Universidade Federal de Juiz de Fora
Instituto de Ciências Exatas
Departamento de Matemática

Franciele do Carmo Silva

O Último Teorema de Fermat: Casos Especiais

Juiz de Fora
2018

Franciele do Carmo Silva

O Último Teorema de Fermat: Casos Especiais

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemáticada Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do título de Bacharel em Matemática.

Orientadora: Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2018

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF com os dados fornecidos pelo(a) autor(a)

Silva, Franciele do Carmo.
O Último Teorema de Fermat : Casos Especiais / Franciele do Carmo Silva. – 2018.
112 f.

Orientadora: Beatriz Casulari da Motta Ribeiro
Trabalho de Conclusão de Curso (Graduação) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Departamento de Matemática, 2018.

1. Último Teorema de Fermat. 2. Teorema de Sophie Germain. 3. Teorema de Kummer. I. Ribeiro, Beatriz Casulari da Motta, orient. II. Título.

Franciele do Carmo Silva

O Último Teorema de Fermat: Casos Especiais

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemáticada Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do título de Bacharel em Matemática.

Aprovada em:

BANCA EXAMINADORA

Prof. Dra. Beatriz Casulari da Motta Ribeiro - Orientadora
Universidade Federal de Juiz de Fora

Professor Dra. Flaviana Andrea Ribeiro
Universidade Federal de Juiz de Fora

Professor Dr. Frederico Sercio Feitosa
Universidade Federal de Juiz de Fora

AGRADECIMENTOS

"It matters little who first arrives at an idea,
rather what is significant is how far that idea can go."
(Sophie Germain)

RESUMO

O objetivo principal deste trabalho é demonstrar alguns casos especiais do famoso Último Teorema de Fermat: não existem x, y, z inteiros satisfazendo $x^n + y^n = z^n$ quando n é maior do que 2, com exceção dos casos triviais. Começamos com os casos em que n é 3 ou 4, para os quais usamos resultados sobre os anéis quadráticos euclidianos. Em seguida, estudamos casos mais gerais, incluindo os casos apresentados no Teorema de Sophie Germain e no Teorema de Kummer para primos regulares, no qual usamos corpos ciclotômicos.

Palavras-chave: Último Teorema de Fermat. Teorema de Sophie Germain. Teorema de Kummer.

ABSTRACT

The main purpose of this work is to prove some special cases of the famous Fermat's Last Theorem: there are no intergers x, y, z such that $x^n + y^n = z^n$ where n is greater than 2, except for the trivial cases. Using results about quadratic euclidean rings, we prove the theorem for $n = 3$ and $n = 4$. We also study some more general cases, including the ones in Sophie Germain's Theorem and Kummer's theorem for regular primes, in which we use cyclotomic fields.

Key-words: Fermat's Last Theorem. Sophie Germain's Theorem. Kummer's Theorem.

LISTA DE ABREVIATURAS E SIGLAS

DIP	Domínio de Ideais Principais
DFU	Domínio de Fatoração Única
UTF	Último Teorema de Fermat
SCR	Sistema Completo de Resíduos
SRR	Sistema Reduzido de Resíduos
TSG	Teorema de Sophie Germain

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{R}$	Conjunto dos números reais
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{C}$	Conjunto dos números complexos
$\mathbb{D}$	Domínio de integridade
$\mathbb{L}$	Corpo algébrico
$\deg f(x)$	Grau do polinômio $f(x)$
$\mathcal{O}_{\mathbb{L}}$	Anel de inteiros algébricos do corpo $\mathbb{L}$
$\mathcal{N}(\alpha)$	Norma do elemento α pertencente ao Corpo Quadrático
$\mathcal{U}$	Conjunto de unidades do Anel Quadrático de Inteiros
φ	Aplicação *phi* de Euler
ζ	Raiz p-ésima da unidade, com p número primo
$\mathbb{Q}(\zeta)$	Corpo Ciclotômico
$P_{\zeta}(x)$	Polinômio minimal de ζ sobre $\mathbb{Q}$
$Ker(\phi)$	Núcleo do homomorfismo ϕ
$Im(\phi)$	Imagem do homomorfimo ϕ
(α)	Norma de α com relação a uma extensão de $\mathbb{Q}$
$Tr(\alpha)$	Traço de α com relação a uma extensão de $\mathbb{Q}$
$\langle\alpha\rangle$	Ideal gerado pelo elemento α
$\mathcal{O}_B(A)$	Conjunto de inteiros de B sobre A
$\#A$	Cardinalidade de um conjunto A
$N(I)$	Norma do ideal I
$\mathcal{F}(\mathbb{L})$	Conjunto dos ideais fracionários do anel $\mathcal{O}_{\mathbb{L}}$
$\mathcal{H}(\mathbb{L})$	Grupo de classe do anel $\mathcal{O}_{\mathbb{L}}$

$\mathcal{P}(\mathbb{L})$	Conjunto dos ideais fracionários principais de $\mathcal{O}_{\mathbb{L}}$
$h(\mathbb{L})$	Número de classe de $\mathcal{O}_{\mathbb{L}}$
$\mathcal{F}$	Conjunto dos ideais fracionários do anel $\mathbb{Z}[\zeta]$
$\mathcal{H}$	Grupo de classe do anel $\mathbb{Z}[\zeta]$
$\mathcal{P}$	Conjunto dos ideais fracionários principais de $\mathbb{Z}[\zeta]$
h	Número de classe de $\mathbb{Z}[\zeta]$

SUMÁRIO

1 INTRODUÇÃO

Esse trabalho se propõe a apresentar provas de casos particulares do Último Teorema de Fermat, o qual afirma que a equação $x^n + y^n = z^n$ não admite solução inteira não trivial para n natural maior que 2.

Motivado pelo estudo de ternos pitagóricos, Pierre de Fermat, em 1617, conjecturou tal resultado às margens do livro *Aritmética*, de Diofante, afirmando possuir uma prova para o mesmo, mas não ter espaço suficiente para apresentá-la. Apesar de tal afirmação e de seu enunciado de simples compreeensão, o teorema permaneceria por mais de 350 anos sem demonstração e motivaria gerações de matemáticos em sua busca.

O primeiro avanço em direção à prova foi feito apenas um século depois, por Leonhard Euler, que, por meio de uma abordagem semelhante à sugerida por Fermat em seu esboço do caso $n = 4$, provou a inexistência de solução para $n = 3$. Em seguida, diversos matemáticos direcionaram seus estudos para o caso dos expoentes primos, visto que eles permitiriam a generalização. Nesse sentido, Sophie Germain forneceu grande contribuição, ao delinear os cálculos com determinados primos, abordagem que inspiraria as demonstrações feitas por Legendre e Dirichlet para o caso $n = 5$.

No século XIX, a Academia Francesa de Ciências ofereceu prêmios a quem solucionasse o problema, intensificando a busca pela demonstração. Contudo, apesar de abordagens fascinantes, como as feitas por Cauchy e Lamé, e da contribuição de Kummer, nenhum matemático fora capaz de comprovar o resultado. Em meados do século XX, a Conjectura Taniyana-Shimura foi apresentada: existiria uma ligação intrínseca entre as formas modulares e as curvas elípticas. Além de estabelecer a relação entre campos tão distintos, a prova de tal conjectura, conforme mostrado por Frey e Ribet, implicaria na demonstração do Último Teorema de Fermat.

Com este avanço, o matemático Andrew Wiles retornou sua dedicação ao problema que o instigara na infância e, em 1994, após anos de estudo, demonstrou a Conjectura Taniyana-Shimura utilizando desde a teoria de grupos à combinação dos métodos de análise de equações elípticas criados por Iwasama e Kolyvagin-Flach, com o auxílio, ao final, de Richard Taylor. Finalmente, o Último Teorema de Fermat estava provado.

Nesse contexto, cabe ressaltar que a relevância de tal teorema ultrapassa sua aplicabilidade em Teoria dos Números, na medida em que a busca por sua solução proporcionou a criação e expansão de inúmeras áreas matemáticas. Por meio dele, novas técnicas foram criadas, enquanto técnicas tradicionais foram utilizadas de modo inovador, ampliando as possibilidades de abordagem de diversos problemas.

Neste trabalho, começaremos apresentando a prova para dois casos pontuais,

quando n é igual a 3 ou a 4, utilizando de corpos e anéis quadráticos euclidianos. Além disso, estudaremos casos mais gerais, como o caso apresentado no Teorema de Sophie Germain, o qual prova o teorema para primos cujos primos auxiliares satisfazem determinadas condições, e o caso apresentado no Teorema de Kummer, o qual demonstra um dos cenários possíveis para o teorema quando n é um primo regular.

Com tal intuito, dividiremos este trabalho da seguinte forma:

No Capítulo 2, serão apresentadas definições e propriedades importantes referentes aos Anéis Quadráticos, principalmente, aos Anéis Quadráticos Euclidianos.

No Capítulo 3, será apresentada um breve histórico do surgimento do Último Teorema de Fermat, com o aprofundamento em sua motivação: o Teorema de Pitágoras. Assim, estudaremos os ternos pitagóricos, especialmente os primitivos.

No Capítulo 4, apresentaremos as provas para os casos $n = 3$ e $n = 4$, sendo a primeira resultante do estudo dos anéis quadráticos euclidianos e a segunda, do estudo dos ternos pitagóricos.

No Capítulo 5, faremos um breve estudo das equações de Barlow e Abel, estabelecidas na busca pela solução do Último Teorema de Fermat, e apresentaremos os conceitos criados por Sophie Germain em sua abordagem para o problema. Ressaltaremos a relevância de suas ideias nas tentativas futuras de demonstrar o teorema e provaremos os resultados por ela provados, tanto em sua versão geral uanto em sua versão mais fraca.

Por fim, no Capítulo 6, apresentaremos a abordagem utilizada por Lamé e o problema que inviabilizou a prova completa do teorema seguindo suas ideias. Mostraremos, ainda, como Kummer utilizou sua abordagem para provar o teorema para os primos regulares. Utilizaremos, para tanto, o estudo feito por Dedekind, incluindo os domínios de Dedekind, os ideais fracionários e suas principais propriedades. Estudaremos também os grupos de classe de um anel de inteiros, permitindo a definição de primos regulares e a posterior demonstração do Teorema de Kummer na última seção.

Ressaltamos que, para a abordagem da fundamentação teórica necessária aos tópicos descritos acima, utilizaremos, sem demonstrar, alguns resultados das teorias de anéis e de grupos, além de domínios euclidianos, domínios de ideais principais e os de fatoração única. Sugerimos as referências [7], [8] e [6] para tais tópicos.

2 ANÉIS QUADRÁTICOS

Embora o Último Teorema de Fermat tenha surgido como um problema no campo da Teoria dos Números, a busca por sua solução impulsionou o desenvolvimento de diversas áreas matemáticas, dentre elas, a Teoria Algébrica dos Números.

Tal teoria concentra seus estudos nos anéis de inteiros algébricos, ou seja, nos quais todos elementos são raízes de polinômios com coeficientes inteiros. Em particular, podemos nos restringir ao estudo de anéis de inteiros algébricos em que tal polinômio possui grau 2, chamados *anéis quadráticos*.

Um desses anéis, em específico, será fundamental para a prova do Último Teorema de Fermat para o caso $n = 3$, a qual irá empregar técnicas semelhantes às desenvolvidas na demonstração feita por Euler.

Nesse contexto, este capítulo se dedica ao estudo aprofundado desses anéis, tal como aos corpo a eles associados, denominados *corpos quadráticos*. Assim, estabeleceremos suas principais propriedades e apresentaremos alguns exemplos esclarecedores. Além disso, direcionaremos nosso estudo aos anéis que também se caracterizam como *anéis euclidianos*.

2.1 CARACTERIZAÇÃO GERAL

Para a definição de *corpos quadráticos*, necessitaremos de alguns conceitos próprios da Teoria Algébrica dos Números:

Definição 2.1.1. *Seja* $\mathbb{Q}[x]$ *o anel de polinômios em* x *com coeficientes em* $\mathbb{Q}$ *representado por:*

$$\mathbb{Q}[x] = \left\{ a_n x^n + a_{n-1} n^{n-1} + \cdots + a_0 : \ a_i \in \mathbb{Q} \quad \text{para todo} \quad i = 0, \ldots, n \right\}$$

Dizemos que um número complexo α *é algébrico sobre* $\mathbb{Q}$ *se existe um polinômio não nulo* $f(x) \in \mathbb{Q}[x]$ *tal que* $f(\alpha) = 0$ *(neste caso, dizemos que* $f(x)$ *anula* α *ou, ainda, que* α *anula* $f(x)$*). Caso não exista tal polinômio, dizemos que* α *é transcendente em* $\mathbb{Q}$*.*

Definição 2.1.2. *Definimos o polinômio mínimo de* α *sobre* $\mathbb{Q}$ *como sendo o polinômio mônico de menor grau em* $\mathbb{Q}$ *que anula* α*.*

Observação 2.1.1. Notemos que o polinômio mínimo de α sobre $\mathbb{Q}$ é único.

De fato, se $f(x), g(x) \in \mathbb{Q}$ são dois polinômios mônicos distintos e de mesmo grau que anulam α, temos que $(f - g)(x)$ é um polinômio em $\mathbb{Q}$, não nulo, e que anula α.

Mais ainda, como $f(x)$ e $g(x)$ são mônicos, temos que $(f - g)(x)$ tem grau menor que o de $f(x)$. Agora, dividindo $(f - g)(x)$ pelo seu coeficiente de menor grau, obtemos um polinômio mônico, não nulo, que anula α e cujo grau é menor que o de $f(x)$. Isso gera uma contradição com a minimalidade do grau de $f(x)$

Nesse contexto, temos a seguinte definição:

Definição 2.1.3. *Dizemos que*

$$\mathbb{Q}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Q}[x]\}$$

é um corpo quadrático quando $\alpha \notin \mathbb{Q}$ *e existe um polinômio de grau 2 em* $\mathbb{Q}[x]$ *que anula* α.

Observação 2.1.2. Consideremos $\mathbb{Q}[\alpha]$ corpo quadrático. Então, como α é raiz de um polinômio de grau 2, temos que α é da forma:

$$\alpha = \frac{a + b\sqrt{m}}{c} \quad \text{em que } a, b \in \mathbb{Z},\ c, z \in \mathbb{Z} \setminus \{0\} \text{ e } m \text{ é livre de quadrados.} \tag{2.1}$$

Sem perda de generalidade, podemos supor que $a, b,$ e c são primos entre si, ou seja, $mdc(a, b, c) = 1$. Da última igualdade, segue que:

$$b\sqrt{m} = c\alpha - a \Rightarrow mb^2 = (c\alpha - a)^2 \Rightarrow mb^2 = c^2\alpha^2 - 2c\alpha a + a^2$$

Assim, α é raiz do polinômio:

$$c^2x^2 - 2acx + a^2 - mb^2 \in \mathbb{Z}[x] \tag{2.2}$$

De modo geral, como $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{m}]$, tem-se que todo elemento $\beta \in \mathbb{Q}[\alpha]$ pode ser expresso como na equação (2.1), consequentemente, satisfaz uma equação de grau 2 com coeficientes em $\mathbb{Z}$.

Observação 2.1.3. Conforme visto na observação acima, temos que o corpo quadrático pode ser escrito como $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{m}]$.

Se $m < 0$, diremos que trata-se de um *corpo quadrático complexo*, visto que ele está contido em $\mathbb{C}$, porém não em $\mathbb{R}$. Enquanto, se $m > 0$, diremos que o mesmo é um *corpo quadrático real.*

Destacamos ainda que, a partir desse momento, sempre que nos referirmos ao corpo $\mathbb{Q}[\sqrt{m}]$, estaremos considerando m inteiro não nulo e livre de quadrados.

Apresentaremos, agora, alguns conceitos que nos permitirão definir um *anel quadrático*.

Definição 2.1.4. *Seja* $\mathbb{L}$ *uma extensão algébrica de* $\mathbb{K}$ *com* $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{C}$. *Dizemos que* $\mathbb{L}$ *é um corpo de números algébrico (ou simplesmente, um corpo algébrico) se* $\mathbb{L}$ *é uma extensão finita de* $\mathbb{Q}$.

Dizemos ainda que $\alpha \in \mathbb{C}$ *é um inteiro algébrico de* $\mathbb{L}$ *sobre* $\mathbb{Q}$ *se* $\alpha \in \mathbb{L}$ *e* α *é raiz de um polinômio mônico* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ *não nulo com coeficientes em* $\mathbb{Q}$. *Quando tal*

polinômio possuir coeficientes em $\mathbb{Z}$, diremos que α é um inteiro algébrico de $\mathbb{L}$ sobre $\mathbb{Z}$ (ou, simplesmente, um inteiro algébrico de $\mathbb{L}$).

Nesse contexto, o anel de inteiros algébricos do corpo $\mathbb{L}$ é definido como:

$$O_{\mathbb{L}} := \{\alpha \in \mathbb{L} : \ \alpha \text{ é inteiro algébrico de } \mathbb{L} \text{ sobre } \mathbb{Z}\}$$

Observação 2.1.4. No caso em que $\mathbb{L}$ corresponde ao próprio corpo complexo $\mathbb{C}$, dizemos apenas que $\alpha \in \mathbb{C}$ é um *inteiro algébrico*.

Neste capítulo, estudamos o conjunto $O_{\mathbb{Q}[\sqrt{m}]}$ dos inteiros algébricos de $\mathbb{Q}[\sqrt{m}]$, ou seja, os elementos $\alpha \in \mathbb{Q}[\sqrt{m}]$ para os quais existe um polinômio mônico com coeficientes em $\mathbb{Z}$ que anula α.

Exemplo 2.1.1. Consideremos $n \in \mathbb{N}$. Temos que o número complexo $e^{\frac{2\pi i}{n}}$ é um inteiro algébrico sobre $\mathbb{Z}$. De fato, utilizando a Identidade de Euler, temos que tal número anula o polinômio $f(x) = x^n - 1 \in \mathbb{Z}[x]$.

Dessa forma, $e^{\frac{2\pi i}{n}}$ é um inteiro de $\mathbb{Q}\left[e^{\frac{2\pi i}{n}}\right]$.

Notemos ainda que:

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

Assim, no caso em que $n \neq 1$, temos ainda que $e^{\frac{2\pi i}{n}}$ anula o polinômio mônico

$$p(x) = (x^{n-1} + x^{n-2} + \cdots + x + 1)$$

Considerando o caso em que $n = p$ é um primo ímpar, é comum denotar $\zeta := e^{\frac{2\pi i}{p}}$ e representar o polinômio por:

$$P_{\zeta}(x) := (x^{p-1} + x^{p-2} + \cdots + x + 1) = \prod_{i=1}^{p-1}(x - \zeta^i)$$

Pode-se provar que tal polinômio é o polinômio mônico irredutível de menor grau que anula ζ, ou seja, trata-se do polinômio mínimo de ζ. Retornaremos ao estudo destes polinômios no Capítulo 6, quando definirmos *corpos ciclotômicos.*

A partir do conceito de inteiros algébricos, temos a seguinte definição:

Definição 2.1.5. *Para cada m livre de quadrados, o anel quadrático de inteiros algébricos (ou apenas, anel quadrático) é definido como sendo o conjunto dos inteiros algébricos de $\mathbb{Q}[\sqrt{m}]$.*

Em outras palavras, o anel quadrático corresponde ao anel de inteiros algébricos de $\mathbb{Q}[\sqrt{m}]$, sendo representado por $O_{\mathbb{Q}[\sqrt{m}]}$.

Para melhor compreensão deste conceito, apresentaremos um resultado relativo aos *inteiros algébricos* no anel quadrático e uma caracterização equivalente para o mesmo.

Conforme mostrado na Observação 2.1.2, sabemos que todo elemento de $\mathbb{Q}[\sqrt{m}]$ satisfaz uma equação de grau 2 em $\mathbb{Z}[x]$. No caso em que tal elemento é *inteiro algébrico de* $\mathbb{Q}[\sqrt{m}]$, obtemos um resultado mais geral:

Proposição 2.1.1. *Seja α um inteiro algébrico de $\mathbb{Q}[\sqrt{m}]$. Então α anula um polinômio mônico de grau 2 em $\mathbb{Z}[x]$.*

Demonstração. Primeiramente, notemos que se α anula um polinômio mônico de grau 1 em $\mathbb{Z}[x]$, então α é um inteiro algébrico e, logo, α anula um polinômio mônico de grau 2.

Com efeito, por hipótese, temos que α anula um polinômio da forma $h(x) = x + c$, com $c \in \mathbb{Z}$. Assim, $c = -\alpha$; consequentemente, $p(x) = x^2 - c^2$ será um polinômio em $\mathbb{Z}[x]$ que anula α.

Desse modo, podemos considerar que α anula um polinômio $f(x)$ de grau 2 em $\mathbb{Z}[x]$ (pois trata-se de um elemento inteiro de $\mathbb{Q}[\sqrt{m}]$), mas não anula um polinômio mônico de grau 1. Temos que $f(x)$ é da forma:

$$f(x) = a_2x^2 + a_1x + a_0 \ \text{, com } a_1, a_2, a_0 \in \mathbb{Z}$$

Sem perda de generalidade, podemos supor $a_2 > 0$, pois, em caso contrário, tomamos o polinômio $\widetilde{f(x)} := -f(x)$, notando que, como $f(\alpha) = 0$ por hipótese, então $\widetilde{f(\alpha)} = 0$. Podemos supor ainda que $f(x)$ é primitivo, ou seja, $\text{mdc}(a_2, a_1, a_0) = 1$. De fato, caso tenhamos $\text{mdc}(a_2, a_1, a_0) = d$, consideramos o polinômio obtido pela divisão de $f(x)$ por d, o qual possui grau 2, tem coeficientes em $\mathbb{Z}$ e anula α.

Mostraremos que $a_2 = 1$ e, portanto, α anula um polinômio mônico em $\mathbb{Z}[x]$ de grau 2; no caso, $f(x)$.

Ora, como α é um inteiro algébrico, sabemos que é raiz de um polinômio $g(x) \in \mathbb{Z}[x]$ com grau maior ou igual a 2. Aplicando o Algoritmo da Divisão para $g(x)$ e $f(x)$, temos que existem $q(x), r(x) \in \mathbb{Q}[x]$ tais que

$$g(x) = f(x)q(x) + r(x), \text{ em que } \deg r(x) < \deg f(x) = 2 \text{ ou } r(x) = \overline{0}$$

Por outro lado, como $g(\alpha) = f(\alpha) = 0$, segue que $r(\alpha) = 0$, ou seja, α anula $r(x)$. No entanto, como, por hipótese, α não anula um polinômio de grau menor que 2, devemos ter $r(x)$ polinômio nulo. Logo, $g(x) = f(x)q(x)$.

Agora, eliminando os denominadores dos coeficientes de $q(x)$, obtemos:

$$dg(x) = f(x)q_1(x), \text{ em que } d \in \mathbb{Z} \text{ e } q_1(x) \text{ é um polinômio primitivo}$$

Denotemos $q_1(x) := b_m x^m + b_{m-1}x^{m-1} + ... + b_0 \in \mathbb{Z}[x]$.

Desse modo, no lado direito da equação temos a multiplicação de dois polinômios primitivos (ou seja, cujos coeficientes sejam relativamente primos) que, pelo Lema de Gaus resulta em um polinômio primitivo.

Por conseguinte, devemos ter $d = 1$ e, então, $g(x) = f(x)q_1(x)$.

Por fim, comparando os coeficientes de maior grau desses polinômios, obtemos $a_2 b_m = 1$, visto que $g(x)$ é mônico, e $a_2 = 1$ (visto que $a_2 \in \mathbb{N}$), conforme queríamos provar. □

Proposição 2.1.2. *Seja*

$$\Theta = \begin{cases} \dfrac{1+\sqrt{m}}{2} & \text{se } m \equiv 1 \pmod 4 \\ \sqrt{m} & \text{se } m \equiv 2,3 \pmod 4 \end{cases}$$

Afirmamos que, para cada m livre de quadrados, $\mathbb{Z}[\Theta]$ *é o anel de inteiros algébricos de* $\mathbb{Q}[\sqrt{m}]$*, ou seja,* $O_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}[\Theta]$.

Demonstração. Primeiramente, notemos que devemos provar que todo inteiro algébrico de $\mathbb{Q}[\sqrt{m}]$ pertence a $\mathbb{Z}[\Theta]$, com Θ definido como acima, e que, nas condições enunciadas, todos os elementos de $\mathbb{Z}[\Theta]$ são inteiros algébricos de $\mathbb{Q}[\sqrt{m}]$.

Para a primeira situação, consideremos α um inteiro algébrico de $\mathbb{Q}[\sqrt{m}]$ definido como:

$$\alpha = \frac{a + b\sqrt{m}}{c}$$

Sem perda de generalidade, podemos supor que $\text{mdc}(a, b, c) = 1$ e, a menos de mudança de sinal de a e b, que $c > 0$. Mostraremos que, sob tais condições, só existem dois valores possíveis para c, a saber 0 e 2.

Se $b = 0$, então $\dfrac{a}{c} \in \mathbb{Q}$.

Além disso, conforme visto na Observação 2.1.2, α é raiz do polinômio

$$c^2x^2 - 2acx + a^2 - mb^2 \in \mathbb{Z}[x]$$

e, pela proposição anterior, devemos ter $c = 1$. Desse modo, segue que $\alpha = a \in \mathbb{Z}$ e, em particular, $\alpha \in \mathbb{Z}[\Theta]$.

Por outro lado, se $b \neq 0$, então, dividindo o polinômio acima por c^2, temos que α anula o polinômio:

$$x^2 - 2\left(\frac{a}{c}\right)x + \left(\frac{a^2 - mb^2}{c^2}\right)$$

Pela unicidade do polinômio mínimo, tal polinômio deve ter coeficientes em $\mathbb{Z}$; consequentemente,

$$c \mid 2a \text{ e } c^2 \mid (a^2 - mb^2).$$

Consideremos $d := \text{mdc}(a, c)$. Em particular, temos que $d^2 \mid c^2$, donde $d^2 \mid (a^2 - mb^2)$. Agora, como pela definição de divisor comum, também sabemos que $d^2 \mid a^2$, concluímos que $d^2 \mid mb^2$. Observemos que, por hipótese, m é livre de quadrados; assim, $d^2 \mid b^2$ e, portanto, $d \mid b$. Mostramos então que $d \mid a, b, c$. Como $\text{mdc}(a, b, c) = 1$, devemos ter $d = 1$.

Dessa forma, como $c \mid 2a$ e $\text{mdc}(a, c) = 1$, segue que $c \mid 2$. Logo, só há dois valores possíveis para c: 1 e 2. Analisaremos cada um deles:

1. Caso $c = 2$, como $\text{mdc}(a, c) = 1$, temos que a é ímpar.

   Além disso, como $c^2 = 4 \mid (a^2 - mb^2)$, segue que

   $$a^2 \equiv mb^2 \equiv 1 \pmod 4,$$

   donde concluímos que b é ímpar e, portanto, $m \equiv 1 \pmod 4$.

   Neste caso, afirmamos que os inteiros algébricos de $\mathbb{Q}[\sqrt{m}]$ são os elementos de $\mathbb{Z}[\Theta]$ com $\Theta = \dfrac{1 + \sqrt{m}}{2}$.

   De fato, sabemos que a e b são ímpares, donde temos que:

   $$\alpha = \frac{a + b\sqrt{m}}{2} = \frac{a - b}{2} + \frac{b + b\sqrt{m}}{2} = \left(\frac{a - b}{2}\right) + b\left(\frac{1 + \sqrt{m}}{2}\right) \in \mathbb{Z}[\Theta]$$

   em que

   $$\Theta = \frac{1 + \sqrt{m}}{2} \text{ e } m \equiv 1 \pmod 4.$$

2. Pela contrapositiva do que foi feito no primeiro caso, temos que, se $m \not\equiv 1 \pmod 4$, ou seja, se $m \equiv 2, 3 \pmod 4$, então $c = 1$.

   Neste caso, afirmamos que os inteiros de $\mathbb{Q}[\sqrt{m}]$ são os elementos de $\mathbb{Z}[\sqrt{m}]$.

   Com efeito, α será dado por:

   $$\alpha = a + b\sqrt{m} = (a - b) + 2b\left(\frac{1 + \sqrt{m}}{2}\right) = (a - b) + 2b\Theta \in \mathbb{Z}[\sqrt{m}].$$

Portanto, todo inteiro algébrico de $\mathbb{Q}[\sqrt{m}]$ pode ser visto como um elemento de $\mathbb{Z}[\Theta]$, com Θ satisfazendo a definição enunciada.

Por outro lado, observemos que, dado um elemento $\beta \in \mathbb{Z}[\Theta]$, ele é da forma $\beta = a + b\Theta$, com $a, b \in \mathbb{Z}$ e Θ conforme as definições enunciadas. Neste caso, teremos:

$$\beta = \begin{cases} \dfrac{(2a + b) + b\sqrt{m}}{2} & \text{se } m \equiv 1 \pmod 4 \\ a + b\sqrt{m} & \text{se } m \equiv 2, 3 \pmod 4 \end{cases}$$

No primeiro caso, seguindo a construção feita na Observação 2.1.2, temos que β é raiz do polinômio:

$$4x^2 - 4(2a+b)x + (2a+b)^2 - mb^2 \in \mathbb{Z}[x] \tag{2.3}$$

Por outro lado, sabemos que $m \equiv 1 \pmod 4$, resultando em:

$$(2a+b)^2 - mb^2 \equiv (2a+b)^2 - b^2 = 4a^2 - 4ab \equiv 0 \pmod 4$$

Desse modo, dividindo o polinômio em (2.3), obtemos um polinômio de grau 2 e com coeficientes em $\mathbb{Z}$. Logo, por definição, β é inteiro algébrico de $\mathbb{Q}[\sqrt{m}]$.

Agora, consideremos o segundo caso, em que $\beta = a + b\sqrt{m}$. Novamente, aplicando a Observação 2.1.2, temos que, como $c = 1$, β é raiz do polinômio:

$$x^2 - 2ax + a^2 - mb^2 \in \mathbb{Z}[x]$$

Portanto, β é raiz de um polinômio mônico em $\mathbb{Z}[x]$ e, então, um inteiro algébrico de $\mathbb{Q}[\sqrt{m}]$. □

Observação 2.1.5. Pela caracterização feita na proposição anterior, nota-se que os elementos do anel de inteiros $\mathbb{Z}[\Theta]$ podem ser escritos de uma das seguintes formas:

1. $a + b\sqrt{m}$, com $a, b \in \mathbb{Z}$, no caso em que $m \equiv 2, 3 \pmod 4$
2. $\dfrac{a}{2} + \dfrac{b}{2}\sqrt{m}$, com $a, b \in \mathbb{Z}$ de mesma paridade, no caso em que $m \equiv 1 \pmod 4$

Vejamos alguns exemplos de anéis quadráticos:

Exemplo 2.1.2. Para o caso em que $m \equiv 2, 3 \pmod 4$, podemos tomar, por exemplo, $m = -1$. Neste caso obtemos que $\mathbb{Z}[i] := \mathbb{Z}[\sqrt{-1}]$, chamado *anel dos inteiros de Gauss*, é o anel quadrático formado pelos inteiros de $\mathbb{Q}[i]$.

Por outro lado, tomando-se $m = -3 \equiv 1 \pmod 4$, obtemos o anel de inteiros do corpo quadrático $\mathbb{Q}[\sqrt{-3}]$, representado por:

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

Este anel, denominado *anel de inteiros de Eisenstein*, será utilizado na demonstração do Último Teorema de Fermat para o caso $n = 3$.

2.2 PRINCIPAIS PROPRIEDADES

Na próxima seção, estudaremos um tipo específico de anéis quadráticos: os *anéis quadráticos euclidianos*. Para tanto, apresentaremos um novo conceito: a *norma*, o qual nos permitirá também obter novas caracterizações para elementos inversíveis e elementos primos em $\mathbb{Z}[\Theta]$. Consideremos o corpo quadrático $\mathbb{Q}[\sqrt{m}]$, com o anel quadrático a ele associado denotado por $\mathbb{Z}[\Theta]$.

Definição 2.2.1. *Seja* $\alpha = r + s\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$.

Definimos o conjugado de α *como* $\overline{\alpha} := r - s\sqrt{m}$. *Nesse contexto, definimos a norma de* α *como sendo o número:*

$$\mathcal{N}(\alpha) := \alpha\overline{\alpha} = \left(r + \sqrt{m}\right)\left(r - \sqrt{m}\right) = r^2 - ms^2$$

O conceito de norma em $\mathbb{Q}[\sqrt{m}]$ *pode ser estendido como sendo a aplicação*

$$\begin{aligned} \mathcal{N} : \mathbb{Q}[\sqrt{m}] &\rightarrow \mathbb{R} \\ \alpha &\mapsto \mathcal{N}(\alpha) = \alpha\overline{\alpha} \end{aligned}$$

A partir de tal definição, temos o seguinte resultado:

Proposição 2.2.1. *Dados* $\alpha, \beta \in \mathbb{Q}[\sqrt{m}]$ *aplicação norma satisfaz as seguintes propriedades:*

1. *A norma é uma função multiplicativa, ou seja, dados* $\alpha, \beta \in \mathbb{Q}[\sqrt{m}]$, *temos que*
$$\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta).$$
2. $\mathcal{N}(\alpha) = 0$ *se, e somente se,* $\alpha = 0$
3. *Se* $m > 0$, *ou seja, se* $\mathbb{Q}[\sqrt{m}]$ *é um corpo quadrático real, temos:*
$$\left|\mathcal{N}(a + b\sqrt{m})\right| = \left|a^2 - mb^2\right| \leq max\left\{a^2, mb^2\right\}$$

Demonstração. Sejam $\alpha, \beta \in \mathbb{Q}[\sqrt{m}]$, com $\alpha = r + s\sqrt{m}$ e $\beta = p + q\sqrt{m}$.

