Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Polinômios Irredutíveis: Critérios e Aplicações

Ricardo Neves Biazzi

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Carina Alves

2014

512 Biazzi, Ricardo Neves
B579p Polinômios Irredutíveis: Critérios e Aplicações/ Ricardo Neves Biazzi- Rio Claro: [s.n.], 2014.
74 f. : il., figs., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas.
Orientadora: Carina Alves

1. Álgebra. 2. Corpos Finitos. 3. Critérios de Irredutibilidade. 4. Anéis de polinômios. I. Título

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Ricardo Neves Biazzi

Polinômios Irredutíveis: Critérios e Aplicações

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Carina Alves
Orientadora

Profa. Dra. Eliris Cristina Rizziolli
Departamento de Matemática - UNESP - Rio Claro

Profa. Dra. Grasiele Cristiane Jorge
Instituto de Ciência e Tecnologia - UNIFESP - São José dos Campos

Rio Claro, 10 de Março de 2014

À minha mãe e ao meu pai.

Agradecimentos

Inicialmente a Deus por suas bênçãos e graças concedidas.

À minha mãe e ao meu pai que sempre foram minha inspiração, meus incentivadores e motivadores na transposição dos obstáculos que a vida me impôs.

Agradeço especialmente à minha mãe por todo apoio, sabedoria e amor que me deu durante toda a vida, especialmente na acadêmica, período que não estive tão próximo dela quanto queria.

Agradeço à minha namorada por compreender a minha ausência em tantos momentos e permanecer ao meu lado me apoiando com todo seu amor e carinho.

Aos meus colegas do PROFMAT, destacando Ana Cecília, Calixto, Glaucia, Luciano, Mariana, Sibeli e Wellington que tornaram nossos sábados de muito estudo em momentos especiais de muita alegria - obrigado por deixar-me caminhar ao lado de vocês nesta jornada.

Aos que integram o PROFMAT e aos professores do Departamento de Matemática da Unesp Rio Claro.

À Prof^{a}. Dr^{a}. Carina Alves, por toda sua orientação neste trabalho. Agradeço muito por todas suas horas de sono, de finais de semana e de suas férias dedicadas à conclusão deste trabalho - muito obrigado, estava perdido, mas graças a você eu me reencontrei.

A natureza é exatamente simples, se conseguirmos encará-la de modo apropriado... Essa crença tem-me auxiliado, durante toda a minha vida, a não perder as esperanças, quando surgem grandes dificuldades de investigação.

Albert Einstein

Resumo

O conceito de irredutibilidade polinomial é um conceito bastante simples mas muito poderoso. A fatoração de um polinômio como o produto de polinômios irredutíveis tem muitas aplicações. O objetivo deste trabalho foi fazer um estudo dos polinômios irredutíveis. Apresentamos critérios de irredutibilidade e vários resultados pertinentes a este tema.

Palavras-chave: Álgebra, Corpos Finitos, Critérios de Irredutibilidade, Anéis de polinômios.

Abstract

The concept of irreducible polynomial is a very simple but very powerful concept. The factorization of a polynomial as a product of irreducible polynomials have many applications. The aim of this work was to do a study of irreducible polynomials. We present irreducibility criteria and various results relevant to this topic.

Keywords: Algebra, Finite Fields, Irreducibility Criteria, Polynomial Rings.

Sumário

1 Introdução **9**

2 Anéis e Corpos **11**
2.1 Propriedades 11
2.2 Alguns pré-requisitos 13

3 Polinômios e Anéis de Polinômios **19**
3.1 Polinômios 19
3.2 O algoritmo da divisão 23
3.3 Relação entre raízes e polinômios 26
3.4 Método de Kronecker para fatoração em $\mathbb{Z}[X]$ 29

4 Critérios de Irredutibilidade **35**
4.1 Irredutibilidade 35
4.2 Extensões de corpos e irredutibilidade 47
4.2.1 Números algébricos 47
4.2.2 Extensões de dimensões finitas 48

5 Irredutibilidade em Corpos Finitos **52**
5.1 Números de polinômios irredutíveis de grau l sobre $\mathbb{F}_{p^n}$ 52
5.2 Métodos para determinar um polinômio irredutível sobre $\mathbb{F}_{p^n}$ 56

6 Polinômios e suas Aplicações nas Impossibilidades Geométricas **58**
6.1 Números construtíveis e corpos 59
6.2 Números não construtíveis 62
6.3 A impossibilidade de algumas construções geométricas 64

7 Aplicações de Polinômios no Ensino Médio **66**
7.1 Estudo dos números racionais. 66
7.2 Resolução de situações problemas. 69
7.3 Raízes de Polinômios 71

8 Conclusão **72**

1 Introdução

Segundo Garbi [2] e Mario [9], foi pelas mãos de Diofanto, que tem seu período de existência indefinido na obscuridade de uma parte da história que varia entre 150 a.C. e 270 d.C. e chamado algumas vezes de "pai da álgebra", que muitos problemas matemáticos de sua época findaram.

Sua engenhosidade ficou evidenciada em seu tratado, *Arithmetica*, composto por treze livros que tratavam, em sua grande parte, de problemas da teoria dos números, mas que demonstra que Diofanto certamente fez grande contribuição ao desenvolvimento da álgebra.

Após a queda da escola de Alexandria foram os indianos e os árabes que mantiveram acesa a chama do desenvolvimento matemático. Durante esse desenvolvimento surge o nome "álgebra", que significa "restauração", gerado a partir de uma aproximação de parte do título Al-Kitab al-jabr wa'l Muqabalah que foi uma obra popular sobre equações, escritas por Abu-Abdullah Muhamed ibn-Musa al-Khwarizmi a pedido do califa Al-Mamun. Esta obra pode não ter sido revolucionária mas foi a primeira a apresentar de forma sistemática a resolução de equações quadráticas.

Seria impossível falar sobre todos os fatos que se sucederam até a álgebra ser o que conhecemos hoje, mas destacaremos alguns fatos interessantes e importantes que ocorreram neste trajeto.

Com diversos colaboradores, durante o passar dos anos a álgebra foi sendo desenvolvida, pela resolução de problemas ou mesmo por desafios intelectuais lançados, quase sempre buscando a resolução de equações algébricas, ou seja, a busca pelas raízes de polinômios. Um exemplo deste tipo de disputa é a que ocorreu entre Antonio Maria Fior e Nicolò Fontana, também conhecido como Tartaglia. O matemático Scipione del Ferro encontrou uma maneira de resolver uma equação do tipo $x^3 + px + q = 0$, mas morreu antes de publicá-la e foi Fior, seu aluno, que tentou receber os méritos por tal feito utilizando o desafio proposto à Tartaglia.

Tartaglia surpreendeu-o apresentando a resolução de equações do tipo $x^3+px+q = 0$ e uma fórmula geral para a resolução de equações do tipo $x^3 + px^2 + q = 0$. Tal feito foi publicado por seu desleal amigo Girolamo Cardano, quem recebeu os créditos e que dá nome à formula de resolução de equações do terceiro grau.

Algum tempo depois François Viète, que apesar de advogado por formação, inovou a

forma de trabalhar com equações algébricas inserindo o uso de letras nas manipulações algébricas, tornando-se conhecido como o "pai da álgebra moderna".

O estudo da matemática e suas teorias foram aprofundadas nos anos que se seguiram por intelectuais como o matemático René Descartes que foi o responsável pela aceitação de raiz quadrada de número negativo como solução de uma equação algébrica, ou mais adiante na história, o matemático Jean Le Rond d'Alembert enunciou o Teorema Fundamental da Álgebra demonstrado efetivamente por Carl Friedrich Gauss em sua tese de doutorado.

Outros matemáticos como Niels Abel e Évariste Galois desenvolveram importantes teorias relacionadas a resolução de equações algébricas, sendo o último considerado um gênio que desenvolveu um trabalho que o qualifica como principal precursor da álgebra moderna, na qual se insere o objeto de nosso estudo.

Mais especificamente, este trabalho está organizado como se segue:

No Capítulo 2 caracterizamos as estruturas algébricas denominadas: anel e corpo. Ainda neste capítulo traremos algumas definições e resultados importantes para o desenvolvimento do trabalho.

No Capítulo 3 exploramos o conceito de polinômios e anéis de polinômios. Apresentamos o teste da raiz racional e também dois métodos de fatoração de polinômios: o algoritmo da divisão e o método de Kronecker, fornecendo importantes resultados para o estudo dos critérios de irredutibilidade estudados no Capítulo 4.

No Capítulo 4 definimos polinômios irredutíveis e estudamos os diferentes critérios que podem ser utilizados como ferramentas para determinar se um dado polinômio é ou não irredutível sobre um corpo. Além disso, exploramos o conceito de números algébricos e com eles as extensões de dimensão finita, o que nos permitiu, no Capítulo 6, determinar o grau de um polinômio sobre um corpo e assim sua construtibilidade utilizando apenas régua e compasso, num número finito de passos.

No Capítulo 5 exploramos o número de polinômios irredutíveis sobre conceito de corpos finitos e os métodos para determinar sua irredutibilidade. O estudo dos polinômios sobre corpos finitos tem aplicação em eletro comunicações, geometria finita, combinatória, criptografia e teoria dos códigos que podem ser encontradas em [7].

No Capítulo 6 aplicamos os resultados obtidos para apresentar a resposta algébrica aos "Três Problemas Clássicos".

No Capítulo 7 abordamos as diferentes formas de aplicar os resultados obtidos neste trabalho às aulas do ensino médio e até mesmo do ensino fundamental. Apesar de não ter abordado as construções geométricas como uma prática, elas podem ser utilizadas no desenvolvimento de atividades de geometria em sala de aula ou mesmo nos laboratórios de informática, com um software apropriado.

No Capítulo 8 fizemos uma reflexão sobre o que foi abordado e como o desenvolvimento das práticas apresentadas no Capítulo 7 podem contribuir para o aprendizado do aluno.

2 Anéis e Corpos

Neste capítulo estudaremos duas estruturas fundamentais: anéis e corpos.

Dentro desse contexto abordaremos alguns resultados que são pré-requisitos necessários para o desenvolvimento dos demais capítulos.

2.1 Propriedades

Anéis e corpos são conjuntos que satisfazem propriedades detalhadas nesta seção, definindo-os como estruturas algébricas, sobre as quais nosso trabalho será realizado.

Definição 2.1. *Um anel* $(A, +, \cdot)$ *é um conjunto não vazio* A *que possui duas operações, as quais chamaremos de soma* $(+)$ *e produto* $(\cdot)$*, definidas da seguinte maneira:*

$$\begin{array}{rccccc} + : & A & \times & A & \longrightarrow & A \\ & (x,y) & & & \longmapsto & x+y \end{array} \qquad \begin{array}{rccccc} \cdot : & A & \times & A & \longrightarrow & A \\ & (x,y) & & & \longmapsto & x.y \end{array}$$

e que satisfazem as propriedades A1 - A6:

A1) $\forall\ x, y, z \in A, (x + y) + z = x + (y + z)$ *(Associatividade da Soma),*

A2) $\exists\ 0 \in A$ *tal que,* $\forall\ x \in A, 0 + x = x$ *e* $x + 0 = x$ *(Elemento Neutro da Soma),*

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

A4) $\forall\ x, y \in A, x + y = y + x$ *(Comutatividade da Soma),*

A5) $\forall\ x, y, z \in A, (x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(Associatividade do Produto),*

A6) $\forall\ x, y, z \in A, x \cdot (z + y) = x \cdot z + x \cdot y$ *e* $(x + z) \cdot y = x \cdot y + z \cdot y$ *(Distributividade à Direita e à Esquerda),*

Caso o anel (A,+, ·) satisfaça algumas outras propriedades ele é classificado de modo diferenciado.

A7) $\forall\ x, y \in A$*, temos* $x \cdot y = y \cdot x$*.*

Neste caso (A,+, ·) é um Anel Comutativo.

A8) $\forall x \in A, \exists\ 1 \in A$ *tal que* $1 \cdot x = x \cdot 1 = x$.

Neste caso (A,+,·) é um Anel com unidade.

A9) $\forall x, y \in A$, *temos* $x \cdot y = 0 \Rightarrow x = 0$ *ou* $y = 0$.

Neste caso (A,+, ·) é um Anel sem Divisores de Zero.

Caso (A, +, ·) satisfaça A7, A8 e A9 dizemos que (A, +, ·) é um Domínio ou Domínio de Integridade, como podemos ver no exemplo a seguir.

A10) $\forall\ x \in A,\ x \neq 0, \exists\ y \in A$, *tal que* $x \cdot y = y \cdot x = 1$.

Neste caso dizemos que (A,+, ·) é um Corpo.

Exemplo 2.1. Temos que $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são exemplos de Domínios de Integridade, mas apenas $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são corpos.

Exemplo 2.2 (Anel dos inteiros módulo n)**.** Seja n um inteiro positivo. É definida a relação $\equiv\ (mod\ n)$ da seguinte maneira: dados $a, b \in \mathbb{Z}$,

$$a \equiv b\ (mod\ n) \text{ se, e somente se, } a - b \text{ é um múltiplo de } n.$$

A congruência módulo n é uma relação de equivalência, isto é,

$$\begin{cases} a \equiv a\ (mod\ n) \\ a \equiv b\ (mod\ n) \Longrightarrow b \equiv a\ (mod\ n) \\ a \equiv b\ (mod\ n) \text{ e } b \equiv c\ (mod\ n) \Longrightarrow a \equiv c\ (mod\ n). \end{cases}$$

Se $a \in \mathbb{Z}$, então, por definição, sua classe de equivalência módulo n consiste no conjunto

$$\{b \in \mathbb{Z} | b \equiv a\ (mod\ n)\}$$

e ela será denotada por $\overline{a}$ ou $a + n\mathbb{Z}$.

Denotaremos por $\mathbb{Z}_n$ o conjunto das classes de equivalência módulo n, portanto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$.

O conjunto $\mathbb{Z}_n$ em relação às operações assim definidas:

$$\overline{a} + \overline{b} = \overline{a + b} \text{ e } \overline{a} \cdot \overline{b} = \overline{ab}$$

satisfaz as propriedades *A1 - A8*. Portanto $(\mathbb{Z}_n, +, \cdot)$ com as operações $+$ e $\cdot$ definidas em $\mathbb{Z}_n$, é um anel comutativo com unidade.

Observação 2.1. Por questão de simplicidade de linguagem, muitas vezes deixaremos de indicar as operações do anel, escrevendo A para denotar um anel $(A, +, \cdot)$. Também quando não existir ambiguidade, escreveremos ab no lugar de $a \cdot b$.

Seja $(A, +, \cdot)$ um anel e B um subconjunto não vazio de A. Se B for um anel com as operações de A dizemos que B é um *subanel de* A. Se o subanel $(B, +, \cdot)$ de um corpo $(K, +, \cdot)$ é também corpo, dizemos que B é um *subcorpo de* K.

Teorema 2.1. *Sendo $(A, +, \cdot)$ um anel comutativo com unidade, $(A, +, \cdot)$ é um domínio de integridade se, e somente se, todo elemento de $A \setminus \{0\}$ é regular, isto é, obedece a lei do cancelamento para a multiplicação $\cdot$.*

Demonstração. Suponhamos que $(A, +, \cdot)$ seja um domínio de integridade. Sejam x e y elementos quaisquer de A e seja a um elemento de A diferente de 0. Suponhamos que $ax = ay$. Assim, $ax - ay = 0$, e, portanto, $a(x - y) = 0$. Como $a \neq 0$ e $(A, +, \cdot)$ se trata de um domínio de integridade, temos então que $x - y = 0$ e, consequentemente, que $x = y$. Agora, para completarmos a prova, suponhamos que todo elemento de $A \setminus \{0\}$ seja regular para $\cdot$. Entretanto, suponhamos também que existam a e b elementos de A diferentes de 0 tais que $ab = 0$. Temos então que $ab = 0 = a0$; mas, como a é regular para $\cdot$, concluímos que $b = 0$, o que é um absurdo. Assim, vale a lei do anulamento do produto. □

Teorema 2.2. *O anel $(\mathbb{Z}_n, +, \cdot)$ é um domínio de integridade (isto é, sem divisores de zero) se, e somente se, n é um número primo.*

Demonstração. Suponhamos que n não seja um número primo. Então sabemos que $n = ab$ onde $1 < a, b < n$. Agora $n = ab$ implica que $\overline{0} = \overline{n} = \overline{a}\overline{b}$ onde $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$, ou seja, se $n > 2$ não for primo $\mathbb{Z}_n$ possui divisores de zero.

Por outro lado, suponhamos que n é um número primo, $n = p$, e sejam $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Se $\overline{a}\overline{b} = \overline{0}$ vamos provar que $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$ (isto é, $\mathbb{Z}_n$ não possui divisores de zero).

Se $\overline{a}\overline{b} = \overline{0}$ temos $\overline{ab} = \overline{0}$, ou seja, $ab \equiv 0$ módulo p, ou ainda, $p \mid ab$, com isso p divide pelo menos um dos fatores do produto, então

$$p \mid a \text{ ou } p \mid b.$$

Se $p \mid a,\ \overline{a} = \overline{0}$ e se $p \mid b,\ \overline{b} = \overline{0}$, como queríamos demonstrar.

□

2.2 Alguns pré-requisitos

Nesta seção apresentamos alguns resultados relacionados à anéis e corpos e que são pré-requisitos para o desenvolvimento dos demais capítulos.

Teorema 2.3. *Todo domínio de integridade finito é um corpo.*

Demonstração. Seja $(A, +, \cdot)$ um domínio de integridade finito. Como $A \setminus \{0\} \neq \emptyset$, já que ao menos $1 \in A \setminus \{0\}$, tomemos um elemento a de A diferente de 0. Vamos encontrar

um elemento simétrico (inverso multiplicativo) para a em relação a $\cdot$. Definamos a função $f_a : A \longrightarrow A$ por:

$$f_a(r) = ar.$$

Sejam x e y elementos de A. Vamos mostrar que se $x \neq y$ então $f_a(x) \neq f_a(y)$ através da forma contrapositiva.

Suponhamos que $f_a(x) = f_a(y)$. Portanto, $ax = ay$, e, assim, do Teorema 2.1, $x = y$. Mostrado que f_a se trata de uma injeção, notemos que se trata também de uma sobrejeção, já que possui domínio e contradomínio finitos e idênticos, ou seja, f_a é uma bijeção. Assim, $1 \in f_a(A)$, e, deste modo, existe um $r_1 \in A$ tal que $f_a(r_1) = 1$. Notemos, ademais, que

$$f_a(r_1) = ar_1 = 1.$$

Logo, r_1 é simétrico de a em relação a $\cdot$, como procurávamos. □

Teorema 2.4. *Sendo p um número primo, o anel $(\mathbb{Z}_p, +, \cdot)$ é um corpo.*

Demonstração. Do Teorema 2.2 e da definição de anel comutativo, sabemos que $(\mathbb{Z}_p, +, \cdot)$ é um domínio de integridade.

Como $\mathbb{Z}_p$ é um conjunto com p elementos, segue que $(\mathbb{Z}_p, +, \cdot)$ se trata de um domínio de integridade finito e, portanto, do Teorema 2.3, se trata de um corpo. □

Para efeito de simplificar a notação, representamos um corpo por K.

Observação 2.2. Dizemos que um corpo $(K, +, \cdot)$ é finito somente quando K é finito. Ademais, dizemos que $|K|$ é a ordem de $(K, +, \cdot)$.

Exemplo 2.3. Sejam p um primo, $\mathbb{F}_p$ o conjunto $\{0, 1, \cdots, p-1\}$ e $\phi : \mathbb{Z}_p \to \mathbb{F}_p$ a aplicação bijetora definida por $\phi(a + p\mathbb{Z}) = a$. Então $\mathbb{F}_p$ com a estrutura de corpo induzida por $\mathbb{Z}_p$ é um corpo finito de ordem p.

Observação 2.3. Se p é primo e $q = p^n$, com $n \in \mathbb{N}$, então um corpo de ordem q é denotado por $\mathbb{F}_q$.

Definição 2.2. *Seja A um anel. Consideremos o conjunto $A_n = \{a \in A : na = 0\}$, para cada $n \in \mathbb{N}$. Se para qualquer natural n, se tem $A_n \neq A$, diz-se que A tem característica zero e escrevemos $car(A) = 0$. Caso contrário, se existe algum $n \in \mathbb{N}$ tal que $A_n = A$, então a característica de A é o menor natural n_0 tal que $A_{n_0} = A$ e escrevemos $car(A) = n_0$.*

Exemplo 2.4. Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ possuem característica igual a 0, enquanto que o conjunto $\mathbb{Z}_p$ possui característica p.

Lema 2.1. *Num corpo finito K de ordem q, qualquer $a \in K$ satisfaz $a^q = a$.*

Demonstração. Isto é trivial se $a = 0$. Caso contrário, como $K^* = K \setminus \{0\}$ é um grupo multiplicativo de ordem $q-1$, segue que $a^{q-1} = 1$ para todo $a \neq 0$. Logo $a \cdot a^{q-1} = a \cdot 1$ e portanto $a^q = a$. □

Lema 2.2. *Seja K um corpo de característica p. Então, para qualquer $n \geq 0$, temos que*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Demonstração. Usamos indução em n para mostrar que vale a igualdade anterior. Para $n = 1$, observamos que todo coeficiente binomial $\begin{pmatrix} p \\ i \end{pmatrix}$ com $0 < i < p$ na expansão de $(a+b)^p$ é zero, já que

$$\begin{pmatrix} p \\ i \end{pmatrix} = \frac{p(p-1)\cdots(p-i+1)}{i!} \pmod{p}.$$

Segue da hipótese de indução que

$$(a+b)^{p^{n+1}} = ((a+b)^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}.$$

Portanto $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ para todo inteiro $n \geq 0$. □

Teorema 2.5. *Sendo $(K, +, \cdot)$ um corpo, um subconjunto E de K é um subcorpo se, e somente se:*

- *$0 \in E$ e $1 \in E$;*
- *se $x \in E$ e $y \in E$ então $x - y \in E$;*
- *se $x \in E$ e $y \in E \setminus \{0\}$ então $xy^{-1} \in E$.*

Demonstração. p.19, [10] □

Definição 2.3. *Sejam A um anel e I um subconjunto não vazio de A. Dizemos que I é um ideal de A se,*

i. $\forall\ x, y \in I, x + y \in I$,

ii. $\forall\ a \in A, ax \in I,\ \forall\ x \in I$.

