UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

INSTITUTO DE CIÊNCIAS EXATAS

CURSO DE LICENCIATURA EM MATEMÁTICA

Ruan José de Alcântara Rodrigues

O Último Teorema de Fermat para Primos Regulares

Seropédica
2020

Ruan José de Alcântara Rodrigues

O Último Teorema de Fermat Para Primos Regulares

Monografia apresentada à Banca Examinadora da Universidade Federal Rural do Rio de Janeiro, como requisito parcial para obtenção do título de Licenciado em Matemática, sob a orientação do Prof. Dr. André Luiz Martins Pereira e coorientação do Prof. Dr. Douglas Monsôres de Melo Santos.

Seropédica
2020

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

COORDENAÇÃO DO CURSO DE GRADUAÇÃO EM MATEMÁTICA.

A monografia "O ÚLTIMO TEOREMA DE FERMAT PARA PRIMOS REGULARES", apresentada e defendida por RUAN JOSÉ DE ALCÂNTARA RODRIGUES, matrícula 201419054-0 foi aprovada pela Banca Examinadora, com conceito "S" recebendo o número 733.

Seropédica, 03 de fevereiro de 2020.

BANCA EXAMINADORA

Prof. Dr. Douglas Monsôres de Melo Santos
Co-orientador

Prof. Dr. Orlando dos Santos Pereira

Profª. Drª. Eulina Coutinho Silva do Nascimento

Agradecimentos

Primeiramente agradeço à minha mãe Angela Maria da Conceição Alcântara por ser o maior exemplo de força que eu poderia ter e que junto ao meu pai Rubem José Rodrigues me ensinaram e deram exemplos dos princípios e valores que levarei pelo resto da minha vida.

Agradeço aos meus irmãos, Rubem, Rubia, Rubiano, Gersica, Roger, Patrícia, Jorge, Renata e Camila, pelo apoio e pelo cuidado durante os mais diversos momentos da minha vida. Em particular à minha irmã Renata, que foi a grande responsável por eu ter escolhido a UFRRJ, abrindo as portas e dando todo suporte durante a graduação.

Agradeço à minha companheira Kézia pelo carinho, lealdade e por ter passado toda essa etapa ao meu lado me apoiando e dando todo suporte emocional.

Agradeço aos amigos Rafael Reis, Gepatrik e Charlan por me receberem no alojamento e serem verdadeiros exemplos de veteranos.

Agradeço aos amigos Marcelo, Calvim, Mateus, Rômulo, Jocivaldo, Rafael Oliveira, Lucas, Targino e Geovane pelos momentos de estudos e pelas melhores resenhas.

Agradeço ao meu orientador Prof. Dr. André Luiz Martins Pereira por aceitar conduzir este trabalho com paciência e dedicação.

Agradeço ao meu coorientador Prof. Dr. Douglas Monsôres de Melo Santos por sua empatia, esforço e dedicação para que este trabalho pudesse ser concluído.

Por fim agradeço ao Departamento de Matemática da UFRRJ pela excelência da qualidade técnica de cada um.

Resumo

Este trabalho de monografia tem por objetivo demonstrar um caso especial do Último Teorema de Fermat, devido a Kummer, que diz que para um número primo p regular, não existem inteiros positivos x, y, z que satisfaçam a equação $x^p + y^p = z^p$. Começaremos relembrando alguns conceitos e resultados das teorias dos grupos, anéis e de galois que são vistos durante a graduação. Em seguida, apresentaremos alguns conceitos e resultados da Álgebra Comutativa, subárea da Álgebra que essencialmente estuda propriedades dos anéis comutativos e módulos sobre esses anéis. Dentro deste campo desenvolveremos os conceitos e estudaremos propriedades de extensões inteiras, ideais fracionários e Domínios de Dedekind. Os ideais fracionários em um domínio de Dedekind têm uma propriedade de fatoração similar a dos números inteiros. De fato, nós construiremos uma multiplicação entre seus ideias fracionários e provaremos que cada ideal fracionário se escreve de maneira única como produto de ideais primos. Tal construção nos permitirá definir a noção de grupo das classes de um domínio de Dedekind que será a base para definir o que vem a ser um primo regular. Por fim pelo estudo dos corpos ciclotômicos e seus anéis dos inteiros definiremos os primos regulares e provaremos o teorema de Kummer.

Palavras-chave: Último Teorema Fermat; Corpos Ciclotômicos; Primos Regulares; Dompinios de Dedekind.

Sumário

Introdução

Imagine que você tenha à sua disposição uma grande quantidade de dados (cubinhos) do mesmo tamanho e é proposto o seguinte desafio: com esses dados você deve formar dois cubos do tamanho que você quiser de forma que com o total de dados usados em ambos seja possível construir outro cubo.

Propor tal desafio numa confraternização de amigos, numa turma de ensino básico ou mesmo de ensino superior, pode render horas de entretenimento. Depois de tentar por algum tempo é provável que alguém se pergunte se realmente é possível resolvê-lo.

Em termos matemáticos, resolver o desafio dos cubos é encontrar inteiros x, y, z positivos que satisfaçam a equação $x^3 + y^3 = z^3$. É natural que alguém que tenha afinidade com a matemática associe tal equação ao teorema de Pitágoras e os inteiros aos ternos pitagóricos. A história por trás do problema com os cubos surgiu com um matemático chamado Pierre de Fermat (1607-1665).

De acordo com Singh (vide [1]), Fermat era um magistrado que tinha a matemática como hobby e teve como uma de suas inspirações a coleção *Aritmética* de Diofante de Alexandria, que era um livro que continha os conhecimentos obtidos por grandes nomes da matemática, como Pitágoras e Euclides, e tentava descrever a teoria dos números através de problemas e soluções.

Fermat não estava interessado em escrever um livro ou artigo para publicar, ele só buscava a satisfação pessoal de resolver um problema sem se importar em escrever provas rigorosas. Ele só escrevia aquilo que era necessário para convencer a si mesmo e frequentemente atirava suas anotações no lixo.

Enquanto estudava o segundo livro da *Aritmética*, Fermat encontrou uma série de observações, problemas e soluções envolvendo o Teorema de Pitágoras e os ternos pitagóricos. Ao substituir o quadrado pelo cubo na equação do Teorema Fermat percebeu que era muito difícil encontrar uma solução para a equação.

Na margem de sua *Aritmética* Fermat escreveu a seguinte nota de observação:

> É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como uma soma de dois números elevados a quatro, ou, em geral, para qualquer número que seja elevado a uma potência maior do que dois ser escrito como a soma de duas potências semelhantes.

Em seguida o seguinte comentário:

> Eu tenho uma demonstração realmente maravilhosa para esta proposição mas a margem é muito estreita para contê-la.

Além de resolver problemas, Fermat enviava cartas para outros matemáticos os desafiando a provar alguns dos seus desafios. Apesar disso Fermat nunca publicava suas descobertas. A publicação só veio depois de sua morte, graças ao seu filho mais velho Clément-Samuel que percebeu a importância do hobby do pai e passou cinco anos reunindo as cartas, anotações e analisando os rabiscos nas margens de sua *Aritmética*, e em 1670 publicou uma edição especial apresentada como *Aritmética de Diofante contendo observações de P. de Fermat*.

Suas anotações tinham uma série de teoremas que, ou não eram acompanhados por nenhuma explicação ou tinham apenas indícios da demonstração que os apoiava e como os teoremas são os "tijolos"que constroem toda a matemática, era essencial que cada um dos teoremas fosse demonstrado. À medida que os séculos foram passando, todas as demonstrações foram feitas, exceto uma, aquele que viria a ser conhecido como: O Último Teorema de Fermat que diz que não existem inteiros positivos x, y, z, n com $n > 3$ que satisfaçam a equação $x^n + y^n = z^n$.

Houve provas para casos particulares e muitas tentativas falhas da resolução do teorema, dentre as quais destacamos aqui: a de Leonhard Euler que completou um esboço de Fermat provando o teorema para o caso $n = 4$ e com a mesma ideia provando para $n = 3$ (O desafio dos cubos); Cauchy e Lamé que pela abordagem dos números complexos, falharam ao utilizar o conceito de fatoração única dos números naturais.

Ernst Kummer percebeu as falhas de Cauchy e Lamé e elaborou sua própria demonstração para alguns casos específios para n: o dos primos regulares. Este caso será o objeto de estudo deste trabalho monográfico.

Para isso, revisaremos os conceitos necessários das teorias de Anéis, Grupos e de Galois que foram estudados durante a graduação. É recomendável que o leitor tenha cursado pelo menos as disciplinas básicas de Teoria dos Grupos e dos Anéis. Estudaremos também algumas propriedades dos domínios de Dedekind, objeto de estudo da Álgebra Comutativa, e definiremos seu grupo das classes. Através do estudo dos corpos ciclotômicos definiremos o que são os primos regulares, para que possamos chegar ao nosso objetivo.

Capítulo 1

Noções preliminares

Neste capítulo realizaremos uma breve revisão de algumas teorias que darão suporte para que possamos chegar ao resultado desejado. Além da revisão, faremos nossas primeiras definições importantes para que o objetivo deste trabalho seja alcançado. A leitura das referências deste trabalho darão uma base mais aprofundada nestas diversas teorias que serão aqui utilizadas.

Admitiremos que o leitor já tenha familiaridade com conceitos básicos da Teoria dos Grupos e dos Anéis. Noções como homomorfismo de anéis e grupos quocientes serão utilizados no decorrer do texto. Recomendamos [2], o livro de Garcia e Lequain, como referência básica desses conceitos.

1.1 Grupos

Definição 1.1.1. Seja G um grupo com identidade e. A *ordem* de G é o número de elementos do conjunto G, e será denotada por $|G|$. Se G tem um número infinito de elementos, diz-se que tem ordem infinita.

Definição 1.1.2. A *ordem* de um elemento $x \in G$ é o menor inteiro positivo n tal que $x^n = e$. Se não existe tal inteiro n dizemos que x tem ordem infinita.

1.2 Anéis

Definição 1.2.1.

- Os elementos de um anel A que possuem inverso multiplicativo são chamados de *invertíveis* de A ou *unidades* de A. Usaremos a notação $A^\times = \{x \in A : x \text{ é uma unidade de } A\}$.
- Elementos a e b de um domínio D são chamados *associados* se $a = ub$ onde u é uma unidade de D.

- Um elemento não nulo a de D é chamado *irredutível* se não for uma unidade e sempre que $a = bc$ com b e c em D então b ou c é uma unidade.
- Sejam D um domínio e $a, b \in D$. Dizemos que a divide b (escrevemos $a \mid b$) se existe $c \in D$ tal que $a \cdot c = b$.
- Um elemento a de um domínio D é dito *primo* se a não for uma unidade e se $a|bc$ então $a|b$ ou $a|c$.

Definição 1.2.2. Um domínio D é de *fatoração única* se todo elemento não nulo e não invertível de D se escreve de maneira única (a menos de associados e ordenação) como produto de elementos irredutíveis de D, isto é:

(i) Todo elemento não nulo e não invertível de D é produto finito de fatores irredutíveis.

(ii) Se $\{p_i\}_{1 \leq i \leq s}$ e $\{q_j\}_{1 \leq j \leq t}$ são famílias finitas de elementos irredutíveis de D tais que $p_1 \cdots p_s = q_1 \cdots q_t$, então

- $s = t$.
- a menos de ordenação, p_i é associado a q_i, $\forall i = 1, \ldots s$ (isto é, existe uma bijeção de σ de $\{1, \ldots, s\}$ sobre $\{1, \ldots, s\}$ tal que p_i é associado a $q_{\sigma(i)}$, $\forall i = 1, \ldots s$).

Definição 1.2.3. A *característica* de um anel A é o menor inteiro positivo n tal que $nx = 0$ para todo $x \in A$. Se tal n não existe nós dizemos que A tem característica 0. Denotamos por $car(A)$, a característica de A.

Teorema 1.2.4. *Seja A um anel com identidade 1. Se n é o menor inteiro positivo tal que $n \cdot 1 = 0$ temos que a característica de A é n. Se não existe um tal inteiro n, então a característica de A é 0.*

Demonstração. Se não existe n inteiro positivo tal que $n \cdot 1 = 0$, então pela definição de característica de A, $car(A) = 0$. Se n é o menor inteiro positivo tal que $n \cdot 1 = 0$ temos que $n \cdot x = n \cdot (1 \cdot x) = (n \cdot 1) \cdot x = 0$ para todo $x \in A$. Isto prova que $car(A) = n$. □

Teorema 1.2.5. *A característica de um domínio ou é 0 ou é um número primo.*

Demonstração. Seja D um domínio. Se $car(D) = 0$ não há nada a se provar. Suponha que $car(D) = n \neq 0$. Pelo teorema anterior, n é o menor inteiro positivo tal que $n.1 = 0$. Suponha que n não é primo. Então existem inteiros s, t tais que $n = st$ com $1 < s, t < n$. Assim $0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1)$ e como D é domínio, temos que $s \cdot 1 = 0$ ou $t \cdot 1 = 0$. Mas isto contraria o fato de n ser o menor inteiro positivo tal que $n \cdot 1 = 0$. Logo n é primo. □

Definição 1.2.6. Seja A um anel comutativo com identidade 1_A. Um *A-módulo M* é um grupo abeliano $(M, +)$ acrescido de uma operação "$\cdot$" que associa cada par $(r, x) \in A \times M$ a um elemento $r \cdot x \in M$, tal que pra todo $r, s \in A$ e $x, y \in M$ temos:

i. $r \cdot (x+y) = r \cdot x + r \cdot y$;

ii. $(r+s) \cdot x = r \cdot x + s \cdot x$;

iii. $(r \cdot s) \cdot x = r(s \cdot x)$;

iv. $1_A \cdot x = x$.

Se A é um corpo então M será um *A-espaço vetorial*.

Definição 1.2.7. Um A-módulo é dito *finitamente gerado* se existem $\beta_1, \ldots, \beta_m \in M$ tais que

$$M = A\beta_1 + \cdots + A\beta_m.$$

O conjunto $\{\beta_1, \ldots, \beta_m\}$ é chamado de um *conjunto gerador* de M. A notação $\langle \beta_1, \ldots, \beta_m \rangle$ também é usada para representar o A-módulo gerado por $\beta_1, \ldots, \beta_m$.

Definição 1.2.8. Um A-módulo M finitamente gerado é dito *livre* se ele admite um conjunto gerador finito cujos elementos são A-linearmente independentes.

Isto é, se existem $\beta_1, \ldots, \beta_n \in M$ com $n \in \mathbb{N}$ tais que $M = \langle \beta_1, \ldots \beta_n \rangle$ e

$$\beta_1 a_1 + \cdots + \beta_n a_n = 0 \Leftrightarrow a_1 = \cdots = a_n = 0.$$

O conjunto $\{\beta_1, \ldots, \beta_n\}$ é uma *base* de M e n é seu *posto*.

Observação 1.2.9. Dados um A-módulo M e $S \subset M$ um subconjunto não vazio, o conjunto $N = \langle S \rangle := \{\sum_{i=1}^{n} a_i s_i \mid a_i \in A,\ s_i \in S,\ i = 1, \ldots n \text{ e } n \in \mathbb{N}\}$ é fechado para as operações de M. Consequentemente, com estas operações, N é um A-módulo. Dizemos que N é *gerado pelo conjunto S.*

Quando um A-módulo N está contido em um A-módulo M e além disso, M e N têm as mesmas operações "$+$" e "$\cdot$", dizemos que N é um *A-submódulo* de M.

Ideais

Definição 1.2.10. Um subanel I de um anel A é chamado ideal de A se para todo $a \in A$ e todo $x \in I$, $x \cdot a \in I$ e $a \cdot x \in I$.

Definição 1.2.11. Seja I um ideal de um anel comutativo A.

1. I é um *ideal principal* de A se $I = \langle a \rangle = \{ax : x \in A\}$, ou seja, I é gerado por a.
2. I é um *ideal primo* de A se $I \neq A$ e para quaisquer $a, b \in A$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.
3. I é um *ideal maximal* de A se $I \neq A$ e sempre que J for um ideal próprio de A e $I \subseteq J$ então $J = I$.

Proposição 1.2.12. *Sejam A um anel comutativo com unidade e I um ideal de A.*

i O anel quociente A/I é um domínio de integridade se, e somente se, I é um ideal primo.

ii O anel quociente A/I é um corpo se, e somente se, I é um ideal maximal

Demonstração. Ver em [3] pag.11, Definição 2.1. □

Corolário 1.2.13. *Todo ideal maximal em um anel comutativo com unidade é também um ideal primo.*

Demonstração. Pela Proposição 1.2.12: I maximal $\Rightarrow A/I$ corpo $\Rightarrow A/I$ domínio $\Rightarrow I$ primo. □

Proposição 1.2.14. *Sejam A um anel e $\mathcal{S} = \{\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \dots\}$ uma cadeia ascendente de ideais de A, então*

$$\mathfrak{a} = \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$$

é um ideal de A.

Demonstração. Dados $a, b \in \mathfrak{a}$ e $r \in A$, temos que $a \in \mathfrak{a}_i$ e $b \in \mathfrak{a}_j$ para $i, j \in \mathbb{N}$. Suponha sem perda de generalidade que $\mathfrak{a}_i \subseteq \mathfrak{a}_j$. Então $a, b \in \mathfrak{a}_j$ e como $\mathfrak{a}_j$ é ideal, $0 \in \mathfrak{a}_j \subseteq \mathfrak{a}$, $a - b \in \mathfrak{a}_j \subseteq \mathfrak{a}$ e $r \cdot a \in \mathfrak{a}_j \subseteq \mathfrak{a}$. Logo $\mathfrak{a}$ é ideal de A. □

1.3 Teoria de Galois

Definição 1.3.1. Um corpo L é dito uma *extensão* de K, e denotamos isto por L/K, se L contém K como um subcorpo. O corpo K é chamado de corpo base da extensão L/K.

Exemplo 1.3.2. $\mathbb{R}$ é uma extensão de $\mathbb{Q}$.

