Universidade Federal da Grande Dourados

Faculdade de Ciências Exatas e Tecnologia

Mestrado Profissional em Matemática em Rede Nacional

Obtenção de Corpos de Números e Corpos Finitos utilizando o Python

Geovane Morato Pinto

Orientadora: Profa. Dra. Ana Cláudia Machado Mendonça Chagas

Dourados

Fevereiro - 2021

Geovane Morato Pinto

Obtenção de Corpos de Números e Corpos Finitos utilizando o Python

Dissertação apresentada ao final do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal da Grande Dourados - UFGD como exigência parcial para obtenção do título de Mestre em Matemática.

Dourados-MS

Fevereiro - 2021

Dados Internacionais de Catalogação na Publicação (CIP).

P659o Pinto, Geovane Morato
Obtenção de Corpos de Números e Corpos Finitos utilizando o Python [recurso eletrônico] / Geovane Morato Pinto. -- 2021.
Arquivo em formato pdf.

Orientadora: Ana Cláudia Machado Mendonça Chagas.
Dissertação (Mestrado em Matemática)-Universidade Federal da Grande Dourados, 2021.
Disponível no Repositório Institucional da UFGD em:
https://portal.ufgd.edu.br/setor/biblioteca/repositorio

1. Corpos de números. 2. Corpos finitos. 3. Polinômios irredutíveis. 4. Python. I. Chagas, Ana Cláudia Machado Mendonça. II. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

MINISTÉRIO DA EDUCAÇÃO
FUNDAÇÃO UNIVERSIDADE FEDERAL DA GRANDE DOURADOS
FACULDADE DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Termo de Aprovação

Após a apresentação, arguição e apreciação pela banca examinadora, foi emitido o parecer APROVADO, para a dissertação intitulada: **"Obtenção de Corpos de Números e Corpos Finitos utilizado o Python"**, de autoria de **Geovane Morato Pinto**, apresentada ao Programa de Mestrado Profissional em Matemática da Universidade Federal da Grande Dourados.

Profª. Drª. Ana Claudia Machado Mendonça Chagas (Orientadora-UFGD)
Presidente da Banca Examinadora

Profª. Drª. Irene Magalhães Craveiro
Membro Examinador (UFGD)

Prof. Dr. Oyran Silva Rayzaro
Membro Examinador Externo (UEMS)

Dourados/MS, 08 de março de 2021

Agradecimentos

Agradeço a minha esposa, minha família e a todos que de alguma forma me apoiaram nessa caminhada.

Agradeço a todos colegas de pós-graduação, aos professores de pós-graduação e em especial a banca examinadora dessa trabalho: Minha orientadora Profª. Drª. Ana Cláudia, a Profª Drª. Irene sempre muito prestativa com os alunos de pós-graduação e ao Profº Dr. Oyran pelo aceite em participar da avaliação desse trabalho.

"O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior Brasil (CAPES) - Código de Financiamento 001"

Resumo

Este trabalho apresenta um pouco da teoria de corpos de números e corpos finitos. O principal objetivo é mostrar a importância de polinômios irredutíveis para construção de extensões finitas dos racionais e de $\mathbb{Z}_p$, com p primo. Apresentaremos um algoritmo, utilizando o Python, para testar a irredutibilidade de polinômios de grau 2 e 3 sobre $\mathbb{Z}_3$, dando uma caracterização de corpos finitos com 9 e 27 elementos, apresentaremos ainda o algorítimo de Rabin possibilitando assim caracterizar extensões de $\mathbb{Z}_p$ com p^n elementos.

Palavras-chaves: Corpos de números, corpos finitos, polinômios irredutíveis, python.

Abstract

This work presents a little of the theory of number fields and finite fields. The main objective is to show the importance of polynomials irreducible for building finite extensions of rationals and $\mathbb{Z}_p$, with p prime. We will present an algorithm, using Python, to test the irreducibility of degree 2 and 3 polynomials over $\mathbb{Z}_3$, giving a characterization of finite fields with 9 and 27 elements, we will also present Rabin algorithm thus making it possible to characterize extensions of $\mathbb{Z}_p$ with p^n.

Key-words: Number fields, finite fields, polynomials irreducible, python

Sumário

Introdução **11**

1 Anéis e Corpos **12**

1.1 Anéis 12

1.1.1 Domínios de Integridade 15

1.1.2 Homomorfismo de Anéis 16

1.1.3 Característica de um Domínio de Integridade 19

1.1.4 Ideais 20

1.2 Corpos 23

2 Polinômios **26**

2.1 Anéis de Polinômios 26

2.1.1 Divisão de Polinômios 29

2.1.2 Raízes de Polinômios 30

2.1.3 Ideais em $\mathbb{K}[x]$ 32

2.2 Critérios de Irredutibilidade de Polinômios 33

3 Extensões de Corpos **36**

3.1 Extensões finitas 38

3.1.1 Corpo de Decomposição de polinômios 40

3.2 Extensões Finitas de $\mathbb{Z}_p$ 40

3.3 Extensões Finitas dos Racionais 44

4 Polinômios irredutíveis utilizando o Python **45**

Lista de Figuras

4.1 Produto de Polinômios. 47
4.2 Exemplo de produto. 48
4.3 Soma de polinômios. 49
4.4 Subtração de polinômios. 50
4.5 Polinômio nulo. 51
4.6 Lista de polinômios de grau ≤ 2. 52
4.7 Lista de polinômios de grau ≤ 3. 53
4.8 Lista dos mônicos de grau 2 e 3. 54
4.9 Mônicos de grau 2. 55
4.10 Mônicos de grau 3. 55
4.11 Irredutíveis de grau 2. 56
4.12 Exemplo de irredutíveis de grau 2 sobre $\mathbb{Z}_3$. 57
4.13 Irredutíveis de grau 3. 57
4.14 Exemplo de irredutíveis de grau 2 sobre $\mathbb{Z}_3$. 58
4.15 Programa que geram G_1, G_2 e G_3. 59
4.16 Console do programa que geram G_1, G_2 e G_3. 60
4.17 Inverso em Z_p. 61
4.18 Divisão de polinômios. 62
4.19 Exemplo de divisão de polinômios. 63
4.20 MDC de polinômios. 64
4.21 Exemplo de MDC de polinômios. 65
4.22 Polinômios do tipo $x^{p^n} - x$ 65
4.23 Algorítimo de Rabin. 66

4.24 Exemplo aplicação do algorítimo de Rabin em $\mathbb{Z}_3$. 67
4.25 Exemplo aplicação do algorítimo de Rabin em $\mathbb{Z}_5$. 67

Introdução

A teoria de corpos finitos e corpos de números são de fundamental importância para o desenvolvimento da teoria dos códigos, como vemos em [1], [7] e [9].

Os primeiros códigos corretores de erros, ou seja, códigos que além de detectar os erros poderiam corrigi-los, surgiram com Richard W. Hamming, Claude E. Shannon e Marcel J. E. Golay, entre 1947 e 1950. O CPF, por exemplo, é um código corretor de erro. A estrutura linear e simétrica de códigos obtidos utilizando corpos finitos e corpos de números é de fundamental importância na tarefa de codificação, decodificação e correção de erros.

Para o estudo da teoria de corpos finitos e corpos de números, apresentamos conceitos e propriedades de anéis, domínios, corpos, anéis de polinômios e polinômios irredutíveis. Testar a irredutibilidade de um polinômios nem sempre é uma tarefa fácil. Sendo assim, nesse trabalho usamos como ferramenta a linguagem de programação python. Em síntese, o trabalho traz a construção de um algoritmo em python para testar a irredutibilidade de alguns polinômios, em casos específicos.

O trabalho está dividido em quatro capítulos. O primeiro capítulo traz os conceitos iniciais de anéis, domínios e corpos. O segundo capítulo define anéis de polinômios sobre um corpo, e descreve alguns critérios de irredutibilidade de polinômios. O terceiro capítulo trata extensões finitas dos racionais e de $\mathbb{Z}_p$. No quarto capítulo, traremos um algoritmo simples, utilizando a linguagem de programação python, capaz de verificar a irredutibilidade de polinômios.

A partir desse trabalho, podemos ter uma ideia de como relacionar a teoria matemática com a programação. De forma simples e compreensiva, faremos do raciocínio matemático alguns algoritmos, que no futuro podem ser melhorados.

Capítulo 1

Anéis e Corpos

Neste capítulo vamos estudar as definições e propriedades de um anel, subanel, domínio de integridade e corpo. Apresentaremos também os conceitos de característica de um domínio de integridade, homomorfismo de anéis e ideais. Esses resultados serão de fundamental importância no desenvolvimento do trabalho. As referências desse capítulo podem ser encontradas em : [3] e [10].

1.1 Anéis

Seja A um conjunto não vazio munido de duas operações: adição (+) e multiplicação ($\cdot$). Vamos denotar este conjunto por$(A, +, \cdot)$.

Definição 1.1. *Dizemos que $(A, +, \cdot)$ é um anel se satisfaz:*

i) $a + b = b + a$ *(Comutatividade da Adição).*

ii) $(a + b) + c = a + (b + c)$ *(Associatividade da adição).*

iii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(Associatividade da multiplicação).*

iv) $\exists\ 0_A \in A$ *tal que* $0_A + a = a$, $\forall a \in A$ *(Elemento neutro da adição).*

v) $\forall a \in A$ *existe* $-a \in A$ *tal que* $a + (-a) = 0_A$ *(Elemento oposto de a).*

vi) $a \cdot (b + c) = a \cdot b + a \cdot c$ *(Distributividade).*

Definição 1.2. *Considere $(A, +, \cdot)$ um anel,*

i) Se a multiplicação é comutativa, ou seja, $a \cdot b = b \cdot a \ \forall a, b \in A$, então dizemos que $(A, +, \cdot)$ é anel comutativo.

ii) Se existe o elemento neutro da multiplicação, ou seja, $\exists 1_A \in A$ tal que $1_A \cdot a = a \cdot 1_A = a, \ \forall a \in A$, então $(A, +, \cdot)$ é chamado anel com unidade.

Exemplo 1.1. *a) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são exemplos de anéis comutativos com unidade.*

b)Seja $n\mathbb{Z} = \{n \cdot a; a \in \mathbb{Z}\}$, logo $(n\mathbb{Z}, +, \cdot)$ para $n \in \mathbb{N}, n \geq 2$ é um anel comutativo, porém sem unidade.

c)Considere $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ o conjunto das classes residuais módulo n. Temos que $(\mathbb{Z}_n, +, \cdot)$, para $n \in \mathbb{N}, n \geq 2$ é um anel comutativo com unidade.

d) Considere $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$. Temos que $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ é um anel comutativo com unidade, com as operações definidas da seguinte forma:
Sejam x e $y \in \mathbb{Z}[\sqrt{2}]$, tal que $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2}$, então

Adição.

$$\begin{aligned} + : \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}] &\longrightarrow \mathbb{Z}[\sqrt{2}] \\ (x, y) &\longmapsto x + y = (a + c) + (b + d)\sqrt{2} \end{aligned}$$

Multiplicação.

$$\begin{aligned} \cdot : \ \mathbb{Z}[\sqrt{2}] \times \mathbb{Z}[\sqrt{2}] &\longrightarrow \mathbb{Z}[\sqrt{2}] \\ (x, y) &\longmapsto x \cdot y = (ac + 2bd) + (ad + cb)\sqrt{2} \end{aligned}$$

Propriedades 1.1. *Seja $(A, +, \cdot)$ um anel. São válidas as seguintes propriedades:*

1) Unicidade do elemento neutro.

2) Unicidade do elemento simétrico.

3) Se $a_1, a_2, \cdots, a_n \in A (n \geq 2)$, então $-(a_1 + a_2 + \cdots + a_n) = -a_1 + (-a_2) + \cdots + (-a_n)$.

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

5) $\forall a, b, c \in A$, *se* $a + b = a + c$, *então* b=c *(Lei do corte da adição).*

6) O conjunto solução da equação $a + x = b$, *na variável* x, *é* $x = -a + b, \quad \forall a, b \in A.$

7) $\forall a \in A, a \cdot 0_A = 0_A = 0_A \cdot a.$

8) $\forall a, b \in A$, *tem-se que* $a(-b) = (-a)b = -(ab).$

9) $\forall a, b \in A$, *tem-se que* $ab = (-a)(-b).$

Definição 1.3. *Sejam* $(A, +, \cdot)$ *um anel e* $a, b \in A$. *Definimos a diferença entre* a *e* b *como* $a - b = a + (-b).$

Com base na multiplicação em um anel A, podemos definir o conceito de potência de um elemento de A.

Definição 1.4. *Seja* $a \in A$ *definimos a n-ésima potência de a da seguinte forma:* $a^1 = a$ *e* $a^n = a^{n-1} \cdot a$ *para* $n \geq 2.$

Utilizando a Definição 1.4 e o raciocínio indutivo é fácil provar as seguintes propriedades de potência de um elemento do anel A.

Propriedades 1.2. *Sejam* $(A, +, \cdot)$ *um anel com* $a, b, c \in A$ *e* $m, n \in \mathbb{N}^*$. *São válidas as propriedades abaixo:*

i) $a^m \cdot a^n = a^{m+n}$

ii) $(a^m)^n = a^{mn}$

Definição 1.5. *Sejam* $(A, +, \cdot)$ *um anel e* $L \subseteq A$ *não vazio. Dizemos que* L *é subanel de* A *se:*

i) L *é fechado para a adição e multiplicação.*

ii) $(L, +, \cdot)$ *é um anel (com as operações de* A *restritas a* L*).*

Notação: $L \leq A.$

Como vimos no Exemplo 1.1, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}[\sqrt{2}]$, e $n\mathbb{Z}$ são anéis. Assim, $n\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ e $\mathbb{Z}[\sqrt{2}] \leq \mathbb{R}$.

A próxima proposição facilitará a verificação de subanéis de um anel A. Note que para quaisquer subconjunto de um anel A herda as propriedades comutativas, associativas e distributiva.

Proposição 1.1. *Sejam $(A, +, \cdot)$ um anel e $L \subseteq A$ não vazio. Tem-se que $L \leq A$ se, e somente se, $a - b \in L$ e $a \cdot b \in L, \forall a, b \in L$.*

Demonstração. ($\Rightarrow$) Como $b \in L$ e $L \leq A$, seque que $-b \in L$. Como L é fechado para a adição e $a - b = a + (-b) \in L$. Obviamente, $a \cdot b \in L$.

($\Leftarrow$) Como observado antes, as condições de comutatividade da adição, associatividade da adição e multiplicação e também a distributiva são herdadas de A. Sendo assim, é suficiente verificar que L é fechado para ambas as operações, existência do elemento neutro e existência do oposto. De fato, tem-se por hipótese que $a \cdot b \in L, \forall a, b \in L$, segue que L é fechado para a multiplicação. Como $L \neq \emptyset$, existe $a \in L$, assim $a - a \in L$. Como $a - a = 0_A$, tem-se que $0_A \in L$. Temos assim, $0_A - a = -a \in L$, ou seja, existe o oposto em L. Como $a + b = a - (-b)$, se $a, b \in L$, então $a + b \in L$, ou seja, L é fechado para a adição. ■

1.1.1 Domínios de Integridade

Definição 1.6. *Seja $(A, +, \cdot)$ um anel comutativo com unidade. Dizemos que A é um domínio de integridade, quando A não possui divisores de zero, ou seja, quando $a \cdot b = 0$, implicar que $a = 0$ ou $b = 0$, com $a, b \in A$.*

Exemplo 1.2. *a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ não tem divisores de zero. Logo, são domínios de integridade.*

b) $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ tem divisores de zero, pois $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$.