Definição 2.4. *Seja A um anel comutativo com unidade.*

i. Um ideal P de A é dito ideal primo se $P \subsetneqq A$ e se

$$\forall x, y \in A \text{ com } xy \in P \Longrightarrow x \in P \text{ ou } y \in P.$$

ii. Um ideal M de A é dito ideal maximal se $M \subsetneqq A$ e se não existe um ideal J tal que

$$M \subsetneqq J \subsetneqq A.$$

Observação 2.4. Um ideal M de A é dito maximal em A se para um J ideal de A com $M \subsetneqq J \subseteqq$ então $J = A$.

Definição 2.5. *Seja $*$ uma operação sobre um conjunto B que possui elemento neutro e. Dizemos que $b \in B$ é um elemento simetrizável para essa operação se existir $b' \in E$ tal que*

$$b' + b = e = b + b'.$$

O elemento b' é chamado simétrico de b para a operação $*$.

Definição 2.6. *Dado a um número inteiro, denomina-se divisor próprio de a todo divisor b de a, com $a \neq b$.*

Definição 2.7. *Diz-se que um elemento a de um anel de integridade A é irredutível se, e somente se, as seguintes condições estiverem verificadas:*

i $a \notin U(A) \bigcup \{0\}$, onde $U(A)$ é o conjunto dos elementos simetrizáveis de A;

ii o conjunto dos divisores próprios de a, representados por $P(a)$ é tal que, $P(a) = \emptyset$, isto é, os únicos divisores de a são os divisores impróprios.

Definição 2.8. *O ideal gerado por um conjunto unitário $\{a\}$ é chamado de ideal principal gerado por a e representado por (a).*

Teorema 2.6. *Seja A um anel comutativo com unidade.*

1. *Um ideal M de A é maximal se e somente se A/M é um corpo.*
2. *Um ideal P de A é primo se e somente se A/P é um domínio de integridade.*
3. *Todo ideal maximal é primo.*
4. *Se A é um domínio de ideais principais, então $A/(p)$ é um corpo se e somente se p é irredutível em A.*
5. *Se A é um domínio de ideais principais e $p \neq 0$, então (p) é um ideal primo se e somente se (p) é um ideal maximal.*

Demonstração. Começaremos com a prova de (1). Seja M um ideal maximal de A. Dado $\alpha \in A \setminus M$, é suficiente mostrar que $\alpha + M$ é invertível em A/M. Para isso, vamos mostrar que $R = \{\alpha r + m : r \in A, m \in M\}$ é um ideal contendo M. Claramente, R é um subgrupo aditivo que contém M. Além disso, para todo $r' \in A$, temos que $(\alpha r + m)r' = (\alpha r r' + m r') \in R$ e portanto R é um ideal. Já que $\alpha \notin M$ e $\alpha = (\alpha \cdot 1 + 0) \in R$, segue que $M \neq R$. Como M é maximal, obtemos que $R = A$. Em particular, $1 = \alpha r + m$ com $r \in A$ e $m \in M$. Portanto, $(\alpha + M)(r + M) = 1 + M$.

Reciprocamente, seja I um ideal de A tal que $I \neq M$ e $M \subseteq I$. Seja $a \in I \setminus M$. Existe $r \in A$ satisfazendo $(a + M)(r + M) = 1 + M$ e assim $ar + m = 1$ para algum $m \in M$. Como $ar + m \in I$, segue que $1 \in I$ e assim $I = A$. Logo M é maximal.

Para demonstrar (2), observamos que o anel quociente A/P é um domínio de integridade se e somente se $(a + P)(b + P) = 0 + P$ implica que $a + P = 0 + P$ ou $b + P = 0 + P$, ou equivalentemente se $ab \in P$ implica que $a \in P$ ou $b \in P$.

Se M é um ideal maximal de A então A/M é um corpo por (1), logo também é um domínio de integridade. Por (2), concluímos que o ideal M é primo. Isto prova (3).

Para a prova de (4), suponhamos que (p) seja maximal e que $p = ab$. Então $(p) \subseteq (a)$, o que implica que $(a) = (p)$ ou $(a) = A$. No primeiro caso, temos que $a = pr$ para algum $r \in A$, isto é $p = prb$, ou equivalentemente, $p(1 - rb) = 0$. Como A é um domínio de integridade, segue que $rb = 1$, ou seja, b é invertível. No caso em que $(a) = A$, temos que a é invertível, pois $1 \in A$ e portanto $ra = 1$ para algum $r \in A$. Em qualquer caso, temos que p é irredutível.

Reciprocamente, suponhamos que p seja irredutível. Então p não é invertível e portanto $(p) \neq A$. Suponhamos que $(p) \subseteq (a)$. Segue que $p = ar$ onde $r \in A$. Como p é irredutível, obtemos que a ou r é invertível, o que implica que $(a) = A$ ou $(a) = (p)$. Logo (p) é maximal.

Finalmente, provamos (5). Sabemos que os ideais maximais são primos por (3). Então, basta provarmos que (p) primo implica que (p) seja maximal quando $p \neq 0$. De acordo com (4), é suficiente demonstrar que p é irredutível. Suponhamos que $p = ab$. Então, $ab = p \in (p)$ e portanto $a \in (p)$ ou $b \in (p)$. Suponhamos sem perda de generalidade que $a \in (p)$, ou seja, $a = pc$ com $c \in A$. Portanto, $p = pcb$, isto é, $p(1 - cb) = 0$. Como $p \neq 0$, temos que $cb = 1$, logo b é invertível. Concluímos que p é irredutível e assim (p) é maximal por (4). □

Teorema 2.7. *Dados A e S anéis. Se $\phi : A \longrightarrow S$ é um homomorfismo de anéis, então $A/ker\phi$ é isomorfo a $\phi(A)$.*

Demonstração. Vamos mostrar que a aplicação $\Phi : A/ker\phi \longrightarrow \phi(A)$ com $\Phi(r + ker\phi) = \phi(r)$ é um isomorfismo de anéis. Primeiramente, veremos que Φ está bem definida e é injetora. Sejam $r_1, r_2 \in A$. Temos que $r_1 + ker\phi = r_2 + ker\phi$ se e somente se $\phi(r_1 - r_2) = 0$, o que é equivalente a $\phi(r_1) = \phi(r_2)$. Como ϕ é um homomorfismo, segue imediatamente que Φ também é um homomorfismo. Além disso, Φ é claramente sobrejetora.

□

Teorema 2.8. *O subcorpo primo de um corpo K é isomorfo a $\mathbb{Z}_p$ ou a $\mathbb{Q}$ de acordo com a característica de K ser um número primo ou zero.*

Demonstração. Seja $\phi : \mathbb{Z} \longrightarrow K$ o homomorfismo de anéis definido por $\phi(n) = n \cdot 1_K$. O núcleo de ϕ é $(carK)\mathbb{Z}$. Se $carK = p$ para algum p primo, então, pelo Teorema 2.7, $\phi(\mathbb{Z}) \cong \mathbb{Z}_p$ que é um corpo primo. Se $carK = 0$, então ϕ é injetora. Neste caso, $\phi(\mathbb{Z})$ é um anel isomorfo a $\mathbb{Z}$. Definimos agora $\phi' : \mathbb{Q} \longrightarrow K$ por $\phi'(m/n) = (m \cdot 1_K)(n \cdot 1_K)^{-1}$, se $n \neq 0$. Temos que ϕ' é um homomorfismo injetor. Com efeito,

$$\begin{aligned} \phi'\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) &= ((m_1n_2 + m_2n_1) \cdot 1_K)((n_1n_2) \cdot 1_K)^{-1} \\ &= (m_1 \cdot 1_K)(n_1 \cdot 1_K)^{-1} + (m_2 \cdot 1_K)(n_2 \cdot 1_K)^{-1} \\ &= \phi'\left(\frac{m_1}{n_1}\right) + \phi'\left(\frac{m_2}{n_2}\right) \end{aligned}$$

e

$$\begin{aligned} \phi'\left(\frac{m_1}{n_1} \cdot \frac{m_2}{n_2}\right) &= ((m_1m_2) \cdot 1_K)((n_1n_2) \cdot 1_K)^{-1} \\ &= (m_1 \cdot 1_K)(n_1 \cdot 1_K)^{-1}(m_2 \cdot 1_K)(n_2 \cdot 1_K)^{-1} \\ &= \phi'\left(\frac{m_1}{n_1}\right) \cdot \phi'\left(\frac{m_2}{n_2}\right). \end{aligned}$$

Além disso, se $\phi'(m/n) = 0$ então $m1_K = 0$ e portanto $m = 0$, já que $carK = 0$. Concluímos que $\phi'(\mathbb{Q})$, que é o menor subcorpo de K contendo 1_K, é isomorfo ao corpo primo $\mathbb{Q}$. □

3 Polinômios e Anéis de Polinômios

Evariste Galois delineou pela primeira vez o conceito de grupo, associando a cada equação um grupo de permutações das raízes da equação. Com isso, observou-se que os polinômios e as estruturas algébricas modernas do século XIX estavam relacionados. Algum tempo depois os polinômios foram formalizados sobre anéis e não demorou muito para que surgisse o conceito de anéis de polinômios.

Neste capítulo estudaremos os polinômios e os anéis de polinômios. Abordaremos também o algoritmo de divisão de polinômios e sua relação com as raízes de um polinômio.

3.1 Polinômios

No que segue, em todo este capítulo, indicaremos por A um anel comutativo com unidade. Um *Polinômio* numa variável sobre A é uma sequência quase nula em que $f = (a_0, a_1, a_2, \cdots, a_n, \cdots)$ em que $a_i \in A,\ \forall i \in \mathbb{N}$.

Considere $\mathcal{A} = \{f; f$é uma sequência quase nula em $A\}$. No conjunto $\mathcal{A}$ definimos

$$\begin{array}{rccc} \oplus: & \mathcal{A} \times \mathcal{A} & \longrightarrow & \mathcal{A} \\ & ((a_0, a_1, a_2, \cdots), (b_0, b_1, b_2, \cdots)) & \longmapsto & (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots) \end{array}$$

$$\begin{array}{rccc} \odot: & \mathcal{A} \times \mathcal{A} & \longrightarrow & \mathcal{A} \\ & ((a_0, a_1, a_2, \cdots), (b_0, b_1, b_2, \cdots)) & \longmapsto & (c_0, c_1, c_2, \cdots), \end{array}$$

onde

$$\begin{cases} c_0 = a_0 b_0 \\ c_1 = a_0 b_1 + a_1 b_0 \\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 \\ \vdots \\ c_n = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_{n-1} b_1 + a_n b_0 \\ \vdots \end{cases}$$

Vamos verificar que $(\mathcal{A}, \oplus, \odot)$ é um anel. Para tanto sejam $f = (a_0, a_1, a_2, \cdots, a_n \cdots)$, $g = (b_0, b_1, b_2, \cdots, b_m, \cdots), h = (c_0, c_1, c_2, \cdots, c_k, \cdots)$ quaisquer em $\mathcal{A}$.

A1) Associatividade: $(f \oplus g) \oplus h = f \oplus (g \oplus h)$.

De fato,

$$\begin{aligned}(f \oplus g) \oplus h &= ((a_0, a_1, a_2, \cdots) \oplus (b_0, b_1, b_2, \cdots)) \oplus (c_0, c_1, c_2, \cdots) \\ &= ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, \cdots) \\ &= (a_0 + b_0 + c_0, a_1 + b_1 + c_1, \cdots) \\ &= (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), \cdots) \\ &= (a_0, a_1, a_2, \cdots) \oplus ((b_0, b_1, b_2, \cdots) \oplus (c_0, c_1, c_2, \cdots)) \\ &= f \oplus (g \oplus h).\end{aligned}$$

A2) Elemento neutro da soma: $\exists\ e \in \mathcal{A}$ tal que $f \oplus e = f = e \oplus f$.

De fato, como A é um anel, temos que $0 \in A$, logo $(0, 0, 0, 0, \cdots) \in \mathcal{A}$, tomando $e = (0, 0, 0, 0, \cdots)$, temos que

$$\begin{aligned}e \oplus f &= (0, 0, 0, 0, \cdots) \oplus (a_0, a_1, a_2, \cdots) \\ &= (0 + a_0, 0 + a_1, 0 + a_3, \cdots) \\ &= (a_0 + 0, a_1 + 0, a_3 + 0, \cdots) \\ &= (a_0, a_1, a_2, \cdots) \oplus (0, 0, 0, 0, \cdots) \\ &= f \oplus e \\ &= (a_0, a_1, a_3, \cdots) \\ &= f.\end{aligned}$$

Assim temos que o polinômio $e = (0, 0, 0, \cdots)$ é o elemento neutro da soma, também chamado de polinômio nulo.

A3) Elemento Oposto: $\exists\ p \in \mathcal{A}$ tal que $f \oplus p = e = p \oplus f$.

Se tomarmos $p = -f = (-a_0, -a_1, -a_2, \cdots)$, onde $-a_i \in A, \forall\ i \in \mathbb{N}$, pois A é um anel, temos

$$\begin{aligned}f \oplus p &= (a_0 + (-a_0), a_1 + (-a_1), a_2 + (-a_2), \cdots) \\ &= (a_0 - a_0, a_1 - a_1, a_2 - a_2, \cdots) \\ &= ((-a_0) + a_0), (-a_1) + a_1, (-a_2) + a_2, \cdots) \\ &= p \oplus f \\ &= (0, 0, 0, \cdots).\end{aligned}$$

A4) Comutatividade da soma: $f \oplus g = g \oplus f$.

De fato,

$$\begin{aligned}f \oplus g &= (a_0, a_1, a_2, \cdots) \oplus (b_0, b_1, b_2, \cdots) \\ &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \cdots) \\ &= (b_0 + a_0, b_1 + a_1, b_2 + a_2, \cdots) \\ &= (b_0, b_1, b_2, \cdots) \oplus (a_0, a_1, a_2, \cdots) \\ &= g \oplus f.\end{aligned}$$

A5) Associatividade do Produto: $(f \odot g) \odot h = f \odot (g \odot h)$.

De fato,

$$\begin{aligned}(f \odot g) \odot h &= ((a_0, a_1, a_2, \cdots) \odot (b_0, b_1, b_2, \cdots)) \odot (c_0, c_1, c_2, \cdots) \\ &= (a_0b_0, a_0b_1 + a_1b_0, \cdots) \odot (c_0, c_1, c_2, \cdots) \\ &= ((a_0b_0)c_0, (a_0b_1)c_0 + (a_1b_0)c_0 + (a_0b_0)c_1, \cdots) \\ &= (a_0(b_0c_0), a_0(b_1c_0) + a_1(b_0c_0) + a_0(b_0c_1), \cdots) \\ &= (a_0, a_1, a_2, \cdots) \odot ((b_0, b_1, b_2, \cdots) \odot (c_0, c_1, c_2, \cdots)) \\ &= f \odot (g \odot h)\end{aligned}$$

A6) Distributividade à Direita e à Esquerda: $f \odot (g \oplus h) = f \odot g \oplus f \odot h$.

De fato,

$$\begin{aligned}f \odot (g \oplus h) &= (a_0, a_1, a_2, \cdots, a_n, \cdots) \odot (b_0 + c_0, b_1 + c_1, b_2 + c_2, \cdots) \\ &= (a_0(b_0 + c_0), a_0(b_1 + c_1) + a_1(b_0 + c_0), \cdots) \\ &= (a_0b_0 + a_0c_0, a_0b_1 + a_0c_1 + a_1b_0 + a_1c_0, \cdots) \\ &= (a_0b_0, a_0b_1 + a_1b_0, \cdots) + (a_0c_0, a_0c_1 + a_1c_0, \cdots) \\ &= f \odot g \oplus f \odot h.\end{aligned}$$

Portanto $(\mathcal{A}, \oplus, \odot)$ satisfaz as propriedades *A1, A2, A3, A4, A5* e *A6* definidas anteriormente, logo temos que $(\mathcal{A}, \oplus, \odot)$ é um anel.

Vejamos também que $(\mathcal{A}, \oplus, \odot)$ satisfaz a propriedade comutativa da multiplicação.

A7) Comutatividade da Multiplicação: $f \odot g = g \odot f$.

De fato,

$$\begin{aligned}f \odot g &= (a_0, a_1, a_2, \cdots, a_n, 0, \cdots) \odot (b_0, b_1, b_2, \cdots, b_m, 0, \cdots) \\ &= (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \cdots) \\ &= (b_0a_0, b_0a_1 + b_1b_0, b_0a_2 + b_1a_1 + b_2a_0, \cdots) \\ &= (b_0, b_1, b_2, \cdots, b_m, 0, \cdots) \odot (a_0, a_1, a_2, \cdots, a_n, 0, \cdots).\end{aligned}$$

A8) Elemento neutro da Multiplicação: $\exists\ 1_{\mathcal{A}} \in \mathcal{A}$ tal que $1_{\mathcal{A}} \odot f = f = f \odot 1_{\mathcal{A}}$.
De fato, tomando $1_{\mathcal{A}} = (1_A, 0, 0, 0, \cdots, 0, \cdots)$, temos que

$$\begin{aligned}f \odot 1_{\mathcal{A}} &= (a_0, a_1, a_2, \cdots, a_n, 0, \cdots) \odot (1_A, 0, 0, 0, \cdots, 0, \cdots) \\ &= (a_01_A, a_00 + a_11_A, a_00 + a_10 + a_21_A, \cdots, a_n1_A, 0, \cdots) \\ &= (a_0, a_1, a_2, \cdots, a_n, 0, \cdots) \\ &= f \\ &= (a_0, a_1, a_2, \cdots, a_n, 0, \cdots) \\ &= (1_Aa_0, 0a_0 + 1_Aa_1, 0a_0 + 0a_1 + 1_Aa_2, \cdots, 1_Aa_n, 0, \cdots) \\ &= (1_A, 0, 0, 0, \cdots, 0, \cdots) \odot (a_0, a_1, a_2, \cdots, a_n, 0, \cdots) \\ &= 1_{\mathcal{A}}.f\end{aligned}$$

Portanto $1_{\mathcal{A}} \odot f = f = f \odot 1_{\mathcal{A}}$.

Assim $(\mathcal{A}, \oplus, \odot)$ é um anel comutativo com unidade.

Por razões de ordem prática utilizaremos o símbolo X para representar o termo $(0, 1, 0, 0, 0 \cdots)$, além disso, quando nos referirmos ao elemento $(a_i, 0, 0, 0, \cdots)$ utilizaremos o símbolo a_i, sendo assim, a_i será utilizado para representar $a_i \in A$ e $(a_i, 0, 0, 0, \cdots) \in \mathcal{A}$.

A partir deste momento as operações $\oplus$ e $\odot$ passarão a ser representadas por $+$ e $\cdot$, que representarão a adição e multiplicação em A e em $\mathcal{A}$.

Com essas convenções podemos representar o elemento $(a_0,\ a_1,\ \cdots, a_n, 0, \cdots) \in \mathcal{A}$ pela soma $a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n$, onde a_iX^i designa $a_i \cdot X^i$.

Denotaremos o anel $(\mathcal{A}, +, \cdot)$ por $A[X]$ e será chamado de anel de polinômios na indeterminada X com coeficientes em A.

Dizemos que dois polinômios $p(X),\ q(X) \in A[X]$, onde $p(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n$ e $q(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + \cdots + b_nX^n$, são iguais se, e somente se, $a_i = b_i, i = 0, 1, 2, 3, \cdots, n$.

Para efeito de simplificar a notação, representamos o polinômio identicamente nulo $q(X) = 0 + 0X + 0X^2 + 0X^3 + \cdots + 0X^n$ por e ou 0 e o chamaremos de *polinômio identicamente nulo* sobre A.

Se $p(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n$, com $a_0 = a$ e $a_i = 0,\ \forall\ i = 1, 2, 3, \cdots, n$, então $p(X)$ é um *polinômio constante* e o representamos por $p(X) = a$. No caso em que $p(X) = 1$, este é o polinômio constante 1 e a unidade em $A[X]$.

Dizemos que um elemento u de A é raiz de $p(X)$ se, e somente se, $p(u) = 0$.

Observação 3.1. Dado $f(X) = \sum_{i=0}^{n} a_iX^i \in A[X]$, podemos considerar a função polinomial associada $\tilde{f} : A \longrightarrow A$, definida por $\tilde{f}(\alpha) = \sum_{i=0}^{n} a_i\alpha^i$.

A função $\phi_\alpha : A[X] \longrightarrow A$ definida por $\phi_\alpha\left(\sum_{i=0}^{n} a_iX^i\right) = \sum_{i=0}^{n} a_i\alpha^i$ é um homomorfismo de $A[X]$ em A e $\phi_\alpha(X) = \alpha$. O homomorfismo ϕ_α é a avaliação de $f(X)$ em α.

É bom observar que um polinômio diferente de zero pode ter a função identicamente nula como função polinomial associada; esse é o caso com $f(X) := \overline{1} \cdot X + \overline{1} \cdot X^2 \in \mathbb{Z}_2[X]$ pois

$$\tilde{f}(\overline{0}) = \overline{1} \cdot \overline{0} + \overline{1} \cdot \overline{0}^2 = \overline{0}$$
$$\tilde{f}(\overline{1}) = \overline{1} \cdot \overline{1} + \overline{1} \cdot \overline{1}^2 = \overline{1} + \overline{1} = \overline{0}.$$

Definição 3.1. *Seja $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n$ um polinômio não nulo sobre A, dizemos que o número natural n é o grau de $f(X)$, representado por $\partial f(X)$, se $a_n \neq 0$ e $a_i = 0,\ \forall i > n$. O termo a_n é denominado coeficiente dominante de $f(X)$. Caso $a_n = 1, f(X)$ é chamado de polinômio unitário ou mônico.*

Exemplo 3.1. $X^2 - 2$ é mônico, mas $3X^2 - 6$ não é.

Teorema 3.1. *Para quaisquer polinômios não nulos $f(X)$ e $g(X)$ de $A[X]$, temos:*

i. se $f(X) + g(X) \neq 0$ então $\partial(f(X) + g(X)) \leq max\{\partial f(X), \partial g(X)\}$

ii. se o coeficiente dominante de $f(X)$ ou de $g(X)$ é regular em A, então $\partial(f(X).g(X)) = \partial f(X) + \partial g(X)$.