Observação 1.3.3. Um fato importante sobre uma extensão de corpos L/K é que L é um K-espaço vetorial com a operação de adição sendo a do corpo L enquanto a multiplicação por escalar sendo a de L também:

$$u \cdot x = ux \qquad (u \in K, x \in L)$$

Definição 1.3.4. A dimensão de L como um K-espaço vetorial será chamada de *grau da extensão*, que será denotado por $[L : K]$. Uma extensão de corpos L/K é dita *finita* se $[L : K] < \infty$, caso contrário, é dita *infinita*. Ou seja,

$$L/K \text{ é finita} \Leftrightarrow L \text{ é um } K\text{-espaço vetorial de dimensão finita.}$$

Exemplo 1.3.5. $\mathbb{C}/\mathbb{R}$ é finita com $[\mathbb{C} : \mathbb{R}] = 2$. Basta notar que $\{1, i\}$ é uma base de $\mathbb{C}$.

Definição 1.3.6. O *corpo gerado* sobre K por uma coleção finita de elementos $\alpha_1, \ldots, \alpha_r \in L$, denotado por $K(\alpha_1, \ldots, \alpha_r)$ é o menor subcorpo de L contendo K e $\alpha_1, \ldots, \alpha_r$.

Definição 1.3.7. Uma extensão L/K é *finitamente gerada* se existem finitos elementos $\alpha_1, \ldots, \alpha_r \in L$ tais que $L = K(\alpha_1, \ldots, \alpha_r)$.

Exemplo 1.3.8. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ é uma extensão finitamente gerada de $\mathbb{Q}$. Note que o inverso de um elemento não nulo $a + b\sqrt{2}$ é $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$.

Definição 1.3.9. Um *corpo numérico* (ou *corpo numérico algébrico*) é uma extensão finita de corpo de $\mathbb{Q}$.

Definição 1.3.10. Seja L/K uma extensão de corpos. Um elemento $\alpha \in L$ é dito *algébrico* sobre K, se existe um polinômio não nulo $f(x) \in K[x]$ tal que $f(\alpha) = 0$.

Exemplo 1.3.11. Note que $i \in \mathbb{C}$ é raiz do polinômio $p(x) = x^2 + 1$, ou seja, é algébrico sobre $\mathbb{Q}$. Mas π não é algébrico sobre $\mathbb{Q}$. Este fato não é nenhum pouco elementar, sua demonstração pode ser verificada em [4], pág. 18, Proposição 3.4.

Definição 1.3.12. Seja L/K uma extensão de corpos e $\alpha \in L$ algébrico sobre K. O *polinômio minimal* de α sobre K, é o polinômio mônico de menor grau em $K[x]$ que tem α como raiz.

Definição 1.3.13. Um corpo L é dito uma *extensão algébrica* de K se todo elemento de L é algébrico sobre K.

Definição 1.3.14. Seja L/K um extensão de corpos e $\alpha \in L$. Definimos $K[\alpha] := \{p(\alpha) \mid p(x) \in K[x]\}$. Note que $K[\alpha]$ é um sub-domínio de L. Denotamos por $K(\alpha)$ o corpo de frações de $K[\alpha]$. Se α é algébrico sobre K então $K[\alpha] = K(\alpha)$. (vide 2.1 em [5])

Proposição 1.3.15. *Sejam L/K uma extensão de corpos e $\alpha \in L$ algébrico sobre K. Denote por n o grau o polinômio minimal de α sobre K. Então $[K(\alpha) : K] = n$ e $K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K, 0 \leq i \leq n-1\}$.*

Demonstração. Seja $p(x) \in K[x]$ o polinômio minimal de α sobre K. Por hipótese, $n = \text{grau } p(x)$. Para provar a proposição, basta mostrar que o conjunto $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é uma base de $K(\alpha)$ como um K-espaço vetorial. Como α é algébrico, $K(\alpha) = K[\alpha]$. Logo um elemento de $K(\alpha)$ é da forma $f(\alpha)$, $f(x) \in K[x]$. Dividindo $f(x)$ por $p(x)$, obtemos:

$$f(x) = p(x) \cdot q(x) + r(x), \quad q(x), r(x) \in K[x],$$

onde $r(x) = 0$ ou grau $r(x) <$ grau $p(x) = n$, isto é,

$$r(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}, \quad a_i \in K \quad \forall i = 0, 1, \ldots, n-1.$$

Fazendo $x = \alpha$ e usando o fato de $p(\alpha) = 0$:

$$f(\alpha) = p(\alpha) \cdot q(\alpha) + r(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}.$$

Logo, B gera $K(\alpha)$ como K-espaço vetorial. Agora, seja $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$ uma combinação linear de B com $b_i \in K \quad \forall i = 0, \ldots, n-1$. Se algum dos b_i fosse não nulo, o polinômio $g(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} \in K[x]$ seria não nulo, teria α como raiz e grau menor que n, o que seria um absurdo pois n é o grau do polinômio minimal de α sobre K. Logo, $b_i = 0 \; \forall i$ e isto mostra que B é linearmente independente. Portanto, B é base de $K(\alpha)/K$. □

Definição 1.3.16. O *corpo de raízes* ou *corpo de decomposição* de um polinômio $f(x) \in K[x]$ o menor corpo contendo K e todas as raízes de $f(x)$.

Exemplo 1.3.17. O corpo de raízes do polinômio $f(x) = x^2 - 2$ sobre $\mathbb{Q}$ é o corpo $\mathbb{Q}(\sqrt{2})$. Note que $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Definição 1.3.18. O *fecho algébrico* de um corpo K, denotado por $\overline{K}$, é um corpo algébrico sobre K onde todo polinômio não constante $f(x) \in K[x]$ se fatora em polinômios de grau 1 com coeficientes em $\overline{K}$.

Exemplo 1.3.19. Temos que $\overline{\mathbb{R}} = \mathbb{C}$. De fato, essa é uma consequência do Teorema Fundamental da Álgebra, que afirma que todo polinômio não constante $p(x) \in \mathbb{C}[x]$ tem alguma raiz complexa.

Observação 1.3.20. Uma raiz α de um polinômio $f(x)$ é dita *simples* se $(x - \alpha)$ divide $f(x)$, mas $(x - \alpha)^2$ não divide $f(x)$.

Definição 1.3.21. Um polinômio irredutível $p(x) \in K[x]$ é *separável* sobre K se todas as suas raízes são simples em seu corpo de raízes.

Definição 1.3.22. Dada uma extensão L/K, um elemento $\alpha \in L$ é dito *separável* sobre K se α é raiz de um polinômio separável em $K[x]$. Em particular, α é algébrico sobre K.

Definição 1.3.23. Uma extensão algébrica L/K é chamada *separável* se todo elemento de L é separável sobre K.

Observação 1.3.24. Toda extensão algébrica L/K tal que $L \subset \mathbb{C}$ é separável. (vide Prop. 3.6 em [5]).

Definição 1.3.25. Para extensões F/K e L/K, denotaremos $\mathrm{Mono}_K(L, F)$ o conjunto de todos homomorfismos injetivos $\varphi : L \to F$ tais que $\varphi(x) = x$ para todo $x \in K$.

Definição 1.3.26. Dada uma extensão finita L/K e $\alpha \in L$ algébrico sobre K, um elemento $\beta \in \overline{K}$ é um *conjugado* de α se existe $\varphi \in \mathrm{Mono}(L, \overline{K})$ tal que $\varphi(\alpha) = \beta$. Pode-se provar que $\mathrm{Mono}(L, \overline{K})$ tem no máximo $[L : K]$ elementos, logo existe um número finito de conjugados de α.

Definição 1.3.27. Uma extensão L/K é *normal* se $\varphi(E) = E$ para todo $\varphi \in \mathrm{Mono}_K(E, \overline{K})$.

Teorema 1.3.28. *Uma extensão finita E/K é normal se, e somente se, é o corpo de decomposição para algum polinômio $p(x) \in K[x]$.*

Demonstração em [6], pág. 54, teorema 3.80.

Definição 1.3.29. Seja K um corpo, uma extensão E/K é chamada *galoisiana* se é normal e separável.

Definição 1.3.30. Para uma extensão finita galoisiana E/K, o grupo

$$\mathrm{Gal}(E/K) = \mathrm{Aut}_K(E)$$

é chamado de grupo galoisiano da extensão ou grupo galoisiano de E sobre K. Os elementos de $\mathrm{Gal}(E/K)$ são automorfismos de E (ou seja, homomorfismos bijetivos de E em E) que fixam os elementos de K.

1.4 Traço e discriminante

Definição 1.4.1. Seja L/K uma extensão finita de corpos. Para $\alpha \in L$, seja $m_\alpha : L \to L$ a transformação linear do K-espaço vetorial L definida pela multiplicação por α.

- A aplicação *traço* $\mathrm{Tr}_{L/K} : L \to K$ é definida por $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}\ m_\alpha$ para $\alpha \in L$,

onde $\mathrm{tr}\ A$ é a soma dos elementos da diagonal principal da matriz A.

Definição 1.4.2. Sejam K um corpo e V um K-espaço vetorial de dimensão finita. Uma forma *K-bilinear* (ou simplesmente, *forma bilinear*) $\Psi : V \times V \to K$ em V é uma função que satisfaz para quaisquer $\lambda \in K$ e $u, v \in V$:

- $\Psi(u+v, w) = \Psi(u, w) + \Psi(v, w)$;
- $\Psi(u, v+w) = \Psi(u, v) + \Psi(u, w)$;
- $\Psi(\lambda v, w) = \lambda\Psi(v, w) = \Psi(v, \lambda w)$.

Definição 1.4.3. Uma forma K-bilinear Ψ em um K-espaço vetorial V é dita *simétrica* se para todo $v, w \in V$,

$$\Psi(v, w) = \Psi(w, v).$$

Exemplo 1.4.4. Tome uma matriz $Q \in M_n(K)$. Podemos definir uma forma bilinear em K^n por

$$\Psi(v, w) = v^T Q w$$

para $v, w \in K^n$, onde v^T denota a transposta do vetor coluna v. Temos que Ψ é simétrica se, e somente se, Q é simétrica, isto é, $Q^T = Q$.

Se Ψ é simétrica então seja $Q = (q_{ij})$. Se $\{e_1, e_2, \ldots, e_n\}$ é a base canônica de K^n então $\forall i, j = 1, \ldots, n$:

$$\Psi(e_i, e_j) = e_i^T Q e_j = q_{ij}$$

$$\Psi(e_j, e_i) = e_j^T Q e_i = q_{ji}$$

Como Ψ é simétrica, $\Psi(e_i, e_j) = \Psi(e_j, e_i)$, logo, $q_{ij} = q_{ji}$, $\forall i, j = 1, \ldots, n$. Portanto $Q = Q^T$.
Por outro lado, se $Q = Q^T$

$$\Psi(v, w) = v^T Q w = (Q^T v)^T w = w^T Q^T v = w^T Q v = \Psi(w, v)$$

Exemplo 1.4.5. Se L/K é um extensão finita de corpos, então $\Psi : L \times L \to K$ definida por

$$\Psi(\alpha, \beta) = \mathrm{Tr}_{L/K}(\alpha\beta)$$

para $\alpha, \beta \in L$, é uma forma K-bilinear simétrica em L. A verificação é imediata, pois como L é corpo, $\alpha\beta = \beta\alpha$.

Definição 1.4.6. O *discriminante* de uma forma bilinear Ψ em um espaço vetorial de dimensão finita V relativo à base ordenada $(v_1, ..., v_n)$ de V é o determinante da matriz $(\Psi(v_i, v_j))_{i,j}$.

Lema 1.4.7. *Seja $\Psi : V \times V \to K$ uma forma K-bilinear em um espaço vetorial V de dimensão finita $n \geq 1$. Sejam $v_1, ..., v_n \in V$ e $T : V \to V$ uma transformação linear. Então:*

$$det(\Psi(Tv_i, Tv_j)) = (detT)^2 \cdot det(\Psi(v_i, v_j)).$$

Demonstração. (1^o caso) Suponhamos que $\{v_1, v_2, \ldots, v_n\}$ é uma base de V. Seja $A = (a_{ij})$ a matriz de T com respeito a base ordenada $(v_1, ..., v_n)$. Temos:

$$\Psi(Tv_i, Tv_j) = \sum_{k=1}^{n} a_{ik} \sum_{l=1}^{n} a_{jl} \Psi(v_k, v_l).$$

Como matrizes, temos então:

$$\Psi(Tv_i, Tv_j) = A(\Psi(v_i, v_j))A^T,$$

$$\det(\Psi(Tv_i, Tv_j)) = \det(A(\Psi(v_i, v_j))A^T),$$

$$\det(\Psi(Tv_i, Tv_j)) = \det A \cdot \det(\Psi(v_i, v_j)) \cdot \det A^T,$$

e o resultado segue do fato de $detT = detA = detA^T$.

(Caso geral) Se os v_i formam uma base de V, então para quaisquer $w_1, ..., w_n \in V$ existe uma

transformação $U : V \to V$ com $U(v_i) = w_i$ para todo i. Nós então temos:

$$det(\Psi(Tw_i, Tw_j)) = det(\Psi(TUv_i, TUv_j)) = det(TU)^2 \cdot det(\Psi(v_i, v_j)) =$$

$$= det(T)^2 \cdot det(U)^2 \cdot det(\Psi(v_i, v_j)) = det(T)^2 \cdot det(\Psi(w_i, w_j)),$$

onde a segunda e a última igualdade seguem do 1º caso. □

Observação 1.4.8. Seja $\Psi : V \times V \to K$ uma forma K-bilinear num espaço vetorial de dimensão finita $n \geq 1$. Então o Lema 1.4.7 implica o seguinte:

a. O discriminante de Ψ relativo a uma base ordenada $(v_1, \ldots, v_n)$ de V independe da ordem desses vetores. De fato, seja $(v_{\varphi(1)}, \ldots, v_{\varphi(n)})$ uma reordenação base e seja $T : V \to V$ a transformação tal que $T(v_i) = v_{\varphi(i)}$. A matriz de T é obtida da matriz identidade através de um número finito de permutações de suas colunas. Uma vez que a permutação das colunas de uma matriz muda apenas o sinal do seu determinante, temos que $(\det T)^2 = (\pm 1)^2 = 1$. O resultado segue do lema 1.4.7.

b. Temos $det(\Psi(v_i, v_j)) = 0$ se $v_1, ..., v_n \in V$ são linearmente dependentes.

Definição 1.4.9. Seja L/K um extensão finita de corpos. O *discriminante de L/K relativo a uma base $B = \{\beta_1, \ldots \beta_n\}$* de L como um K-espaço vetorial é o discriminante da forma bilinear

$$(\alpha, \beta) \mapsto Tr_{L/K}(\alpha\beta)$$

relativo à base B. Denotaremos este discriminante por $D(\beta_1, \ldots, \beta_n)$. Assim:

$$D(\beta_1, \ldots, \beta_n) = det((Tr_{L/K}(\beta_i \beta_j)).$$

Definição 1.4.10. Seja K um corpo e seja $\alpha_1, ..., \alpha_n \in K$. Então a matriz

$$Q(\alpha_1, ..., \alpha_n) = \begin{bmatrix} 1 & \alpha_1 & ... & \alpha_1^{n-1} \\ 1 & \alpha_2 & ... & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & ... & \alpha_n^{n-1} \end{bmatrix}$$

é chamada de *matriz Vandermonde* para $\alpha_1, ..., \alpha_n$.

Lema 1.4.11. *Seja K um corpo, e seja $Q(\alpha_1, ..., \alpha_n)$ a matriz Valdermonde para os elementos $\alpha_1, ..., \alpha_n$ de K. Então*

$$detQ(\alpha_1, ..., \alpha_n) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i).$$

Demonstração. Faremos por indução em $n \geq 1$, no caso $n = 1$ é imediato que $detQ(\alpha) = 1$ para qualquer $\alpha \in K$. Para calcular o determinante de $Q = Q(\alpha_1, ..., \alpha_n)$, subtraia $\alpha_1 \times i-$ésima

coluna de sua $(i+1)-$ésima coluna de cada $1 \leq i \leq n-1$, o que não altera o determinante. Nós então obtemos:

$$detQ = det \begin{bmatrix} 1 & 0 & ... & 0 \\ 1 & \alpha_2 - \alpha_1 & ... & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n - \alpha_1 & ... & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{bmatrix} = det \begin{bmatrix} \alpha_2 - \alpha_1 & ... & \alpha_2^{n-2}(\alpha_2 - \alpha_1) \\ \vdots & & \vdots \\ \alpha_n - \alpha_1 & ... & \alpha_n^{n-2}(\alpha_n - \alpha_1) \end{bmatrix} =$$

$$= det \begin{bmatrix} \alpha_2 - \alpha_1 & 0 & \dots & 0 \\ 0 & \alpha_3 - \alpha_1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \alpha_n - \alpha_1 \end{bmatrix} \cdot det \begin{bmatrix} 1 & \alpha_2 & \dots & \alpha_2^{n-2} \\ 1 & \alpha_3 & \dots & \alpha_3^{n-2} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{n-2} \end{bmatrix}$$

Logo, como o determinante de uma matriz diagonal é o produto dos elementos da diagonal principal, pela hipótese da indução segue o resultado. □

Proposição 1.4.12. *Suponha que L/K é uma extensão separável de grau n, e seja $\alpha \in L$ tal que $L = K(\alpha)$. Então*

$$D(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2 \neq 0,$$

onde $\alpha_1, \dots, \alpha_n$ são os conjugados de α em um fecho algébrico de K.

Demonstração. [7], Proposição 1.4.13, p.24. □

Capítulo 2

Anéis Noetherianos e Extensões Inteiras

2.1 Anéis Noetherianos

Seja A um anel comutativo com unidade. Provaremos que as seguintes propriedades são equivalentes:

1. Todo ideal $\mathfrak{a}$ de A é finitamente gerado.

2. Toda cadeia ascendente de ideais de A estabiliza, isto é, dado $\mathcal{S}$ uma cadeia de ideais

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq ...$$

   para algum $i \in \mathbb{N}$ temos $\mathfrak{a}_i = \mathfrak{a}_j$, para todo $j > i$.

3. Toda coleção não vazia $\mathcal{S}$ de ideais possui um ideal que é maximal em $\mathcal{S}$ com relação à inclusão.

Demonstração. $(1) \Rightarrow (2)$ Seja $\mathcal{S} = \{a_n\}_{n\in\mathbb{N}}$ uma cadeia ascendente de ideais. Tome $\mathfrak{a} = \bigcup_{n\in\mathbb{N}} \mathfrak{a}_n$ que pela proposição 1.2.14 é ideal de A. Sejam $a_1, a_2, ..., a_n \in A$ geradores de $\mathfrak{a}$, onde cada $a_i \in \mathfrak{a}_{\lambda_i}$ para $i = 1, ..., n$. Suponha sem perda de generalidade que para todo $i = 1, ..., n-1$, $\mathfrak{a}_{\lambda_i} \subseteq \mathfrak{a}_{\lambda_n}$. Assim $a_1, a_2, ..., a_n \in \mathfrak{a}_{\lambda_n}$, portanto $\mathfrak{a} \subseteq \mathfrak{a}_{\lambda_n}$ e como $\mathfrak{a}_{\lambda_n} \subseteq \mathfrak{a}$ temos $\mathfrak{a} = \mathfrak{a}_{\lambda_n}$. Logo para todo $n > \lambda_n$, teremos $\mathfrak{a} = \mathfrak{a}_n$. Logo a cadeia S estabiliza.