1. Primeiramente, notemos que $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.

   Com efeito:

$$\begin{aligned} \overline{\alpha}\overline{\beta} = \left(r - s\sqrt{m}\right)\left(p - q\sqrt{m}\right) &= (rp + sqm) - (rq + sp)\sqrt{m} \\ &= \overline{\left((rp + sqm) + (rq + sp)\sqrt{m}\right)} \\ &= \overline{\alpha\beta} \end{aligned}$$

   Consequentemente, segue que:

$$\mathcal{N}(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \mathcal{N}(\alpha)\mathcal{N}(\beta).$$

2. Temos que $\mathcal{N}(\alpha) = 0 \Leftrightarrow \alpha\overline{\alpha} = 0$. Assim, se $\alpha = 0$, é imediato que $N(\alpha) = 0$. Por outro lado, caso $\mathcal{N}(\alpha) = 0$, devemos ter $\alpha = 0$ ou $\overline{\alpha} = 0$. No segundo caso, segue que $r - s\sqrt{m} = 0$ e, como $r, s \in \mathbb{Q}$, resulta que $r = s = 0$, donde $\alpha = 0$.

3. Se $m > 0$, tem-se que $-mb^2 \leq a^2 - mb^2 \leq a^2$. Assim, $\left|\mathcal{N}(a + b\sqrt{m})\right| \leq max\{a^2, mb^2\}$.

□

Considerando a norma sobre o anel $\mathbb{Z}[\Theta]$ obtemos ainda outras propriedades:

Proposição 2.2.2. *Seja $\mathcal{N}$ a aplicação norma e $\beta \in \mathbb{Z}[\Theta]$. Então:*

1. *$\mathcal{N}(\beta) \in \mathbb{Z}$*
2. *β é inversível se, e somente se, $\mathcal{N}(\beta) = \pm 1$*
3. *Se $\mathcal{N}(\beta) = p$, com p número primo, então β é irredutível.*

Demonstração. Consideremos $\beta \in \mathbb{Z}[\Theta]$.

1. Se $\beta = r + s\sqrt{m}$, em que $m \equiv 2, 3 \pmod 4$, é direto que $\mathcal{N}(\beta) = r^2 - ms^2 \in \mathbb{Z}$. Por outro lado, se $m \equiv 1 \pmod 4$, temos que

$$\beta = \frac{(2a + b) + b\sqrt{m}}{2} \text{ , donde } \mathcal{N}(\beta) = \frac{(2a + b)^2 - mb^2}{4}$$

   Nesse caso, $\mathcal{N}(\beta) \in \mathbb{Z}$ pois

$$(2a + b)^2 - mb^2 \equiv (2a + b)^2 - b^2 \equiv 0 \pmod 4$$

2. Se β é inversível, existe $\alpha \in \mathbb{Z}[\Theta]$ tal que $\beta\alpha = 1$. Aplicando a norma nesta igualdade, temos $\mathcal{N}(\beta\alpha) = \mathcal{N}(\beta)\mathcal{N}(\alpha) = 1$. Como $\mathcal{N}(\beta) \in \mathbb{Z}$, temos que $N(\beta) = \pm 1$, como queríamos.

   Reciprocamente, se $\mathcal{N}(\beta) = \pm 1$, temos que $\beta\overline{\beta} = \pm 1$. Desse modo, se $\mathcal{N}(\beta) = 1$, então $\beta^{-1} = \overline{\beta}$; enquanto, se $\mathcal{N}(\beta) = -1$, então $\beta^{-1} = -\overline{\beta}$.

3. Como $\mathcal{N}(\beta) = p$, com p primo, temos que $\mathcal{N}(\beta) \neq 0$ e $\mathcal{N}(\beta) \neq \pm 1$, ou seja, β não pode ser nulo nem inversível. Seja $\beta = \alpha\gamma$, com $\alpha, \gamma \in \mathbb{Z}[\Theta]$. Temos:

$$p = \mathcal{N}(\beta) = \mathcal{N}(\alpha\gamma) = \mathcal{N}(\alpha)N(\gamma)$$

   Como p é primo, resulta que $\mathcal{N}(\alpha) = \pm 1$ ou $\mathcal{N}(\gamma) = \pm 1$. Por (2), concluímos que α ou γ é inversível e, portanto, β é irredutível.

□

No caso dos anéis de inteiros do corpo quadrático complexo, é possível ainda determinar o conjunto de unidades a partir da norma.

Proposição 2.2.3. *O anel de inteiros $\mathbb{Z}[\Theta]$ do corpo quadrático complexo $\mathbb{Q}[\sqrt{m}]$, com $m < 0$, possui o seguinte conjunto de unidades:*

1. *Se $m \equiv 1 \pmod 4$, temos as possibilidades:*

   i) $\mathcal{U} = \{\pm 1, \pm\Theta, \pm 1 \pm \Theta\}$, *se* $m = -3$;

   ii) $\mathcal{U} = \{\pm 1\}$, *caso contrário.*

2. *Se $m \equiv 2, 3 \pmod 4$, temos as possibilidades:*

   i) $\mathcal{U} = \{\pm 1, \pm i\}$, *se* $m = -1$;

   ii) $\mathcal{U} = \{\pm 1\}$, *caso contrário.*

Demonstração. Primeiramente, observemos que 1 é sempre uma unidade de $\mathbb{Z}[\Theta]$; mais ainda, $\mathcal{N}(1) = 1$ pela definição de norma.

Seja u é uma unidade de $\mathbb{Z}[\Theta]$. Temos que $u \mid 1$ e $1 \mid u$. Por outro lado, sabemos que a norma é uma aplicação multiplicativa e não negativa, donde segue que:

$$\mathcal{N}(u) \leq \mathcal{N}(u)\mathcal{N}(u^{-1}) = \mathcal{N}(uu^{-1}) = \mathcal{N}(1) = 1$$

Como $\mathcal{N}(u) \in \mathbb{N}$, tem-se que $\mathcal{N}(u) = 1$.

Consideremos $u := a + b\Theta$ com $a, b \in \mathbb{Z}$ e, para efeito de notação, façamos $D := -m$, a fim de que tenhamos $D > 0$.

Vejamos cada um dos casos:

1. Caso $m \equiv 1 \pmod 4$, temos que $-D \equiv 1 \pmod 4 \therefore D \equiv -1 \pmod 4$.

   Além disso, como $m \equiv 1 \pmod 4$, temos que $\Theta = \dfrac{1 + \sqrt{-D}}{2}$ e, assim:

   $$u = \left(a + \frac{b}{2}\right) + \frac{b\sqrt{-D}}{2}$$

   Desse modo,

   $$\begin{aligned} 1 = \mathcal{N}(u) &= \left(a + \frac{b}{2}\right)^2 + \frac{b^2 D}{4} \\ &= a^2 + ab + b^2\left(\frac{1}{4} + \frac{D}{4}\right) \end{aligned}$$

   Agora, como $D \equiv -1 \pmod 4$, podemos escrever $D = 4k - 1$ com $k \geq 1$, pois $D > 0$. Então:

   $$1 = a^2 + ab + b^2 k$$

i) Se $m = -3$, então $D = 3$ e, consequentemente, $k = 1$. Nessas condições, temos:

$$1 = a^2 + ab + b^2$$

Dessa forma, há dois casos a serem analisados: se $ab \geq 0$ e se $ab \leq 0$.

Caso $ab \geq 0$, temos a soma de três parcelas inteiras não negativas resultando em 1. Assim, as únicas possibilidades são:

$$a^2 = 1 \text{ e } b^2 = 0 \quad \text{ou} \quad a^2 = 0 \text{ e } b^2 = 1$$

Neste caso, temos então que $u = \pm 1$ ou $u = \pm\Theta$.

Por outro lado, caso $ab \leq 0$, podemos reescrever a equação $1 = a^2 = ab + b^2$ como:

$$1 = (a + b)^2 + (-ab)$$

Como trata-se da soma de duas parcelas inteiras resultando em 1, as únicas soluções possíveis são:

$$(a + b)^2 = 1 \text{ e } ab = 0 \quad \text{ou} \quad (a + b)^2 = 0 \text{ e } ab = -1$$

No primeiro caso, temos: $a = 0$ e $b = \pm 1$ ou $b = 0$ e $a = \pm 1$. Enquanto no segundo, devemos ter $a = \pm 1$ e $b = \pm 1$.

Assim, se $ab \leq 0$, temos as seguintes possibilidades $u = \pm\Theta, \pm 1$ ou $\pm 1 \pm \Theta$.

Portanto, de modo geral, quando $m = -3$, temos

$$\mathcal{U} = \{\pm 1, \pm\Theta, \pm 1 \pm \Theta\} \text{ em que } \Theta = \frac{1 + \sqrt{-3}}{2}.$$

ii) Se $m < -3$, temos $D > 3$, ou seja, $k > 1$. Assim, analisando a equação obtida:

$$1 = a^2 + ab + b^2k,$$

nota-se que, caso $b^2 > 0$, teríamos $b^2k > 1$, gerando uma contradição.

Então, devemos ter $b^2 = 0$ e, então, $a^2 = 1$.

Portanto, $u = \pm 1$, ou seja, $\mathcal{U} = \{\pm 1\}$.

2. Se $m \not\equiv 1 \pmod 4$, ou seja, $m \equiv 2, 3 \pmod 4$ temos que $\Theta = \sqrt{-D}$ e, então:

$$u = a + b\sqrt{-D}$$

Desse modo,

$$1 = \mathcal{N}(u) = a^2 + b^2D$$

i) Se $m = -1$, ou seja, $D = 1$, temos:

$$a^2 + b^2 = 1$$

Como $a, b \in \mathbb{Z}$, as únicas soluções são:

$$a^2 = 1 \text{ e } b^2 = 0 \quad \text{ou} \quad a^2 = 0 \text{ e } b^2 = 1$$

Logo, $u = \pm 1$ ou $u = \pm i$; portanto, $\mathcal{U} = \{\pm 1, \pm i\}$.

ii) Se $m < -1$, temos que $D > 1$ e analisando a equação anteriormente obtida:

$$1 = \mathcal{N}(u) = a^2 + b^2 D$$

verificamos, novamente, que, caso $b^2 > 0$, teríamos $Db^2 > 1$, uma contradição. Assim, devemos ter $b^2 = 0$ e, consequentemente $a^2 = 1$.
Portanto, $u = \pm 1$, donde segue que $\mathcal{U} = \{\pm 1\}$.

□

Observação 2.2.1. Para o caso em que $\mathbb{Q}[\sqrt{m}]$ é um corpo quadrático real, ou seja, $m \in \mathbb{N}$, avaliar quais são as unidades do anel $\mathbb{Z}[\Theta]$ a partir da norma torna-se um pouco mais complicado, essencialmente no segundo caso. Com efeito, dado $u = a + b\Theta$ unidade de $Z[\Theta]$, se $m \equiv 2, 3 \pmod 4$, deveremos analisar sob quais valores de $a, b \in \mathbb{Z}$, temos:

$$\mathcal{N}(a + b\Theta) = a^2 - b^2 m$$

No entanto, como a equação acima consiste da diferença de dois termos positivos, avaliar suas possíveis soluções, com $m \in \mathbb{N}$ em um intervalo fixado, é mais difícil.

Neste caso, o cálculo das unidades para qualquer anel $\mathbb{Z}[\Theta]$ de um corpo quadrático real envolve outras ferramentas, como, por exemplo, o estudo de *unidades fundamentais*.

Contudo, como o estudo das unidades destes tipos de anéis não será utilizado ao longo de nosso trabalho, ao contrário dos anéis dos corpos complexos, não iremos apresentá-lo. O mesmo pode ser encontrado em Stewart [18] (Teorema 3.3, p. 34).

2.3 ANÉIS QUADRÁTICOS EUCLIDIANOS

A fim de definirmos *anéis quadráticos euclidianos*, necessitaremos, primeiramente, do conceito de *anel euclidiano*, o qual é semelhante ao conceito de Domínio Euclidiano.

Definição 2.3.1. *Dizemos que um anel A é um anel euclidiano se existir uma aplicação*

$$d : A \setminus \{0\} \to \mathbb{N}$$

tal que

i) $d(\alpha\beta) \geq d(\alpha)$, *para todo* $\alpha, \beta \in A \setminus \{0\}$;

ii) *Existe um algoritmo da divisão em* A, *ou seja, dados* $\alpha, \beta \in A$, *com* $\beta \neq 0$ *existem* $\gamma, \rho \in A$ *tais que* $\alpha = \gamma\beta + \rho$, *com* $\rho = 0$ *ou* $d(\rho) < d(\beta)$.

Nesse contexto:

Definição 2.3.2. *Dizemos que um anel quadrático é euclidiano se ele é um anel quadrático para o qual existe uma aplicação, chamada aplicação euclidiana, satisfazendo as propriedades i e ii da definição anterior.*

Nos anéis quadráticos complexos que estudaremos, utilizaremos d como sendo a aplicação norma definida na seção anterior (chamada *norma usual*). Já no caso dos anéis quadráticos reais, a fim de que a norma fique sempre positiva, usaremos:

$$N\left(a + b\sqrt{m}\right) := \left|a^2 - mb^2\right| \tag{2.4}$$

Observamos que, como a norma é uma função multiplicativa, a condição (*i*) é sempre satisfeita. No entanto, como será mostrado na próxima seção, a segunda condição nem sempre é válida.

Além disso, como as definições acima estendem a noção de divisibilidade em $\mathbb{Z}$ (em que consideramos a aplicação *módulo*), podemos nos referir aos elementos γ e ρ como sendo um quociente e um resto da divisão de α por β. Cabe ressaltar que tais definições não exigem que γ e ρ sejam únicos. Em geral, é possível encontrar pares distintos de quociente e resto em uma mesma divisão.

Exemplo 2.3.1. Consideremos, por exemplo, $\alpha, \beta \in \mathbb{Z}[i]$, com $\alpha = 3 + 2i$ e $\beta = -1 + 3i$. Temos que:

(i) $3 + 2i = (-1 + 3i)(-i) + i$, em que $1 = N(i) < N(3 + 2i) = 13$;

(ii) $3 + 2i = (-1 + 3i)(1 - i) + (1 + 2i)$, em que $5 = N(1 + 2i) < N(3 + 2i) = 13$.

Assim, na divisão de $3 + 2i$ por $(-1 + 3i)$ podemos obter quociente $-i$ e resto i ou quociente $1 - i$ e resto $1 + 2i$, sendo que ambos satisfazem ao algoritmo da divisão.

Vejamos agora alguns exemplos de anéis euclidianos reais e complexos. Para o caso real, utilizaremos a definição de norma expressa na equação (2.4).

Teorema 2.3.1. *Existe um algoritmo da divisão em* $\mathbb{Z}[\Theta]$, *anel de inteiros de* $\mathbb{Q}[\sqrt{m}]$, *quando* $m = 2, 3, 5, 7$.

Demonstração. Dados $\alpha, \beta \in \mathbb{Z}[\Theta]$, se $\beta \mid \alpha$, então existe $\sigma \in \mathbb{Z}[\Theta]$ tal que $\alpha = \beta\sigma$ e, logo o resultado segue, visto que $0 \in \mathbb{Z}[\Theta]$.

Assim, só precisaremos considerar o caso em que $\beta \nmid \alpha$. E, neste caso, queremos obter $\gamma, \rho \in \mathbb{Z}[\Theta]$ tais que $\alpha = \beta\gamma + \rho$ com $\mathcal{N}(\rho) < \mathcal{N}(\beta)$. No entanto, notemos que:

$$\mathcal{N}(\rho) = N(\alpha - \beta\gamma) = \mathcal{N}\left(\left(\frac{\alpha}{\beta} - \gamma\right)\beta\right) = \mathcal{N}\left(\frac{\alpha}{\beta} - \gamma\right)\mathcal{N}(\beta)$$

Desse modo, basta mostrarmos que existe $\gamma \in \mathbb{Z}[\Theta]$ satisfazendo:

$$\mathcal{N}\left(\frac{\alpha}{\beta} - \gamma\right) < 1$$

Além disso, lembremos que, pela Proposição 2.2.1 (item 3), dado $\left(a + b\sqrt{m}\right)$ em $\mathbb{Q}[\sqrt{m}]$ tem-se:

$$\mathcal{N}\left(a + b\sqrt{m}\right) := \left|a^2 - mb^2\right| \leq max\left\{a^2, mb^2\right\}$$

Como $\mathbb{Q}[\sqrt{m}]$ é corpo, podemos escrever $\dfrac{\alpha}{\beta} = a + b\sqrt{m}$, com $a, b \in \mathbb{Q}$. Agora, temos dois casos a analisar.

Caso $m \equiv 2, 3 \pmod 4$, ou seja, quando $m = 2, 3$, escolhemos $x, y \in \mathbb{Z}$ tais que

$$|a - x| \leq \frac{1}{2} \quad \text{e} \quad |b - y| \leq \frac{1}{2}$$

Dessa forma, tomando $\gamma = x + y\sqrt{m}$ segue:

$$\begin{aligned} \mathcal{N}\left(\frac{\alpha}{\beta} - \gamma\right) &= \mathcal{N}\left(a - x + (b - y)\sqrt{m}\right) \\ &= \left|(a - x)^2 - m(b - y)^2\right| \\ &\leq max\left\{\frac{1}{4}, \frac{m}{4}\right\} < 1 \end{aligned}$$

Caso $m \equiv 1 \pmod 4$, ou seja, quando $m = 5, 13$, escolhemos $y = \dfrac{v}{2}$ e $x = \dfrac{u}{2}$, com $u, v \in \mathbb{Z}$ e $u \equiv v \pmod 2$, tais que:

$$|a - x| \leq \frac{1}{2} \quad \text{e} \quad |b - y| \leq \frac{1}{4}$$

Tomamos $\gamma = x + y\sqrt{m}$

Notemos que neste momento, conforme ressaltado na Observação 2.1.5, como $m \equiv 1 \pmod 4$, a exigência de que u e v possuam a mesma paridade é fundamental para que $\gamma \in Z[\Theta]$.

Nessas condições, segue que:

$$\begin{aligned}\mathcal{N}\left(\frac{\alpha}{\beta}-\gamma\right) &= \mathcal{N}\left(a-x+(b-y)\sqrt{m}\right)\\ &= \left|(a-x)^2-m(b-y)^2\right|\\ &\leq max\left\{\frac{1}{4},\frac{m}{16}\right\}<1\end{aligned}$$

Logo, em ambos os casos, obtivemos $\gamma \in Z[\Theta]$ tal que $\alpha = \beta\gamma+\rho$ com $\mathcal{N}(\rho) < \mathcal{N}(\beta)$ e, portanto, segue o resultado. □

Observemos que na demonstração do teorema acima, utiilizamos fortemente os valores de m a fim de obter uma limitação para a norma de ρ. Nesse contexto, torna-se relativamente complicado generalizar o resultado para outros valores de m utilizando exatamente a mesma argumentação.

É possível provar que para $m = 6, 17, 21, 29$ também existe um algoritmo da divisão em $\mathbb{Z}[\Theta]$. Uma demonstração desse fato pode ser encontrada em Andrade [2] (Teorema 1.3, p. 10).

Para o caso complexo, temos o seguinte resultado:

Teorema 2.3.2. *Se $m < 0$, existe um algoritmo da divisão em $\mathbb{Z}[\Theta]$, anel de inteiros de $\mathbb{Q}[\sqrt{m}]$, quando $m = -1, -2, -3, -7$ e -11.*

Demonstração. De modo análogo à demonstração do Teorema 2.3.1, dados $\alpha, \beta \in \mathbb{Z}[\Theta]$ tal que $\beta \nmid \alpha$, existe $\gamma \in \mathbb{Z}[\Theta]$ tal que:

$$\mathcal{N}\left(\frac{\alpha}{\beta}-\gamma\right)<1$$

Consideremos $\dfrac{\alpha}{\beta} = a + b\sqrt{m}$.

Caso $m \equiv 2, 3 \pmod 4$, ou seja, quando $m = -1, -2$, tomamos $x, y \in \mathbb{Z}$ satisfazendo:

$$|a-x| \leq \frac{1}{2} \quad \text{e} \quad |b-y| \leq \frac{1}{2}$$

Então, tomando $\gamma = x + y\sqrt{m}$, segue:

$$\begin{aligned}\mathcal{N}\left(\frac{\alpha}{\beta}-\gamma\right) &= \mathcal{N}\left(a-x+(b-y)\sqrt{m}\right)\\ &= (a-x)^2-m(b-y)^2\\ &\leq \frac{1}{4}+|m|\left(\frac{1}{4}\right)<1\end{aligned}$$

Caso $m \equiv 1 \pmod 4$, ou seja, quando $m = -3, -7, -11$, tomamos $y = \frac{v}{2}$ e $x = \frac{u}{2}$, com $u, v \in \mathbb{Z}$ e $u \equiv v \pmod 2$, satisfazendo:

$$|a - x| \leq \frac{1}{2} \quad \text{e} \quad |b - y| \leq \frac{1}{4}$$

Assim, tomando $\gamma = x + y\sqrt{m}$, temos:

$$\begin{aligned} \mathcal{N}\left(\frac{\alpha}{\beta} - \gamma\right) &= \mathcal{N}\left(a - x + (b - y)\sqrt{m}\right) \\ &= (a - x)^2 - m(b - y)^2 \\ &\leq \frac{1}{4} + |m|\left(\frac{1}{16}\right) < 1 \end{aligned}$$

□

Pode-se demonstrar que os valores de m listados no teorema anterior são os únicos valores negativos de m para os quais $\mathbb{Q}[\sqrt{m}]$ é um corpo quadrático complexo euclidiano. A demonstração da unicidade pode ser encontrada em Hardy [9] (Teorema 246, p. 275).

As demonstrações apresentadas nos fornecem um algoritmo para o cálculo de um quociente e um resto em uma divisão em $\mathbb{Z}[\Theta]$. Apresentamos a seguir um exemplo que ilustra o funcionamento deste algoritmo:

Exemplo 2.3.2. Consideremos o anel $\mathbb{Z}\left[\frac{1 + \sqrt{-7}}{2}\right]$.

Sejam $\alpha = 19 + 10\sqrt{-7}$ *e* $\beta = 6$.

Vamos obter $\gamma = x + y\sqrt{-7}$ e $\rho = s + t\sqrt{-7}$ no anel de inteiros acima tais que $\alpha = \beta\gamma + \rho$ com $\mathcal{N}(\rho) < \mathcal{N}(\beta)$.

Notemos que:

$$\frac{\alpha}{\beta} := a + b\sqrt{-7} = \frac{19}{6} + \frac{10}{6}\sqrt{-7}$$

ou seja,

$$a = \frac{19}{6} \quad \text{e} \quad b = \frac{10}{6} = \frac{5}{3}$$

Inicialmente, tomemos $y = \frac{v}{2}$, com $v \in \mathbb{Z}$, tal que $|b - y| \leq \frac{1}{4}$.

Seja, por exemplo, $v = 3$:

$$|b - y| = \left|\frac{5}{3} - \frac{3}{2}\right| = \frac{1}{6} \leq \frac{1}{4}$$

Como v é um número ímpar, devemos tomar agora $x = \frac{u}{2}$, com $u \in \mathbb{Z}$ número ímpar e tal que $|a - x| \leq \frac{1}{2}$.

Consideremos $u = 7$:

$$|a - x| = \left|\frac{19}{6} - \frac{7}{2}\right| = \frac{1}{3} \leq \frac{1}{2}$$

Logo, temos que $\gamma = x + y\sqrt{-7} = \frac{7}{2} + \frac{3}{2}\sqrt{-7}$ é um quociente para tal divisão.

Consequentemente, o resto associado será:

$$\rho = \alpha - \beta\gamma = \left(19 + 10\sqrt{-7}\right) - 6\left(\frac{7}{2} + \frac{3}{2}\sqrt{-7}\right) = -2 + \sqrt{-7}$$

e, de fato:

$$\mathcal{N}(\rho) = \mathcal{N}\left(-2 + \sqrt{-7}\right) = 4 + 7 = 11 < 36 = N(6) = \mathcal{N}(\beta).$$

Por outro lado, conforme já afirmado, a norma de um anel de inteiros, ainda que tomada como o módulo da norma usual, pode não satisfazer o algoritmo da divisão. Como exemplo, temos o anel $\mathbb{Z}[\sqrt{23}]$.

Exemplo 2.3.3. O anel $\mathbb{Z}[\sqrt{23}]$ não é um anel euclidiano com a norma $\mathcal{N}$, definida como $\mathcal{N}\left(a + b\sqrt{m}\right) := \left|a^2 - mb^2\right|$.

Suponhamos que $\mathbb{Z}[\sqrt{23}]$ seja um anel euclidiano com a norma $\mathcal{N}$.

Dados $\alpha = 7$ e $\beta = \sqrt{23}$, devemos obter $\gamma, \rho \in \mathbb{Z}[\sqrt{23}]$ tais que $\alpha = \beta\gamma + \rho$ com $\left|\mathcal{N}(\rho)\right| < \left|\mathcal{N}(\sqrt{23})\right|$. Ou, equivalentemente, devemos encontrar $\gamma = x + y\sqrt{23}$ tal que:

$$\left|\mathcal{N}\left(\frac{\alpha}{\beta} - \gamma\right)\right| = \left|\mathcal{N}\left(\gamma - \frac{\alpha}{\beta}\right)\right| < 1$$

Como $\frac{\alpha}{\beta} = \frac{7}{23}\sqrt{23}$ devemos obter $x, y \in \mathbb{Z}$ tais que:

$$\left|\mathcal{N}\left(x - \left(\frac{7}{23} - y\right)\sqrt{23}\right)\right| < 1$$

Ou seja,

$$\left|x^2 - \left(\frac{7}{23} - y\right)^2\right| < 1 \quad \therefore \quad \left|23x^2 - (7 - 23y)^2\right| < 23$$

Seja

$$t := 23x^2 - (7 - 23y)^2 = 23x^2 - z^2, \text{ em que } z = 23 - y$$

Assim, $t \equiv -49 \equiv -3 \pmod{23}$.

Agora, como $|t| < 23$, devemos ter $t = -3$ ou $t = 20$.

Caso $t = -3$, temos que $23x^2 - z^2 = -3$. Observemos que x e z não podem ser divisíveis por 3, pois, caso contrário, teríamos as seguintes possibilidades:

$$23x^2 - z^2 \equiv 0, -1 \text{ ou } 23 \pmod{9}$$

Sendo a primeira para o caso em que ambos são divisíveis por 3, a segunda para o caso em que somente x é dividível por 3 e a última, se 3 divide apenas z. No entanto, todas essas possibilidades contradizem o fato de $23x^2 - z^2 \equiv -3 \pmod 3$.

Dessa forma, temos que $x^2 \equiv z^2 \equiv 1 \pmod 3$ e, então, segue que:

$$t = 23x^2 - z^2 \equiv 23 - 1 \equiv 1 \pmod 3,$$

contradizendo o fato de que $t = -3$.

Por outro lado, caso tenhamos $t = 20$, temos $23x^2 - z^2 = 20$ e, de modo semelhante ao feito acima, não podemos ter x ou z divisíveis por 5. Assim, temos $x^2 \equiv z^2 \pmod 5$ e, consequentemente:

$$t = 23x^2 - z^2 \equiv 3 - 1 \equiv 0 \pmod 5,$$

uma contradição com o fato de t ser igual a 20.

Logo, não foi possível obter $\gamma, \rho \in \mathbb{Z}[\sqrt{23}]$ tais que $\alpha = \beta\gamma + \rho$ satisfazendo $\left|\mathcal{N}(\rho)\right| < \left|\mathcal{N}(\sqrt{23})\right| = 23$.

Concluímos, portanto, que $\mathbb{Z}[\sqrt{23}]$ não é um anel euclidiano com a norma $\mathcal{N}$.

Apesar de $\mathbb{Z}[\sqrt{23}]$ não ser de fato um anel euclidiano, em princípio, a argumentação utilizada no exemplo acima não poderia ser utilizado como prova, uma vez que poderia existir outra aplicação para o qual o algoritmo da divisão fosse válido.

Nessas circunstâncias, surge o questionamento: como provar que determinados anéis não são euclidianos em geral, ou seja, não é possível definir uma aplicação satisfazendo o algoritmo da divisão?

As demonstrações deste fato diferem conforme os valores de m em $\mathbb{Q}[\sqrt{m}]$ são alterados. Na próxima seção, apresentaremos a prova para o caso $m = -19$. Uma demonstração mais geral, envolvendo os caso em que $m = -19, -43, -67$ e -163 pode ser encontrada em Peric [12] (Teorema 3.4, p. 151).

2.4 ALGUNS EXEMPLOS

Conforme apresentado no primeiro capítulo, todo Domínio Euclidiano é um Domínio de Ideais Principais (DIP), o qual é, necessariamente, um Domínio de Fatoração Única (DFU). No entanto, a recíproca não é válida em geral.

Os exemplos de Domínios de Fatoração Única que não são Domínios de Ideais Principais são relativamente simples. De fato, os aneis de polinômios $\mathbb{Z}[x_1, ..., x_n]$ e $\mathbb{K}[x_1, ..., x_n]$, em que $\mathbb{K}$ é um corpo e $n \geq 1$, são domínios de fatoração única. Contudo, para $n \geq 1$ em $\mathbb{Z}[x_1, ..., x_n]$ e para $n \geq 2$ em $\mathbb{K}[x_1, ..., x_n]$, tais anéis não são domínios de ideais principais.

Os exemplos de Domínios de Ideais Principais que não são Euclidianos, por outro lado, envolvem, por vezes, demonstrações mais trabalhosas. Nesta seção, mostraremos que o anel $\mathbb{Z}[\Theta]$ de inteiros algébricos sobre o corpo quadrático dos complexos $\mathbb{Q}[\sqrt{m}]$ quando $m = -19$ é um domínio de ideais principais, porém, não é um domínio euclidiano.

Para efeito de notação, a partir desse momento, consideraremos:

$$\theta := \frac{1 + \sqrt{-19}}{2}$$

Primeiramente, provaremos que o anel $\mathbb{Z}[\theta]$ não é um anel euclidiano. Para tanto utilizaremos o seguinte lema:

Lema 2.4.1. *Os elementos $\theta, \theta - 1, \theta + 1, 2$ e 3 são elementos irredutíveis em $\mathbb{Z}[\theta]$.*

Demonstração. Utilizando a definição de norma, em que $N(\alpha) = \alpha\overline{\alpha}$, temos que:

$$\mathcal{N}(\theta) = \mathcal{N}(\theta - 1) = 5 \text{ e } \mathcal{N}(\theta + 1) = 7.$$

E, como 5 e 7 são primos, pela Proposição 2.2.2 (item 3) segue que $\theta, \theta - 1$ e $\theta + 1$ são elementos irredutíveis.

Para o caso de 2 e 3, notemos que $\mathcal{N}(2) = 2$ e $\mathcal{N}(3) = 9$. Utilizando a mesma proposição citada acima, basta mostrarmos que não existem elementos em $\mathbb{Z}[\theta]$ com norma 2 ou 3.

Seja n igual a um dos valores 2 ou 3 e suponhamos que exista $(a + b\theta) \in \mathbb{Z}[\theta]$ tal que $\mathcal{N}(a + b\theta) = n$. Observemos que:

$$\begin{aligned} \mathcal{N}(a + b\theta) = (a + b\theta)(a - b\theta) &= a^2 + ab + 5b^2 \\ &= (a + b)^2 - ab + 4b^2 \end{aligned}$$

Caso $ab \geq 0$, utilizando a primeira igualdade temos que $n = a^2 + ab + 5b^2$. Como $n \leq 3$, deve-se ter necessariamente $b = 0$, donde segue que $a = \pm\sqrt{n}$. Agora, caso $ab < 0$, pela segunda igualdade, temos que $n = (a + b)^2 - ab + 4b^2$. Novamente, como $n \geq 3$, devemos ter $b = 0$ e, consequentemente, $a = \pm\sqrt{n}$. Entretanto, como $n = 2$ ou $n = 3$, temos que $\sqrt{n} \notin \mathbb{Z}$, contradizendo o fato de que $(a + b\theta) \in \mathbb{Z}[\theta]$.