Exemplo 1.3. *$\mathbb{Z}[\sqrt{2}]$ é um domínio de integridade.*

Justificativa: Primeiramente consideramos que $\mathbb{Z}$ não tem divisores de zero. Sejam $x = a + b\sqrt{2}$ e $y = c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Assim, $xy = 0$ se, e só se,

$$\begin{aligned}
(ac + 2bd) + (ad + bc)\sqrt{2} = 0 + 0[\sqrt{2}] &\Leftrightarrow ac + 2bd = 0 \quad e \quad ad + bc = 0 \\
&\Leftrightarrow ac = -2bd \quad e \quad ad = -bc \\
&\Leftrightarrow adc = -2bd^2 \quad e \quad ad = -bc \\
&\Leftrightarrow -bc^2 = -2bd^2 \\
&\Leftrightarrow b(c^2 - 2d^2) = 0 \\
&\Leftrightarrow b = 0 \quad ou \quad c^2 = 2d^2.
\end{aligned}$$

Temos que $c^2 = 2d^2$ se, e somente se, $c = d = 0$. De fato, vejamos que se $c^2 = 2d^2$, teremos que c^2 é par, e portanto, c também é par, então a decomposição de c^2 possui um número par de fatores iguais a 2 em sua decomposição em fatores primos. Segue ainda que se d^2 também é par, contendo um número par de fatores iguais a 2 em sua decomposição em fatores primos, teremos $2d^2$ com um número ímpar de fatores 2 em sua decomposição. O que não pode ocorrer pois, $c^2 = 2d^2$. E portanto, esta igualdade só ocorre quando $c = d = 0$. Sendo assim temos que $b = 0 \quad ou \quad c = d = 0$. Se $c = d = 0$ está demonstrado, caso contrário teremos que $ad = -bc$ com $b = 0$, isso se, e só se, $a = 0$. E portanto, concluímos que $a = b = 0$ ou $c = d = 0$.

Proposição 1.2. *Seja $m \in \mathbb{N}^*$ tem-se que $\mathbb{Z}_m$ é um domínio de integridade se, e só se, m é primo.*

Demonstração. ($\Rightarrow$) Suponha m composto, ou seja, existe $n, l \in \mathbb{Z}$ tal que $nl = m$, com $1 < n, l < m$. Temos que, $\overline{n} \cdot \overline{l} = \overline{nl} = \overline{m} = \overline{0}$ em $\mathbb{Z}_m$. Como $\mathbb{Z}_m$ é domínio, segue que $\overline{n} = \overline{0}$ ou $\overline{l} = \overline{0}$, absurdo pois $1 < n, l < m$. Portanto, m é primo.
($\Leftarrow$) Suponhamos que $\overline{n} \cdot \overline{l} = \overline{0}$ em $\mathbb{Z}_m$ e m primo, tem-se que $m \mid (n \cdot l)$ se, e somente se, $m \mid l$ ou $m \mid l$. Logo, temos que $\overline{n} = \overline{0}$ ou $\overline{l} = \overline{0}$. ■

1.1.2 Homomorfismo de Anéis

Vamos considerar nessa seção $(A, +, \cdot)$ e $(B, +, \cdot)$ anéis.

Definição 1.7. *Uma aplicação $\varphi : A \to B$, é um homomorfismo de anéis se satisfaz:*

i) $\varphi(a + b) = \varphi(a) + \varphi(b)$

ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,

Para todo $a, b \in A$.

Exemplo 1.4. *a)A aplicação identidade*

$$id : A \longrightarrow A$$
$$a \longmapsto a$$

é um homomorfismo de anéis.

b) Considere o produto cartesiano diretoA $\times B = \{(a, b), a \in A \text{ e } b \in B\}$. *Temos que as projeções*

$$\pi_1 : A \times B \longrightarrow A$$
$$(a, b) \mapsto a$$

e

$$\pi_2 : A \times B \longrightarrow B$$
$$(a, b) \longmapsto b$$

são homomorfismo de anéis.

c) Seja $m \in \mathbb{Z}$ *positivo, tem-se que*

$$f : \mathbb{Z} \to \mathbb{Z}_m$$
$$a \mapsto \overline{a}$$

é homomorfismo de anéis.

Definição 1.8. *Seja* $f : A \longrightarrow B$ *um homomorfismo de anéis, chamaremos o subconjunto de* A, $\{a \in A; f(a) = 0\}$ *de núcleo de* f. *Notação:* $N(f)$ *ou* $ker(f)$.

Vejamos que, no Exemplo 1.4, $ker(f) = \{a \in \mathbb{Z}; f(a) = \overline{a} = \overline{0}\} = a\mathbb{Z}$. Nas funções $\pi_1 : A \times B \to A$ tal que, $\pi_1((a,b)) = a$ e $\pi_2 : A \times B \to A$ tal que, $\pi_2((a,b)) = b$ temos que, $ker(\pi_1) = \{0_A\} \times B$ e $ker(\pi_2) = A \times \{0_B\}$.

Para simplificar a escrita daqui para frente, vamos chamar um homomorfismo $f : A \longrightarrow B$ de:

i) monomorfismo, se f é injetor.

ii) epimorfismo, se f é sobrejetor.

iii) endomorfismo, se $A = B$.

iv) automorfismo, se f é endomorfismo bijetor.

v) isomorfismo, se f é homomorfismo bijetor. Neste caso, usaremos o símbolo $\simeq$, para dizer que A é isomorfo a B.

Em seguida apresentaremos alguns resultados importantes de homomorfismo de anéis, para isto definiremos os inversíveis de um anel A, como sendo todo elemento de A que possui inverso multiplicativo em A e o conjunto dos invencíveis sera denotado por $U(A)$, isto é $U(A) = \{a \in A; ab = 1, b \in A\}$.

Proposição 1.3. *Sejam A, B anéis e $f : A \to B$ homomorfismo, são válidas:*

1. $f(0_A) = 0_B$;
2. $f(-a) = -f(a)$;
3. $f(a-b) = f(a) - f(b)$;
4. *f é injetor se, e só se,* $ker(f) = \{0_A\}$;
5. *Se f é sobrejetora e A possui unidade, então B possui unidade e* $f(1_A) = 1_B$;
6. *Se f é sobrejetora, A possui unidade e $a \in U(A)$, então $f(a) \in U(B)$ e* $f(a^{-1}) = (f(a))^{-1}$.

1.1.3 Característica de um Domínio de Integridade

O conceito de característica tem grande importância em nosso estudo uma vez que nosso foco são os corpos de números e corpos finitos.

Vamos considerar D um domínio de integridade e o conjunto

$$\mathbb{Z}.1_D = \begin{cases} m.1_D = 1_D + 1_D + \ldots + 1_D (m \text{ vezes}), \text{ se } m > 0 \\ m.1_D = -1_D - 1_D \ldots - 1_D (m\text{vezes}), \text{ se } m < 0. \\ 0.1_D = 0_D \end{cases}$$

Claramente, $\mathbb{Z}.1_D$ é subanel de D.

Definição 1.9. *Seja D um domínio de integridade. Definimos característica como o menor inteiro positivo m tal que $m1_D = 0$, isto é,*

$$car(D) = min\{m \in \mathbb{Z}_+^*; m1_D = 0\}.$$

Caso não exista $m \in \mathbb{Z}_+^*$ tal que $m1_D = 0$, diremos que a característica é zero.

Um exemplo é $\mathbb{Z}_p$ com p primo. Pela Proposição 1.2, $\mathbb{Z}_p$ é um domínio de integridade e claramente $\mathbb{Z}_p$ tem característica p. Temos que $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ tem característica zero.

Teorema 1.1. *Se D é um domínio de integridade, então $car(D) = 0$ ou $car(D) = p$, com p um número primo.*

Demonstração. Suponhamos $car(D) = n = n_1 n_2$, com $1 < n_1, n_2, < n$. Assim, temos $n1_D = n_1 n_2 1_D = (n_1 1_D)(n_2 1_D) = 0$. Como D é domínio temos que $n_1 1_D = 0$ ou $n_2 1_D = 0$, o que contradiz a minimalidade de n. Portanto, n é um número primo. ■

Corolário 1.2. *Se D é um domínio de integridade e $car(D) = 0$, então D tem um subanel isomorfo a $\mathbb{Z}$.*

Demonstração. Basta considerar a aplicação $\varphi : \mathbb{Z} \to \mathbb{Z}.1_D$, dada por $\varphi(m) = m.1_D$. Tem-se que φ está bem definida, pois a adição em D está bem definida. Claramente, $N(\varphi) = \{0\}$ e $Im(\varphi) = \mathbb{Z}.1_D$, ou seja, φ é injetora e sobrejetora. Por fim, $\varphi(m+n) = (m+n).1_D = m.1_D + n.1_D = \varphi(m) + \varphi(n)$ e $\varphi(mn) = (mn).1_D = m.1_D.n.1_D = \varphi(m).\varphi(n)$. Portanto, φ é um isomorfismo. ■

Corolário 1.3. *Se D é um domínio de integridade e $car(D) = p$, com p um número primo, então D tem um subanel isomorfo a $\mathbb{Z}_p$.*

Demonstração. Basta considerar $\psi : \mathbb{Z}_p \to \mathbb{Z}.1_D$, dada por $\psi(\overline{m}) = m.1_D$. Tem-se que ψ está bem definida, pois se $\overline{m} = \overline{n}$, então $m - n = kp$, para algum $k \in \mathbb{Z}$, e assim, $(m-n).1_D = 0_D$, ou seja, $m.1_D = n.1_D$. Note que $N(\psi) = kp$, com $k \in \mathbb{Z}$. Logo, ψ é injetora. Como $Im(\psi) = \{0.1_D, 1.1_D, \ldots, (p-1).1_D\} = \mathbb{Z}.1_D$, pois $car(D) = p$, segue que ψ é sobrejetora. Ainda, $\psi(\overline{m} + \overline{n}) = \psi(\overline{m+n}) = (m+n).1_D = m.1_D + n.1_D$ e $\psi(\overline{m}.\overline{n}) = \psi(\overline{mn}) = mn.1_D = m.1_D n.1_D$, tem-se que ψ é um isomorfismo. ■

Observação 1.1. *Note que se $car(D) = 0$, pelo Corolário 1.2, D tem um cópia de $\mathbb{Z}$. Logo, D é infinito. E se D é finito, então $car(D) = p$, com p primo e D tem uma cópia de $\mathbb{Z}_p$.*

Proposição 1.4. *Sejam D um domínio de integridade de característica p e $q \in \mathbb{Z}$ tal que $q = p^r$, para algum inteiro positivo r. Se $a, b \in D$, então $(a \pm b)^q = a^q \pm b^q$.*

Demonstração. A demonstração é consequência direta do binômio de Newton e do fato que p divide $\begin{pmatrix} p \\ i \end{pmatrix}$, para todo $i = 1, \ldots, p-1$. Vamos denotar $m = \begin{pmatrix} q \\ 1 \end{pmatrix} a^{q-1}b + \cdots + \begin{pmatrix} q \\ q-1 \end{pmatrix} ab^{q-1}$ em $(a+b)^q = a^q + \begin{pmatrix} q \\ 1 \end{pmatrix} a^{q-1}b + \cdots + \begin{pmatrix} q \\ q-1 \end{pmatrix} ab^{q-1} + b^q = a^q + m + b^q$. Como q divide m e p divide q temos que $m = 0$. Assim, concluímos que $(a+b)^q = a^q + b^q$. Para o caso $(a-b)^q$ a demonstração será análoga. ■

1.1.4 Ideais

Vamos considerar nessa seção A um anel comutativo.

Definição 1.10. *Seja I subconjunto não-vazio de A, dizemos que I é ideal de A se as condições a seguir são verificadas:*

i)$x - y \in I$, para todo $x, y \in I$;

ii)$a \cdot x \in I$, para todo $a \in A$ e $x \in I$.

Notação: $I \trianglelefteq A$.

Chamaremos $\{0\}$ e A de ideais triviais e os ideais não triviais chamaremos de ideais próprios.

Definição 1.11. *Chamaremos um ideal I de ideal principal gerado por $a \in A$, se todo elemento $x \in I$ é da forma $x = a \cdot y$, com $y \in A$. Vamos denotar o ideal principal gerado por a da seguinte forma $I = \langle a \rangle$.*

Um domínio de integridade que só possui ideais principais é chamado de domínio principal.

Proposição 1.5. *Temos que $\mathbb{Z}$ é um domínio principal.*

Demonstração. Devemos mostrar que para todo $J \trianglelefteq \mathbb{Z}$, tem-se que J é principal. De fato, como $J \neq \emptyset$, segue que existe $x \in J$, e assim, $x - x = 0 \in J$. Se 0 é o único elemento de J temos que $J = \langle 0 \rangle$, ou seja, J é principal.

Agora, se existe $a \in J$, com $a \neq 0$, então $-a \in J$. Logo, existe um subconjunto de J com elementos positivos. Pelo princípio do menor inteiro positivo, existe $b \in J$ menor elemento positivo de J. Seja $m \in J$, pelo algorítimo de Euclides existem q e $r \in \mathbb{Z}$, tais que $m = bq + r$, com $0 \leq r < b$. Como m e $b \in J$, segue que $r = m - bq \in J$. Logo $r = 0$, pois b é o menor elemento positivo de J. Assim, $m = bq$, e dai, $m \in \langle b \rangle$, ou seja, $J \subset \langle b \rangle$. Claramente, $\langle b \rangle \subset J$, e assim, $J = \langle b \rangle$, com b o menor elemento de J. ■

Definição 1.12. *i) Um ideal P de A é chamado de ideal primo, se $P \neq A$ e sempre que $x \cdot y \in P$, tem se $x \in P$ ou $y \in P$*

ii) Um ideal próprio J de A é dito ideal maximal, quando $J \subseteq I \subseteq A$, implicar que, $I = A$ ou $I = J$.

Proposição 1.6. *i) Os ideais primos de $\mathbb{Z}$ são ideais gerados por um número primo ou por 0.*

ii)Todo ideal primo de $\mathbb{Z}$ é maximal.

Demonstração. i) Se $P = \{0\}$, temos que $\langle 0 \rangle = P$. Se $P = \langle a \rangle$ com $a \neq 0$, suponhamos que $a = x.y$, com $1 < x, y < a$. Como $\langle a \rangle$ é primo, temos que $x \in \langle a \rangle$ ou $y \in \langle a \rangle$, contradizendo a minimalidade de a. Portanto, a é primo.

ii) Sejam $J, I \trianglelefteq \mathbb{Z}$ tal que $J \subseteq I \subseteq \mathbb{Z}$ e J é ideal primo de $\mathbb{Z}$. Como $\mathbb{Z}$ é domínio principal, temos que $J = \langle p \rangle$ e $I = \langle m \rangle$. Sendo p primo e $J \subseteq I$ temos que $p = mk$, mas isso só é possível se $m = 1$ ou $k = 1$, ou seja, $I = \mathbb{Z}$ ou $J = I$.

■

Seja I um ideal do anel A. Vamos inicialmente definir a seguinte relação;

$$x, y \in A, x \cong y(modI), \Leftrightarrow x - y \in I$$

Podemos facilmente verificar que se trata de uma relação de equivalência e denotaremos por $a + I = \{x \in A; x \cong a(modI)$ a classe de equivalência do elemento $a \in A$, com a relação $\cong (modI)$.

Agora, vamos considerar $I \trianglerighteq A$ e $\dfrac{A}{I}$ o **anel quociente** de A por I, com as operações $(a+I)+(b+I) = (a+b)+I$ e $(a+I).(b+I) = (a.b)+I$. Claramente, $a+I = b+I$ se, e somente se, $a - b \in I$, em que $0 + I$ é o elemento neutro e $1 + J$ é a unidade de $\dfrac{A}{I}$.