$(2) \Rightarrow (3)$ Suponha que $\mathcal{S}$ não possua elemento maximal e seja $\mathfrak{a}_0$ um ideal qualquer de $\mathcal{S}$. Como $\mathcal{S}$ não possui elemento maximal, então $\exists \mathfrak{a}_1 \in \mathcal{S}$ tal que $\mathfrak{a}_0 \subsetneq \mathfrak{a}_1$. Repetindo o argumento anterior para o ideal $\mathfrak{a}_1$, $\exists \mathfrak{a}_2 \in \mathcal{S}$ tal que $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2$. Por indução construímos uma cadeia ascendente de ideais:

$$\mathfrak{a}_0 \subsetneq \mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \mathfrak{a}_3 \subsetneq ...,$$

que não estabiliza, o que é uma contradição. Logo $\mathcal{S}$ possui um elemento maximal.

$(3) \Rightarrow (1)$ Suponha por absurdo que $\mathfrak{a}$ seja um ideal de A que não é finitamente gerado. Seja

$\mathcal{S}$ a coleção de ideais próprios de $\mathfrak{a}$ construída da seguinte forma:

$$\mathcal{S} = \{\langle a_1\rangle, \langle a_1, a_2\rangle, \langle a_1, a_2, a_3\rangle, \ldots | a_i \in \mathfrak{a} \text{ e } a_{i+1} \notin \langle a_1, ..., a_i\rangle, i \in \mathbb{N}\}$$

Note que como $\mathfrak{a}$ não é finitamente gerado, $\forall i \in \mathbb{N}$, $\exists a_{i+1} \in \mathfrak{a}$ tal que $a_{i+1} \notin \langle a_1, \ldots, a_i\rangle$. Segue que $\mathcal{S}$ não tem elemento maximal, o que contradiz a hipótese. Logo $\mathfrak{a}$ é finitamente gerado. □

Definição 2.1.1. Um anel A é *Noetheriano* se satisfaz qualquer uma (e portanto todas) das propriedades 1,2 e 3 anteriores.

Observação 2.1.2. Em um anel Noetheriano, todo ideal próprio está contido em um ideal maximal do anel. Isto decorre da Propriedade 2 da definição de anel Noetheriano. Para anéis comutativos com unidade em geral, esta afirmação também é verdadeira, mas é necessário utilizar o axioma da escolha (equivalentemente, o Lema de Zorn) em sua demonstração. Vide Teorema 0.27 de [5].

Proposição 2.1.3. *Se A é um anel Noetheriano e M é um A-módulo finitamente gerado, então todo A-submódulo de M é finitamente gerado.*

Demonstração. [8], proposição 1.4, p.28. □

2.2 Extensões Inteiras

Definição 2.2.1. Dizemos que B/A é uma *extensão* de anéis comutativos se A e B são anéis comutativos e A é um subanel de B.

Definição 2.2.2. Seja B/A uma extensão de anéis comutativos com unidade. Dizemos que $\beta \in B$ é inteiro sobre A se β é raiz de um polinômio mônico em $A[x]$.

Exemplos 2.2.3. .

1. Todo elemento $a \in A$ é inteiro sobre A, pois é raiz do polinômio $x - a$.
2. Se L/K é uma extensão de corpo e $\alpha \in L$ é algébrico sobre K, então α é inteiro sobre K, sendo raiz de seu polinômio minimal que é mônico.
3. O elemento $\sqrt{2}$ de $\mathbb{Q}(\sqrt{2})$ é inteiro sobre $\mathbb{Z}$, sendo raiz do polinômio $x^2 - 2$.

Proposição 2.2.4. *Seja B/A uma extensão de anéis comutativos com unidade. Para $\beta \in B$, as seguintes condições são equivalentes:*

i. O elemento β é inteiro sobre A;

ii. Existe $n \geq 0$ tal que $\{1, \beta, \beta^2 \ldots, \beta^n\}$ geram $A[\beta]$ como um A-módulo;

iii. O anel $A[\beta]$ é um A-módulo finitamente gerado;

iv. Existe um A-submódulo finitamente gerado M de B tal que $\beta M \subseteq M$.

Demonstração.

$(i) \Rightarrow (ii)$ Se β é inteiro sobre A, β é raiz de um polinômio monico $g \in A[x]$. Para todo $f \in A[x]$, pelo algoritmo da divisão $f = qg + r$ com $q, r \in A[x]$ temos que ou $r = 0$ ou $grau\, r < grau\, g$. Daí segue que $f(\beta) = r(\beta)$, concluímos que $f(\beta)$ pertence ao A-submódulo gerado por $\{1, \beta, \ldots, \beta^{(grau\, g)-1}\}$, portanto segue (ii).

$(ii) \Rightarrow (iii)$ Consequência direta da hipótese.

$(iii) \Rightarrow (iv)$ Basta tomar $M = A[\beta]$.

$(iv) \Rightarrow (i)$ Seja $M = A[\delta_1, \ldots, \delta_n] \subseteq B$ tal que $\beta M \subseteq M$. Temos que $\forall i = 1, \ldots n, \exists a_{ij} \in A$ com $j = 1, \ldots, n$ tais que:

$$\beta\delta_i = \sum_{j=1}^{n} a_{ij}\delta_j.$$

Por definição, β é um autovalor para um autovetor $(\delta_1, \ldots, \delta_j)$ de $T : B^n \to B^n$ definido pela matriz quadrada (a_{ij}). O polinômio característico $f(x) = char(xI - (a_{ij}))$ de T é mônico e tem β como raiz, assim segue (i). □

Definição 2.2.5. Seja B/A uma extensão de anéis comutativos com unidade. Dizemos que B é uma *extensão inteira* de A se todo elemento de B é inteiro sobre A.

Lema 2.2.6. *Suponha que B/A é uma extensão de anéis comutativos tal que B é um A-módulo finitamente gerado, e seja M um B-submódulo finitamente gerado. Então M é um A-módulo finitamente gerado.*

Demonstração. Em [9], Proposição 2.16, p.28. □

Proposição 2.2.7. *Seja B/A uma extensão de anéis comutativos com unidade e suponha que*

$$B = A[\beta_1, \beta_2, \ldots \beta_k]$$

onde $\beta_i \in B$ com $1 \leq i \leq k$. Isto significa que os elementos de B são dados por expressões polinomiais em $\beta_1, \beta_2, \ldots \beta_k$ com coeficientes em A. Então os seguintes itens são equivalentes.

i. O anel B é inteiro sobre A;

ii. Cada β_i com $1 \leq i \leq k$ é inteiro sobre A;

iii. O anel B é um A-módulo finitamente gerado.

Demonstração. $(i) \Rightarrow (ii)$ é trivial.

$(ii) \Rightarrow (iii)$ Fazemos indução em k.

Para $k = 1$, o resultado segue da proposição 2.2.4. Supondo que o resultado vale para $k \geq 1$, temos que $B_k := A[\beta_1, \ldots, \beta_k]$ é A-módulo finitamente gerado. Seja $B_{k+1} := A[\beta_1, \ldots, \beta_{k+1}]$ com

cada β_i inteiro sobre A. Então β_{k+1} é inteiro sobre B_k. Segue da proposição 2.2.4 que B_{k+1} é um B_k-módulo finitamente gerado. Pelo Lema 2.2.6, B_{k+1} é um A-módulo finitamente gerado.

$(iii) \Rightarrow (i)$ Para todo $\beta \in B$, $\beta B \subset B$. Pela proposição 2.2.4, β é inteiro sobre A. □

Proposição 2.2.8. *(Transitividade de Extensões Inteiras) Suponha que C/B e B/A são extensões inteiras de anéis comutativos com unidade. Então C/A é uma extensão inteira.*

Demonstração. Dado $\delta \in C$, existe $f(x) = x^n + b_{n-1}X^{n-1} + \cdots + b_0 \in B[x]$ tal que $f(\delta) = 0$. Seja $B' = A[b_0, \ldots, b_{n-1}] \subset B$. Como cada b_i é inteiro sobre A, pela Proposição 2.2.7, B' é um A-módulo finitamente gerado. Como δ é inteiro sobre B', pela Proposição 2.2.4, $B'[\delta]$ é B'-módulo finitamente gerado. Pelo Lema 2.2.6, $B'[\delta]$ é um A-módulo finitamente gerado. Pela Proposição 2.2.7, $B'[\delta]$ é inteiro sobre A, portanto δ é inteiro sobre A. □

Definição 2.2.9. Seja B/A uma extensão de anéis comutativos com unidade. Então o *fecho inteiro de A em B* é o conjunto de elementos de B que são inteiros sobre A.

Proposição 2.2.10. *Seja B/A uma extensão de anéis comutativos com unidade. Então o fecho inteiro de A em B é um subanel de B.*

Demonstração. Sejam $x, y \in B$ inteiros sobre A. Pela Proposição 2.2.7, $A[x,y]$ é inteiro sobre A. Como $x \pm y, x \cdot y \in A[x,y]$ segue que esses elementos são inteiros sobre A. Portanto, o fecho inteiro de A é um subanel de B. □

Definição 2.2.11. Seja B/A uma extensão de anéis comutativos com unidade. Dizemos que A é *integralmente fechado* em B se A é seu próprio fecho inteiro em B.

Dizemos que um domínio de integridade A é integralmente fechado se ele é integralmente fechado em seu corpo de frações.

Observação 2.2.12. Todo corpo é integralmente fechado. De fato, o corpo de frações de K é o próprio K e $\alpha \in K \Rightarrow \alpha$ é raiz de $x - \alpha \in K[x]$. Logo todo elemento de K é inteiro sobre K.

Proposição 2.2.13. *Sejam A um domínio integralmente fechado, K seu corpo quociente e seja L/K uma extensão de corpos. Se $\beta \in L$ é inteiro sobre A com polinômio minimal $f \in K[x]$, então $f \in A[x]$.*

Demonstração. Em [7], Proposição 1.2.18, p.16. □

Proposição 2.2.14. *Sejam A um domínio de fatoração única, K o corpo quociente de A e L/K uma extensão de corpos. Suponha que $\beta \in L$ é algébrico sobre K com polinômio minimal $f \in K[x]$. Se β é inteiro sobre A, então $f \in A[x]$.*

Demonstração. [7], Proposição 1.2.19, p.17. □

Corolário 2.2.15. *Todo domínio de fatoração única é integralmente fechado.*

Demonstração. Seja A um domínio de fatoração única e K seu corpo de frações. Seja $a \in K$ inteiro sobre A. Evidentemento a é algébrico sobre K com polinômio minimal $f(x) = x - a$. Pela Proposição 2.2.14, $f(x) \in A[x]$, logo $a \in A$. Portanto, A é integralmente fechado. □

Proposição 2.2.16. *Seja B/A uma extensão de anéis comutativos com unidade, e suponha que B é um domínio integralmente fechado. Então o fecho inteiro de A em B é integralmente fechado.*

Demonstração. Denote por $\tilde{A}$ o fecho inteiro de A em B e seja K o seu corpo de frações. Dado $\alpha \in K$ inteiro sobre $\tilde{A}$, temos que mostrar que $\alpha \in \tilde{A}$. Pela Proposição 2.2.7, $\tilde{A}[\alpha]$ é inteiro sobre $\tilde{A}$. Como $\tilde{A}$ é inteiro sobre A, pela Proposição 2.2.8, $\tilde{A}[\alpha]$ é inteiro sobre A. Segue que α é inteiro sobre A e portanto, $\alpha \in \tilde{A}$. □

Definição 2.2.17. O *anel dos inteiros* O_K de um corpo numérico K é o fecho inteiro de $\mathbb{Z}$ em K.

Definição 2.2.18. Seja B/A uma extensão inteira de domínio tal que A é integralmente fechado, e suponha que B é livre de posto n como um A-módulo. Seja $\{\beta_1, \ldots, \beta_n\}$ uma base ordenada de B como um A-módulo livre. O discriminante B sobre A relativo à base $\{\beta_1, \ldots, \beta_n\}$ é o elemento $D(\beta_1, \ldots, \beta_n) \in A$.

Lema 2.2.19. *Sejam K um corpo numérico e O_K o seu anel dos inteiros. Então O_K é um $\mathbb{Z}$-módulo livre de posto $[K : \mathbb{Q}]$ e o discriminante de O_K sobre $\mathbb{Z}$ é independente da escolha da base ordenada de O_K como um $\mathbb{Z}$-módulo.*

Demonstração. [7], Lema 1.4.25. p.27. □

Definição 2.2.20. Se K é um corpo numérico, então o *discriminante de K* $disc(K)$, é o discriminante de O_K sobre $\mathbb{Z}$ relativo a qualquer uma das bases de O_K como um $\mathbb{Z}$-modulo livre.

Capítulo 3

Domínios de Dedekind

3.1 Ideais fracionários

Definição 3.1.1. Um *ideal fracionário* de um domínio A é um A-submódulo $\mathfrak{a}$ diferente de zero do corpo quociente de A para o qual existe um $d \in A$, $d \neq 0$ tal que $d\mathfrak{a} \subseteq A$.

Observação 3.1.2. Todo ideal diferente de zero em um domínio A é um ideal fracionário, sendo referido algumas vezes como *ideal inteiro*. Note que todo ideal fracionário de A que está contido em A é um ideal inteiro.

Exemplo 3.1.3. Os ideais fracionários de $\mathbb{Z}$ são exatamente os $\mathbb{Z}$-submódulos de $\mathbb{Q}$ gerados por um número racional diferente de zero. De fato, seja $\mathfrak{a}$ ideal fracionário de $\mathbb{Z}$. Então $\exists d \in \mathbb{Z}$ tal que $d\mathfrak{a} \subseteq \mathbb{Z}$. Como $\mathfrak{a}$ é um $\mathbb{Z}$-módulo e $d \in \mathbb{Z}$, temos que $d\mathfrak{a}$ é um ideal de $\mathbb{Z}$. Como $\mathbb{Z}$ é um domínio de ideais principais, $\exists a \in \mathbb{Z}$ tal que $d\mathfrak{a} = \langle a \rangle$, portanto $\mathfrak{a} = \langle \frac{a}{d} \rangle$.

Lema 3.1.4. *Seja A um Domínio Noetheriano. Um A-submódulo diferente de zero do corpo de frações de A é um ideal fracionário se, e somente se, ele é finitamente gerado.*

Demonstração. ($\Rightarrow$) Se $\mathfrak{a}$ é um ideal fracionário de A, então $\exists d \in A$ tal que $d\mathfrak{a} \subseteq A$. Note que $d\mathfrak{a}$ é um ideal de A. Sendo A um domínio Noetheriano $d\mathfrak{a} = \langle b_1, \ldots, b_n \rangle$. Então $\mathfrak{a} = \langle \frac{b_1}{d}, \ldots, \frac{b_n}{d} \rangle$ e portantoé finitamente gerado.

($\Leftarrow$) Seja $\mathfrak{a}$ um A-módulo finitamente gerado contido no corpo de frações de A. Então $\mathfrak{a} = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle$. Tomando $d = b_1, \ldots, b_n$, teremos $d\mathfrak{a} \subseteq A$.

□

Definição 3.1.5. Seja A um domínio com corpo de frações K, e sejam $\mathfrak{a}$ e $\mathfrak{b}$ ideais fracionários de A. Definimos:

1. O *inverso* de $\mathfrak{a}$ é $\mathfrak{a}^{-1} = \{b \in K | b\mathfrak{a} \subseteq A\}$. Note que pela definição de ideal fracionário, $\mathfrak{a}^{-1} \neq \{0\}$.

2. O *produto* de $\mathfrak{a}$ e $\mathfrak{b}$ é o A-submódulo de K gerado pelo conjunto $\{ab | a \in \mathfrak{a} \text{ e } b \in \mathfrak{b}\}$.

3. Dado $n \in \mathbb{Z}$, definimos a potência $\mathfrak{a}^n$ da seguinte forma:

   - Se $n = 0$ ou $n = 1$, definimos $\mathfrak{a}^0 := A$ e $\mathfrak{a}^1 := \mathfrak{a}$.
   - Se $n > 1$, definimos $\mathfrak{a}^n$ por indução, pondo $\mathfrak{a}^n = \mathfrak{a}^{n-1} \cdot \mathfrak{a}$.
   - Se $n < 0$ definimos $\mathfrak{a}^n = (\mathfrak{a}^n)^{-1}$.

Observação 3.1.6. O inverso como definido em 3.1.5 é um A-submódulo de K.

Para isso, basta mostrar que $\mathfrak{a}^{-1}$ é um grupo aditivo de K fechado para "$\cdot$".

Dados $b_1, b_2 \in \mathfrak{a}^{-1}$ e $a \in \mathfrak{a}$, temos que $b_1 a$, $b_2 a \in \mathfrak{a}$, logo, $(b_1 - b_2)a = b_1 a - b_2 a \in \mathfrak{a}$ pois $\mathfrak{a}$ é um A-módulo. Se $c \in A$ então $(c \cdot b_1) \cdot a = c \cdot (b_1 a) \in \mathfrak{a}$ pois $b_1 a \in \mathfrak{a}$ é um A-módulo. Segue que $\mathfrak{a}^{-1}$ é um A-submódulo de K.

Observação 3.1.7. Pela definição, a multiplicação de ideais fracionários em um domínio é uma operação associativa e comutativa.