Portanto, temos que 2 e 3 são de fato irredutíveis em $\mathbb{Z}[\theta]$, como queríamos provar. □

Teorema 2.4.1. *O anel de inteiros $\mathbb{Z}[\theta]$ não é um anel euclidiano.*

Demonstração. Suponhamos, por absurdo, que $\mathbb{Z}[\theta]$ seja um anel euclidiano com a função $d : \mathbb{Z}[\Theta] \setminus \{0\} \to \mathbb{N}$.

Consideremos o conjunto $M := \mathbb{Z}[\theta] - \mathcal{U} \cup \{1, -1\}$, em que $\mathcal{U}$ é o conjunto das unidades de $\mathbb{Z}[\theta]$. Notemos que $m = -19 \equiv 1 \pmod 4$ e, assim, pela Proposição 2.2.3, $\mathcal{U} = \{\pm 1\}$, ou seja, os únicos elementos inversíveis de $\mathbb{Z}[\theta]$ são 1 e -1.

Seja $\alpha \in M$ tal que $d(\alpha)$ seja mínimo em $d(M)$. Observemos que tal escolha de α é possível visto que $d(M)$ é um subconjunto não vazio dos naturais.

Pelo algoritmo da divisão, existem $\gamma, \rho \in \mathbb{Z}[\theta]$ tais que

$$2 = \gamma\alpha + \rho \text{ , em que } \rho = 0 \text{ ou } d(\rho) < d(\alpha).$$

Além disso, pela escolha de m, a princípio, os únicos valores possíveis para ρ são $-1, 0$ ou 1. No entanto, notemos que caso tivéssemos $\rho = 1$, então $1 = \gamma\alpha$, donde α seria inversível, uma contradição. Desse modo, segue que $\gamma\alpha = 2$ (se $\rho = 0$) ou $\gamma\alpha = 3$ (se $\rho = -1$). Assim, $\alpha \mid 2$ ou $\alpha \mid 3$. Agora, como pelo lema anterior 2 e 3 são elementos irredutíveis, os valores possíveis para α se restringem a ± 2 ou ± 3.

Aplicando novamente o algoritmo da divisão, existem $\beta, \tau \in \mathbb{Z}[\theta]$ tais que

$$\theta = \beta\alpha + \tau \text{ , em que } \tau = 0 \text{ ou } d(\tau) < d(\alpha).$$

Pela escolha de m, os únicos valores de τ são $-1, 0$ ou 1. Dessa forma:

$$\beta\alpha = \theta + 1 \text{ , } \beta\alpha = \theta \text{ ou } \beta\alpha = \theta - 1$$

Consideremos ϵ um dos valores $\theta + 1, \theta,$ ou $\theta - 1$. Então, temos $\epsilon = \beta\alpha$.

Como $\theta + 1, \theta,$ e $\theta - 1$ são irredutíveis, temos que ϵ também o é. Logo, β ou α é inversível.

Como m é irredutível (visto que os valores possíveis para m são ± 2 e ± 3), concluímos que m não pode ser inversível. Consequentemente, β o é. Pela caracterização de elemento inversível via norma, devemos ter então

$$N(\beta) = 1 \text{ , resultando que } N(\epsilon) = N(\beta)N(\alpha) = N(\alpha)$$

Mas, conforme visto no lema anterior, $N(\epsilon) = 5$ ou $N(\epsilon) = 7$ enquanto $N(\alpha) = 4$ ou $N(\alpha) = 9$, gerando uma contradição.

Portanto, concluímos a demonstração de que $\mathbb{Z}[\theta]$ não é euclidiano. □

Para a demonstração de que $\mathbb{Z}[\theta]$ é um DIP, necessitaremos de um novo conceito: o de *anel quasi euclidiano*.

Definição 2.4.1. *Dizemos que um anel A é um anel quasi euclidiano se existir uma aplicação*

$$m : A \setminus \{0\} \to \mathbb{N}$$

tal que

i) $m(\alpha\beta) \geq m(\alpha)$, *para todo* $\alpha, \beta \in A \setminus \{0\}$;

ii) *Para todos* $\alpha, \beta \in A \setminus \{0\}$ *tais que* $m(\alpha) \geq m(\beta)$, *temos que* $\beta \mid \alpha$ *ou existem* $\gamma, \delta \in A$ *tais que*

$$0 < m(\alpha\delta - \beta\gamma) < m(\beta).$$

Observação 2.4.1. Tal aplicação pode ser estendida a um domínio $\mathbb{D}$ com unidade. Nesse caso, se a aplicação satisfaz as condições *i* e *ii*, dizemos que $\mathbb{D}$ é um *domínio quasi-euclidiano* e que a aplicação m é uma *norma de Dedekind- Hassen.*

Esta definição nos fornece um importante resultado. Apesar de anéis euclidianos não serem em geral anéis principais, temos que:

Teorema 2.4.2. *Todo anel quasi euclidiano é um anel principal.*

Demonstração. Seja A um anel quasi euclidiano e seja I um ideal não nulo de A.

Escolhemos $\beta \in I \setminus \{0\}$ tal que $m(\beta)$ assuma valor mínimo entre todos os elementos não nulos de I (novamente, tal escolha é possível visto que o contradomínio de m é $\mathbb{N}$). Assim, dado $\gamma \in I \setminus \{0\}$, temos que $m(\gamma) \geq m(\beta)$. Afirmamos que β gera o ideal I, ou seja, $I = \langle\beta\rangle$.

Como $\beta \in I$, é imediato que $\langle\beta\rangle \subset I$. Agora, seja $\alpha \in I$ e suponha, por absurdo, que $\alpha \notin \langle\beta\rangle$. Pela escolha de β e como $\alpha \in I$, segue que $m(\alpha) \geq m(\beta)$. Por outro lado, como $\alpha \notin \langle\beta\rangle$, então $\beta \nmid \alpha$. Como A é quasi euclidiano, existem $\gamma, \delta \in A$ tais que

$$0 < m(\alpha\delta - \beta\gamma) < m(\beta).$$

No entanto, $(\alpha\delta - \beta\gamma) \in I$, pois I é ideal, e $(\alpha\delta - \beta\gamma) \neq 0$ pela definição da aplicação m. Tal fato contradiz a minimalidade de $m(\beta)$. Assim, devemos ter $I \subset \langle\beta\rangle$.

Logo, segue que $I = \langle\beta\rangle$ e, como I foi tomado como um ideal não nulo arbitrário, concluímos que A é um anel principal. □

Observemos que, por meio do teorema anterior, concluímos ainda que todo domínio quasi euclidiano é um domínio de ideais principais. Nesse contexto, cabe ressaltar que a recíproca do teorema também é válida. Assim, obtemos uma nova caracterização para domínios de ideais principais e para domínios quasi euclidianos:

Teorema 2.4.3. *Um domínio* $\mathbb{D}$ *é quasi euclidiano se, e somente se,* $\mathbb{D}$ *é um domínio de ideais principais.*

Demonstração. Pelo teorema anterior, só precisamos provar que todo DIP é um domínio quasi euclidiano.

Com efeito, para qualquer domínio de ideais principais, podemos definir a aplicação $\phi : \mathbb{D} \longrightarrow \mathbb{N}$ dada por:

$$\phi(\alpha) = \begin{cases} 0 & \text{se } \alpha = 0 \\ 2^{n_1+\ldots+n_i} & \text{se } \alpha = p_1^{n_1}\ldots p_i^{n_i} \text{ e } \alpha \neq 0 \end{cases}$$

em que $p_1^{n_1}\ldots p_i^{n_i}$ é a fatoração de α em fatores primos. Notemos que tal escrita é possível visto que todo DIP é, em particular, um DFU.

A primeira condição (i) é imediatamente satisfeita. Verificaremos a segunda condição.

Sejam $\alpha, \beta \in A \setminus \{0\}$ tais que $\phi(\alpha) \geq \phi(\beta)$. Se $\beta \nmid \alpha$, não há nada a ser feito. Consideremos então que $\beta \nmid \alpha$.

Assim, temos que existem $\delta, \gamma \in \mathbb{D}$ tais que $\text{mdc}(\alpha, \beta) = \alpha\delta - \beta\gamma$. Observemos primeiramente que $\phi(\alpha\delta - \beta\gamma) > 0$, uma vez que $\beta \neq 0$, resultando que $\alpha\delta - \beta\gamma \neq 0$. Por outro lado, pela condição de ser mdc, temos que $(\alpha\delta - \beta\gamma) \mid \beta$. Então, pela definição da aplicação ϕ, segue que $\phi(\alpha\delta - \beta\gamma) < \phi(\beta)$.

De fato, a última desigualdade é estrita, visto que se tivéssemos $\phi(\alpha\delta - \beta\gamma) = \phi(\beta)$, teríamos que $\beta \mid (\alpha\delta - \beta\gamma)$ e, consequentemente, $\beta \mid \alpha$, contrariando a hipótese inicial.

Portanto, segue que

$$0 < \phi(\alpha\delta - \beta\gamma) < \phi(\beta).$$

□

Para o caso do anel $\mathbb{Z}[\theta]$ que estamos analisando, temos, por fim, o seguinte teorema:

Teorema 2.4.4. *O anel $\mathbb{Z}[\theta]$ de inteiros algébricos do corpo quadrático $\mathbb{Q}[\sqrt{-19}]$ é um anel principal.*

Demonstração. Pelo Teorema 2.4.2, basta provarmos que $\mathbb{Z}[\theta]$ é um anel quasi euclidiano.

Consideremos a norma usual do anel $\mathbb{Z}[\theta]$ dada por

$$\begin{aligned} \mathcal{N} : \mathbb{Z}[\theta] &\to \mathbb{R} \\ \alpha &\mapsto \mathcal{N}(\alpha) = \alpha\overline{\alpha} \end{aligned}$$

Sabemos que $\mathcal{N}$ é uma aplicação multiplicativa e não negativa, ou seja, $\mathcal{N}$ satisfaz a propriedade (i) da Definição 2.4.1. Provaremos que $\mathcal{N}$ satisfaz também a condição (ii).

Sejam $\alpha, \beta \in \mathbb{Z}[\theta]$, $\beta \neq 0$ e $\mathcal{N}(\alpha) \geq \mathcal{N}(\beta)$.

Se $\beta \mid \alpha$, segue o resultado. Assim, consideremos que $\alpha \neq 0$ e $\beta \nmid \alpha$.

Queremos provar que existem $\delta, \gamma \in \mathbb{Z}[\theta]$ tais que

$$0 < \mathcal{N}(\alpha\delta - \beta\gamma) < \mathcal{N}(\beta).$$

Notemos que mostrar tal desigualdade é equivalente a mostrar que:

$$0 < \mathcal{N}\left(\left(\frac{\alpha}{\beta}\right)\delta - \gamma\right) < \mathcal{N}(1).$$

Agora, como $\frac{\alpha}{\beta} \in \mathbb{Q}[\sqrt{-19}]$, corpo de fração de $\mathbb{Z}[\theta]$, podemos escrever:

$$\frac{\alpha}{\beta} = \left(\frac{a + b\sqrt{-19}}{c}\right), \text{ em que } a, b \in \mathbb{Z},\ c > 0 \text{ e } \text{mdc}(a, b, c) = 1$$

Mais ainda, temos que $c > 1$, pois, se $c = 1$, então $\frac{\alpha}{\beta} \in \mathbb{Z}[\theta]$, donde $\beta \mid \alpha$. Desta forma, consideraremos as seguintes possibilidades para c:

1. *Caso* $c = 2$

   Como $\frac{\alpha}{\beta} \notin \mathbb{Z}[\theta]$ e $\text{mdc}(a, b, c) = 1$, a e b têm paridade distinta.

   De fato, se a e b forem ímpares, existem $A, B \in \mathbb{Z}$ tais que $a = 2A + 1$ e $b = 2B + 1$, e, consequentemente:

   $$\frac{\alpha}{\beta} = (A - B) + (2B + 1)\left(\frac{a + b\sqrt{-19}}{2}\right) \in \mathbb{Z}[\theta]$$

   Por outro lado, caso a e b sejam ambos pares, teremos uma contradição com o fato de que $\text{mdc}(a, b, c) = 1$.

   Visto a paridade distinta de a e b, é possível tomar $\delta = 1$ e $\gamma = \frac{(a-1) + b\sqrt{-19}}{2}$ em $\mathbb{Z}[\theta]$. Assim:

   $$\left(\frac{\alpha}{\beta}\right)\delta - \gamma = \left(\frac{a + b\sqrt{-19}}{2}\right) - \left(\frac{a - 1 + b\sqrt{-19}}{2}\right) = \frac{1}{2} \neq 0,$$

   donde segue que

   $$0 < \mathcal{N}\left(\left(\frac{\alpha}{\beta}\right)\delta - \gamma\right) = \mathcal{N}\left(\frac{1}{2}\right) = \frac{1}{4} < 1.$$

2. *Caso* $c = 3$

   Como $\text{mdc}(a, b, c) = 1$, temos que a e b não podem ser ambos divisíveis por 3. Então, $a^2 + b^2 \equiv 1$ ou $a^2 + b^2 \equiv 2 \pmod 3$ e, consequentemente,

   $$a^2 + 19b^2 \equiv a^2 + b^2 \not\equiv 0 \pmod 3.$$

Logo, existem $q, r \in \mathbb{Z}$ com $0 < r < 3$ tais que $a^2 + 19b^2 = 3q + r$.

Nessas condições, podemos tomar $\delta = a - b\sqrt{-19}$ e $\gamma = q$ em $\mathbb{Z}[\theta]$ e teremos:

$$\begin{aligned}\left(\frac{\alpha}{\beta}\right)\delta - \gamma &= \left(\frac{a + b\sqrt{-19}}{3}\right)\left(a - b\sqrt{-19}\right) - q \\ &= \left(\frac{a^2 + 19b^2}{3}\right) - q = \left(\frac{3q + r}{3}\right) - q \\ &= \frac{r}{3} \neq 0\end{aligned}$$

Portanto, como $r \leq 2$:

$$0 < \mathcal{N}\left(\left(\frac{\alpha}{\beta}\right)\delta - \gamma\right) = \mathcal{N}\left(\frac{r}{3}\right) \leq \frac{4}{9} < 1$$

3. *Caso* $c = 4$

   De modo semelhante ao caso $c = 2$, como $\text{mdc}(a, b, c) = 1$, a e b não podem ser ambos pares. Assim, temos as seguintes possibilidades: ou a e b são ambos ímpares, ou possuem paridades distintas. Vejamos cada um desses casos.

   Considerando que a e b sejam ambos ímpares, teremos

$$a^2 + 19b^2 \equiv a^2 + 3b^2 \equiv 1 + 3 \cdot 1 \equiv 4 \pmod 8$$

   Então, existe $q \in \mathbb{Z}$ tal que $a^2 + 19b^2 = 3q + 4$.

   Logo, tomando $\delta = \left(\frac{a - b\sqrt{-19}}{2}\right)$ e $\gamma = q$ em $\mathbb{Z}[\theta]$, teremos:

$$\begin{aligned}\left(\frac{\alpha}{\beta}\right)\delta - \gamma &= \left(\frac{a + b\sqrt{-19}}{4}\right)\left(\frac{a - b\sqrt{-19}}{2}\right) - q \\ &= \left(\frac{a^2 + 19b^2}{8}\right) - q = \left(\frac{8q + 4}{8}\right) - q \\ &= \frac{1}{2} \neq 0\end{aligned}$$

   e, portanto:

$$0 < \mathcal{N}\left(\left(\frac{\alpha}{\beta}\right)\delta - \gamma\right) = \mathcal{N}\left(\frac{1}{2}\right) = \frac{1}{4} < 1$$

   Por outro lado, caso a e b tenham paridades distintas, segue que:

$$a^2 + 19b^2 \equiv a^2 - b^2 \not\equiv 0 \pmod 4.$$

   Assim, existem $q, r \in \mathbb{Z}$ com $0 < r < 4$ tais que $a^2 + 19b^2 = 4q + r$. Mais epecificamente, como a e b têm paridades distintas, então $r \neq 2$, ou seja, $r = 1$ ou $r = 3$.

Dessa forma, tomando-se $\delta = a - b\sqrt{-19}$ e $\gamma = q$ em $\mathbb{Z}[\theta]$, temos:

$$\begin{aligned}\left(\frac{\alpha}{\beta}\right)\delta - \gamma &= \left(\frac{a + b\sqrt{-19}}{4}\right)\left(a - b\sqrt{-19}\right) - q \\ &= \left(\frac{a^2 + 19b^2}{4}\right) - q = \left(\frac{4q + r}{4}\right) - q \\ &= \frac{r}{4} \neq 0\end{aligned}$$

E, utilizando que $r \leq 3$, resulta:

$$0 < \mathcal{N}\left(\left(\frac{\alpha}{\beta}\right)\delta - \gamma\right) = \mathcal{N}\left(\frac{r}{4}\right) \leq \frac{9}{16} < 1$$

4. *Caso* $c \geq 5$

Como $\text{mdc}(a, b, c) = 1$, existem $d, e, f \in \mathbb{Z}$ tais que $ad + be + cf = 1$. Agora, dividindo $ae - 19bd$ por c, temos que existem $q, r \in \mathbb{Z}$ tais que $ae - 19bd = qc + r$, em que $|r| \leq \frac{c}{2}$. Então, tomando $\delta = e + \sqrt{-19}$ e $\gamma = q - f\sqrt{-19}$, ambos em $\mathbb{Z}[\theta]$, segue:

$$\begin{aligned}\left(\frac{\alpha}{\beta}\right)\delta - \gamma &= \left(\frac{a + b\sqrt{-19}}{c}\right)\left(e + d\sqrt{-19}\right) - \left(q - f\sqrt{-19}\right) \\ &= \left(\frac{ae - 19bd + (ad + be)\sqrt{-19}}{c}\right) - \left(q - f\sqrt{-19}\right) \\ &= \frac{(ae - 19bd - qc) + (ad + be + cf)\sqrt{-19}}{c} \\ &= \frac{r + \sqrt{-19}}{c} \neq 0\end{aligned}$$

Como $r, c \in \mathbb{Z}$, segue que tal elemento pertence a $\mathbb{Z}[\theta]$, donde

$$\mathcal{N}\left(\left(\frac{\alpha}{\beta}\right)\delta - \gamma\right) > 0$$

Resta-nos mostrar que $\mathcal{N}\left(\left(\frac{\alpha}{\beta}\right)\delta - \gamma\right) < 1$

Para tanto, notemos que, se $c = 5$, então $|r| \leq 2$ e, logo:

$$\mathcal{N}\left(\left(\frac{\alpha}{\beta}\right)\delta - \gamma\right) = \mathcal{N}\left(\frac{r + \sqrt{-19}}{5}\right) = \frac{r^2 + 19}{25} \leq \frac{4 + 19}{25} = \frac{23}{25} < 1$$

Finalmente, se $c \geq 6$, então $|r| \leq \frac{c}{2}$ e, consequentemente:

$$\mathcal{N}\left(\left(\frac{\alpha}{\beta}\right)\delta - \gamma\right) = \mathcal{N}\left(\frac{r + \sqrt{-19}}{c}\right) \leq \left(\frac{c^2}{4} + 19\right)\frac{1}{c^2} = \frac{1}{4} + \frac{19}{36} = \frac{7}{9} < 1$$

Portanto, concluímos a demonstração de que $\mathbb{Z}[\theta]$ é um anel principal. □

3 O TEOREMA DE PITÁGORAS

Segundo relata o livro Simon [17], antes de conjecturar um dos seus mais famosos teoremas, afirmando que a equação $x^n + y^n = z^n$ não possui solução inteira para $n \geq 3$, Fermat estaria se concentrando na busca por soluções de equações diofantinas, motivado pelo Teorema de Pitágoras.

Tal teorema estabelece que, em um triângulo retângulo de catetos x e y e hipotenusa z, a seguinte relação é satisfeita:

$$x^2 + y^2 = z^2$$

Mais ainda, se esta relação é válida em um triângulo, o mesmo é retângulo.

Neste contexto, torna-se natural buscar soluções positivas não triviais, chamadas de *ternos pitagóricos*, para a equação acima. Tal busca ficou conhecida como *Problema de Diofante* e teria sido uma das principais motivações para que Fermat enunciasse seu famoso teorema.

Na primeira seção desse capítulo, apresentaremos alguns resultados associados à equação de Fermat (conhecida como *equação fermatiana*), os quais serão essenciais para os casos específicos de seu teorema que provaremos, inclusive os Teoremas de Sophie e de Kummer. Em seguida, estudaremos as soluções inteiras do Teorema de Pitágoras, que serão utilizadas na prova do caso $n = 4$ no capítulo 4.

3.1 RESULTADOS PRELIMINARES

Na busca por ternos pitagóricos, é interessante destacar que podemos nos restringir aos ternos (x, y, z) em que $\text{mdc}(x, y) = 1$ (ou, equivalentemente, em que $\text{mdc}(x, z) = \text{mdc}(y, z) = 1$), os quais denominamos *ternos pitagóricos primitivos*.

Nessa seção, apresentaremos resultados que justificam tal abordagem para o caso geral; mais precisamente, mostraremos que, dado n natural, caso a equação fermatiana:

$$x^n + y^n = z^n$$

possua solução inteira e não trivial, podemos nos limitar às soluções formadas por inteiros relativamente primos.

Primeiramente, notemos que:

Lema 3.1.1. *Sejam $x, y, z \in \mathbb{N}$ tais que $x^n + y^n = z^n$, com $n \in \mathbb{N}$. Então são equivalentes as seguintes afirmações:*

(i) $mdc(x, y) = 1$

(*ii*) $mdc(x, z) = 1$

(*iii*) $mdc(y, z) = 1$

Demonstração. Provaremos apenas uma das implicações; as demais são demonstradas de modo analogo.

(i) $\Rightarrow$ (ii)

Seja $d = \text{mdc}(x, z)$. Assim, existem $a, b \in \mathbb{N}$ tais que $x = ad$ e $z = bd$ e, consequentemente:

$$\begin{aligned} x^n + y^n = z^n &\Rightarrow (ad)^n + y^n = (bd)^n \\ &\Rightarrow y^n = d^n(b - a) \end{aligned}$$

Logo, $d^n \mid y^n$, donde segue que $d \mid y$. Como $d \mid x, y$ e $\text{mdc}(x, y) = 1$, segue que $d = 1$.

□

Proposição 3.1.1. *Caso a equação $x^n + y^n = z^n$, sendo $n \in \mathbb{N}$, admita solução inteira não trivial, digamos (x_0, y_0, z_0), podemos considerar, sem perda de generalidade, que $mdc(x_0, y_0) = 1$.*

Demonstração. Para a prova desta proposição, mostraremos que: se (x, y, z) é uma solução inteira não trivial para a equação $x^n + y^n = z^n$, então existe uma solução inteira não trivial (x_0, y_0, z_0) tal que $\text{mdc}(x_0, y_0) = 1$.

Seja $d = \text{mdc}(x, y)$. Se $d = 1$, o resultado é imediato, bastando tomar $x_0 = x$ e $y_0 = y$. Consideremos, então, que $d \neq 1$.

Pela definição de máximo divisor comum, temos que $d \neq 0$, $d \mid x$ e $d \mid y$. Assim, existem $x_0, y_0 \in \mathbb{Z}$ tais que $x = dx_0$ e $y = dy_0$. Além disso, pela Identidade de Bezout, como $d = \text{mdc}(x, y)$, existem $u, v \in \mathbb{Z}$ tais que $ux + vy = d$. Assim, temos:

$$\begin{aligned} u(dx_0) + v(dy_0) &= d \\ ux_0 + vy_0 &= 1 \end{aligned}$$

Como conseguimos uma combinação linear entre x_0 e y_0 resultando em 1, segue que $\text{mdc}(x_0, y_0) = 1$.

Por outro lado, utilizando o fato de que (x, y, z) é solução, temos:

$$\begin{aligned} x^n + y^n = z^n &\Rightarrow (dx_0)^n + (dy_0)^n = z^n \\ &\Rightarrow d^n(x_0^n + y_0^n) = z^n \end{aligned}$$

Assim, temos que $d^n \mid z^n$, donde segue que $d \mid z$. Dessa forma, existe $z_0 \in \mathbb{Z}$ tal que $z = dz_0$ e, consequentemente, temos:

$$d^n(x_0^n + y_0^n) = (dz_0)^n \quad \therefore \quad x_0^n + y_0^n = z_0^n$$

Logo, a tripla (x_0, y_0, z_0) constitui uma solução para a equação $x^n + y^n = z^n$, com $\text{mdc}(x_0, y_0) = 1$. □

3.2 TERNOS PITAGÓRICOS

Nesta seção, apresentaremos teoremas que nos fornecem as condições necessárias e suficientes a fim de que (x, y, z) seja um terno pitagórico. Tais caracterizações serão retomadas na prova do Último Teorema de Pitágoras (UTF) no caso em que $n = 4$.

No caso de um terno pitagórico arbitrário, temos o seguinte resultado:

Teorema 3.2.1. *(x, y, z) é um terno pitagórico se e, somente se, existem naturais u e v de mesma paridade, tais que uv é um quadrado perfeito, e valem as igualdades:*

$$x = \sqrt{uv}\,, \; y = \frac{u - v}{2} \; e \; z = \frac{u + v}{2}$$

Demonstração. Consideremos (x, y, z) um terno pitagórico.

Sabemos, então, que:

$$x^2 + y^2 = z^2 \;\Rightarrow\; x^2 = z^2 - y^2 = (z + y)(z - y).$$

Sejam $u = z + y$ e $v = z - y$. Assim, u e v são inteiros positivos com a mesma paridade, tais que uv é um quadrado perfeito e valem as relações:

$$x = \sqrt{uv}\,, \; y = \frac{u - v}{2} \text{ e } z = \frac{u + v}{2}.$$

Reciprocamente, suponha que u e v satisfazem as condições do teorema. Como u e v possuem a mesma paridade e são ambos positivos, tem-se que

$$y = \frac{u - v}{2} \text{ e } z = \frac{u + v}{2} \text{ são ambos inteiros positivos.}$$

E pelo fato de uv ser um quadrado perfeito, $x = \sqrt{uv}$ também é inteiro positivo. Desse modo:

$$x^2 + y^2 = (\sqrt{uv}) + \left(\frac{u - v}{2}\right)^2 = \frac{4uv + u^2 - 2uv + v^2}{4} = \left(\frac{u + v}{2}\right)^2,$$

donde (x, y, z) é um terno pitagórico. □

Já no caso dos ternos pitagóricos primitivos, temos a caracterização que se segue:

Teorema 3.2.2. *Sejam $x, y, z \in \mathbb{N}$. Então (x, y, z) constitui uma solução primitiva para a equação $x^2 + y^2 = z^2$ se, e somente se, satisfaz as condições:*

$$\begin{cases} x = 2ab \\ y = a^2 - b^2 \\ z = a^2 + b^2 \end{cases}$$

em que $a, b \in \mathbb{N}$ têm paridades distintas, $a > b$ e $mdc(a, b) = 1$.

Demonstração. Sejam $x, y, z \in \mathbb{Z}$ definidos como acima. Então a equaação pitagórica é de fato satisfeita:

$$x^2 + y^2 = (2ab)^2 + (a^2 - b^2)^2 = a^4 + 2a^2b^2 + b^4 = (a^2 + b^2)^2 = z^2$$

Resta-nos provar que tal solução é primitiva, ou seja, $\text{mdc}(x, y) = 1$. Observemos que, como a e b por hipótese têm paridades distintas, então $y = a^2 - b^2$ é um número ímpar; enquanto $x = 2ab$ é par.

Suponhamos, por absurdo, que $\text{mdc}(x, y) \neq 1$. Consideremos p um primo ímpar tal que $p \mid x$ e $p \mid y$. Como $p \mid 2ab$ e p é primo ímpar, segue que $p \mid a$ ou $p \mid b$. Suponhamos, sem perda de generalidade, que $p \mid a$. Como, por outro lado, temos que $p \mid y = a^2 - b^2$, concluímos que $p \mid b$. Logo, $p \mid a, b$, contradizendo o fato de que $\text{mdc}(a, b) = 1$.

Logo, devemos ter $\text{mdc}(x, y) = 1$.

Reciprocamente, consideremos que (x, y, z) seja um terno pitagórico, ou seja, uma solução inteira não trivial de $x^2 + y^2 = z^2$, em que $\text{mdc}(x, y) = 1$. Pela proposição anterior, temos que existem $u, v \in \mathbb{N}$ de mesma paridade tais que uv é um quadrado perfeito e

$$x = \sqrt{uv}\,, \;\; y = \frac{u - v}{2} \;\text{ e }\; z = \frac{u + v}{2}.$$

Caso u e v sejam pares, podemos escrever $u = 2m$ e $v = 2n$, com $m, n \in \mathbb{N}$. Assim:

$$x = 2\sqrt{mn}\,, \;\; y = m - n \;\text{ e }\; z = m + n$$

Notemos que $\text{mdc}(m, n) = 1$. Com efeito, seja $d = \text{mdc}(m, n)$; então, $d \mid m$ e $d \mid n$, resultando que $d \mid x$ e $d \mid y$. Logo, $d = 1$. Por outro lado, m e n devem ter paridades distintas, pois, caso contrário, teríamos que $2 \mid x, y$, uma contradição com o fato de que $\text{mdc}(x, y) = 1$.

Observemos ainda que $x^2 = 4mn$, em que $\text{mdc}(m, n) = 1$. Desse modo, m e n são quadrados perfeitos, ou seja, existem $a, b \in \mathbb{N}$ tais que $m = a^2$ e $n = b^2$, sendo a e b de paridades distintas.

Portanto,

$$x = 2ab\,, \;\; y = a^2 - b^2 \;\text{ e }\; z = a^2 + b^2,$$

com $\text{mdc}(a,b) = 1$ e a e b de paridades distintas, como queríamos provar.

Agora, consideremos o caso em que u e v sejam ambos ímpares. Como $\text{mdc}(x,y) = 1$, tem-se que $\text{mdc}(u,v) = 1$. De fato, seja $d = \text{mdc}(u,v)$. Assim, teremos que $d \mid x, y$, donde resulta que $d = 1$. Dessa forma, como $x^2 = uv$ e u e v não possuem fatores em comum, segue que u e v são quadrados perfeitos. Então, existem $m, n \in \mathbb{N}$ tais que $u = m^2$ e $v = n^2$.

Logo:

$$\begin{aligned} y &= \frac{u-v}{2} = \frac{m^2-n^2}{2} = 2\left(\frac{m+n}{2}\right)\left(\frac{m-n}{2}\right) \\ x &= \sqrt{uv} = mn = \left(\frac{m+n}{2}\right)^2 - \left(\frac{m-n}{2}\right)^2 \end{aligned}$$

Assim, lembrando que $z^2 = x^2 + y^2$ e definindo a e b como a seguir

$$a := \frac{m+n}{2} \text{ e } b := \frac{m-n}{2},$$

conclui-se que:

$$y = 2ab\,,\ x = a^2 - b^2 \text{ e } z = a^2 + b^2,$$

Portanto, a menos de mudança de variáveis, temos as igualdades esperadas.

Assim, resta-nos mostrar apenas que a e b têm paridades distintas. Primeiramente, notemos que, como u e v são ímpares, então m e n também o são. Desse modo, temos as seguintes possibilidades:

(1) $m \equiv n \equiv 1, 3 \pmod 4$

Neste caso, temos $m + n \equiv 2 \pmod 4$ e $m - n \equiv 0 \pmod 4$. Consequentemente, a é ímpar e b é par.

(2) $m \equiv 1$ e $n \equiv 3 \pmod 4$ ou $m \equiv 3$ e $n \equiv 1 \pmod 4$

Neste caso, segue que $m + n \equiv 0 \pmod 4$ e $m - n \equiv 2 \pmod 4$. Resulta então que a é par e b é ímpar.

Em ambas as situações, concluímos que $a \not\equiv b \pmod 2$. □

4 OS CASOS $n = 3$ e $n = 4$

Nesse capítulo, começaremos utilizando os resultados sobre ternos pitagóricos do capítulo 3 para demonstrarmos o Último Teorema de Fermat para o caso em que $n = 4$. Em seguida, utilizaremos resultados do capítulo 2 para o caso em que $n = 3$, sob uma abordagem semelhante à desenvolvida por Euler.

4.1 O CASO $n = 4$

Teorema 4.1.1 (Último Teorema de Fermat: Caso n = 4). *A equação $X^4 + Y^4 = Z^2$ não possui solução não trivial em $\mathbb{Z}$, ou seja, exceto com pelo menos uma das variáveis nulas. Em particular, o Último Teorema de Fermat é válido para $n = 4$.*

Demonstração. Demonstraremos tal resultado utilizando redução ao absurdo.

Consideremos que a equação $X^4 + Y^4 = Z^2$ possua solução não trivial (x, y, z). Sem perda de generalidade, podemos supor que $x, y, z \in \mathbb{N}$. Escolhemos a solução com o menor valor possível para z e, então, podemos considerar $\text{mdc}(x, y) = 1$.