Demonstração.

i. Se $f(x) = 0$ ou $g(x) = 0$, nada temos a provar. Seja $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n$ e $g(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + \cdots + b_mX^m$, polinômios não nulos de grau n e m, respectivamente. Suponha, sem perda de generalidade que $n > m$, neste caso o termo dominante de $f(X) + g(X)$ será a_n e assim $\partial(f(X) + g(X)) = n = max\{\partial f(X), \partial g(X)\}$. Caso $n = m$, temos que o termo dominante de $f(x) + g(x)$ será $a_n + b_n$, deste modo $\partial(f(X) + g(X)) = n$ caso $a_n + b_n \neq 0$ ou $\partial(f(X) + g(X)) \leq n$ caso $a_n + b_n = 0$.

ii. Seja $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots + a_nX^n$ e $g(X) = b_0 + b_1X + b_2X^2 + b_3X^3 + \cdots + b_mX^m$, polinômios não nulos de grau n e m, respectivamente. Por definição temos que $f(X).g(X) = c_0 + c_1X + c_2X^2 + \cdots + c_kX^k$, onde $c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i$. Temos que $a_i = 0, \forall i > n$ e $b_i = 0, \forall i > m$, assim $c_{n+m} = a_nb_m$ e $c_{n+m} \neq 0$, pois a_n ou b_m é um elemento regular. Observe que se $i > m+n$, c_i será a soma de termos do tipo a_ib_{i-j}, com $i = j + (i-j) > m+n$, implicando que, ou $j > n$ ou $i - j > m$, assim o produto $a_ib_{i-j} = 0, \forall i > n + m$. Concluindo que o maior número natural k tal que $c_i \neq 0, \forall i > k$ é $k = n + m$.

Portanto $\partial(f(X).g(X)) = m + n = \partial f(X) + \partial g(X)$.

□

Corolário 3.1. *$A[X]$ é um domínio de integridade se, e somente se, A é um domínio de integridade.*

Demonstração. p.11, [17]. □

3.2 O algoritmo da divisão

Nesta seção apresentamos o algoritmo da divisão e sua relação com raízes de polinômios. Um polinômio dividido por outro resulta em um polinômio no quociente e um polinômio no resto, o procedimento para isto é chamado de *algoritmo da divisão para polinômios*. Veremos, ainda no Capítulo 3, que existe uma relação direta entre o conceito de divisibilidade polinomial e irredutibilidade polinomial.

Exemplo 3.2. Dividir o polinômio $X^3 + 2X^2 + 3X + 4$ pelo polinômio $X + 1$, irá resultar em um quociente e um resto em $\mathbb{Q}[X]$.

$$\begin{array}{rl|l} X^3 + 2X^2 + 3X + 4 & & X + 1 \\ \cline{3-3} -X^3 - X^2 & & X^2 + X + 2 \\ \cline{1-1} \quad X^2 + 3X + 4 & & \\ \quad -X^2 - X & & \\ \cline{1-1} \quad 2X + 4 & & \\ \quad -2X - 2 & & \\ \cline{1-1} \quad 2 & & \end{array}$$

Observe que:

$$dividendo = divisor \cdot quociente \ + \ resto$$

$$X^3 + 2X^2 + 3X + 4 = (X + 1)X^2 + (X^2 + 3X + 4)$$

$$X^2 + 3X + 4 = (X + 1)X + (2X + 4)$$

$$2X + 4 = (X + 1)2 + 2.$$

O grau do resto deve ser menor que o grau do divisor para que o processo de divisão seja finalizado.

Exemplo 3.3. Encontrar o quociente e o resto da divisão do polinômio $f(X) = 10X^5 + 6X^4 - 6X^3 + 3X^2 - 3X + 1$ pelo polinômio $d(X) = 2X^2 + 1$ em $\mathbb{Z}_5$. Temos

$$f(X) = 10X^5 + 6X^4 - 6X^3 + 3X^2 - 3X + 1 \equiv X^4 + 4X^3 + 3X^2 + 2X + 1 \ (mod\ 5).$$

$$\begin{array}{rl|l} X^4 + 4X^3 + 3X^2 + 2X + 1 & & 2X^2 + 1 \\ \cline{3-3} -X^4 - 0X^3 - 3X^2 - 0X - 0 & & 3X^2 + 2X \\ \cline{1-1} \quad 4X^3 + 2X + 1 & & \\ \quad -4X^3 - 2X - 0 & & \\ \cline{1-1} \quad 1 & & \end{array}$$

Logo, podemos escrever:

$$X^4 + 4X^3 + 3X^2 + 2X + 1 = (3X^2 + 2X).(2X^2 + 1) + 1 \ (mod\ 5).,$$

obtendo $q(X) = 3X^2 + 2X$ e $r(X) = 1$.

Nos ateremos agora aos anéis sobre corpos. Isso se faz necessário para a construção do embasamento teórico que se segue. Note que a demonstração do teorema a seguir é muito parecida com a utilizada para mostrar a validade do algoritmo da divisão para números inteiros.

Teorema 3.2. *(Algoritmo da divisão para polinômios.)*

Considere A um anel de integridade. Se $f(X)$ e $g(X)$ estão em $A[X]$ e $g(X) \neq 0$, então existem únicos $q(X)$ e $r(X)$ em $A[X]$ tais que:

$$f(X) = q(X)g(X) + r(X)$$

onde $r(X) = 0$ ou $\partial r(X) < \partial g(X)$.

Demonstração. Seja $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, $\partial f(X) = n$ e $g(X) = b_0 + b_1X + b_2X^2 + \cdots + b_mX^m, \partial g(X) = m$.

Existência: Se $f(X) = 0$ basta tomar $q(X) = r(X) = 0$. Suponha que $f(X) \neq 0$ e $\partial f(X) = n$. Caso $n < m$ basta tomar $q(X) = 0$ e $r(X) = f(X)$, portanto assumiremos que $n \geq m$.

Seja $f_1(X) = f(X) - a_nb_m^{-1}X^{n-m}.g(X)$, então $\partial f_1(X) < \partial f(X)$.

A demonstração será realizada por indução sobre $\partial f(X)$. Caso $n = 0$ e como $n \geq m$ segue que $m = 0$ e assim $f(X) = a_0 \neq 0, g(X) = b_0 \neq 0$, logo $f(X) = a_0b_0^{-1}g(X)$, obtendo assim $q(X) = a_0b_0^{-1}$ e $r(X) = 0$.

Tomando $f_1(X) = q_1(X).g(X) + r(X)$, onde $r(X) = 0$ ou $\partial r(X) < \partial g(X)$, temos que $f(X) - a_nb_m^{-1}X^{n-m}.g(X) = q_1(X)g(X) + r(X)$ e consequentemente $f(X) = (q_1(X) + a_nb_m^{-1}X^{n-m}).g(X) + r(X)$.

Utilizando $q(X) = (q_1(X)+a_nb_m^{-1}.X^{n-m})$, obtemos $f(X) = q(X).g(X)+r(X)$ onde $q(X), r(X) \in K[X]$ e $r(X) = 0$ ou $\partial r(X) < \partial g(X)$.

Unicidade: Sejam $q_1(X), q_2(X), r_1(X), r_2(X)$, tais que $f(X) = q_1(X).g(X)+r_1(X)$ e $f(X) = q_2(X).g(X) + r_2(X)$, onde $r_i(X) = 0$ ou $\partial r_i(X) < \partial g(X), i = 1, 2$.

Deste modo, temos que $q_1(X).g(X)+r_1(X)-(q_2(X).g(X)+r_2(X)) = f(X)-f(X)$, ou seja, $q_1(X).g(X) + r_1(X) - q_2(X).g(X) - r_2(X) = 0$, logo

$$(q_1(X) - q_2(X)).g(X) = r_2(X) - r_1(X).$$

Caso $q_1(X) \neq q_2(X)$, temos

$$\begin{aligned} \partial(r_2(X) - r_1(X)) &= \partial(g(X).(q_1(X) - q_2(X)) \\ &= \partial(g(X)) + \partial(q_1(X) - q_2(X)) \\ &\geq \partial g(X) \end{aligned}$$

Por outro lado, $\partial(r_2(X)-r_1(X)) \leq max\{\partial r_1(X), \partial r_2(X)\} \leq \partial g(X)$, o que nos leva a uma contradição.

Portanto $q_1(X) = q_2(X)$ e consequentemente, $r_1(X) = r_2(X)$, provando a unicidade de $q(X)$ e $r(X)$. □

Definição 3.2. *Seja K um corpo. Dados $f(X), g(X) \in K[X]$, se existe um único polinômio mônico $d(X) \in K[X]$ tal que*

(a) $d(X)$ *divide* $f(X)$ *e* $g(X)$,

(b) qualquer polinômio $h(X) \in K[X]$ *dividindo ambos* $f(X)$ *e* $g(X)$ *também divide* $d(X)$.

Este polinômio $d(X)$ *é o máximo divisor comum de* $f(X)$ *e* $g(X)$*, denotado por* $mdc(f(X), g(X))$.

Observação 3.2. O $mdc(f(X), g(X))$ é o polinômio mônico de maior grau dentre os polinômios que dividem ambos $f(X)$ e $g(X)$ em $K[X]$.

Teorema 3.3 (Teorema de Bézout)**.** *Dados dois polinômios* $f(X),\ g(X) \in K[X]$*, existem polinômios* $r(X),\ s(X) \in K[X]$ *tais que* $f(X)r(X) + g(X)s(X) = mdc(f(X), g(X))$.

Demonstração. Análogo ao caso $K = \mathbb{Z}$, p.40, [1]. □

Exemplo 3.4. Consideremos os polinômios $f(X) = X^6 + 5X^4 + 3X^3 + 2X^2 + 3X + 2$ e $g(X) = X^3 + 2X^2 + 3X + 2$ pertencentes a $\mathbb{Z}_7$. Temos

$$f(X) = (X^3 + 5X^2 + 6X + 2) \cdot g(X) + (5X^2 + 6X + 5) \text{ e}$$
$$g(X) = (3X + 1)(5X^2 + 6X + 5) + (3X + 4).$$

Como

$$(5X^2 + 6X + 5) = (4X + 6)(3X + 4) + 2,$$

logo, $mdc(f(X), g(X)) = 2$. Além disso temos

$$\begin{aligned} 2 &= (5X^2 + 6X + 5) + (3X + 1)(3X + 4) \\ &= (5X^2 + 6X + 5) + (3X + 1)[(4X + 6)(5X^2 + 6X + 5) + g(X)] \\ &= (3X + 1) \cdot g(X) + (5X^2 + X)(5X^2 + 6X + 5) \\ &= (3X + 1) \cdot g(X) + (5X^2 + X) \cdot [f(X) + (6X^3 + 2X^2 + X + 5)] \\ &= (5X^2 + X) \cdot f(X) + (2X^5 + 2X^4 + 5X^2 + X + 1) \cdot g(X), \end{aligned}$$

logo,

$$r(X) = 6X^2 + 4X \text{ e } s(X) = X^5 + X^4 + 6X^2 + 4X + 4.$$

3.3 Relação entre raízes e polinômios

Uma das consequências do Algoritmo da Divisão é o resultado clássico sobre o número máximo de raízes de um polinômio não-nulo.

Proposição 3.1. *Sejam* K *um corpo e* $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ *um polinômio não nulo em* $K[X]$*, com* $\partial f(X) = n$*. Então* $f(X)$ *tem no máximo* n *raízes em* K*, onde* $n = \partial f(X)$.

Demonstração. Caso $\nexists\ a \in K$ tal que $f(a) = 0$, a proposição está provada.

Seja $a \in K$ tal que $f(a) = 0$.

Temos que $g(X) = X - a \in K[X]$, logo, pelo algoritmo da divisão, temos que $\exists\ q(X), r(X) \in K[X]$ tais que $f(X) = q(X).(X - a) + r(X)$, onde $r(X) = 0$ ou $\partial r(X) < \partial g(X) = 1$, e, neste caso, $r(X) = b_0$ é um polinômio constante. Como $f(X) = q(X).(X-a)+b_0$ e $f(a) = 0$ temos que $b_0 = 0$. Como $\partial f(X) = \partial q(X)+\partial(X-a)$ segue que $\partial q(X) = n - 1$.

Sabemos que K é um corpo, logo se $b \in K$ temos $f(b) = (b - a).q(b) = 0 \Rightarrow b = a$ ou b é raiz de $q(X) \in K[X]$. Assim as raízes de $f(X)$ são as raízes de $q(X)$ e a.

Para finalizar a demonstração utilizamos indução sobre n. Se $n = 0, f$ não possui raízes em K e nesse caso não há o que demonstrar.

Suponhamos que vale para $q(X)$ com $\partial q(X) = n - 1$, ou seja, $q(X)$ possui no máximo $n - 1$ raízes em K.

Por construção $f(X) = q(X).g(X)$ e como as raízes de $q(X)$ e a são as raízes de $f(X)$ segue que, $f(X)$ possui no máximo n raízes.

□

Corolário 3.2. *Sejam $f(X)$ e $g(X)$ polinômios em $K[X]$, onde K é um corpo com número infinito de elementos. Temos*

$$f(X) = g(X) \text{ se, e somente se, } f(a) = g(a),\ \forall a \in K.$$

Demonstração. Suponhamos que, $f(X) = g(X)$ e pela definição de polinômios, temos que $f(X) - g(X) = 0$, assim, $\forall\ a \in K$, a função polinomial $h(X) = f(X) - g(X) = 0$, ou seja,$\forall\ a \in K,\ f(a) = g(a)$.

Por outro lado, considere $h(X) = f(X) - g(X) \in K[X]$. Por hipótese temos que $\forall\ a \in K,\ f(a) = g(a)$, logo $h(a) = 0\ \forall a \in K$, como K é infinito, segue que $h(X) = 0$, ou seja, $f(X) = g(X)$. □

Proposição 3.2. *Se um número complexo α é uma raiz de um polinômio não nulo $f(X) \in K[X]$ então α é uma raiz de um polinômio mônico $g(X) \in K[X]$ com $\partial g(X) = \partial f(X)$.*

Demonstração. Seja α uma raiz de um polinômio $f(X) = a_0+a_1X^1+a_2X^2+\cdots+a_nX^n$ com $\partial f(X) = n$ e $a_i \in K, i = \{1, 2, 3, \cdots, n\}$. Tome

$$g(X) = \frac{1}{a_n}f(X) = \frac{a_0}{a_n} + \frac{a_1}{a_n}X^1 + \frac{a_2}{a_n}X^2 + \cdots + X^n.$$

Todos os coeficientes de $g(X)$ estão em K, pois K é um corpo, portanto $g(X) \in K[X]$, além disso, obtemos g(X) mônico tendo α como uma raiz e o mesmo grau n de $f(X)$. □

Apresentamos inicialmente o teste da raiz racional e em seguida, estudamos as raízes dos polinômios em $\mathbb{Z}$, visto que qualquer polinômio em $\mathbb{Q}$ pode ser reescrito com coeficientes em $\mathbb{Z}$, bastando para isso, multiplicar todo o polinômio pelo mínimo múltiplo comum dos denominadores do polinômio em $\mathbb{Q}$.

Teorema 3.4 (Teste da raiz racional)**.** *Seja $f(X) \in \mathbb{Z}[X]$ um polinômio de grau n tal que*

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

para algum $a_0, a_1, a_2, \ldots, a_n \in \mathbb{Z}$, com $a_n \neq 0$.

Se β é um número racional, escrito como $\beta = \frac{r}{s}$, β é uma raiz de $f(X)$, e com r e s sem fatores em comum exceto pelo 1 e -1, ou seja, o máximo divisor comum de r e s é 1, então:

(i) r é um fator de a_0.

(ii) s é um fator de a_n.

Demonstração. Como $\beta = \frac{r}{s}$ é raiz de $f(X)$, segue que

$$a_0 + a_1\left(\frac{r}{s}\right) + a_2\left(\frac{r}{s}\right)^2 + \ldots + a_n\left(\frac{r}{s}\right)^n = 0.$$

Multiplicando ambos os membros por s^n temos

$$a_0s^n + a_1rs^{n-1} + a_2r^2s^{n-2} + \ldots + a_nr^n = 0.$$

Logo

$$a_0s^n = -r\left(a_1s^{n-1} + a_2rs^{n-2} + \ldots + a_nr^{n-1}\right).$$

Portanto r é um fator de a_0s^n.

Como r e s não tem fator em comum exceto pelo 1 e -1, implica que r é um fator de a_0.

Um processo análogo nos fornece a igualdade

$$a_nr^n = -s\left(a_0s^{n-1} + a_1rs^{n-2} + \ldots + a_{n-1}r^{n-1}\right),$$

logo s é um fator de a_n.

□

Exemplo 3.5. Vamos mostrar que o número real $\sqrt[5]{2}$ não é racional.

Note que $\sqrt[5]{2}$ é raiz do polinômio $f(X) = X^5 - 2$ em $\mathbb{Z}[X]$, portanto podemos utilizar o teste da raiz racional para averiguar se o polinômio possui raízes em $\mathbb{Q}$.

Utilizando o teste da raiz racional temos que r deve ser um fator de 2 e s um fator de -1. Logo as possibilidades para $\frac{r}{s}$ são $1, -1, 2, -2$.

Desta forma temos que ± 1 e ± 2 são as únicas possíveis de raízes de $f(X)$ em $\mathbb{Q}$, porém ao substituirmos X por ± 1 e ± 2, veremos que não são raízes de $f(X)$.

Portanto $\sqrt[5]{2}$ é raiz de $f(X) \in \mathbb{Z}[X]$, mas não está em $\mathbb{Q}$.

Definição 3.3. *Seja K um corpo. Um polinômio $f(X) \in K[X]$ é dito ter um fator de grau 1 em $K[X]$ se*

$$f(X) = (aX + b) \cdot g(X)$$

onde $a, b \in K$, com $a \neq 0$ e $g(X) \in K[X]$.

Teorema 3.5. *Seja K um corpo. Um polinômio $f(X) \in K[X]$ possui um fator de grau 1 em $K[X]$ se, e somente se, $f(X)$ tem uma raiz em K.*

Demonstração. Assuma que $f(X)$ tem fator de grau 1. Utilizando a notação da Definição 3.3, obtemos que $\frac{-b}{a} \in K$ é uma raiz de $f(X)$ pois

$$f\left(\frac{-b}{a}\right) = \left(a\left(\frac{-b}{a}\right) + b\right) \cdot g\left(\frac{-b}{a}\right) = 0.g\left(\frac{-b}{a}\right) = 0.$$

Reciprocamente, assuma que $\alpha \in K$ é uma raiz de $f(X)$.

Se dividirmos $f(X)$ por $X - \alpha$ então, pelo Teorema 3.2, existirá $q(X)$, $r(X)$ em $K[X]$ com

$$f(X) = (X - \alpha)\, q(X) + r(X), \tag{3.1}$$

onde

$$r(X) = 0 \text{ ou } \partial\, r(X) \ < \ \partial\,(X - \alpha) = 1.$$

Deste modo, $r(X)$ deve ser um polinômio constante $c \in K \subseteq K[X]$, assim podemos reescrever a igualdade (3.1) como

$$f(X) = (X - \alpha)\, q(X) + c. \tag{3.2}$$

Substituindo X por α na equação (3.2) e utilizando o fato de que $f(\alpha) = 0$, obtemos que

$$0 = f(\alpha) = (\alpha - \alpha)\, q(\alpha) + c = 0 + c = c.$$

Portanto da equação (3.2) temos

$$f(X) = (X - \alpha)\, q(X),$$

logo $f(X)$ tem o fator $(X - \alpha)$ de grau 1 em $K[X]$. □

3.4 Método de Kronecker para fatoração em $\mathbb{Z}[X]$

Descreveremos a seguir, o método de Kronecker, que nos permite fatorar um polinômio $p(X) \in \mathbb{Z}[X]$. Este método é simples de ser realizado, porém exige muitos cálculos, isto o torna extenso e assim nada eficiente.

O método de Kronecker será apresentado utilizando exemplos que nos permitirão entender o seu algoritmo. Este método consiste na busca dos polinômios divisores de $p(X)$, em que esses possuem grau menor do que o grau de $p(X)$.

Dado um polinômio $p(X)$ de grau n analisaremos separadamente seus possíveis divisores.

- Procura dos polinômios divisores de $p(X)$ de grau 1.

  Suponha que $q(X) = aX + b$, com $q(X) \in \mathbb{Z}[X]$ seja um fator de $p(X)$, ou seja, temos $p(X) = (aX + b).q(X)$.

  Dado $\beta \in \mathbb{Z}$ temos que $p(\beta) = (a\beta + b)q(\beta)$ e assim $(a\beta + b)|p(\beta)$. Reduzimos essa fatoração à busca dos valores de a e b de modo que a fatoração seja possível.

  Como β é arbitrário, tomando dois inteiros β e ϕ com $\beta \neq \phi$, tais que $p(\beta) \neq 0$ e $p(\phi) \neq 0$ obtemos duas igualdades que dependem de a e b o que nos fornece sistemas de equações como:

$$\begin{cases} a\beta + \text{b} = d_1 \\ a\phi + \text{b} = d_2. \end{cases}$$

  onde d_1 é um divisor de $p(\beta)$ e d_2 é um divisor de $p(\phi)$. Assim obtemos todos os possíveis candidatos a divisores da forma $aX + b$ de $p(X)$. Observe que a escolha de β e ϕ, utilizados acima, deve levar em consideração que quanto menor for o número de divisores de $p(\beta)$ e de $p(\phi)$, menor será o número de sistemas de equações que teremos que resolver.

- Procura dos polinômios divisores de $p(X)$ de grau 2.

  Para determinar fatores quadráticos de $p(X)$, da forma $aX^2 + bX + c$ de $p(X) \in \mathbb{Z}[X]$, tome três inteiros β, ϕ e γ, dois a dois distintos, e tais que nenhum deles seja raiz de $p(X)$. Se $aX^2 + bX + c$ é um divisor de $p(X) \in \mathbb{Z}[X]$, devemos ter,

$$\begin{cases} a\beta^2 + b\beta + \text{c} = d_1 \\ a\phi^2 + b\phi + \text{c} = d_2 \\ a\gamma^2 + b\gamma + \text{c} = d_3 \end{cases}$$

  onde d_1 é um divisor de $p(\beta)$, d_2 é um divisor de $p(\phi)$ e d_3 é um divisor de $p(\gamma)$. Com a resolução deste sistema de equações obtemos os possíveis candidatos a divisores da forma $aX^2 + bX + c$ de $p(X)$, onde devemos ser criteriosos com relação à escolha dos valores de β, ϕ e γ.