Teorema 1.4. *(Teorema do Isomorfismo) Sejam A e B anéis comutativos. Se $f : A \to B$ é um epimorfismo, então $\dfrac{A}{N(f)} \simeq B$.*

Demonstração. Primeiramente, vamos mostrar que $N(f)$ é um ideal de A. Temos que $N(f) \neq \varnothing$, pois $0 \in N(f)$. Se $x, y \in N(f)$, então $f(x-y) = f(x) - f(y) = 0_B - 0_B = 0_B$, ou seja, $x - y \in N(f)$. E se $x \in N(f)$ e $a \in A$, então $f(xa) = f(x)f(a) = 0_B f(a) = 0_B$, ou seja, $xa \in N(f)$. Logo, $N(f)$ é ideal de A. Para facilitar a escrita, consideramos $N(f) = I$.

Agora, considere $\varphi : \dfrac{A}{I} \to B$ dada por $\varphi(a + I) = f(a)$. Mostraremos que φ é um isomorfismo.

De fato, note que φ está bem definida, pois se $\varphi(a + I) = f(a)$ e $\varphi(a + I) = f(a')$, então f não estaria bem definida, o que não ocorre.

Claramente, φ é homomorfismo, pois f é homomorfismo. Agora, considere $b \in B$. Como f é epimorfismo, existe $a \in A$ tal que $f(a) = b$. Assim, basta tomar $\varphi(a + I) = f(a) = b$ e φ é sobrejetora.

Por fim, note que $N(\varphi) = \{a + N(f); \varphi(a + N(f)) = f(a) = 0_B\} = N(f)$, ou seja, $N(\varphi) = 0 + N(f)$, ou seja, φ é injetora. Portanto, φ é um isomorfismo. ■

O próximo resultado é um dos resultados mais importantes do capítulo. E terá uma versão mais forte na seção de corpos.

Proposição 1.7. *Tem-se que $I \trianglerighteq A$ primo se, e somente se, $\frac{A}{I}$ é um domínio de integridade.*

Demonstração. Sejam $a+I$ e $b+I \in \frac{A}{I}$, com $(a+I)(b+I) = 0+I$, ou seja, $ab+I = 0+I$. Logo, $ab \in I$ com I ideal primo de A, ou seja, $a \in I$ ou $b \in I$. Desta forma, $a+I = 0+I$ ou $b+I = 0+I$. Portanto, $\frac{A}{I}$ é um domínio de integridade.

Reciprocamente, considere $ab \in I$. Logo, $ab + I = 0 + I$ em $\frac{A}{I}$. Como $ab + I = (a+I)(b+I)$, segue que $a+I = 0+I$ ou $b+I = 0+I$, pois $\frac{A}{I}$ é domínio . Assim, $a \in I$ ou $b \in I$. Portanto, $I \trianglerighteq A$ primo. ■

1.2 Corpos

Agora, vamos definir corpos que é o principal conceito do trabalho.

Definição 1.13. *Um corpo é um anel comutativo com unidade $(A, +, \cdot)$, em que todo elemento não nulo é invertível, ou seja, $\forall a \in A^*, \exists\ a^{-1} \in A^*$ tal que $aa^{-1} = 1$.*

Exemplo 1.5. *a) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ são corpos.*

b) $\mathbb{Z}$ não é um corpo. Em particular, somente 1 e -1 são inversíveis em $\mathbb{Z}$.

Proposição 1.8. *Todo corpo é um domínio de integridade.*

Demonstração. Seja $\mathbb{K}$ um corpo e $a, b \in \mathbb{K}$, tais que $ab = 0$. Se $a \neq 0$, então existe $a^{-1} \in \mathbb{K}$, tal que $aa^{-1} = 1$. Logo $a^{-1}ab = 1b$ e $a^{-1}ab = a^{-1}0 = 0$, ou seja, $b = 0$. De modo análogo, se $b \neq 0$, então $a = 0$. Portanto $\mathbb{K}$ é domínio. ■

Proposição 1.9. *Todo domínio de integridade finito é corpo.*

Demonstração. Seja A um domínio de integridade finito, $A = \{a_1, a_2, \cdots a_n\}$. Considere $a_i \neq 0$ e a aplicação

$$f_{a_i} : A \longrightarrow A$$

$$a_j \longmapsto a_j a_i.$$

i)Temos que f_{a_i} está bem definida, pois A é fechado para a multiplicação, ou seja, $a_j a_i \in A$ e se tivéssemos $a_j a_i = a_k$ e $a_j a_i = a_l$, com $a_k \neq a_l$ a multiplicação em A não estaria bem definida, o que não ocorre.

ii)Se $a_k a_i = a_j a_i$, então $(a_k - a_j)a_i = 0$. Como A é domínio e $a_i \neq 0$ segue que $a_k = a_j$, e portanto, f é injetora.

iii) Como f_{a_i} é injetora e A é finito, segue que f_{a_i} é sobrejetora.

Assim existe $a_j \in A^*$ tal que $a_i a_j = 1$, $\forall a_i \in A^*$.

Portanto A é corpo. ■

Exemplo 1.6. *Se p é um número primo, então $\mathbb{Z}_p$ é finito e é um domínio de integridade, e portanto, um corpo.*

Observação 1.2. *Como vimos na Observação 1.1 se $\mathbb{K}$ é um corpo de característica p, temos que $\mathbb{K}$ tem uma cópia de $\mathbb{Z}_p$. Além disso, $\mathbb{Z}_p$ é isomorfo ao menor corpo contido em $\mathbb{K}$. Para isso, basta notar que $\mathbb{Z}.1_{\mathbb{K}}$ está contido em todo subcorpo de $\mathbb{K}$.*

Proposição 1.10. *Se $\mathbb{K}$ é um corpo e $car(\mathbb{K}) = 0$, então o menor subcorpo de $\mathbb{K}$ é isomorfo a $\mathbb{Q}$.*

Demonstração. O menor subcorpo de $\mathbb{K}$ é a interseção de todos os subcorpos de $\mathbb{K}$. Seja $\mathbb{F} = \cap \mathbb{K}_i$, com $\mathbb{K}_i$ subcorpo de $\mathbb{K}$. Devemos mostra que $\mathbb{F} \simeq \mathbb{Q}$.

De fato, considere a aplicação $\psi : \mathbb{Q} \to \mathbb{K}$, dada por $\psi\left(\frac{a}{b}\right) = \frac{a \cdot 1}{b \cdot 1}$.

Vejamos inicialmente que ψ esta bem definida. Sejam $\frac{a}{b}$ e $\frac{c}{d}$, com $mdc(b, d) = 1$ e $a \neq c$, isto é $\frac{a}{b} \neq \frac{c}{d}$, logo teremos que $a \cdot 1 \neq c \cdot 1$ com $b \cdot 1$ e $d \cdot 1$ primos entre si, e portanto $\frac{a \cdot 1}{d \cdot 1} \neq \frac{c \cdot 1}{d \cdot 1}$.

i) Claramente ψ é um homomorfismo de anéis.

ii) Como $N(\psi) = \left\{\frac{a}{b} \in \mathbb{Q}; a.1 = 0\right\}$ e $car(\mathbb{K}) = 0$ segue que $N(\psi) = \left\{\frac{0}{b} = 0\right\}$, ou seja, ψ é injetora.

iii) Logo, pelo Teorema 1.4, $\mathbb{Q} \simeq \psi(\mathbb{Q})$, ou seja, $\psi(\mathbb{Q})$ é subcorpo de $\mathbb{K}$.

iv) Basta notar que $\psi(\mathbb{Q}) = \mathbb{F}$. Claramente, $\mathbb{F} \subset \psi(\mathbb{Q})$, e como, $a.1, b.1 \in \mathbb{F}$ segue que $a.1(b.1)^{-1} \in \mathbb{F}$, ou seja, $\frac{a.1}{b.1} \in \mathbb{F}$.

Portanto, $\mathbb{F} \simeq \mathbb{Q}$. ■

Neste capítulo vimos que existem dois tipos de corpos. Os corpos de característica zero, que contém um cópia dos racionais, que por consequência são corpos com uma infinidade de elementos. E os corpos de característica um número primo p, que contém uma cópia de $\mathbb{Z}_p$.

Nosso objetivo nos próximos capítulos é entender como esses corpos são obtidos.

Capítulo 2

Polinômios

Neste capítulo iremos estudar polinômios com coeficientes em um corpo e alguns critérios de irredutibilidade de polinômios. As principais referências são: [2], [4], [8] e [10].

2.1 Anéis de Polinômios

Seja A um anel e x uma variável. A expressão $f(x) = a_0 + a_1x + \cdots + a_nx^n$, onde $a_i \in A$, para $i = 0, 1, 2, \cdots, n$ e $n \in \mathbb{N} = \{0, 1, 2, \cdots\}$ é chamado de polinômio na variável x com coeficientes em A.

Se $a_i = 0, \forall i = 0, 1, \cdots, n$, chamamos $f(x)$ de polinômio identicamente nulo e denotamos $f \equiv 0$.

Para os termos em que $a_i = 0$, omitiremos o termo a_ix^i.

Dois polinômios $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_nx^n$ são iguais se, e somente se, $a_i = b_i$, para todo $i = 0, 1, \cdots, n$.

Chamaremos de grau do polinômio não nulo $f(x) = a_0 + a_1x + \cdots + a_nx^n$, o maior n tal que $a_n \neq 0$ e denotaremos $\partial(f(x))$, ou simplesmente, $\partial(f)$. Se $\partial(f) = n$, chamamos a_n de coeficiente líder. Se $\partial(f) = n$ e $a_n = 1$, chamaremos f de polinômio mônico.

Vamos denotar por $A[x]$, o conjunto de todos os polinômios na variável x com coeficientes em A.

Observação 2.1. *Claramente $A \subset A[x]$. Basta tomar $f(x) = a$, com $a \in A$.*

Definiremos agora duas operações em $A[x]$. Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$ em $A[x]$.

$$+ : A[x] \times A[x] \longrightarrow A[x]$$
$$(f(x), g(x)) \longmapsto (f+g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k,$$

onde $k = max\{m, n\}$

$$\cdot : A[x] \times A[x] \longrightarrow A[x]$$
$$(f(x), g(x)) \longmapsto (f \cdot g)(x) = \sum_{i=0}^{m+n} c_i x^i,$$

onde $c_i = \sum_{j=0}^{i} a_j b_{i-j}$.

Observação 2.2. *Se $f(x), g(x) \in A[x]$ não nulos, com $\partial(f) = n$ e $\partial(g) = m$, então $\partial(f+g) \leq max\{\partial(f), \partial(g)\}$ ou $f + g \equiv 0$ e $\partial(f.g) \leq \partial(f) + \partial(g)$ ou $f.g \equiv 0$.*

Exemplo 2.1. *Sejam $f(x) = -1 + x + 2x^2$ e $g(x) = 4 + 3x$ em $\mathbb{Z}[x]$. Temos que $(f+g)(x) = 3 + 4x + 2x^2$ e $(f \cdot g)(x) = c_0 + c_1x + c_2x^2 + c_3x^3$, onde.*

$$c_0 = a_0b_0 = (-1)4 = -4$$
$$c_1 = a_0b_1 + a_1b_0 = (-1)3 + 1 \cdot 4 = 1$$
$$c_2 = a_0b_2 + a_1b_1 + a_2b_0 = 0 + 1 \cdot 2 + 2 \cdot 4 = 11$$
$$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_1 = 0 + 0 + 2 \cdot 3 + 0 = 6$$

ou seja, $(f \cdot g)(x) = -4 + x + 11x^2 + 6x^3$.

Logo, se A um anel comutativo com unidade, então $(A[x], +, \cdot)$ também é um anel comutativo com unidade, onde $f(x) = 0$ é o elemento neutro e $g(x) = 1$ é a unidade.

Proposição 2.1. *Se A é um domínio de integridade, então $A[x]$ é um domínio de integridade.*

Demonstração. Se A não tem divisores de zero, temos que $a \neq 0$ e $b \neq 0$ implica que $ab \neq 0$. Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n \not\equiv 0$ e $g(x) = b_0 + b_1x^1 + \cdots + b_mx^m \not\equiv 0$ e supondo que $\partial(f) = n$ e $\partial(g) = m$, tem-se que $a_n \neq 0$ e $b_m \neq 0$. Como $f(x)g(x) =$

$\sum_{i=0}^{m+n} c_i x^i$ e $c_i = \sum_{j=0}^{i} a_j b_{i-j}$, temos então que $c_{n+m} = a_n b_m \neq 0$, consequentemente temos $f(x)g(x) \not\equiv 0$.

■

Observação 2.3. *De acordo com a Proposição 2.1, se $f(x), g(x) \in A[x]$ não nulos, com A domínio de integridade, $\partial(f) = n$ e $\partial(g) = m$, teremos que $\partial(f.g) = n + m$.*

Na próxima Proposição vamos considerar $U(A)$ o conjunto dos elementos inversíveis do anel A.

Proposição 2.2. *Se A é um domínio de integridade, então $U(A[x]) = U(A)$.*

Demonstração. Claramente temos que $U(A) \subset U(A[X])$, pois se $a \in U(A)$ existe $b \in U(A)$ tal que $ab = 1$. Logo, se $f(x) = a \in A[x]$, existe $g(x) = b \in A[x]$, tal que $f(x)g(x) = ab = 1$.

Agora, seja $p(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$, não nulo e inversível. Logo, existe $q(x) = \sum_{j=0}^{m} b_j x^j \in A[x]$, não nulo tal que

$$p(x)q(x) = \sum_{k=0}^{m+n} c_k x^k = 1,$$

em que $c_k = \sum_{t=0}^{k} a_t b_{k-t}$, ou seja,

$$\begin{aligned} c_{m+n} &= a_n b_m = 0 \\ c_{m+n-1} &= a_n b_{m-1} + a_{n-1} b_m = 0 \\ &\vdots \\ c_0 &= a_0 b_0 = 1 \end{aligned}$$

Se $a_n \neq 0$ teremos $b_m = 0$, em c_{m+n}. Da mesma forma teremos $b_{m-1} = 0$ em c_{m+n-1}. Repetindo esse processo concluiremos que $b_m = b_{m-1} = \cdots = b_1 = 0$. Assim, $q(x) = b_0$, com $b_0 \in A$, não nulo e inversível. Assim $p(x)$ também é constante, não nulo e inversível como queríamos.

■

2.1.1 Divisão de Polinômios

Vamos considerar a partir desta seção $\mathbb{K}$ um corpo e $\mathbb{K}[x]$ o anel de polinômios sobre $\mathbb{K}$.

Teorema 2.1. *(Algoritmo da divisão euclidiana) Sejam $f(x), g(x) \in \mathbb{K}[x]$ e $g(x)$ não nulo. Então existem únicos $q(x), r(x) \in \mathbb{K}[x]$, tais que $f(x) = g(x)q(x) + r(x)$, com $\partial(r) < \partial(g)$ ou $r \equiv 0$.*

Demonstração. Caso $f \equiv 0$, basta tomar $q \equiv 0$ e $r \equiv 0$. Se $f \not\equiv 0$, temos $\partial(f) = n \geq \partial(g) = m$ ou $n < m$. Se $n < m$, consideramos $g \equiv 0$ e $r(x) = f(x)$ garantido a condição que $\partial(r) < \partial(g)$.

Se $n \geq m$ vamos definir $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$, onde a_n é o coeficiente líder de $f(x)$ e b_m o coeficiente líder de $g(x)$. Vejamos que o coeficiente líder de $a_n b_m^{-1} x^{n-m} g(x)$ é a_n, assim teremos que $\partial(f_1) < \partial(f)$. Sendo suficiente mostrar agora a existência de $f_1(x)$, para todo $n \geq 0$. Façamos por indução sobre n.