Com efeito, caso tenhamos $d = \text{mdc}(x, y) \neq 1$, dividimos a equação inicial por d^4 e obtemos uma solução com um menor valor para z:

$$x^4 + y^4 = z^2 \Rightarrow \left(\frac{x}{d}\right)^4 + \left(\frac{y}{d}\right)^4 = \left(\frac{z}{d^2}\right)^2$$

(Lembrando que, pela definição de mdc, essa nova solução é inteira e não trivial.)

Agora, pelo Teorema 3.2.2, temos que existem $a, b \in \mathbb{N}$, sendo as paridades de a e b distintas e $\text{mdc}(a, b) = 1$, tais que:

$$\begin{cases} x^2 = 2ab \\ y^2 = a^2 - b^2 \\ z^2 = a^2 + b^2 \end{cases}$$

Caso a seja par e b ímpar, teremos $y^2 = a^2 - b^2 \equiv -1 \pmod 4$, o que não é possível, visto que existem apenas duas possibilidades para o resto de um quadrado perfeito na divisão por 4, no caso, 0 e 1. Então, devemos ter a ímpar e b par. Consequentemente, podemos escrever $b = 2c$, com $c \in \mathbb{Z}$ e, assim:

$$x^2 = 2ab = 4ac \Rightarrow \left(\frac{x}{2}\right)^2 = ac$$

Pela igualdade acima, podemos escrever $a = l^2$ e $c = m^2$, com $l, m \in \mathbb{N}$ e l ímpar. Mais ainda, como a e b são primos entre si, temos que o mesmo vale para a e c, implicando que $\text{mdc}(l, m) = 1$.

Além disso, temos que:

$$y^2 = a^2 - b^2 = a^2 - (2c)^2 = l^4 - 4m^4,$$

donde resulta:

$$(l^2)^2 = (2m^2)^2 + y^2 \tag{4.1}$$

Notemos que, pelo fato de $\text{mdc}(l, m) = 1$ e de l ser ímpar, temos $\text{mdc}(2m^2, l^2) = 1$ e, logo, $\text{mdc}(2m^2, y) = 1$ (utilizando o Lema 3.1.1). Nessas condições, aplicando novamente o Teorema 3.2.2 na equação (4.1), temos que existem $p, q \in \mathbb{N}$ de paridades distintas e tais que $\text{mdc}(p, q) = 1$ satisfazendo:

$$\begin{cases} 2m^2 = 2pq \\ y^2 = p^2 - q^2 \\ l^2 = p^2 + q^2 \end{cases}$$

Como $m^2 = pq$ e $\text{mdc}(p, q) = 1$, segue que existem $r, s \in \mathbb{N}$, primos entre si, tais que $p = r^2$ e $q = s^2$. Assim, resulta que:

$$l^2 = r^4 + s^4 \tag{4.2}$$

Observemos que $l < z$ pois, pela definição de l, temos:

$$l^2 = a \leq a^2 < a^2 + b^2 = z^2$$

Desse modo, pela equação (4.2), obtivemos outra solução inteira para a equação $X^4 + Y^4 = Z^2$, a saber, a tripla (r, s, l), em que $l < z$. No entanto, esse resultado contradiz a minimalidade de z.

Portanto, a equação $X^4 + Y^4 = Z^2$ não possui solução não trivial em $\mathbb{Z}$, como queríamos provar. □

4.2 O CASO $n = 3$

Para a demonstração do UTF quando $n = 3$, utilizaremos uma abordagem semelhante à prova feita por Euler e, posteriormente, modificada por Gauss. Para tanto, utilizaremos um anel específico:

Definição 4.2.1. *Consideremos a seguinte raiz cúbica da unidade:*

$$\omega := \frac{e^{2\pi i}}{3} = \frac{-1 + \sqrt{-3}}{2}$$

O anel dos inteiros de Eisenstein é definido como:

$$\mathbb{Z}[\omega] := \mathbb{Z}\left[\frac{1 + \sqrt{-3}}{2}\right] = \{a + b\omega : a, b \in \mathbb{Z}\}$$

e caracteriza-se como o anel dos inteiros do corpo quadrático $\mathbb{Q}[\omega] := \mathbb{Q}[\sqrt{-3}]$.

Em princípio, Euler teria utilizado em sua demonstração o subanel dos inteiros de Eisenstein dado por $\mathbb{Z}[\sqrt{-3}]$. No entanto, o mesmo não é um anel fatorial, ou seja, a unicidade da fatoração em elementos irredutíveis não é garantida em geral, como inicialmente Euler teria utilizado. Contudo, no caso específico em que estava trabalhando, havia unicidade. A demonstração detalhada disso foi feita posteriormente por Gauss. Entretanto, outros resultados publicados por Euler forneceram uma prova alternativa para o caso $n = 3$, em que não havia nenhuma lacuna lógica. Dessa forma, o crédito da demonstração deste caso é frequentemente atribuído somente a ele.

Em nossa abordagem, utilizaremos o anel $\mathbb{Z}[\omega]$, visto que é possível provar que o mesmo é um Domínio de Fatoração Única[1]. Nesse contexto, para a demonstração, provaremos uma versão mais geral do Último Teorema, a saber: *A equação* $x^3 + y^3 = z^3$ *não possui solução não trivial em* $\mathbb{Z}[\omega]$.

Nos resultados seguintes, para simplificar os cálculos, denotaremos $\lambda := 1 - \omega$ e utilizaremos o fato, que pode ser verificado diretamente, de que ω é raiz da equação $x^2 + x + 1 \in \mathbb{Z}[x]$.

Proposição 4.2.1. *$\lambda = 1 - \omega$ é um elemento primo de $\mathbb{Z}[\omega]$.*

Demonstração. Notemos que a norma de λ é um número primo:

$$\mathcal{N}(\lambda) = \mathcal{N}\left(1 - \left(\frac{-1 + i\sqrt{3}}{2}\right)\right) = \mathcal{N}\left(\frac{3}{2} - \frac{i\sqrt{3}}{2}\right) = \frac{9}{4} + \frac{3}{4} = 3$$

Assim, λ é irredutível (utilizando a Proposição 2.2.2). Por outro lado, como $m = -3$, temos que $\mathbb{Z}[\omega]$ é um anel euclideano (Teorema 2.3.2), donde segue que λ é primo. □

Proposição 4.2.2. *Os elementos inversíveis de $\mathbb{Z}[\omega]$ são $\pm 1, \pm\omega$ e $\pm\omega^2$.*

Demonstração. Consideremos γ um elemento inversível, com

$$\gamma = \frac{a + bi\sqrt{3}}{2} \in \mathbb{Z}[\omega]$$

Assim, pela Proposição 2.2.2, temos que

$$\mathcal{N}(\gamma) = 1 \therefore \frac{a^2 + 3b^2}{4} = 1 \therefore a^2 = 3b^2 = 4,$$

cujas soluções inteiras são $a = \pm 2$ e $b = 0$ ou $a = \pm 1$ e $b = \pm 1$.

Desse modo, $\gamma = \pm 1, \pm\omega$ ou $\pm\omega^2$, como queríamos provar. □

[1] A prova de que $\mathbb{Z}[\omega]$ é um DFU envolve métodos mais complexos, os quais não serão detalhados agora. Retomaremos a justificativa desse fato no último capítulo.

Agora, apresentaremos resultados que auxiliarão na prova do UTF para $n = 3$.

Lema 4.2.1. *Para quaisquer $\alpha, \beta \in \mathbb{Z}[\omega]$, vale a igualdade:*

$$\alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \omega\beta)(\alpha + \omega^2\beta)$$

Demonstração. Temos que:

$$(\alpha + \beta)(\alpha + \omega\beta)(\alpha + \omega^2\beta) = \alpha^3 + \alpha^2\beta(1 + \omega + \omega^2) + \alpha\beta^2(1 + \omega + \omega^2) + \beta^3 = \alpha^3 + \beta^3\,,$$

pois $1 + \omega + \omega^2 = 0$. □

Nos próximos lemas, utilizaremos a seguinte definição:

Definição 4.2.2. *De modo semelhante à relação de congruência em $\mathbb{Z}$, dados $\alpha, \beta, \rho \in \mathbb{Z}[\omega]$, dizemos que α é congruente a β módulo ρ, e escrevemos $\alpha \equiv \beta \pmod{\rho}$, se $\rho \mid (\alpha - \beta)$.*

Lema 4.2.2. *O anel de inteiros $\mathbb{Z}[\omega]$ possui exatamente três classes distintas módulo λ, a saber: $0, 1$ e -1.*

Demonstração. Primeiramente, vamos mostrar que tais classes existem e, em seguida, que as mesmas são distintas.

Seja $\alpha = a + b\omega = a + b(1 - \lambda) = a + b - b\lambda \in \mathbb{Z}[\omega]$. Então, $\alpha \equiv a + b \pmod{\lambda}$. Por outro lado, como $\omega^2 + \omega = -1$ e ω é uma raiz cúbica da unidade, tem-se:

$$3 = 1 - (\omega^2 + \omega) + 1 = (1 - \omega)(1 - \omega^2) =: \lambda(1 - \omega^2) \therefore \lambda \mid 3$$

Assim, como $a + b \equiv 0, 1, \text{ ou } -1 \pmod{3}$, segue que $a + b \equiv 0, 1, \text{ ou } -1 \pmod{\lambda}$. Logo, existem, no máximo, três classes distintas módulo λ.

Agora, vejamos que $0, 1$ e -1 não são congruentes mod λ. De fato, caso contrário, teríamos que $1 - 0$, $0 - (-1)$ e $1 - (-1)$ seriam divisíveis por λ.

Ora, observemos que, dado qualquer $\delta \in \mathbb{Z}[\omega]$ tal que $\lambda \mid \delta$, então $\delta = \lambda\sigma$ para algum $\sigma \in \mathbb{Z}[\omega]$. E, como a norma é uma função multiplicativa, temos $N(\delta) = N(\lambda)N(\sigma)$, ou seja, $N(\lambda)$ é um divisor de $N(\delta)$.

Contudo, nessa situação, isso implicaria que a norma de λ seria um divisor das normas de 1 e 2, o que não ocorre, pois: $N(1) = 1$ e $N(2) = 4$, enquanto $N(\lambda) = 3$. □

Lema 4.2.3. *Dado $\rho \in \mathbb{Z}[\omega]$, se $\lambda \nmid \rho$, então $\rho^3 \equiv \pm 1 \pmod{\lambda^4}$*

Demonstração. Pelo Lema anterior, dado $\rho \in \mathbb{Z}[\omega]$, sabemos que $\rho \equiv 0, 1, \text{ ou } -1 \pmod{\lambda}$. Como, por hipótese, $\lambda \nmid \rho$, restringimo-nos ao caso $\rho \equiv \pm 1 \pmod{\lambda}$.

Escolhemos $\alpha = \rho$ ou $\alpha = -\rho$, de modo que $\alpha \equiv 1 \pmod{\lambda}$. Nessas condições, existe $\beta \in \mathbb{Z}[\omega]$ tal que $\alpha = 1 + \beta\lambda$ e, assim, pelo Lema (4.2.1), temos:

$$\begin{aligned} \alpha^3 - 1 &= (\alpha - 1)(\alpha - \omega)(\alpha - \omega^2) \\ &= \beta\lambda(\beta\lambda + 1 - \omega)(\beta\lambda + 1 - \omega^2) \\ &= \beta\lambda(\beta\lambda + \lambda)(\beta\lambda - \lambda\omega^2) \\ &= \beta\lambda^3(\beta + 1)(\beta - \omega^2) \end{aligned} \tag{4.3}$$

Na penúltima igualdade, foi utilizado que $-\lambda\omega^2 = 1 - \omega^2$, uma vez que

$$1 - \omega^2 = (1 + \omega)(1 - \omega) = \lambda(1 + \omega) = -\lambda(-1 - \omega) = -\lambda\omega^2.$$

Notemos que, dessa forma, $\omega^2 = 1 + \lambda\omega^2$, ou seja, $\omega^2 \equiv 1 \pmod{\lambda}$.

Assim,

$$\beta(\beta + 1)(\beta - \omega^2) \equiv \beta(\beta + 1)(\beta - 1) \pmod{\lambda}.$$

Agora, pelo Lema 4.2.2, temos que os únicos restos possíveis de β por λ são $0, 1$ ou -1, donde λ divide $\beta, \beta + 1$ ou $\beta - 1$. Consequentemente, pela equação (4.3), segue que $\alpha^3 - 1 \equiv 0 \pmod{\lambda^4}$, ou seja, $\alpha^3 \equiv 1 \pmod{\lambda^4}$.

Como definimos α como sendo ρ ou $-\rho$, concluímos que $\rho^3 \equiv 1 \pmod{\lambda^4}$ ou $\rho^3 \equiv -1 \pmod{\lambda^4}$. □

Lema 4.2.4. *Se $\alpha^3 + \beta^3 + \gamma^3 = 0$, então ao menos um dos elementos α, β ou γ é divisível por λ.*

Demonstração. Suponhamos, por absurdo, que λ não divida α, β e γ. Então, pelo lema anterior, temos que:

$$0 = \alpha^3 + \beta^3 + \gamma^3 \equiv \pm 1 \pm 1 \pm 1 \pmod{\lambda^4}.$$

Dessa forma, $\pm 3 \equiv 0 \pmod{\lambda^4}$ ou $\pm 1 \equiv 0 \pmod{\lambda^4}$. No entanto, tal fato gera uma contradição, pois $N(\pm 1) = 1$ e $N(\pm 3) = 9$, enquanto $N(\lambda^4) = N(\lambda)^4 = 3^4 = 81$.

Logo, λ divide α, β ou γ. □

Com estes lemas, concluímos a prova do Teorema esperado:

Teorema 4.2.1 (Último Teorema de Fermat: Caso n = 3). *A equação $x^3 + y^3 = z^3$ não possui solução não trivial, ou seja, com pelo menos uma das variáveis nulas, no anel de inteiros $\mathbb{Z}[\omega]$. Em particular, não possui solução inteira não trivial e, portanto, o Último Teorema de Fermat é válido para $n = 3$.*

Demonstração. Como $\mathbb{Z}[\omega]$ é anel, podemos, sem perda de generalidade, trocar z por $-z$ na equação inicial. Assim, provar o Teorema acima é equivalente a mostrar que $x^3 + y^3 + z^3 = 0$ não possui solução (não trivial) em $\mathbb{Z}[\omega]$.

Suponhamos, por absurdo, que existam $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$, com $\alpha\beta\gamma \neq 0$, tais que $\alpha^3 + \beta^3 + \gamma^3 = 0$.

Pelo Lema 4.2.4, sabemos que α, β ou γ é divisível por λ. Suponhamos, sem perda de generalidade que $\lambda \mid \gamma$. Assim, podemos escrever $\gamma = \lambda^n \delta$, em que $n \in \mathbb{N}$, $\delta \in \mathbb{Z}[\omega]$ e $\lambda \nmid \delta$.

Por outro lado, de modo semelhante ao feito no Lema 3.1.1, podemos considerar, sem perda de generalidade, que α, β e γ não possuem fatores em comum, ou seja, são dois a dois primos entre si. Dessa forma, segue que $\lambda \nmid \alpha$ e $\lambda \nmid \beta$.

Reescrevendo a equação inicial, obtemos:

$$\alpha^3 + \beta^3 + \lambda^{3n}\delta^3 = 0, \text{ em que } \mathrm{mdc}(\alpha, \beta) = 1, \ n \geq 1 \text{ e } \lambda \nmid \alpha, \beta, \delta \tag{4.4}$$

Mostraremos, no entanto, que, sob tais condições, a seguinte equação não tem solução para todo elemento inversível $\varepsilon \in \mathbb{Z}[\omega]$:

$$\alpha^3 + \beta^3 + \varepsilon\lambda^{3n}\delta^3 = 0. \tag{4.5}$$

Em particular, a equação (4.4) não terá solução em $\mathbb{Z}[\omega]$, contrariando a existência de α, β e γ e comprovando o Teorema.

Para provarmos que a equação (4.5) não possui solução, consideraremos as seguintes afirmações:

Afirmação 1: *Se α, β, γ satisfazem a equação (4.5) com as condições exigidas em (4.4), então $n \geq 2$.*
Prova. Pelo Lema 4.2.3, temos que:

$$-\varepsilon\lambda^{3n}\delta^3 = \alpha^3 + \beta^3 \equiv \pm 1 \pm 1 \pmod{\lambda^4}.$$

Caso os sinais de α e β sejam os mesmos, teremos $-\varepsilon\lambda^{3n}\delta^3 \equiv \pm 2 \pmod{\lambda^4}$, o que não é possível, visto que $\lambda \nmid 2$. Logo, os sinais devem ser contrários, resultando em $-\varepsilon\lambda^{3n}\delta^3 \equiv 0 \pmod{\lambda^4}$. Portanto, como $\lambda \nmid \delta$, teremos que $\lambda^4 \mid \lambda^{3n}$, donde $n \geq 2$.

Afirmação 2: *Se a equação (4.5) possui solução para $n = m > 1$, então ela possui solução para $n = m - 1$.*
Prova. Pela equação (4.5) e pelo Lema 4.2.1, sabemos que:

$$-\varepsilon\lambda^{3m}\delta^3 = \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \omega\beta)(\alpha + \omega^2\beta) \tag{4.6}$$

Calculando as diferenças dos fatores à direita desta última igualdade, temos:

$$(\alpha+\beta)-(\alpha+\omega\beta)=\beta(1-\omega)=\beta\lambda \tag{4.7}$$

$$(\alpha+\omega\beta)-(\alpha+\omega^2\beta)=\omega\beta(1-\omega)=\omega\beta\lambda \tag{4.8}$$

$$(\alpha+\omega^2\beta)-(\alpha+\beta)=\beta(\omega^2-1)=-\beta(1-\omega)(1+\omega)=\beta\lambda\omega^2 \tag{4.9}$$

Assim, tais diferenças são divisíveis por λ, mas não são divisíveis por λ^2, visto que ω é inversível e $\lambda \nmid \beta$.

Pela *Afirmação 1*, temos que $m \geq 2$, isto é, $3m \geq 4$. Assim, exatamente um dos fatores $\alpha+\beta, \alpha+\omega\beta$ ou $\alpha\omega^2\beta$ é divisível por λ^2 e, consequentemente, divisível por λ^{3m-2}. Os demais serão divisíveis por λ, mas não por λ^2 (equivalentemente, λ^{3m-2}), pois as diferenças acima possuem tal propriedade.

Além disso, como podemos trocar β por um de seus associados $\omega\beta$ ou $\omega^2\beta$, podemos supor, sem perda de generalidade, que $\alpha+\beta$ é divisível por λ^2 e, então, por λ^{3m-2}. Então, temos que existem $\xi_1, \xi_2, \xi_3 \in \mathbb{Z}[\omega]$ satisfazendo:

$$\begin{cases} \alpha+\beta=\lambda^{3m-2}\xi_1 \\ \alpha+\omega\beta=\lambda\xi_2 \\ \alpha+\omega^2\beta=\lambda\xi_3 \end{cases} \qquad \text{em que } \lambda \nmid \xi_1\xi_2\xi_3.$$

Notemos que a condição $\lambda \nmid \xi_1\xi_2\xi_3$ é resultado da equação (4.7), juntamente ao fato de que ε é inversível em $\mathbb{Z}[\omega]$ e $\lambda \nmid \delta$. Com efeito, caso $\lambda \mid \xi_1\xi_2\xi_3$, teríamos, no lado esquerdo da equação (4.7) o fator λ^{3m}, enquanto ao lado direito, o fator $\lambda^{3m-2}\lambda^2\lambda=\lambda^{3m+1}$, uma contradição. Cabe ressaltar que neste argumento, estamos utilizando fortemente o fato de que $\mathbb{Z}[\omega]$ é um domínio de fatoração única.

Logo, temos

$$\begin{aligned} -\varepsilon\lambda^{3m}\delta^3 &= \alpha^3+\beta^3=(\alpha+\beta)(\alpha+\omega\beta)(\alpha+\omega^2\beta) \\ &= \lambda^{3m-2}\xi_1\lambda\xi_2\lambda\xi_3=\lambda\xi_1\xi_2\xi_3 \end{aligned}$$

e, consequentemente, $-\varepsilon\delta^3=\xi_1\xi_2\xi_3$.

Agora, afirmamos que $\mathrm{mdc}(\xi_1,\xi_2)=\mathrm{mdc}(\xi_2,\xi_3)=\mathrm{mdc}(\xi_2,\xi_3)=1$.

De fato, suponha que $\mu \mid \xi_1$ e $\mu \mid \xi_2$. Pela equação (4.8), temos que:

$$\lambda\beta=(\alpha+\beta)-(\alpha+\omega\beta)=\lambda^{3m-2}\xi_1-\lambda\xi_2=\lambda(\lambda^{3m-3}\xi_1-\xi_2)$$

Então, $\beta=\lambda^{3m-3}\xi_1-\xi_2$. Mais ainda, como $\mu \mid \xi_1$ e $\mu \mid \xi_2$, segue que $\mu \mid \beta$.

Por outro lado, notemos que:

$$\omega^2(\alpha+\omega\beta)-(\alpha+\beta)=(\omega^2-1)\alpha=\omega^2\lambda\alpha$$

e também

$$\omega^2(\alpha + \omega\beta) - (\alpha + \beta) = (\omega^2 - 1)\alpha = \omega^2\lambda\xi_2 - \lambda^{3m-2}\xi_1 = \lambda(\omega^2\xi_2 - \lambda^{3m-3}\xi_1).$$

Comparando essas equações, concluímos que $\omega^2\alpha = \omega^2\xi_2 - \lambda^{3m-3}\xi_1$. Como ω^2 é inversível, temos que $\mu \mid \alpha$.

Por fim, como $\mu \mid \alpha$, $\mu \mid \beta$ e $\text{mdc}(\alpha, \beta) = 1$ (por hipótese), segue que μ é inversível e, assim, $\text{mdc}(\xi_1, \xi_2) = 1$.

De modo análogo, prova-se que $\text{mdc}(\xi_2, \xi_3) = 1$ e $\text{mdc}(\xi_2, \xi_3) = 1$.

Com efeito, suponha que $\mu \mid \xi_2$ e $\mu \mid \xi_3$. A partir da equação (4.8), obtemos:

$$\omega\lambda\beta = (\alpha + \omega\beta) - (\alpha + \omega^2\beta) = \lambda\xi_2 - \lambda\xi_3 = \lambda(\xi_2 - \xi_3)$$

Assim, $\omega\beta = \xi_2 - \xi_3$ e, como $\mu \mid \xi_2$ e $\mu \mid \xi_3$, tem-se que $\mu \mid \beta$.

Sabemos ainda que:

$$\begin{aligned} (\alpha + \omega^2\beta) - \omega(\alpha + \omega\beta) &= (1 - \omega)\alpha = \lambda\alpha \\ &= \lambda(\xi_3 - \omega\xi_2)\,, \end{aligned}$$

donde conclui-se que $\alpha = \xi_3 - \omega\xi_2$ e, logo, $\mu \mid \alpha$.

Agora, como μ divide α e β e $\text{mdc}(\alpha, \beta) = 1$, segue que μ é inversível e $\text{mdc}(\xi_2, \xi_3) = 1$.

Para o caso $\text{mdc}(\xi_1, \xi_3) = 1$ procedemos da mesma forma. Seja μ tal que $\mu \mid \xi_1$ e $\mu \mid \xi_3$. Pela equação (4.9):

$$\omega^2\lambda\beta = (\alpha + \omega^2\beta) - (\alpha + \beta) = \lambda(\xi_3 - \lambda^{3m-3}\xi_1)$$

logo, $\omega^2\beta = \xi_3 - \lambda^{3m-3}\xi_1$ e, como $\mu \mid \xi_1$ e $\mu \mid \xi_3$, segue que $\mu \mid \beta$.

Além disso,

$$\begin{aligned} (\alpha + \beta) - \omega(\alpha + \omega^2\beta) &= \lambda\alpha \\ &= \lambda(\lambda^{3m-3}\xi_1 - \omega\xi_3), \end{aligned}$$

donde conclui-se que $\alpha = \lambda^{3m-3}\xi_1 - \omega\xi_3$ e, logo, $\mu \mid \alpha$.

Como $\mu \mid \alpha$, $\mu \mid \beta$ e $\text{mdc}(\alpha, \beta) = 1$, temos que μ é inversível e $\text{mdc}(\xi_1, \xi_3) = 1$.

Assim, como ξ_1, ξ_2 e ξ_3 são dois a dois primos entre si, temos que cada um deles está associado a um cubo de modo que:

$$\begin{cases} \alpha + \beta = \lambda^{3m-2}\xi_1 = \varepsilon_1\lambda^{3m-2}\theta^3 \\ \alpha + \omega\beta = \lambda\xi_2 = \varepsilon_2\lambda\phi^3 \\ \alpha + \omega^2\beta = \lambda\xi_3 = \varepsilon_3\lambda\varphi^3 \end{cases}$$

sendo $\varepsilon_1, \varepsilon_2$ e ε_3 elementos inversíveis.Mais ainda, θ, ϕ, φ não possuem fatores em comum e não são divisíveis por λ (caso contrário, teríamos $\lambda \mid \xi_1\xi_2\xi_3$). Logo, lembrando que $\omega = \omega^4$, temos:

$$\begin{aligned} 0 &= (1 + \omega\omega^2)(\alpha + \beta) = (\alpha + \beta) + \omega(\alpha + \omega\beta) + \omega^2(\alpha + \omega^2\beta) \\ &= \varepsilon_1\lambda^{3m-2}\theta^3 + \varepsilon_2\lambda\phi^3 + \varepsilon_3\lambda\varphi^3 \end{aligned}$$

Dividindo a última equação por $\varepsilon_2\omega\lambda$ e fazendo as mudança de variáveis

$$\varepsilon_4 := \frac{\varepsilon_3\omega}{\varepsilon_2} \text{ e } \varepsilon_5 := \frac{\varepsilon_1}{\omega\varepsilon_2},$$

obtemos a equação: $\phi^3 + \varepsilon_4\varphi^3 + \varepsilon_5\lambda^{3m-3}\theta^3 = 0$.

Notemos que, por construção, ε_4 e ε_5 são elementos inversíveis. Além disso, como $m \geq 2$, temos que $\lambda^2 \mid (\phi^3 + \varepsilon_4\varphi^3)$ e, logo, $\phi^3 + \varepsilon_4\varphi^3 \equiv 0 \pmod{\lambda^2}$.

Agora, como $\lambda \nmid \phi$ e $\lambda \nmid \varphi$, aplicando o Lema 4.2.3, temos que $\phi^3 \equiv \pm 1 \pmod{\lambda^4}$ e $\varphi^3 \equiv \pm 1 \pmod{\lambda^4}$. Desse modo, segue que $\phi^3 \equiv \pm 1 \pmod{\lambda^2}$ e $\varphi^3 \equiv \pm 1 \pmod{\lambda^2}$ e, portanto, $\pm 1 \pm \varepsilon_4 \equiv 0 \pmod{\lambda^2}$.

Por outro lado, sabemos que $\varepsilon_4 = \pm 1$, $\varepsilon_4 = \pm\omega$ ou $\varepsilon_4 = \pm\omega^2$ (utilizando o Lema 4.2.2). Mas, como $\pm 1 \pm \omega$ e $\pm 1 \pm \omega^2$ ou são inversíveis ou são associados a λ, não podem ser divisíveis por λ^2. Assim, devemos ter $\varepsilon_4 = \pm 1$.

Caso $\varepsilon_4 = 1$, temos que

$$\phi^3 + \varphi^3 + \varepsilon_5\lambda^{3m-3}\theta^3 = 0 \therefore \phi^3 + \varphi^3 + \varepsilon_5\lambda^{3(m-1)}\theta^3 = 0$$

Caso $\varepsilon_4 = -1$, trocando φ por $-\varphi$, obtemos, também, a equação acima. Em ambos os casos, encontramos uma solução para a equação (4.5) com $n = m - 1$, como queríamos.

Dessa forma, para a prova do Teorema, suponhamos que a equação (4.5) possua solução com $n = m$. Utilizando a *Afirmação 2*, juntamente com argumento indutivo, concluímos que a equação tem solução para $n = m - 1, m - 2, \cdots, 2$ e, finalmente, para $n = 1$. No entanto, pela *Afirmação 1*, dadas as condições iniciais, devemos ter $n \geq 2$, uma contradição. Portanto, a equação (4.5) não tem solução, concluindo a prova. □

Observação 4.2.1. Ainda no início do século XIX, foram apresentadas provas para alguns outras casos particulares do UTF: o caso $n = 5$, provado separadamente por Dirichlet e Legendre, e os casos $n = 7$ e $n = 14$, atribuídos a Dirichlet e Lamé. Tais demonstrações utilizam algumas técnicas semelhantes às utilizadas na prova de Euler para o caso $n = 3$, na medida em que também empregam determinados anéis de inteiros algébricos euclidianos, e podem ser encontradas em Edwards [5].

5 O TEOREMA DE SOPHIE GERMAIN

Apesar do caso $n = 3$ ter sido resolvido por Euler por volta de 1753 (sendo alguns pontos rigorosamente provados por Gauss), ele percebeu que a prova apresentada mostrava-se muito diferente da prova para o caso $n = 4$. Dessa forma, a demonstração para o caso geral parecia um tanto remota.

Neste contexto, Sophie Germain, uma das poucas mulheres a se destacar no meio masculinizado da matemática, dedicou-se a uma nova abordagem para o UTF. Mais ainda, Sophie foi a primeira pessoa que se conhece a ter optado por uma abordagem que permitisse demonstrar o UTF para uma infinidade de expoentes primos e não apenas para casos particulares.

Ainda que suas ideias não tenham proporcionado a prova final do teorema, as mesmas forneceram resultados de grande importância, não apenas para o estudo do Último Teorema de Fermat, como para o desenvolvimento da Teoria dos Números em geral. Historicamente, contudo, ela não recebeu o devido crédito por sua contribuição. Muitos de seus resultados foram atribuídos unicamente a Legendre que, inclusive, em seus trabalhos, reconheceu a importância da abordagem desenvolvida por Sophie para suas conclusões.

Neste capítulo, provaremos alguns dos principais resultados feitos por Sophie durante seu estudo do UTF, os quais se inserem no período entre a demonstração fornecida por Euler e os trabalhos feitos por Kummer.

Antes, porém, apresentaremos brevemente o estudo feito pelos matemáticos Barlow e Abel e a *aplicação φ de Euler*, os quais serão utilizados ao longo da demonstração do Teorema de Sophie Germain.

5.1 AS EQUAÇÕES DE BARLOW E ABEL

Como $\mathbb{Z}$ é um domínio de fatoração única, sabe-se que qualquer inteiro maior que 2 é ou múltiplo de 4 ou múltiplo de algum fator primo ímpar. Dessa forma, a demonstração do UTF se reduz ao caso em que o expoente n é um primo ímpar.

Com efeito, se $n = pm$, em que p é um número primo, temos que:

$$x^n + y^n = z^n \quad \Rightarrow \quad (x^m)^p + (y^m)^p = (z^m)^p$$

Assim, caso a equação à esquerda possua solução, tem-se que a equação seguinte, à direita, também possui. Logo, ao provarmos que a equação fermatiana com expoente primo ímpar p não possui solução, estaremos provando que a mesma não possui solução para qualquer expoente natural maior que 2.

Por outro lado, conforme utilizado nas demonstrações dos casos $n = 3$ e $n = 4$, uma abordagem um tanto natural para se tentar provar o teorema é considerar que exista solução inteira não trivial (x, y, z) para a equação [1]:

$$x^p + y^p + z^p = 0, \tag{5.1}$$

sendo p um primo ímpar.

Utilizando a equação acima, espera-se obter uma contradição, demonstrando, assim, que a equação 5.1 não possui solução não nula em $\mathbb{Z}$.

Observemos que:

$$\begin{aligned} -z^p &= x^p + y^p \\ &= (x+y)(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1}) \end{aligned}$$

Como $x, y,$ e z são inteiros, temos que

$$\frac{x^p + y^p}{x+y} = (x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1}) \tag{5.2}$$

também deve ser um número inteiro.

Tal equação e suas propriedades de divisibilidade foram objetos de estudo de Barlow e Abel no início do século XIX. Primeiramente, eles estidaram a identidade:

$$Q_n(a,b) = \sum_{k=0}^{n-1} a^k(-b)^{n-k-1}$$

em que a, b são inteiros não nulos e n é natural.

De forma semelhante à argumentação inicial, que forneceu a igualdade 5.2, no caso em que $a + b \neq 0$ e n é ímpar, temos que:

$$Q_n(a,b) = (-b)^{n-1} + a(-b)^{n-2} + \cdots + a^{n-2}(-b) + a^{n-1} = \frac{a^n + b^n}{a+b}$$

Assim, considerando x, y e p como na equação fermatiana de expoente p primo ímpar, podemos definir:

$$Q_p(x,y) := \frac{x^p + y^p}{x+y} = (x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1})$$

Nesse contexto, Barlow e Abel estabeleceram várias relações envolvendo os inteiros x, y e z, que se tornaram resultados auxiliares para o estudo do UTF. Estas relações, juntamente às suas respectivas demonstrações, não serão exploradas diretamente em nosso estudo e, portanto, não serão apresentadas. Uma explicação detalhada pode ser encontrada em Ribenboim [13] (p.51 a 54).