- A determinação dos divisores de $p(X)$ com grau maior do que 2 segue processo análogo ao realizado até agora.

  Para ficar mais claro o que foi trabalhado até este momento sobre o método de Kronecker para fatoração de polinômios em $\mathbb{Z}[X]$ vamos apresentar alguns exemplos:

Exemplo 3.6. A forma fatorada de $p(X) = X^4 + 2X^3 + X^2 - 1$ é $p(X) = (X^2 + X + 1)(X^2 + X - 1)$.

Utilizando o teste da raiz racional podemos verificar que este polinômio não admite raízes racionais, assim este polinômio pode possuir apenas fatores quadráticos ou ser irredutível, visto que seus fatores devem estar em $\mathbb{Z}[X]$. Utilizando o que foi estudado com relação à escolha de β, ϕ e γ, tomamos $\beta = 0$, $\phi = 1$ e $\gamma = -1$, obtendo assim os sistemas:

$$\begin{cases} a \cdot 0^2 + b \cdot 0 + \mathrm{c} = d_1 \\ a \cdot 1^2 + b \cdot 1 + \mathrm{c} = d_2 \\ a \cdot (-1)^2 + b \cdot (-1) + \mathrm{c} = d_3. \end{cases}$$

Temos $p(0) = -1$, $p(1) = 3$ e $p(-1) = -1$ o que nos fornece $d_1 = \pm 1$, $d_2 = \pm 1, \pm 3$ e $d_3 = \pm 1$.

Para obter todas as combinações possíveis variando os valores de d_1, d_2 e d_3 utilizaremos a seguinte tabela:

	d_1	d_2	d_3	a	b	c
1	1	1	1	0	0	1
2	1	1	-1	-1	1	1
3	1	-1	1	-1	-1	1
4	1	-1	-1	-2	0	1
5	1	3	1	1	1	1
6	1	3	-1	0	2	1
7	1	-3	1	-2	-2	1
8	1	-3	-1	-3	-1	1
9	-1	1	1	2	0	-1
10	-1	1	-1	1	1	-1
11	-1	-1	1	1	-1	-1
12	-1	-1	-1	0	0	-1
13	-1	3	1	3	1	-1
14	-1	3	-1	2	2	-1
15	-1	-3	1	0	-2	-1
16	-1	-3	-1	-1	-1	-1

Temos que $p(X)$ é mônico, assim seus fatores também são pelo fato de pertencerem a $\mathbb{Z}[X]$, ou seja, os coeficientes das linhas 1, 4, 6, 7, 8, 9, 12, 13, 14 e 15 devem ser excluídos. Testando os demais polinômios obtemos que $X^2 + X + 1$ e $X^2 + X - 1$ dividem $p(X)$. Portanto podemos escrever $P(X) = (X^2 + X + 1).(X^2 + X - 1)$.

Exemplo 3.7. A forma fatorada de $p(X) = X^5 + X^3 + X^2 + 1$ é $p(X) = (X + 1)(X^2 - X + 1)(X^2 + 1)$.

Utilizando o teste da raiz racional podemos verificar que este polinômio admite -1 como raiz racional, assim este polinômio possui um fator de grau 1. Efetuando a divisão de $p(X)$ por $X+1$ obtemos o polinômio $X^4-X^3+2X^2-X+1$ que não possui raízes racionais, logo não possui fatores de grau 1 em $\mathbb{Z}[X]$.

Caso o polinômio seja redutível vamos determinar os fatores quadráticos de $X^4 - X^3 + 2X^2 - X + 1$ em $\mathbb{Z}[X]$.

Utilizando o que foi estudado com relação à escolha de β, ϕ e γ, tomamos $\beta = 0$, $\phi = 1$ e $\gamma = -1$, obtendo assim os sistemas:

$$\begin{cases} a\cdot 0^2 + b\cdot 0 + \mathrm{c} = d_1 \\ a\cdot 1^2 + b\cdot 1 + \mathrm{c} = d_2 \\ a\cdot(-1)^2 + b\cdot(-1) + \mathrm{c} = d_3. \end{cases}$$

Temos $p(0) = 1$, $p(1) = 2$ e $p(-1) = 6$ o que nos fornece $d_1 = \pm 1$, $d_2 = \pm 1, \pm 2$ e $d_3 = \pm 1, \pm 2, \pm 3, \pm 6$.

Para obter todas as combinações possíveis variando os valores de d_1, d_2 e d_3 utilizaremos a seguinte tabela:

	d_1	d_2	d_3	a	b	c
1	1	1	1	0	0	1
2	1	1	-1	-1	1	1
3	1	1	2	0,5	-0,5	1
4	1	1	-2	-1,5	1,5	1
5	1	1	3	1	-1	1
6	1	1	-3	-2	2	1
7	1	1	6	2,5	-2,5	1
8	1	1	-6	-3,5	3,5	1
9	1	-1	1	-1	-1	1
10	1	-1	-1	-2	0	1
11	1	-1	2	-0,5	-1,5	1
12	1	-1	-2	-2,5	0,5	1
13	1	-1	3	0	-2	1
14	1	-1	-3	-3	1	1
15	1	-1	6	1,5	-3,5	1
16	1	-1	-6	-4,5	2,5	1
17	1	2	1	0,5	0,5	1
18	1	2	-1	-0,5	1,5	1
19	1	2	2	1	0	1

	d_1	d_2	d_3	a	b	c
20	1	2	-2	-1	2	1
21	1	2	3	1,5	-0,5	1
22	1	2	-3	-1,5	2,5	1
23	1	2	6	3	-2	1
24	1	2	-6	-3	4	1
25	1	-2	1	-1,5	-1,5	1
26	1	-2	-1	-2,5	-0,5	1
27	1	-2	2	-1	-2	1
28	1	-2	-2	3	0	1
29	1	-2	3	-0,5	-2,5	1
30	1	-2	-3	-3,5	0,5	1
31	1	-2	6	1	-4	1
32	1	-2	-6	-5	2	1
33	-1	1	1	2	0	1
34	-1	1	-1	1	1	-1
35	-1	1	2	2,5	-0,5	-1
36	-1	1	-2	0,5	1,5	-1
37	-1	1	3	3	-1	-1
38	-1	1	-3	0	2	-1
39	-1	1	6	4,5	-2,5	-1
40	-1	1	-6	-1,5	3,5	-1
41	-1	-1	1	1	-1	-1
42	-1	-1	-1	0	0	-1
43	-1	-1	2	1,5	-1,5	-1
44	-1	-1	-2	-0,5	0,5	-1
45	-1	-1	3	2	-2	-1
46	-1	-1	-3	-1	1	-1
47	-1	-1	6	3,5	-3,5	-1
48	-1	-1	-6	-2,5	2,5	-1
49	-1	2	1	2,5	0,5	-1
50	-1	2	-1	1,5	1,5	-1
51	-1	2	2	3	0	-1
52	-1	2	-2	1	2	-1
53	-1	2	3	3,5	-0,5	-1
54	-1	2	-3	0,5	2,5	-1
55	-1	2	6	5	-2	-1
56	-1	2	-6	-1	4	-1
57	-1	-2	1	0,5	-1,5	-1

	d_1	d_2	d_3	a	b	c
58	-1	-2	-1	-0,5	-0,5	-1
59	-1	-2	2	1	-2	-1
60	-1	-2	-2	-1	0	-1
61	-1	-2	3	1,5	-2,5	-1
62	-1	-2	-3	-1,5	0,5	-1
63	-1	-2	6	3	-4	-1
64	-1	-2	-6	-3	2	-1

Como $p(X) \in \mathbb{Z}[X]$ é mônico, segue que seus únicos divisores possíveis são: $X^2 + X + 1, X^2 - X + 1, -X^2 - X + 1, X^2 + 1, -X^2 + 2X + 1, -X^2 - 2X + 1, X^2 - 4X + 1, X^2 + X - 1, X^2 - X - 1, -X^2 + X - 1, X^2 + 2X - 1, -X^2 + 4X - 1, X^2 - 2X - 1, -X^2 - 1$.

Testando as possibilidades de polinômios, verificamos que os polinômios $X^2 - X + 1$ e $X^2 + 1$ são fatores de $p(X)$.

Obtemos assim que $p(X) = X^5 + X^3 + X^2 + 1 = (X + 1)(X^2 - X + 1)(X^2 + 1)$.

4 Critérios de Irredutibilidade

Se K é corpo, os anéis de integridade $K[X]$ apresentam importantes semelhanças algébricas com o anel $\mathbb{Z}$ dos números inteiros. O conceito de polinômio irredutível corresponde, no anel dos inteiros, ao de número primo.

Neste capítulo estudaremos a definição de polinômio irredutível e alguns critérios de irredutibilidade.

4.1 Irredutibilidade

Apresentamos a seguir a definição que contribuiu para o foco do presente trabalho. O conceito de irredutibilidade polinomial é um conceito bastante simples, mas muito poderoso.

Definição 4.1. *Dizemos que um polinômio não constante $f(X)$ é irredutível em $K[X]$ (ou irredutível sobre K) se é impossível expressar $f(X)$ como um produto $g(X)h(X)$ de dois polinômios $g(X)$ e $h(X)$ em $K[X]$ cujos graus são ambos maiores ou iguais a 1.*

Um polinômio $f(X) \in K[X]$, não constante e não irredutível, chama-se redutível ou composto.

Exemplo 4.1. O polinômio $X^2 - 2$ é redutível sobre $\mathbb{R}$.

Observe que

$$X^2 - 2 = \left(X - \sqrt{2}\right)\left(X + \sqrt{2}\right)$$

onde cada um dos fatores de $X^2 - 2$ pertencem a $\mathbb{R}[X]$ e tem grau menor que $X^2 - 2$.

Exemplo 4.2. O polinômio $X^2 - 2$ é irredutível sobre $\mathbb{Q}$.

Para mostrar isto suponha o contrário, que $X^2 - 2$ não é irredutível sobre $\mathbb{Q}$. Isto significa que

$$X^2 - 2 = (aX + b)(cX + d)$$

com a, b, c e $d \in \mathbb{Q}$. Claramente nem a e nem c, podem ser zero. Como $\sqrt{2}$ é raiz de $X^2 - 2$, substituindo X por $\sqrt{2}$ em ambos os membros da igualdade, obtemos

$$0 = \left(a\sqrt{2} + b\right)\left(c\sqrt{2} + d\right).$$

A igualdade acima nos fornece que $\sqrt{2} = \frac{-b}{a}$ ou $\sqrt{2} = \frac{-d}{c}$, chegando a contradição que $\sqrt{2}$ é racional.

Exemplo 4.3. Todo polinômio de grau 1 sobre um corpo K é irredutível.

Se um polinômio é irredutível sobre um corpo, então é irredutível sobre todos os subcorpos deste corpo, ou seja, se E é um subcorpo de K e $f(X) \in K[X]$ é irredutível sobre K, então $f(X)$ é irredutível sobre E.

Observação 4.1. Os polinômios constantes não são redutíveis e nem irredutíveis sobre um corpo, porém todos os outros polinômios tem de ser redutíveis ou irredutíveis sobre um corpo.

Teorema 4.1. *Seja $p(X)$ um polinômio irredutível em $K[X]$. Se $a(X), b(X) \in K[X]$ são tais que $p(X)|a(X)b(X)$, então $p(X)|a(X)$ ou $p(X)|b(X)$.*

Demonstração. Suponha que $p(X)$ não divide $a(X)$, e seja $d(X) = mdc(p(X), a(X))$. Como $p(X)$ é irredutível e não divide $a(X)$, segue que o grau de $d(X)$ não pode ser maior que zero. Logo $d(X) = 1$. Pelo teorema de Bézout, existem $r(X)$ e $s(X)$ tais que $a(X)r(X) + p(X)s(X) = 1$. Multiplicando a igualdade acima por $b(X)$ e observando que $p(X)|a(X)b(X) \iff a(X)b(X) = p(X)q(X)$ para algum $q(X)$, obtemos $a(X)b(X)r(X) + p(X)b(X)s(X) = b(X) \iff p(X)(q(X)r(X) + b(X)s(X)) = b(X)$, isto é, $p(X)|b(X)$. □

Observe que o passo principal na demonstração acima é observar que $mdc(p(X), a(X)) = 1$. Assim, temos o seguinte resultado: se $p(X)|a(X)b(X)$ e $mdc(p(X), a(X)) = 1$, então $p(X)|b(X)$, com a mesma demonstração dada acima.

O próximo resultado é a versão para polinômios do *Teorema Fundamental da Aritmética.*

Teorema 4.2. *Todo polinômio de grau maior ou igual a 1 em $K[X]$ pode ser fatorado em $K[X]$ como um produto de polinômios irredutíveis. Esta fatoração é única, a menos da ordem dos fatores e da multiplicação por constantes não nulas de K.*

Demonstração. Seja $p(X) \in K[X]$ um polinômio de grau maior ou igual a 1. Se $p(X)$ for irredutível, não há o que fazer (ele já está fatorado como produto de irredutíveis).

Caso contrário, escrevemos $p(X) = a(X)b(X)$, com $a(X)$ e $b(X)$ ambos de grau menor que o grau de $p(X)$. Se $a(X)$ e $b(X)$ forem irredutíveis, a fatoração termina. Caso contrário, repetimos este processo até obtermos uma fatoração de $p(X)$ como um produto de irredutíveis (o leitor mais experiente percebe que a formalização deste argumento envolve uma indução finita, mas a ideia é clara). Resta ainda mostrar a unicidade da fatoração. Suponha que

$$p(X) = q_1(X)q_2(X)\cdots q_m(X) = r_1(X)r_2(X)\cdots r_n(X)$$

são duas fatorações de $p(X)$ como produto de polinômios irredutíveis e $m \leq n$. É uma consequência do Teorema 4.1 que $q_1(X)$ divide algum dos polinômios $r_j(X)$, e podemos assumir sem perda de generalidade que $j = 1$. Então $q_1(X)|r_1(X)$. Mas $r_1(X)$ é irredutível, logo $r_1(X) = uq_1(X)$, com $u \in K$. Substituindo $r_1(X)$ na equação destacada anteriormente e cancelando, ficamos com

$$q_2(X) \cdots q_m(X) = u_1 r_2(X) \cdots r_n(X).$$

Repetindo o argumento, eventualmente chegamos em

$$1 = u_1 \cdots u_m r_{m+1}(X) \cdots r_n(X),$$

o que só é possível se $m = n$. Logo os fatores irredutíveis $q_i(X)$ e $r_i(X)$ são os mesmos a menos da ordem e de constantes de K. □

Os critérios de irredutibilidade podem variar de acordo com o corpo sobre o qual está sendo estudado, em que possuem características específicas, como por exemplo a irredutibilidades sobre corpos finitos que veremos a seguir.

Definição 4.2. *Seja K um corpo. Se todo polinômio não constante de $K[X]$ tem pelo menos uma raiz em K, diz se que K é um corpo algebricamente fechado.*

Exemplo 4.4. O exemplo mais familiar de corpo algebricamente fechado é o corpo $\mathbb{C}$ dos números complexos, [1].

Definição 4.3. *O conjugado de um número complexo $z = a + bi$ é $\overline{z} = a - bi$.*

Proposição 4.1. *Seja $f(X) = a_0 + a_1X + \cdots + a_nX^n$ um polinômio sobre $\mathbb{R}$. Se o número complexo z é raiz de $f(X)$ então $\overline{z}$ também é raiz desse polinômio.*

Demonstração. Por hipótese:

$$f(z) = a_0 + a_1 z + \cdots + a_n z^n = 0.$$

Então, pelas propriedades dos números complexos, temos

$$\begin{aligned}
f(\overline{z}) &= \overline{a_0} + \overline{a_1}(\overline{z}) + \overline{a_2}(\overline{z}^2) + \cdots + \overline{a_n}(\overline{z}^2) \\
f(\overline{z}) &= \overline{a_0} + \overline{a_1}(\overline{z}) + \overline{a_2}(\overline{z^2}) + \cdots + \overline{a_n}(\overline{z^n}) \\
f(\overline{z}) &= \overline{a_0} + \overline{a_1 z} + \overline{a_2 z^2} + \cdots + \overline{a_n z^n} \\
f(\overline{z}) &= \overline{a_0 + a_1 z + \cdots + a_n z^n} \\
f(\overline{z}) &= \overline{0} \\
f(\overline{z}) &= 0.
\end{aligned}$$

□

Proposição 4.2. *Um polinômio sobre um corpo K algebricamente fechado é irredutível se, e somente se, tem grau* 1.

Demonstração. Seja $f(X) \in K[X]$ um polinômio irredutível. Como K é algebricamente fechado, existe $u \in K$ tal que $f(u) = 0$. Logo, $x - u | f(X)$ e, portanto, existe $g(X) \in K[X]$ tal que

$$f(X) = (X - u)g(X).$$

Como, porém $f(X)$ é irredutível, então o polinômio $g(X)$ é constante não nulo, isto é, existe $a \in K$ tal que $g(X) = a$, para todo $x \in K$. Portanto:

$$f(X) = aX - au$$

em que au é constante. Logo, o grau de $f(X)$ é 1.

Por outro lado, seja $f(X) \in K[X]$ é um polinômio de grau 1, suponhamos que $f(X) = g(X) \cdot h(X)$, com $g(X), h(X) \in K[X]$, então $\partial(f(X)) = \partial(g(X)) + \partial(h(X))$. Mas como $\partial(f(X)) = 1$, então $\partial(g(X)) + \partial(h(X)) = 1$. Como essa igualdade só é possível se $\partial(g(X)) = 0$ e $\partial(h(X)) = 1$ ou $\partial(g(X)) = 1$ e $\partial(h(X)) = 0$, segue pela Definição 4.1 que $f(X)$ é irredutível sobre K. □

Proposição 4.3. *Seja K um corpo algebricamente fechado e $f(X)$ um polinômio com $\partial(f(X)) \geq 1$ sobre K cujo coeficiente dominante denotaremos por a. Então podem ser determinados elementos $u_1, u_2, \cdots, u_n \in K$ tais que*

$$f(X) = a(X - u_1)(X - u_2) \cdots (X - u_n).$$

Demonstração. A demonstração será realizada por indução sobre n. Se o $\partial(f(X)) = 1$, então $f(X) = aX + b$, com $a \neq 0$. Pondo a em evidência, temos:

$$f(X) = a\left(X - \frac{b}{a}\right)$$

o que demonstra o teorema para $n = 1$.

Seja $f(X)$ um polinômio de grau $n > 1$ e suponhamos a proposição verdadeira para todo polinômio $f(X)$ com $\partial(f(X)) = n - 1$. Como K é algebricamente fechado, $f(X)$ tem uma raiz em u_1 em K e, portanto:

$$f(X) = (X - u_1)q(X)$$

para um conveniente $q(X) \in K[X]$, com $\partial(q(X)) = n - 1$ e coeficiente dominante igual ao de $f(X)$. Pela hipótese de indução, existem $u_2, u_3, \cdots, u_n \in K$ tais que

$$q(X) = a(X - u_2)(X - u_3) \cdots (X - u_n)$$

e que a é o coeficiente dominante de $q(X)$ e portanto de $f(X)$. Concluimos assim que

$$f(X) = a(X - u_1)(X - u_2) \cdots (X - u_n).$$

□

A Proposição 4.2 garante que os únicos polinômios irredutíveis em $\mathbb{C}$ são os de grau 1, pois $\mathbb{C}$ é algebricamente fechado. O mesmo, porém, não vale em $\mathbb{R}[X]$: o polinômio $f(X) = X^2 + 1$, por exemplo, é irredutível sobre $\mathbb{R}$. De fato, se não o fosse teria uma raiz em $\mathbb{R}$, devido ao Teorema 3.5. Mas sabemos que as raízes de $f(X) = X^2 + 1$ são i e $-i$, que não pertencem ao conjunto dos números reais.

Teorema 4.3. *Teorema Fundamental da Álgebra Todo polinômio não nulo $p(X) \in \mathbb{C}$ raiz em $\mathbb{C}$.*

Demonstração. p.71, [**?**]. □

É uma consequência do Teorema Fundamental da Álgebra que os únicos polinômios irredutíveis em $\mathbb{C}[X]$ são os polinômios de grau 1.

Proposição 4.4. *Um polinômio $f(X) \in \mathbb{R}[X]$ é irredutível sobre $\mathbb{R}$ se, e somente se, $\partial(f(X)) = 1$ ou $\partial(f(X)) = 2$ e seu discriminante, definido como $\Delta = b^2 - 4ac$, é menor que zero.*

Demonstração. Suponhamos que, $f(X)$ é irredutível sobre $\mathbb{R}$. Devido ao Teorema Fundamental da Álgebra, $f(X)$ tem uma raiz $\alpha \in \mathbb{C}$. Há então duas possibilidades. Uma delas é $\alpha \in \mathbb{R}$. Neste caso, $(X - \alpha)|f(X)$, o que equivale a dizer que

$$f(X) = (X - \alpha)q(X)$$

para um conveniente $q(X) \in \mathbb{R}[X]$. Porém, como $f(X)$ é irredutível, isso obriga $q(X)$ a ser constante não nulo, digamos $q(X) = c$, com $c \in \mathbb{R}$, para $\forall x \in \mathbb{R}$. Logo:

$$f(X) = cx - c\alpha$$

o que mostra que $\partial(f(X)) = 1$.

A outra possibilidade é $\alpha \notin \mathbb{R}$, ou seja, $\alpha = a + bi$, com $b \neq 0$. Neste caso, devido a Proposição 4.1, $\overline{\alpha}$ também é raiz de $f(X)$. Então $f(X)$ é divisível em $\mathbb{C}$ por $(X - \alpha)$ e $(X - \overline{\alpha})$ e, portanto, por

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - 2aX + (a^2 + b^2)$$

que é um polinômio com coeficientes reais. Então existe $q(X) \in \mathbb{C}$ tal que

$$f(X) = [X^2 - 2aX + (a^2 + b^2)]q(X).$$

Por outro lado, como $X^2 - 2aX + (a^2 + b^2)$ é um polinômio real, pode-se usar o algoritmo euclidiano em $\mathbb{R}[X]$ para o par formado por esse polinômio, como divisor, e $f(X)$ como dividendo. Se $q_1(X)$ e $r(X)$ são respectivamente o quociente e o resto, então

$$f(X) = [X^2 - 2aX + (a^2 + b^2)]q_1(X) + r(X).$$

Mas, lembrando o fato de que $q_1(X)$ e $r(X)$ também pertencem a $\mathbb{C}[X]$ e a unicidade do quociente e do resto, concluímos que $q_1(X) = q(X)$ e $r(X) = 0$, e assim $q(X) \in \mathbb{R}[X]$. Então, como $f(X)$ é irredutível sobre $\mathbb{R}$, segue que o polinômio real $q(X)$ é constante, digamos $q(X) = c$, para algum $c \in \mathbb{R}^*$.