Para $n = 0$ temos $m = 0$, e assim, $f(x) = a_0 \neq 0$ e $g(x) = b_0 \neq 0$, o que implica, que $f_1 \equiv 0$ e $f(x) = a_0 b_0^{-1} g(x) \neq 0$, ou seja, $q(x) = a_0 b_0^{-1}$ e $r \equiv 0$.

Agora vamos mostrar a unicidade do teorema. Suponhamos agora que existam $q(x), r(x) \in \mathbb{K}[x]$ para todo $k < n$. Temos então que existem $q_1(x)$ e $r_1(x)$ tal que $f_1(x) = q_1(x)g(x) + r_1(x)$, com $r_1 \equiv 0$ ou $\partial(r_1) < \partial(g)$. Substituindo $f_1(x)$ em $f(x) = f_1(x) + a_n b_m^{-1} g(x)$ temos $f(x) = q_1(x)g(x) + r_1(x) + a_n b_m^{-1} x^{n-m} g(x) = (q_1(x) + a_n b_m^{-1} x^{n-m})g(x) + r_1(x)$, ou seja, existe $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ e $r(x) = r_1(x)$.

Suponhamos que existam $q_1(x), r_1(x), q_2(x), r_2(x) \in \mathbb{K}[x]$ tal que $f(x) = q_1(x)g(x) + r_1(x)$ e $f(x) = q_2(x)g(x) + r_2(x)$, assim temos a igualdade;

$$\begin{aligned} q_1(x)g(x) + r_1(x) &= q_2(x)g(x) + r_2(x) \\ \Leftrightarrow q_1(x)g(x) + r_1(x) - q_2(x)g(x) &= r_2(x) \\ \Leftrightarrow (q_1(x) - q_2(x))g(x) &= r_2(x) - r_1(x) \end{aligned}$$

Sendo assim $\partial((q_1 - q_2)g) = \partial(r_2 - r_1)$. Suponhamos $q_1(x) \neq q_2(x)$. Analisando os graus temos $\partial((q_1 - q_2)g) = \partial(q_1 - q_2) + \partial(g) \geq \partial g$ e $\partial(r_2 - r_1) \leq max\{\partial(r_1), \partial(r_2)\} < \partial(g)$,

que é uma contradição ou $\partial(r_2 - r_1) = 0$. Portanto, só podemos ter $q_1(x) = q_2(x)$, consequentemente $r_1(x) = r_2(x)$. ■

Sejam $f(x)$ e $g(x) \in \mathbb{K}[x]$. Assim, pelo Teorema 2.1 existem únicos $q(x)$ e $r(x) \in \mathbb{K}[x]$, tais que, $f(x) = g(x)q(x) + r(x)$, com $r(x) = 0$ ou $\partial(r) < \partial(g)$. Logo, se $r \equiv 0$, dizemos que $g(x)$ divide $f(x)$, e denotaremos por $g|f$, caso $r(x) \not\equiv 0$, temos que $g(x)$ não divide $f(x)$ e denotamos por $g \nmid f$.

Definição 2.1. *Seja A um anel comutativo com unidade. Dizemos que $f(x) \in A[x]$ é irredutível sobre A se, e somente se, $f(x) \notin U(A[x])$ e sempre que $f(x) = p(x)g(x)$, tivermos $p(x)$ ou $g(x) \in U(A[x])$. Se $f(x)$ não é irredutível dizemos que $f(x)$ é redutível.*

Exemplo 2.2. *a) Vejamos que todo polinômio de grau um em $A[x]$ é irredutível.*

b) Seja $f(x) \in A[x]$ em que $\partial f = n > 1$. Vejamos que se o termo independente for nulo, teremos que $f(x)$ será redutível por x pois podemos escrever $f(x)$ da seguinte forma;

$$f(x) = x(a_1 + a_2x + \cdots a_nx^{n-1})$$

De acordo com a Definição 2.1, se tivermos $f(x) \in \mathbb{K}[x]$, então $f(x)$ é irredutível se, e somente se, $f(x) \notin \mathbb{K}^*$ e sempre que $f(x) = p(x)g(x)$, tivermos $p(x)$ ou $g(x) \in \mathbb{K}^*$.

Mais adiante iremos apresentar alguns critérios de irredutibilidade de polinômios. Mas antes vamos definir raiz de um polinômio.

2.1.2 Raízes de Polinômios

Vamos continuar considerando $\mathbb{K}$ um corpo.

Definição 2.2. *Seja $f(x) \in \mathbb{K}[x]$ um polinômio não nulo. Dizemos que $\alpha \in \mathbb{K}$ é raiz de $f(x) \in \mathbb{K}[x]$ quando $f(\alpha) = 0$.*

Proposição 2.3. *Se $f(x) \in \mathbb{K}[x]$ é não nulo e $\partial(f) = n$, então f tem no máximo n raízes em $\mathbb{K}$.*

Demonstração. Se f não tiver raízes em $\mathbb{K}$ não há o que demonstrar. Caso contrário vamos mostrar por indução sobre $\partial(f) = n$. Se $\partial(f) = 0$, então $f(x) = a \neq 0$, e assim, f não possui raiz em $\mathbb{K}$.

Suponhamos que existe $\alpha \in \mathbb{K}$ raiz de f. Temos que α também é raiz de $x-\alpha \in \mathbb{K}[x]$. Utilizando o algoritmo euclidiano existem $q(x)$ e $r(x)$ em $\mathbb{K}[x]$ tais que $f(x) = (x-\alpha)q(x)+ r(x)$, com $0 \leq \partial(r) < 1$ ou $r \equiv 0$. Assim, $r(x) = b \in \mathbb{K}$ ou $r \equiv 0$. Como $f(\alpha) = 0$, segue que $(\alpha-\alpha)q(\alpha)+r(\alpha) = r(\alpha) = 0$. Logo, $r \equiv 0$, ou seja, $f(x) = (x-\alpha)q(x)$. Note que se $\beta \neq \alpha \in \mathbb{K}$ é raiz de $f(x)$, então β é raiz de $q(x)$, pois $\mathbb{K}$ é um corpo. Como $\partial(q) = n-1$ podemos aplicar a hipótese de indução, e assim, q tem no máximo $n-1$ raízes em $\mathbb{K}$, o que implicará que f tem no máximo n raízes em $\mathbb{K}$ como queríamos. ■

Corolário 2.2. *Sejam $f(x) \in \mathbb{K}[x]$ não nulo e $\alpha \in \mathbb{K}$. Temos que $(x-\alpha) \mid f$ se, e somente se, α é raiz de f.*

Demonstração. Temos que $(x-\alpha) \mid f$ se, e somente se, existe $q(x) \in \mathbb{K}[x]$ tal que $f(x) = (x-\alpha)q(x)$ se, e somente se, $f(\alpha) = (\alpha-\alpha)q(\alpha) = 0$ se, e somente se, α é raiz de f. ■

Corolário 2.3. *Se $f(x) \in \mathbb{K}[x]$, com $\partial(f) = 2$ ou 3, temos que f é redutível se, e somente se, existe $\alpha \in \mathbb{K}$ tal que $f(\alpha) = 0$.*

Demonstração. Em ambos os casos, f é redutível se, e somente se, $f(x) = g(x)q(x)$, com pelo menos $\partial(g) = 1$. Logo, sem perda de generalidade podemos considerar f mônico, e assim, $g(x) = x-\alpha$, com $\alpha \in \mathbb{K}$. Portanto, α é raiz de f. ■

Vejamos que para polinômios de grau maior que três, existe a possibilidade de que o polinômio pode ser redutível por polinômios irredutíveis de grau maior ou igual a dois, Justificando assim o por que o corolário acima não é válido para polinômios de grau maior que três.

Definição 2.3. *Sejam $f(x)$ e $g(x) \in \mathbb{K}[x]$. Se existe $d(x) \in \mathbb{K}[x]$ tal que $d(x) \mid f(x)$, $d(x) \mid g(x)$ e sempre que existir $d'(x)$ tal que $d'(x) \mid f(x)$ e $d'(x) \mid g(x)$ tivermos que $d(x) \mid d'(x)$, diremos que $d(x)$ é o Máximo Divisor Comum, e denotaremos $d(x) = MDC(f(x), g(x))$.*

Agora, vamos considerar $f(x), g(x) \in \mathbb{K}[x]$ não simultaneamente nulos. Suponhamos $\partial(f) \geq \partial(g)$. Logo, existem $q_1(x)$ e $r_1(x) \in \mathbb{K}[x]$ tais que

$$f(x) = g(x)q_1(x) + r_1(x), \text{ com } 0 \leq \partial(r_1) < \partial(g) \text{ ou } r_1 \equiv 0$$

Se $\partial(r_1) < \partial(g)$, existem $q_2(x)$ e $r_2(x) \in \mathbb{K}[x]$ tais que

$$g(x) = r_1(x)q_2(x) + r_2(x), \text{ com } 0 \leq \partial(r_2) < \partial(r_1) \text{ ou } r_2 \equiv 0$$

Aplicando o processo sucessivamente até chegarmos em $r_n \equiv 0$, temos que r_{n-1} será chamado de $mdc(f, g)$.

Claramente, se $g \mid f$, temos que $mdc(f, g) = g$.

Como consequência desse processo de sucessões sucessivas pode-se afirmar que se $d(x) = mdc(f(x), g(x))$, então existem $m(x)$ e $n(x) \in \mathbb{K}[x]$ tais que $d(x) = m(x)f(x) + n(x)g(x)$. A recíproca também é válida. Quando $mdc(f, g) = 1$, diremos que f e g são primos entre si.

2.1.3 Ideais em $\mathbb{K}[x]$

Continuaremos considerando $\mathbb{K}$ um corpo. Nessa seção mostraremos que $\mathbb{K}[x]$ é um domínio de ideais principais e analisaremos quais polinômios geram os ideais primos e maximais de $\mathbb{K}[x]$.

Teorema 2.4. *$\mathbb{K}[x]$ é um domínio de ideais principais.*

Demonstração. Seja $I \trianglelefteq \mathbb{K}[x]$ não nulo. Claramente, se $I = \{0\}$, então $I = \langle 0 \rangle$, ou seja, é principal. Agora, se existe $p(x) \in I$, com $p \not\equiv 0$, temos que $\partial(p) = 0$ ou $\partial(p) > 0$. Se $\partial(p) = 0$, ou seja, $p(x) = a \neq 0$, com $a \in \mathbb{K}$, teremos que $aa^{-1} = 1 \in I$. Com isso, $I = \mathbb{K}[x] = \langle 1 \rangle$. Se $\partial(p) > 0$, então vamos supor sem perda de generalidade que $\partial(p)$ é o menor de I. Logo, se $f(x) \in I$, como $\partial(f) > \partial(p)$, existem $q(x), r(x) \in \mathbb{K}[x]$ tais que $f(x) = p(x)q(x) + r(x)$, com $\partial(r) < \partial(p)$ ou $r \equiv 0$. Como $f(x) \in I$ e $p(x)q(x) \in I$, segue que $r(x) \in I$, mas como $p(x)$ é o de menor grau em I, tem-se que $r \equiv 0$. Portanto, $f(x) \in \langle p(x) \rangle$, ou seja, $I = \langle p(x) \rangle$. ■

Seja $f(x) \in \mathbb{K}[x]$, mônico não constante de grau n. Temos o anel quociente $\mathbb{F} = \dfrac{\mathbb{K}[x]}{\langle f(x) \rangle}$ e como $\mathbb{K}[x]$ é domínio de ideais principais, podemos escrever o anel quociente da seguinte forma:

$$\mathbb{F} = \frac{\mathbb{K}[x]}{\langle f(x) \rangle} = \{r(x); r(x) \in \mathbb{K}[x], \text{ com } r \equiv 0 \text{ ou } \partial(r) < \partial(f)\}.$$

Podemos facilmente verificar que $\mathbb{F} = \dfrac{\mathbb{K}[x]}{\langle f(x)\rangle}$ é um anel comutativo com unidade, pois as propriedades são herdadas de $\mathbb{K}[x]$.

Proposição 2.4. *Seja* $g(x) \in \mathbb{F} = \dfrac{\mathbb{K}[x]}{\langle f(x)\rangle}$ *não nulo, temos que* $g(x)$ *é inversível se, e somente se,* $mdc(f, g) = 1$.

Demonstração. Suponhamos $g(x)$ não nulo e inversível em $\mathbb{F}$. Assim, existe $h(x) \in \mathbb{F}$, tal que $g(x)h(x) = 1$ em $\mathbb{F}$, isto é, existe $q(x) \in \mathbb{K}[x]$ tal que $g(x)h(x) = f(x)q(x) + 1$, ou seja, $g(x)h(x) - f(x)q(x) = 1$. Portanto, $mdc(f, g) = 1$.

Agora, se $mdc(f, g) = 1$, então existem $h(x)$ e $q(x) \in \mathbb{K}[x]$ tal que $g(x)h(x) + f(x)q(x) = 1$. Assim, $g(x)h(x) = f(x)(-q(x)) + 1$. Portanto existe $h(x) \in \mathbb{K}[x]$ tal que $g(x)h(x) = 1$ em $\mathbb{F}$, ou seja, $g(x)$ é inversível. ■

Proposição 2.5. *O anel* $\mathbb{F} = \dfrac{\mathbb{K}[x]}{\langle f(x)\rangle}$ *é um corpo se, e somente se,* $f(x)$ *é irredutível.*

Demonstração. Suponhamos $f(x)$ redutível, isto é, existem $g(x)$ e $q(x) \in \mathbb{K}[x]$ não nulos, tais que $f(x) = g(x)q(x)$. Como $f(x) = 0$ em $\mathbb{F}$, segue que $g(x)q(x) = 0$ em $\mathbb{F}$ o que não ocorre pois $\mathbb{F}$ é corpo.

Agora se $\mathbb{F}$ é corpo, então todo $g(x) \in \mathbb{F}$ não nulo é inversível. Segue da Proposição 2.4 que $g \nmid f$, ou seja, f é irredutível. ■

2.2 Critérios de Irredutibilidade de Polinômios

Nessa seção daremos alguns resultados sobre irredutibilidade de polinômios sobre $\mathbb{Q}$ e sobre $\mathbb{Z}_p$, com p primo. A principal referência desta seção será [2].

Inicialmente vamos considerar $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$ não nulo. Como $a_n, \ldots, a_1, a_0 \in \mathbb{Q}$, podemos encontrar o $mmc = m$ dos denominadores $a_n, \ldots, a_1, a_0$, e assim, escrever $f(x) = \frac{f_1(x)}{m}$, com $f_1(x) \in \mathbb{Z}[x]$. Supondo $f_1(x)$ irredutível sobre $\mathbb{Z}$ conseguimos mostrar que $f_1(x)$ é irredutível sobre $\mathbb{Q}$, consequentemente, $f(x)$ será irredutível sobre $\mathbb{Q}$. Esse resultado é conhecido como Lema de Gauss.

Lema 2.5. *(Lema de Gauss) Seja* $f(x) \in \mathbb{Z}[x]$. *Se* $f(x)$ *é irredutível sobre* $\mathbb{Z}$, *então* $f(x)$ *é irredutível sobre* $\mathbb{Q}$.

Demonstração. [2], pág. 43. ■

A seguir daremos um critério para irredutibilidade em $\mathbb{Z}$.

Teorema 2.6. *(Critério de Eisenstein) Seja* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. *Se existir primo* p *tal que*

$i) p \nmid a_n$

$ii) p \mid a_0, a_1, \ldots, p \mid a_n$

$iii) p^2 \nmid a_0$.

então $f(x)$ *é irredutível sobre* $\mathbb{Z}$.

Demonstração. [2], pág. 44. ■

Utilizando então o lema de Gauss, podemos verificar que se as condições do critério de Eisenstein forem satisfeitas, então $f(x)$ será irredutível sobre $\mathbb{Q}$.