[1] Notemos que, a menos de mudança de sinal, ou seja, trocando-se z por $-z$, tal equação de fato equivale à equação fermatiana.

5.2 A FUNÇÃO φ DE EULER

Definição 5.2.1. *A função φ de Euler é uma aplicação que associa a cada natural n a quantidade de naturais menores que n que são relativamente primos a n, ou seja,*

$$\begin{aligned} \varphi : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \varphi(n) = \#\{a \in \mathbb{N} : mdc(a,n) = 1 \text{ e } a \leq n\} \end{aligned}$$

Por convenção, considera-se $\varphi(1) = 1$.

Observação 5.2.1. Notemos que no caso em que p é primo, segue diretamente da definição que $\varphi(p) = p - 1$.

Em geral, $\varphi(p^k) = p^k - p^{k-1}$ para todo $k \in \mathbb{N}$. Com efeito, consideremos a inteiro tal que $1 \leq a \leq n$. Sabemos que $\text{mdc}(a, p^k) = 1$ se, e somente se, a não é múltiplo de p; além disso, há p^{k-1} múltiplos de p no intervalo acima, a saber:

$$p, 2p, \ldots, p^{k-1}p$$

Logo, a quantidade de coprimos com p^k e menores que p^k é exatamente $p^k - p^{k-1}$.

Pode-se provar ainda que, se m e n são inteiros positivos tais que $\text{mdc}(m, n) = 1$, então:

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Esta definição, juntamente com o conceito de *sistema completo de resíduos*, fornece-nos o Teorema de Euler, de grande importância na Teoria dos Números e cujo resultado será utilizado para demonstrar o Teorema de Sophie Germain.

Definição 5.2.2. *Seja $m \in \mathbb{N}$. Um sistema completo de resíduos (SCR) módulo m é uma lista de inteiros $a_1, \ldots, a_m$ dois a dois incongruentes (módulo m). Já um sistema reduzido de resíduos (SRR) módulo m é uma lista de inteiros $r_1, \ldots, r_s$ tais que:*

(*i*) $mdc(r_i, m) = 1 \ \ \forall i = 1, \ldots, s$

(*ii*) $r_i \not\equiv r_j \pmod{m}$ *se* $i \neq j$

(*iii*) *Para cada $n \in \mathbb{Z}$ primo com m, tem-se que $n \equiv r_i \pmod{m}$ para algum $i = 1, \ldots, s$*

Assim, temos:

Teorema 5.2.1 (Teorema de Euler). *Sejam $a, n \in \mathbb{Z}$, com $n > 0$, tais que $mdc(a, n) = 1$, então:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Demonstração. Seja $r_1, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Então, $ar_1, \ldots, ar_{\varphi(m)}$ é também um SRR módulo m para qualquer $a \in \mathbb{N}$ fixado. Temos

$$a^{\varphi(m)} \cdot r_1 \cdots r_{\varphi(m)} = (ar_1) \cdots (ar_{\varphi(m)}) \equiv r_1 \cdots r_{\varphi(m)} \pmod{m}$$

Como para cada $i \in \{1, ..., s\}$, sabemos que r_i é invertível, segue que:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

□

Corolário 5.2.2 (Pequeno Teorema de Fermat). *Seja $a \in \mathbb{Z}$ e p um primo que não divide a. Então:*

$$a^{p-1} \equiv 1 \pmod{p}$$

Notamos que, usando o Pequeno Teorema de Fermat, temos que para todo primo p, independende de p dividir ou não a:

$$a^p \equiv a \pmod{p}$$

Outro corolário Teorema de Euler é:

Corolário 5.2.3. *Seja $q = 2np + 1$ um primo e seja $1 \leq a \leq q - 1$. Então $x^p \equiv a \pmod{q}$ tem solução se, e somente se, $a^{2n} \equiv 1 \pmod{q}$.*

Demonstração. De fato, caso $x^p \equiv a \pmod{q}$ possua solução, temos que $\text{mdc}(a, q) = 1$ e, como $\varphi(q) = 2np$, aplicando o Teorema de Euler, segue o resultado.

Reciprocamente, suponhamos que $a^{2n} \equiv 1 \pmod{q}$. Se $a = 1$, escolhemos $x = 1$. Assim, podemos supor $a \neq 1$. Assim, $a = g^p$ para alguma raiz primitiva módulo q e, como $g^k = 1$ para algum $k \in \mathbb{N}$, temos $k = 2np$. Logo, a é solução para $x^p \equiv a \pmod{q}$. □

5.3 O TEOREMA DE SOPHIE GERMAIN

A partir do estudo inicial apresentado na primeira seção e desenvolvido inicialmente por Sophie, o UTF pode ser dividido em dois casos:

Caso 1: A equação $x^p + y^p = z^p$ não possui soluções inteiras quando nenhum dos elementos x, y e z é divisível por p.

Caso 2: A equação $x^p + y^p = z^p$ não possui soluções inteiras quando apenas um dos elementos x, y e z é divisível por p.

Observemos que os casos acima realmente contemplam todas as possibilidades do UTF, na medida em que, conforme elucidado no capítulo anterior, podemos supor sem perda de generalidade que x, y e z são dois a dois primos entre si.

Antes de apresentar os resultados necessários para a demonstração do Teorema de Sophie Germain (TSG), torna-se essencial a seguinte definição:

Definição 5.3.1. *Seja p um primo ímpar tal que $q := 2np + 1$, com $n \in \mathbb{N}$, é um número primo. Diremos que q é um primo auxiliar (associado a p) se o conjunto de resíduos não nulos $x^p \pmod{q}$, em que $1 \leq x \leq q-1$, não contiver quaisquer classes de resíduos inteiros consecutivas.*

Em outras palavras, consideremos $m \in \mathbb{Z} \setminus \{0, -1\}$. Se m e $m+1$ pertencem a classes consecutivas de resíduos inteiros, então dados quaisquer inteiros não nulos a e b, as condições

$$a^p \equiv m \pmod{q} \text{ e } b^p \equiv m+1 \pmod{q}$$

não podem ser simultaneamente satisfeitas.

Exemplo 5.3.1. Seja $p = 5$. Calcularemos seus primos auxiliares no caso em que $1 \leq n \leq 10$.

Primeiramente, notemos que nos casos em que $n = 2, 5$ ou 8, os valores de q são, respectivamente, $21, 51$ e 81, os quais não são números primos. Portanto, nestes casos, q não é primo auxiliar de 5.

Analisando os demais casos, temos:

- $\underline{n = 1}$: Temos que $q = 2p + 1 = 11$. Assim, devemos observar quais são as classes de resíduos inteiros (módulo 11) para a 5-ésima potência de x, em que $1 \leq x \leq 10$. Neste caso, temos:

$$\begin{aligned} & \left\{1^5, 2^5, 3^5, 4^5, 5^5, 6^5, 7^5, 8^5, 9^5, 10^5\right\} \pmod{11} \\ = \ & \{1, 32, 243, 1024, 3125, 7776, 16807, 32768, 59049, 100000\} \pmod{11} \\ = \ & \{1, 10, 1, 1, 1, 10, 10, 10, 1, 10\} \pmod{11} \\ = \ & \{1, 10\} \pmod{11} \end{aligned}$$

  Como 1 e 10 não são inteiros consecutivos módulo 11, temos que 11 é um primo auxiliar de 5.

- $\underline{n = 3}$: Temos $q = 2 \cdot 3p + 1 = 31$. Analisando apenas as 5 primeiras classes de resíduos inteiros (módulo 31) para a 5-ésima potência de x (sendo $1 \leq x \leq 30$), notamos que há classes consecutivas. De fato tais classes são dadas por:

$$\{1, 1, 26, 1, 25\} \pmod{31}$$

  Assim, $n = 3$ não gera primo auxiliar.

Na verdade, tal resultado é mais geral: considerando qualquer primo ímpar p, é possível mostrar que no caso em que n é um múltiplo de 3, q não é um primo auxiliar de p. A demonstração envolve uma caracterização equivalente para os primos auxiliares, que será enunciada no Lema 5.3.1, e, portanto, será provada em seguida.

Utilizando este resultado, concluímos que nos casos em que $n = 6$ ou 9, os valores $q = 61$ e 91 não são primos auxiliares de 5.

- $\underline{n = 4}$: Temos que $q = 2 \cdot 4p + 1 = 41$. Calculando as as classes de resíduos inteiros (módulo 41) para a 5-ésima potência de x, em que $1 \leq x \leq 40$, nota-se que as mesmas se reduzem a:

$$\{1, 3, 9, 14, 27, 32, 38, 42\} \pmod{41}$$

Desse modo, não há classes de resíduos consecutivas, resultando que 41 é um primo auxiliar de 5.

- $\underline{n = 7 \text{ ou } 10}$: Temos que os valores de q são, respectivamente, 71 e 101. Procedendo de forma semelhante à feita nos casos anteriores, verifica-se que, dentre as classes de resíduos inteiros das respectivas 5-ésimas potências (módulo 71 e 101), não há inteiros consecutivos.

Portanto, 71 e 101 são primos auxiliares de 5.

Consequentemente, conclui-se que, para $p = 5$ e $1 \leq n \leq 10$, os únicos primos auxiliares de 5 são $11, 41, 71$ e 101.

A definição apresentada fornece-nos ainda outra caracterização para os primos auxiliares, a qual será utilizada na prova do TSG (tanto na versão original quanto na versão fraca).

Lema 5.3.1. *Seja p um primo ímpar e x, y, z inteiros não nulos.*
Não existem p-ésimas potências de resíduos inteiros não-nulos e consecutivos módulo q se, e somente se, $x^p + y^p + z^p \equiv 0 \pmod{q}$ resulte em x, y ou $z \equiv 0 \pmod{q}$.

Demonstração. Provaremos cada uma das implicações utilizando sua contrapositiva. ($\Rightarrow$) Suponhamos que $x^p + y^p + z^p \equiv 0 \pmod{q}$ admita solução inteira não trivial mas x, y e $z \not\equiv 0 \pmod{q}$. Assim, a menos de mudança de sinal, temos:

$$x^p + y^p \equiv -z^p = (-z)^p \pmod{q}$$

Multiplicando ambos os lados por $(x^{-1})^p$ segue:

$$1 + (x^{-1}y)^p \equiv -(x^{-1}z)^p \pmod{q}$$

Logo, $x^{-1}y$ e $x^{-1}z$ são tais que suas p-ésimas potências são resíduos inteiros consecutivos, uma contradição.

($\Leftarrow$) Reciprocamente, suponhamos que existam y e z inteiros não nulos tais que

$$y, z \not\equiv 0 \pmod{q} \quad \text{e} \quad z^p \equiv 1 + y^p \pmod{q}$$

Seja g uma raiz primitiva da unidade módulo q. Ao multiplicar a última equivalência acima por g^p, obtemos:

$$g^p + (gy)^p + (-zg)^p \equiv 0 \pmod{q}$$

Dessa forma, conclui-se que a equação $X^p + Y^p + Z^p \equiv 0 \pmod{q}$ possui solução inteira não trivial, sendo que $X, Y, Z \not\equiv 0 \pmod{q}$, contrariando a hipótese. □

Com essa caracterização, prova-se a afirmação feita no Exemplo 5.3.1.

Proposição 5.3.1. *Se p é um primo e $q = 2 \cdot 3kp + 1$, com $k \in \mathbb{N}$, é também primo, então existem x, y e z, não nulos módulo q, tais que $x^p + y^p + z^p \equiv 0 \pmod{q}$.*

Em particular, existem p-ésimas potências de resíduos inteiros não nulos que são consecutivas, ou seja, $q = 2 \cdot 3kp + 1$ não é um primo auxiliar qualquer que seja o natural k.

Demonstração. Como q é primo, sabemos que $\varphi(q) = 2 \cdot 3kp$.

Consideremos g uma raiz primitiva da unidade módulo q. Assim, $g^n \not\equiv 0 \pmod{q}$ para todo $n \in \mathbb{N}$. Como, pelo Teorema de Euler, $|g| = \varphi(q) = 6kp$, podemos definir $m = g^{2kp} \not\equiv 1 \pmod{q}$. Dessa forma, temos que:

$$\begin{aligned} m^3 = g^{6kp} \equiv 1 \pmod{q} \quad &\Rightarrow \quad m^3 - 1 \equiv 0 \pmod{q} \\ &\Rightarrow \quad (m-1)(m^2 + m + 1) \equiv 0 \pmod{q} \end{aligned}$$

Além disso, como $m \not\equiv 1 \pmod{q}$, segue que $m^2 + m + 1 \equiv 0 \pmod{q}$. Logo,

$$g^{4kp} + g^{2kp} + 1 \equiv 0 \pmod{q}$$

Sabe-se ainda que nenhum deses elementos pode ser congruente a 0 módulo q. Assim, pelo Lema anterior, conclui-se que existem p-ésimas potências de resíduos inteiros não nulos que são consecutivas. □

Inicialmente, Sophie pretendia provar que para cada primo ímpar p existiria uma infinidade de primos auxiliares, ou seja, primos que satisfizessem o critério da não consecutividade dos resíduos inteiros não nulos módulo q. Caso isso fosse verdade, dada uma solução inteira não trivial para a equação $x^p + y^p = z^p$, existiria uma infinidade

de primos auxiliares que dividiriam um dos elementos x, y ou z (aplicando o Lema 5.3.1). Mais ainda, caso o conjunto de primos que dividissem x, y ou z fosse infinito, resultaria que infinitos primos dividiriam ao menos um dos elementos x, y ou z, gerando uma contradição com a finitude da fatoração em irredutíveis no anel $\mathbb{Z}$. Consequentemente, estaria provado o UTF para o caso em que o expoente é primo e, portanto, seguiria o caso geral.

No entanto, posteriormente, Sophie notou que para o caso $p = 3$, existem apenas dois primos auxiliares: 7 e 13 (uma demonstração completa pode ser encontrada em Alkalay [1], Proposição 3, p. 5). Dessa forma, sua ideia inicial não poderia ser aplicada a todos os primos.

Ainda assim, o resultado por ela provado solucionou o UTF para uma infinidade de primos que satisfizessem determinadas propriedades, algo que até o momento não havia sido feito.

Teorema 5.3.1 (**Teorema de Sophie Germain**). *Se p é um número primo ímpar e existe um primo auxiliar $q = 2np + 1$, com $n \in \mathbb{N}$, satisfazendo:*

1. *Não existem p-ésimas potências cujas classes não nulas de resíduos módulo q sejam constituídas de inteiros consecutivos.*
2. *p não é congruente a p-ésima potência de nenhum resíduo inteiro módulo q. Em outras palavras, $x^p \equiv p \pmod{q}$ é impossível para todos valores de x com $1 \leq x \leq q - 1$.*

então, em qualquer possível solução inteira não trivial para a equação $x^p + y^p = z^p$, tem-se que p^2 divide um dos elementos x, y ou z.

Em particular, o Caso 1 do Último Teorema de Fermat é verdadeiro para tais valores de p.

Demonstração. Conforme já visto no capítulo anterior, podemos supor, sem perda de generalidade que x, y e z são dois a dois primos entre si.

Utilizando as equações estudadas por Barlow e Abel, apresentadas na seção 5.1, podemos analisar os seguintes pares:

$$\begin{aligned} x + y \quad &\text{e} \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1} \\ z - y \quad &\text{e} \quad z^{p-1} - z^{p-2}y + z^{p-3}y^2 - \cdots - zy^{p-2} + y^{p-1} \\ z - x \quad &\text{e} \quad z^{p-1} - z^{p-2}x + z^{p-3}x^2 - \cdots - zx^{p-2} + x^{p-1} \end{aligned}$$

Afirmação 1: *O único fator comum que cada um desses pares pode ter é p.*

Demonstraremos esta afirmação para o primeiro par. Seja $Q_p(x, y)$ o segundo elemento da primeira linha.

Suponhamos, por absurdo, que algum primo s diferente de p divida o primeiro par. Então, $y \equiv -x \pmod{s}$ e, por substituição direta, obtemos que $Q_p(x, y) \equiv px^{p-1} \pmod{s}$, o qual, por hipótese, deve ser divisível por s. Agora, como s e p são primos distintos, segue que $s \mid x$. Assim, temos que s divide x e $x + y$, ou seja, s é um divisor comum de x e y, gerando uma contradição.

Afirmação 2: *Temos que p divide um dos elementos x, y ou z.*

Com efeito, suponhamos por absurdo que x, y, z e p sejam relativamente primos. Nesse caso, podemos considerar $z = lr, x = hn$ e $y = vm$. Como $x^p + y^p = z^p$ temos:

$$\begin{aligned} x + y = l^p \quad &\text{e} \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1} = r^p \\ z - y = h^p \quad &\text{e} \quad z^{p-1} - z^{p-2}y + z^{p-3}y^2 - \cdots - zy^{p-2} + y^{p-1} = n^p \\ z - x = v^p \quad &\text{e} \quad z^{p-1} - z^{p-2}x + z^{p-3}x^2 - \cdots - zx^{p-2} + x^{p-1} = m^p \end{aligned}$$

Notemos que, pela afirmação anterior, sabemos que para cada um dos pares, o único fator primo possível em comum é p. Tal fato explica porque, por exemplo, $x + y = l^p$ não tem fator r e $Q_p(x, y) = r^p$ não possui o fator l.

Agora, observemos que, pela condição 1 enunciada no teorema, temos que q divide um dos elementos x, y ou z (e apenas um deles, visto que x, y e z são dois a dois primos entre si). Sem perda de generalidade, consideremos que q divide z.

Desse modo, $q \mid 2z$ e, por definição,

$$2z = (z - y) + (z - x) + (x + y) = h^p + v^p + l^p \equiv 0 \pmod{q}$$

Novamente pela caracterização de primos auxiliares (estabelecida no Lema 5.3.1) e pela condição 1 do teorema, temos que q divide um dos elementos l, h ou v. Vejamos cada um dos casos.

Se q divide h, usando que $q \mid z$ e que $z - y = h^p$, temos que q divide y; de modo semelhante, se q divide v, como $q \mid z$, então devemos ter $q \mid x$ pela equação $z - x = v^p$. Em ambos os casos, contrariamos a hipótese de que x, y e z são primos entre si. Logo, segue que q divide l.

Como $x + y = l^p$ e $q \mid l$, segue que $y \equiv -x \pmod{q}$. Consequentemente, teremos:

$$Q_p(x, y) \equiv px^{p-1} \equiv r^p \pmod{q}.$$

Além disso, como $q \mid z$, temos que:

$$z - x = v^p \equiv -x \pmod{q}$$

Ou seja, x é uma p-ésima potência módulo q. Utilizando as duas últimas equivalências, obtemos:

$$px^{p-1} \equiv p(-v^p)^{p-1} \equiv p(v^{p-1})^p \equiv r^p \pmod{q}$$

Como q não divide x, devemos ter $p \equiv r^p \pmod{q}$, isto é, p é uma p-ésima potência de um inteiro módulo q. No entanto, isso contradiz a condição 2 do teorema.

Portanto, necessariamente, temos que p divide um dos inteiros x, y ou z.

A partir desse momento, iremos supor, sem perda de generalidade que p divide z (note que a suposição que fizemos de que q dividiria z vale apenas para a prova da *Afirmação 2*; aqui, ela não é necessariamente verdadeira).

Seja $z = lrp$. Como x e y são relativamente primos com p, podemos escrever $x = hn$ e $y = vm$. Afirmamos que

$$x + y = l^p p^{p-1} \quad \text{e} \quad x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots - xy^{p-2} + y^{p-1} = pr^p$$

Primeiramente, observemos que $z^p = (x + y) \cdot Q_p(x, y)$ é divisível por p^p; assim, é suficiente mostrarmos que $Q_p(x, y)$ é divisível por p mas não por p^k qualquer que seja o natural $k > 1$.

Sabemos que

$$Q_p(x, y) = \frac{x^p + y^p}{x + y}$$

Definindo $s := x + y$, temos:

$$Q_p(x, y) = \frac{(s - x)^p + x^p}{s} = s^{p-1} - \binom{p}{1} s^{p-2}x + \cdots - \binom{p}{p-2} sx^{p-2} + \binom{p}{p-1} x^{p-1}$$

Além disso, pelo Pequeno Teorema de Fermat, segue que $s = x + y \equiv x^p + y^p \equiv z^p \pmod{q}$, donde p divide s. Desse modo, todos os termos, com exceção do último, são divisíveis por p^2. De fato, o último termo é divisível exatamente por p, uma vez que $\text{mdc}(x, p) = 1$. Portanto, $Q_p(x, y)$ é divisível exatamente pela primeira potência de p.

Por outro lado, de forma semelhante à afirmação 2, temos $z - y = h^p$ e $z - x = v^p$, donde

$$2z - (x + y) = 2z - x - y = h^p - v^p$$

Logo, p divide $h^p + v^p$, pois p divide $s = x + y$ e p divide z. Aplicando novamente o Pequeno Teorema de Fermat, temos que p divide $h + v$. Assim, $h \equiv -v \pmod{q}$, donde existe $m \in \mathbb{Z}$ tal que $h = -v + mp$. Consequentemente:

$$h^p = (-v + mp)^p = -v^p + v^{p-1}p^2m - \cdots + (mp)^p \equiv -v^p \pmod{q}$$

Agora, conforme mostrado anteriormente, $x + y = l^p p^{p-1}$, ou seja, $p^2 \mid (x + y)$.

Portanto, como $2z = (h^p + v^p) + (x + y)$ e p^2 divide ambas as parcelas, segue que p^2 divide z. □

Observação 5.3.1. Notemos que, pelo resultado estabelecido na Proposição 5.3.1, a condição 1 do Teorema de Sophie Germain não vale para os valores de q da forma $6kp+1$ em que $k, p \in \mathbb{N}$ e p é um primo ímpar.

Embora o Teorema anterior seja a versão original feita por Sophie Germain, é comum que o resultado a ela atribuído seja enunciado em sua versão mais fraca, como se segue:

Teorema 5.3.2. *Sejam x, y e z inteiros não nulos e p primo ímpar tais que a equação $x^p + y^p = z^p$ seja satisfeita e $q = 2p + 1$ seja também um número primo. Então, p divide um dos elementos x, y ou z. Consequentemente, o Caso 1 do Último Teorema de Fermat é verdadeiro para estes valores de p.*

Demonstração. Para esta demonstração, basta mostrar que sendo p primo ímpar tal que $q = 2p + 1$ é também primo, as condições 1 e 2 do Teorema de Sophie Germain são satisfeitas.

Como q é primo, temos $\varphi(q) = q-1 = 2p$. Assim, utilizando o Pequeno Teorema de Fermat, dado $a \in \mathbb{Z}$ tal que $\text{mdc}(a, q) = 1$, segue que $a^{2p} = (a^p)^2 \equiv 1 \pmod{q}$. Utilizando novamente que q é primo, resulta:

$$\begin{aligned} a^{2p} - 1 \equiv 0 \pmod{q} \quad &\Rightarrow \quad (a^p - 1)(a^p + 1) \equiv 0 \pmod{q} \\ &\Rightarrow \quad a^p \equiv 1 \pmod{q} \text{ ou } a^p \equiv 1 \pmod{q} \end{aligned}$$

Desse modo, como $x^p \equiv \pm 1 \pmod{q}$, é impossível que tenhamos $x^p \equiv p \pmod{q}$. Então, a condição 2 do Teorema de Sophie é satisfeita.

Para verificar que a condição 1 também é válida, usaremos o Lema 5.3.1. De fato, caso x, y e $z \not\equiv 0 \pmod{q}$, segue que:

$$x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1 \not\equiv 0 \pmod{q}$$

Então, a fim de que a relação $x^p + y^p + z^p \equiv 0 \pmod{q}$ seja verdadeira, deve-se ter um dos inteiros x, y ou z congruentes a 0 módulo q.

Logo, a condição 1 se verifica. □

Observação 5.3.2. Uma vez que a versão mais fraca tornou-se mais conhecida, um primo p tal que $2p + 1$ seja também primo é denominado *primo de Sophie Germain.*

Cabe ressaltar que Sophie provou resultados mais fortes que o enunciado acima. Em seus trabalhos, ela provou, por exemplo, que se $x^p \not\equiv 2 \pmod{q}$, então, para todo inteiro x e todo primo auxiliar q da forma $4p + 1, 8p + 1, 10p + 1, 14p + 1$ ou $16p + 1$, a condição 1 de seu teorema (na versão original) seria válida.

Sophie também verificou alguns dos casos em que x fosse um inteiro tal que $x^p \equiv 2 \pmod{q}$. Considerando as situações em que $p \leq 100$, ela encontrou os primos auxiliares da forma $2np + 1$ com $1 \leq n \leq 10$ que verificavam a condição 1. Mais ainda, ela mostrou que todos esses primos auxiliares verificavam também a condição 2. Dessa forma, provou o UTF para vários primos menores que 100. Tal estudo destaca-se não apenas pelo resultado que proporciona, como mostra-se ainda mais significante se considerarmos que sistemas computacionais algébricos só seriam criados 175 anos depois. Esse resultado é muitas vezes atribuído somente a Legendre, responsável por sua publicação. Entretanto, aparece no trabalho de ambos, tendo se desenvolvido independentemente e por meio de técnicas distintas. Legendre, por exemplo, provou um resultado que impossibilitava a aplicação do Teorema de Sophie Germain. Segundo seus estudos, no caso em que p fosse um primo tal que os números da forma $4p + 1, 8p + 1, 10p + 1, 14p + 1$ ou $16p + 1$ também fossem primos, então as condições 1 e 2 do teorema em questão não seriam satisfeitas.

Por meio do estudo de ambos, foram encontrados alguns dos primos auxiliares para os naturais entre 1 e 197. A tabela 1 apresenta, para cada primo menor que 197, o primeiro primo auxiliar encontrado que satisfaz as condições do Teorema de Sophie Germain. Os primos em destaque correspondem aos primos de Sophie Germain.

p	θ=kp+1	k	p	θ=kp+1	k	p	θ=kp+1	k	p	θ=kp+1	k
3	7	2	5	11	2	7	29	4	11	23	2
13	53	4	17	137	8	19	191	10	23	47	2
29	59	2	31	311	10	37	149	4	41	83	2
43	173	4	47	659	14	53	107	2	59	827	14
61	977	16	67	269	4	71	569	8	73	293	4
79	317	4	83	167	2	89	179	2	97	389	4
101	809	8	103	1031	10	107	857	8	109	1091	10
113	227	2	127	509	4	131	263	2	137	1097	8
139	557	4	149	1193	8	151	1511	10	157	1571	10
163	653	4	167	2339	14	173	347	2	179	359	2
181	1811	10	191	383	2	193	773	4	197	7487	38

Tabela 1 – Primos auxiliares que satisfazem o Teorema de Sophie Gemain [14]

Notemos que tal tabela mostra o motivo de Sophie e Legendre não terem continuado seus cálculos para os primos maiores que 197. Com efeito, para 197, o primeiro primo auxiliar que satisfaz as condições do teorema é 7487 e, para a verificação de tal fato, já era necessário lidar com números muito grandes. Dessa forma, para os primos maiores, seria um trabalho extremamente árduo.

6 O TEOREMA DE KUMMER

Apesar dos avanços para casos particulares, no início do século XIX, a prova para o caso geral do UTF permanecia remota. Em 1847, no entanto, Lamé anunciou ter provado totalmente o UTF. Contudo, os matemáticos Liouville e Kummer perceberam que sua tentativa dependia diretamente da existência e da unicidade de fatoração de elementos em irredutíveis dentro de anéis específicos, denominados *anéis de inteiros ciclotômicos*. Entretanto, conforme Kummer provara anos antes, a unicidade de tal fatoração não era verdadeira para todos anéis desse formato, o que inviabilizava a demonstração completa do Último Teorema de Fermat. Ainda assim, era possível reestruturar a abordagem utilizada por Lamé de modo a demonstrar o UTF para certos primos, o que foi feito por Kummer.

Neste último capítulo, portanto, apresentaremos a abordagem inicial adotada por Lamé, mostrando o porquê de a mesma não ser suficiente para a prova do UTF. Além disso, apresentaremos a generalização feita por Dedekind para os chamados *números ideais* de Kummer, em que mostrou-se válida a unicidade da fatoração. Por fim, por meio do aprofundamento de alguns conceitos inerentes ao estudo elaborado por Kummer, provaremos o teorema a ele atribuído.

6.1 A TENTATIVA DE LAMÉ

Estudando as provas dos casos $p = 3, 4, 5$ e 7, Lamé notou que, em todas, a ideia central envolvia a fatoração algébrica da expressão $x^p + y^p$. Assim, no esboço de sua possível prova, ele introduziu o conceito de *raízes n-ésimas da unidade* a fim de obter uma fatoração em termos lineares para a equação $x^p + y^p = z^p$.

Definição 6.1.1. *Seja n natural. Dizemos que ζ_n é uma n-ésima raiz da unidade se $\zeta_n^n = 1$. No caso em que $\zeta_n^m = 1$ e $m \in \{1, \ldots, n-1\}$, dizemos ainda que ζ_n é uma n-ésima raiz primitiva da unidade.*

Restringindo-se à análise das p-ésimas raízes da unidade, Lamé obteve a seguinte decomposição:

$$x^p + y^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdots (x + \zeta_p^{p-1} y) \tag{6.1}$$

sendo $\zeta_p = e^{\frac{2\pi i}{p}}$ e p um primo ímpar.

Para demonstrar tal igualdade, realizou uma mudança de variáveis, trocando y por $-y$ e analisou a expressão $x^p - y^p$ como sendo um polinômio na variável x e coeficientes em $\mathbb{C}[y]$, ou seja, um polinômio em $\mathbb{C}[y][x]$. Esta última equação tem solução quando $x^p = y^p$ e, como ζ_p é uma p-ésima raiz da unidade, tal condição é equivalente a

$$x = \zeta_p^k y \ \text{, em que } \ 0 \leq k \leq p-1$$

Desse modo, $x^p - y^p$ é divisível por $x - \zeta_p^k y$ para cada valor de k pertencente ao intervalo acima. Logo, é divisível pelo produto:

$$(x-y)(x-\zeta_p y)\cdots(x-\zeta_p^{p-1}y)$$

Por outro lado, este produto tem grau p e o coeficiente de maior grau é 1, tal como o polinômio $x^p - y^p$, garantindo a igualdade em (6.1). Notemos que, desse modo, obtivemos uma fatoração para a expressão $x^p + y^p$ no anel $\mathbb{Z}[\zeta_p]$.

Além disso, como já foi mostrado, podemos supor, sem perda de generalidade, que $\text{mdc}(x, y, z) = 1$. Neste caso, Lamé afirmou ainda ser possível considerar que os fatores presentes na decomposição apresentada em (6.1) são dois a dois primos entre si. De fato, temos a seguinte Proposição:

Proposição 6.1.1. *Suponhamos que, dado p número primo, a equação fermatiana possua solução inteira* (x, y, z) *com* $mdc(x, y, z) = 1$. *Neste caso, podemos supor que a decomposição*

$$x^p + y^p = z^p = (x+y)(x+\zeta_p y)(x+\zeta_p^2 y)\cdots(x+\zeta_p^{p-1}y)$$

é tal que seus fatores são dois a dois primos entre si.

Demonstração. Sabemos que a igualdade acima é verdadeira, conforme argumentamos anteriormente. Quanto à demonstração de que seus fatores podem ser considerados dois a dois primos entre si, apresentaremos uma prova por redução ao absurdo.

Suponhamos, por absurdo, que existam $a, b \in \{0, ..., p-1\}$ tais que os fatores $x + \zeta_p^a y$ e $x + \zeta_p^b y$ não sejam relativamente primos.

Assim, existe um fator inteiro primo m que divide ambos. Ou seja, existem $k_a, k_b \in \mathbb{Z}$ tais que:

$$x + \zeta_p^a y = mk_a \quad \text{e} \quad x + \zeta_p^b y = mk_b$$

Subtraindo estes fatores, obtemos que

$$\zeta_p^a y - \zeta_p^b y = mk_a - mk_b \quad \therefore \quad y(\zeta_p^a - \zeta_p^b) = m(k_a - k_b)$$

Agora, como m é um número primo, segue que $m \mid y$ ou $m \mid \zeta_p^a - \zeta_p^b$.

Caso m divida y, como m divide $x + \zeta_p^a y$, temos que m dividirá também x, contradizendo a hipótese inicial de que x e y são relativamente primos.

Consideremos, então, que m divide $\zeta_p^a - \zeta_p^b$. Sem perda de generalidade, podemos supor $a > b$. Assim, como

$$\zeta_p^a - \zeta_p^b = -\zeta_p^b(1 - \zeta_p^{a-b}),$$

resulta que

$$m \mid \zeta_p^b(1 - \zeta^{a-b}) \tag{6.2}$$

Ora, sabemos que ζ_p é uma p-ésima raiz da unidade, isto é, $(\zeta_p)^p = 1$. Assim, como m é um número primo, não é possível que m divida ζ_p^b.