Obtemos assim que

$$\begin{aligned} f(X) &= [X^2 - 2aX + (a^2 + b^2)]q(X) \\ f(X) &= [X^2 - 2aX + (a^2 + b^2)]c \\ f(X) &= cX^2 - 2acX + (a^2 + b^2)c. \end{aligned}$$

Mostrando assim que $\partial(f(X)) = 2$. Além disso, o discriminante de $f(X)$ é

$$\Delta = (2ac)^2 - 4c(a^2 + b^2)c = -4b^2c^2 < 0$$

uma vez que $b \neq 0$ e $c \neq 0$.

Por outro lado, se $\partial(f(X)) = 1$, então, pela Proposição 4.2, $f(X)$ é irredutível sobre $\mathbb{R}$. Se $\partial(f(X) = 2$, então, como já vimos, ou $f(X)$ tem uma raiz em $\mathbb{R}$ ou é irredutível sobre $\mathbb{R}$. Como não tem raízes em $\mathbb{R}$, pois seu discriminante é menor que zero, então $f(X)$ é irredutível sobre $\mathbb{R}$. □

Consideremos um polinômio $f(X) \in \mathbb{R}[X]$. Indiquemos por $c_1, c_2, \cdots, c_r$ suas raízes reais e por $\beta_1, \overline{\beta_1}, \beta_2, \overline{\beta_2}, \cdots, \beta_s, \overline{\beta_s}$ suas raízes complexas não reais. Então, pelo que vimos na Proposição 4.3:

$$f(X) = a(X - c_1)(X - c_2)\cdots(X - c_r)(X - \beta_1)(X - \overline{\beta_1})\cdots(X - \beta_s)(X - \overline{\beta_s})$$

que é uma igualdade em $\mathbb{C}[X]$. Observemos, porém, que, fazendo $\beta_1 = a_1 + b_1 i$, temos:

$$(X - \beta_1)(X - \overline{\beta_1}) = X^2 - (2a_1)X + (a_1^2 + b_1^2).$$

Como o discriminante desse polinômio quadrático é

$$(2a_1)^2 - 4 \cdot 1 \cdot (a_1^2 + b_1^2) = -4b_1^2 < 0$$

então ele é irredutível sobre $\mathbb{R}$. O mesmo se verifica para os demais produtos $(X - \beta_k)(X - \overline{\beta_k})$.

Repetindo esse raciocínio com os demais pares de produtos envolvendo raízes complexas, obtemos:

$$f(X) = a(X-c_1)(X-c_2)\cdots(X-c_r)[X^2-2a_1X+(a_1^2+b_1^2)]\cdots[X^2-2a_sX+(a_s^2+b_s^2)]$$

em que os fatores são polinômios reais. Essa é a decomposição de $f(X)$ em fatores irredutíveis sobre $\mathbb{R}$. É claro que podem haver fatores iguais, tanto entre os de grau 1 como entre os de grau 2, que poderiam ser reunidos de maneira óbvia.

Conforme vimos, não há polinômios complexos irredutíveis de grau maior que 1, assim como não há polinômios irredutíveis de grau maior que 2 em $\mathbb{R}[X]$. Em $\mathbb{Q}[X]$, porém, a situação é diferente, o polinômio $f(X) = X^3 + X + 1$ é irredutível sobre $\mathbb{Q}$. De fato, pelo teste da raiz racional temos que as possíveis raízes racionais de $f(X)$ são ± 1, mas como $f(1) = 3$ e $f(-1) = -1$, segue, pelo Teorema 3.5, que $f(X)$ é irredutível sobre $\mathbb{Q}$.

Para analisar a irredutibilidade de um polinômio, veremos primeiramente que caso um polinômio $f(X) \in K[X]$ possua uma raiz em K ele é redutível sobre K.

Teorema 4.4. *Seja K um corpo qualquer. Seja $f(X) \in K[X]$ com grau 2 ou 3. Então $f(X)$ é redutível sobre K se e somente se $f(X)$ possui raiz em K.*

Demonstração. Seja $f(X) \in K[X]$ com *grau* 2 ou 3, assuma primeiramente que $f(X)$ é redutível sobre K, tal que

$$f(X) = g(X)h(X)$$

para algum polinômio não constante $g(X), h(X) \in K[X]$.

Como o *grau* de $g(X)$ e $h(X)$ somados é 2 ou 3, segue que, um ou ambos os polinômios devem ter *grau* 1. Assim pelo Teorema 3.5, um deles deve ter raiz em K, logo $f(X)$ deve ter uma raiz em K.

Reciprocamente, suponhamos que $f(X)$ tem raiz em K. Pelo Teorema 3.5, $f(X)$ têm um fator de *grau* 1, logo temos que $f(X) \in K[X]$ é redutível sobre K.

□

A partir do Teorema 4.4 conclui-se que: se o grau de um polinômio $f(X)$ sobre um corpo K é 2 ou 3, então ou $f(X)$ é irredutível sobre K ou tem pelo menos uma raiz sobre K.

Exemplo 4.5. Vamos mostrar que o polinômio $f(X) = 2X^3 - 5$ é irredutível sobre $\mathbb{Q}$.

Utilizando o teste da raiz racional obtemos que as únicas possíveis raízes racionais deste polinômio são

$$\pm 1, \pm\frac{1}{2}, \pm\frac{5}{2}, \pm 5.$$

Quando substituímos X por esses valores observamos que nenhum deles é raiz de $f(X)$, ou seja, $f(X)$ não possui raízes em $\mathbb{Q}$.

Como $\partial f(X) = 3$, segue do Teorema 4.4, que $f(X)$ é irredutível sobre $\mathbb{Q}$.

É importante ressaltar que o Teorema 4.4 pode não ser válido se retirarmos a restrição de ser de *grau* 2 ou 3. Por exemplo, o polinômio $f(X) = X^4 + 5X^2 + 4$ pode ser reescrito da seguinte forma

$$f(X) = \left(X^2 + 1\right)\left(X^2 + 4\right),$$

ou seja, é redutível em $\mathbb{Q}$, mas não possui raiz em $\mathbb{Q}$.

Quando consideramos polinômios em $\mathbb{Z}[X]$ ou $\mathbb{Q}[X]$, o problema fica bem mais difícil.

Definição 4.4. *Um polinômio não constante pertencente a $A[X]$ se diz primitivo se a unidade de A é um máximo divisor comum de seus coeficientes. Em outras palavras, isso significa que os únicos divisores dos coeficientes do polinômio são os elementos inversíveis do anel.*

Exemplo 4.6. Seja $f(X) = X^4 - X^2 + 1 \in \mathbb{Z}[X]$. Vamos mostrar que $f(X)$ é irredutível em $\mathbb{Z}[X]$. Claramente $f(X)$ é primitivo, de modo que basta mostrar que $f(X)$ não é um produto de dois fatores de grau maior ou igual a 1 em $\mathbb{Z}[X]$.

- $f(X)$ não tem fator de grau 1 em $\mathbb{Z}[X]$; com efeito, se ele tivesse, este fator (que tem que ser mônico pois $f(X)$ é mônico) seria do tipo $X - a$, com $a \in \mathbb{Z}$, isto é, teríamos $X^4 - X^2 + 1 = (X - a)g(X)$ com $g(X) \in \mathbb{Z}[X]$; olhando para o termo constante, teríamos $1 = am$ com $m \in \mathbb{Z}$, logo $a = \pm 1$, isto é, ± 1 seria raiz de $X^4 - X^2 + 1$; no entanto, é imediato verificar que nem 1, nem -1, são raízes de $X^4 - X^2 + 1$.

  (Observe que se tivéssemos trabalhando em $\mathbb{Q}[X]$ no lugar de $\mathbb{Z}[X]$, a priori a poderia ser qualquer elemento diferente de zero pertencente a $\mathbb{Q}$ e logo não daria para verificar, um por um, que nenhum a de $\mathbb{Q}$ é raiz de $f(X)$).

- $f(X)$ não tem fator $g(X)$ de grau 3 em $\mathbb{Z}[X]$; com efeito, se ele tivesse, teríamos $f(X) = g(X)h(X)$, onde $h(X) \in \mathbb{Z}[X]$ teria necessariamente grau 1; mas isto é impossível pelo caso precedente.

- $f(X)$ não tem fator de grau 2 em $\mathbb{Z}[X]$; com efeito, se ele tivesse, teríamos

$$
\begin{array}{lrcll}
X^4 - X^2 + 1 = (X^2 + aX + b)(X^2 + cX + d) \text{ com } a,\ b,\ c,\ d \in \mathbb{Z} & & & & \\
\text{(termo constante)} & 1 & = & bd, & \text{logo } b = d = \pm 1; \\
\text{(termo em X)} & 0 & = & ad + bc & \\
 & & = & b(a + c), & \text{logo } a = -c; \\
\text{(termo em } X^2\text{)} & -1 & = & d + ac + b & \\
 & & = & 2b - a^2, & \text{logo } a^2 - 1 = 2b = \pm 2;
\end{array}
$$

  assim $a^2 = 3$ ou $a^2 = -1$, o que é impossível.

Considere $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$, com $a_i \in \mathbb{Q}, \forall\ i = 0, 1, \cdots, n$.

Para verificarmos a irredutibilidade de um polinômio sobre um corpo estudaremos um teorema que nos fornece condições suficientes para que um polinômio $f(X) \in \mathbb{Q}[X]$ seja irredutível sobre $\mathbb{Q}$.

Se multiplicarmos $f(X)$ pelo mínimo múltiplo comum de $a_0, a_1, a_2, \cdots, a_n$ obtemos $f_1(X) \in \mathbb{Z}[X]$. Para utilizar esses resultados iniciaremos provando a proposição a seguir que nos diz que a irredutibilidade de $f(X)$ sobre $\mathbb{Z}$ é equivalente a sua irredutibilidade em $\mathbb{Q}$.

Lema 4.1 (Gauss)**.** *Seja $f(X) \in \mathbb{Z}[X]$ tal que $f(X)$ é irredutível sobre $\mathbb{Z}$ então $f(X)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. A demonstração se dará por contradição. Suponha que $f(X) \in \mathbb{Q}[X]$ é redutível sobre $\mathbb{Q}$, ou seja, por hipótese $f(X) = g(X).h(X)$, onde $g(X),\ h(X) \in \mathbb{Q}[X]$ e $1 \leq \partial g(X), \partial h(X) \leq \partial f(X)$.

Como $g(X),\ h(X) \in \mathbb{Q}[X]$, segue que existe um inteiro positivo m, que é o mínimo múltiplo comum dos coeficientes de $g(X)$ e $h(X)$, tal que $mf(X) = g_1(X) \cdot h_1(X)$, onde $g_1(X),\ h_1(X) \in \mathbb{Z}[X]$.

Assim temos,$g_1(X) = a_0 + a_1X + \cdots + a_rX^r, a_i \in \mathbb{Z}$ e $h_1(X) = b_0 + b_1X + \cdots + b_sX^s, b_i \in \mathbb{Z}$.

Suponha que $p|m$, para algum p primo. Provaremos que ou $p|a_i, \forall\ i \in \{1, \cdots, r\}$ ou $p|b_j, \forall\ j \in \{1, \cdots, s\}$.

De fato, se $\exists\, i \in 1, \cdots, r$ e $\exists\, j \in 1, \cdots, s$ tais que $p \nmid a_i$ e $p \nmid b_j$ consideremos i e j os menores possíveis com esta propriedade.

Como $p|m$ temos que p divide o coeficiente de x^{i+j} do polinômio $mf(X) = g_1(X) \cdot h_1(X)$, isto é, $p|(b_0a_{i+j} + b_1a_{i+j-1} + b_2a_{i+j-2} + \cdots + b_ja_i + \cdots + b_{i+j-1}a_1 + b_{i+j}a_0)$.

Pela nossa escolha de i e j temos que p divide cada parcela, exceto b_ja_i do coeficiente de x^{i+j} de $g_1(X) \cdot h_1(X)$.

Como p divide toda a expressão segue também que $p|b_ja_i$ e como p é um número primo temos que $p|b_j$ ou $p|a_i$ o que é uma contradição.

Assim, se p é primo, $p|m \Rightarrow p|a_i\ \forall i \in 1, \cdots, r$ ou $p|b_j\ \forall j \in 1, \cdots, s$.

Sem perda de generalidade, suponhamos que $p|a_i\ \forall i \in 1, 2, \cdots, r$. Assim, $g_1(X) = pg_2(X)$, onde $g_2(X)\ \in \mathbb{Z}[X]$ e se $m = p\ m_1$ temos

$$p\ m_1f(X) = pg_2(X) \cdot h_1(X)$$
$$m_1f(X) = g_2(X) \cdot h_1(X).$$

Como o número de fatores primos de m é finito, prosseguindo no argumento acima chegaremos que:

$$f(X) = g^*(X).h^*(X), \text{ onde } g^*(X), h^*(X) \in \mathbb{Z}[X]$$

e $g^*(X)$ e $h^*(X)$ são múltiplos racionais de $g(X)$ e $h(X)$, respectivamente, contradizendo a irredutibilidade de $f(X)$ sobre $\mathbb{Z}$. □

Exemplo 4.7. Mostremos que $p(x) = x^4 - 2x^2 + 8x + 1$ é irredutível sobre $\mathbb{Q}$.

Pelo Lema de Gauss (4.1), é suficiente ver que o polinômio é irredutível sobre $\mathbb{Z}$. Uma fatoração de $p(x)$ pode ser de dois tipos: um polinômio linear vezes um polinômio de grau 3, ou então o produto de dois polinômios quadráticos.

Se existe um polinômio linear que divide $p(x)$, isso quer dizer que $p(x)$ tem uma raiz racional. As únicas possíveis raízes racionais de $p(x)$ são ± 1, e podemos ver facilmente

que nenhuma dela é raiz. Logo uma possível fatoração de $p(x)$ só pode ser um produto de dois polinômios quadráticos. Seja então $p(x) = (x^2 + ax + b)(x^2 + cx + d)$, com a, b, c e d inteiros. Fazendo a distributiva e comparando coeficientes, temos $bd = 1$, $ad + bc = 8$, $ac + b + d = -2$ e $a + c = 0$.

De $bd = 1$ temos $b = d = 1$ ou $b = d = -1$. Se $b = d = 1$, ficamos com $ac = -4$ e portanto $a = -c = \pm 2$ e não podemos ter $ad + bc = 8$. Se $b = d = -1$, obtemos $ac = 0$, logo $a = c = 0$ e novamente não temos $ad + bc = 8$. Portanto a fatoração como dois polinômios quadráticos também é impossível, e concluímos que o polinômio $p(x)$ é irredutível sobre $\mathbb{Q}$.

Outro critério de irredutibilidade muito útil é o seguinte:

Teorema 4.5 (Critério de Eisenstein)**.** *Seja $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ um polinômio em $\mathbb{Z}[X]$. Se existe um inteiro primo p tal que:*

i- $p \nmid a_n$;

ii- $p | a_0, a_1, a_2, \cdots, a_{n-1}$;

iii- $p^2 \nmid a_0$,

então $f(X)$ é irredutível sobre $\mathbb{Q}$.

Demonstração. Utilizando o Lema 4.1 é suficiente provar que $f(X)$ é irredutível sobre $\mathbb{Z}$. Suponhamos por contradição que,

$$f(X) = g(X) \cdot h(X), \text{ com } g(X),\ h(X) \in \mathbb{Z}[X] \text{ e } 1 \leqslant \partial g(X), \partial h(X) < \partial f(X) = n.$$

Seja,
$g(X) = b_0 + b_1X + b_2X^2 + \cdots + b_rX^r \ \in \mathbb{Z}[X], \partial g(X) = r$ e
$h(X) = c_0 + c_1X + c_2X^2 + \cdots + c_sX^s \ \in \mathbb{Z}[X], \partial g(X) = s.$
Assim $n = r + s$.

Sabemos que $b_0c_0 = a_0$ e assim $p | b_0$ ou $p | c_0$. Como $p^2 \nmid a_0$ segue que p divide apenas um dos inteiros b_0, c_0. Vamos admitir sem perda de generalidade, que $p | b_0$ e $p \nmid c_0$.

Temos $a_n = b_rc_s$ e este é o coeficiente de $x^n = x^{r+s}$ e como $p \nmid a_n$ segue que $p \nmid b_r$. Seja b_i o primeiro coeficiente de $g(X)$ tal que $p \nmid b_i$.

O coeficiente de X^i é $a_i = b_0c_i + b_1c_{i-1} + \cdots + b_ic_0$ e como $p | b_0,\ b_1, \cdots, b_{i-1}, p \nmid b_i$ e $p \nmid c_0$ segue que $p \nmid a_i \Rightarrow i = n$, o que é um absurdo pois $1 \leq i \leq r < n$.

□

Para exemplificar o que estudamos a respeito da irredutibilidade dos polinômios vamos analisar alguns exemplos de polinômios irredutíveis sobre $\mathbb{Q}$.

Exemplo 4.8. Mostraremos que o polinômio $X^4 + 4X^2 + 8X - 2$ é irredutível em $\mathbb{Q}[X]$.

Considere $p = 2$, observe que $p|(-2)$, $p|8$, $p|4$, $p|0$, $p \nmid 1$ e $p^2 \nmid (-2)$. Logo, utilizando o Critério de Eisenstein, temos que $X^4 + 4X^2 + 8X - 2$ é irredutível sobre $\mathbb{Q}$.

Exemplo 4.9. Vamos determinar qual é o polinômio mônico de grau mínimo que tem $1 + \sqrt[3]{2}$ como raiz.

Seja $\alpha = 1 + \sqrt[3]{2}$, temos que

$$\begin{aligned} \alpha &= 1 + \sqrt[3]{2} \\ \alpha - 1 &= \sqrt[3]{2} \\ (\alpha - 1)^3 &= (\sqrt[3]{2})^3 \\ \alpha^3 - 3\alpha^2 + 3\alpha - 1 &= 2 \\ \alpha^3 - 3\alpha^2 + 3\alpha - 3 &= 0. \end{aligned}$$

Utilizando o Critério de Eisenstein, com $p = 3$ determinamos que o polinômio $X^3 - 3X^2 + 3X - 3 = 0$ é irredutível sobre $\mathbb{Q}$, ou seja, este é o polinômio mônico de menor grau em que $1 + \sqrt[3]{2}$ é raiz.

Exemplo 4.10. Vamos verificar que o polinômio $X^n - p$, onde p é um número inteiro primo, é irredutível sobre $\mathbb{Q}$.

Observe que $p|(-p)$, $p \nmid 1$ e $p^2 \nmid (-p)$. Logo, utilizando o Critério de Eisenstein obtemos a irredutibilidade de $X^n - p$ sobre $\mathbb{Q}$.

Exemplo 4.11. Vamos mostrar que o polinômio $X^4 + 120X^3 - 90X + 60$ é irredutível sobre $\mathbb{Q}$.

De fato, omitindo o coeficiente de X^4, temos que o máximo divisor comum dentre os outros coeficientes é $30 = 2.3.5$. Isto mostra que os únicos números primos, que podem ser utilizados diretamente são $p = 2, 3, 5$. Como 60 é divisível por 2^2, mas não por 3^2 ou 5^2, segue que o critério de Eisenstein vale para $p = 3$ e para $p = 5$. Como $5|120$, $5|90$, $5|60$, $5 \nmid 1$ e $25 \nmid 60$ mostramos que o polinômio é irredutível sobre $\mathbb{Q}$.

Exemplo 4.12. Vamos mostrar que o polinômio $3X^5 + 18X^2 + 24X + 6$ é irredutível sobre $\mathbb{Q}$.

Dividindo o polinômio $3X^5 + 18X^2 + 24X + 6$ por 3 obtemos o polinômio $X^5 + 6X^2 + 8X + 2$ que satisfaz o Critério de Eisenstein para $p = 2$, logo é irredutível sobre $\mathbb{Q}$.

Exemplo 4.13. Vamos mostrar que o polinômio $2X^{10} + 25X^3 + 10X^2 - 30$ é irredutível sobre $\mathbb{Q}$.

Observe que este polinômio satisfaz o Critério de Eisenstein para $p = 5$, logo é irredutível sobre $\mathbb{Q}$.

Um modo de provar que um polinômio é irredutível sobre $\mathbb{Z}$ (logo sobre $\mathbb{Q}$ também) é considerá-lo módulo p, para algum primo p conveniente e usar fatoração única em $\mathbb{Z}_p[X]$.

Proposição 4.5. *Sejam $p(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$ e um número primo p, tal que $p \nmid a_n$. Caso $\overline{p}(X)$ seja irredutível sobre $\mathbb{Z}_p$, temos que $p(X)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. Sejam $p(X) = a_0+a_1X+\cdots+a_nX^n$; $\partial f(X) = n$ e $p \nmid a_n$. Suponhamos que $p(X) \in \mathbb{Z}[X]$ é redutível sobre $\mathbb{Q}$. Então sabemos, pelo Lema 4.1, que

$$\exists\ q(X) = b_0 + b_1X + \cdots + b_rX^r \in \mathbb{Z}[X]$$

e

$$\exists\ f(X) = c_0 + c_1X + \cdots + c_sX^s \in \mathbb{Z}[X],$$

onde $\partial q(X) = r$ e $\partial f(X) = s$, de modo que $1 \leqslant r < n$ e $1 \leqslant s < n$ tais que $p(X) = q(X).f(X)$.

Disto segue que $\overline{p}(X) = \overline{q}(X).\overline{f}(X)$, onde $\overline{q}(X) \in \mathbb{Z}_p[X]$ e $\overline{f}(X) \in \mathbb{Z}_p[X]$.

Como $a_n = b_r.c_s$ e $p \nmid a_n$, segue que $p \nmid b_r$ e $p \nmid c_s$ e portanto $\overline{b_r} \neq 0$ e $\overline{c_s} \neq 0$, isto é, $\partial\overline{q}(X) = r$ e $\partial\overline{f}(X) = s$ e portanto $\overline{p}(X)$ é redutível sobre $\mathbb{Z}_p$.

□

Exemplo 4.14. Vamos verificar que $f(X) = X^2 + 1$ é irredutível sobre $\mathbb{Z}_3$.