Lema 3.1.8. *Seja A um domínio com corpo de frações K e sejam $\mathfrak{a}$ e $\mathfrak{b}$ ideais fracionários de A. Então $\mathfrak{a}+\mathfrak{b}, \mathfrak{a}\mathfrak{b}, \mathfrak{a} \cap \mathfrak{b}$ e $\mathfrak{a}^{-1}$ são ideais fracionários de A.*

Demonstração. Sejam $d, d' \in A$ tais que $d\mathfrak{a} \subset A$ e $d'\mathfrak{b} \subset A$. Evidentemente $dd'(\mathfrak{a}+\mathfrak{b}) \subset A$. Temos $dd'(\mathfrak{a}+\mathfrak{b}) = d'(d\mathfrak{a}) + d(d'\mathfrak{b}) \subset A$, pois por hipótese, $d\mathfrak{a} \subset A$ e $d'\mathfrak{b} \subset A$ e $d, d' \in A$. Por fim $d \cdot d'(\mathfrak{a}\mathfrak{b}) = (d\mathfrak{a})(d'\mathfrak{b}) \subset A$.

Por fim, vamos provar que $\mathfrak{a}^{-1}$ é um ideal fracionário. Seja $a \in \mathfrak{a}$, $a \neq 0$. Existem $e, f \in A$ com $f \neq 0$ tais que $a = \frac{e}{f}$. Como $\mathfrak{a}$ é um A-submódulo de K e $a \in \mathfrak{a}$, segue que $e = f \cdot a \in \mathfrak{a}$. Dado qualquer $b \in \mathfrak{a}^{-1}$, pela definição de $\mathfrak{a}^{-1}$, temos que $b \cdot e \in A$. Portanto, $e \cdot \mathfrak{a}^{-1} \subset A$. Como $\mathfrak{a}^{-1}$ é um A-submódulo não nulo de K, segue que $\mathfrak{a}^{-1}$ é um ideal fracionário. □

Definição 3.1.9. Dizemos que um ideal fracionário $\mathfrak{a}$ de um domínio A é *invertível* se existe um ideal fracionário $\mathfrak{b}$ de A tal que $\mathfrak{a}\mathfrak{b} = A$.

Lema 3.1.10. *Um ideal fracionário $\mathfrak{a}$ de um domínio A é invertível se e somente se $\mathfrak{a}\mathfrak{a}^{-1} = A$.*

Demonstração. Seja $\mathfrak{a}$ um ideal fracionário de um domínio A. Pelo Lema 3.1.8, $\mathfrak{a}^{-1}$ é um ideal fracionário de A. Portanto, se $\mathfrak{a} \cdot \mathfrak{a}^{-1} = A$ então A é invertível. Reciprocamente, suponha que $\mathfrak{a}$ seja invertível. Então existe ideal fracionário $\mathfrak{b}$ tal que $\mathfrak{a} \cdot \mathfrak{b} = A$. Pela definição de $\mathfrak{a}^{-1}$, temos que $\mathfrak{b} \subset \mathfrak{a}^{-1}$. Como A é comutativo:

$$A = \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a} \subset \mathfrak{a}\mathfrak{a}^{-1} \subset A.$$

Portanto, $\mathfrak{a} \cdot \mathfrak{a}^{-1} = A$ como queríamos. □

Exemplo 3.1.11. Considere o ideal maximal $\langle x, y \rangle$ de $\mathbb{Q}[x, y]$. Se $f \in \mathbb{Q}(x, y)$, $f \neq 0$, é tal que $fx \in \mathbb{Q}[x, y]$(resp.,$fy \in \mathbb{Q}[x, y]$) então seu denominador é um divisor de x (resp.,y). Assim sendo$\langle x, y \rangle^{-1} = \mathbb{Q}[x, y]$, e teremos

$$\langle x, y \rangle \langle x, y \rangle^{-1} = \langle x, y \rangle \neq \mathbb{Q}[x, y].$$

Portanto $\langle x, y\rangle$ é um ideal fracionário não invertível.

Definição 3.1.12. Um ideal fracionário de A é dito *principal* se ele é um A-submódulo $\langle a\rangle$ gerado por um elemento a diferente de zero do corpo quociente de A.

Lema 3.1.13. *Seja A um domínio, e seja a um elemento diferente de zero de seu corpo quociente. Então $\langle a\rangle$ é invertível, e $\langle a\rangle^{-1} = \langle a^{-1}\rangle$.*

Demonstração. Primeiramente, mostraremos que $\langle a\rangle^{-1} = \langle a^{-1}\rangle$. Se $x \in \langle a\rangle^{-1}$ então $xa = b$, $b \in A$, logo $x = ba^{-1} \in \langle a^{-1}\rangle$. Portanto $\langle a\rangle^{-1} \subset \langle a^{-1}\rangle$. Reciprocamente, se $x \in \langle a^{-1}\rangle$ então $\exists b \in A$ tal que $x = b\mathfrak{a}^{-1}$. Um elemento de $\langle a\rangle$ é da forma $c \cdot a$, $c \in A$. Temos:

$$x \cdot c \cdot a = ba^{-1}ca = bca^{-1}a = bc \in A.$$

Portanto $x \in \langle a\rangle^{-1}$ e daí, $\langle a\rangle^{-1} \supset \langle a^{-1}\rangle$. Segue que $\langle a\rangle^{-1} = \langle a^{-1}\rangle$ e:

$$\langle a\rangle \cdot \langle a^{-1}\rangle = \langle a \cdot a^{-1}\rangle = \langle 1\rangle = A.$$

Portanto, $\langle a\rangle$ é invertível. □

3.2 Definição e Exemplos de Domínios de Dedekind

Definição 3.2.1. Um *domínio de Dedekind* é um Domínio Noetheriano e integralmente fechado tal que todo ideal primo diferente de zero é maximal.

Lema 3.2.2. *Todo Domínio de Ideais Principais (DIP) é um domínio de Dedekind. Assim se D é um DIP, valem:*

i. D é Noetheriano;

ii. D é integralmente fechado;

iii. Todo ideal primo não nulo de D é maximal.

Demonstração. Seja D um domínio de ideais principais (DIP).

i. Dado $\mathfrak{a}$ um ideal de D, temos $\mathfrak{a} = \langle a\rangle$ para algum $a \in \mathfrak{a}$. Logo D é Noetheriano.

ii. Iremos usar o corolário 2.2.15 que diz que todo DFU é integralmente fechado. Portanto basta mostrar que todo Domínio de Ideais Principais (DIP) é Domínio de Fatoração Única (DFU).

(a) Existência da fatoração por elementos irredutíveis:

Seja $a \neq 0$ e não irredutível, suponha por absurdo que a não possua divisor irredutível, então $a = a_1b_1$ onde a_1, b_1 são não nulos e não invertíveis, assim $\langle a\rangle \subsetneq \langle a_1\rangle$. Uma vez que

a não possui divisor irredutível, temos $a_1 = a_2 b_2$ onde a_2, b_2 são não nulos e não invertíveis, assim $\langle a_1 \rangle \subsetneq \langle a_2 \rangle$, repetindo o processo teremos a cadeia estritamente crescente:

$$\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \langle a_3 \rangle \dots$$

Absurdo, pois D é Noetheriano.

Agora suponha por absurdo que a não possa ser fatorado por primos irredutíveis. Pelo argumento anterior, $a = q_1 b_1$, com q_1 irredutível e $b_1 \neq 0$ não invertível, utilizando novamente o argumento anterior, em $b_1 = q_2 b_2$, com q_2 irredutível e $b_2 \neq 0$ não invertível, repetindo o processo teremos a cadeia:

$$\langle a \rangle \subsetneq \langle b_1 \rangle \subsetneq \langle b_2 \rangle \subsetneq \langle b_3 \rangle \dots$$

Absurdo, pois D é Noetheriano.

(b) Unicidade da fatoração (a menos de ordem e de elementos associados):

Primeiro temos que provar que se $p \in D$ é irredutível e $p \mid ab$, com $a, b \in D$ então $p \mid a$ ou $p \mid b$.

Se $p \mid a$ então nada a se provar. Suponha que $p \nmid a$. Como D é DIP $\exists d \in D$ tal que $\langle a, p \rangle = \langle d \rangle$. Daí obtemos que $p = dm$ e $a = dn$, com $m, n \in D$. Afirmamos que d é invertível. De fato, se não fosse, teríamos que p e d seriam associados, isto é, $d = up$ com $u \in D$ invertível. Daí $a = dn = upn$, ou seja, $p \mid a$, contradição.

Sendo d invertível, $\langle a, p \rangle = D$. Existem $k, l \in D$ tais que $1 = ka + lp$. Multiplicando a igualdade por b, obtemos $b = kab + lpb$.

Como $p \mid ab$, segue que p divide cada parcela do 2º membro da igualdade, logo $p \mid b$.

Suponha que um elemento $a \in D$ tenha duas fatorações:

$$a = p_1 \dots p_r = q_1 \dots q_s,$$

onde cada p_i e q_i são irredutíveis. Aplicaremos indução em r:

Se $r = 1$, teremos $a = p_1$ irredutível, assim $s = 1$ e $p_1 = q_1$.

Suponha que todo elemento que pode ser expresso como um produto de $r - 1$ elementos irredutíveis é escrito de modo único (a menos de associados e ordem).

Como $p_r | a$ e $a = q_1 \dots q_s$ então $p_r | q_1 \dots q_s$, assim $p_r | q_i$ para algum i. Suponha sem perda de generalidade que $p_r | q_s$, uma vez que q_s é irredutível, temos $q_s = u p_r$ onde u é uma unidade, temos então:

$$a = p_1 \dots p_{r-1} p_r = q_1 \dots q_{s-1} q_s$$

$$a = p_1 \dots p_{r-1} p_r = q_1 \dots q_{s-1} u p_r.$$

Por cancelamento

$$a = p_1 \dots p_{r-1} = q_1 \dots q_{s-1} u$$

Pela hipótese de indução as fatorações são idênticas a menos de ordenação e de elementos

associados. Logo, por (a) e por (b) temos que D é DFU.

Pelo Corolário 2.2.15. Todo DFU é integralmente fechado.

iii. Seja I um ideal primo de D. Como D é DIP, $I = \langle a \rangle$ para algum $a \in D$ não invertível e não nulo. Escreva a como um produto de irredutíveis $a = p_1 \dots p_k$. Observe primeiramente que todo ideal principal gerado por um elemento irredutível é maximal.

Como $\langle a \rangle$ é primo, p_1 ou $p_2 \dots p_k \in \langle a \rangle$.

Se $p_1 \in \langle a \rangle$ então $p_1 = aq$ e como p_1 é irredutível então q é uma unidade. Assim $\langle a \rangle = \langle p_1 \rangle$ que é maximal pois p_1 é irredutível.

Se $p_2 \dots p_k \in \langle a \rangle$ então como $\langle a \rangle$ é primo, p_2 ou $p_3 \dots p_k \in \langle a \rangle$

Se $p_2 \in \langle a \rangle$ então $\langle a \rangle = \langle p_2 \rangle$ que por sua vez é maximal, pelo mesmo argumento usado para p_1. Por indução teremos todos os casos possíveis, assim $I = \langle a \rangle = \langle p_i \rangle$ para algum $i = 1, \dots, k$. Logo I é maximal. □

Exemplos 3.2.3. .

i. O anel $\mathbb{Z}$ é um domínio de Dedekind pelo lema anterior, pois $\mathbb{Z}$ é DIP. De fato, se $I \subset \mathbb{Z}$ é um ideal não nulo, se n é o menor número positivo pertencente a I, segue do Algoritmo da divisão que $I = \langle n \rangle$.

ii. Se K é um corpo, então $K[x]$ é um domínio de Dedekind, pois $K[x]$ é DIP pelo Teorema 5.2.7 em [10].

Lema 3.2.4. *Sejam A um domínio de integridade e B uma A-álgebra finitamente gerada e inteira sobre A. Se $\mathfrak{b}$ é um ideal primo diferente zero de B, então $\mathfrak{b} \cap A$ é um ideal diferente de zero de A.*

Demonstração. Sejam $\mathfrak{b}$ um ideal primo de B e $\beta \in \mathfrak{b}$ com $\beta \neq 0$. Como B é inteiro sobre A, existe $g \in A[x]$ mônico tal que $g(\beta) = 0$. Seja:

$$g(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$

$a_i \in A$ para todo $i = 1, \dots, n$. Seja $k = \text{mín}\{i = 0, \dots, n-1 \mid a_i \neq 0\}$. Escrevemos $g = x^k f$. Então:

$$f(x) = a_k + a_{k+1} x + a_{k+2} x^2 + \cdots + a_{n-1} x^{n-1-k} + x^{n-k}$$

Com isso temos $f \in A[x]$, $f(0) = a_k \neq 0$ e $f(\beta) = 0$, pois $A[x]$ é domínio, uma vez que A é domínio. Como $\beta \in \mathfrak{b}$ e $f(0) = a_k$

$$-a_k = -f(0) = f(\beta) - f(0) = a_{k+1}\beta + a_{k+2}\beta^2 + \cdots + a_{n-1}\beta^{n-1-k} + \beta^{n-k} \in \mathfrak{b}$$

Logo $\mathfrak{b} \cap A$ contém um elemento não nulo. □

Proposição 3.2.5. *Seja A um domínio de integridade tal que todo ideal primo não nulo é maximal, e seja B uma A-álgebra finitamente gerada e inteira sobre A. Então todo ideal primo não nulo em B é maximal.*

Demonstração. Dizer que B é uma A-álgebra finitamente gerada, significa que B é um domínio e que existem $\beta_1, \ldots, \beta_k \in B$ tais que $B = A[\beta_1, \ldots, \beta_k]$. Se $\mathfrak{b}$ é um ideal primo em B, pelo Lema 3.2.4 $\mathfrak{p} = \mathfrak{b} \cap A$ é um ideal não nulo em A. Como $\mathfrak{b}$ é primo, $\mathfrak{p} = \mathfrak{b} \cap A$ é ideal primo de A. Pela hipótese, $\mathfrak{p}$ é maximal. Com isso $F = A/\mathfrak{p}$ é um corpo.

O núcleo do homomorfismo $h : A \to B/\mathfrak{b}$, $h(a) = \overline{a}$ é $\mathfrak{p} = \mathfrak{b} \cap A$. O teorema dos homomorfismos nos permite identificar $F = A/\mathfrak{p}$ como um subcorpo de $B/\mathfrak{b}$. Via essa identificação consideramos $F \subset B/\mathfrak{b}$.

Como B é inteiro sobre A, para cada i, tome $f_i \in A[x]$ o polinômio mônico tal que β_i é uma raiz de f_i. Seja $\overline{f_i} \in F[x]$ a imagem de f_i sob a aplicação canônica $A[x] \to F[x]$ e seja $\overline{\beta_i}$ a imagem de β_i em $B/\mathfrak{b}$. Então $\overline{f_i}(\overline{\beta_i})$ é a imagem de $f_i(\beta_i) = 0$ em $B/\mathfrak{b}$ que também é 0. Em outras palavras $\overline{\beta_i}$ é algébrico sobre F $\forall i = 1, \ldots, n$. Segue que a F-álgebra $F[\overline{\beta_1}, \ldots, \overline{\beta_n}]$ é um corpo (vide propriedade informada no final da definição 1.3.14). Daí:

$$\frac{B}{\mathfrak{b}} = \frac{A[\beta_1, \ldots, \beta_n]}{\mathfrak{b}} = \frac{A}{A \cap \mathfrak{b}}[\overline{\beta_1}, \ldots, \overline{\beta_n}] = \frac{A}{\mathfrak{p}}[\overline{\beta_1}, \ldots, \overline{\beta_n}] = F[\overline{\beta_1}, \ldots, \overline{\beta_n}].$$

Logo $B/\mathfrak{b}$ é um corpo e portanto, $\mathfrak{b}$ é maximal. □

Proposição 3.2.6. *Seja A um domínio de Dedekind, e seja B o fecho inteiro de A em uma extensão finita e separável do corpo de frações de A. Então B é um domínio de Dedekind.*

Demonstração. Pelo Corolário 1.4.22 em [7] temos que B é um A-módulo finitamente gerado. Se $\mathfrak{b}$ é um ideal de B, então $\mathfrak{b}$ é um A-submódulo de B. Como A é Noetheriano, $\mathfrak{b}$ é finitamente gerado pela Proposição 2.1.3. Assim B é Noetheriano. Pela Proposição 2.2.16, B é integralmente fechado. Por fim, pela Proposição 3.2.5 todo ideal diferente de zero de A é maximal. □

Corolário 3.2.7. *O anel dos inteiros de qualquer corpo numérico é um domínio de Dedekind.*

Demonstração. Imediata da Proposição 3.2.6, fazendo $A = \mathbb{Z}$. □

3.3 Fatoração e Divisibilidade de Ideais

Lema 3.3.1. *Seja A um domínio Noetheriano, e seja $\mathfrak{a}$ um ideal de A diferente de zero.*

(*a*) *Existem $k \geq 1$ e ideais primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ de A tais que o produto $\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq \mathfrak{a}$.*

(*b*) *Suponha que todo ideal primo diferente de zero de A é maximal. Se $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ são como no item (a) e $\mathfrak{p}$ é um ideal primo de A contendo $\mathfrak{a}$, então $\mathfrak{p} = \mathfrak{p}_i$ para algum i positivo, $i \leq k$.*

Demonstração. (a) Suponha por absurdo que a afirmação é falsa. Considere o conjunto $\mathcal{S}$ de ideais diferentes de zero de A que não contenham produtos de um número finito de ideais primos de A. Temos que $\mathfrak{a} \in \mathcal{S}$, logo $\mathcal{S} \neq \emptyset$. Como A é Noetheriano, $\mathcal{S}$ tem um elemento maximal $\mathfrak{b}$. Como $\mathfrak{b} \in \mathcal{S}$, $\mathfrak{b}$ não é primo. Sejam $a, b \in A - \mathfrak{b}$ com $ab \in \mathfrak{b}$. Então $\mathfrak{b} + \langle a \rangle$ e $\mathfrak{b} + \langle b \rangle$ contém propriamente o ideal $\mathfrak{b}$. Assim, pela maximalidade de $\mathfrak{b}$, existem ideais primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ e $\mathfrak{q}_1, \ldots, \mathfrak{q}_l$ de A para algum $k, l \geq 0$ tal que $\mathfrak{p}_1 \ldots \mathfrak{p}_k \subseteq \mathfrak{b} + \langle a \rangle$ e $\mathfrak{q}_q \ldots \mathfrak{q}_l \subseteq \mathfrak{b} + \langle b \rangle$. Assim, temos

$$\mathfrak{p}_1 \ldots \mathfrak{p}_k \mathfrak{q}_1 \ldots \mathfrak{q}_l \subseteq (\mathfrak{b} + \langle a \rangle)(\mathfrak{b} + \langle b \rangle) \subseteq \mathfrak{b},$$

o que contradiz o fato de $\mathfrak{b} \in \mathcal{S}$.

b. Suponha que $\mathfrak{a}$ é próprio, e seja $\mathfrak{p}$ um ideal primo contendo $\mathfrak{a}$. Por hipótese todo ideal primo diferente de zero de A é maximal. Suponha por contradição que $\mathfrak{p}_i \neq \mathfrak{p}$ para todo $i = 1, \ldots k$. Sendo $\mathfrak{p}_i$ maximal, segue que $\mathfrak{p}_i \nsubseteq \mathfrak{p}$, logo existe $b_i \in \mathfrak{p}_i - \mathfrak{p}$ para cada $1 \leq i \leq k$. Teremos $b_1 \ldots b_k \notin \mathfrak{p}$ pois $\mathfrak{p}$ é primo, assim $b_1 \ldots b_k \notin \mathfrak{a}$, o que contradiz o fato de $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \subset \mathfrak{a}$. Logo $\mathfrak{p}_i = \mathfrak{p}$ para algum $i = 1, \ldots, k$. □

Lema 3.3.2. *Sejam A um domínio de Dedekind e $\mathfrak{p}$ um ideal primo diferente de zero de A. Então $\mathfrak{p}\mathfrak{p}^{-1} = A$. Em outras palavras, todo ideal primo não nulo em um domínio de Dedekind é invertível.*

Demonstração. Lembramos que $\mathfrak{p}^{-1} = \{b \in K \mid b \cdot \mathfrak{p} \subset A\}$, onde K é o corpo de frações de A. Como $\mathfrak{p} \subset A$, $1 \in \mathfrak{p}^{-1}$ e portanto, $\mathfrak{p} \subset \mathfrak{p} \cdot \mathfrak{p}^{-1} \subset A$. Como A é domínio de Dedekind, $\mathfrak{p}$ é ideal maximal de A. Segue que $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}$ ou $\mathfrak{p} \cdot \mathfrak{p}^{-1} = A$. Suponha por absurdo que $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}$.