Vimos no Corolário 2.3, que se $\partial(f) = 2$ ou 3, f é redutível sobre $\mathbb{K}$ se, e somente, se f tem raiz em $\mathbb{K}$. Uma forma de verificar se um polinômio de grau 2 ou 3 sobre $\mathbb{Q}$ tem raiz em $\mathbb{Q}$ é usar o Teste da raiz racional a seguir.

Teorema 2.7. *(Teste da raiz racional) Seja* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, *com* $\partial(f) = n$. *Se* $\alpha = \frac{r}{s} \in \mathbb{Q}$ *é raiz de* $f(x)$ *e* $mdc(r, s) = 1$, *então* $r|a_0$ *e* $s|a_n$.

Demonstração. [2], pág. 28. ■

Exemplo 2.3. *Seja* $f(x) = x^5 + 6x^4 - 3x^2 + 3 \in \mathbb{Z}[x]$. *Pelo critério de Eisenstein para* $p = 3$, *temos que* $3 \nmid 1, 3 \mid 3, 3 \mid -3$ *e* $3 \mid 6$, *mas* $3^2 \nmid 3$. *Logo,* $f(x)$ *é irredutível sobre* $\mathbb{Q}$.

Exemplo 2.4. *Seja* $g(x) = 5x^3 + 3x^2 - 1 \in \mathbb{Z}[x]$. *As possíveis raízes racionais de* $g(x)$ *estão no conjunto* $\left\{\pm 1, \pm\frac{1}{5}\right\}$. *Como* $g(1) = 7, g(-1) = -3g\left(\frac{1}{5}\right) = \frac{-21}{25}$ *e* $g\left(\frac{-1}{5}\right) = \frac{-23}{25}$, *segue que* $g(x)$ *é irredutível sobre* $\mathbb{Q}$.

Agora vamos apresentar o **Algoritmo de Rabin**[2], para irredutibilidade sobre $f(x) \in \mathbb{Z}_p[x]$, neste momento o algorítimo irá parecer um tanto confuso, porem no capitulo 3 mostraremos porque ele funciona.

Queremos analisar se $f(x) \in \mathbb{Z}_p[x]$ é irredutível sobre $\mathbb{Z}_p$. Primeiramente, $f(x)$ deve ser mônico e seu termo constante não poderá ser nulo, pois caso isso ocorra $f(x)$ terá

o fator x. Em seguida, verificaremos se $f(x)$ divide $x^{p^n} - x$, onde $n = \partial(f)$. Por fim, devemos ter que $mdc(f, x^{p^j} - x) = 1$, para todo $j \mid n$. Se $f(x)$ satisfizer essas 3 condições $f(x)$ será irredutível sobre $\mathbb{Z}_p$.

Capítulo 3

Extensões de Corpos

A fim de estudar as extensões de $\mathbb{Q}$ e $\mathbb{Z}_p$, com p primo. Iniciaremos apresentando resultados e definições sobre extensões de um corpo $\mathbb{K}$ qualquer. As referências dessa capítulo são: [7], [8] e [10].

Definição 3.1. *Sejam $\mathbb{L}$ e $\mathbb{K}$ corpos tais que $\mathbb{K} \subset \mathbb{L}$. Dizemos que $\mathbb{L}$ é uma extensão de $\mathbb{K}$, e denotaremos por $\mathbb{L}|\mathbb{K}$.*

Exemplo 3.1. *i) Como $\mathbb{Q}$ e $\mathbb{R}$ são corpos e $\mathbb{Q} \subset \mathbb{R}$, temos que $\mathbb{R}$ é uma extensão de $\mathbb{Q}$.*

ii) Seja $\mathbb{Q}(\sqrt{2})$ o menor subcorpo de $\mathbb{C}$ contendo $\sqrt{2}$ e $\mathbb{Q}$. Temos que $\mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$, ou seja, é uma extensão de $\mathbb{Q}$.

Definição 3.2. *i) Seja $\mathbb{L}|\mathbb{K}$ extensão de corpos. Dizemos que $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$ se existe $f(x) \in \mathbb{K}[x]$, não nulo tal que $f(\alpha) = 0$.*

ii)Dizemos que $\mathbb{L}|\mathbb{K}$ é algébrica se $\forall \alpha \in \mathbb{L}, \alpha$ é algébrico sobre $\mathbb{K}$.

Observação 3.1. *Se $f(x) \in \mathbb{K}[x]$ não nulo e $f(\alpha) = 0$, então existe um polinômio mônico irredutível $p(x) \in \mathbb{K}[x]$ tal que $p(\alpha) = 0$. Vamos denotar $p(x)$ com essas características por $irr(\alpha, \mathbb{K})$.*

Teorema 3.1. *Se $\alpha \in \mathbb{L}$ e $\varphi : \mathbb{K}[x] \longrightarrow \mathbb{L}$ tal que $\varphi(f(x)) = f(\alpha)$, então φ é homomorfismo tal que*

i) $Im\varphi = \mathbb{K}[\alpha]$ e $\mathbb{K} \subset \mathbb{K}[\alpha] \subset \mathbb{L}$

ii) Se α é algébrico sobre $\mathbb{K}$, então $N(\varphi) = \langle p(x)\rangle$, onde $p(x) = irr(\alpha, \mathbb{K})$.

iii)Se α é algébrico sobre $\mathbb{K}$, então $\dfrac{\mathbb{K}[x]}{\langle p(x)\rangle} \simeq \mathbb{K}[\alpha]$, onde $p(x) = irr(\alpha, \mathbb{K})$.

Demonstração. Claramente φ é homomorfismo, pois ;
$\varphi(f(x) + g(x)) = \varphi((f + g)(x)) = (f + g)(\alpha) = f(\alpha) + g(\alpha)$
$\varphi(f(x) \cdot g(x)) = \varphi((f \cdot g)(x) = (f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)$

i) Temos que $Im(\varphi) \subset \mathbb{K}[\alpha]$, pois $\varphi(f(x)) = f(\alpha) \in \mathbb{K}[\alpha]$. Tomando $f(\alpha) \in \mathbb{K}[\alpha]$, basta tomar $f(x) \in \mathbb{K}[x]$, que assim $\varphi(f(x)) = f(\alpha)$, ou seja $\mathbb{K}[\alpha] \subset Im(\varphi)$. Concluindo que $Im(\varphi) = \mathbb{K}[\alpha]$. Claramente $\mathbb{K} \subset \mathbb{K}[\alpha]$, pois basta tomar $f(x) = a_0 + 0\alpha + \cdots + 0\alpha^n$, com $a_0 \in \mathbb{K}$.

Portanto, $\mathbb{K}[\alpha] = Im(\varphi)$ e $\mathbb{K} \subset \mathbb{K}[\alpha] \subset \mathbb{L}$.

ii) Tomando $f(x) \in N(\varphi)$, segue que existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que

$$f(x) = p(x)q(x) + r(x); r \equiv 0 \text{ ou } \partial(r) < \partial(p)$$

Como $f(\alpha) = 0$, segue que $f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = 0$, sendo $p(x) = irr(\alpha, \mathbb{K})$, tem-se $p(\alpha) = 0$, e assim $r(x) = 0$. Portanto, $f(x) = p(x)q(x)$, ou seja, $N(\varphi) \subset \langle p(x)\rangle$. Claramente, se $f(x) \in \langle p(x)\rangle$, então $f(x) = p(x)q(x)$, para algum $q(x) \in \mathbb{K}[x]$. Logo $f(\alpha) = p(\alpha)q(\alpha) = 0$ e portanto, $\langle p(x)\rangle \subset N(\varphi)$. Concluímos então que $N(\varphi) = \langle p(x)\rangle$

iii) Segue diretamente do Teorema 1.4.

■

Proposição 3.1. *Seja $\mathbb{L}|\mathbb{K}$ extensão de corpos e $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$. Se $\partial(irr(\alpha, \mathbb{K})) = n$, então*

a) $\forall f(x) \in \mathbb{K}[x], f(\alpha)$ pode ser escrito de modo único na forma $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, com a_i's $\in \mathbb{K}$.

b) $\mathbb{K}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}; a_i \in \mathbb{K}\}$ é subcorpo de $\mathbb{L}$ que contém $\mathbb{K}$.

Demonstração. a) Seja $p(x) = irr(\alpha, \mathbb{K})$ e $\partial(p) = n$. Assim dado $f(x) \in \mathbb{K}[x]$ existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que

$$f(x) = p(x)q(x) + r(x), \text{ com } r \equiv 0 \text{ ou } \partial(r) < \partial(p).$$

Logo, $f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$. Como $\partial(r) < \partial(p) = n$ e $r(x)$ é único, tem-se que podemos escrever de forma única $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, com a_i's $\in \mathbb{K}$.

b) Temos que $\mathbb{K}[\alpha] = \{f(\alpha); f(x) \in \mathbb{K}[x]\} = \{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}; a_i\text{'s} \in \mathbb{K}\}$, pelo item a. Sejam $f(x), g(x) \in \mathbb{K}[x]$ assim $f(x) - g(x) \in \mathbb{K}[x]$, logo temos que $f(\alpha) - g(\alpha) \in \mathbb{K}[\alpha]$, de modo análogo temos $f(x)g(x)^{-1} \in \mathbb{K}[x]$, e assim, temos $f(\alpha)g(\alpha)^{-1} \in \mathbb{K}[\alpha]$. Portanto, $K[\alpha]$ é subcorpo de $\mathbb{L}$. ■

Observação 3.2. *Seja $\mathbb{K}(\alpha)$ o menor corpo que contém $\mathbb{K}$ e α. Como $\mathbb{K}[\alpha] \simeq \dfrac{\mathbb{K}[x]}{\langle p(x)\rangle}$ é corpo, segue que $\mathbb{K}[\alpha]$ coincide com $\mathbb{K}(\alpha)$, quando α é algébrico, pois $\mathbb{K}$ e α pertencem a $\mathbb{K}[\alpha]$, e com isso, $\mathbb{K}(\alpha) \subseteq \mathbb{K}[\alpha]$ e por $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ser base de $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$ todo elemento de $\mathbb{K}[\alpha]$ está contido em $\mathbb{K}(\alpha)$.*

Exemplo 3.2. 1) *Considere $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. Temos que $f(x)$ é irredutível sobre $\mathbb{Q}$, mais precisamente, $f(x) = irr(\sqrt[3]{2}, \mathbb{Q})$. Logo, $\dfrac{\mathbb{Q}[x]}{< x^3 - 2 >} \simeq \mathbb{Q}(\sqrt[3]{2})$.*

2) *Considere $p(x) = x^2+x+1 \in \mathbb{Z}_2[x]$. Temos que $p(x) = irr(\alpha, \mathbb{Z}_2)$, com $\alpha \in \mathbb{F}_4 \supset \mathbb{Z}_2$ tal que $\alpha^2 = \alpha + 1$. Logo, $\dfrac{\mathbb{Z}_2[x]}{< x^2 + x + 1 >} \simeq \mathbb{Z}_2(\alpha) \simeq \mathbb{F}_4$.*

Exemplo 3.3. *Considerando o exemplo 3.2.*

$$\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2; a_i \in \mathbb{Q}\}$$

e

$$\mathbb{Z}_2(\alpha) = \{a_0 + a_1\alpha; a_0, a_1 \in \mathbb{Z}_2\} = \{0, 1, \alpha, 1 + \alpha\}$$

3.1 Extensões finitas

Se $\mathbb{L}|\mathbb{K}$ é uma extensão de corpos, podemos ver $\mathbb{L}$ como um $\mathbb{K}$-espaço vetorial, considerando a adição em $\mathbb{L}$ e a multiplicação de um elemento de $\mathbb{K}$ por um elemento de $\mathbb{L}$, como a multiplicação em $\mathbb{L}$.

Assim se existe $B \subset \mathbb{L}$, tal que B é base de $\mathbb{L}$ sobre $\mathbb{K}$ com B é finito, então $\mathbb{L}$ é $\mathbb{K}$-espaço vetorial de dimensão finita e $\#B = dim_{\mathbb{K}}\mathbb{L}$.

Definição 3.3. *Dizemos que $B = \{a_1, a_2, \cdots a_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ quando B gera $\mathbb{L}$ sobre $\mathbb{K}$ e os elementos de B são linearmente independente.*

Definição 3.4. *Seja $dim_{\mathbb{K}}\mathbb{L} = n$ (finita) diremos que $\mathbb{L}|\mathbb{K}$ é uma extensão finita, denotaremos $dim_{\mathbb{K}}\mathbb{L} = [\mathbb{L} : \mathbb{K}]$ e chamaremos de grau de $\mathbb{L}$ sobre $\mathbb{K}$, ou simplesmente, grau da extensão $\mathbb{L}|\mathbb{K}$.*

Proposição 3.2. *Seja $\mathbb{L}|\mathbb{K}$ uma extensão de corpos.*

i) Se $\mathbb{L}|\mathbb{K}$ é finita, então $\mathbb{L}|\mathbb{K}$ é algébrica.

ii) Se $\alpha \in \mathbb{L}$ algébrico sobre $\mathbb{K}$ e $\partial(irr(\alpha, \mathbb{K})) = n$, então $B = \{1, \alpha, \cdots \alpha^{n-1}\}$ é $\mathbb{K} -$ base de $\mathbb{K}(\alpha)$ e $[\mathbb{K}(\alpha) : \mathbb{K}] = n$.

Demonstração. i) Se $\mathbb{L}|\mathbb{K}$ é finita com $[\mathbb{L} : \mathbb{K}] = m$ e $\alpha \in$ Ł, então $\mathbb{K}(\alpha)$ é um $\mathbb{K}$-subespaço de $\mathbb{L}$. Logo $dim_{\mathbb{K}}\mathbb{K}(\alpha)$ é finita e digamos que $dim_{\mathbb{K}}\mathbb{K}(\alpha) = n$. Logo, $\{1, \alpha, \alpha^2, \cdots, \alpha^n\}$ é um conjunto linearmente dependente. Desta forma, existem $a_0, a_1, \cdots, a_n \in \mathbb{K}$ não todos nulos tais que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, ou seja, tomando $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{K}[x]$ temos que $f(\alpha) = 0$. Portanto, $\mathbb{K}[\alpha] \simeq \mathbb{K}(\alpha)$ é algébrico sobre $\mathbb{K}$.

ii) Como vimos se α é algébrico sobre $\mathbb{K}$, então $\mathbb{K}[\alpha]$ é um corpo. Pelo item (a) da Proposição (3.1) temos que $f(\alpha)$ é escrito de modo único da forma $f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$. Assim, $B = \{1, \alpha, \cdots, \alpha^{n-1}\}$ é base de $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$. ■

Proposição 3.3. *Se $\mathbb{L}|\mathbb{K}$ e $\mathbb{M}|\mathbb{L}$ são extensões de corpos finitas, então*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}].$$

Demonstração. Sejam $\{v_1, v_2, \cdots v_m\}$ base de $\mathbb{M}$ sobre $\mathbb{L}$ e $\{u_1, u_2, \cdots u_l\}$ base de $\mathbb{L}$ sobre $\mathbb{K}$. É suficiente mostrar que $C = \{v_iu_j; i = 1, \cdots, m \text{ e } j = 1, \cdots, l\}$ é base de $\mathbb{M}$ sobre $\mathbb{K}$.