Para verificar que esse polinômio é irredutível sobre $\mathbb{Z}_3$ basta verificar que ele não possui raízes em $\mathbb{Z}_3$.

Observe que $f(0) = 1, f(1) = 2$ e por fim $f(-1) = 2$. Portanto $f(X)$ é irredutível sobre $\mathbb{Z}_3$.

Exemplo 4.15. Vamos verificar que $f(X) = X^4 + 10X^3 + 15X^2 + 5X + 12 \in \mathbb{Z}[X]$ é irredutível sobre $\mathbb{Q}$.

Considere $p = 5$ e $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ então $\overline{f}(X) = X^4 + \overline{2} \in \mathbb{Z}_5[X]$.

Observe que $5 \nmid 1$ e pela Proposição 4.5 é suficiente provarmos que $\overline{f}(X) = X^4 + \overline{2}$ é irredutível sobre $\mathbb{Z}_5$.

A primeira observação que fazemos é que $\overline{f}(X)$ não possui raízes em $\mathbb{Z}_5$. Assim a única forma possível de fatorarmos $\overline{f}(X)$ seria a seguinte:

$$X^4 + \overline{2} = (aX^2 + bX + c).(a'X^2 + b'X + c'X),$$

onde $a,\ b,\ c,\ a',\ b',\ c' \in \mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Desenvolvendo os cálculos chegamos que é impossível essa última fatoração.

Logo, $f(X) = X^4 + 10X^3 + 15X^2 + 5X + 12$ é irredutível sobre $\mathbb{Q}$.

Exemplo 4.16. Vamos mostrar que $p(X) = X^3 + (3m-1)X + (3n+1)$ é irredutível sobre $\mathbb{Q}$, $\forall\ m, n \in \mathbb{Z}$.

Realizaremos o estudo da redutibilidade desse polinômio sobre $\mathbb{Z}_3$, então obtemos a seguinte equivalência,

$$X^3 + (3m-1)X + (3n+1) \equiv X^3 - X + 1\,(mod\ 3).$$

Observe que $0, \pm\overline{1}$ não são raízes do polinômio $\overline{p}(X)$, ou seja, $\overline{p}(X)$ é irredutível sobre $\mathbb{Z}_3$, consequentemente $p(X)$ é irredutível sobre $\mathbb{Q}$.

4.2 Extensões de corpos e irredutibilidade

O objetivo desta seção é estudar a construção de corpos pelo processo de adjunção de raízes de um polinômio.

4.2.1 Números algébricos

Temos que $\mathtt{e}$, π e $\sqrt{2}$ são números irracionais, porém temos que $\sqrt{2}$ é raiz do polinômio

$$X^2 - 2$$

com coeficientes em $\mathbb{Q}$ e isso não ocorre com $\mathtt{e}$ e π. Assim dizemos que $\sqrt{2}$ é algébrico em $\mathbb{Q}$ enquanto que $\mathtt{e}$ e π são transcendentes. Podemos ver a demonstração de que π é transcendental consultando Jones [6].

Definição 4.5. *Um número $\alpha \in \mathbb{C}$ é dito algébrico sobre um corpo $K \subseteq \mathbb{C}$ se existe um polinômio não nulo $f(X) \in K[X]$, tal que α é uma raiz de $f(X)$, isto é, um polinômio*

$$f(X) = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$$

com coeficientes $a_0, a_1, \ldots, a_n \in K$, com ao menos um coeficiente não nulo e com $f(\alpha) = 0$.

Um número complexo que não é algébrico é denominado transcendente.

É importante ressaltar que para todo corpo K, para todo $\alpha \in K$ temos que α é algébrico sobre K, visto que α é a raiz do polinômio $X - \alpha \in K[X]$.

Podemos concluir que $\mathtt{e}$ e π são algébricos sobre $\mathbb{R}$, mas não são algébricos sobre $\mathbb{Q}$.

Exemplo 4.17. O número $\sqrt[3]{5}$ é algébrico sobre $\mathbb{Q}$ porque é uma raiz do polinômio não nulo $X^3 - 5$, que possui coeficientes em $\mathbb{Q}$.

Exemplo 4.18. O número $\sqrt[6]{5}\cdot\sqrt[3]{3}$ é algébrico sobre $\mathbb{Q}$, porque é uma raiz do polinômio não nulo $X^6 - 45$, que possui coeficientes em $\mathbb{Q}$.

Exemplo 4.19. O número $2+\sqrt{3}$ é algébrico sobre $\mathbb{Q}$.

De fato, seja $\alpha = 2+\sqrt{3}$. Isolando $\sqrt{3}$, temos

$$\alpha - 2 = \sqrt{3}.$$

Elevando ambos os membros da equação ao quadrado, obtemos

$$(\alpha - 2)^2 = 3$$

e assim

$$\alpha^2 - 4\alpha + 1 = 0.$$

Portanto α é uma raiz do polinômio $X^2 - 4X + 1$, não nulo e com coeficientes em $\mathbb{Q}$.

Definição 4.6. *Seja $\alpha \in \mathbb{C}$ algébrico sobre um corpo $K \subseteq \mathbb{C}$. O único polinômio de menor grau entre os polinômios $f(X)$ em $K[X]$ satisfazendo:*

(i) $f(\alpha) = 0$

(ii) $f(x)$ *é mônico*
é chamado o polinômio irredutível de α sobre K e denotado por

$$irr(\alpha, K).$$

O grau de α sobre K é denotado por

$$\partial(\alpha, K).$$

4.2.2 Extensões de dimensões finitas

A partir de um corpo K e $\alpha \in \mathbb{C}$ algébrico sobre K, podemos produzir um corpo $K(\alpha)$ maior que K, sendo este um espaço vetorial sobre K e um subcorpo de $\mathbb{C}$.

Podemos assim determinar o grau de uma extensão de um corpo sobre outro corpo, nos permitindo determinar quais números são construíveis e assim resolver "Os Três Problemas Clássicos".

Definição 4.7. *Seja K um subcorpo de $\mathbb{C}$ e seja $\alpha \in \mathbb{C}$ algébrico sobre K com*

$$\partial(\alpha, K) = n.$$

A extensão de K por α é o conjunto $K(\alpha) \subseteq \mathbb{C}$, onde

$$K(\alpha) = \left\{ b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} : b_0, b_1, \ldots, b_{n-1} \in K \right\}.$$

Definição 4.8. *O grau de uma extensão de F sobre K é a dimensão de F considerado como um espaço vetorial sobre K. Caso o grau dessa extensão seja finito dizemos que é uma extensão de dimensão finita.*

Teorema 4.6. *Se M é uma extensão finita de L e L é uma extensão finita de K, então M é uma extensão finita de K com $[M : K] = [M : L][L : K]$.*

Demonstração. Suponhamos que $\alpha_1, \alpha_2, \cdots, \alpha_m$ e $\beta_1, \beta_2, \cdots \beta_n$ sejam bases de M sobre L e de L sobre K, respectivamente. Então $[M : L] = m, [L : K] = n$ e queremos provar que $[M : K] = mn$. Qualquer elemento $\alpha \in M$ pode ser escrito como

$$\alpha = \gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_m\alpha_m$$

onde $\gamma_1, \cdots, \gamma_m \in L$. Agora, para cada i tal que $1 \leq i \leq m$, temos

$$\gamma_i = r_{i1}\beta_1 + r_{i2}\beta_2 + \cdots + r_{in}\beta_n$$

onde $r_{i1}, \cdots, r_{in} \in K$. Logo, combinando as duas expressões anteriores, obtemos

$$\alpha = \sum_{i=1}^{m} \gamma_i\alpha_i = \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\beta_j\alpha_i$$

onde cada r_{ij} pertence a K. A seguir, mostraremos que o conjunto $\{\beta_j\alpha_i; 1 \leq j \leq n, 1 \leq i \leq m\}$ é linearmente independente e assim é uma base de M sobre K. Seja

$$\sum_{i=1}^{m}\sum_{j=1}^{n} s_{ij}\beta_j\alpha_i = 0$$

onde cada $s_{ij} \in K$. Como $\alpha_1, \cdots, \alpha_m$ forma uma base de M sobre L, obtemos

$$\sum_{j=1}^{n} s_{ij}\beta_j = 0$$

para qualquer i. Finalmente, como $\beta_1, \cdots, \beta_n$ é uma base de L sobre K, concluímos que cada s_{ij} é zero. □

Teorema 4.7. *[Masuda, p.27, [10]] Sejam K um corpo e $f(X)$ um polinômio mônico de grau n sobre K. Então o anel quociente $K[X]/(f(X))$ pode ser descrito como*

$$\{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : a_0, a_1, \cdots, a_{n-1} \in K \text{ e } f(\alpha) = 0\}.$$

Definição 4.9. *Seja $\theta \in F$ um elemento algébrico sobre K. O único polinômio mônico $M \in K[X]$ que gera o ideal*

$$I = \{f \in K[X] : f(\theta) = 0\}$$

é chamado o polinômio minimal de θ sobre K.

Teorema 4.8. *Seja F uma extensão do corpo K e $\theta \in F$ um elemento algébrico sobre K. O polinômio minimal M de θ sobre K possui as seguintes propriedades.*

1. *M é irredutível sobre K.*
2. *Seja $f(X)$ um polinômio em $K[X]$. Então $f(\theta) = 0$ se e somente se M divide $f(X)$.*
3. *M é o único polinômio mônico sobre K de menor grau tal que $M(\theta) = 0$.*
4. *M é o único polinômio mônico irredutível sobre K satisfazendo $M(\theta) = 0$.*
5. *Temos que $\partial(M)$ divide $[K : F]$. Em particular, $\partial(M) \leq [F : K]$. Além disso, $\partial(M) = [F : K]$ se e somente se $F = K(\theta)$.*

Demonstração. Vamos provar (1). Definimos um homomorfismo de anéis $\phi : K[X] \longrightarrow F$ por $\phi(f(X)) = f(\theta)$. Temos que $ker\phi = (M)$. Como $K[X]/(M) \cong \phi(K[X])$ é um domínio de integridade, o ideal (M) é primo e assim é maximal, pelo Teorema 2.6. Uma outra aplicação do mesmo teorema resulta que M é irredutível sobre K.

Segue diretamente da definição de polinômio minimal e de (1) que (2) e (4) se verificam.

Para provar (5), temos que $K[X]/(M)$ é um corpo e é isomorfo a $\phi(K[X])$, que então deve ser $K(\theta)$. Pelo Teorema 4.7 tem-se $[K(\theta) : K] = \partial(M)$. Portanto, temos que $\partial(M)$ divide $[F : K]$, pela fórmula dada pelo Teorema 4.6:

$$[F : K] = [F : K(\theta)][K(\theta) : K].$$

Além disso, $\partial(M) = [F : K]$ se e somente se $[F : K(\theta)] = 1$. Em outras palavras, $F = K(\theta)$. □

Observação 4.2. Nas condições do Teorema 4.8, denotamos M por $irr(\theta, K)$.

Corolário 4.1. *[Jones, p.72, [6]] Seja K um subcorpo de $\mathbb{C}$ e seja α um número complexo algébrico sobre K de grau n. Todo número $\beta \in K(\alpha)$ é então algébrico sobre K e tem $\partial(\beta, K) \leq n$*

Há vários polinômios que podem ser decompostos e ter $\sqrt{2}$ como uma raiz. Por exemplo, é possível observar que $\sqrt{2}$ é raiz dos seguintes polinômios

$$\left(X^2 - 2\right) \cdot \left(X^4 - 4\right), \left(X^2 - 2\right)^2,$$

todos em $\mathbb{Q}[X]$, mas o polinômio $X^2 - 2$ difere dos polinômios citados acima pois é o de menor grau que possui $\sqrt{2}$ como raiz.

Desta maneira, se α é raiz de um polinômio mônico, então temos infinitos polinômios mônicos com α como raiz, embora não exista o maior grau possível, há um menor grau possível.

Exemplo 4.20. O polinômio irredutível de $\sqrt{2}$ sobre $\mathbb{Q}$ é $X^2 - 2$.

De fato, podemos observar que o polinômio $X^2 - 2$ tem $\sqrt{2}$ como raiz e seus coeficientes pertencem a $\mathbb{Q}$, além disso, esse polinômio é mônico. Provaremos que não existe um outro polinômio com essas propriedades e que tenha um menor grau.

Se existisse, o polinômio seria da forma

$$a + X, \text{ para algum } a \in \mathbb{Q}.$$

implicando que,

$$a + \sqrt{2} = 0$$

logo

$$\sqrt{2} = -a \in \mathbb{Q},$$

uma contradição.

Deste modo temos,

$$irr(\sqrt{2}, \mathbb{Q}) = X^2 - 2$$

e portanto,

$$\partial(\sqrt{2}, \mathbb{Q}) = 2.$$

Observe que $X^2 - 2$ é o polinômio irredutível de $\sqrt{2}$ sobre $\mathbb{Q}$, porém o polinômio $X - \sqrt{2}$ é o polinômio irredutível de $\sqrt{2}$ sobre $\mathbb{R}$, pois $X - \sqrt{2}$ está em $\mathbb{R}[X]$, mas não está em $\mathbb{Q}[X]$.

5 Irredutibilidade em Corpos Finitos

Como a construção de um corpo finito depende inicialmente da existência de um polinômio irredutível, sobre um corpo base $\mathbb{F}_q,\ q = p^n,\ p$ um primo, além de sabermos encontrá-lo, é importante que saibamos quantos polinômios irredutíveis sobre o corpo base existem, pois quanto mais abundante for o número de polinômios irredutíveis mais fácil será de encontrá-lo, [16].

Fatorar um polinômio $f(X)$ em $\mathbb{F}_q[X]$ significa encontrar polinômios mônicos irredutíveis. A fatoração de polinômios é um requisito essencial em muitas aplicações na teoria de códigos, álgebra computacional, criptografia, teoria computacional de números e várias outras áreas, [10]. Apesar do esforço de vários pesquisadores, fatorar polinômios sobre um corpo finito de maneira efetiva ainda é um problema em aberto.

Vamos iniciar esta seção determinando uma fórmula para o número de polinômios irredutíveis de grau l sobre $\mathbb{F}_q$ e depois provaremos que o número de polinômios irredutíveis sobre $\mathbb{F}_q$ é abundante, deixando para a próxima seção a descrição de métodos que encontrem um polinômio irredutível sobre $\mathbb{Z}_p[X]$.

5.1 Números de polinômios irredutíveis de grau l sobre $\mathbb{F}_{p^n}$

Necessitamos primeiramente de alguns resultados, cujas provas podem ser encontradas, por exemplo, em [7] ou [13]. Assumimos que $q = p^n$, onde p é um número primo e n é um inteiro positivo.

Teorema 5.1. *Seja $f(X) \in \mathbb{F}_q[X]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então $f(X)$ divide $X^{q^k} - X$ se, e somente se m divide k.*

Demonstração. p.59, [10]. □

Teorema 5.2. *Para cada corpo finito $\mathbb{F}_q$ e cada $k \in \mathbb{N}$, o produto de todos polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujo grau divide k é igual a $X^{q^k} - X$.*

Demonstração. p.23, [16] □

Uma consequência do Teorema 5.2 é que ele pode ser usado para testar a irredutibilidade de um polinômio sobre $\mathbb{F}_q$ conforme veremos mais adiante (Teste de Rabin).

Exemplo 5.1. Consideremos um polinômio mônico irredutível sobre $\mathbb{F}_2$ e $k = 4$.

O primeiro passo para exemplificarmos o teorema é procurarmos quais são os polinômios mônicos irredutíveis sobre $\mathbb{F}_{2^4}$ de grau 1, 2 ou 4, ou seja, os números que dividem k.

Os polinômios mônicos irredutíveis neste caso são: $X,\ X+1,\ X^2+X+1,\ X^4+X+1,\ X^4+X^3+1$ e $X^4+X^3+X^2+X+1$.

Partimos então para o exemplo propriamente dito:

$X^{q^k}-X = (X)(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1) = X^{16}-X$.

Vamos denotar o número de polinômios mônicos irredutíveis de grau l sobre $\mathbb{F}_q$ por $N_q(l)$. Pelo resultado do teorema anterior tem-se o seguinte.

Corolário 5.1. *Se $N_q(l)$ é o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau l, então*

$$q^n = \sum_{l/n} l.N_q(l), \forall\ n \in \mathbb{N}$$

onde a soma é estendida sobre todos divisores positivos l de n.

Exemplo 5.2. Como no exemplo anterior, encontramos todos os polinômios irredutíveis sobre $\mathbb{F}_2$ de grau no máximo 4, podemos contar quantos polinômios irredutíveis tem de grau $1, 2$ e $4 \in \mathbb{F}_{2^4}$ e assim substituir na fórmula do corolário anterior exemplificando o mesmo.

$$2^4 = \sum_{l/4} l.N_q(l)$$
$$16 = 1 \cdot N_q(1) + 2 \cdot N_q(2) + 4 \cdot N_q(4) = 1 \cdot 2 + 2 \cdot 1 + 4 \cdot 3 = 16$$

Porém ainda não encontramos uma fórmula explícita que determine o número de polinômios irredutíveis sobre $\mathbb{F}_q$. Para obtermos a mesma precisamos definir primeiramente a função de Moebius e a inversão de Moebius.

A *função de Moebius* μ é definida por,

$$\mu(l) = \begin{cases} 1 & \text{se } l = 1 \\ (-1)^j & \text{se } l \text{ é o produto de } j \text{ números primos distintos} \\ 0 & \text{caso contrário.} \end{cases}$$

Esta função foi introduzida por Moebius (1832), mas a notação $\mu(l)$ foi primeiramente usada por Mertens (1874).

Lema 5.1. *Para $l \in \mathbb{N}$ a função de Moebius μ satisfaz:*

$$\sum_{k/l} \mu(k) = \begin{cases} 1 & se\ l = 1 \\ 0 & se\ l > 1. \end{cases}$$

Demonstração. O caso $l = 1$ é óbvio. Para $l > 1, l \in \mathbb{N}$, seja $l = p_1^{m_1} \cdots p_r^{m_r} (m_i \in \mathbb{N}, 1 \leq i \leq r)$ a fatoração em produto de números primos de l. Os únicos divisores de l que produzem um somatório diferente de zero são aqueles cujos expoentes de p_i são 1 ou 0 $(1 \leq i \leq r)$. Existem exatamente $\begin{pmatrix} \mathrm{r} \\ \mathrm{j} \end{pmatrix}$ divisores de l para os quais j expoentes são 1. O restante é zero. Portanto nós temos:

$$\sum_{k/l} \mu(k) = \sum_{j=0}^{r} (-1)^j \begin{pmatrix} \mathrm{r} \\ \mathrm{j} \end{pmatrix} = \sum_{j=0}^{r} \begin{pmatrix} \mathrm{r} \\ \mathrm{j} \end{pmatrix} 1^{r-j}(-1)^j = (1-1)^r = 0.$$

□

Exemplo 5.3. Se $l = 12$, os divisores de l são: $D(12) = 1, 2, 3, 4, 6, 12$

$$\sum_{k/12} \mu(k) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)$$

$$\sum_{k/12} \mu(k) = 1 - 1 - 1 + 0 + 1 + 0$$

$$\sum_{k/12} \mu(k) = 0.$$

Teorema 5.3. *A clássica inversão de Moebius é dada por*

$$f(l) = \sum_{k/l} g(k) \Leftrightarrow g(l) = \sum_{k/l} \mu(k) f(\frac{l}{k}).$$

Demonstração. p.24, [16]. □

Teorema 5.4. *O número $N_q(l)$ de polinômios mônicos irredutíveis em $\mathbb{F}_q$ de grau l é dado por*

$$N_q(l) = \frac{1}{l} \sum_{k/l} \mu(k) \cdot q^{\frac{l}{k}}.$$

Demonstração. Seja $f(l) = q^l,\ g(l) = l \cdot N_q(l)\ \ \forall\ l \in \mathbb{N}$.

Pela definição, $f(l) = q^l$. Pelo corolário 5.1

$$q^l = \sum_{k/l} k \cdot N_q(k)$$

então

$$f(l) = \sum_{k/l} k \cdot N_q(k)$$

se $g(l) = l \cdot N_q(l)$ fazendo mudança de variável $l = k$, obtemos, $g(k) = k \cdot N_q(k)$ e, portanto

$$f(l) = \sum_{k/l} g(k).$$

Pela definição, temos $g(l) = l \cdot N_q(l)$.

Aplicando a inversão de Moebius, obtemos

$$g(l) = \sum_{k/l} \mu(k) \cdot f\left(\frac{l}{k}\right)$$

portanto

$$g(l) = l \cdot N_q(l) = \sum_{k/l} \mu(k) \cdot f\left(\frac{l}{k}\right)$$

sabemos que $f(l) = q^l$, fazendo mudança de variável $l = \dfrac{l}{k}$

$$f\left(\frac{l}{k}\right) = q^{\frac{l}{k}}$$

portanto

$$g(l) = \sum_{k/l} \mu(k) \cdot q^{\frac{l}{k}}.$$

Pela definição, $g(l) = l \cdot N_q(l)$, então

$$l \cdot N_q(l) = \sum_{k/l} \mu(k) \cdot g^{\frac{l}{k}}$$

$$N_q(l) = \frac{1}{l} \sum_{k/l} \mu(k) \cdot q^{\frac{l}{k}}.$$

□

Exemplo 5.4. O número de polinômios mônicos irredutíveis em $\mathbb{F}_q[X]$ de grau 20 é dado por

$$\begin{aligned} N_q(20) &= \frac{1}{20} \sum_{k/20} \mu(k) \cdot q^{\frac{20}{k}} \\ &= \frac{1}{20}[\mu(1) \cdot q^{20} + \mu(2) \cdot q^{10} + \mu(4) \cdot q^5 + \mu(5) \cdot q^4 + \mu(10) \cdot q^2 + \mu(20) \cdot q \\ &= \frac{1}{20}[q^{20} - q^{10} - q^4 + q^2] \end{aligned}$$

Ao exemplificarmos a fórmula dada pelo Teorema 5.4 como foi feito anteriormente poderemos verificar que para cada corpo finito $\mathbb{F}_q$ e cada $l \in \mathbb{N}$ existe um polinômio irredutível em $\mathbb{F}_q[X]$ de grau l. De fato se usarmos a definição da função de Moebius, a estimativa irá produzir sempre $n_q(l) \geq \dfrac{1}{l}(q^l - q^{l-1} - q^{l-2} - \cdots q) = \dfrac{1}{l}(q^l - \dfrac{q^l - 1}{q - 1}) > 0$, ou

seja, sempre existe polinômio irredutível de grau l. Essa mesma estimativa mostra que $N_q(l) \longrightarrow \frac{q^l}{l}$ (quando $l \longrightarrow +\infty$). Se observamos que existem q^l polinômios mônicos de grau l em $\mathbb{F}_q$, então obtemos o seguinte corolário.