Seja $a \in \mathfrak{p}$ diferente de zero. Pelo Lema 3.3.1a, tomaremos $k \geq 1$ o menor inteiro tal que existem ideais primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ de A com $\mathfrak{p}_1 \ldots \mathfrak{p}_k \subseteq \langle a \rangle$. Pelo Lema 3.3.1b, podemos supor sem perda de generalidade que $\mathfrak{p}_k = \mathfrak{p}$. Pela minimalidade de k, $\mathfrak{p}_1 \ldots \mathfrak{p}_{k-1} \nsubseteq \langle a \rangle$.

Seja $b \in \mathfrak{p}_1 \ldots \mathfrak{p}_{k-1}$ sendo tal que $b \notin \langle a \rangle$. Afirmamos que $a^{-1}b \notin A$. De fato, caso contrário, teríamos $b = a(a^{-1}b) \in \langle a \rangle$, pois $\langle a \rangle$ é ideal de A. Assim:

$$a^{-1}b\mathfrak{p} = a^{-1}b\mathfrak{p}_k \subseteq a^{-1}\mathfrak{p}_1 \ldots \mathfrak{p}_k \subseteq a^{-1}\langle a \rangle \subseteq A,$$

o que implica que $a^{-1}b \in \mathfrak{p}^{-1}$. Combinando esta informação com a igualdade $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$, segue que $a^{-1}b\mathfrak{p} \subseteq \mathfrak{p}$. Uma vez que $\mathfrak{p}$ é finitamente gerado (pois A é Noetheriano), pela Proposição 2.2.4 temos que $a^{-1}b$ é inteiro sobre A. Mas A é integralmente fechado e $a^{-1}b \notin A$, o que é uma contradição. Portanto, $\mathfrak{p}^{-1}\mathfrak{p} = A$. □

Lema 3.3.3. *Sejam A um domínio de Dedekid e $\mathfrak{p}, \mathfrak{q} \subset A$ ideais primos. Então $(\mathfrak{p}\mathfrak{q})^{-1} = \mathfrak{p}^{-1}\mathfrak{q}^{-1}$.*

Demonstração. Da definição de inverso de ideal fracionário, temos que $(\mathfrak{p}\mathfrak{q})(\mathfrak{p}\mathfrak{q})^{-1} \subset A$. Pelo Lema 3.3.2, $\mathfrak{p}^{-1}\mathfrak{p} = A$ e $\mathfrak{q}^{-1}\mathfrak{q} = A$. Daí:

$$(\mathfrak{p}\mathfrak{q})(\mathfrak{p}\mathfrak{q})^{-1} \subset A \Rightarrow \mathfrak{p}^{-1}(\mathfrak{p}\mathfrak{q})(\mathfrak{p}\mathfrak{q})^{-1} \subset \mathfrak{p}^{-1}A \Rightarrow \mathfrak{q}(\mathfrak{p}\mathfrak{q})^{-1} \subset \mathfrak{p}^{-1},$$

onde $\mathfrak{p}^{-1}A = \mathfrak{p}^{-1}$ pois $\mathfrak{p}^{-1}$ é um A-módulo. Multiplicando a inclusão agora por $\mathfrak{q}^{-1}$ e usando a comutatividade do produto, obtemos que $(\mathfrak{pq})^{-1} \subset \mathfrak{p}^{-1}\mathfrak{q}^{-1}$.

Recíprocamente, seja $\sum_{i=1}^{m} a_i \cdot b_i$, onde $m \in \mathbb{N}$, $a_i \in \mathfrak{p}^{-1}$ e $b_i \in \mathfrak{q}^{-1}$ $\forall i = 1, \ldots, m$. Um elemento arbitrário de $\mathfrak{pq}$ é da forma $\sum_{j=1}^{n} c_j \cdot d_j$, com $c_j \in \mathfrak{p}$ e $d_j \in \mathfrak{q}$, $\forall j = 1, \ldots, n$. Daí:

$$\left(\sum_{i=1}^{m} a_i b_i\right)\left(\sum_{j=1}^{n} c_j d_j\right) = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} (a_i c_j)(b_i d_j)\right) \in A,$$

pois $a_i c_j \in A$ e $b_i d_j \in A$. Logo, $(\mathfrak{pq})^{-1} \supset \mathfrak{p}^{-1}\mathfrak{q}^{-1}$.

□

Teorema 3.3.4. *Sejam A um domínio de Dedekind e $\mathfrak{a}$ um ideal fracionário de A. Então existem $k \geq 0$, ideais primos distintos diferentes de zero $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, únicos a menos de ordenação, e $r_i \in \mathbb{Z}$ únicos e diferentes de zero, $\forall i = 1, \ldots, k$, tal que $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$. Além disso, $\mathfrak{a}$ é um ideal de A se e somente se cada r_i é positivo.*

Demonstração. Existência da fatoração

1º caso: Suponha que $\mathfrak{a}$ é um ideal próprio diferente de zero de A. Pelo Lema 3.3.1a existem $m > 0$ e ideais primos diferentes de zero $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ de A (não necessariamente distintos) tais que $\mathfrak{p}_1 \ldots \mathfrak{p}_m \subseteq \mathfrak{a}$.

Se $m = 1$, então $\mathfrak{p}_1 \subseteq \mathfrak{a}$. Como $\mathfrak{a}$ é próprio e $\mathfrak{p}_1$ é maximal, pois é primo e A é domínio de Dedekind, temos que $\mathfrak{a} = \mathfrak{p}_1$.

Suponha por indução que $\mathfrak{p}_1 \ldots \mathfrak{p}_{m-1} = \mathfrak{b}$ para todo ideal $\mathfrak{b}$ de A tal que $\mathfrak{p}_1 \ldots \mathfrak{p}_{m-1} \subseteq \mathfrak{b}$.

Para $\mathfrak{p}_1 \ldots \mathfrak{p}_m \subseteq \mathfrak{a}$, Pela Observação 2.1.2 existe um ideal maximal $\mathfrak{p}$ que contém $\mathfrak{a}$, pois $\mathfrak{a}$ é ideal próprio. Pelo Corolário 1.2.13, $\mathfrak{p}$ é primo. Pelo Lema 3.3.1b, $\mathfrak{p} = \mathfrak{p}_i$ para algum $i \leq m$. Sem perda de generalidade tomamos $i = m$. Então

$$\mathfrak{p}_1 \ldots \mathfrak{p}_{m-1} \subseteq \mathfrak{p}_1 \ldots \mathfrak{p}_{m-1}\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{p}_1 \ldots \mathfrak{p}_m\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq A,$$

onde a última inclusão segue do fato de $\mathfrak{a} \subset \mathfrak{p}$. Logo $\mathfrak{a}\mathfrak{p}^{-1}$ é ideal de A.

Pela hipótese da indução, existem ideais primos $\mathfrak{p}'_1 \ldots \mathfrak{p}'_{m-1}$ de A tais que $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}'_1 \ldots \mathfrak{p}'_{m-1}$. Fazendo $\mathfrak{p}'_m = \mathfrak{p}$, a fatoração de $\mathfrak{a}$ em ideais primos desejada é obtida multiplicando ambos os lados por $\mathfrak{p}$ e usando o Lema 3.3.2:

$$\mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}'_1 \ldots \mathfrak{p}'_{m-1}\mathfrak{p} \Rightarrow \mathfrak{a} = \mathfrak{p}'_1 \ldots \mathfrak{p}'_m.$$

2º caso (Geral): Seja $\mathfrak{a}$ um ideal fracionário de A. Existe $d \in A$ tal que $d\mathfrak{a} \subseteq A$. Pelo 1º caso, $d\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_m$ para algum $m \geq 1$ e $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ ideais primos. Então escrevemos $\langle d \rangle = \mathfrak{l}_1 \ldots \mathfrak{l}_n$ para algum $n \geq 1$ e $\mathfrak{l}_1, \ldots, \mathfrak{l}_n$ ideais primos de. Pelo Lema 3.3.2 e pelo Lema 3.3.3:

$$\mathfrak{a} = \langle d \rangle^{-1} d\mathfrak{a} = \mathfrak{l}_1^{-1} \ldots \mathfrak{l}_n^{-1}\mathfrak{p}_1 \ldots \mathfrak{p}_m.$$

Se $\mathfrak{p}_i = \mathfrak{l}_j$ para algum i e j, então basta usar em Lema 3.3.2 para removê-los do produto. Assim teremos a fatoração desejada.
Unicidade da Fatoração:

Agora suponha que existam duas fatorações para o ideal fracionário $\mathfrak{a}$:

$$\mathfrak{p}_1^{r_1} \dots \mathfrak{p}_k^{r_k} = \mathfrak{q}_1^{s_1} \dots \mathfrak{q}_l^{s_l},$$

para certos $k, l \geq 0$, para $\mathfrak{p}_1, \dots, \mathfrak{p}_k, \mathfrak{q}_1, \dots, \mathfrak{p}_l$ ideais primos distintos, $r_1, \dots r_k, s_1, \dots, s_l$ inteiros diferentes de zero. Se $r_i < 0$(resp. $s_i < 0$) para algum i, multiplicamos ambos os lados por $\mathfrak{p}_i^{-r_i}$ (resp. $\mathfrak{q}_i^{-s_i}$) e obtemos uma igualdade de dois produtos que envolvem apenas ideais com potências positivas.

Assim assumimos sem perda de generalidade que todo r_i e s_i é positivo. Podemos supor que $t = \sum_{i=1}^{k} r_i$ é mínimo dentre todas as fatorações de $\mathfrak{a}$. Faremos indução em t. Se $t = 0$, então $k = 0$ e portanto, $\mathfrak{a} = A$. Então l deve ser zero, pois do contrário, algum s_j seria positivo e daí $\mathfrak{q}_1^{s_1} \dots \mathfrak{q}_l^{s_l}$ seria próprio, uma contradição. Suponha que a fatoração seja única a menos de ordenação para $t - 1$.

Se $t > 0$, então $\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$ é não próprio e como $\mathfrak{p}_k$ é ideal, $\mathfrak{a} \subset \mathfrak{p}_k$. Pelo Lema 3.3.1b temos $\mathfrak{p}_k = q_i$ para algum $1 \leq i \leq l$. Multiplicando os dois lados por $\mathfrak{p}_k^{-1}$ a quantidade t decresce por 1. Pela hipótese da indução, temos que os termos restantes são iguais a menos de ordenação, assim temos o resultado. □

Definição 3.3.5. Dizemos que um ideal $\mathfrak{b}$ de um anel comutativo com unidade A *divide* um ideal $\mathfrak{a}$ de A se existe um ideal $\mathfrak{c}$ de A tal que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Escrevemos $\mathfrak{b} \mid \mathfrak{a}$ para denotar que $\mathfrak{b}$ divide $\mathfrak{a}$.

Definição 3.3.6. Dados um ideal $\mathfrak{a}$ de um anel comutativo com unidade A e um elemento x em A, dizemos que $\mathfrak{a}$ divide x quando $\mathfrak{a}$ divide o ideal principal $\langle x \rangle$.

Corolário 3.3.7. *Sejam $\mathfrak{a}$ e $\mathfrak{b}$ ideais diferentes de zero em um domínio de Dedekind A.*

(i) *Os ideais $\mathfrak{a}$ e $\mathfrak{b}$ não são divisíveis por um mesmo ideal primo se, e somente se, $\mathfrak{a} + \mathfrak{b} = A$.*

(ii) *Suponha que $\mathfrak{a} \subseteq \mathfrak{b}$. Então $\mathfrak{b} \mid \mathfrak{a}$.*

Demonstração. $(i)(\Leftarrow)$ Se $\mathfrak{p} \mid \mathfrak{a}$ e $\mathfrak{p} \mid \mathfrak{b}$ para algum ideal primo $\mathfrak{p}$, então

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{p}\mathfrak{c} + \mathfrak{p}\mathfrak{d} = \mathfrak{p}(\mathfrak{c} + \mathfrak{d}) \subseteq \mathfrak{p},$$

Assim $\mathfrak{a} + \mathfrak{b} \neq A$ e como $\mathfrak{p}$ é primo, $\mathfrak{p} \neq A$.

$(\Rightarrow)$ Suponha que não exista um ideal primo que divida $\mathfrak{a}$ e $\mathfrak{b}$ simultaneamente. Se $\mathfrak{a}$ e $\mathfrak{b}$ estivessem contidos em um mesmo ideal maximal $\mathfrak{p}$, este ideal seria um dos ideais primos dos fatorares de $\mathfrak{a}$ e $\mathfrak{b}$, logo $\mathfrak{p}$ dividiria ambos, contradizendo a hipótese . Assim $\mathfrak{a} + \mathfrak{b}$ não pode estar contido em nenhum ideal maximal, logo $\mathfrak{a} + \mathfrak{b} = A$.

(ii) Pelo Teorema 3.3.4, escrevemos $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_k$ e $\mathfrak{b} = \mathfrak{q}_1 \dots \mathfrak{q}_l$ para ideais primos não nulos $\mathfrak{p}_i$ e $\mathfrak{q}_i$ de A. Suponha sem perda de generalidade que $\mathfrak{p}_i = \mathfrak{q}_i$ para todo $1 \leq i \leq t$ para algum $t \leq min(k,l)$ e que $\mathfrak{p}_i$ (resp. $\mathfrak{q}_i$) não ocorra na fatoração de $\mathfrak{b}$ (resp. $\mathfrak{a}$) para $i > t$. Então:

$$\mathfrak{q}_1 \dots \mathfrak{q}_l = \mathfrak{b} \overset{\mathfrak{a}\subset\mathfrak{b}}{=} \mathfrak{a} + \mathfrak{b} = \mathfrak{p}_1 \dots \mathfrak{p}_t \dots \mathfrak{p}_k + \mathfrak{q}_1 \dots \mathfrak{q}_t \dots \mathfrak{q}_l = \mathfrak{q}_1 \dots \mathfrak{q}_t \dots \mathfrak{p}_k + \mathfrak{q}_1 \dots \mathfrak{q}_t \dots \mathfrak{q}_l =$$

$$= \mathfrak{q}_1 \dots \mathfrak{q}_t (\mathfrak{p}_{t+1} \dots \mathfrak{p}_k + \mathfrak{q}_{t+1} \dots \mathfrak{q}_l) = \mathfrak{q}_1 \dots \mathfrak{q}_t A = \mathfrak{q}_1 \dots \mathfrak{q}_t,$$

onde a penúltima igualdade segue do item (i) e do fato de $\mathfrak{p}_{t+1}, \dots, \mathfrak{p}_k, \mathfrak{q}_{t+1}, \dots \mathfrak{q}_l$ serem distintos dois a dois. Assim $t = l$, logo $\mathfrak{b} \mid \mathfrak{a}$. □

Definição 3.3.8. Seja A um domínio de Dedekind, e sejam $\mathfrak{a}$ e $\mathfrak{b}$ ideais de A. O *máximo divisor comum* de $\mathfrak{a}$ e $\mathfrak{b}$ é $\mathfrak{a} + \mathfrak{b}$.

Observação 3.3.9. Pelo Corolário 3.3.7, $\mathfrak{a} + \mathfrak{b}$ contém e divide ambos $\mathfrak{a}$ e $\mathfrak{b}$ e é o menor ideal que faz isso.(Na definição 3.3.8, o uso da palavra "máximo"ao invés de "mínimo"é usada para fazer uma analogia à noção de MDC dos números inteiros).

3.4 O Grupo das Classes de um Domínio de Dedekind

Definição 3.4.1. Seja A um domínio de Dedekind. O conjunto $I(A)$ de ideais fracionários de A é chamado de *grupo ideal* de A.

Temos o seguinte resultado direto do Teorema 3.3.4:

Corolário 3.4.2. *O grupo ideal $I(A)$ de um domínio de Dedekind A é um grupo abeliano para a operação multiplicação de ideais fracionários. O elemento neutro é o anel A e o inverso de $\mathfrak{a} \in I(A)$ é $\mathfrak{a}^{-1}$. Em particular, em um domínio de Dedekind, todo ideal fracionário é invertível.*

Definição 3.4.3. Seja A um domínio de Dedekind. Vamos denotar por $P(A)$ o conjunto de seus ideais fracionários principais. Vamos nos referir a ele como *grupo de ideais principais* de A.

O corolário a seguir é imediato do Teorema 3.3.4 e do Lema 3.1.13:

Corolário 3.4.4. *Seja A um domínio de Dedekind. O grupo $P(A)$ é um subgrupo de $I(A)$.*

Definição 3.4.5. O *grupo das classes $Cl(A)$*, de um domínio de Dedekind A é dado por $I(A)/P(A)$, ou seja, o quociente do grupo ideal de A pelo grupo de ideais principais de A.