Com efeito, tal potência será divisível apenas pelas potências de ζ cujos expoentes sejam menores ou iguais a b e pelas unidades de $\mathbb{Z}[\zeta_p]$. No entanto, pela primalidade de m, o mesmo não poderia ser uma unidade. Além disso, observemos que, se m dividisse ζ_p ou uma de suas potências (neste caso, menores ou iguais a b-ésima potência), em particular teríamos que m dividiria as partes real e imaginária de tais números. Entretanto, como p é primo ímpar, qualquer potência de ζ_p terá módulo no máximo igual a 1 (no caso em que $b = p$), implicando que m será sempre estritamente maior que cada uma das partes, real e imaginária, da potência de ζ em questão. Logo, m não divide nenhuma potência de ζ_p.

Portanto, pela equação (6.2), como m é primo e $m \nmid \zeta_p^b$, obrigatoriamente devemos ter que $m \mid 1 - \zeta^{a-b}$.

Mas, como consideramos que $a > b$, temos que $0 < 1 - \zeta^{a-b} < 1$, resultando que m não divide $1 - \zeta_p^{a-b}$.

Por fim, como em ambos os casos possíveis, obtivemos uma contardição, concluímos que não podem existir dois elementos na fatoração (6.1) os quais não sejam relativamente primos. □

Com essa abordagem, segundo Lamé, a igualdade:

$$z^p = (x + y)(x + \zeta_p y)(x + {\zeta_p}^2 y) \cdots (x + {\zeta_p}^{p-1} y) \tag{6.3}$$

deveria implicar que existiriam $\tau_1, \ldots, \tau_{p-1} \in \mathbb{Z}[\zeta]$ tais que:

$$\begin{aligned} x + y &= \tau_1^p \\ x + \zeta_p y &= \tau_2^p \\ &\vdots \\ x + {\zeta_p}^{p-1} y &= \tau_{p-1}^p \end{aligned}$$

Dessa forma, ele pretendia gerar uma descida infinita nos naturais, demonstrando o UTF. No entanto, sua ideia apresentava um problema, o qual foi notado por Liouville (que também participara de alguns dos resultados provados): como garantir que cada fator $x + \zeta_p^k$ seria uma p-ésima potência sabendo apenas que os fatores eram relativamente primos e o seu produto resultava em uma p-ésima potência?

Com efeito, a ideia de Lamé seria válida caso os fatores envolvidos fossem inteiros, contudo, como a fatoração fora feita sobre o anel $\mathbb{Z}[\zeta_p]$, era preciso assegurar a unicidade da fatoração apresentada na equação (6.3), o que, como foi provado mais tarde, não é verdade para qualquer primo ímpar p. De outro modo, caso houvesse outra

decomposição em $\mathbb{Z}[\zeta_p]$ para z^p, não seria necessário que cada fator $x + \zeta_p^k y$ fosse uma p-ésima potência.

Nesse cenário, poucos meses após o anúncio feito por Lamé, o matemático polonês Kummer enviou uma carta a Liouville com trabalhos anteriores seus os quais provavam que a unicidade da fatoração não era válida nos casos utilizados por Lamé. Contudo, Kummer concluía dizendo que a ideia poderia ser ainda utilizada, por meio da introdução de um conceito criado por ele, o de *números ideais*.

Antes de apresentarmos esta definição, porém, necessitaremos estudar os chamados *corpos ciclotômicos* e suas principais propriedades.

6.2 CORPOS CICLOTÔMICOS

Em seu estudo, Kummer percebeu que seria apropriado considerar os números complexos obtidos a partir de ζ_p e dos números racionais por meio da soma e da multiplicação usuais. Logo, fixado p primo ímpar, e sendo ζ_p uma raiz imaginária pura (ou seja, não real) da equação $x^p = 1$, consideraria os números da forma:

$$a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-2}, \tag{6.4}$$

em que $a_i \in \mathbb{Z}$ para todo $i \in \{0, \ldots, p-2\}$.

Observação 6.2.1. Em alguns livros, a equação acima é representada com o acréscimo de uma parcela do tipo $a_{p-1}\zeta_p^{p-1}$, com $a_{p-1} \in \mathbb{Z}$. No entanto, esse acréscimo não é necessário, visto que $\zeta_p^p = 1$ e $\zeta_p \neq 1$, donde resulta a relação:

$$1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0$$

Dessa forma, parcelas que envolvam ζ_p^{p-1} podem ser expressas, através da igualdade acima, em função das potências menores de ζ_p.

Nessas circunstâncias, torna-se necessário definir uma nova estrutura algébrica, em que os elementos têm o formato representado na equação (6.4). Esta estrutura, denominada *corpo ciclotômico*, juntamente com suas principais propriedades, será objeto de estudo desta seção.

6.2.1 **Caracterização**

Definição 6.2.1. *Seja ζ_n uma n-ésima raiz da unidade. O corpo $\mathbb{Q}(\zeta_n)$ é denominado n-ésimo corpo ciclotômico.*

Observação 6.2.2. A denominação acima deve-se à interpretação geométrica de ζ_n, pois trata-se de um ponto do círculo $|z| = 1$ do plano complexo z. Mais ainda, tais raízes dividem este círculo em exatamente n partes iguais.

A partir desse momento, a fim de simplificar as notações, sempre que utilizarmos ζ, estaremos nos referindo especificamente à p-ésima raiz da unidade (que anteriormente denotamos por ζ_p), sendo p um primo ímpar. Assim, fixado p primo ímpar, temos $\zeta := e^{\frac{2\pi i}{p}}$. Sob essas condições, denominaremos o corpo $\mathbb{Q}(\zeta)$ como *corpo ciclotômico*. Para melhor caracterizá-lo, apresentaremos o polinômio minimal de ζ, chamado *polinômio ciclotômico*.

Proposição 6.2.1. *O polinômio minimal de ζ sobre $\mathbb{Q}$ é*

$$P_\zeta(x) := 1 + x + \cdots + x^{p-2} + x^{p-1}$$

Em particular, $\deg P_\zeta(x) = p - 1$ *e* $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$.

Demonstração. Sabemos que ζ satisfaz a equação $\zeta^p = 1$ e que $\zeta \neq 1$. Por outro lado,

$$\zeta^p - 1 = (\zeta - 1)(1 + \zeta + \cdots + \zeta^{p-2} + \zeta^{p-1})$$

Assim, é imediato que ζ anula o polinômio mônico $P_\zeta(x) \in \mathbb{Q}$. Agora, utilizando o Critério de Eisenstein, provaremos que $P_\zeta(x)$ é irredutível.

Primeiramente, observemos que um polinômio $f(x)$ é irredutível em $\mathbb{Q}[x]$ se, e somente se, $f(x + c)$ é irredutível em $\mathbb{Q}[x]$, sendo c inteiro.

Assim, basta provar que $P_\zeta(x + 1)$ é irrredutível sobre $\mathbb{Q}[x]$ e, consequentemente estará provado que $P_\zeta(x)$ é irredutível. Desenvolvendo o polinômio $P_\zeta(x + 1)$ pelo Binômio de Newton, temos que:

$$P_\zeta(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{p-1} x^{p-2} + \binom{p}{p-2} x^{p-3} + \cdots + \binom{p}{2} x + \binom{p}{1}$$

Dessa forma, $P_\zeta(x + 1)$ é um polinômio mônico cujos coeficientes, exceto o de maior grau, são divisíveis por p. De fato, dado $k \in \{1, \ldots, p - 1\}$, sabemos que:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

é um número natural.

Assim, $k!$ divide o produto $p(p - 1) \cdots (p - k + 1)$. Mas, como $k!$ é um produto de fatores menores que p e como p é primo, temos que $k!$ não divide p. Desse modo, p dividirá tal coeficiente qualquer que seja o natural $k \in \{1, \ldots, p - 1\}$. Além disso, $p^2 \nmid p$, em que p é o coeficiente independente. Logo, aplicando o Critério de Eisenstein, obtemos que $P_\zeta(x + 1)$ é irredutível; consequentemente, $P_\zeta(x)$ é irredutível. □

Corolário 6.2.1. *O corpo ciclotômico $\mathbb{Q}(\zeta)$ é dado por:*

$$\mathbb{Q}(\zeta) = \left\{ q_0 + q_1\zeta + q_2\zeta^2 + \cdots + q_{p-2}\zeta^{p-2} : \ q_i \in \mathbb{Q} \ \textit{para todo} \ \ i = 0, \ldots, p-2 \right\}$$

Demonstração. Pela proposição anterior, sabemos que o grau do polinômio minimal de ζ sobre $\mathbb{Q}$ é $p-1$. Além disso, dados $a, b \in \mathbb{N}$, $a \neq b$, tais que $a, b = 0, \ldots, p-2$, temos que $\zeta^a \neq \zeta^b$. Assim, $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ constitui uma base para $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$, implicando que qualquer elemento α de $\mathbb{Q}(\zeta)$ pode ser representado como:

$$\alpha = q_0 + q_1\zeta + q_2\zeta^2 + \cdots + q_{p-2}\zeta^{p-2},$$

em que $q_i \in \mathbb{Q}$ para todo $i = 0, \ldots, p-2$.

Desse modo, α pode ser visto como o valor de um polinômio com coeficientes em $\mathbb{Q}$ aplicado em ζ, resultando em:

$$\begin{aligned} \mathbb{Q}(\zeta) &= \{f(\zeta) : f(x) \in \mathbb{Q}[x]\} \\ &= \left\{q_0 + q_1\zeta + q_2\zeta^2 + \cdots + q_{p-2}\zeta^{p-2} : \ q_i \in \mathbb{Q} \ \text{ para todo } \ i = 0, \ldots, p-2\right\}. \end{aligned}$$

□

Observação 6.2.3. Seguindo a abordagem de Lamé, utilizada para a decomposição da equação $x^p + y^p = z^p$ em função de p-ésimas raízes da unidade e apresentada na seção anterior, pode-se reescrever o polinômio minimal de ζ como sendo:

$$\begin{aligned} P_\zeta(x) &= 1 + x + x^2 + \cdots + x^{p-1} \\ &= (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1}) \end{aligned}$$

De maneira simplificada temos, portanto, que:

$$P_\zeta(x) = \prod_{i=1}^{p-1}(x - \zeta^i)$$

Essa caracterização do corpo ciclotômico nos fornece um resultado análogo a uma relação já conhecida, segundo a qual $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$.

Proposição 6.2.2. *O corpo de frações de $\mathbb{Z}[\zeta]$ é igual a $\mathbb{Q}(\zeta)$.*

Demonstração. Pela proposição anterior, sabemos que

$$\mathbb{Z}[\zeta] = \left\{a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2} : \ a_i \in \mathbb{Z} \ \text{ para todo } \ i = 0, \ldots, p-2\right\}$$

Assim, é imediato que $\mathbb{Z}[\zeta] \subseteq \mathbb{Q}(\zeta)$.

Consideremos $\mathbb{K}$ o corpo de fração de $\mathbb{Z}[\zeta]$, ou seja,

$$\mathbb{K} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}[\zeta]\right\}$$

Tomemos $x \in \mathbb{Q}(\zeta)$. Como $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, segue que:

$$x = \frac{a_0}{b_0} + \frac{a_1}{b_1}\,\zeta + \frac{a_2}{b_2}\,\zeta^2 + \cdots + \frac{a_{p-2}}{b_{p-2}}\,\zeta^{p-2}$$

em que $a_i, b_i \in \mathbb{Z}$ para todo $i = 0, \ldots, p-2$.

Desse modo,

$$x = \frac{a_0 b_1 \cdots b_{p-2} + a_1 b_0 b_2 \cdots b_{p-2}\zeta + a_2 b_0 b_1 b_3 \cdots b_{p-2}\zeta^2 + \cdots + a_{p-2} b_0 \cdots b_{p-2}\zeta^{p-2}}{b_0 b_1 \cdots b_{p-2}}$$

resultando que $x \in \mathbb{K}$.

Como x foi escolhido de forma arbitrária em $\mathbb{Q}(\zeta)$, concluímos que $\mathbb{Q}(\zeta) \subseteq \mathbb{K}$. Então,

$$\mathbb{Z}[\zeta] \subseteq \mathbb{Q}(\zeta) \subseteq \mathbb{K}$$

Por outro lado, caso $x \in \mathbb{K}$, por definição, temos que existem $a, b \in \mathbb{Z}[\zeta]$ com $b \neq 0$ tais que $x = \frac{a}{b}$. Agora, como b é invertível e $a, b \in \mathbb{Z}[\zeta] \subseteq \mathbb{Q}(\zeta)$, sendo $\mathbb{Q}(\zeta)$ corpo, obtemos que:

$$x = \frac{a}{b} = ab^{-1} \in \mathbb{Q}(\zeta)$$

Portanto $\mathbb{K} \subseteq \mathbb{Q}$, implicando que $\mathbb{K} = \mathbb{Q}(\zeta)$. □

6.2.2 **Norma e Traço**

Com o intuito de melhor caracterizar o anel de inteiros $\mathcal{O}_{\mathbb{Q}(\zeta)}$ do corpo $\mathbb{Q}(\zeta)$, apresentaremos as definições de *norma* e *traço* para corpos da forma $\mathbb{L} = \mathbb{Q}(\Theta)$ e, em seguida, exemplificaremos tais conceitos no caso dos corpos ciclotômicos. Estas definições também serão utilizadas nas próximas seções para a demonstração de resultados auxiliares ao Teorema de Kummer.

Definição 6.2.2. *Seja $\mathbb{L} = \mathbb{Q}(\Theta)$ extensão finita de $\mathbb{Q}$. Uma imersão $\sigma : \mathbb{L} \hookrightarrow \mathbb{C}$ é uma função injetora que preserva soma e produto de elementos em $\mathbb{L}$, ou seja, dados $\alpha, \beta \in \mathbb{L}$, tem-se que:*

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) \quad e \quad \sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta)$$

Em outras palavras, σ é um homomorfismo injetivo entre corpos.

Observação 6.2.4. Relembramos que, como σ é um homomorfismo, então $\sigma(1) = 1$, donde segue por indução que $\sigma(n) = n$ para todo $n \in \mathbb{N}$. Podemos provar ainda que $\sigma(n) = n$ quando $n \in \mathbb{Z}$, e, consequentemente, temos que $\sigma(q) = q$ para todo $q \in \mathbb{Q}$.

Definição 6.2.3. *Seja $\mathbb{L} \supset \mathbb{Q}$ uma extensão de corpos e seja $\alpha \in \mathbb{L}$ um número algébrico sobre $\mathbb{Q}$, cujo polinômio minimal seja dado por $p(x) \in \mathbb{Q}[x]$. Dizemos que as raízes de $p(x)$ em $\mathbb{L}$ são conjugados de α.*

Observação 6.2.5. Daqui em diante, salvo em menção contrária, sempre que nos referirmos aos conjugados de α, estaremos considerando a definição acima.

Teorema 6.2.2. *Seja* $\mathbb{L} = \mathbb{Q}(\Theta)$ *um corpo de grau n sobre* $\mathbb{Q}$*, ou seja, tal que* $[\mathbb{L} : \mathbb{Q}] = n$*. Então existem exatamente n imersões distintas* $\sigma_i : \mathbb{L} \to \mathbb{C}$*,* $i = 1, \ldots, n$*. Mais ainda,* $\sigma_i(\Theta) = \Theta_i$ *são as raízes em* $\mathbb{C}$ *do polinômio minimal de* Θ *sobre* $\mathbb{Q}$*, ou seja, os conjugados de* Θ *sobre* $\mathbb{Q}$*.*

Demonstração. Seja $\sigma : \mathbb{L} \hookrightarrow \mathbb{C}$ uma imersão.

Observemos que para qualquer polinômio $p(x) \in \mathbb{Q}[x]$, temos que $\sigma(p(\Theta)) = p(\sigma(\Theta))$. Com efeito, consideremos

$$p(x) = q_m x^m + q_{m-1} x^{m-1} + \cdots + q_1 x + q_0 \in \mathbb{Q}[x]$$

Utilizando que σ é um homomorfismo e $q_i \in \mathbb{Q}$ para todo $i = 0, \ldots, m$, segue que:

$$\begin{aligned} \sigma(p(\Theta)) &= \sigma(q_m x^m + q_{m-1} x^{m-1} + \cdots + q_1 x + q_0) \\ &= q_{m-1}\sigma(\Theta)^m + q_{m-1}\sigma(\Theta)^{m-1} + \cdots + q_1\sigma(\Theta) + q_0 \\ &= p(\sigma(\Theta)) \end{aligned}$$

implicando que σ é unicamente determinado pelo valor de $\sigma(\Theta)$.

Por outro lado, sabemos que $p(x)$ é o polinômio minimal de Θ sobre $\mathbb{Q}$, ou seja,

$$p(\Theta) = 0 \Rightarrow \sigma(p(\Theta)) = \sigma(0) = 0 \Rightarrow p(\sigma(\Theta)) = 0$$

Desse modo, $\sigma(\Theta)$ só pode ser uma das raízes de $p(x)$ e, então, há no máximo $n = \deg p(x)$ imersões $\sigma : \mathbb{L} \hookrightarrow \mathbb{C}$.

Portanto, resta-nos mostrar que, para cada conjugado Θ_i de Θ, com $i \in \mathbb{N}$, (sobre $\mathbb{Q}$), é possível definir uma imersão tal que $\sigma(\Theta) = \Theta_i$ e que há exatamente n conjugados Θ_i em $\mathbb{C}$.

Conforme já visto, sabemos que $\left\{1, \Theta, \Theta^2, \ldots, \Theta^{n-1}\right\}$ constitui uma base de $\mathbb{L}$ sobre $\mathbb{Q}$, donde dado um elemento $\alpha \in \mathbb{L}$, ele tem a forma

$$\alpha = a_0 + a_1\Theta + \cdots + a_{n-1}\Theta^{n-1}, \text{ em que } a_i \in \mathbb{Q} \text{ sempre que } i = 0, \ldots, n-1$$

Assim, para cada i, definimos σ_i como sendo a aplicação $\sigma : \mathbb{L} \hookrightarrow \mathbb{C}$ dada por:

$$\sigma_i(a_0 + a_1\Theta + \cdots + a_{n-1}\Theta^{n-1}) = a_0 + a_1\Theta_i + \cdots + a_{n-1}\Theta_i^{n-1}$$

Neste caso, é imediato que cada σ_i preserva a soma. Para a demonstração de que σ_i preserva o produto, consideremos $\alpha, \beta \in \mathbb{L}$ tais que:

$$\begin{aligned} \alpha &= a_0 + a_1\Theta + \cdots + a_{n-1}\Theta^{n-1} \\ \beta &= b_0 + b_1\Theta + \cdots + b_{n-1}\Theta^{n-1} \\ \alpha \cdot \beta &= c_0 + c_1\Theta + \cdots + c_{n-1}\Theta^{n-1} \end{aligned}$$

em que $a_i, b_i, c_i \in \mathbb{Q}$ para todo $i = 0, \ldots, n-1$.

Nessas condições, tomando $f(x)$ como o polinômio em $\mathbb{Q}[x]$ dado por:

$$f(x) = (a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) \cdot (b_0 + b_1x + \cdots + b_{n-1}x^{n-1}) - (c_0 + c_1x + \cdots + c_{n-1}x^{n-1}),$$

temos que $f(x)$ anula Θ.

Por outro lado, sabemos que se $g(x) \in \mathbb{Q}[x]$ é um polinômio tal que $g(\Theta) = 0$, então $g(\Theta_i) = 0$ para todo Θ_i conjugado de Θ sobre $\mathbb{Q}$. Dessa forma, comon $f(x)$ anula Θ, temos que $f(x)$ anula Θ_i. Consequentemente, temos:

$$\begin{aligned}
\sigma_i(\alpha \cdot \beta) &= \sigma_i(c_0 + c_1\Theta + \cdots + c_{n-1}\Theta^{n-1}) \\
&= c_0 + c_1\Theta_i + \cdots + c_{n-1}\Theta_i^{n-1} \\
&= (a_0 + a_1\Theta_i + \cdots + a_{n-1}\Theta_i^{n-1}) \cdot (b_0 + b_1\Theta_i + \cdots + b_{n-1}\Theta_i^{n-1}) \\
&= \sigma_i(a_0 + a_1\Theta + \cdots + a_{n-1}\Theta^{n-1}) \cdot \sigma_i(b_0 + b_1\Theta + \cdots + b_{n-1}\Theta^{n-1}) \\
&= \sigma_i(\alpha) \cdot \sigma_i(\beta)
\end{aligned}$$

Logo, σ_i como definido acima é de fato um homomorfismo injetivo.

Além disso, notemos que $p(x)$ é irredutível sobre $\mathbb{Q}$, donde $p(x)$ e $p'(x)$ (derivada do polinômio $p(x)$) são relativamente primos. Consequentemente, $p(x)$ não possui raízes múltiplas, garantindo a existência de exatamente n conjugados Θ_i de Θ.

Portanto, concluímos a demonstração de que há exatamente n imersões distintas $\sigma : \mathbb{L} \hookrightarrow \mathbb{C}$. □

Nessas condições, podemos definir o *traço* e a *norma* de um elemento com relação ao corpo a que pertence.

Definição 6.2.4. *Seja $\mathbb{L} = \mathbb{Q}(\Theta)$ um corpo de grau n sobre $\mathbb{Q}$ e $\sigma_1, \sigma_2, \ldots, \sigma_n$ os monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Dado $\alpha \in \mathbb{L}$, definimos a norma e o traço de α com relação à extensão $\mathbb{L}$ de $\mathbb{Q}$ como sendo, respectivamente,*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad e \quad Tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

Observação 6.2.6. Ao considerarmos $\mathbb{L} = \mathbb{Q}(\Theta)$, estamos reduzindo o estudo geral destas propriedades sobre extensões finitas ao estudo das mesmas sobre extensões simples. De fato, sabemos que, dada uma extensão finita $\mathbb{K}$ de $\mathbb{Q}$, existe um elemento Θ, chamado *elemento primitivo*, tal que $\mathbb{K} = \mathbb{Q}(\Theta)$ (para a demonstração, consultar Teorema 6.33, p. 271, em Martinez [10]). No entanto, destacamos que as noções de *norma* e *traço* apresentadas podem ser generalizadas para qualquer extensão $\mathbb{L}$ de um corpo arbitrário $\mathbb{F}$ (fixado), conforme é mostrado em Silva [16].

Exemplo 6.2.1. Consideremos o corpo $\mathbb{L} = \mathbb{Q}\left(\sqrt{-19}\right)$ e o elemento $\alpha = 1 + \sqrt{-19} \in \mathbb{L}$.

O polinômio minimal de $\sqrt{-19}$ sobre $\mathbb{Q}$ é dado por $p(x) = x^2 + 19$.

Como as raízes de $p(x)$ em $\mathbb{L}$ são exatamente $\sqrt{-19}$ e $-\sqrt{-19}$, temos que as imersões de $\mathbb{Q}[\sqrt{-19}]$ em $\mathbb{C}$ são aplicações que fixam $\mathbb{Q}$ satisfazendo:

$$\begin{aligned} \sigma_1\left(\sqrt{-19}\right) &= \sqrt{-19} \\ \sigma_2\left(\sqrt{-19}\right) &= -\sqrt{-19} \end{aligned}$$

Assim, utilizando diretamente a definição de norma e traço, segue que:

$$\begin{aligned} N(\alpha) &= \sigma_1(\alpha) \cdot \sigma_2(\alpha) = \left(1 + \sqrt{-19}\right)\left(1 - \sqrt{-19}\right) = 20 \\ Tr(\alpha) &= \sigma_1(\alpha) + \sigma_2(\alpha) = \left(1 + \sqrt{-19}\right) + \left(1 - \sqrt{-19}\right) = 2 \end{aligned}$$

Observação 6.2.7. Observemos que, estendendo o exemplo acima, podemos concluir que a norma de α em relação ao corpo quadrático $\mathbb{Q}[\sqrt{m}]$, quando $m < 0$, equivale, numericamente, ao conceito de norma euclidiana, apresentado no Capítulo 3.

Com efeito, quaisquer imersões de $\mathbb{Q}[\sqrt{m}]$ em $\mathbb{C}$ fixam $\mathbb{Q}$, ou seja, podem ser inteiramente determinadas pela imagem de $\sqrt{m}$. No entanto, visto que toda imersão é um homomorfismo, temos que as únicas possibilidades para a imagem de $\sqrt{m}$ via tais imersões são $\sqrt{m}$ e $-\sqrt{m}$.

Agora, como $\alpha \in \mathbb{Q}[\sqrt{m}]$, temos que o mesmo é da forma $\alpha = p + q\sqrt{m}$, sendo $p, q \in \mathbb{Q}$. Assim, segue da definição de norma que:

$$N(\alpha) = (p + q\sqrt{m}) \cdot (p - q\sqrt{m}) = p^2 - mq^2 = \mathcal{N}(\alpha)$$

Ressaltamos que tal igualdade só foi possível tendo em vista que $\mathbb{Q}[\sqrt{m}]$ é um corpo de dimensão 2 em relação a $\mathbb{Q}$. Em outras palavras, o polinômio minimal de qualquer um de seus elementos possui grau 2.

Notemos ainda que para o caso em que $\mathbb{Q}[\sqrt{m}]$ é um corpo quadrático real, teríamos apenas:

$$|N(\alpha)| = \mathcal{N}(\alpha)$$

Proposição 6.2.3. *Sejam $\mathbb{L} = \mathbb{Q}(\Theta)$ um corpo de grau n sobre $\mathbb{Q}$, $\alpha, \beta \in \mathbb{L}$ e $q \in \mathbb{Q}$. Então, são válidas as seguintes propriedades:*

1. *O traço é aditivo e a norma, multiplicativa, ou seja,*

$$\begin{aligned} Tr(\alpha + \beta) &= Tr(\alpha) + Tr(\beta) \\ N(\alpha + \beta) &= N(\alpha) \cdot N(\beta) \end{aligned}$$

2. *Temos que*

$$Tr(q \cdot \alpha) = q \cdot Tr(\alpha) \quad e \quad N(q \cdot \alpha) = q^n \cdot N(\alpha)$$

Em particular, os números $Tr(q)$ e $N(q)$ são racionais. Mais ainda,

$$Tr(q) = n \cdot q \quad e \quad N(q) = q^n$$

Demonstração. O primeiro item decorre diretamente da definição. De fato, considerando as imersões $\sigma_1, \sigma_2, \ldots, \sigma_n$ de $\mathbb{L}$ em $\mathbb{C}$ e os elementos $x, y \in \mathbb{L}$, temos que:

$$\begin{aligned} Tr(\alpha+\beta) &= \sum_{i=1}^{n} \sigma_i(\alpha+\beta) = \sum_{i=1}^{n} \sigma_i(\alpha) + \sum_{i=1}^{n} \sigma_i(\beta) = Tr(\alpha) + Tr(\beta) \\ N(\alpha+\beta) &= \prod_{i=1}^{n} \sigma_i(\alpha+\beta) = \prod_{i=1}^{n} \sigma_i(\alpha) + \prod_{i=1}^{n} \sigma_i(\beta) = N(\alpha) + N(\beta) \end{aligned}$$

Por outro lado, como σ_i é um homorfismo, temos que $\sigma_i(q) = q$ para todo $q \in \mathbb{Q}$, donde segue a afirmação 2:

$$\begin{aligned} Tr(q \cdot \alpha) &= \sum_{i=1}^{n} \sigma_i(q \cdot \alpha) = \sum_{i=1}^{n} \sigma_i(q) \cdot \sigma_i(\alpha) = \sum_{i=1}^{n} q \cdot \sigma_i(\alpha) = q \cdot \sum_{i=1}^{n} \sigma_i(\alpha) = q \cdot Tr(\alpha) \\ N(q \cdot \alpha) &= \prod_{i=1}^{n} \sigma_i(q \cdot \alpha) = \prod_{i=1}^{n} \sigma_i(q) \cdot \sigma_i(\alpha) = \prod_{i=1}^{n} q \cdot \sigma_i(\alpha) = q^n \cdot \prod_{i=1}^{n} \sigma_i(\alpha) = q^n \cdot N(\alpha) \end{aligned}$$

Para o caso particular, basta notarmos que:

$$\begin{aligned} Tr(q) &= \sum_{i=1}^{n} \sigma_i(q) = \sum_{i=1}^{n} q = n \cdot q \\ N(q) &= \prod_{i=1}^{n} \sigma_i(q) = \prod_{i=1}^{n} q = q^n \end{aligned}$$

□

A partir dessas propriedades, somos capazes de definir a norma e o traço de elementos em $\mathbb{Q}(\zeta)$.

Exemplo 6.2.2. Primeiramente, consideremos o elemento ζ no corpo ciclotômico.

Sabemos que os elementos $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ são todos p-ésimas raízes da unidade. Além disso, conforme demonstrado na seção 6.2 (Observação 6.2.3), o polinômio minimal de ζ é dado por:

$$P_\zeta(x) = 1 + x + x^2 + \cdots + x^{p-1} = \prod_{j=1}^{p-1} (x - \zeta^j)$$

Pela segunda igualdade, temos que os únicos conjugados de ζ sobre $\mathbb{Q}$ são $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. Dessa forma, todos esses elementos possuem a mesma norma, dada por:

$$N(\zeta^j) = N(\zeta) = \zeta \cdot \zeta^2 \cdots \zeta^{p-1} = \zeta^{\frac{p(p-1)}{2}} = (\zeta^p)^{\frac{p-1}{2}} = 1$$

para todo $j = 1, \ldots, p-1$.

Cabe ressaltar que o expoente de ζ na igualdade acima é natural visto que p é um primo ímpar, garantindo que 2 divide $(p-1)$.

Analogamente, ζ e seus conjugados possuem o mesmo traço, o qual é dado por:

$$Tr(\zeta^j) = Tr(\zeta) = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1$$

Neste caso, a igualdade segue da primeira identidade apresentada para o polinômio minimal $P_\zeta(x)$.

Finalmente, por meio dos resultados, podemos obter o anel de inteiros de $\mathbb{Q}(\zeta)$, o qual será dado por $\mathbb{Z}[\zeta]$.

Lema 6.2.1. *Os elementos $1-\zeta$ e $1-\zeta^j$ são associados em $\mathcal{O}_{\mathbb{Q}(\zeta)}$ para todo inteiro $j = 1, \cdots, p-1$.*

Demonstração. Notemos que dado $j = 1, \ldots, p-1$, os elementos $1-\zeta$ e $1-\zeta^j$ são associados em $\mathbb{Z}[\zeta]$. Com efeito, sabemos que para cada valor de j vale a relação:

$$1 - \zeta^j = (1-\zeta)(1 + \zeta + \cdots + \zeta^{j-2} + \zeta^{j-1}),$$

donde $1-\zeta$ divide $1-\zeta^j$.

Por outro lado, fixado o valor de j, temos que 1 (unidade) é um mdc entre j e p. Assim, pela Identidade de Bézout, existem $t, s \in \mathbb{Z}$ tais que $jt + p(-s) = 1$, ou seja, $jt + ps = 1$. Agora, utilizando que

$$1 - x^p = (1-x)(1 + x + \cdots + x^{p-2} + x^{p-1})$$

e fazendo $x = \zeta^j$ e $p = t$, obtemos:

$$1 - \zeta^{jt} = (1-\zeta^j)(1 + \zeta^j + \cdots + \zeta^{jt-2} + \zeta^{jt-1})$$

Assim, $1-\zeta^j$ divide $1-\zeta^{jt}$. Porém, observemos ainda que $1-\zeta^{jt} = 1-\zeta$, pois:

$$\zeta^{jt} = \zeta^{ps+1} = (\zeta^p)^s \cdot \zeta = \zeta$$

Portanto, concluímos que, para cada valor de j especificado acima, $1-\zeta$ e $1-\zeta^j$ são associados. □

Proposição 6.2.4. *O anel dos inteiros de $\mathbb{Q}(\zeta)$ é igual a $\mathbb{Z}[\zeta]$.*

Demonstração. Seja $a = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, com $a_j \in \mathbb{Q}$ para todo $j = 0, \ldots, p-2$, um inteiro algébrico sobre $\mathbb{Q}(\zeta)$. Queremos mostrar que $a_j \in \mathbb{Z}$ para cada j nesse intervalo.

Tal notação para o inteiro algébrico a nos fornece a igualdade:

$$a - a\zeta = a(1-\zeta) = a_0(1-\zeta) + a_1(\zeta - \zeta^2) + \cdots + a_{p-2}(\zeta^{p-2} - \zeta^{p-1})$$

Dessa forma, utilizando as propriedades do traço (Proposição 6.2.3), segue que:

$$\begin{aligned} Tr\,(a(1-\zeta)) &= Tr(a_0(1-\zeta)) + Tr(a_1(\zeta-\zeta^2)) + \cdots + Tr(a_{p-2}(\zeta^{p-2}-\zeta^{p-1})) \\ &= a_0 \cdot Tr(1-\zeta) + a_1 \cdot Tr(\zeta-\zeta^2) + \cdots + a_{p-2} \cdot Tr(\zeta^{p-2}-\zeta^{p-1}) \end{aligned}$$

Além disso, sabemos que ζ e ζ^j, com $j = 0, \cdots, p-2$, possuem o mesmo traço. Assim, como o traço é uma função aditiva, temos $Tr(\zeta - \zeta^j) = 0$ para qualquer valor inteiro de j no intervalo acima. Consequentemente, temos:

$$\begin{aligned} Tr(a(1-\zeta)) &= a_0 \cdot Tr(1-\zeta) \\ &= a_0 \cdot [Tr(1) - Tr(\zeta)] \\ &= a_0 \cdot [(p-1) - (-1)] \\ &= a_0 p \in \mathbb{Q}\,, \end{aligned}$$

onde a penúltima igualdade decorre da Proposição 6.2.3, visto que $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1$.