Corolário 5.2. *Um polinômio mônico randômico de grau l sobre um corpo finito é redutível com uma probabilidade próxima a* $1 - \frac{1}{l}$.

Mais propriedades sobre $N_q(l)$ podem ser encontradas em [13] e [11].

5.2 Métodos para determinar um polinômio irredutível sobre $\mathbb{F}_{p^n}$

Pelo Teorema 5.4 determinamos o número de polinômios irredutíveis que existem sobre um dado corpo finito. Nossa tarefa agora é encontrar um polinômio irredutível, pois como já frisamos anteriormente é a partir dele que conseguimos representar um corpo finito.

Se o número de elementos do corpo primo for pequeno, um procedimento que torna-se fácil é o de encontrarmos os polinômios por tentativa e erro. Nesse caso listamos os polinômios mônicos de grau l sobre $\mathbb{F}_q$, em seguida devemos eliminar da lista todos os polinômios que não tem um termo constante, pois se o polinômio não tiver um termo constante não nulo ele pode ser fatorado e portanto é redutível. Para os polinômios restantes devemos substituir X pelos elementos de $\mathbb{F}_{p^n}$ um a um e efetuar os cálculos utilizando $(mod\ p)$. Se algum destes elementos de $\mathbb{F}_{p^n}$ zerar o polinômio podemos afirmar que este é raiz do polinômio o que implica que este polinômio pode ser fatorado e portanto redutível. Se o grau escolhido for dois, após eliminarmos os polinômios que não tem termo constante. Poderíamos tomar todos os fatores lineares sobre $\mathbb{F}_{p^n}$ e multiplicá-los, em todos os pares possíveis, assim verificaríamos quais são quadráticos fatoráveis e eliminaríamos eles da lista. Encontramos finalmente os polinômios mônicos irredutíveis sobre $\mathbb{F}_{p^n}$.

Se o corpo finito for grande, um dos métodos que podemos aplicar é o teste de Rabin. Este algoritmo leva em consideração que existe um número elevado de polinômios irredutíveis sobre um determinado corpo finito.

O algoritmo de Rabin [16] consta das seguintes etapas:

Passo 1: Gerar um polinômio mônico, $g(X)$ aleatoriamente, de grau l sobre $\mathbb{F}_q$.

Teste 1: Se este polinômio $g(X)$ dividir $(X^q - X)$, é porque o passo 1 teve sucesso.

Teste 2: Verificar se $mdc(g(X), X^{p^{n_i}} - X) = 1$ para todo $n_i = \frac{n}{k_i}$, onde o k_i são todos os divisores primos de n, caso se verifique esta condição então o teste dois teve sucesso.

Deve-se repetir esse algoritmo até que os testes 1 e 2 tenham sucesso. Note que a justificativa para a correção do algoritmo é o Teorema 5.2.

Exemplo 5.5. Para determinarmos os polinômios irredutíveis sobre $\mathbb{F}_3$ de grau 2, podemos usar tentativa e erro já que o corpo finito é pequeno.

Iniciamos listando todos os polinômios quadráticos sobre $\mathbb{F}_3$, visto que $n = 2$.

$$\mathbb{F}_3 = \{X^2, X^2+1, X^2+2, X^2+X+1, X^2+X+2, X^2+2X, X^2+2X+1, X^2+2X+2\}.$$

Todos os polinômios que não tem termo constante são fatoráveis. Portanto, X^2, X^2+X, X^2+2X, são eliminados da lista.

Podemos saber se os polinômios que sobraram na lista são irredutíveis substituindo os valores de X pelos elementos que compõem $\mathbb{F}_3$, que são 0, 1 e 2. Realizando os cálculos verificamos se esse polinômio não possui raiz em $\mathbb{F}_3$, ou seja, se é irredutível sobre esse corpo.

Ao fazer isso constataremos que X^2+1, X^2+X+2 e X^2+2X+2 são polinômios quadráticos mônicos irredutíveis em $\mathbb{F}_3$.

Exemplo 5.6. Para encontrarmos os polinômios irredutíveis de grau 4 sobre $\mathbb{F}_2$, aplicando o algoritmo de Rabin escolhemos um polinômio $g(X)$.

1) O polinômio escolhido é $X^4 + X^3 + 1$ sobre $\mathbb{F}_{2^4}$.

2) Então: $g(X) = X^4 + X^3 + 1$

   Sabemos que $q = p^n$ como $p = 2$ e $n = 4$ então $q = 2^4$ e portanto $q = 16$.

   Devemos verificar se $g(X)$ divide $X^{16} - X$. Fazendo o cálculo verifica-se que ele divide e gera o quociente $X^{12} - X^{11} + X^{10} - X^9 + X^7 + X^5 - X^4 - X$.

3) No segundo teste devemos fazer o $mdc(g(X), X^{p^{n_i}} - X)$ e este deve ser 1. Sabendo que $n = 4$ e $p = 2$, verificamos o valor de k_i, sendo estes os divisores de n, portanto $k_i = 2$. Temos $n_i = \dfrac{n}{k_i} = 2$.

   Então o $mdc(X^4+X^3+1,\ X^{2^2} - X) = mdc(X^4+X^3+1,\ X^4 - X) = mdc(X^4 - X,\ X^4 + X^3 + 1) = mdc(X^3 + X + 1,\ -X^2) = mdc(-X^2,\ X + 1) = mdc(X + 1,\ X) = mdc(X, 1) = mdc(1,\ 0)$.

   Como o $mdc(X^4+X^3+1,\ X^{2^2} - X) = 1$, então o teste dois também teve sucesso, e portanto $X^4 + X^3 + 1$ é um polinômio irredutível sobre $\mathbb{F}_{2^4}$.

6 Polinômios e suas Aplicações nas Impossibilidades Geométricas

Neste capítulo veremos como a irredutibilidade de um polinômio está relacionada a números construtíveis e com a impossibilidade de algumas construções geométricas. Na Grécia Clássica, as construções geométricas eram objetos de grande interesse dos matemáticos, mas com as restrições do uso apenas de dois instrumentos: a régua (sem marcas) e o compasso. Essas construções refletiam o conceito de elegância com a qual a geometria era tratada e a atração, tipicamente helênica que tinham os matemáticos pelos desafios intelectuais, mesmo sem aplicação imediata.

Alguns problemas ficaram sem resposta, dentre eles temos "Os três problemas clássicos" que são:

- Duplicação do Cubo;
- Quadratura do Círculo;
- Trissecção do Ângulo.

A resposta para estes problemas foi obtida com a evolução da matemática, ou especificamente, da Teoria das Equações Algébricas, quando se demonstra que essas construções são impossíveis se apenas os instrumentos citados anteriormente forem utilizados.

Antes de estudar essas impossibilidades vamos analisar o que é "impossível" em matemática. O primeiro barco à vapor a cruzar o Atlântico levava, como parte de sua carga, um livro que "provava" que era impossível um barco à vapor cruzar qualquer coisa, quanto mais o Atlântico. Ao longo da história muitas coisas que foram ditas ser impossíveis de fazer caíram diante da genialidade do ser humano.

Na matemática, as declarações de que algo é impossível significa, teoricamente impossível e não tem nada a ver com o nível do desenvolvimento humano. A busca pela solução de um problema tem sentido, mesmo que seu sucesso pareça improvável, enquanto não se demonstra que teoricamente ele não possui solução.

Deste modo, baseando-se nos axiomas e teoremas de Euclides, tem sentido a afirmação que a Duplicação do Cubo, a Quadratura do Círculo e a Trissecção do Ângulo

são impossíveis com um número finito de construções utilizando a régua e o compasso descritos anteriormente.

6.1 Números construtíveis e corpos

Dada uma régua (não graduada) e um compasso, as operações que podemos realizar com estes instrumentos são chamadas construções fundamentais e são:

1. Dados dois pontos, podemos traçar uma reta que passa pelos dois pontos e prolonga-la até ao infinito nas duas direções;

2. Dados dois pontos podemos traçar o segmento de reta que une os dois pontos;

3. Dado um ponto e um segmento de reta, podemos traçar a circunferência com centro nesse ponto e raio igual ao comprimento do segmento de reta.

Definição 6.1. *Dizemos que um número real α é construtível se, dado um segmento de comprimento 1, é possível construir, num número finito de passos, um segmento de comprimento $\mid \alpha \mid$.*

O lema seguinte diz-nos que a soma e o produto de números reais construtíveis ainda é um número construtível. A sua demonstração será omitida mas uma demonstração análoga será feita na Proposição 6.1.

Lema 6.1. *Dados segmentos de comprimentos $1, \alpha$ e β com $\alpha > \beta$ e $\beta \neq 0$, é possível construir segmentos de comprimentos $\alpha + \beta, \alpha - \beta, \alpha\beta$ e $\dfrac{\alpha}{\beta}$.*

Pelo Lema 6.1 podemos concluir que todos os números racionais são construtíveis. A proposição seguinte é apenas uma reformulação deste Lema usando o conceito de números reais construtíveis:

Proposição 6.1. *Sejam α e β dois números reais construtíveis. Então também $\alpha + \beta, \alpha - \beta, \alpha\beta$ e $\dfrac{\alpha}{\beta}$ são construtíveis.*

Demonstração. Consideremos dois números reais construtíveis α e β, com $\alpha > \beta$. Traçamos sobre uma reta s um segmento AB de comprimento α e um segmento de reta CD de comprimento igual a β de modo que B coincida com C. Construa uma circunferência com centro em B e raio $\overline{CD}$. A circunferência intersecta a reta s nos pontos D e E tais que B está entre A e D enquanto que E está entre A e B. Então, o comprimento de AD, $\overline{AD}$, é $\alpha + \beta$ e o de AE é $\alpha - \beta$, concluindo-se que $\alpha + \beta$ e $\alpha - \beta$ são construtíveis. (Figura 6.1)

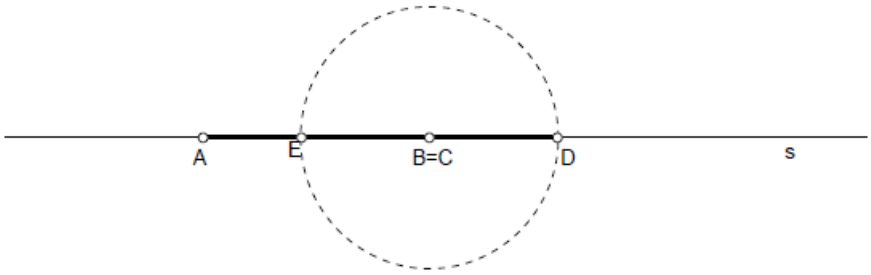

Figura 6.1: Construção da soma e da diferença de dois reais construtíveis

Com vista a demonstrar a segunda parte da Proposição, marcamos sobre uma reta dada s um segmento de reta AB de comprimento igual a α. Por A, traçamos outra reta r, concorrente com a anterior. Em r marcamos a partir de A um segmento unitário, digamos AC, e o segmento AD de comprimento igual a β. Em seguida traçamos a reta t que contém os pontos B e C e construímos a reta t' paralela a t que passa por D. Seja P o ponto de intersecção das retas t' e s.

Então o comprimento de AP, $\overline{AP} = \alpha\beta$, uma vez que, pelo Teorema de Tales,

$$\frac{\overline{AC}}{\overline{AD}} = \frac{\overline{AB}}{\overline{AP}},$$

isto é,

$$\frac{1}{\beta} = \frac{\alpha}{\overline{AP}}.$$

Concluímos assim que $\alpha\beta$ é construtível. (Figura 6.2)

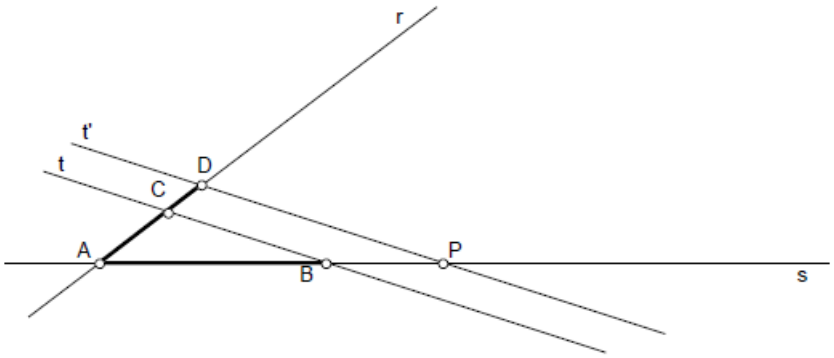

Figura 6.2: Construção do produto de dois reais construtíveis.

Nas mesmas condições do caso anterior, traçamos a reta t que contém os pontos B e D e construímos por C a reta t' paralela a t que intersecta a reta s no ponto Q.

Então $\overline{AQ} = \dfrac{\alpha}{\beta}$ uma vez que

$$\frac{\overline{AC}}{\overline{AD}} = \frac{\overline{AQ}}{\overline{AB}},$$

isto é,

$$\frac{1}{\beta} = \frac{\overline{AQ}}{\alpha},$$

ou seja,

$$\frac{\alpha}{\beta} = \overline{AQ}.$$

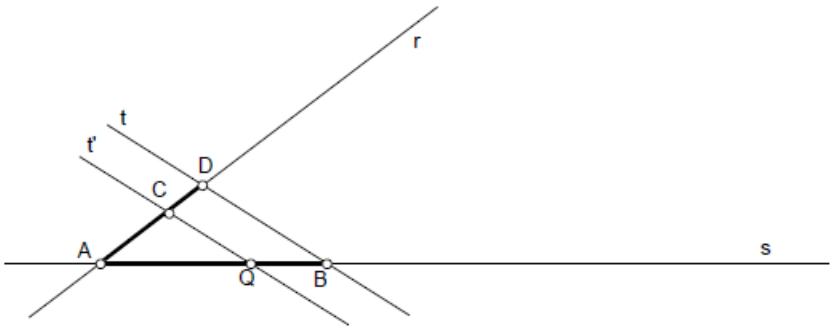

Figura 6.3: Construção do quociente de dois reais construtíveis.

□

Lema 6.2. *Dados segmentos de comprimento* 1 *e* α*, é possível construir um segmento de comprimento* $\sqrt{\alpha}$

Demonstração. Consideremos sobre uma reta s o segmento unitário AB e o segmento BC de comprimento $BC = \alpha$. Seja M o ponto médio do segmento AC e construa uma semicircunferência com centro em M e diâmetro $\overline{AC}$. Em seguida traçamos a perpendicular s' a s pelo ponto B e seja D o ponto de intersecção da reta s' com a semicircunferência.

Então, BD é um segmento de comprimento $\sqrt{\alpha}$ já que

$$\frac{\overline{BC}}{\overline{BD}} = \frac{\overline{BD}}{\overline{AB}},$$

isto é,

$$\frac{\alpha}{\overline{BD}} = \frac{\overline{BD}}{1},$$

ou seja,

$$\alpha = \overline{BD}^2,$$

portanto,

$$\sqrt{\alpha} = \overline{BD}.$$

concluindo-se o pretendido.

□

Demonstraremos algebricamente que utilizando régua e compasso, com um número finito de passos, é impossível a construção de alguns segmentos que permitiriam as construções geométricas descritas anteriormente.

Teorema 6.1. *O conjunto CON de todos os números construtíveis é um subcorpo de $\mathbb{R}$. Além disso temos que todos os números racionais pertencem a CON, e por último temos que se $\alpha \in CON$ e $\alpha > 0$ então $\sqrt{\alpha} \in CON$.*

Demonstração. Para mostrarmos que CON é um subcorpo de $\mathbb{R}$, devemos mostrar que as operações de adição, subtração, multiplicação e divisão (exceto por 0) são satisfeitas pelos elementos de CON.

Seja α e β pertencentes a CON, ou seja, os segmentos de tamanho $|\alpha|$ e $|\beta|$ podem ser construídos com um número finito de construções utilizando régua e compasso, partindo de um segmento de 1 unidade.

Por construções geométricas também é possível obter, segmentos do tipo $|\alpha + \beta|$, $|\alpha - \beta|$, $|\alpha\beta|$ e $|\alpha/\beta|$, se $\beta \neq 0$.

Assim os números $\alpha + \beta$ e $\alpha - \beta$ $\alpha\beta$ e α/β, se $\beta \neq 0$ são todos construtíveis, e portanto pertencem a CON. Assim CON é um corpo.

Tendo o segmento do tamanho de 1 unidade como base, podemos construir segmentos de tamanhos variados, podemos observar então que podemos construir segmentos inteiros e positivos.

Utilizando construções com régua e compasso podemos construir segmento de tamanho m e n, consequentemente m/n, com $m, n \in \mathbb{N}$. Aplicando a Definição 6.1 para $|\gamma|$ segue que todo número racional pertence ao CON.

Finalmente podemos concluir que se $\alpha \in CON$ e $\alpha > 0$ então, utilizando construções com régua e compasso, podemos construir $\sqrt{\alpha}$, ou seja, $\sqrt{\alpha}$ é construtível.

□

6.2 Números não construtíveis

Nesta seção iremos ver que todos os números construtíveis são obtidos através de raízes quadradas sucessivas e operações que são bem definidas nos corpos, partindo de números que estão nos $\mathbb{Q}$.

Teorema 6.2 (Raízes quadradas sucessivas geram números construtíveis)**.** *Um número real γ é construtível se existem números reais positivos $\gamma_1, \gamma_2, \gamma_3, \cdots, \gamma_n$ tal que*

$$\begin{array}{lll} \gamma_1 \in \mathbb{K}_1, & \textit{onde} & \mathbb{K}_1 = \mathbb{Q} \\ \gamma_2 \in \mathbb{K}_2, & \textit{onde} & \mathbb{K}_2 = \mathbb{K}_1(\sqrt{\gamma_1}) \\ \gamma_3 \in \mathbb{K}_3, & \textit{onde} & \mathbb{K}_3 = \mathbb{K}_2(\sqrt{\gamma_2}) \\ \vdots & & \vdots \\ \gamma_n \in \mathbb{K}_n, & \textit{onde} & \mathbb{K}_n = \mathbb{K}_{n-1}(\sqrt{\gamma_{n-1}}) \end{array}$$

e finalmente,

$$\gamma \in \mathbb{K}_{n+1}, \quad onde \quad \mathbb{K}_{n+1} = \mathbb{K}_n(\sqrt{\gamma_n}).$$

Demonstração. A demonstração segue imediatamente do Teorema 6.1

□

Sabemos que números reais como $2+\sqrt{3+\sqrt{\frac{2}{5}\sqrt{2}}}$ que são obtidos de elementos de $\mathbb{Q}$ por sucessivas operações em corpos e utilizando raízes quadradas são todos construtíveis. É de suma importância saber se podemos seguir a implicação no sentido inverso, ou seja, os números construtíveis podem ser expressos em termos de raízes quadradas repetidas e operações de corpo a partir de elementos em $\mathbb{Q}$?

O teorema a seguir mostra que a resposta é sim.

Teorema 6.3 (Todos números construtíveis vem de raízes quadradas)**.** *Se um número real γ é construtível, então existe números reais positivos $\gamma_1, \gamma_2, \gamma_3, \cdots \gamma_n$ tal que*

$$\begin{array}{lll} \gamma_1 \in \mathbb{K}_1, & onde & \mathbb{K}_1 = \mathbb{Q} \\ \gamma_2 \in \mathbb{K}_2, & onde & \mathbb{K}_2 = \mathbb{K}_1(\sqrt{\gamma_1}) \\ \gamma_3 \in \mathbb{K}_3, & onde & \mathbb{K}_3 = \mathbb{K}_2(\sqrt{\gamma_2}) \\ \vdots & & \vdots \\ \gamma_n \in \mathbb{K}_n, & onde & \mathbb{K}_n = \mathbb{K}_{n-1}(\sqrt{\gamma_{n-1}}) \end{array}$$

e finalmente,

$$\gamma \in \mathbb{K}_{n+1}, \quad onde \quad \mathbb{K}_{n+1} = \mathbb{K}_n(\sqrt{\gamma_n}).$$

Demonstração. p. 100, [6]. □

Teorema 6.4 (Teorema do grau de um número construtível)**.** *Se um número α é construtível, então α é algébrico sobre $\mathbb{Q}$ e $\partial(\alpha, \mathbb{Q})$ é uma potência de 2, $2^s (s \geq 0)$.*

Demonstração. Seja α um número construtível e sejam $\lambda_1, \ldots, \lambda_n$ definidos no Teorema 6.2. O número $\sqrt{\lambda_i}$ é raiz do polinômio $X^2 - \lambda_i$, que pertence a $K_i[X]$ desde que $\lambda_i \in K_i$.

Assim, pelo Corolário 4.1

$$\partial\left(\sqrt{\lambda_i}, K_i\right) = 1 \text{ } ou \text{ } 2$$

e como $K_{i+1} = K_i(\lambda_i)$, segue do Teorema 4.8 que

$$[K_{i+1} : K_i] = 1 \text{ ou } 2, (1 \leq i \leq n).$$

Temos a seguinte torre de corpos

$$\mathbb{Q} = K_1 \subseteq K_2 \subseteq K_3 \subseteq \ldots \subseteq K_{n+1}.$$

Sabemos que

$$\begin{aligned}[K_{n+1} : \mathbb{Q}] &= [K_{n+1} : K_n]\,[K_n : K_{n-1}] \ldots [K_2 : K_1] \\ &= 2^u, \text{ para algum inteiro } u \geq 0.\end{aligned}$$

Segue do Corolário 4.1 que γ é algébrico sobre $\mathbb{Q}$ e considerando a torre

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq K_{n+1}$$

vemos que o $\partial(\lambda, \mathbb{Q})$ é um fator de $[K_{n+1} : \mathbb{Q}]$. Assim

$$\partial(\lambda, \mathbb{Q}) = 2^s$$

para algum inteiro $s \geq 0$.

□

6.3 A impossibilidade de algumas construções geométricas

Mostraremos que as construções geométricas citadas neste capítulo são impossíveis de serem realizadas com régua e compasso num número finito de passos.

