6 + 4z^2 + \frac{4}{z^2}\right)$$

$$= 5 - 5z^2 - 10 - \frac{5}{z^2} + z^4 + \frac{1}{z^4} + 6 + 4z^2 + \frac{4}{z^2}$$

$$= z^4 - z^2 + 1 - \frac{1}{z^2} + \frac{1}{z^4}$$

$$= \frac{z^8 - z^6 + z^4 - z^2 + 1}{z^4} \cdot \frac{z^2 + 1}{z^2 + 1}$$

$$= \frac{z^{10} - z^8 + z^6 - z^4 + z^2 + z^8 - z^6 + z^4 - z^2 + 1}{z^4(z^2 + 1)}$$

$$= \frac{z^{10} + 1}{z^4(z^2 + 1)} = 0 \ \ em \ \mathbb{F}_p.$$

Assim temos que $z^{10} + 1 = 0 \Longrightarrow z^{10} = -1 \Longrightarrow z^{20} = 1$. Pela proposição 2.10 a $o(z)$ divide 20, ou seja, $o(z) \in \{1, 2, 4, 5, 10, 20\}$

Se $o(z) = 1$ então $5 - 5(a^{-1})^2 + (a^{-1})^4 = \frac{z^8 - z^6 + z^4 - z^2 + 1}{z^4} = 1 - 1 + 1 - 1 + 1 = 1 = 0 \Longrightarrow p = 1$. *Absurdo*.

Se $o(z) = 2$ então $\frac{z^8 - z^6 + z^4 - z^2 + 1}{z^4} = 1 - 1 + 1 - 1 + 1 = 1 = 0 \Longrightarrow p = 1$. *Absurdo*.

Se $o(z) = 4$ então $z^{10} = z^6 = z^2 = -1$ e portanto $\frac{z^8 - z^6 + z^4 - z^2 + 1}{z^4} = 1 + 1 + 1 + 1 + 1 = 5 = 0$, ou seja, $p = 5$. Absurdo, pois se $p = 5$ vem que $5 \mid 5a^4 - 5a^2 + 1$ e consequentemente $5 \mid 1$ que é um absurdo.

Se $o(z) = 5$ então $z^{10} + 1 = 1 + 1 = 2 = 0$ e portanto $p = 2$. Absurdo, pois se $p = 2 \Longrightarrow 2 \mid 5a^4 - 5a^2 + 1$, o que não ocorre pois $5a^4 - 5a^2 + 1$ é sempre impar. De fato,

$$5a^4 - 5a^2 + 1 = \underbrace{5a^2(a^2 - 1)}_{sempre\ par} + 1 \ \ (sempre\ impar)$$

Assim, temos que $o(z) = 20$

Faremos a analise de dois casos.

Se $z \in \mathbb{F}_p$, então $z \in \mathbb{F}_p^*$, pois $z \neq 0$, como $\mathbb{F}_p^*$ é um grupo multiplicativo de ordem $p - 1$, então pelo corolário 2.2 temos que $20 \mid p - 1$ e portanto $p = 20k + 1$, para algum $k \in \mathbb{Z}$.

Suponha agora $z \notin \mathbb{F}_p$.

Como z e $\frac{1}{z}$ são raízes do polinômio $p(x) = x^2 - a^{-1}x + 1$, ou seja

$$p(x) = (x - z)(x - \frac{1}{z})$$

Mas como $z \notin \mathbb{F}_p$, pela proposição 4.6 temos que $p(x)$ é irredutível em $\mathbb{F}_p[x]$ e assim pelo teorema 5.14 $p(x)$ possui uma raiz z em $\mathbb{F}_{p^2}$ e ainda pelo teorema 5.14 as raízes de $p(x)$ são simples e são os elementos distintos z, z^p, daí temos que $\frac{1}{z} = z^p$ e portanto também temos $z^{p+1} = 1$ e consequentemente pela proposição 2.10 temos que $20 \mid p+1$ e portanto $p = 20k-1$.

7 CONSIDERAÇÕES FINAIS

Estudamos aqui um pouco sobre algumas estruturas algébricas como grupo, anéis e corpos. Conhecemos a construção de corpos finitos através de polinômios irredutíveis e vimos que todo corpo finito é completamente determinado pelo seu número de elementos, além disso podemos verificar a aplicação de um corpo finito na solução de dois problemas olímpicos que foram propostos em olimpíadas de matemática em nível médio (OBM 2017) e nível universitário (XIII olimpíada Ibero-americana de matemática universitária).

Portanto, apresentamos aqui um material mais amplo e com noções que possam auxiliar estudantes olímpicos e estudantes de graduação de matemática em seus estudos em álgebra abstrata.

REFERÊNCIAS

CONRAD, Keith. **Finite fields**. 2013. Disponível em : https://kconrad.math.uconn.edu/blurbs/galoistheory/finitefields.pdf. Acesso em: 01 de Agosto de 2019

GONÇALVES, A. **Introdução á álgebra** . 5. ed. Rio de Janeiro : IMPA, 2007.

HESRTEIN, I.N. **Topics in algebra**. 2nd ed. New York : John Wiley, 1975.

HUCZYNSKA, S.; NEUNHOFFER, M. **Finite fields**. 2012. Disponível em: http://www.math.rwth-aachen.de/∼ Max.Neunhoeffer/Teaching/ff/ffchap3.pdf. Acesso em: 18 de julho de 2019

JANESCH, O.R**. Algebra II** . Florianópolis : UFSC/EAD/CED/CFM, 2008. v. 1.

JANESCH, O.R; TANEJA, I.J. **Algebra I**. 2.ed. rev. Florianópolis : UFSC/EAD/CED/CFM, 2011.

MARTINEZ, Fabio E. Brochero et al. **Introdução á teoria dos números**: funções aritméticas. Rio de Janeiro: [s..ed.] 2011.

MORANDI, Patrick. **Field and galois theory**. New York: Springer-verlag, 1996.

SILVA, Ednailton Santos**. Polinômios de permutação sobre corpos finitos**. 2018. 60 f. Dissertação (Mestrado em Matemática), Instituto de Ciências Exatas, Universidade Federal de Juiz de Fora, Juiz de Fora, Minas Gerais, 2018.

STEWART, I. **Galois theory**. London : Chapman and Hall, 1975.