Vamos verificar se C é linearmente independente. Seja $\alpha_{ij} \in \mathbb{K}$, para $1 \leq i \leq m$ e $1 \leq j \leq l$.Se $\sum_{i,j=1}^{m,l} \alpha_{ij}v_iu_j = 0$, então $\sum_{j=1}^{l} \alpha_{1j}v_1u_j + \sum_{j=1}^{l} \alpha_{2j}v_2u_j + \cdots + \sum_{j=1}^{l} \alpha_{mj}v_mu_j = 0$, ou seja, $v_1\sum_{j=1}^{l} \alpha_{1j}u_j + v_2\sum_{j=1}^{l} \alpha_{2j}u_j + \cdots + v_m\sum_{j=1}^{l} \alpha_{mj}u_j = 0$. Como $v_1, v_2, \cdots v_m$ é um conjunto linearmente independente sobre $\mathbb{L}$, e portanto, sobre $\mathbb{K}$, segue que $\sum_{j=1}^{l} \alpha_{ij}u_j = 0$,

para todo $1 \leq i \leq m$. Como $\{u_1, u_2, \cdots u_l\}$ é um conjunto linearmente independente sobre $\mathbb{K}$ e $\alpha_{ij} \in \mathbb{K}$, segue que $\alpha_{ij} = 0$, $\forall 1 \leq i \leq m$ e $1 \leq j \leq l$.

Agora vamos verificar se C gera $\mathbb{M}$ sobre $\mathbb{K}$. Seja $y \in \mathbb{M}$. Sendo $\{v_1, \cdots, v_m\}$ base de $\mathbb{M}$ sobre $\mathbb{L}$, temos que $y = \lambda_1 v_1 + \lambda_2 v_2 + \cdots \lambda_m v_m$, com $\lambda_i \in \mathbb{L}$ e $1 \leq i \leq m$. Como $\lambda_i' s \in \mathbb{L}$, segue que $\lambda_i = \alpha_{i1} u_1 + \alpha_{i2} u_2 + \cdots + \alpha_{il} u_l$, pois $\{u_1, u_2, \cdots u_l\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$. Assim, $y = \sum_{i=1}^{m} v_i \sum_{j=1}^{l} \alpha_{ij} u_j = \sum_{i,j=1}^{m,l} \alpha_{ij} v_i u_j$. Portanto, $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$. ■

3.1.1 Corpo de Decomposição de polinômios

Vamos considerar nessa seção $\mathbb{K}$ um corpo e $f(x) \in \mathbb{K}[x]$ não constante.

Definição 3.5. *O menor corpo que contém $\mathbb{K}$ e todas as raízes de $f(x) \in \mathbb{K}[x]$ é chamado de corpo de decomposição de $f(x)$.*

Se $\partial(f) = n$ e digamos que $\alpha_1, \alpha_2, \ldots, \alpha_n$ são as raízes de $f(x)$, assim, $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é o corpo de decomposição de f. O próximo resultado garante a existência de uma extensão de $\mathbb{K}$ que contém todas as raízes de $f(x)$.

Proposição 3.4. *Existe uma extensão $\mathbb{L}$ de $\mathbb{K}$ que é o corpo de decomposição de $f(x) \in \mathbb{K}[x]$. Além disso, quaisquer dois corpos de decomposição de $f(x) \in \mathbb{K}[x]$ são isomorfos.*

Demonstração. [8], pág. 29. ■

Exemplo 3.4. *Considere $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$. As raízes de $f(x)$ são $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}$ e $-i\sqrt[4]{2}$. Logo, $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$ é o corpo de decomposição de $x^4 - 2$.*

Na seção a seguir veremos a relação entre o corpo de decomposição de um polinômio com corpos finitos.

3.2 Extensões Finitas de $\mathbb{Z}_p$

Nesta seção vamos considerar p um número primo. No Capítulo 1, vimos que $\mathbb{Z}_p$ é um corpo e que todo corpo de característica p tem um subcorpo isomorfo a $\mathbb{Z}_p$. Em particular, todo corpo finito é uma extensão de $\mathbb{Z}_p$. Neste capítulo veremos que para todo natural n

e todo p primo existe um corpo com p^n elementos e que dois corpos com p^n elementos são isomorfos.

Vimos também que se $\mathbb{F}$ uma extensão finita de $\mathbb{Z}_p$ e $\alpha \in \mathbb{F}$, então α é algébrico sobre $\mathbb{Z}_p$ e $\mathbb{Z}_p(\alpha)$ é uma extensão de grau n sobre $\mathbb{Z}_p$, onde $n = \partial(irr(\alpha, \mathbb{Z}_p))$. Na Proposição 3.2, vimos que $B = \{1, \alpha, \ldots, \alpha^{n-1}\}$ é base de $\mathbb{Z}_p(\alpha)$ sobre $\mathbb{Z}_p$. Com isso, claramente $\mathbb{Z}_p(\alpha)$ tem p^n elementos. E sendo $[\mathbb{F} : \mathbb{Z}_p]$ finito, $\mathbb{F}$ também terá p^m elementos, para algum m tal que $m|n$ pela Proposição 3.3.

Na Proposição 2.5, vimos uma forma de construir extensões, com p^n elementos, de $\mathbb{Z}_p$. Para isso, basta encontrarmos um polinômio irredutível sobre $\mathbb{Z}_p$ de grau n. Mas não podemos garantir, para todo n, que exista $f(x)$ irredutível sobre $\mathbb{Z}_p$. A seguir, daremos alguns resultados afim de mostrar que todo corpo finito com p^n elementos é isomorfo ao corpo de decomposição de $x^{p^n} - x$.

Vamos utilizar a Proposição 3.5 para mostrar a existência de um corpo de ordem p^n.

Proposição 3.5. *Seja $\mathbb{F}$ um corpo finito de característica p, com $q = p^n$ elementos. O conjunto $K = \{\alpha \in \mathbb{F}; \alpha^q - \alpha = 0\}$ é um subcorpo de $\mathbb{F}$.*

Demonstração. Vamos considerar $x, y \in K$, assim temos que $x^q - x = 0$ e $y^q - y = 0$. Logo segue a igualdade $0 = 0 - 0 = (x^q - x) - (y^q - y) = (x^q - y^q) - (x - y)$, ou seja, $x - y \in K$. Vamos verificar que $xy^{-1} \in K$, com $x, y \in K$ e $y \neq 0$. Vejamos que $(xy^{-1})^q - xy^{-1} = x^q y^{-q} - xy^{-1} = (x^q - xy^{q-1})y^{-q}$.

Como $y^q - y = y(y^{q-1} - 1) = 0$, com $y \neq 0$, implica que $y^{q-1} = 1$. Concluímos que $(x^q - xy^{q-1})y^{-q} = (x^q - x)y^{-q} = 0$. Portanto K é subcorpo de $\mathbb{F}$. ■

Os resultados a seguir serão usados para mostrar a unicidade de um corpo finito.

Proposição 3.6. *Seja $\mathbb{F}$ um corpo finito com $q = p^n$ elementos. Para todo $\alpha \in \mathbb{F}^* = \mathbb{F} - 0$, temos que $\alpha^{q-1} = 1$.*

Demonstração. Considere a aplicação:

$$f_\alpha : \mathbb{F}^* \longrightarrow \mathbb{F}^*$$

$$x \longmapsto \alpha x$$

Vejamos que se f_α for injetora teremos f_α sobrejetora. Claramente f_α é injetora, pois se $x_1, x_2 \in \mathbb{F}^*$, tal que $x_1 \neq x_2$, teremos $f(x_1) = \alpha x_1 \neq \alpha x_2 = f_\alpha(x_2)$. Logo, $\{a_1, a_2, \cdots a_{q-1}\} = \{\alpha a_1, \alpha a_2, \cdots \alpha a_{q-1}\}$, realizando o produto temos $\alpha^{q-1}(a_1 \cdot a_2 \cdots a_{q-1}) = a_1 \cdot a_2 \cdots a_{q-1}$, isso ocorre se, e só se, $\alpha^{q-1} = 1$. ■

Teorema 3.2. *(Existência e unicidade de corpos finitos)Sejam p um número primo e n inteiro positivo. Existe um corpo finito com p^n elementos e, além disso, quaisquer corpo finitos com p^n elementos são isomorfos ao corpo de decomposição de $x^{p^n} - x$ sobre $\mathbb{Z}_p$.*

Demonstração. Seja $x^{p^n} - x \in \mathbb{Z}_p[x]$. Vamos considerar $\mathbb{F}$ o corpo de decomposição de $x^{p^n} - x$, ou seja, o menor corpo que contém $\mathbb{Z}_p$ e todas as raízes de $x^{p^n} - x$. Se considerarmos $x^{p^n} - x \in \mathbb{F}[x]$, teremos que $x^{p^n} - x$ tem no máximo p^n raízes. Note que $mdc(x^{p^n} - x, p^n x^{p^n - 1} - 1) = 1$, ou seja, $x^{p^n} - x$ não tem raiz múltipla. Logo, em $\mathbb{F}$, $x^{p^n} - x$ tem todas raízes distintas. Agora considere $K = \{a \in \mathbb{F}; a^{p^n} = a\} \subset \mathbb{F}$. Temos que K tem p^n elementos e pela Proposição 3.5, K é um corpo. Assim, pela minimalidade de $\mathbb{F}$ temos que $K = \mathbb{F}$.

Agora, seja $\mathbb{F}$ um corpo com $q = p^n$ elementos. Logo, $\mathbb{F}$ tem característica p e contém $\mathbb{Z}_p$. Considere $x^{p^n} - x \in \mathbb{F}[x]$. Temos que $x^{p^n} - x$ tem no máximo p^n raízes em $\mathbb{F}$ e pela Proposição 3.6 temos que $\forall a \in \mathbb{F}$, $a^{p^n} = a$, ou seja, $x^{p^n} - x = \prod_{a \in \mathbb{F}} (x - a)$ em $\mathbb{F}$. Portanto, $\mathbb{F}$ é o corpo de decomposição de $x^{p^n} - x$ sobre $\mathbb{Z}_p$. ■

Nosso objetivo agora é escrever $x^{p^n} - x$ como produtos de polinômios mônicos irredutíveis em $\mathbb{Z}_p[x]$.

Definição 3.6. *Chamamos de $G_n(x)$ o produto de todos os polinômios mônicos irredutíveis de grau n em $\mathbb{Z}_p[x]$.*

Exemplo 3.5. *i) Temos que x, $x + 1$ são os mônicos irredutíveis de grau 1 em $\mathbb{Z}_2[x]$ e $x^2 + x + 1$ é o único mónico irredutível em $\mathbb{Z}_2[x]$. Assim temos $G_1(x) = x^2 - x$ e $G_2(x) = x^2 + x + 1$.*

ii)Em $\mathbb{Z}_3[x]$ temos x, $x + 1$ e $x + 2$ são mônicos e irredutíveis de grau um. Assim, $G_1(x) = x(x + 1)(x + 2) = x^3 - x$. Vejamos ainda que $x^2 + 1$, $x^2 + 2$ e $x^2 + x + 2$ são os mônicos e irredutíveis de grau dois em $\mathbb{Z}_3[x]$. Assim, $G_2(x) = (x^2+1)(x^2+2)(x^2+x+2) = (x^4 + 2)(x^2 + x + 2) = x^6 + x^5 + 2x^4 + 2x^2 + 2x + 1$

Proposição 3.7. *Se $\mathbb{F}$ é um corpo finito com $q = p^n$ elementos, então*

$$x^q - x = \prod_{t|n} G_t(x).$$

Demonstração. [7], pág. 73. ■

Corolário 3.3. *Seja $\mathbb{F}$ um corpo finito com $q = p^n$ elementos e $I(t)$ o número de polinômios mônicos irredutíveis de grau t em $\mathbb{Z}_p[x]$. Assim,*

$$q^n = \sum_{t|n} tI(t).$$

Demonstração. Vejamos que $tI(t) = \partial G_t(x)$, assim comparando os graus da igualdade na proposição anterior temos

$$\sum_{t|n} tI(t) = \partial \prod_{t|n} G_t(x) = \partial(x^{q^n} - x) = q^n.$$

■

Exemplo 3.6. *Vamos determinar $I(n)$ para $n = 1, 2, \cdots, 6$ em $\mathbb{Z}_2[x]$*

Solução: Vejamos que $q = \#\mathbb{K} = 2$ assim, aplicando o corolário 3.3

i) $I(1) = q^1 = 2$

ii) $2^2 = 1I(1) + 2I(2) \Rightarrow I(2) = 1$

iii) $2^3 = 1I(1) + 3I(3) \Rightarrow I(3) = 2$

iv) $2^4 = 1I(1) + 2I(2) + 4I(4) \Rightarrow I(4) = 3$

v) $2^5 = 1I(1) + 5I(5) \Rightarrow I(5) = 6$

vi) $2^6 = 1I(1) + 2I(2) + 3I(3) + 6I(3) \Rightarrow I(6) = 9$

3.3 Extensões Finitas dos Racionais

Chamaremos uma extensão finita $\mathbb{K}$ de $\mathbb{Q}$ de **Corpo de Números**.

Pela Proposição 2.5, vimos que podemos construir extensões finitas de $\mathbb{Q}$, de grau n, através de um polinômio irredutível $f(x)$ sobre $\mathbb{Q}$ de grau n. E no Teorema 3.1, vimos que se α é algébrico sobre $\mathbb{Q}$, então $\frac{\mathbb{Q}[x]}{\langle f(x)\rangle} \simeq \mathbb{Q}(\alpha)$, com $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial(f)$ e $f(x) = irr(\alpha, \mathbb{Q})$. Neste caso, α é chamado de Elemento Primitivo [11].

Nosso objetivo nesse trabalho é a partir de um polinômio mônico e irredutível $f(x) \in \mathbb{Q}[x]$, com $\partial(f) = n$, construir um corpo de números de grau n tal que $\frac{\mathbb{Q}[x]}{\langle f(x)\rangle} \simeq \mathbb{Q}(\alpha)$, com α raiz de f. O contrário, ou seja, a partir de $[\mathbb{F} : \mathbb{Q}] = n$ explicitar α e $f = irr(\alpha, \mathbb{Q})$ não iremos abordar aqui.

Exemplo 3.7. *Vimos no Exemplo 2.4, que* $g(x) = 5x^3 + 3x^2 - 1$ *é irredutível sobre* $\mathbb{Q}$. *Logo,* $\frac{\mathbb{Q}[x]}{\langle 5x^3 + 3x^2 - 1\rangle} \simeq \mathbb{Q}(\alpha)$, *com* $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ *e* α *raiz de* $g(x)$.

Exemplo 3.8. *Seja* $g(x) = x^3 - 5 \in \mathbb{Q}[x]$. *Claramente,* g *é irredutível sobre* $\mathbb{Q}$. *Neste caso,* $g(\sqrt[3]{5}) = 0$, *e assim,teremos* $\frac{\mathbb{Q}[x]}{\langle x^3 - 5\rangle} \simeq \mathbb{Q}(\sqrt[3]{5})$. *E com isso,* $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$.

Capítulo 4

Polinômios irredutíveis utilizando o Python

Nesse capítulo iremos dar a ideia de criar um programa para encontrar polinômios irredutíveis utilizando a linguagem de programação Python. Para iniciar o estudo sobre a linguagem de programação Python usamos [6] e [5] como referências. O Python por ser um software livre, de fácil compreensão e em crescimento mundial foi o escolhido. Em [6] é possível entender como instalar o Python e o Pycharm, que é um interpretador Python. A junção dos algoritmos, lógica matemática e programação foi um grande desafio. As ideais apresentadas nesse trabalho foram construídas através na compreensão da teoria matemática por trás dos objetivos alcançados.

Para melhor compreensão dos módulos criados para fazer os cálculos com polinômios, vamos considerar os polinômios listas no Python. As listas são colocadas entre colchetes. O sinal de igualdades é ==, o sinal de diferente ! =, o resta da divisão por %, a multiplicação pode *, a potenciação por **, o comprimento de uma lista f por $len(f)$ e um parâmetro t variando em uma lista $\{0, 1, \ldots, p\}$ por "t in range(0,p)". São usados *if* para designar *se*, *else* para designar *senão*, *while* para *enquanto*, e assim, por diante.