Teorema 6.5 (Problema da duplicação do cubo)**.** *Com a medida inicial de 1 unidade podemos construir um cubo com* $1u^3$ *de volume. Para duplicarmos um cubo devemos ser capazes de construir um outro cubo com* $2u^3$ *de volume que possui arestas de medidas iguais a* $\sqrt[3]{2}$*, ou seja, esta aresta deve ser construída usando somente régua e compasso, com número finito de passos, a partir de um segmento de linha de tamanho* $1u$*.*

Demonstração. Sabemos que

$$irr\left(\sqrt[3]{2}, \mathbb{Q}\right) = X^3 - 2 = f(X)$$

e $\sqrt[3]{2}$ é raiz desse polinômio.

Pelo teste da raiz racional as únicas possibilidades de raízes para o polinômio $f(X) = X^3 - 2$ em $\mathbb{Q}$ são ± 1 e ± 2, porém nenhum desses números é raiz de $f(X)$. Segue do Teorema 4.4, que $f(X)$ é irredutível sobre $\mathbb{Q}$.

Obtemos assim que

$$\partial\left(\sqrt[3]{2}, \mathbb{Q}\right) = 3,$$

que não é uma potência de 2, mostrando que $\sqrt[3]{2}$ não é construtível, pelo Teorema 6.4, e portanto o cubo não pode ser duplicado.

□

Teorema 6.6 (Problema da quadratura do círculo)**.** *Se um círculo de raio 1 possui área igual a π unidades, então um quadrado com mesma área deverá ter lados iguais a $\sqrt{\pi}$, ou seja, para que se possa construir um quadrado de mesma área que esse círculo, devemos ter que $\sqrt{\pi}$ deve ser construtível.*

Demonstração. Pelo Teorema 6.4, se $\sqrt{\pi}$ for algébrico sobre $\mathbb{Q}$ então $\pi = \sqrt{\pi} \cdot \sqrt{\pi}$ será algébrico sobre $\mathbb{Q}$, porém é de nosso conhecimento que π é transcendental, ou seja, não é algébrico sobre $\mathbb{Q}$ e portanto $\sqrt{\pi}$ não é construtível. □

Se conseguimos trissectar qualquer ângulo, então conseguimos trissectar o ângulo de 60^o. A seguir verificaremos que isso não é possível.

Teorema 6.7 (Problema da trissecção do ângulo)**.** *É impossível, usando apenas régua e compasso, trissectar um ângulo de 60^o.*

Demonstração. Sabemos que o ângulo de 60^o é construtível utilizando um número finito de construções com régua e compasso, isso significa que deveríamos conseguir construir um ângulo de 20^o também, ou seja, devemos conseguir construir um segmento de tamanho $\cos(20^o)$.

Seja $\theta = 20^o$, temos que $\cos(3\theta) = \dfrac{1}{2}$.

$$\begin{aligned}
\cos(3\theta) &= \cos(2\theta + \theta) \\
\cos(3\theta) &= \cos(2\theta).\cos(\theta) - \operatorname{sen}(2.\theta)\operatorname{sen}(\theta) \\
\cos(3\theta) &= [\cos^2(\theta) - \operatorname{sen}^2(\theta)]\cos(\theta) - 2\operatorname{sen}(\theta)\cos(\theta)\operatorname{sen}(\theta) \\
\cos(3\theta) &= \cos^3(\theta) - \operatorname{sen}^2(\theta)\cos(\theta) - 2\operatorname{sen}^2(\theta)\cos(\theta) \\
\cos(3\theta) &= \cos^3(\theta) - 3[1 - \cos^2(\theta)]\cos(\theta) \\
\cos(3\theta) &= 4\cos^3(\theta) - 3\cos(\theta) \\
\frac{1}{2} &= 4\cos^3(\theta) - 3\cos(\theta).
\end{aligned}$$

Multiplicando ambos os membros da última equação por 2, obtemos

$$1 = 8\cos^3(\theta) - 6\cos(\theta).$$

Substituindo $2\cos(\theta) = r$, temos

$$r^3 - 3r - 1 = 0.$$

Obtemos assim que

$$\partial(\cos(20^o), \mathbb{Q}) = 3,$$

portanto $\cos(20^o)$ não é construtível, pelo Teorema 6.4, portanto não é possível trissectar o ângulo de 60^o.

□

7 Aplicações de Polinômios no Ensino Médio

O estudo dos polinômios no ensino médio concentra-se na resolução de uma situação problema utilizando um polinômio que a represente e em seguida resolvendo uma equação algébrica. Este tema também é explorado para analisar um determinado evento, que pode ser representado por uma função polinomial e que está associada a um polinômio. Geralmente temos que um polinômio $p(X)$ é associado a uma função polinomial $p : \mathbb{R} \to \mathbb{R}$ ou $p : \mathbb{C} \to \mathbb{C}$.

Uma aplicação, pouco explorada dos polinômios, que pode ser desenvolvida em sala de aula é o seu uso para determinar se uma raiz α de um polinômio $p(X) \in \mathbb{Q}[X]$ pertence a $\mathbb{Q}$, ou seja, podemos utilizar polinômios para definir a racionalidade ou não de um número.

Para determinar a forma fatorada de um polinômio podemos utilizar o método de Kronecker para fatoração em $\mathbb{Z}$, mas ele é pouco utilizado devido ao fato de ser extenso.

Durante o estudo de polinômios no ensino médio podemos utilizar critérios de irredutibilidade de um polinômio sobre um corpo para determinar se ele pode ser fatorado ou não, como a avaliação do valor de Δ, que é realizado no ensino fundamental e médio, para determinar se um polinômio do segundo grau pode ser fatorado sobre $\mathbb{R}$.

Vamos estudar alguns dos diferentes enfoques que podemos dar ao trabalharmos com esse conteúdo no ensino médio.

7.1 Estudo dos números racionais.

Muitos alunos tem dificuldade quanto a determinar se um dado número α é racional ou não apenas por uma análise visual. Para deixar mais claro para os alunos essa abordagem podemos determinar um polinômio $p(X)$ de modo que α seja raiz e utilizando o Teorema 3.4 determinamos se α é uma das possíveis raízes racionais que este polinômio possui. Observe os exemplos a seguir:

Exemplo 7.1. Vamos verificar que $\sqrt[5]{7} \notin \mathbb{Q}$.

Tomando $\alpha = \sqrt[5]{7}$ e elevando ambos os membros da igualdade a 5 obtemos $\alpha^5 = 7$, assim essa igualdade por ser escrita como

$$\alpha^5 - 7 = 0.$$

Assim obtemos $p(X) = X^5 - 7$ para o qual α é raiz.

Temos que $X^5 - 7 \in \mathbb{Z}[X]$. Utilizando o teste da raiz racional, obtemos que as possíveis raízes racionais de $p(X)$ são ± 1 e ± 7, mas estes números não são raízes de $p(X)$. Observe que $\sqrt[5]{7}$ é raiz de $p(X)$, mas não está em $\mathbb{Q}$.

Analisando o exemplo anterior pode se questionar a aplicação dos polinômios para determinar se dado número α é racional ou não, mas em alguns casos essa tarefa não será trivial, como pode ser visto no exemplo a seguir:

Exemplo 7.2. Vamos verificar se o número $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}} \in \mathbb{Q}$.

Seja $u = \sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$. Elevando ambos os membros da igualdade ao cubo obtemos

$$u^3 = \left(\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}\right)^3$$

$$u^3 = (\sqrt[3]{2+\sqrt{5}})^3 + 3(\sqrt[3]{2+\sqrt{5}})^2(\sqrt[3]{2-\sqrt{5}}) + 3(\sqrt[3]{2+\sqrt{5}})(\sqrt[3]{2-\sqrt{5}})^2 + (\sqrt[3]{2-\sqrt{5}})^3$$

que pode ser reescrita como

$$u^3 = 2 + \sqrt{5} + 3\left(\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}\right).\left(\sqrt[3]{2+\sqrt{5}}\right)\left(\sqrt[3]{2-\sqrt{5}}\right) + 2 - \sqrt{5}.$$

Efetuando a multiplicação das raízes que estão entre parêntese e observando que a soma que está entre parênteses é o que, inicialmente, definimos como sendo u, obtemos

$$u^3 = 4 + 3u(-1).$$

A igualdade acima pode ser reescrita da seguinte forma

$$u^3 + 3u - 4 = 0.$$

Obtemos assim $p(X) = X^3 + 3X - 4$ para o qual u é raiz e $p(X) \in \mathbb{Z}[X]$. Utilizando o teste da raiz racional obtemos que as possíveis raízes racionais de $p(X)$ são ± 1 e ± 4. Verificamos que $p(1) = 0$, ou seja, 1 é raiz de $p(X)$.

Aplicando o algoritmo da divisão de polinômios, vamos obter $q(X) \in \mathbb{Z}[X]$ tal que $p(X) = (X-1).q(X)$.

$$\begin{array}{r|l} X^3+3X-4 & X-1 \\ \cline{2-2} -X^3+X^2 & X^2+X+4 \\ \cline{1-1} \quad X^2+3X-4 & \\ -X^2+\ X & \\ \cline{1-1} \qquad 4X-4 & \\ \qquad -4X+4 & \\ \cline{1-1} \qquad\quad 0 & \end{array}$$

Obtemos assim $q(X) = X^2 + X + 4$, que nos permite reescrever $p(X)$ da seguinte forma

$$p(X) = (X-1)(X^2+X+4).$$

Temos que as raízes de $p(X)$ são as raízes de $(X-1)$ e de (X^2+X+4). Observe que $q(X)$ não possui raízes reais e como sabemos u é raiz e $u \in \mathbb{R}$, obtemos assim que

$$\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}} = 1.$$

Portanto $u \in \mathbb{Q}$.

Exemplo 7.3. Verifique se o número $\sqrt[3]{20+14\sqrt{2}} + \sqrt[3]{20-14\sqrt{2}} \in \mathbb{Q}$.

Seja $\alpha = \sqrt[3]{20+14\sqrt{2}} + \sqrt[3]{20-14\sqrt{2}}$. Elevando ambos os membros da igualdade ao cubo obtemos

$$\alpha^3 = \left(\sqrt[3]{20+14\sqrt{2}} + \sqrt[3]{20-14\sqrt{2}}\right)^3$$

que pode ser reescrita como

$$\alpha^3 = 40 + 3\left(\sqrt[3]{20+14\sqrt{2}} + \sqrt[3]{20-14\sqrt{2}}\right).\left(\sqrt[3]{20+14\sqrt{2}}\right)\left(\sqrt[3]{20-14\sqrt{2}}\right).$$

Efetuando a multiplicação das raízes que estão entre parênteses e observando que a soma que está entre parênteses é o que, inicialmente, definimos como sendo α, obtemos

$$\alpha^3 = 4 + 3\alpha 2.$$

A igualdade acima pode ser reescrita da seguinte forma

$$\alpha^3 - 6\alpha - 40 = 0.$$

Obtemos assim $p(X) = X^3 - 6X - 40$ para o qual α é raiz e $p(X) \in \mathbb{Z}[X]$. Utilizando o teste da raiz racional obtemos que as possíveis raízes racionais de $p(X)$ são $\pm 1, \pm 2$ e ± 5. Verificamos que $p(4) = 0$, ou seja, 4 é raiz de $p(X)$.

Aplicando o algoritmo da divisão de polinômios, vamos obter $q(X) \in \mathbb{Z}[X]$ tal que $p(X) = (X-4).q(X)$.

$$\begin{array}{r|l} X^3 - 6X - 40 & X - 4 \\ \cline{2-2} -X^3 + 4X^2 & X^2 + 4X + 10 \\ \cline{1-1} 4X^2 - 6X - 40 & \\ -4X^2 + 16X & \\ \cline{1-1} 10X - 40 & \\ -10X + 40 & \\ \cline{1-1} 0 & \end{array}$$

Obtemos assim $q(X) = X^2 + 4X + 10$, que nos permite reescrever $p(X)$ da seguinte forma

$$p(X) = (X - 4)(X^2 + 4X + 10).$$

Temos que as raízes de $p(X)$ são as raízes de $(X - 1)$ e de $(X^2 + 4X + 10)$. Observe que $q(X)$ não possui raízes reais e como sabemos α é raiz e $\alpha \in \mathbb{R}$, obtemos assim que

$$\sqrt[3]{20 + 14\sqrt{2}} + \sqrt[3]{20 - 14\sqrt{2}} = 4.$$

Portanto $\alpha \in \mathbb{Q}$.

O processo de verificar se um número $\alpha \in \mathbb{Q}$ aborda alguns tópicos que devem ser desenvolvidos em sala de aula como por exemplo, divisão de polinômios, raízes de polinômios e o cálculo de um polinômio $p(X)$ para um dado valor de X.

7.2 Resolução de situações problemas.

Na resolução de situações problemas pode-se fazer necessário o uso da função polinomial definida por um polinômio $p(X)$ para analisar e resolver o problema de acordo com os dados utilizados e que desejamos alcançar, porém nem sempre obtemos funções polinomiais do segundo grau, com as quais já estamos acostumados a trabalhar e calcular suas raízes. Nesses casos utilizaremos o teste da raiz racional para determinar uma das raízes e assim poder reduzir o grau do polinômio, utilizando o algoritmo da divisão de polinômios, até que seja possível aplicar as técnicas conhecidas para o cálculo das outras raízes.

Exemplo 7.4. Cortando-se quadrados em cada canto de uma folha de papelão quadrada, com $18\,cm$ de lado e dobrando conforme a Figura 7.1, obtém-se uma caixa retangular sem tampa. Qual deve ser o lado do quadrado a ser recortado para que o volume da caixa seja igual a $400\,cm^3$?

As dimensões da caixa formada após o recorte são dadas por $18-2X$, $18-2X$ e X. Podemos determinar o volume dessa caixa em função de X utilizando a representação polinomial

$$V(X) = (18 - 2X)(18 - 2X)X$$

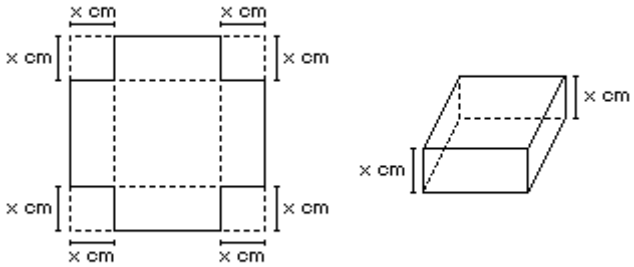

Figura 7.1: Caixa

ou, equivalentemente,

$$V(X) = 4X^3 - 72X^2 + 324X.$$

Sabemos que o volume desejado é de $400\,cm^3$ obtemos assim a seguinte igualdade

$$4X^3 - 72X^2 + 324X = 400$$

equivalente a

$$X^3 - 18X^2 + 81X - 100 = 0.$$

O que nos interessa é resolver a equação algébrica acima, mas isso é equivalente a determinar as raízes do polinômio $V_1(X) = X^3 - 18X^2 + 81X - 100$. Como $V_1(X) \in \mathbb{Z}[X]$, aplicaremos o teste da raiz racional que nos diz que as possíveis raízes racionais desse polinômio são $\pm 1, \pm 2$ e ± 5.

De fato, $V_1(4) = 0$, logo 4 é raiz e a medida do lado do quadrado recortado da folha de papelão que tínhamos no início, porém o polinômio $V_1(X)$ possui até 3 raízes pelo fato de $\partial V_1(X) = 3$, assim aplicaremos o algoritmo da divisão para reduzirmos o seu grau e assim poder estudar as demais raízes.

$$\begin{array}{r|l}
X^3 - 18X^2 + 81X - 100 & X - 4 \\
\cline{2-2}
-X^3 + 4X^2 & X^2 - 14X + 25 \\
\cline{1-1}
-14X^2 + 81X - 100 & \\
14X^2 - 56X & \\
\cline{1-1}
25X - 100 & \\
-25X + 100 & \\
\cline{1-1}
0 &
\end{array}$$

Obtemos que $V_1(X) = (X - 4)(X^2 - 14X + 25)$, denominamos $q(X) = (X^2 - 14X + 25)$. Sabemos que as raízes de $V_1(X)$ são as raízes de $q(X)$ e 4. Calculando as

raízes de $q(X)$ obtemos $X_1 = 7 + 2\sqrt{6}$ e $X_2 = 7 - 2\sqrt{6}$, mas observando a restrição de que $0 < 2X < 18$ e consequentemente $0 < X < 9$ descartamos X_1 como resposta do problema inicial.

Portanto a medida do lado do quadrado a ser recortado para que o volume da caixa seja igual a $400\,cm^3$ é $4\,cm$ ou $7 - 2\sqrt{6}\,cm$.

É mais frequente que uma situação problema seja expressa por um polinômio $p(X)$ com $\partial p(X) = 3$, mas nada impede que tenhamos $\partial p(X) > 3$, com processo de resolução análogo ao do Exemplo 7.4.

7.3 Raízes de Polinômios

Polinômios irredutíveis podem ser usados indiretamente no ensino médio no que diz respeito a fatoração de polinômios e suas raízes em $\mathbb{Q}$.

Seja $p(X)$ uma função polinomial induzida por $p(X) \in K$, onde K é um corpo com infinitos elementos e $\partial p(X) = n$.

Essa função pode representar uma situação problema que deve ser analisada num intervalo de variação para X e para isso a representação gráfica é uma ferramenta importante.

Temos que um dado polinômio $p(X)$ com $r_1, r_2, r_3, \cdots, r_n$, como raízes, aplicando o Teorema 3.5, possui a seguinte decomposição

$$p(X) = c(X - r_1)(X - r_2)(X - r_3)\cdots(X - r_n)$$

para algum valor de $c \in K$.

Utilizando os conceitos trabalhados anteriormente podemos obter a representação do polinômio $p(X)$ a partir de suas raízes em $\mathbb{R}$ ou obter o polinômio $p(X)$ a partir de sua representação, que apresente suas raízes e o valor de $p(0)$ para determinar o valor de c, permitindo assim a análise do evento que essa função polinomial está representando para um valor qualquer de X.

Recomendamos, para trabalhar com esta abordagem do conteúdo de polinômios, o software "Jogo dos Polinômios" disponível no site "http://www.m3.ime.unicamp.br". Este é um material que permite um trabalho dinâmico em sala de aula, pois possibilita que o aluno seja o protagonista do seu aprendizado, permitindo que ele construa o seu conhecimento realizando as atividades propostas pelo software.

8 Conclusão

O trabalho desenvolvido culminou em algumas aplicações, em sala de aula do ensino médio, não propriamente dos polinômios irredutíveis, mas dos resultados alcançados durante seu estudo.

Como professor do ensino médio, sei que é inviável apresentar toda a teoria referente aos números construtíveis com régua e compasso com um número finito de passos, mas a apresentação superficial das impossibilidades em construções geométricas podem ser utilizadas como motivador para o aprendizado de como construir um segmento com uma medida desejada e também para apresentar algo impossível em matemática, já que a maneira como alguns professores desenvolvem o estudo da matemática a torna "perfeita demais" e assim inalcançável na mente de alguns alunos.

Sabendo da dificuldade dos alunos em compreender se um número é racional ou não, quando não for óbvio, a aplicação do teste da raiz racional de um polinômio, que possua o número estudado como raiz, deve despertar a curiosidade dos alunos, pois números que "visualmente" não demonstravam ser racionais o são.

No estudo dos gráficos de funções o uso do software e a divisão de polinômios favorecerá esse aprendizado, o que é muito importante devido à analise de gráficos que os alunos deverão realizar em processos seletivos para o ensino superior ou mesmo na realização de suas atividades cotidianas em seus empregos.

Por fim, e de uma maneira mais aplicável ao cotidiano do aluno, a resolução de situações problemas utilizando a redutibilidade de um polinômio sobre um dado corpo permite a resolução de um problema real ou mesmo a irredutibilidade de um polinômio sobre um corpo nos permite analisar criticamente os possíveis resultados e sua pertinência como solução da situação problema abordada.

Os frutos do nosso estudo permitem que os professores realizem abordagens interessantes para o desenvolvimento do estudo sobre polinômios no ensino médio, como construções geométricas, conjuntos numéricos e resolução de situações problemas.

Referências

[1] DOMINGUES, H. H. and IEZZI, G. *Álgebra moderna*. Atual, São Paulo, 2013.

[2] GARBI, G. G. *O romance das equações algébricas*. Livraria da Física, São Paulo, 2010.

[3] GARCIA, A.; LEQUAIN, A. *Elementos de Álgebra*. IMPA, Rio de Janeiro, 2012.

[4] GONÇALVES, A. *Introdução à Álgebra*. IMPA, Rio de Janeiro, 2012.

[5] HERSTEIN, I. N. *Topics in Algebra*. John Wiley and Sons, New York,1975.

[6] JONES, A.; MORRIS, S. A.; PEARSON, K. R. *Abstract Algebra and Famous Impossibilities*. Springer-Verlag, New York, 1991.

[7] LIDL, R. and NIEDERREITER, H. *Introduction to finite fields and their applications*. Cambridge University Press, New York, 1994.

[8] LIMA,E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C. *A matemática do Ensino Médio*. SBM, Rio de Janeiro, 2006.

[9] LIVIO, M. *A equação que ninguém conseguia resolver*. Tradução: Jesus de Paula Assis. Record, Rio de Janeiro, 2011.

[10] MASUDA, A. and PANARIO, D. *Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos*. IMPA, Rio de Janeiro, 2007.

[11] MIGNOTTE, M. and STEFANESEU, D. *Polynomials - An Algorithmic Approach*. Springer, Singapore, 1999.

[12] PICADO, J. *Apontamentos de álgebra II*. Universidade de Coimbra - Departamento de Matemática, Coimbra, 2006.

[13] POHST, M. and ZASSENHAUS, H. *Algorithmic Algebraic Number Theory*. Cambridge University Press, New York, 1989.

[14] STEWART, I. N. *Galois Theory*. Chapman and Hall/CRC, Coventry, 2003.

[15] TOREZZAN, C. *Jogo dos Polinômios*. 2010. Disponível em: <http://m3.ime.unicamp.br/recursos/1235>. Acesso: 30 nov. 2013.

[16] ZANOELLO, S. F. *Raízes polinomiais em corpos finitos.*102f. Dissertação de Mestrado. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2004.

[17] ZATESKO, L. M. *Irredutibilidade Polinomial e Algoritmos em Corpos Finitos.*75f. Monografia de revisão bibliográfica. Universidade Federal do Paraná, Curitiba, 2008.