Como $I(A)$ é abeliano, $P(A)$ é subgrupo normal de $I(A)$, logo o quociente é de fato um grupo.

Lema 3.4.6. *Um domínio de Dedekind A é um DIP se e somente se $Cl(A) = A$.*

Demonstração. Todo ideal de $I(A)$, pelo Teorema 3.3.4 é da forma $\mathfrak{a}\mathfrak{b}^{-1}$, onde $\mathfrak{a}$ e $\mathfrak{b}$ são ideais não nulos de A. Se A é um DIP, então $\mathfrak{a}$ e $\mathfrak{b}$ são principais, isto é, $\mathfrak{a} = \langle a \rangle$ e $\mathfrak{b} = \langle b \rangle$ para $a \in \mathfrak{a}$ e $b \in \mathfrak{b}$. Assim $\mathfrak{a}\mathfrak{b}^{-1} = \langle a \rangle \langle b^{-1} \rangle = \langle ab^{-1} \rangle$ também é principal, logo $I(A) = P(A)$ e portanto $Cl(A) = \{A\}$ é trivial.

Por outro lado, se $Cl(A)$ é trivial, temos $I(A)/P(A) = \{A\}$ então $I(A) = P(A)$. Assim se $\mathfrak{a}$ é um ideal de A, em particular $\mathfrak{a} \in I(A)$, assim $\mathfrak{a} = \langle a \rangle$ para algum $a \in \mathfrak{a} \subset A$, logo $\mathfrak{a}$ é principal. Portanto A é um DIP. □

Observação 3.4.7. Pode-se provar que se $K = \mathbb{Q}(\sqrt{-5})$, então Cl_K é não trivial com $| Cl_K | = 2$ (vide [7], Exemplo 4.3.10). Isto reflete o fato de que o grupo das classes de um corpo numérico é sempre finito. A demonstração deste fato envolve conceitos avançados de Teoria dos números Algébricos e foge ao escopo desse trabalho. Vide [7], Teorema 4.3.8, para uma prova desse fato.

Notação 3.4.8. Seja K um corpo numérico. Vamos denotar I_K, P_K, e Cl_K o grupo ideal, grupo de ideais principais, e a grupo das classes de O_K respectivamente. Também nos referimos a estes como o *grupo ideal de K*, o *grupo de ideais principais de K*, e o *grupo das classes de K*, respectivamente.

Teorema 3.4.9. *Um domínio de Dedekind é um Domínio de Fatoração Única se, e somente se, é um Domínio de Ideais Principais.*

Demonstração. Segue da prova do Lema 3.2.2 que todo DIP é um DFU. Precisamos mostrar apenas que um domínio de Dedekind que é um domínio de fatoração única é um domínio de ideais principais. Seja A um domínio de Dedekind. Pelo Teorema 3.3.4, é suficiente mostrar que cada ideal primo não nulo $\mathfrak{p}$ de A é principal.

Sendo $\mathfrak{p}$ primo e A um domínio de fatoração única, qualquer elemento não nulo de $\mathfrak{p}$ é divisível por um elemento irredutível $\pi \in \mathfrak{p}$. Temos que $\langle \pi \rangle \subset \mathfrak{p}$. Dados $a, b \in A$ com $a \cdot b \in \langle \pi \rangle$ então $a \cdot b = \pi \cdot c$, $c \in A$. Como A é DFU o fator irredutível π apararece na fatoração de a ou de b, isto é, $a \in \langle \pi \rangle$ ou $b \in \langle \pi \rangle$. Segue que $\langle \pi \rangle$ é ideal primo. Como A é domínio de Dedekind, $\langle \pi \rangle$ e $\mathfrak{p}$ são maximais, portanto, $\mathfrak{p} = \langle \pi \rangle$. □

O fecho inteiro B de um domínio de Dedekind A em uma extensão finita e seperável L de seu corpo de frações K também é um domínio de Dedekind (Corolário 3.2.6). Se $\mathfrak{p}$ é um ideal primo não nulo de A, então podemos considerar o ideal $\mathfrak{p}B$ de B. Este ideal pode não ser primo, mas ele admite uma fatoração

$$\mathfrak{p}B = \mathfrak{b}_1^{e_1} \dots \mathfrak{b}_g^{e_g} \tag{3.4.1}$$

para ideais primos distintos $\mathfrak{b}_i$ de B e inteiros positivos e_i, para $i = 1, \dots, g$ para algum $g \geq 1$. Assim faremos as seguintes definições:

Definição 3.4.10. Seja B/A uma extensão de anéis comutativos. Dizemos que um ideal primo $\mathfrak{b}$ de B *está sobre* (ou *acima de*) um ideal primo $\mathfrak{p}$ de A se $\mathfrak{p} = \mathfrak{b} \cap A$. Dizemostambém que $\mathfrak{p}$ *está sob* (ou *abaixo de*) $\mathfrak{b}$.

Em (3.4.1), os ideais primos de B sobre $\mathfrak{p}$ são exatamente os $\mathfrak{b}_i$ para $i = 1, \ldots, g$.

Definição 3.4.11. Seja A um domínio de Dedekind, e seja B o fecho inteiro de A em uma extensão finita e separável L do corpo de frações K de A. Seja $\mathfrak{p}$ um ideal primo de A.

Dizemos que $\mathfrak{p}$ é *totalmente ramificado* em L/K se $\mathfrak{p}B = \mathfrak{b}^m$ com $\mathfrak{b}$ ideal primo e $m > 1$.

Finalizamos esta seção com o resultado abaixo, que é imediato de [7], Teorema 2.5.11. Omitiremos sua demonstração.

Proposição 3.4.12. *Sejam A um domínio de Dedekind e B o fecho inteiro de A numa extensão L/K finita e separável do corpo de frações K de A. Seja $\mathfrak{p}$ um ideal não nulo de A. Considere a fatoração $\mathfrak{p}B = \mathfrak{b}_1^{e_1} \ldots \mathfrak{b}_g^{e_g}$ do ideal $\mathfrak{p}B$, onde os $\mathfrak{b}_i$ são ideais primos de B. Então*

$$\sum_{i=1}^{g} e_i \leq [L : K].$$

Capítulo 4

O Último Teorema de Fermat para Primos Regulares

4.1 Corpos Ciclotômicos

Definição 4.1.1. Sejam n um inteiro positivo e K um corpo. Dizemos que $\alpha \in K$ é uma *raiz n-ésima da unidade* se $\alpha^n = 1$. Quando $\alpha^n = 1$ e $\alpha^k \neq 1$, $\forall k = 1, ..., n-1$, dizemos que α é uma *raiz n-ésima primitiva da unidade*.

Exemplos 4.1.2.

1. As raízes n-ésimas da unidade em $\mathbb{Q}$ ou $\mathbb{R}$ são ± 1 se n é par e 1 se n é ímpar.
2. Em $\mathbb{C}$, as raízes n-ésimas da unidade são da forma $e^{\frac{2k\pi i}{n}} = cos(\frac{2k\pi}{n}) + isen(\frac{2k\pi}{n})$ para $k = 1, ..., n$. Elas são as raízes do polinômio $x^n - 1 \in \mathbb{C}[x]$. Consequentemente, todas as raízes desse polinômio são distintas.

Denotaremos ζ_n^k, a raiz n-ésima da unidade $e^{\frac{2k\pi i}{n}} \in \mathbb{C}$.

Proposição 4.1.3.

(i) *As raízes n-ésimas primitivas da unidade em* $\mathbb{C}$ *são da forma* ζ_n^k *tal que* $mdc(n,k) = 1$.

(ii) *Em* $\mathbb{C}$*, fixada uma raiz n-ésima primitiva da unidade* ζ*, qualquer outra raiz n-ésima da unidade é uma potência como potência de* ζ.

Demonstração.

(i) Seja ζ_n^k tal que $mdc(n,k) = 1$, suponha que ζ_n^k não seja uma raiz n-ésima primitiva da unidade. Então existe a com $1 \leq a \leq n-1$ tal que $(\zeta_n^k)^a = 1$, assim:

$$1 = (\zeta_n^k)^a = (e^{\frac{2k\pi i}{n}})^a = e^{\frac{2ka\pi i}{n}},$$

o que implica $\frac{2ka\pi}{n} = 2\pi q$ para algum $q \in \mathbb{N}$. Assim $\frac{ka}{n} \in \mathbb{N}$ e consequentemente $n \mid ka$. Como $mdc(k,n) = 1$ temos que $n \mid a$, um absurdo, pois $1 \leq a < n$. Logo ζ_n^k é uma raiz n-ésima primitiva da unidade.

(ii) Seja ζ_n^k uma raiz n-ésima primitiva da unidade, e seja ζ_n^a uma raiz n-ésima da unidade. Pelo item (i), $mdc(k,n) = 1$. Pelo Algoritmo de Euclides Estendido existem $x, y \in \mathbb{Z}$ tais que $xk + yn = 1$. Assim $xka + yna = a$, então como $\zeta_n^{yna} = (\zeta_n^n)^{ya} = 1$, temos:

$$\zeta_n^a = \zeta_n^{xka+yna} = \zeta_n^{xka} \cdot \zeta_n^{yna} = \zeta_n^{xka} = (\zeta_n^k)^{xa}.$$

□

Definição 4.1.4. Seja n um inteiro positivo e K um corpo. Note que se ζ e ζ' são raízes n-ésimas da unidade em K, $\zeta \cdot \zeta'$ e ζ^{-1} também são raízes n-ésimas da unidade. Vamos denotar por $\mu_n(K)$ o grupo das raízes n-ésimas da unidade em K, com a operação multiplicação. Em particular, $\mu_n(\mathbb{C})$ tem n elementos e os geradores desse grupo são precisamente as raízes n-ésimas primitivas da unidade.

Exemplo 4.1.5. Para todo $n \in \mathbb{N}$, $\mu_{2n}(\mathbb{R}) = \{-1, 1\}$ e $\mu_{2n-1}(\mathbb{R}) = \{1\}$.

Definição 4.1.6. Vamos denotar por μ_n o grupo das raízes n-ésimas da unidade em um fecho algébrico de K, fixado antecipadamente. Pode se provar que este grupo sempre tem ordem n, se $car(K) = 0$ ou se $car(K) = p$ primo e p não divide n (vide [5], Proposição 8.1, p.125).

Exemplo 4.1.7. Se $K = \mathbb{R}$, teremos $\overline{\mathbb{R}} = \mathbb{C}$ e $\mu_4 = \{-1, 1, i, -i\}$.

Notação 4.1.8. Seja K um corpo e L uma extensão de K. Se S é um conjunto de elementos de L, então o corpo $K(S)$ é o menor subcorpo de L contendo a união de K e de todos os elementos de S. Se $car(K)$ não divide n então $K(\mu_n)$ será o corpo gerado sobre K pela adjunção de todas as raízes n-ésimas da unidade em um fecho algébrico de K.

Observação 4.1.9. O corpo $\mathbb{Q}(\mu_n)$ é Galoisiano sobre $\mathbb{Q}$, pois $\mathbb{Q}(\mu_n) \subset \mathbb{C}$ e $\mathbb{Q}(\mu_n)$ é o corpo de decomposição de $x^n - 1$. Todas as raízes n-ésimas da unidade são potências de qualquer raiz n-ésima primitiva da unidade ζ_n. Assim $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$.

Definição 4.1.10. O corpo $\mathbb{Q}(\zeta_n)$ é chamado de *n-ésimo corpo ciclotômico.*

Definição 4.1.11. O n-ésimo polinômio ciclotômico $\Phi_n(x) \in \mathbb{C}[x]$ é o polinômio mônico de grau mínimo cujas raízes são precisamente as raízes n-ésimas primitivas da unidade. Assim:

$$\Phi_n(x) = \prod_{\substack{1 \leq k < n \\ mdc(k,n)=1}} (x - \zeta_n^k).$$

Proposição 4.1.12. *Os itens a seguir se verificam:*

(a) Se $r,s \in \mathbb{N}$ são distintos então $\Phi_r(x)$ e $\Phi_s(x)$ não tem fatores irredutíveis em comum;

(b) $x^n - 1 = \prod_{d|n} \Phi_d(x)$*;*

(c) $\Phi_n(x)$ é mônico de coeficientes inteiros e tem grau $\varphi(n)$, onde φ é a função Phi de Euler[1]

Demonstração. (a) Sejam r e s naturais distintos. Suponha sem perda de generalidade que $r < s$. Se houvesse um fator irredutível em comum na fatoração de $\Phi_r(x)$ e $\Phi_s(x)$, teríamos que pelo menos uma raiz r-ésima primitiva da unidade também seria uma raiz s-ésima primitiva da unidade, o que é uma contradição.

(b) Quando d percorre o conjunto de todos os divisores positivos de n, o número n/d percorre esse conjunto de divisores. Note que $\zeta_{n/d} = \zeta_n^d$:

$$\prod_{d|n} \Phi_d(x) = \prod_{d|n} \prod_{\substack{1\leq k\leq d \\ mdc(k,d)=1}} (x - \zeta_d^k) = \prod_{d|n} \prod_{\substack{1\leq k\leq n/d \\ mdc(k,n/d)=1}} (x - \zeta_n^{dk}),$$

onde a última igualdade é obtida trocando d por n/d. Agora iremos mostrar que para cada $t = 1,\ldots,n$ o fator $(x - \zeta_n^t)$ está neste produtório. Tomando $t \in \{1,\ldots,n\}$ e $d = mdc(t,n)$, escrevemos $t = dk$ e $n = d\frac{n}{d}$ com $k, \frac{n}{d} \in \mathbb{N}$.

Como $d \mid n$, $1 \leq k \leq n/d$ e $mdc(k,n/d) = 1$, temos que $(x - \zeta_n^t) = (x - \zeta_n^{dk})$ é fator do produtório. Como os $\Phi_d(x)$ são todos mônicos, com raízes distintas e não possuem fatores irredutíveis em comum entre si, temos:

$$\prod_{d|n} \Phi_d(x) = \prod_{t=1}^{n} (x - \zeta_n^t) = x^n - 1.$$

(c) Faremos a prova por indução sobre $n \geq 1$ para provar que $\Phi_n(x)$ é mônico de coeficientes inteiros.

Para $n = 1$, $\Phi_1(x) = x - 1$ mônico e de coeficientes inteiros. Suponha que o mesmo vale para todos os naturais menores que n. Então, pela hipótese da indução, o polinômio:

$$q(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x)$$

é mônico de coeficientes inteiros. Como $x^n - 1 = \Phi_n(x)q(x)$, pelo algoritmo da divisão para polinômios que $\Phi_n(x)$ é mônico de coeficientes inteiros. Por fim, note que, pela definição de Φ_n, seu grau é a quantidade de fatores lineares que aparecem na fatoração de $\Phi_n(x)$, que é a quantidade de inteiros k tais que $1 \leq k \leq n$ e $mdc(k,n) = 1$. Este é exatamente o valor $\varphi(n)$.

□

[1] $\varphi(x) = \#\{n \in \mathbb{N} \mid n \leq x \text{ e } \mathrm{mdc}(n,x) = 1\}$.

Exemplos 4.1.13. O item (b) da Proposição 4.1.12 permite que calculemos efetivamente os polinômios ciclotômicos de forma recursiva. De fato, se p é primo, temos que $x^p-1=\Phi_1(x)\cdot\Phi_p$. Como $\Phi_1(x)=x-1$ segue que $\Phi_p=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+...+x^2+x+1$. Como consequência, temos que $\Phi_2=x+1$, $\Phi_3=x^2+x+1$ e $\Phi_5=x^4+x^3+x^2+x+1$. Para calcular $\Phi_4(x)$, observe que $x^4-1=\Phi_1(x)\cdot\Phi_2(x)\cdot\Phi_4(x)$. Logo $\Phi_4=\frac{x^4-1}{(x-1)(x+1)}=x^2+1$;

A próxima proposição é apresentada em um primeiro curso de Teoria de Galois. Uma prova pode ser encontrada em [5], (7.14).

Proposição 4.1.14. *Para todo $n\in\mathbb{N}$, $\Phi_n(x)$ é irredutível sobre $\mathbb{Q}$. Em particular, $\Phi_n(x)$ é o polinômio minimal de ζ_n sobre $\mathbb{Q}$ e $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=$ grau $\Phi_n(x)=\varphi(n)$.*

Lema 4.1.15. *Seja $n\geq 1$ e seja $i,j\in\mathbb{Z}$ relativamente primos a n. Então:*

$$\frac{1-\zeta_n^i}{1-\zeta_n^j}\in O^{\times}_{\mathbb{Q}(\zeta_n)}.$$

Demonstração. Seja $k\in\mathbb{Z}$ com $jk\equiv 1 \bmod n$. A existência de k vem do fato de $mdc(j,n)=1$. Então:

$$jki\equiv i \bmod n \;\Rightarrow\; jki=nq+i \text{ para } q\in\mathbb{Z}.$$

Portanto:

$$\frac{1-\zeta_n^i}{1-\zeta_n^j}=\frac{1-\zeta_n^i\zeta_n^{nq}}{1-\zeta_n^j}=\frac{1-\zeta_n^{i+nq}}{1-\zeta_n^j}=\frac{1-\zeta_n^{ijk}}{1-\zeta_n^j}=1+\zeta_n^j+...+\zeta_n^{j(ik-1)}$$

Como $\zeta_n\in O_{\mathbb{Q}(\zeta_n)}$, isto é, ζ_n é um inteiro algébrico, a soma de suas potências também o é . Assim $\frac{1-\zeta_n^i}{1-\zeta_n^j}\in O_{\mathbb{Q}(\zeta_n)}$. Pelo mesmo argumento

$$\left(\frac{1-\zeta_n^i}{1-\zeta_n^j}\right)^{-1}=\frac{1-\zeta_n^j}{1-\zeta_n^i}\in O_{\mathbb{Q}(\zeta_n)}.$$

Portanto temos o resultado desejado. □

Iremos denotar $\mathbb{Z}[\zeta_n]$ o anel gerado sobre $\mathbb{Z}$ pelas raízes n-ésimas da unidade.