Mais precisamente, traremos produto, soma e subtração de polinômios, polinômios de grau 2 e 3 irredutíveis sobre $\mathbb{Z}_3$, encontraremos os G_i's definidos no capítulo 3. O raciocínio feito aqui pode ser expandido para polinômios de graus maiores e sobre p maior do que 3, Para isto apresentaremos um programa que utiliza do algorítimo de Rabin para

verificar se um polinômio de grau n qualquer é irredutível sobre $\mathbb{Z}_p$ com p primo qualquer.

A seguir temos um código que realiza o produto entre dois polinômios. Ao final do código apresentarei um exemplo.

Figura 4.1: Produto.

```python
                ### PRODUTO ###
def prodpol(f, g, p):
    """>>>
    :param pol1: Polinômio de grau n na forma de
     lista: ex a_0+a_1x+...+a_nx^n = [a_0, a_1, ..., a_n]
    :param pol2: Polinômio de grau m na forma de lista:
    ex b_0+b_1x+...+b_nx^n = [b_0, b_1, ..., b_m]
    :param p: Ordem do corpo K. ex Z_3 temos p = 3,
     Z_5 temos p = 5.
    :return: Retorna o produto do pol1 pelo pol2 na forma
     de lista. [c_0, c_1,... c_(m+n)]
    onde c_i = Sum_(j = 0) ^(i) a_j.b_(i-j).
    """
    prod = []
    t = len(f)+len(g)-2
# A função len(f) é o número de elementos da lista
# com os coeficientes de f, ou seja, o grau de f é len(f)-1.
# t é o grau do produto.
    for i in range(0, t + 1):
#Vamos fazer i variar de 0 até t.
        if i == 0:
            c0 = (f[0]*g[0]) % p
            prod.append(c0)
# Para i = 0 teremos c_0 = a_0b_0 e em seguida adicionamos a lista prod.
        else:
            ci = 0
            for j in range(0, i+1):
# Caso i diferente de 0 faremos j variando de 0 até i
                try:
                    dj = f[j] * g[i-j]
# dj cada parcela de ci para i fixo.
                except:
                    dj = 0
                ci += dj
            r = ci % p
# r o resto da divisão de ci por p.
            prod.append(r)
    return prod
# EXEMPLO:
f = [2, 2, 1]
g = [1, 1, 0, 1]
p = 3
prod = prodpol(g, f, p)
print(f'O produto entre {f}, e  {g} é igual a {prod}')
```

Fonte: Autor.

Rogando o programa anterior obtemos.

Figura 4.2: Exemplo de produto.

```
O produto entre [2, 2, 1], e  [1, 1, 0, 1] é igual a [2, 1, 0, 0, 2, 1]
```

Fonte: Autor.

No código a seguir temos a soma, juntamente com um exemplo.

Figura 4.3: Soma de polinômios.

```
47              #SOMA
48  def somapol(pol1, pol2, p):
49      """>>>
50      :param pol1: Polinomio de grau n na forma de lista: ex a_0+a_1x+...+a_nx^n = [a_0, a_1, ..., a_n]
51      :param pol2: Polinomio de grau m na forma de lista: ex b_0+b_1x+...+b_nx^n = [b_0, b_1, ..., b_m]
52      :param p: Ordem do corpo. ex Z_3 temos p = 3, Z_5 temos p = 5.
53      :return: Retorna a soma do pol1 pelo pol2 na forma de lista. [a_0+b_0, a_1+b_1+...+a_k+b_k],
54      onde k é o maximo entre os graus de pol1 e pol2.
55      """
56      soma = []
57      graumin =  min(len(pol1), len(pol2))
58      cont = 0
59      for n in range(0, graumin):
60          an = pol1[cont]+pol2[cont]
61          r = an % p
62          soma.append(r)
63          cont +=1
64      if len(pol1)< len(pol2):
65          c = 0
66          for n in range(len(pol1), len(pol2)):
66          for n in range(len(pol1), len(pol2)):
67              an = pol2[len(pol1)+c]
68              c +=1
69              soma.append(an)
70      if len(pol1) > len(pol2):
71          c = 0
72          for n in range(len(pol2), len(pol1)):
73              an = pol1[len(pol2)+c]
74              c +=1
75              soma.append(an)
76      return soma
77
78
79  #EXEMPLO
80  f = [0, 1, 2, 1]
81  g = [0, 2]
82  print(f'A soma entre o polinômio {f} e o polinômio {g} resulta em {somapol(f, g, 3)}')
```

```
A soma entre o polinômio [0, 1, 2, 1] e o polinômio [0, 2] resulta em [0, 0, 2, 1]
```

Fonte: Autor.

Com pequenas alterações podemos construímos um código que realiza a subtração, como veremos.

Figura 4.4: Subtração de polinômios.

```python
#              SUBTRAÇÃO DE POLINÔMIOS
def subpol(pol1, pol2, p):
    """>>>
    :param pol1: Polinomio de grau n na forma de
    lista: ex a_0+a_1x+...+a_nx^n = [a_0, a_1, ..., a_n]
    :param pol2: Polinomio de grau m na forma de
    lista: ex b_0+b_1x+...+b_nx^n = [b_0, b_1, ..., b_m]
    :param p: Ordem do corpo. ex Z_3 temos p = 3,
     Z_5 temos p = 5.
    :return: Retorna a subtração do pol1 pelo pol2 na
    forma de lista. [a_0+b_0, a_1+b_1+...+a_k+b_k],
    onde k é o maximo entre os graus de pol1 e pol2.
    """
    sub = []
    graumin =  min(len(pol1), len(pol2))
# Inicialmente trabalharemos a subtração dos coeficientes cujo indece é igual ao mínimo dos graus.
    cont = 0
    for n in range(0, graumin):
        an = pol1[cont] - pol2[cont] + p
        r = an % p
        sub.append(r)
        cont +=1
    if len(pol1)< len(pol2):
        c = 0
        for n in range(len(pol1), len(pol2)):
# Como visto antes len(pol1) é igual grau de pol1+1. Os coeficientes de pol1 a partir de len(pol1) são nulos.
            an = (- pol2[len(pol1)+c] + p) % p
            c +=1
            sub.append(an)
    if len(pol1) > len(pol2):
        c = 0
        for n in range(len(pol2), len(pol1)):
            an = pol1[len(pol2)+c]
            c +=1
            sub.append(an)
    return sub
#EXEMPLO
g = [1, 2, 0, 0, 2]
f = [2, -1, 2]
sub = subpol(f, g, 3)
print(f'A subtração do polinômio {f}, por {g} é igual a {sub}')
```

```
A subtração do polinômio [2, -1, 2], por [1, 2, 0, 0, 2] é igual a [1, 0, 2, 0, 1]
```

Fonte: Autor.

Na imagem abaixo temos um código que gera polinômio com n coeficientes, todos nulos, este sendo fundamental para determinar a lista de todos os polinômios de grau 2 ou 3 e ainda o utilizarei para construir o MDC.

Figura 4.5: Polinômio nulo.

```
1
2               # Polinômio nulo com n coeficientes
3   def polnulo(grau):
4       """>>> Esta def apresenta uma lista de ordem grau,
5        represntando o polinômio nulo.ex [0, 0, 0]
6       :param grau: grau do polinômio que será trabalhado.
7       :return: retorna uma lista com grau+1 coeficientes nulos.
8       """
9       pol = []
10      for i in range(0, grau+1):
11          pol.append(0)
12      return pol
13  #EXEMPLO
14  n = polnulo(4)
15  print(f'O polinômio nulo com cinco coeficientes é {n}')
```

```
O polinômio nulo com cinco coeficientes é [0, 0, 0, 0, 0]
```

Fonte: Autor.

A seguir temos um código que gera uma lesta de listas com três termos representando todos os polinômios de grau menor ou igual a dois.

Figura 4.6: Lista de polinômios de grau ≤ 2.

```python
    # Lista de polinômios de grau 2
def listapol2(n, p):
    """>>> Gera uma lista de todos os polinômios de
    grau <= n, com coeficientes em Z_p.
    :param n: grau desejado = 2.
    :param p: Ordem do corpo.
    :return: Retorna uma lista que representa os
    polinômios de grau menor ou igual a n, coeficientes em Z_p.
    """
    lista = []
    for i in range(0, p):
        pol = [0, 0, 0]
        for d in range(0, p):
            pol[0] = i
            pol[1] = d
            for m in range(0, p):
                pol[2] = m
                lista.append(pol[:])
    return lista
#EXEMPLO
list = listapol2(2, 3)
print(list)
```

```
[[0, 0, 0], [0, 0, 1], [0, 0, 2], [0, 1, 0], [0, 1, 1], [0, 1, 2],
 [0, 2, 0], [0, 2, 1], [0, 2, 2], [1, 0, 0], [1, 0, 1], [1, 0, 2],
 [1, 1, 0], [1, 1, 1], [1, 1, 2], [1, 2, 0], [1, 2, 1], [1, 2, 2],
 [2, 0, 0], [2, 0, 1], [2, 0, 2], [2, 1, 0], [2, 1, 1], [2, 1, 2],
 [2, 2, 0], [2, 2, 1], [2, 2, 2]]
```

Fonte: Autor.

Veja que ao final da imagem temos uma lista de listas, representando os polinômio $p_0(x) = 0 + 0x + 0x^2, p_1(x) = 1 + 0x + 0x^2, \cdots, p_{27}(x) = 2 + 2x + 2x^2$.

De modo análogo, listamos os polinômios de grau 3. Neste caso não apresentarei a lista de listas de todos os polinômios de grau menor ou igual a três, pois, está possui um total de 3^4 polinômios.

Figura 4.7: Lista de polinômios de grau ≤ 3.

```
14          # LISTA DE POLINÔMIOS GRAU <= 3
15      def listapol3(n, p):
16          """>>> Gera uma lista de todos os polinômios de
17          grau <= 3, com coeficientes em Z_p.
18          :param n: grau desejado = 3.
19          :param p: Ordem do corpo.
20          :return: Retorna uma lista de listas que representa os
21          polinômios de grau menor ou igual a n, coeficientes em Z_p.
22          """
23          lista = []
24          for i in range(0, p):
25              pol = [0, 0, 0, 0]
26              for d in range(0, p):
27                  pol[0] = i
28                  pol[1] = d
29                  for m in range(0, p):
30                      pol[2] = m
31                      for s in range(0, p):
32                          pol[3] = s
33                          lista.append(pol[:])
34          return lista
```

Fonte: Autor.

A partir da lista dos polinômios de grau menor igual a 2 e da lista dos polinômios de grau menor igual a 3, extraímos os polinômios em que o termo independente seja não nulo e com coeficiente líder igual a um, para posteriormente obter os mônicos irredutíveis. Para isto construímos os seguintes códigos.

Figura 4.8: Lista dos mônicos de grau 2 e 3.

```
7   def polmonico2(grau, p):
8       """>>MÔNICOS COM TERMO CONSTANTE DIFERENTE DE ZERO
9       :param grau: Grau do polinômio desejado.
10      :param p: Ordem de K.
11      :return: retorna uma lista com todos os polinômios
12      mônicos de grau n com a_0 diferente de zero.
13      """
14      listap = []
15      lista = listapol2(grau, p)
16      for l in lista:
17          if l[grau] == 1 and l[0] != 0:
18              listap.append(l)
19      return listap
20  #POLINÔMIOS MÔNICOS DE GRAU 3 COM TERMOS CONSTANTE NÃO NULO.
21  def polmonico3(grau, p):
22      """>>> Este programa fornece todos os polinômios
23      mônicos de grau n, em que a_0 diferente de 0.
24      Pois de a_0 == 0 temos que o pol é redutivel por x.
25      :param grau: Grau do polinômio desejado.
26      :param p: Ordem de K.
27      :return: retorna uma lista com todos os polinômios
28      mônicos de grau n com a_0 diferente de zero.
29      """
30      listap = []
31      lista = listapol3(grau, p)
32      for l in lista:
33          if l[grau] == 1 and l[0] != 0:
34              listap.append(l)
35      return listap
```

Fonte: Autor.

Este código retorna uma lista com seis polinômios de grau dois mônicos com termos constante não nulo que apresentaremos na lista abaixo.

Figura 4.9: Mônicos de grau 2.

```
[[1, 0, 1], [1, 1, 1], [1, 2, 1], [2, 0, 1], [2, 1, 1], [2, 2, 1]]
```

Fonte: Autor.

Para polinômios de grau 3 temos um total de dezoito polinômios mônicos com termo constante não nulo, os quais estão representados por listas na imagem abaixo.

Figura 4.10: Mônicos de grau 3.

```
[[1, 0, 0, 1], [1, 0, 1, 1], [1, 0, 2, 1], [1, 1, 0, 1], [1, 1, 1, 1], [1, 1, 2, 1],
 [1, 2, 0, 1], [1, 2, 1, 1], [1, 2, 2, 1], [2, 0, 0, 1], [2, 0, 1, 1], [2, 0, 2, 1],
 [2, 1, 0, 1], [2, 1, 1, 1], [2, 1, 2, 1], [2, 2, 0, 1], [2, 2, 1, 1], [2, 2, 2, 1]]
```

Fonte: Autor.

Utilizando o corolário 2.3 construímos dois códigos um para grau dois e outro para grau três, capazes de verificar quais dos polinômios listados anteriormente são irredutíveis. Códigos que estão na imagem abaixo.

Figura 4.11: Irredutíveis de grau 2.

```
# MÔNICOS IRREDUTÍVEIS DE GRAU 2.
def irr2(grau, p):
    """>> O irr fornece todos os polinomios monicos
     irredutiveis de grau 2 com coeficientes em Z_p.
    :param grau: grau 2
    :param p: Ordem do corpo.
    :return: retorna uma lista com todos os polinômios
    irredutiveis e mônicos de grau 2
    """
    listap = []
    lista = polmonico2(grau, p)
    for l in lista:
        for i in range(0, p):
            s = 0
            for m in range(0, grau+1):
                s+= l[m]*i**m
# s+= é soma dos monômios é a_mi^m para i variando de 0 a p.
            if s % p == 0:
                listap.append(l)
    listapp = []
# Da lista dos mônicos retiraremos os que possuem raiz em Z_p.
    for l in lista:
        if l not in listap:
            listapp.append(l)
    return listapp
```

Fonte: Autor.

Obtendo assim uma lista com os polinômios mônicos irredutíveis de grau dois. Tomando como exemplo polinômios sobre $\mathbb{Z}_3$ temos um total de três polinômios mônicos irredutíveis que estão na lista abaixo.

Figura 4.12: Exemplo de irredutíveis de grau 2 sobre $\mathbb{Z}_3$.

```
[[1, 0, 1], [2, 1, 1], [2, 2, 1]]
```

Fonte: Autor.

De modo semelhante obtemos os irredutíveis de grau 3.

Figura 4.13: Irredutíveis de grau 3.

```
#DE MODO ANÁLOGO OBTEMOS OS MÔNICOS IRREDUTÍVEIS DE GRAU 3
def irr3(grau, p):
    """>>> O irr fornece todos os polinomios mônicos
    irredutiveis de grau 3 com coeficientes em Z_p.
    :param grau: grau 3
    :param p: Ordem do corpo.
    :return: retorna uma lista com todos os polinômios
    irredutiveis e monicos de grau (grau)
    """
    listap = []
    lista = polmonico3(grau, p)
    for l in lista:
        for i in range(0, p):
            s = 0
            for m in range(0, grau+1):
                s+= l[m]*i**m
            if s % p == 0:
                listap.append(l)
    listapp = []
    for l in lista:
        if l not in listap:
            listapp.append(l)
    return listapp
```

Fonte: Autor.

Para polinômios de grau três sobre $\mathbb{Z}_3$ obtemos um total de oito polinômios mônicos irredutíveis, como mostra a lista abaixo.