Por outro lado, considerando os conjugados de a dados por $\sigma_i(a) = b_i$, em que $i = 1, \ldots, p-1$, obtemos:

$$\begin{aligned} Tr(a(1-\zeta)) &= Tr(a - a\zeta) \\ &= Tr(a) - Tr(a\zeta) \\ &= (b_1 + \cdots + b_{p-1}) - (b_1\zeta + \cdots + b_{p-1}\zeta^{p-1}) \\ &= b_1(1-\zeta) + \cdots + b_{p-1}(1-\zeta^{p-1}) \end{aligned}$$

Agora, como já visto, sabemos que $1-\zeta$ divide $1-\zeta^j$ para todo $j = 1, \ldots, p-1$ e, assim, podemos escrever:

$$Tr(a(1-\zeta)) = b'(1-\zeta) \in \mathbb{Q}(\zeta)$$

em que b' é um número racional.

Dessas igualdades, resulta $Tr(a(1-\zeta)) \in \mathbb{Q} \cap \mathbb{Q}(\zeta)$; mais precisamente, pela segunda igualdade, $Tr(a(1-\zeta)) \in \langle 1-\zeta \rangle$, sendo $\langle 1-\zeta \rangle$ o ideal do anel de inteiros $\mathcal{O}_{\mathbb{Q}(\zeta)}$ gerado por $1-\zeta$. Nessas condições, segue que:

$$Tr(a(1-\zeta)) \in \mathcal{O}_{\mathbb{Q}(\zeta)} \cap \mathbb{Q}$$

Além disso, como $\mathbb{Z}$ é o anel de inteiros de $\mathbb{Q}$, temos que $\mathbb{Z} \subset \mathcal{O}_{\mathbb{Q}(\zeta)}$, implicando em $Tr(a(1-\zeta)) \in \mathbb{Z}$. Logo,

$$Tr(a(1-\zeta)) \in \langle 1-\zeta \rangle \cap \mathbb{Z} \tag{6.5}$$

Por outro lado, sabemos que $1-\zeta$ e $1-\zeta^j$, com $j = 1, \cdots, p-1$, são associados, donde obtemos:

$$P_\zeta(1) = p = \prod_{j=1}^{p-1}(1-\zeta^j) = u(1-\zeta)^{p-1},$$

em que u é uma unidade de $\mathcal{O}_{\mathbb{Q}(\zeta)}$.

Desse modo, concluímos que $p\mathbb{Z} \subseteq \langle 1-\zeta \rangle$. Sabemos ainda que $p\mathbb{Z}$ e $\langle 1-\zeta \rangle \cap \mathbb{Z}$ são ideais de $\mathbb{Z}$ e, como p é primo, $p\mathbb{Z}$ é ideal maximal. Temos, portanto, que $\langle 1-\zeta \rangle \cap \mathbb{Z} = p\mathbb{Z}$ ou $\langle 1-\zeta \rangle \cap \mathbb{Z} = \mathbb{Z}$.

Mas, caso $\langle 1-\zeta \rangle \cap \mathbb{Z} = \mathbb{Z}$, como $1 \in \mathbb{Z}$, deveria existir $x \in \mathcal{O}_{\mathbb{Q}(\mathbb{Z})}$ satisfazendo

$$1 = x \cdot (1-\zeta)$$

No entanto, isso não é possível pois, caso contrário, $1-\zeta$ seria inversível em $\mathcal{O}_{\mathbb{Q}(\zeta)}$ e, como $p = u(1-\zeta)^{p-1}$, teríamos que p também seria inversível em $\mathcal{O}_{\mathbb{Q}(\zeta)}$. Assim, o candidato a inverso multiplicativo de p estaria em $\mathcal{O}_{\mathbb{Q}(\zeta)}$ e em $\mathbb{Q}$. Porém, como $\mathcal{O}_{\mathbb{Q}(\zeta)} \cap \mathbb{Z} = \mathbb{Z}$, teríamos que p seria inversível em $\mathbb{Z}$, uma contradição.

Então, $\langle 1-\zeta \rangle \cap \mathbb{Z} = p\mathbb{Z}$ e, pela equação (6.5), temos que:

$$a_0 p = Tr(a(1-\zeta) \in p\mathbb{Z} \text{ e, assim, } a_0 \in \mathbb{Z}$$

Resta-nos provar que $a_1, \ldots, a_{p-2} \in \mathbb{Z}$. Pela definição inicial de a, dado $j = 1, \ldots, p-2$, temos:

$$a\zeta^{p-j} = a_0\zeta^{p-j} + a_1\zeta^{p-j+1} + \cdots + a_{j-1}\zeta^{p-1} + a_j + a_{j+1}\zeta + \cdots + a_{p-2}\zeta^{p-j-2}$$

Dessa forma, obtemos:

$$a(1-\zeta^{p-j}) = a_0(1-\zeta^{p-j}) + \cdots + a_j(\zeta^j - 1) + \cdots + a_{p-2}(\zeta^{p-2} - \zeta^{p-j-2})$$

Novamente, utilizando as propriedades do traço, segue que:

$$\begin{aligned} Tr(a(1-\zeta^{p-j})) &= Tr(a_0(1-\zeta^{p-j})) + Tr(a_{p-2}(\zeta^j - 1)) \\ &= a_0[(p-1)-1] + a_{p-2}[-1-(p-1)] \\ &= a_0 p - a_j p \in \mathbb{Q} \end{aligned}$$

Procedendo de maneira semelhante à feita acima, mostra-se que $Tr(a(1-\zeta^{p-j}) \in p\mathbb{Z}$. Logo, temos que $a_j \in \mathbb{Z}$ para todo $j = 0, \ldots, p-1$, como queríamos provar.

Consequentemente, demonstramos que o anel de inteiros do corpo ciclotômico é dado por:

$$\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$$

□

Observação 6.2.8. Devido ao resultado estabelecido acima, o anel $\mathbb{Z}[\zeta]$ é denominado *anel de inteiros ciclotômicos.*

Destacamos ainda que, a partir de tal resultado, poderíamos obter o fato já demonstrado de que $\mathbb{Q}(\zeta)$ é o corpo de frações de $\mathbb{Z}[\zeta]$. Com efeito, mais geralmente, pode-se demonstrar que, se $\mathbb{L}$ é uma extensão finita de $\mathbb{Q}$, então o corpo de frações de $\mathcal{O}_{\mathbb{L}}$ corresponde ao próprio corpo $\mathbb{L}$ (consultar Proposição 11.46, p. 925 em Rotman [15]).

6.3 A GENERALIZAÇÃO DE DEDEKIND

Como destacado na primeira seção, a ideia inicial de Lamé não pode ser utilizada para a prova geral do UTF, tendo em vista que a unicidade da fatoração em irredutíveis verifica-se apenas em certos anéis. Com o intuito de reduzir este problema, Kummer incluiu novos elementos, chamados *números ideais*, ao anel inicial, obtendo, assim, uma extensão deste anel em que a unicidade fosse válida.

Para exemplificar a técnica utilizada por Kummer, consideremos o anel $\mathbb{Z}[\sqrt{10}]$. Observemos que o número 6 possui duas fatorações em irredutíveis[1], a saber:

$$6 = 2 \cdot 3 = \left(4 + \sqrt{10}\right)\left(4 - \sqrt{10}\right)$$

No entanto, se introduzimos $\sqrt{5}$ à fatoração, temos que:

$$4 \pm \sqrt{10} = \sqrt{2}\left(2\sqrt{2} \pm \sqrt{5}\right)$$

donde segue que as fatorações acima se reduzem a:

$$6 = \sqrt{2}\,\sqrt{2}\left(2\sqrt{2} + \sqrt{5}\right)\left(2\sqrt{2} - \sqrt{5}\right)$$

Assim, ao estendermos o anel $\mathbb{Z}[\sqrt{10}]$ ao anel $\mathbb{Z}[\sqrt{2}, \sqrt{5}]$, obtemos a unicidade da fatoração para o elemento 6, visto que 2 e 3 deixam de ser irredutíveis neste novo anel. Neste contexto, segundo a teoria proposta por Kummer, a adição de tal elemento ao anel inicial restaura a unicidade da fatoração neste caso, motivo pelo qual o elemento $\sqrt{5}$ é denominado um *número ideal*.

Motivado por tal ideia, posteriormente, o matemático alemão Dedekind introduziu o conceito de *ideal* de um anel, o qual generaliza a ideia de números ideais

[1] A verificação de que tais elementos são irredutíveis decorre da análise dos possíveis valores para a norma de cada um deles, resultando que a mesma deve ser, necessariamente, igual a 1.

sugerida por Kummer. Sob essa ótica, Dedekind desenvolveu a noção de fatoração em *ideais primos* e mostrou que, apesar de alguns ideais não apresentarem a unicidade da fatoração em irredutíveis, eles poderiam apresentar fatoração única em ideais. Com efeito, sabemos que, dado um elemento inversível u, vale a igualdade $I = uI$ para todo ideal I; nesse sentido, os elementos inversíveis não precisam ser considerados na fatoração em ideais primos, ao contrário do que ocorre com a fatoração usual em elementos irredutíveis.

Destacamos, porém, que o trabalho desenvolvido por Kummer não explicitava diretamente o conceito de *ideais*, estabelecido por Dedekind. Historicamente, aliás, tal conceito surgiu depois da demonstração completa do Teorema de Kummer. Entretanto, a demonstração que forneceremos para o teorema em questão será fundamentada na Teoria de Ideais de Dedekind, uma vez que a mesma possibilita uma das diversas conexões entre duas importantes áreas matemáticas: a Teoria dos Números e Álgebra Abstrata. Além disso, a demonstração inicial, embora utilize uma terminologia mais leve, necessita de uma série de resultados auxiliares, tornando-se relativamente mais extensa, ainda que não menos elegante. Para uma apresentação detalhada dessa primeira abordagem, sugerimos consultar Ribenboim [13] e Edwards [5].

Seguindo a generalização feita por Dedekind, nosso objetivo agora será mostrar que o anel de inteiros ciclotômicos $\mathbb{Z}[\zeta]$ satisfaz a unicidade da fatoração em ideais primos. Para tanto, necessitaremos de alguns conceitos, como *domínio de Dedekind,* e *ideais fracionários*, os quais serão apresentados ao longo desta seção.

6.3.1 **Anéis Noetherianos**

A fim de definirmos os *Domínios de Dedekind*, apresentaremos o conceito de *anéis Noetherianos*, criado pela matemática Emmy Noether, juntamente com algum dos principais resultados a eles associados.

Teorema 6.3.1. *Seja A um domínio. Então as seguintes condições são equivalentes:*

(*i*) *Todo ideal I de A é finitamente gerado, ou seja, existem $x_1, \ldots, x_n \in I$ com $n \in \mathbb{N}$ tais que $I = \langle x_1, \ldots, x_n \rangle$.*

(*ii*) *A satisfaz a condição da cadeia ascendente, ou seja, dada uma cadeia ascendente de ideais de A*

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

existe $m \in \mathbb{N}$ tal que $I_n = I_m$ para todo natural n com $n \geq m$.

Em outras palavras toda cadeia ascendente de ideais em A é estacionária.

(*iii*) *Toda família $\mathcal{S}$ não vazia de ideais de A possui um elemento maximal, ou seja, existe um ideal $M \in \mathcal{S}$ tal que, se $I \in \mathcal{S}$ e $I \supset M$, então $I = M$.*

Demonstração. Seja A um domínio de integridade.

$(i) \Rightarrow (ii)$ Consideremos uma cadeia ascendente de A denotada por:

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

Definimos $I = \bigcup_{n \in \mathbb{N}} I_n$.

Sabemos que I é um ideal de A; assim, por hipótese, temos que I é finitamente gerado, ou seja, existem $x_1, \ldots, x_k \in I$, com $k \in \mathbb{N}$, tais que $I = \langle x_1, \ldots, x_k \rangle$.

Além disso, para cada x_i fixado, em que $i = 1, \ldots, k$, existe $n_i \in \mathbb{N}$ tal que $x_i \in I_{n_i}$. Tomemos $m = max\{x_1, \ldots, x_k\}$. Então, temos que $I \subset I_m$. Por outro lado, como $m \in \mathbb{N}$, temos que $I_m \subset I$.

Logo, $I = I_m$, fazendo com que I_n seja igual a I_m para todo natural $n \geq m$.

Portanto, a cadeia ascendente acima (arbitrária) estabiliza.

$(ii) \Rightarrow (iii)$ Seja $\mathcal{S}$ uma família não vazia de ideais de A e seja $I_1 \in \mathcal{S}$.

Caso I_1 seja um elemento maximal, não temos nada a fazer. Assim, suponhamos que exista $I_2 \in \mathcal{S}$ tal que $I_1 \subsetneq I_2$.

Novamente, caso I_2 seja elemento maximal, o resultado segue. Caso contrário, existe $I_3 \in \mathcal{S}$ tal que $I_2 \subsetneq I_3$. Procedendo desta forma, obtemos um elemento maximal de $\mathcal{S}$ ou então uma cadeia ascendente de ideais em A dada por

$$I_0 \subsetneq I_1 \subsetneq \ldots \subsetneq I_n \subsetneq \ldots ,$$

que não estabiliza.

No entanto, neste caso, teríamos uma contradição com a hipótese. Logo, segue que $\mathcal{S}$ possui um elemento maximal.

$(iii) \Rightarrow (i)$ Seja I ideal de A. Consideremos

$$\mathcal{S} := \{J \subset A : J \text{ é ideal finitamente gerado de } A \text{ e } J \subset I\}$$

Observemos que $\mathcal{S} \neq \emptyset$, visto que $\langle 0 \rangle \in \mathcal{S}$. Assim, como $\mathcal{S}$ é uma família não vazia de ideais de A, temos que $\mathcal{S}$ possui um elemento maximal, digamos M. Como M é finitamente gerado, podemos escrever $M = \langle x_1, \ldots, x_n \rangle$ em que n é natural. Provaremos que $M = I$.

Por construção, sabemos que $M \subset I$. Suponhamos, por absurdo, que $I \not\subset M$. Então, existe $a \in I$ tal que $a \notin M$.

Dessa forma, definimos o ideal $M' = \langle a, x_1, \ldots, x_n \rangle$. Temos que $M' \in \mathcal{S}$, pois M' é um ideal de A finitamente gerado e $M' \subset I$. Entretanto, temos que $M \subsetneq M'$, contrariando

a maximalidade de M. Portanto, concluímos que $I = M$ e, assim, I é finitamente gerado, como queríamos provar. □

Definição 6.3.1. *Dizemos que um anel A é Noetheriano se satisfaz as condições equivalentes apresentadas no Teorema 6.3.1.*

Exemplo 6.3.1. Utilizando a caracterização fornecida por (i), é imediato que $\mathbb{Z}$ é um anel noteheriano, uma vez que todos os seus ideais podem ser gerados por um único elemento. Mais precisamente, dado um ideal I de $\mathbb{Z}$, ele é da forma $n\mathbb{Z}$, em que n é um número inteiro.

Com efeito, seja I ideal de $\mathbb{Z}$. Se $I = \{0\}$, temos que $I = 0\mathbb{Z}$. Assim, podemos supor sem perda de generalidade que $I \neq \{0\}$. Assim, existe $a \in I$, tal que $a \neq 0$. Além disso, como $0 - a = -a \in I$, temos que I contém números naturais. Dessa forma, utilizando o Princípio da Boa Ordenação, é possível tomar $n \in \mathbb{Z}$ como sendo o menor número natural em I.

Consideremos $m \in I$; como $\mathbb{Z}$ é um domínio euclidiano, existem $q, r \in \mathbb{Z}$ tais que $m = nq + r$ e $0 \leq r < n$. Agora, como I é ideal, temos que $r = m - nq \in I$, resultando, pela minimalidade de n, que $r = 0$. Logo, $m = nq$ e, consequentemente, $I \subseteq n\mathbb{Z}$.

Por outro lado, se $m \in n\mathbb{Z}$, temos que $m = nt$, em que $t \in \mathbb{Z}$. Assim, $m \in \mathbb{Z}$, implicando que $n\mathbb{Z} \subseteq \mathbb{Z}$.

Portanto, segue que $I = n\mathbb{Z}$. Como I foi tomado arbitrariamente, concluímos que todos os ideais de $\mathbb{Z}$ são finitamente gerados e, então, $\mathbb{Z}$ é um anel noetheriano.

Observemos que, utilizando (i), concluímos ainda que todo domínio de ideais principais é, em particular, um anel noetheriano, uma vez que todos seus ideais são gerados por um único elemento. No entanto, a recíproca não é verdadeira. De fato, sabemos que todo domínio de ideais principais possui fatoração única em irredutíveis (i.e, é um domínio de fatoração única). Mas, como será mostrado a seguir, nos anéis noetherianos garantimos apenas a existência da fatoração em irredutíveis, mas não a unicidade.

Proposição 6.3.1. *Sejam A um anel noetheriano e $a \in A$ um elemento não nulo e não inversível. Então a é um produto finito de elementos irredutíveis.*

Demonstração. Consideremos a família de ideais de A dada por:

$$\mathcal{S} = \{\langle a \rangle : a \in A, a \neq 0 \text{ e } a \text{ não possui fatoração em irredutíveis em A}\}$$

Provaremos que $\mathcal{S} = \emptyset$. Suponhamos, por absurdo, que $\mathcal{S}$ seja não vazio. Como A é noetheriano, $\mathcal{S}$ admite um elemento maximal, digamos $\langle m \rangle$.

Sabemos que m não é irredutível, caso contrário, ele próprio constituiria uma fatoração em irredutíveis. Desta forma, existem $a, b \in A$ não nulos e não inversíveis satisfazendo $m = ab$. Assim, $\langle m \rangle \subseteq \langle a \rangle$ e $\langle m \rangle \subseteq \langle b \rangle$.

Por outro lado, notemos que $\langle m \rangle \neq \langle a \rangle$. De fato, caso contrário, teríamos que $m \mid a$ e $a \mid m$, donde a e m seriam associados. Entretanto, neste caso, resultaria que b é inversível, uma contradição com a hipótese inicial. De modo análogo, temos que $\langle m \rangle \neq \langle b \rangle$.

Então, obtemos que $\langle m \rangle \subsetneq \langle a \rangle$ e $\langle m \rangle \subsetneq \langle b \rangle$ e, consequentemente, $\langle a \rangle$ e $\langle b \rangle$ não podem estar em $\mathcal{S}$, pois, do contrário, teríamos uma contradição com a maximalidade de m. Mas, como $a, b \in A$ são elementos não nulos não inversíveis em A, segue que os mesmos possuem fatoração finita em irredutíveis em A. No entanto, como $m = ab$, concluímos que m também possuirá uma fatoração finita em irredutíveis, gerando uma contradição.

Consequentemente, $S = \emptyset$ e, assim, todos os elementos não nulos e não inversíveis possuem uma fatoração finita em irredutíveis em A. □

Pela proposição acima, conclui-se que um anel noetheriano deixa de ser um anel fatorial somente no caso em que existe um elemento com mais de uma fatoração em irredutíveis. Como será provado posteriormente, de fato, existem aneis noetherianos para os quais não vale a unicidade da fatoração de um elemento em irredutíveis. Com efeito, mostraremos que o anel de inteiros $\mathbb{Z}[\zeta]$ é um anel noetheriano, no entanto, o mesmo só é um DFU sob condições específicas, as quais dependem do chamado *número de classe*.

Por fim, apresentamos um resultado relevante a respeito dos anéis euclidianos, o qual nos permitirá provar que o anel dos inteiros ciclotômicos $\mathbb{Z}[\zeta]$ é um anel noetheriano.

Proposição 6.3.2. *Seja $f : A \to B$ um homomorfismo sobrejetor de anéis. Se A é um anel noetheriano, então B também é noetheriano.*

Demonstração. Seja J um ideal de B. Mostraremos que J é um ideal finitamente gerado.

Notemos que, como f é um homorfismo sobrejetor, $f^{-1}(J)$ é um ideal de A; por outro lado, como A é anel noetheriano, $f^{-1}(J)$ é finitamente gerado. Sem perda de generalidade, consideremos $f^{-1}(J) = \langle x_1, \ldots, x_n \rangle$.

Sejam $y \in J$ e $x \in A$ tais que $f(x) = y$. Como $x \in f^{-1}(J)$, temos que existem $a_i \in A$, com $i = 1, \ldots, n$, satisfazendo:

$$x = a_1 x_1 + \ldots + a_n x_n$$

Utilizando novamente que f é um homomorfismo, temos que:

$$y = f(x) = f(a_1x_1 + \ldots + a_nx_n) = f(a_1)f(x_1) + \ldots + f(a_n)f(x_n)$$

em que $f(a_i) \in B$ para todo $i = 1, \ldots, n$.

Agora, como $f(x_i) \in J$ e y foi tomado de forma arbitrária em J, concluímos que $J = \langle f(x_1), \ldots, f(x_n) \rangle$, ou seja, J é finitamente gerado.

Portanto, B é noetheriano. □

Corolário 6.3.2. *Se A é um anel noetheriano e I um ideal de A, então o anel quociente $\left(\frac{A}{I}\right)$ também é noetheriano.*

Exemplo 6.3.2. Vamos provar que o anel $\mathbb{Z}[\zeta]$ é noetheriano. Consideremos o polinômio minimal de ζ denotado por $P_\zeta(x)$. Sabemos que o anel dos inteiros ciclotômicos pode ser visto como o seguinte anel quociente:

$$\mathbb{Z}[\zeta] = \frac{\mathbb{Z}}{\langle P_\zeta(x) \rangle}$$

Além disso, conforme já mostrado, $\mathbb{Z}$ é um anel noetheriano. Logo, pelo corolário anterior, segue que $\mathbb{Z}[\zeta]$ é noetheriano.

6.3.2 **Domínios de Dedekind**

Estendendo a noção de inteiro algébrico da definição 2.1.4, para um anel arbitrário A obtemos:

Definição 6.3.2. *Sejam A e B anéis comutativos com unidade, com A subanel de B. Dizemos que $\alpha \in B$ é inteiro sobre A se existir um polinômio mônico não nulo $f(x) \in A[x]$ tal que $f(\alpha) = 0$. Quando todos os elementos de B forem inteiros sobre A, diremos ainda que B é inteiro sobre A. O conjunto (ou anel) de inteiros de B sobre A será denotado, em geral, por $\mathcal{O}_B(A)$.*

Observação 6.3.1. No caso em que A e B da definição anterior são corpos, é comum nos referirmos ao elemento α como sendo *algébrico sobre A*.

Sob as condições iniciais da definição anterior, cabe destacar que a seguinte relação sempre se verifica:

$$A \subseteq \mathcal{O}_B(A)$$

uma vez que, se $\alpha \in A$, basta tomarmos o polinômio $f(x) = x$, o qual possui coeficientes em A, a fim de que tenhamos $f(\alpha) = 0$.

Definição 6.3.3. *Seja A um domínio e $\mathbb{K}$ seu corpo de frações. Dizemos que A é integralmente fechado se todo $\alpha \in \mathbb{K}$ que for raiz de um polinômio mônico de $A[x]$ estiver em A.*

Em outras palavras, para todo polinômio mônico $f(x) \in A[x]$ tal que $f(\alpha) = 0$, com $\alpha \in \mathbb{K}$, tem-se que $\alpha \in A$.

Observação 6.3.2. Utilizando a definição anterior de *inteiro sobre A*, obtemos uma caracterização equivalente para A ser *integralmente fechado*. Neste caso, temos que A é integralmente fechado quando o conjunto de inteiros sobre A corresponde ao próprio conjunto A, ou seja, quando tivermos:

$$O_B(A) = A$$

Apresentaremos agora um resultado que nos auxiliará na busca por domínios integralmente fechados.

Proposição 6.3.3. *Seja A um domínio de fatoração única. Então A é integralmente fechado.*

Demonstração. Seja A um DFU com corpo de frações $\mathbb{K}$.

Consideremos $\alpha \in \mathbb{K}$ raiz do polinômio mônico não nulo dado por:

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in A[x]$$

Como A é um DFU, existem $b, c \in A$ relativamente primos tais que $\alpha = \frac{b}{c}$. Assim, utilizando o fato de que $f(\alpha) = 0$, temos:

$$\left(\frac{b}{c}\right)^n + a_{n-1}\left(\frac{b}{c}\right)^{n-1} + \cdots + a_1\left(\frac{b}{c}\right) + a_0 = 0$$

resultando que

$$b^n + a_{n-1}cb^{n-1} + \cdots + a_1c^{n-1}b + a_0c^n = 0$$
$$\therefore b_n = -c\left(a_{n-1}b^{n-1} + \cdots + a_1c^{n-2} + a_0c^{n-1}\right)$$

Assim, $c \mid b^n$.

Agora, suponhamos, por absurdo, que c não seja inversível em A. Então, existe um primo p em sua fatoração em irredutíveis. Como $c \mid b^n$, segue que p também divide b, uma contradição com o fato de que b e c são relativamente primos. Portanto, c é invertível, donde concluímos que $\alpha = bc^{-1} \in A$, como queríamos provar. □

A partir das noções já apresentadas, somos capazes de definir os *Domínios de Dedekind*.

Definição 6.3.4. *Dizemos que um domínio A é um Domínio de Dedekind se ele é integralmente fechado, Noetheriano e todos os seus ideais primos não nulos são maximais.*

Exemplo 6.3.3. O anel $\mathbb{Z}$ é um Domínio de Dedekind. Com efeito, sabemos que $\mathbb{Z}$ é Noetheriano pelo Exemplo 6.3.1. Por outro lado, como $\mathbb{Z}$ é um domínio de ideais principais, temos que todo ideal primo é ideal maximal. Além disso, temos ainda que $\mathbb{Z}$ é também um domínio de fatoração única, resultando que $\mathbb{Z}$ é integralmente fechado.

Mostraremos agora que o anel de inteiros ciclotômicos, nosso objeto de estudo, também se caracteriza como um domínio de Dedekind.

Proposição 6.3.4. *O anel de inteiros ciclotômicos $\mathbb{Z}[\zeta]$ é um Domínio de Dedekind.*

Demonstração. Conforme mostrado na seção anterior, sabemos que $\mathbb{Z}[\zeta]$ é um anel noetheriano. Provaremos, então, as outras duas condições.

1. $\mathbb{Z}[\zeta]$ é integralmente fechado.

Primeiramente, lembramos que, conforme já demonstrado na Proposição 6.2.2, $\mathbb{Q}(\zeta)$ é o corpo de fração de $\mathbb{Z}[\zeta]$.

Assim, seja $\alpha \in \mathbb{Q}(\zeta)$ tal que $f(x)$ é um polinômio mônico em $\mathbb{Z}[\zeta][x]$ que anula α. Queremos mostrar que $\alpha \in \mathbb{Z}[\zeta]$.

Seguindo a notação de inteiro sobre A (Observação 6.3.2), queremos provar que

$$\mathcal{O}_{\mathbb{Q}(\zeta)}(\mathbb{Z}[\zeta]) = \mathbb{Z}[\zeta]$$

Utilizando a mesma observação, já sabemos que

$$\mathbb{Z}[\zeta] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)}(\mathbb{Z}[\zeta])$$

Para a inclusão contrária, notemos que $\mathcal{O}_{\mathbb{Q}(\zeta)}(\mathbb{Z}[\zeta])$ é, por definição, inteiro sobre $\mathbb{Z}[\zeta]$. Além disso, como foi mostrado na Proposição 6.2.4, o conjunto dos inteiros de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Z}$ é $\mathbb{Z}[\zeta]$. Em outras palavras, $\mathbb{Z}[\zeta]$ é inteiro sobre $\mathbb{Z}$.

Agora, usaremos que a condição de ser inteiro é transitiva [2], isto é, se A, B, C são ideais tais que $A \subseteq B \subseteq C$, em que C é inteiro sobre B e B é inteiro sobre A, então C é inteiro sobre A. Dessa forma, concluímos que $\mathcal{O}_{\mathbb{Q}(\zeta)}(\mathbb{Z}[\zeta])$ é inteiro sobre $\mathbb{Z}$. Portanto, segue que:

$$\mathcal{O}_{\mathbb{Q}(\zeta)}(\mathbb{Z}[\zeta]) \subseteq \mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$$

concluindo nossa prova.

2. Todo ideal primo não nulo de $\mathbb{Z}[\zeta]$ é maximal.

Seja I ideal primo não nulo de $\mathbb{Z}[\zeta]$. A fim de provarmos que I é maximal, mostraremos o seguinte resultado auxiliar.

Afirmação 1: *O ideal $I \cap \mathbb{Z}$ é um ideal primo não nulo de $\mathbb{Z}$.*

[2] Uma demonstração desse resultado pode ser encontrada em Boeing [3] (Proposição 3.1, p. 71).

Prova. O fato de $I \cap \mathbb{Z}$ ser ideal de $\mathbb{Z}$ segue diretamente da definição de ideal, juntamente com a informação de que I é ideal de $\mathbb{Z}[\zeta]$.

Para a prova de que o mesmo é um ideal primo de $\mathbb{Z}$, notemos primeiramente, que $I \cap \mathbb{Z} \neq \mathbb{Z}$. Agora, consideremos $a, b \in \mathbb{Z}$ tais que $ab \in I \cap \mathbb{Z}$. Assim, $ab \in I$ e, como I é primo, segue que $a \in I$ ou $b \in I$. Consequentemente, $a \in I \cap \mathbb{Z}$ ou $b \in I \cap \mathbb{Z}$, comprovando que $I \cap \mathbb{Z}$ é ideal primo de $\mathbb{Z}$.

Resta mostrarmos que $I \cap \mathbb{Z}$ é não nulo. Como I é não nulo, temos que existe $\alpha \in I$ com $\alpha \neq 0$. Além disso, sabemos, pelo fato de I ser um ideal do anel de inteiros ciclotômicos, que $I \subseteq \mathbb{Z}[\zeta]$, donde α é, em particular, um inteiro algébrico sobre $\mathbb{Z}$.

Nessas condições, existe um polinômio mônico não nulo em $\mathbb{Z}[x]$ que anula α. Sem perda de generalidade, consideremos o polinômio mônico de menor grau n que satisfaz esta propriedade. Dessa forma, existem $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ satisfazendo:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

donde segue que:

$$a_0 = -\alpha\left(a_1 + \ldots + a_{n-1}\alpha^{n-2} + \alpha^{n-1}\right)$$

Assim, $a_0 \in \langle\alpha\rangle \cap \mathbb{Z}$, sendo $\langle\alpha\rangle$ o ideal de $\mathbb{Z}[\zeta]$ gerado por α. Por outro lado, α é um elemento de I, resultando que $\langle\alpha\rangle \subseteq I$ e, por consequência,

$$\langle\alpha\rangle \cap \mathbb{Z} \subseteq I \cap \mathbb{Z}$$

Logo, $a_0 \in I \cap \mathbb{Z}$.

Por fim, observemos que, pela minimalidade de n, a_0 tem que ser diferente de zero. Com efeito, caso contrário, poderíamos reescrever a equação acima como:

$$\alpha\left(a_1 + \ldots + a_{n-1}\alpha^{n-2} + a_{n-2}\right) = 0$$

Utilizando que $\alpha \neq 0$, obterímos um novo polinômio, de grau $n-2$ o qual anularia α, contradizendo a minimalidade de n.

Agora, como $I \cap \mathbb{Z}$ é ideal primo não nulo de $\mathbb{Z}$ e $\mathbb{Z}$ é domínio de Dedekind, temos que $I \cap \mathbb{Z}$ é um ideal maximal (não nulo) de $\mathbb{Z}$. Dessa forma, usando que $\mathbb{Z}$ é um anel, temos que o anel quociente $\dfrac{\mathbb{Z}}{I \cap \mathbb{Z}}$ é um corpo.

Consideremos a aplicação $\phi := \pi \circ Id$

$$\phi : \mathbb{Z} \xrightarrow{Id} \mathbb{Z}[\zeta] \xrightarrow{\pi} \frac{\mathbb{Z}[\zeta]}{I},$$

onde Id o homomorfismo identidade e π homomorfismo canônico, ou seja, tal que $\pi(x) = x + I$ para todo $x \in \mathbb{Z}[\zeta]$. Pode-se verificar diretamente que $Ker(\varphi) = I \cap \mathbb{Z}$. Assim, utilizando o Teorema de Isomorfismos de Anéis, obtemos o seguinte isomorfismo:

$$\frac{\mathbb{Z}}{I \cap \mathbb{Z}} \simeq Im(\phi) \subseteq \frac{\mathbb{Z}[\zeta]}{I} \tag{6.6}$$

Agora, utilizando o isomorfismo acima, juntamente ao fato de $\frac{\mathbb{Z}}{I \cap \mathbb{Z}}$ ser corpo, provaremos que $\frac{\mathbb{Z}[\zeta]}{I}$ também é corpo. Desse modo, como $\mathbb{Z}[\zeta]$ é um domínio de integridade, concluiremos que I é um ideal maximal de $\mathbb{Z}[\zeta]$, como queremos.