Proposição 4.1.16. *Se ζ_{p^r} uma raiz p^r-ésima primitiva da unidade, então o elemento $1-\zeta_{p^r}$ é um elemento primo de $O_{\mathbb{Q}(\zeta_{p^r})}$, e $\langle p\rangle=\langle 1-\zeta_{p^r}\rangle^{\varphi(p^r)}$. Em particular, o ideal $p\mathbb{Z}$ é totalmente ramificado em $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$. (vide Definição 3.4.11)*

Demonstração. Por definição, ζ_{p^r} é raiz de $\Phi_{p^r}(x)$. Como $\Phi_{p^r}(x)\in\mathbb{Z}[x]$, ζ_{p^r} é inteiro sobre $\mathbb{Z}$. Assim pela Proposição 2.2.10, o anel $\mathbb{Z}[\zeta_{p^r}]$ está contido em $O_{\mathbb{Q}(\zeta_{p^r})}$. Usando o item (b) da

Proposição 4.1.12 para $n = p^r$ e lembrando que $1 \leq d < p^r$, $d \mid p^r \Rightarrow d \mid p^{r-1}$ temos:

$$\Phi_{p^r}(x) = \frac{x^{p^r}-1}{\prod\limits_{d|p^{r-1}} \Phi_d(x)} = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = \frac{t^p-1}{t-1} = 1+t+\ldots+t^{p-1}, \text{ onde } t = x^{p^{r-1}}.$$

Assim:

$$\Phi_{p^r}(1) = p,$$

portanto, pela definição de polinômio ciclotômico:

$$p = \Phi_{p^r}(1) = \prod_{\substack{1\leq i\leq p^r-1 \\ mdc(p^r,i)=1}} (1-\zeta_{p^r}^i) = \prod_{\substack{1\leq i\leq p^r-1 \\ mdc(p^r,i)=1}} \frac{1-\zeta_{p^r}^i}{1-\zeta_{p^r}}(1-\zeta_{p^r}). \tag{4.1.1}$$

Pelo Lema 4.1.15 e sua prova, os quocientes $\frac{1-\zeta_{p^r}^i}{1-\zeta_{p^r}} \in \mathbb{Z}[\zeta_{p^r}]$ e são invertíveis neste anel para $1 \leq i \leq p^r-1$ e $\text{mdc}(p^r,i) = 1$. Existem $\varphi(p^r)$ inteiros i com estas propriedades, logo por (4.1.1) $p = u \cdot (1-\zeta_{p^r})^{\varphi(p^r)}$, com u uma unidade em $O_{\mathbb{Q}(\zeta_{p^r})}$. Assim, temos uma igualdade de ideais em $O_{\mathbb{Q}(\zeta_{p^r})}$:

$$\langle p \rangle = \langle 1-\zeta_{p^r} \rangle^{\varphi(p^r)}.$$

Como $O_{\mathbb{Q}(\zeta_{p^r})}$ é um domínio de Dedekind, existem ideais primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ de $O_{\mathbb{Q}(\zeta_{p^r})}$ e inteiros positivos $r_1, \ldots r_n$ tais que:

$$\langle 1-\zeta_{p^r} \rangle = \mathfrak{p}_1^{r_1} \ldots \mathfrak{p}_n^{r_n}.$$

Segue que $\langle p \rangle = \langle 1-\zeta_{p^r} \rangle^{\varphi(p^r)} = \mathfrak{p}_1^{r_1\varphi(p^r)} \cdots \mathfrak{p}_n^{r_n\varphi(p^r)}$, o que dá a fatoração do ideal $\langle p \rangle$ em $O_{\mathbb{Q}(\zeta_{p^r})}$ como o produto de ideais primos neste anel. Pela proposição 3.4.12, temos que:

$$r_1\varphi(p^r) + \cdots + r_n\varphi(p^r) = \varphi(p^r) \cdot (r_1 + \cdots + r_n) \leq [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = \varphi(p^r).$$

Segue que $n = 1$ e $r_1 = 1$. Denotando $\mathfrak{p} := \mathfrak{p}_1$, concluímos que $\langle 1-\zeta_{p^r} \rangle = \mathfrak{p}$ e que $\langle p \rangle = \mathfrak{p}^{\varphi(p^r)}$. Segue que $1-\zeta_{p^r}$ é um elemento primo de $O_{\mathbb{Q}(\zeta_{p^r})}$ e $\langle p \rangle$ é totalmente ramificado em $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$. □

Na prova da Proposição 4.1.16, provamos que $\mathbb{Z}[\zeta_p] \subset O_{\mathbb{Q}(\zeta_p)}$. Utilizando noções mais avançadas da Teoria dos Números, pode-se provar que a inclusão é uma igualdade, num contexto bem geral (vide [7], proposição 3.1.20).

Proposição 4.1.17. *Para todo $n \in \mathbb{N}$, o anel $\mathbb{Z}[\zeta_n]$ é o anel dos inteiros de $\mathbb{Q}(\zeta_n)$*

Demonstração. Em [7], Proposição 3.1.20. □

Proposição 4.1.18. *Sejam $K \subset \mathbb{C}$ um corpo, $\alpha \in \mathbb{C}$ algébrico sobre K e $p(x) \in K[x]$ o polinômio minimal de α sobre K. Se $n = grau\ p(x)$ então:*

$$p(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_n(\alpha)),$$

onde $\sigma_1, \ldots, \sigma_n$ são todos os homomorfismos injetivos possíveis de $K(\alpha)$ em $\mathbb{C}$ que fixam os elementos de K.

Demonstração. Seja $\sigma : K(\alpha) \to \mathbb{C}$ um homomorfismo injetivo que fixa os elementos de K. Um elemento de $K(\alpha)$ é da forma $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, onde $a_i \in K\ \forall i$. Temos que $\sigma(\beta) = a_0 + a_1\sigma(\alpha) + \cdots + a_{n-1}\alpha^{n-1}$, logo, σ fica inteiramente definido pelo seu valor em α.

Como α é raiz de $p(x)$ e σ é homomorfimo, temos:

$$p(\alpha) = 0 \Rightarrow \sigma(p(\alpha)) = \sigma(0) \Rightarrow \sigma(p(\alpha)) = 0 \Rightarrow p(\sigma(\alpha)) = 0.$$

Logo $\sigma(\alpha)$ é raiz de $p(x)$.

Reciprocamente, para toda raiz γ de $p(x)$, o homomorfismo $\psi : K[x] \to K[\gamma]$, $\psi(f(x)) = f(\gamma)$ é sobrejetivo e tem núcleo igual a $\langle p(x) \rangle$ visto que $p(x)$ é irredutível. O teorema dos homomorfismos nos dá o seguinte isomorfismo:

$$K[x]/\langle p(x) \rangle \simeq K[\gamma],$$

que leva $\bar{x}$ em γ. Segue que $K(\alpha) = K[\alpha] \simeq K[x]/\langle p(x) \rangle \simeq K[\gamma] = K(\gamma)$ e essa composta de isomorfismos define um isomorfismo $\sigma : K(\alpha) \to K(\gamma) \subset \mathbb{C}$ tal que $\sigma(\alpha) = \gamma$ e que fixa K. Isto conclui a prova. □

Corolário 4.1.19. *Seja $\zeta_n \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade. Os automorfismos de $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ são da forma $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$, $\sigma(\zeta_n) = \zeta_n^i$ onde $1 \leq i < n$ e $mdc(i,n) = 1$. Em particular $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq \mathbb{Z}_n^*$, o grupo multiplicativo das classes invertíveis em $\mathbb{Z}_n$.*

Demonstração. O n-ésimo polinômio ciclotômico $\Phi_n(x)$ é o polinômio minimal de ζ_n. Pela Proposição 4.1.18, se $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ é um automorfismo, $\sigma(\zeta_n)$ é raiz de $\Phi_n(x)$, logo é uma raiz n-ésima primitiva da unidade. Portanto $\sigma(\zeta_n) = \zeta_n^i$, $1 \leq i < n$ e $mdc(i,n) = 1$. Como os elementos de $\mathbb{Z}_n^*$ são exatamente as classes $\bar{i}$ com $mdc(i,n) = 1$, é imediado que a função $\mathbb{Z}_n^* \to Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ que associa $\bar{i} \in \mathbb{Z}_n^*$ a $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$, $\sigma(\zeta_n) = \zeta_n^i$ é um isomorfismo. □

Lema 4.1.20. *Sejam $n, N \in \mathbb{N}$. O conjunto dos inteiros algébricos α tais que $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq n$ e $|\ \sigma(\alpha)\ | \leq N$ para todos os homomorfismos injetivos $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$ é finito.*

Demonstração. Seja $p(x) \in \mathbb{Q}[x]$ o polinômio minimal de α sobre $\mathbb{Q}$. Pela Proposição 4.1.18, $p(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_m(\alpha))$, onde σ_i são os homomorfismos injetivos de $\mathbb{Q}(\alpha) \to \mathbb{C}$ e $m = grau\ p(x) = [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq n$. Pela Proposição 2.2.13, $p(x) \in \mathbb{Z}[x]$. O coeficiente a_i de $p(x)$,

de grau i, é a soma dos $\binom{m}{i}$ produtos $(-1)^{m-i} \cdot \sigma_{k_1}(\alpha) \cdots \sigma_{k_{m-i}}(\alpha)$, com $1 \leq k_1 < k_2 < \cdots < k_{m-i} \leq m$. Logo:

$$| a_i | \leq \binom{m}{i} \cdot máx\{| \sigma_j(\alpha) |^{m-i} | \ j = 1, \ldots, m\} \leq \binom{n}{i} \cdot N^{m-i}$$

Como cada $a_i \in \mathbb{Z}$, existem finitos polinômios em $\mathbb{Z}[x]$ tais que seus coeficientes satisfaçam a última desigualdade, logo o conjunto dos inteiros algébricos considerado no enunciado do Lema é finito. □

Proposição 4.1.21. *Seja K um corpo numérico. O grupo $\mu(K)$ das raízes da unidade em K é finito e:*

$$\mu(K) = \{\alpha \in O_K \,||\, \sigma(\alpha) |= 1 \quad \text{para todo homomorfismo injetivo } \sigma : \mathrm{K} \to \mathbb{C}\}.$$

Demonstração. Se $\alpha \in O_K$ e $| \sigma(\alpha) |= 1$ para todo $\sigma : K \to \mathbb{C}$ homomorfismo injetivo, então $| \sigma(\alpha^n) |=| \sigma(\alpha)^n |=| \sigma(\alpha) |^n = 1 \ \forall n \in \mathbb{N}$ e $\forall \sigma$. Pelo Lema 4.1.20, o grupo cíclico $\langle \alpha \rangle$ é finito. Segue que $\exists m \in \mathbb{N}$ tal que $\alpha^m = 1$, isto é, $\alpha \in \mu(K)$.

Reciprocamente, se $\zeta \in \mu(K)$ então ζ é uma raiz n-ésima primitiva da unidade para algum $n \in \mathbb{N}$. Então $\mathbb{Q}(\zeta) \subset K$, o que implica que $\zeta \in O_{\mathbb{Q}(\zeta)} \subset O_K$. Além disso, pelo Corolário 4.1.19, se $\sigma : K \to \mathbb{C}$ é um homomorfismo injetivo, $\sigma(\zeta) = \zeta^i$ para algum $i = 1, \ldots, n-1$ com $mdc(i,n) = 1$. Logo $| \sigma(\zeta) |=| \zeta^i |=| \zeta |^i = 1$. Isto conclui a prova. □

O seguinte resultado, que terá sua demonstração omitida, diz respeito a quais raízes da unidade pertencem ao corpo $\mathbb{Q}(\zeta_n)$. Indicamos [11], Lema 11.4, pág 189, para uma prova.

Lema 4.1.22. *As únicas raízes da unidade pertencendo a $\mathbb{Q}(\zeta_n)$ são da forma $\pm\zeta_n^j$, $j = 0, \ldots n-1$.*

4.2 O Último Teorema de Fermat

O Último Teorema de Fermat(UTF), afirma a não existência de soluções inteiras para $x^n + y^n = z^n$ com $xyz \neq 0$ pra todo $n \geq 3$. Fermat provou a conjectura para $n = 4$. O UTF foi provado por Andrew Wiles em 1996 usando métodos muito além deste trabalho. Provaremos aqui um caso particular do UTF, devido a Kummer, para expoentes primos ímpares de uma classe especial: a dos primos regulares.

Definição 4.2.1. Dizemos que um primo ímpar p é *regular* se p não divide a ordem de $Cl_{\mathbb{Q}(\zeta_p)}$.

Observação 4.2.2. O grupo de classe nem sempre tem ordem finita, mas para um corpo numérico esse resultado é verdadeiro, a demonstração para isso encontra-se em [12] teorema 4.4.

Fixando um primo p e uma raiz p-ésima da unidade em $\mathbb{Q}(\zeta_p)$. Vamos precisar de alguns lemas.

Lema 4.2.3. *Sejam $x, y \in \mathbb{Z}$ primos entre si, e suponha que $p \nmid x+y$. Então os elementos $x+\zeta_p^i y$ de $\mathbb{Z}[\zeta_p]$ para $0 \leq i \leq p-1$ são dois a dois primos entre si.*

Demonstração. Suponha que exista $\mathfrak{q}$ um ideal primo de $\mathbb{Z}[\zeta_p]$ dividindo ambos $x+\zeta_p^i y$ e $x+\zeta_p^j y$ para certos i, j com $0 \leq i < j < p$. então:

$$\begin{array}{ccccc} \mathfrak{q} \mid x+\zeta_p^i y & \rightarrow & \mathfrak{q} \mid \zeta_p^j(x+\zeta_p^i y) & \rightarrow & \mathfrak{q} \mid \zeta_p^j x+\zeta_p^j\zeta_p^i y \\ \mathfrak{q} \mid x+\zeta_p^j y & \rightarrow & \mathfrak{q} \mid \zeta_p^i(x+\zeta_p^j y) & \rightarrow & \mathfrak{q} \mid \zeta_p^i x+\zeta_p^j\zeta_p^i y \\ \hline \mathfrak{q} \mid \zeta_p^j y-\zeta_p^i y & & & & \mathfrak{q} \mid \zeta_p^j x-\zeta_p^i x \end{array}$$

ou seja, $\mathfrak{q} \mid (\zeta_p^j-\zeta_p^i)y$ e $\mathfrak{q} \mid (\zeta_p^j-\zeta_p^i)x$. Como x e y são primos entre si, $\mathfrak{q}$ não pode dividir x e y simultaneamente, pois do contrário, teríamos $x, y \in \mathfrak{q} \Rightarrow 1 = mdc(x,y) \in \mathfrak{q}$, o que impossível, pois $\mathfrak{q}$ é primo. Logo $\mathfrak{q} | (\zeta_p^j-\zeta_p^i)$. Como $\mathfrak{q}$ é primo segue da igualdade

$$(\zeta_p^j-\zeta_p^i) = \zeta_p^j(1-\zeta_p)\frac{(1-\zeta_p^{i-j})}{(1-\zeta_p)},$$

que $\zeta_p^j \in \mathfrak{q}$ ou $1-\zeta_p \in \mathfrak{q}$ ou $\frac{1-\zeta_p^{i-j}}{1-\zeta_j}$. A primeira possibilidade implicaria em $\mathfrak{q}$ conter uma raiz p-ésima da unidade e a terceira em conter um elemento invertível de $\mathbb{Z}[\zeta_p]$, pelo Lema 4.1.15. Qualquer uma dessas possibilidades implicaria $1 \in \mathfrak{q}$, o que é impossível. Segue que $1-\zeta_p \in \mathfrak{q}$. Como $1-\zeta_p$ é um elemento primo de $\mathbb{Z}[\zeta_p]$ e este anel é domínio de Dedekind, segue que $\mathfrak{q} = \langle 1-\zeta_p \rangle$. Portanto, como $1-\zeta_p^i = (1-\zeta_p)(1+\zeta_p+\cdots+\zeta_p^{i-1}) \in \mathfrak{q}$, temos:

$$\begin{array}{rcll} y(1-\zeta_p^i) & \equiv & 0 & mod\ (1-\zeta_p) \\ y\zeta_p^i - y & \equiv & 0 & mod\ (1-\zeta_p) \\ y\zeta_p^i & \equiv & y & mod\ (1-\zeta_p) \\ x+y\zeta_p^i & \equiv & x+y & mod\ (1-\zeta_p) \\ & \Downarrow & & \\ x+y & \equiv & 0 & mod\ (1-\zeta_p) \\ & \Downarrow & & \\ x+y & \equiv & 0 & mod\ (p) \end{array}$$

onde a penúltima implicação segue da suposição de que $\mathfrak{q} \mid x+\zeta_p^i y$ e a última do fato de $\langle p \rangle = \mathfrak{q} \cap \mathbb{Z}$ (vide Proposição 4.1.16). Assim, $p \mid x+y$, o que é uma contradição, logo $\mathfrak{q}$ não pode existir. □

Lema 4.2.4. *Seja $\varepsilon \in \mathbb{Z}[\zeta_p]^\times$. Então existe um $j \in \mathbb{Z}$ tal que $\varepsilon\zeta_p^j$ é fixado pela conjugação de números complexos (ou seja, é um número real).*

Demonstração. Para $p = 2$ o resultado é imediato. Seja p ímpar. Se $\alpha \in \mathbb{Q}(\zeta_p)$ então

$$\alpha = \sum_{j=0}^{p-2} a_j \zeta_p^j,\ a_j \in \mathbb{Q},\ \forall j.$$

Logo,

$$\overline{\alpha} = \sum_{j=0}^{p-2} a_j \overline{\zeta_p}^j = \sum_{j=0}^{p-2} a_j \zeta_p^{-j},$$

onde a última igualdade segue do fato de $\zeta_p \cdot \overline{\zeta_p} = |\ \zeta_p\ |^2 = 1$. Se $\sigma \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ então como $\sigma(\zeta_p) = \zeta_p^i$ para algum $i = 0, \ldots, p-1$, $mdc(i,p) = 1$, temos que $|\ \sigma(\zeta_p)\ | = 1$ e novamente, $\sigma(\overline{\zeta_p}) = \overline{\sigma(\zeta_p)}$. Segue que:

$$\sigma(\overline{\alpha}) = \sigma(\sum_{j=0}^{p-2} a_j \zeta_p^{-j}) = \sum_{j=0}^{p-2} a_j \sigma(\zeta_p)^{-j} = \sum_{j=0}^{p-2} a_j \overline{\sigma(\zeta_p)^j} = \overline{\sum_{j=0}^{p-2} a_j \sigma(\zeta_p)^j} = \overline{\sigma(\alpha)}.$$

Portanto:

$$|\ \sigma(\overline{\varepsilon}\varepsilon^{-1})\ | = |\ \sigma(\overline{\varepsilon})\sigma(\varepsilon^{-1})\ | = \left|\frac{\sigma(\overline{\varepsilon})}{\sigma(\varepsilon)}\right| = \left|\frac{\overline{\sigma(\varepsilon)}}{\sigma(\varepsilon)}\right| = 1,$$

pois todo complexo tem o mesmo módulo que seu conjugado. Segue que $\sigma(\overline{\varepsilon}\varepsilon^{-1})$ tem módulo 1, $\forall \sigma \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Pela Proposição 4.1.21, $\overline{\varepsilon}\varepsilon^{-1}$ é uma raiz da unidade. Pelo Lema 4.1.22, $\overline{\varepsilon}\varepsilon^{-1} = \pm\zeta_p^i$ para algum $i \in \{0, 1, \ldots, p-1\}$.