Figura 4.14: Exemplo de irredutíveis de grau 2 sobre $\mathbb{Z}_3$.

```
[[1, 0, 2, 1], [1, 1, 2, 1], [1, 2, 0, 1], [1, 2, 1, 1],
 [2, 0, 1, 1], [2, 1, 1, 1], [2, 2, 0, 1], [2, 2, 2, 1]]
```

Fonte: Autor.

Após obter com os códigos citados anteriormente os mônicos irredutíveis de grau dois e três sobre $\mathbb{Z}_3$ e sabendo que os mônicos irredutíveis de grau um sobre Z_3 são $x, x+1$ e $x+2$, podemos então calcular G_1, G_2 e G_3, onde G_i é o produto de todos os polinômios mônicos irredutíveis de grau i, para isto foi feito o programa a seguir.

Figura 4.15: Programa que geram G_1, G_2 e G_3.

```
listapol2 = listapol2(2, 3)
listapol3 = listapol3(3, 3)

list1 = [[0, 1], [1, 1], [2, 1]]
list2 = irr2(2, 3)
list3 = irr3(3, 3)
# Gn é o produto dos polinômios mônicos irredutiveis
# de grau n, neste caso sobre Z_3[x].
G1 = [1]
for l in list1:
    G1 = prodpol(G1, l, 3)

G2 = [1]
for m in list2:
    G2 = prodpol(G2, m, 3)

G3 = [1]
for p in list3:
    G3 = prodpol(G3, p, 3)
#EXEMPLO
print('=='*30)
print(f'Segue a lista dos mônicos irredutíveis de grau 1')
print([[0, 1], [1, 1], [2, 1]])
print(f'O produto entre os mônicos irredutíveis de grau 1 é G1 = {G1}.')
print('=='*30)
print(f'Segue a lista dos mônicos irredutíveis de grau 2')
print(list2)
print(f'O produto entre os mônicos irredutíveis de grau 2 é: \n G2 = {G2}.')
print('=='*30)
print(f'Segue a lista dos mônicos irredutíveis de grau 3')
print(list3)
print(f'O produtos entre os mônicos irredutíveis de grau 3 é: \n G3 = {G3}')
print('--'*30)
print('=='*30)
print(f'O produto entre G1 e G2 é: \n {prodpol(G2, G1, 3)}.')
print(f'O produto entre G1 e G3 é: \n {prodpol(G3, G1, 3)}.')
print(' ')
print('=='*30)
```

Fonte: Autor.

Veja que ao fim do programa acima foi realizado o produto de G_1 por G_2, obtendo assim o polinômio $x^{3^2} - x$ de forma semelhante realizamos o produto de G_1 por G_3 gerando

$x^{3^3} - x$. Vejamos a seguir o console após rodar o programa.

Figura 4.16: Console do programa que geram G_1, G_2 e G_3.

```
============================================================
Segue a lista dos mônicos irredutíveis de grau 1
[[0, 1], [1, 1], [2, 1]]
O produto entre os mônicos irredutíveis de grau 1 é G1 = [0, 2, 0, 1].
============================================================
Segue a lista dos mônicos irredutíveis de grau 2
[[1, 0, 1], [2, 1, 1], [2, 2, 1]]
O produto entre os mônicos irredutíveis de grau 2 é:
 G2 = [1, 0, 1, 0, 1, 0, 1].
============================================================
Segue a lista dos mônicos irredutíveis de grau 3
[[1, 0, 2, 1], [1, 1, 2, 1], [1, 2, 0, 1], [1, 2, 1, 1], [2, 0, 1, 1], [2, 1, 1, 1], [2, 2, 0, 1], [2, 2, 2, 1]]
O produtos entre os mônicos irredutíveis de grau 3 é:
 G3 = [1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1]
------------------------------------------------------------
============================================================
O produto entre G1 e G2 é:
 [0, 2, 0, 0, 0, 0, 0, 0, 0, 1].
O produto entre G1 e G3 é:
 [0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1].

============================================================
```

Fonte: Autor.

Como já visto no trabalho as extensões de $\mathbb{Z}_p$ possui p^n elementos com p primo e ainda é isomorfo ao corpo de decomposição de $x^{p^n} - x$, vejamos que os códigos estão limitados para $n \leq 3$ pois o critério utilizado esta restrito a polinômios de grau dois ou três e assim obtemos polinômios da forma $x^{p^n} - x$ de grau p^2 e p^3 com p primo. Para abranger um pouco mais estas extensões precisamos de um critério de irredutibilidade mais amplo, para isto utilizaremos o critério de Rabin já descrito anteriormente. Assim precisaremos construir dois outros códigos, uma para realizar a divisão de polinômios e outro para determinar o MDC.

Figura 4.17: Inverso em Z_p.

```
    # INVERSO DE t em Z_p
def inverso(t, p):
    """
    :param t: Elemento de Z_p
    :param p: Grau do corpo
    :return: Retorna um elemento o inveros de t em Z_p
    """
    inv = 0
    for n in range(0, p):
        if (n * t) % p == 1:
            inv = n
            break
    return inv
```

Fonte: Autor.

O código a acima será utilizado para construir a divisão, ele tem por objetivo determinar o inverso de um elemento em Z_p com p primo. O algorítimo abaixo realiza a divisão de polinômios da mesma forma coma a qual realizamos cotidianamente utilizando a chave.

Figura 4.18: Divisão de polinômios.

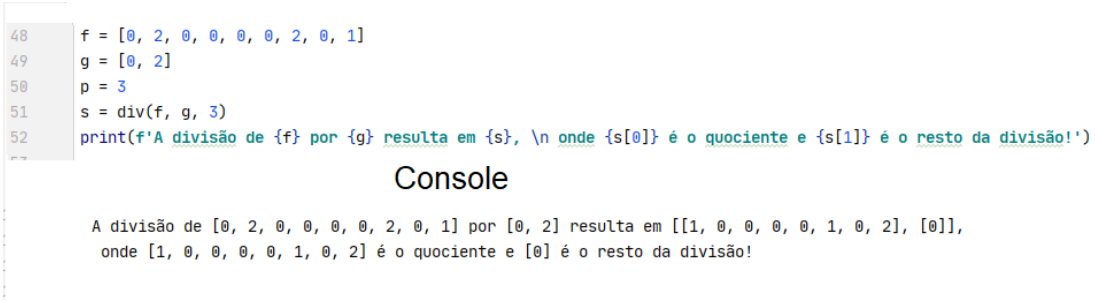
```
        # DIVISÃO DE POLINÔMIOS
def div(f, g, p):
    """>>> Realiza a divisão do polinômio f pelo g:
    :param f: Dividendo
    :param g: Divisor
    :param p: Ordem do corpo.
    :return: Retorna uma lista contendo o quociente e o
    resto da divisão, nesta ordem.
    """
    listaq = []
    listn = []
    listaf = []
    if len(f) >= len(g):
        while len(f) >= len(g):
            q = polnulo(len(f)-len(g))
            q[len(q)-1] = (inverso(g[len(g)-1], p) * (f[len(f)-1])) % p
            sub = prodpol(q, g, p)
            f = subpol(f, sub, p)
            f.pop(len(f)-1)
            listaf.append(f[:])
            listaq.append(q[:])
            q.clear()
    else:
        q = [0]
        listaq.append(q[:])
    for t in range(0, len(f)):
        listn.append(polnulo(t))
# Se f estiver na lista de polinômios nulos o resto é zero.
    if f not in listn:
        for i in range(0, len(f)):
            if f[len(f)-1] == 0:
                f.pop(len(f)-1)

    s = [0]
    for l in listaq:
        s = somapol(s, l, p)
    return [s, f]
```

Fonte: Autor.

Vejamos no exemplo a seguir que o código nos retorna dois polinômios, o quociente e o resto da divisão, ambos necessários para a construção do método para determinar o MDC.

Figura 4.19: Exemplo de divisão de polinômios.



Fonte: Autor.

Para determinar o MDC utilizaremos o método de divisões sucessivas pelo resto, como no código abaixo.

Figura 4.20: MDC de polinômios.

```
3           #MDC DE POLINÔMIOS
4   def mdc(f, g, p):
5       """>>> Calcula o MDC entre dois polinômios.
6       :param f: Polinômio de maior grau.
7       :param g: Polinômio de menor grau
8       :param p: Ordem do corpo Z_p
9       :return: Retorna o MDC entre f e g."""
10      listn = []
11      for t in range(0, len(f)):
12          listn.append(polnulo(t))
13      while True:
14          #print(f' O valor de {f}   e o resto é {g}')
15          if g in listn:
16              break
17          m = div(f, g, p)
18          if len(m[1]) > 0:
19              f = g
20              g = m[1]
21          if len(m[1]) == 0:
22              break
23      if g in listn:
24          mdc = f
25      else:
26          mdc = g
27      return mdc
```

Fonte: Autor.

Neste programa temos um exemplo e ainda o console após rodar o programa.

Figura 4.21: Exemplo de MDC de polinômios.

```
29  # EXEMPLO DE MDC
30  f = [1, 1, 2, 1, 1, 0, 1]
31  g = [1, 1, 2, 1]
32  p = 3
33  mdc = mdc(f, g, 3)
34  print('....No console obtemos....')
35  print(f'O mdc entre {f} e {g} é igual a {mdc}!')
```

```
....No console obtemos....
O mdc entre [1, 1, 2, 1, 1, 0, 1] e [1, 1, 2, 1] é igual a [1]!
```

Fonte: Autor.

O código a seguir gera polinômios do tipo $x^{p^n} - x$, para ser utilizado no algorítimo de Rabin.

Figura 4.22: Polinômios do tipo $x^{p^n} - x$.

```
4   def pn(grau, p):
5       """>>> Gera polinômios do tipo x^(p^n)-x
6       :param grau: Grau de f
7       :param p: Ordem do corpo.
8       :return: Retorna uma lista representando o polinômio x^(p^n)-x
9       """
10      d = [0, -1 + p]
11      for c in range(2, p ** (grau)):
12          d.append(0)
13      d.append(1)
14      return d
```

Fonte: Autor.

Apresentaremos agora um programa capaz de verificar se um polinômio sobre $\mathbb{Z}_p$ é ou não redutível. Este programa trata o algorítimo de Rabin. Posteriormente apresentare-

mos um exemplo.

Figura 4.23: Algorítimo de Rabin.

```
f = [2, 2, 2, 0, 0, 1]
# preciso dos pol nulos para verificar de f divide x^(p^n)-x
nulos = []
for n in range(0, len(f)):
    nulo = polnulo(n)
    nulos.append(nulo[:])
    nulo.clear()
grau = len(f) - 1
p = 3
djs =[]
d = pn(grau, p)
#Abaixo temos a divisão de x^(p^n)-x por f.
div = div(d, f, p)
for j in range(1, grau):
# j divide n vamos calcular os mdcs.
    if grau%j == 0:
        dj = pn(j, p)
        djs.append(dj[:])
mdcs = []
for l in djs:
        m = mdc(f, l, p)
        mdcs.append(m[:])
red = []
# Para que o mdc seja diferente de 1 o len(k) tem de ser maior que 1.
for k in mdcs:
    if len(k)>1:
        red.append(k[:])
#print(red)
if len(red) == 0 and div[1] in nulos:
    #print(div[1])
    print(f'O polinômio {f} é irredutivel')
if len(red) == 0 and div[1] not in nulos:
    print(f'O polinômio {f} é redutivel, pois f não divide x^({p}^{grau})-x')
if len(red)>0:
    for i in red:
        print(f'O polinômio {f} é redutível por {i} ')
```

Fonte: Autor.

Ressaltando que este programa é capaz de verificar se um polinômio qualquer de grau n qualquer é irredutível sobre $\mathbb{Z}_p$ com p primo qualquer. Vejamos alguns exemplos sobre $\mathbb{Z}_3$.

Figura 4.24: Exemplo aplicação do algorítimo de Rabin em $\mathbb{Z}_3$.

```
O polinômio [2, 2, 2, 0, 0, 1] é redutivel, pois f não divide x^(3^5)-x

O polinômio [0, 2, 0, 0, 0, 1] é redutível por [0, 2, 0, 1]

O polinômio [1, 2, 0, 0, 0, 1, 1] é redutível por [1, 1, 0, 1, 2]
```

Fonte: Autor.

Vejamos agora alguns exemplos de polinômios sobre $\mathbb{Z}_5$

Figura 4.25: Exemplo aplicação do algorítimo de Rabin em $\mathbb{Z}_5$.

```
O polinômio [1, 2, 1, 1] é redutível por [1, 4]

O polinômio [1, 2, 4, 1] é redutível por [2, 1]

O polinômio [3, 3, 4, 1] é redutível por [4, 2]

O polinômio [3, 3, 0, 1] é irredutivel

O polinômio [3, 3, 0, 1, 1] é redutível por [1, 4, 3]
```

Fonte: Autor.

Veja que no caso do polinômio $[3, 3, 0, 1, 1]$, $f(x) = 3 + 3x + 0x^2 + x^3 + x^4$ o programa realiza a divisão de $x^{5^4} - x$ por $f(x)$ tarefa inviável sem o uso do programa.

Considerações finais e perspectivas

Nesse trabalho, vimos a importância dos polinômios irredutíveis para obtenção de corpos de números e corpos finitos. A existência de critérios de irredutibilidade de polinômios sobre $\mathbb{Q}$ e $\mathbb{Z}_p$ são de grande importância, porém a criação de um código, utilizando uma linguagem de programação, ajuda nessa tarefa árdua.

A linguagem de programação Python foi escolhida, pois é uma linguagem simples e livre. A ideia de transformar a sistematização dos conceitos matemáticos em um algoritmo em python pode ser estendida a outras teorias matemáticas. Pode-se usar a linguagem python para criar uma calculadora ou reproduzir algoritmos matemáticos em sala de aula, por exemplo. Fazendo assim, as aulas de matemáticas do ensino básico mais interessantes. A importância da lógica matemática também merece destaque, pois sem ela essa sistematização não seria possível.

Entender definições matemáticas e a lógica matemática é crucial para programação e codificação.

Referências Bibliográficas

[1] Araújo, R. R. *Reticulados algébricos e alpicações a códigos e criptografia*. Tese de doutorado. Unicamp - IMECC, Campinas, 2018.

[2] Biazzi, R. N. *Polinômios Irredutíveis: Critérios e Aplicações*. Dissertação de Mestrado do Profmat, 74f. Rio Claro, 2014.

[3] Domingues, H. H., Iezzi, G. *Álgebra Moderna*. 2ª ed. Atual Editora. São Paulo, 1982.

[4] Endler, O. *Teoria dos Corpos*. Publicações Matemáticas. Rio de Janeiro: Impa, 2010.

[5] Foundation, Python Software versão 3. Disponível em: < www.pyhton.org >. Acesso: 26 de fevereiro de 2021.

[6] Guanabara, G. *Curso em vídeo: Python* Disponível em:
< www.youtube.com/watch?v=S9uPNppGsGo&list=PLvE-ZAFRgX8hnE
CDn1v9HNTI71veL3oW0 > Acesso: 26 de fevereiro de 2021.

[7] Hefez, A., Villela, M. L. T. *Códigos Corretores de Erros*. Rio de Janeiro: Impa, 2017.

[8] Masuda, A. M., Panario, D. *Tópicos de Corpos Finitos com Aplicação em Criptografia e Teoria dos Códigos*. 26º Colóquio Brasileiro de Matemática. Rio de Janeiro: Impa, 2007.

[9] Milies, C. P. *Introdução à Teoria dos Códigos Corretores de Erros*. Colóquio de Matemática da Região Centro-Oeste, Departamento de Matemática, UFMS. Campo Grande, 2009.

[10] Roman, S. *Fields Theory*. 2ª ed. Graduate Texts in Mathematics. Springer, 2005.

[11] Samuel, P. *Algebraic Theory od Numbers*. Hermann, Paris, 1970.