Suponha por absurdo que o Lema seja falso. Então $\forall j \in \mathbb{Z}$, $\varepsilon\zeta_p^j \neq \overline{\varepsilon\zeta_p^j} = \overline{\varepsilon}\zeta_p^{-j}$. Assim, $\frac{\overline{\varepsilon}\zeta_p^{-j}}{\varepsilon\zeta_p^j} = \overline{\varepsilon}\varepsilon^{-1}\zeta_p^{-2j} \neq 1$, $\forall j \in \mathbb{Z}$, ou seja, $\overline{\varepsilon}\varepsilon^{-1} \neq \zeta_p^{2j}$, $\forall j \in \mathbb{Z}$. Segue desta última afirmação que $\overline{\varepsilon}\varepsilon^{-1}$ não é uma raiz p-ésima da unidade. Portanto, $\overline{\varepsilon}\varepsilon^{-1} = -\zeta_p^i$.

Como $\varepsilon \in \mathbb{Z}[\zeta_p]$, podemos "dividir" ε por $1 - \zeta_p$, obtendo $c \in \mathbb{Z}$ e $x \in \mathbb{Z}[\zeta_p]$ tais que:

$$\varepsilon = x(1 - \zeta_p) + c.$$

Portanto $\varepsilon \equiv c \bmod(1 - \zeta_p)$ e daí, $\overline{\varepsilon} \equiv c \bmod(1 - \zeta_p)$.

Repare que $1 - \zeta_p^i = (1 - \zeta_p)(1 + \zeta_p + \cdots + \zeta_p^{i-1}) \equiv 0 \bmod(1 - \zeta_p)$, logo $\zeta_p^i \equiv 1 \bmod(1 - \zeta_p)$. Portanto:

$$\overline{\varepsilon} = -\zeta_p^i \varepsilon \equiv -\varepsilon \equiv -c \bmod(1 - \zeta_p).$$

Como $\overline{\varepsilon} \equiv c \bmod(1 - \zeta_p)$, segue que $2\overline{\varepsilon} \equiv 0 \bmod(1 - \zeta_p)$, isto é, $2\overline{\varepsilon} \in \langle 1 - \zeta_p \rangle$. Pela Proposição 4.1.16, $\langle 1 - \zeta_p \rangle$ é um ideal primo e $p \in \langle 1 - \zeta_p \rangle$. Como p é ímpar, $2 \notin \langle 1 - \zeta_p \rangle$, pois do contrário, $1 = mdc(2, p) \in \langle 1 - \zeta_p \rangle$, o que não é possível. Segue que $\overline{\varepsilon} \in \langle 1 - \zeta_p \rangle$, isto é, $\overline{\varepsilon} \equiv 0 \bmod(1 - \zeta_p)$. Como $\overline{\varepsilon} \equiv \varepsilon \bmod(1 - \zeta_p)$, concluímos que $\varepsilon \in \langle 1 - \zeta_p \rangle$. Mas isto é um absurdo, pois por hipótese, ε é invertível em $\mathbb{Z}[\zeta_p]$. Isto conclui a prova do Lema. □

Lema 4.2.5. *Para todo $\alpha \in \mathbb{Z}[\zeta_p]$ e p primo, $\alpha^p \in \mathbb{Z} + p\mathbb{Z}[\zeta_p]$.*

Demonstração. Escreva $\alpha = a_0 + a_a\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, $a_i \in \mathbb{Z}\ \forall i$. Como os binomiais $\binom{p}{i}$ são múltiplos de p (e portanto nulos módulo p) para todo $i = 1, \ldots, p-1$, temos:

$$\alpha^p = (a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2})^p \equiv a_0^p + (a_1\zeta_p)^p + \cdots + (a_{p-2}\zeta_p^{p-2})^p \equiv$$

$$\equiv a_0^p + a_1^p + \cdots + a_{p-2}^p \bmod p$$

Portanto, existe $x \in \mathbb{Z}[\zeta_p]$ tal que

$$\alpha^p = (a_0^p + \cdots + a_{p-2}^p) + px.$$

Como a soma entre parênteses é um número inteiro, o Lema está provado. □

Lema 4.2.6. *Seja $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$ com $a_i \in \mathbb{Z}\ \forall i$ tal que ao menos um dos a_i é nulo. Se α é divisível por um número inteiro n, isto é, se $\alpha \in n\mathbb{Z}[\zeta_p]$, então todos os coeficientes a_i são divisíveis por n.*

Demonstração. Como $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, segue que $1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$. Como $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, qualquer subconjunto de $\{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$ com $p-1$ elementos também será uma base dessa extensão.

Suponha que $a_{p-1} = 0$. Por hipótese, $\alpha \in n\mathbb{Z}[\zeta_p]$, logo:

$$a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta^{p-2} = n(b_0 + b_1\zeta_p + \cdots + b_{p-2}\zeta_{p-2}),$$

onde $b_i \in \mathbb{Z}\ \forall i$. Isto nos dá a seguinte combinação linear nula em $\mathbb{Z}[\zeta_p]$:

$$(a_0 - nb_0) + (a_1 - nb_1)\zeta_p + \cdots + (a_{p-2} - nb_{p-2})\zeta_p^{p-2} = 0.$$

Portanto, $a_i = nb_i$, $\forall i$.

Suponha agora que $a_{p-1} \neq 0$. Então, outro coeficiente de α deverá ser nulo, digamos a_0. Logo:

$$\alpha = a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}.$$

Como $\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\}$ também é uma base, temos que todo $\beta \in \mathbb{Z}[\zeta_p]$ pode ser escrito como combinação de seus elementos. Logo, como $\alpha \in n\mathbb{Z}[\zeta_p]$:

$$a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1} = nb_1\zeta_p + \cdots + nb_{p-1}\zeta_p^{p-1},$$

onde $b_i \in \mathbb{Z}\ \forall i$. Da mesma forma que o caso anterior, concluímos que $a_i = nb_i\ \forall i$.

Os demais casos em que $a_j = 0$, $1 \leq j \leq p-2$, se procede de forma análoga, utilizando a base $\{1, \zeta_p, \ldots \zeta_p^{j-1}, \zeta_p^{j+1}, \ldots, \zeta_p^{p-1}\}$.

□

Agora finalmente temos todas as ferramentas para provar o resultado principal desta monografia.

Teorema 4.2.7. *(Kummer). Seja p um primo regular. Então não existem inteiros x,y,z com $p \nmid xyz$ tal que $x^p + y^p = z^p$.*

Demonstração. Suponha por absurdo existam $x,y,z \in \mathbb{Z}$ com $p \nmid xyz$ tais que $x^p + y^p = z^p$. Removendo os fatores em comum podemos supor $mdc(x,y,z) = 1$.

Para o caso onde $p = 3$, note que sendo $x \in \mathbb{Z}$ e $x \neq 3q$ temos que ou $x = 3q+1$, ou $x = 3q+2$, com $q \in \mathbb{Z}$. Temos:

$$\begin{array}{lll} x = 3q+1 & \Rightarrow & x^3 = 9\cdot 3q^3 + 9\cdot 3q^2 + 9q + 1 \quad \Rightarrow \quad x^3 \equiv 1 \pmod 9. \\ x = 3q+2 & \Rightarrow & x^3 = 9\cdot 3q^3 + 9\cdot 6q^2 + 9\cdot 12q + 8 \quad \Rightarrow \quad x^3 \equiv -1 \pmod 9. \end{array}$$

como vale o mesmo para y e para z, as únicas possibilidades são:

- ou $x^3 + y^3 \equiv 0 (\text{mod } 9)$;
- ou $x^3 + y^3 \equiv 2 (\text{mod } 9)$;
- ou $x^3 + y^3 \equiv -2 (\text{mod } 9)$.

Mas $x^3 + y^3 = z^3 \equiv -1, 1$ ou $0 (\text{mod } 9)$, contradição. Assim o Teorema está provado para $p = 3$.

Então, podemos assumir $p \geq 5$ a partir de agora.

Se $x \equiv y \pmod p$ e $x \equiv -z \pmod p$ então $x^p \equiv y^p \pmod p$ e $x^p \equiv -z^p \pmod p$, assim como $x^p + y^p = z^p$, temos:

$$2x^p \equiv y^p - z^p (\text{mod } p) \Rightarrow 2x^p \equiv -x^p (\text{mod } p) \Rightarrow 3x^p \equiv 0 (\text{mod } p),$$

ou seja, p divide $3x^p$, o que não pode acontecer uma vez que $p \nmid xyz$ e $p \geq 5$. Segue que uma das congruências $x \equiv y (\text{mod } p)$ e $x \equiv z (\text{mod } p)$ não é verdadeira. Se a primeira não ocorre, $p \nmid x - y$. Se a segunda congruência não ocorre, $p \nmid x - (-z)$, daí rearrumamos a equação para $x^3 + (-z)^3 = (-y)^3$, chamamos $-y = z'$ e $-z = y'$ obtendo $x^3 + y'^3 = z'^3$ assim teremos que $p \mid x + z'$ e $p \nmid x - y'$. Então sem perda de generalidade, podemos assumir que $p \nmid x - y$.

Em $\mathbb{Z}[\zeta_p]$, $x^p + y^p$ pode ser fatorado, e temos

$$\prod_{i=0}^{p-1} (x + \zeta_p^i y) = z^p.$$

De fato, as raízes do polinômio $T^p + 1$ são $-1, -\zeta_p, \ldots, -\zeta_p^{p-1}$. Logo

$$T^p + 1 = \prod_{i=0}^{p-1} (T + \zeta_p^i).$$

Fazendo $T = \frac{x}{y}$ e multiplicando os dois lado das igualdade por y^p, obtemos:

$$z^p = x^p + y^p = \prod_{i=0}^{p-1}(x + \zeta_p^i y).$$

Em termos de ideais, isto significa que

$$\prod_{i=0}^{p-1}\langle x + \zeta_p^i y\rangle = \langle z\rangle^p.$$

Pelo Lema 4.2.3, os ideais $\langle x + \zeta_p^i y\rangle$ são primos dois a dois, assim para que o produtório seja uma p-ésima potência de um ideal, temos que cada ideal $\langle x + \zeta_p^i y\rangle$ também deve ser uma p-ésima potência de algum ideal $\mathfrak{a}$ de $\mathbb{Z}[\zeta_p]$. Então:

$$\langle x + \zeta_p y\rangle = \mathfrak{a}^p.$$

Esta igualdade significa que $\overline{\mathfrak{a}}^p = \overline{1}$ em $Cl_{\mathbb{Q}(\zeta_p)}$. Seja $h = \mid Cl_{\mathbb{Q}(\zeta_p)} \mid$. Por hipótese, p não divide a ordem h de $Cl_{\mathbb{Q}(\zeta_p)}$. Assim $mdc(p,h) = 1$, então $\exists r,s \in \mathbb{Z}$ tais que $rp + sh = 1$. Temos:

$$\bar{\mathfrak{a}} = \bar{\mathfrak{a}}^{rp+sh} = \bar{\mathfrak{a}}^{rp} \cdot \bar{\mathfrak{a}}^{sh} = (\bar{\mathfrak{a}}^p)^r \cdot (\bar{\mathfrak{a}}^h)^s = \bar{1}^r \cdot \bar{1}^s = \bar{1},$$

ou seja, o ideal $\mathfrak{a}$ é principal. Seja $\alpha \in \mathbb{Z}[\zeta_p]$ um gerador de $\mathfrak{a}$. Então temos que $\langle x + \zeta_p^y\rangle = \langle \alpha^p\rangle$. Portanto:

$$x + \zeta_p y = \varepsilon\alpha^p,$$

para algum $\varepsilon \in \mathbb{Z}[\zeta_p]^\times$. Pelo Lema 4.2.5, $\exists c \in \mathbb{Z}$ tal que $\alpha^p \equiv c \bmod p$.

Pelo Lema 4.2.4, existe $j \in \mathbb{Z}$ tal que $\varepsilon' = \zeta_p^j\varepsilon$ é fixado pela conjugação complexa. Então temos que $x + \zeta_p y = \varepsilon'\zeta_p^{-j}\alpha^p$, logo:

$$x + \zeta_p y \equiv \zeta_p^{-j}\varepsilon' c \bmod (p),$$

então, aplicando o conjugado em ambos os membros da congruência temos:

$$x + \zeta_p^{-1} y \equiv \zeta_p^j\varepsilon' c \bmod (p),$$

pois $\overline{\varepsilon'} = \bar{\varepsilon}$. As duas últimas congruências implicam que $\zeta_p^j(x + \zeta_p y) \equiv \zeta_p^{-j}(x + \zeta_p^{-1} y) \bmod p$.

Portanto, $x + \zeta_p^{-1} y - \zeta_p^{2j} x - \zeta_p^{2j+1} y$ é divisível por p.

Se ζ_p^{2j} , ζ_p^{2j+1} , 1 e ζ_p^{-1} são raízes p-ésimas da unidade distintas, então uma vez que $p - 1 \geq 4$, pelo Lema 4.2.6 x e y são divisíveis por p, uma contradição.

Logo, dois dos termos ζ_p^{2j}, ζ_p^{2j+1}, 1 e ζ_p^{-1} devem ser iguais. Não podemos ter $\zeta_p^{-1} = 1$, pois

$\zeta_p \neq 1$. Pelo mesmo motivo, $\zeta_p^{2j} \neq \zeta_p^{2j+1}$. Assim, restam as seguintes possibilidades:

$$(1)\ \zeta_p^{2j} = 1; \quad (2)\ \zeta_p^{2j+1} = 1; \quad (3)\ \zeta_p^{2j} = \zeta_p^{-1}; \quad (4)\ \zeta_p^{2j+1} = \zeta_p^{-1}.$$

Note que (2) e (3) são equivalentes e que (4) é equivalente a $\zeta_p^{2j+2} = 1$. Segue que $1 = \zeta_p^{2j}, \zeta_p^{2j+1}$ ou ζ_p^{2j+2}.

No primeiro desses casos, temos que $\zeta_p^{-1}y - \zeta_p^{2j+1}$ é divisível por p, logo pelo Lema 4.2.6 p divide y, uma contradição.

No segundo caso, temos que $(x-y) + \zeta_p^{-1}y - \zeta_p^{2j+1}x$ é divisível por p, logo pelo Lema 4.2.6 p divide $x-y$, novamente uma contradição.

No último caso, temos que $\zeta_p^{2j+1} = \zeta_p^{-1}$, logo $x - \zeta_p^{2j}x$ é divisível por p, logo pelo Lema 4.2.6 p divide x, contradição, finalizando a prova. □

Considerações finais

Neste trabalho foi provado um caso particular do UTF, que apesar no fim ter sido uma falha, foi responsável por expandir o estudo de estruturas e objetos matemáticos, desenvolvendo a matemática principalmente na área da teoria dos números algébricos.

A principal motivação para a escolha do tema, foi poder estudar uma aplicação para os polinômios e extensões ciclotômicas, que foi um assunto que me chamou atenção durante a disciplina de introdução à Teoria de Galois.

Até que se chegasse na prova do teorema, ficou claro o quanto as disciplinas de base e boas referências são importantes numa pesquisa, e em alguns momentos compreender plenamente alguns resultados foi desafiador, o que certamente me trouxe grande amadurecimento na pesquisa em matemática, principalmente na área de Álgebra.

Apesar de não ter sido possível demonstrar todos os resultados devido a complexidade do tema para um aluno de graduação, os objetivos traçados foram cumpridos satisfatoriamente.

Pode ser percebido que algumas proposições e teoremas foram apenas enunciados e referenciados. Espero poder dar continuidade nos estudos nesta área específica da álgebra para que essas lacunas deixadas no texto possam demonstradas de forma completa numa futura pesquisa ou num curso de Teoria dos Números.

Referências Bibliográficas

[1] SINGH, S. **O último teorema de Fermat**: a história do enigma que confundiu as mais brilhantes mentes do mundo durante 358 anos, 1ª ed., Rio de Janeiro: BestBolso, 2014.

[2] GARCIA, A.; LEQUAIN, Y. **Elementos de álgebra**, 1ª ed., Rio de Janeiro: SBM, 2014.

[3] TENGAN, E. **Álgebra comutativa:** um tour ao redor dos anéis comutativos, São Paulo, 2010.

[4] LAFETÁ, A.C.; LELIS J.; SILVA E. **Teoria dos números transcendentes**: do teorema de Liouville à conjectura de Shanuel, 1ª ed., Rio de Janeiro: SBM, 2016.

[5] ENDLER, O. **Teoria dos Corpos**, Rio de Janeiro,IMPA,2006.

[6] BAKER, A. **An introduction to Galois theory**, 2013.

[7] SHARIFI, R. **Algebraic number theory**.

[8] EISENBUD, D. **Commutative Algebra with a View Toward Algebraic Geometry**, Springer, 2004.

[9] ATIYAH, M. F.:MACDONALD, I. G. **Introduction to commutative Álgebra**, Addison-Wesley Publishing Company, 1969.

[10] MARQUES, C.M. **Introdução à teoria de anéis**, UFMG, 1999.

[11] STEWART,I.,TALL,D. **Algebraic Number Theory and Fermat Last Theorem**, Editora AK Peters, 4ª edição, 2002.

[12] MILNE, J.S. **Algebraic number theory**, 2017.

[13] SOUZA, M.A de. **Introdução a teoria de Galois**, Universidade Federal do Rio Grande, 2017.

[14] CAMINHA, A. **Polinômios ciclotômicos e o teorema dos primos de Dirichlet**, 2003.