Para essa parte da demonstração, utilizaremos outras afirmações.

Afirmação 2: *Sejam A e B domínios tais que $A \subseteq B$ e B é inteiro sobre A. Se B é corpo, então A também é corpo.*[3]

Prova. Seja $a \in A$ com $a \neq 0$. Queremos provar que a possui inverso multiplicativo em A.

Como $A \subseteq B$, temos que existe $a^{-1} \in B$ tal que $a \cdot a^{-1} = 1$. Por outro lado, como B é inteiro sobre A e $a^{-1} \in B$, temos que existem $a_0, \ldots, a_{n-1} \in A$, não todos nulos, tais que:

$$\left(a^{-1}\right)^n + a_{n-1}\left(a^{-1}\right)^{n-1} + \ldots + a_1\left(a^{-1}\right) + a_0 = 0$$

Multiplicando a equação acima por a^{n-1} temos:

$$a^{-1} + a_{n-1} + \ldots + a_1 a^{n-2} + a_0 a^{n-1} = 0$$

resultando que

$$a^{-1} = -\left(a_{n-1} + \ldots + a_1 a^{n-2} + a_0 a^{n-1}\right)$$

Ou seja, $a^{-1} \in A$, como queríamos.

Afirmação 3: *O anel quociente $\frac{\mathbb{Z}[\zeta]}{I}$ é inteiro sobre $\frac{\mathbb{Z}}{I \cap \mathbb{Z}}$.*

Prova. Seja $\beta \in \frac{\mathbb{Z}[\zeta]}{I}$, ou seja, $\beta = \gamma + I$ para algum $\gamma \in \mathbb{Z}[\zeta]$. Para efeito de notação, façamos $\beta = \gamma + I =: \overline{\gamma}$. Queremos provar que existe polinômio mônico não nulo em $\frac{\mathbb{Z}}{I \cap \mathbb{Z}}$ que anula β. Sabemos que γ é inteiro sobre $\mathbb{Z}$, uma vez que o anel $\mathbb{Z}[\zeta]$ é inteiro sobre $\mathbb{Z}$. Assim, existem $a_0, \ldots, a_n \in \mathbb{Z}$ satisfazendo:

$$a_0 + a_1\gamma + \ldots + a_n\gamma^n = 0$$

sendo n o menor natural para o qual isso ocorre.

Tomando a classe da equação acima módulo $\frac{\mathbb{Z}}{I \cap \mathbb{Z}}$, obtemos um polinômio que satisfaz a condição esperada:

$$\overline{a_0} + \overline{a_1}\,\overline{\gamma} + \ldots + \overline{a_n}\,\overline{\gamma^n} = \overline{0}$$

Assim, utilizando a inclusão em (6.6) e a Afirmação 3 acima, pela Afirmação 2, concluímos que $\frac{\mathbb{Z}}{I \cap \mathbb{Z}}$ é corpo, provando que I é ideal maximal. □

[3] Pode-se provar mais: nessas circunstâncias, B ser corpo é condição necessária e suficiente para que A também o seja, conforme é mostrado em [3] (Proposição 3.2, p. 72).

Observação 6.3.3. O resultado que demonstramos acima pode ser generalizado para qualquer anel de inteiros de um corpo algébrico. Nesse contexto, pode-se demonstrar que $O_{\mathbb{L}}$ é sempre um domínio de Dedekind quando $\mathbb{L}$ é uma extensão finita de $\mathbb{Q}$, conforme é feito em [4] (Proposição 14, p. 764).

Na próxima subseção, provaremos que em um domínio de Dedekind, todo ideal próprio não nulo se fatora unicamente em um produto de ideais primos. Dessa forma, concluiremos que todo ideal próprio e não nulo em $\mathbb{Z}[\zeta]$ pode ser escrito como o produto de ideais primos.

Assim, ainda que não tenhamos necessariamente que cada elemento em $\mathbb{Z}[\zeta]$ seja fatorado unicamente em elementos irredutíveis, obtemos uma noção semelhante ao fatorarmos em ideais primos, os quais Kummer havia denominado *números ideais*.

Para a demonstração desse fato, necessitaremos de um tipo específico de ideais, chamados *ideais fracionários*, os quais serão também fundamentais para o estudo dos *primos regulares*.

6.3.3 Ideais Fracionários

Definição 6.3.5. *Sejam $\mathbb{L}$ um corpo algébrico (i.e., uma extensão finita de $\mathbb{Q}$) e $M \subseteq \mathbb{L}$. Dizemos que M é um ideal fracionário de $O_{\mathbb{L}}$ (anel de inteiros algébricos de $\mathbb{L}$ sobre $\mathbb{Z}$) se as seguintes condições são satisfeitas:*

(*i*) *Existe $\gamma \in O_{\mathbb{L}}$ tal que $\gamma M \subseteq O_{\mathbb{L}}$;*

(*ii*) *M é um $O_{\mathbb{L}}$-módulo, ou seja,*

- *Dados $x, y \in M$, tem-se que $x + y \in M$;*
- *Dados $x \in M$ e $\alpha \in O_{\mathbb{L}}$, tem-se que $\alpha x \in M$.*

Observação 6.3.4. Notemos que todo ideal de A é um ideal fracionário, bastando tomar $\gamma = 1$ na definição acima. Porém, existem ideais fracionários que não são ideais. Na verdade, os ideais fracionários são apenas uma classe especial de *módulos* (veja [11]).

Embora a noção de ideal fracionário possa ser utilizada sobre qualquer corpo algébrico, quando tomamos $O_{\mathbb{L}}$ como um domínio de Dedekind, o seu conjunto de ideais fracionários adquire uma estrutura de grupo multiplicativo, como será mostrado adiante.

Antes de provarmos tal resultado, relembramos o conceito de *produto de ideais* e apresentamos a noção de divisibilidade envolvendo os mesmos.

Definição 6.3.6. *Sejam I e J ideais de um domínio A. Definimos o produto de I por J, denotado por IJ, como:*

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \text{ , em que } x_i \in I, y_i \in J \text{ e } n \in \mathbb{N} \right\}$$

Em outras palavras, o produto IJ é definido como sendo o conjunto de todas as somas finitas de elementos da forma xy, em que $x \in I$ e $y \in J$.

Observação 6.3.5. Apesar de os ideais fracionários não serem, necessariamente, ideais, estenderemos a noção de produto de ideais, tal como foi apresentada acima, para os ideais fracionários.

Definição 6.3.7. *Seja $\mathbb{L}$ um corpo algébrico, cujo anel de inteiros algébricos seja dado por $\mathcal{O}_{\mathbb{L}}$. Consideremos I e J ideais de $\mathcal{O}_{\mathbb{L}}$. Dizemos que J divide I se existe um ideal $K \in \mathcal{O}_{\mathbb{L}}$ tal que $I = KJ$.*

Nessas circunstâncias, o seguinte resultado garante a estrutura de grupo multiplicativo para o conjunto de ideais fracionários quando $\mathcal{O}_{\mathbb{L}}$ é um domínio de Dedekind.

Proposição 6.3.5. *Seja $\mathbb{L}$ um corpo algébrico. O conjunto de ideais fracionários $\mathcal{F}(\mathbb{L})$ de $\mathcal{O}_{\mathbb{L}}$, quando o mesmo é um domínio de Dedekind, constitui um grupo abeliano multiplicativo sob o produto de ideais. Em particular, o conjunto de ideais fracionários $\mathcal{F}$ de $\mathbb{Z}[\zeta]$ é um grupo multiplicativo abeliano.*

Demonstração. A demonstração completa desta proposição para o caso em que $\mathbb{L} = \mathbb{Z}[\zeta]$ pode ser encontrada em [3] (Teorema 4.1, p. 102). Para o caso geral, a prova é completamente análoga. Apresentaremos aqui apenas uma ideia geral da prova.

Notemos que, a fim de que $\mathcal{F}(\mathbb{L})$ seja um grupo multiplicativo, devemos ter que tal conjunto é não vazio (o que é imediato, visto que todo ideal de $\mathcal{O}_{\mathbb{L}}$ é, em particular, um ideal fracionário), fechado para a multiplicação de ideais e dotado de um elemento neutro (a saber, o próprio anel $\mathcal{O}_{\mathbb{L}}$). Além disso, a operação em questão deve ser associativa e comutativa e, por fim, todo ideal fracionário deve admitir um inverso multiplicativo em $\mathcal{F}(\mathbb{L})$.

Com exceção da existência de inverso multiplicativo, todos os demais resultados decorrem exclusivamente das definições de ideal fracionário e produto de ideais, sendo necessários apenas alguns cálculos algébricos. Dessa forma, para a prova dos mesmos não se faz necessária a condição de $\mathbb{L}$ ser um domínio de Dedekind.

No entanto, para a existência do inverso multiplicativo, tal exigência é, não somente necessária, como, também, suficiente. Com efeito, o resultado aqui enunciado constitui uma outra caracterização para os domínios de Dedekind. Para a demonstração deste fato, são necessárias uma série de afirmações auxiliares, envolvendo o cálculo

com os ideais fracionários. Destacaremos apenas o formato do inverso multiplicativo e algumas de suas propriedades, as quais serão utilizadas posteriormente.

Dado $I \in \mathcal{F}(\mathbb{L})$, sabemos que existe $\gamma \in \mathcal{O}_{\mathbb{L}}$ tal que $\gamma I \subseteq \mathcal{O}_{\mathbb{L}}$. Utilizando que $\mathcal{O}_{\mathbb{L}}$ é domínio de Dedekind, pode-se provar que $\gamma I =: J$ é um ideal de $\mathcal{O}_{\mathbb{L}}$. Nessas condições, o inverso multiplicativo de I é dado por:

$$I^{-1} := \gamma J^{-1} := \gamma\{x \in \mathbb{L} : \ xJ \subseteq \mathcal{O}_{\mathbb{L}}\}$$

Além disso, mostra-se que, se M é um ideal maximal de $\mathcal{O}_{\mathbb{L}}$ satisfazendo $I \subseteq M$, então tem-se que $I \subseteq IM^{-1}$ e que, para todo ideal J de $\mathcal{O}_{\mathbb{L}}$, segue que $(JI^{-1})I = J$. □

Corolário 6.3.3. *Sejam I e J ideais de $\mathcal{O}_{\mathbb{L}}$. Então, I divide J se, e somente se, $J \subseteq I$.*

Demonstração. Caso tenhamos que I divide J, então existe $K \in \mathcal{O}_{\mathbb{L}}$ tal que $J = KI$, donde resulta que $J \subseteq I$. Por outro lado, caso $J \subseteq I$, temos que:

$$JI^{-1} \subseteq II^{-1} = \mathcal{O}_{\mathbb{L}}$$

Assim, JI^{-1} é um ideal de $\mathcal{O}_{\mathbb{L}}$. E, como $(JI^{-1})I = J$, concluímos que I divide J. □

A partir da definição de grupo de classe, e sabendo que o mesmo adquire uma estrutura de grupo multiplicativo no caso em que o domínio a ele associado é de Dedekind, obtemos um dos principais resultados referentes à unicidade da fatoração em ideais primos.

Teorema 6.3.4. *Se A é um domínio de Dedekind, então todo ideal próprio não nulo tem fatoração única em ideais primos.*

Demonstração. Seja $\mathcal{S}$ o conjunto de todos ideais próprios não nulos em A que não são produto de ideais primos.

Caso tenhamos $\mathcal{S} = \emptyset$, não há nada a fazer, visto que todos ideais próprios e não nulos em A serão, consequentemente, o produto de ideais primos.

Assim, consideremos $\mathcal{S} \neq \emptyset$. Como A é um domínio de Dedekind, em particular, A é um anel noetheriano. Dessa forma, $\mathcal{S}$ admite um elemento maximal, digamos I. Observemos que I não pode ser um ideal maximal, uma vez que todo ideal maximal é um ideal primo (pois A é anel comutativo) e, caso fosse ideal primo, I seria sua própria fatoração em ideais primos.

Então, podemos considerar o ideal M como sendo o ideal maximal (e, consequentemente, ideal primo) contendo I, ou seja, $I \subsetneq M$. Desse modo, temos que:

$$I \subsetneq IM^{-1} \subsetneq MM^{-1} = A,$$

donde $M^{-1}I$ é um ideal próprio de A que contém I.

Destacamos que a primeira inclusão decorre diretamente do fato de I ser um ideal e, em particular, ser um ideal fracionário de A.

Por outro lado, notemos que, como I está contido tanto em M quanto em IM^{-1}, nenhum deles pode estar em $\mathcal{S}$, pois, caso contrário, teríamos uma contradição com o fato de I ser elemento maximal de $\mathcal{S}$. Assim, temos, pela definição de $\mathcal{S}$, que M e IM^{-1} se escrevem como produto de ideais primos.

Consequentemente, existem $M_1, \ldots, M_r$, com $r \in \mathbb{N}$, ideais primos não nulos de A que satisfazem:

$$IM^{-1} = M_1 \cdots M_r$$

Multiplicando a equação anterior pelo inverso multiplicativo de M^{-1}, obtemos:

$$I = IM^{-1}M = MM_1 \cdots M_r$$

Como M também se escreve como produto de ideais primos, concluímos que I se decompõe em ideais primos, uma contradição com o fato de $I \notin \mathcal{S}$. Logo, temos que $\mathcal{S} \neq \emptyset$, resultando que todo ideal próprio não nulo em A se fatora em ideais primos.

Resta, então, demonstrarmos a unicidade de tal fatoração. Para tanto, consideremos $I_1, \ldots, I_r$ e $J_1, \ldots, J_s$, sendo $r, s \in \mathbb{N}$ e $r \leq s$, ideais primos não nulos e próprios de A tais que:

$$I_1 \cdots I_r = J_1 \cdots J_s \tag{6.7}$$

Notemos que I_1 divide o produto $J_1 \cdots J_s$ e, como I_1 é um ideal primo, segue que ele divide J_i para algum $i \in \{1, \ldots, s\}$. Sem perda de generalidade, consideremos que I_1 divida J_1. Assim, existe um ideal K em A tal que $J_1 = I_1 K \subseteq I_1$.

Por outro lado, como A é um domínio de Dedekind, sabemos que todos ideais primos não nulos são ideais maximais. Nesse contexto, temos que J_1 e I_1 são maximais, resultando que os mesmos são iguais (visto que $I_1, J_1 \neq A$ por hipótese). Desta forma, multiplicando a equação (6.7) por I^{-1}, temos:

$$I_2 \cdots I_r = J_2 \cdots J_s$$

Repetindo esse processo, obtemos:

$$A = J_{r+1} \cdots J_s$$

Consequentemente, segue que $J_{r+2} \cdots J_s = (J_{r+1})^{-1} \not\supseteq A$, uma contradição, pois $J_{r+2} \cdots J_s \subseteq A$.

Logo, devemos ter $r = s$, donde segue que as fatorações tomadas inicialmente são as mesmas a menos da ordem dos fatores. □

Corolário 6.3.5. *Todo ideal próprio e não nulo do anel de inteiros ciclotômicos $\mathbb{Z}[\zeta]$ se fatora unicamente em ideais primos.*

Além de estabelecer a unicidade da fatoração em ideais primos para o anel de inteiros $\mathbb{Z}[\zeta]$, como mostrado acima, a noção de ideal fracionário permite ainda estabelecer sob quais condições temos a unicidade da fatoração de elementos de $\mathbb{Z}[\zeta]$ em irredutíveis.

Teorema 6.3.6. *A fatoração de elementos em $\mathbb{Z}[\zeta]$ é única se, e somente se, $\mathbb{Z}[\zeta]$ é um domínio de ideais principais.*

Demonstração. Já sabemos que todo DIP é, em particular, um DFU. Assim, para a demonstração do teorema, precisamos provar apenas que, se a fatoração de elementos em $\mathbb{Z}[\zeta]$ é única, então, $\mathbb{Z}[\zeta]$ é um DIP.

Pelo corolário 6.3.5, sabemos que todo ideal próprio e não nulo de $\mathbb{Z}[\zeta]$ se fatora unicamente em ideais primos. Além disso, como o produto de ideais principais é também um ideal principal, segue que a demonstração do teorema se reduz a mostrar que, sob a hipótese acima, todo ideal primo de $\mathbb{Z}[\zeta]$ é principal.

Seja I ideal primo não nulo de $\mathbb{Z}[\zeta]$. Consideremos $\alpha \in I$ com $\alpha \neq 0$. Notemos que α não é inversível pois, em caso contrário, teríamos que $1 \in I$ resultando que $I = \mathbb{Z}[\zeta]$. No entanto, isso geraria uma contradição com o fato de I ser ideal primo.

Por outro lado, sabemos, da hipótese inicial, que $\mathbb{Z}[\zeta]$ é um domínio de fatoração única. Então, existem $m \in \mathbb{N}$ e $p_1, \ldots, p_m \in \mathbb{Z}[\zeta]$ elementos irredutíveis tais que:

$$\alpha = p_1 \cdots p_m \in I$$

Como I é um ideal primo, devemos ter $p_i \in I$ para algum $i \in \{1, \ldots, m\}$, ou seja, $\langle p_i \rangle \subseteq I$. Agora, sabemos que em um DFU, todo elemento irreudível é primo, resultando que p_i é primo em $\mathbb{Z}[\zeta]$. Desse modo, segue que o ideal $\langle p_i \rangle$ é primo. Como $\mathbb{Z}[\zeta]$ é um domínio de Dedekind, temos que tal ideal é, consequentemente, um ideal maximal. Nesse contexto, analisando as inclusões:

$$\langle p_i \rangle \subseteq I \subseteq \mathbb{Z}[\zeta]$$

e utilizando o fato de $\langle p_i \rangle$ ser maximal, devemos ter que $I = \langle p_i \rangle$, visto que $I \neq \mathbb{Z}[\zeta]$.

Logo, concluímos que I é um ideal principal e, por consequência, pela argumentação feita acima, temos que $\mathbb{Z}[\zeta]$ é um domínio de ideais principais. □

Notemos que, por meio desse resultado, conseguimos avaliar melhor o porquê de a ideia inicial de Lamé não ser válida para todos os domínios $\mathbb{Z}[\zeta]$, uma vez que,

dependendo do valor de p, o anel $\mathbb{Z}[\zeta]$ pode não ser um domínio de fatoração única. Sob tais circunstâncias, sua ideia não seria capaz de demonstrar o Último Teorema de Fermat para todos expoentes primos.

Dessa forma, a utilização da fatoração de ideais em ideais primos torna-se mais promissora, tendo em vista que sua unicidade é sempre garantida em $\mathbb{Z}[\zeta]$, conforme demonstrado no Corolário 6.3.5, ao contrário da unicidade da fatoração de elementos em irredutíveis.

Com o intuito de melhor nos aprofundarmos na fatoração de ideais e demonstrarmos o teorema estabelecido por Kummer, o qual generaliza a abordagem pretendidaa por Lamé para os *primos regulares*, apresentaremos na próxima seção conceitos fundamentais para o entendimento e a prova de tal teorema.

6.4 GRUPO DE CLASSE E PRIMOS REGULARES

A fim de definirmos *grupo de classe* e melhor compreendermos a noção da fatoração em ideais, apresentamos o conceito de norma de um ideal.

Definição 6.4.1. *Sejam $\mathbb{L}$ um corpo algébrico I um ideal não nulo de $\mathcal{O}_{\mathbb{L}}$. A norma de I (ou ainda, a ordem de I) é definida como a cardinalidade do anel quociente $\left(\frac{\mathcal{O}_{\mathbb{L}}}{I}\right)$, ou seja,*

$$N(I) = \#\left(\frac{\mathcal{O}_{\mathbb{L}}}{I}\right)$$

Provaremos agora que, nas condições da definição acima, a norma de um ideal está bem definida, isto é, $N(I)$ é finita. Para tanto, consideraremos o seguinte resultado, cuja demonstração pode ser encontrada em [18] (Corolário 5.10, p. 115) e em [10] (Lema 6.60, p. 293):

Lema 6.4.1. *Sejam $\mathbb{L}$ um corpo algébrico e $\alpha \in \mathcal{O}_{\mathbb{L}}$, com $\alpha \neq 0$. Consideremos o ideal principal de $\mathcal{O}_{\mathbb{L}}$ gerado por α, ou seja, o ideal $I = \langle\alpha\rangle$. Então, temos que a norma de I satisfaz a seguinte igualdade:*

$$N(I) = N(\langle\alpha\rangle) = \#\left(\frac{\mathcal{O}_{\mathbb{L}}}{\langle\alpha\rangle}\right) = |N(\alpha)|$$

em que $N(\alpha)$ é a norma[4] de α com relação ao corpo algébrico $\mathbb{L}$.

Em particular, a norma de um ideal principal é finita.

Proposição 6.4.1. *Sejam $\mathbb{L}$ um corpo algébrico e I ideal não nulo de $\mathcal{O}_{\mathbb{L}}$. Então, $N(I)$ é finita.*

Demonstração. Seja $\alpha \in I$, com $\alpha \neq 0$. Como I é ideal de $\mathcal{O}_{\mathbb{L}}$, temos que $\mathcal{O}_{\mathbb{L}}\alpha \subseteq I$. Em outras palavras, temos que $\langle\alpha\rangle \subseteq I$, sendo $\langle\alpha\rangle$ o ideal de $\mathcal{O}_{\mathbb{L}}$ gerado por α. Desse modo,

[4] Tal noção foi apresentada na Definição 6.2.4.

temos que:

$$\frac{I}{\langle\alpha\rangle} \subseteq \frac{O_{\mathbb{L}}}{\langle\alpha\rangle}$$

Consideremos a seguinte aplicação:

$$\begin{array}{rccc} \phi : & \left(\dfrac{O_{\mathbb{L}}}{\langle\alpha\rangle}\right) & \longrightarrow & \left(\dfrac{O_{\mathbb{L}}}{I}\right) \\ & x + \langle\alpha\rangle & \longmapsto & x + I \end{array}$$

Notemos que, por construção, ϕ é um homomorfismo sobrejetor de anéis. Além disso, seu núcleo é dado por:

$$\begin{aligned} Ker(\phi) &= \{x + \langle\alpha\rangle : \phi(x + \langle\alpha\rangle) = 0\} \\ &= \{x + \langle\alpha\rangle : x + I = 0\} \\ &= \{x + \langle\alpha\rangle : x \in I\} \\ &= \left(\frac{I}{\langle\alpha\rangle}\right) \end{aligned}$$

Assim, aplicando o Teorema dos Isomorfismos de Anéis, obtemos o isomorfismo:

$$\frac{\left(\dfrac{O_{\mathbb{L}}}{\langle\alpha\rangle}\right)}{\left(\dfrac{I}{\langle\alpha\rangle}\right)} \simeq \left(\frac{O_{\mathbb{L}}}{I}\right)$$

Consequentemente, temos que a cardinalidade de $\left(\dfrac{O_{\mathbb{L}}}{I}\right)$ é igual à cardinalidade do quociente à esquerda na equação acima.

Observemos ainda que, como $\left(\dfrac{O_{\mathbb{L}}}{\langle\alpha\rangle}\right)$ e $\left(\dfrac{I}{\langle\alpha\rangle}\right)$ são anéis quocientes, em particular, eles são grupos abelianos aditivos. Mais ainda, temos que o segundo é subgrupo do primeiro.

Por outro lado, pelo lema anterior, sabemos que a cardinalidade do primeiro é finita, no caso, igual a $|N(\alpha)|$. Dessa forma, também a cardinalidade do segundo é finita, pois o mesmo é um de seus subgrupos.

Agora, como o grupo $\left(\dfrac{O_{\mathbb{L}}}{\langle\alpha\rangle}\right)$ é finito, aplicando o Teorema de Lagrange, temos que as ordens destes grupos são tais que:

$$\left|\frac{I}{\langle\alpha\rangle}\right| \text{ divide } \left|\frac{O_{\mathbb{L}}}{\langle\alpha\rangle}\right| = |N(\alpha)|$$

Portanto, segue que a cardinalidade do quociente à esquerda equivale à divisão das ordens dos grupos acima, donde resulta que:

$$\frac{\left|\frac{\mathcal{O}_{\mathbb{L}}}{\langle\alpha\rangle}\right|}{\left|\frac{I}{\langle\alpha\rangle}\right|} = \#\left(\frac{\mathcal{O}_{\mathbb{L}}}{I}\right) =: N(I)$$

Como as ordens acima são ambas finitas, concluímos que a cardinalidade de $\left(\frac{\mathcal{O}_{\mathbb{L}}}{I}\right)$ é finita. Logo, $N(I)$ é finita, como queríamos provar. □

De modo semelhante à norma de um elemento em $\mathbb{Z}[\zeta]$, temos que a norma de um ideal é multiplicativa, ou seja, vale o seguinte resultado, que pode ser encontrado em [3] (Proposição 4.7, p. 112):

Proposição 6.4.2. *Se I e J são ideais não nulos de $\mathbb{Z}[\zeta]$, então $N(IJ) = N(I)N(J)$.*

Segue daí o seguinte corolário:

Corolário 6.4.1. *Seja I um ideal não nulo de $\mathbb{Z}[\zeta]$. Se $N(I)$ é um número primo em $\mathbb{Z}$, então I é um ideal primo.*

Demonstração. Seja $N(I) = p$, com p número primo. Pela existência da fatoração em ideais primos, temos que existem ideais $I_1, \ldots, I_n$ em $\mathbb{Z}[\zeta]$ satisfazendo $I = I_1 \cdots I_n$, donde, pela proposição acima, segue que:

$$N(I) = N(I_1) \cdots N(I_n) = p$$

Por outro lado, como $N(I_j)$ é um número natural para cada $j = 1, \ldots, n$ e p é um número primo, devemos ter $N(I_j) = 1$ ou $N(I_j) = p$. Assim, a decomposição de I em ideais primos, a qual é única, consiste apenas de $n - 1$ ideais unitários e um único ideal I_{j_0}, com $j_0 \in \{1, \ldots, n\}$, tal que $N(I_{j_0}) = p$. Consequentemente, temos que $I = I_{j_0}$, demonstrando que I é um ideal primo. □

Tais propriedades da norma de um ideal serão fundamentais na demonstração do Teorema de Kummer.

Neste momento, já somos capazes de definir o conceito de grupo de classe.

Definição 6.4.2. *Seja $\mathbb{L}$ um corpo algébrico e $\mathcal{F}(\mathbb{L})$ o grupo de seus ideais fracionários não nulos. Consideremos ainda $\mathcal{P}(\mathbb{L})$ o subgrupo de $\mathcal{F}(\mathbb{L})$ constituído pelos ideais fracionários principais. O grupo de classe, denotado por $\mathcal{H}(\mathbb{L})$ é dado por:*

$$\mathcal{H}(\mathbb{L}) = \frac{\mathcal{F}(\mathbb{L})}{\mathcal{P}(\mathbb{L})}$$

A norma de $\mathcal{H}(\mathbb{L})$ é denominada número de classe [5] *de $\mathcal{O}_{\mathbb{L}}$ e é representada por:*

$$h(\mathbb{L}) = N(\mathcal{H}) := \#\left(\frac{\mathcal{O}_{\mathbb{L}}}{\mathcal{H}}\right)$$

Observação 6.4.1. No caso em que $\mathbb{L} = \mathbb{Z}[\zeta]$, ou seja, corresponde ao anel de inteiros ciclotômicos, omitiremos a referência a $\mathbb{Z}[\zeta]$. Desse modo, denotaremos seu grupo de ideais fracionários como $\mathcal{F}$ e o subgrupo de ideais fracionários principais como $\mathcal{P}$. Nessas circunstâncias, diremos que $\mathcal{H}$ é o grupo de classes de $\mathbb{Z}[\zeta]$, em que:

$$\mathcal{H} := \frac{\mathcal{F}}{\mathcal{P}}$$

De modo semelhante, representaremos o número de classe de $\mathbb{Z}[\zeta]$ por h.

Definição 6.4.3. *Dado $\mathbb{L}$ corpo algébrico, dizemos que dois ideais em $\mathcal{O}_{\mathbb{L}}$ estão relacionados, e escrevemos $I \sim J$, se existe um ideal fracionário principal K em $\mathcal{O}_{\mathbb{L}}$ tal que $I = KJ$ ou, equivalentemente, quando $IJ^{-1} \in \mathcal{P}(\mathbb{L})$.*

Em particular, se I, J são ideais fracionários de $\mathcal{O}_{\mathbb{L}}$, diremos que I e J são equivalentes se eles pertencerem à mesma classe de $\mathcal{P}(\mathbb{L})$ em $\mathcal{F}(\mathbb{L})$, ou seja, se forem levados para o mesmo elemento de $\mathcal{H}(\mathbb{L})$.

A definição acima nos permite definir a classe de equivalência de um ideal I de $\mathbb{Z}[\zeta]$ de modo a obter a estrutura de grupo multiplicativo abeliano no conjunto das classes de equivalência de $\mathbb{Z}[\zeta]$.

Para tanto, podemos definir a classe de equivalência do ideal I como:

$$[I] = \{J \in \mathcal{F} : \ I = KJ \text{ para algum } K \in \mathcal{P}\}$$

Além disso, considerando I um ideal fracionário, temos que existem $\gamma \in \mathbb{Z}[\zeta]$ e J ideal de $\mathbb{Z}[\zeta]$ satisfazendo $I = d^{-1}J$. Dessa forma, segue que:

$$J = dI = \langle d \rangle I$$

Agora, como $\langle d \rangle \in \mathcal{P}$, temos que $J \sim I$, ou seja, toda classe de equivalência de um ideal em $\mathbb{Z}[\zeta]$ é não vazia.

Por outro lado, caso tenhamos I, J ideais fracionários equivalentes, então deve existir um ideal principal $K \in \mathcal{P}$ tal que $I = KJ$ e $K = c^{-1}L$, para algum $c \in \mathbb{Z}[\zeta]$ e algum $L \in \mathcal{P}$. Consequentemente, temos que:

$$I = KJ = c^{-1}LJ \text{ , ou seja, } \ I\langle c \rangle = LJ$$

[5] Notemos que, pela Proposição 6.4.1, o número de classe está bem definido como um número natural.

De modo semelhante, caso tenhamos $IM = JN$, em que M, N são ideais em $\mathcal{P}$, resulta que I e J são equivalentes.

Logo, podemos redefinir a classe de equivalência do ideal I de modo mais geral:

$$[I] = \{J \in \mathcal{F} : \ IM = JN \text{ em que } M, N \in \mathcal{P}\}$$

Definimos, então, o produto de classes de equivalência da seguinte forma:

$$[I][J] := [IJ]$$

Sob tais condições, é possível provar que tal operação é comutativa e associativa. Além disso, seu elemento neutro é dado por:

$$1_{\mathcal{H}} := \left[\mathbb{Z}[\zeta]\right]$$

Com efeito, utilizando a definição do produto de classes e a definição do ideal I^{-1} apresentada na Proposição 6.3.5, obtemos as seguintes relações:

$$\begin{aligned} \left[I\right]\left[\mathbb{Z}[\zeta]\right] &= \left[I\mathbb{Z}[\zeta]\right] = \left[I\right] \\ \left[I\right]\left[I^{-1}\right] &= \left[II^{-1}\right] = \left[\mathbb{Z}[\zeta]\right] \end{aligned}$$

Portanto, concluímos que, sob tal operação, o grupo de classes $\mathcal{H}$ é um grupo multiplicativo abeliano.

Observação 6.4.2. Destacamos que essa análise pode ser feita para qualquer anel de inteiros $\mathcal{O}_{\mathbb{L}}$. Utilizamos o anel $\mathbb{Z}[\zeta]$ apenas para simplificar a notação. Contudo, sob qualquer anel de inteiros define-se a classe de equivalência de um ideal de modo inteiramente análogo.

Consequentemente, prova-se que o conjunto das classes de equivalência $\mathcal{H}(\mathbb{L})$ em $\mathcal{O}_{\mathbb{L}}$ é de fato um grupo. Mais precisamente, um grupo multiplicativo abeliano sob a operação de produto de classes definida como acima.

Definição 6.4.4. *Dizemos que p é um primo regular se p é um primo que não divide o número de classe h de* $\mathbb{Z}[\zeta]$.

A partir do número de classe, obtemos um importante resultado sobre o anel $\mathbb{Z}[\zeta]$, o qual estabelece quando a unicidade da fatoração em irredutíveis será válida para todo elemento de $\mathbb{Z}[\zeta]$ em função de h.

Teorema 6.4.2. *O anel de inteiros ciclotômicos* $\mathbb{Z}[\zeta]$ *é um DFU se, e somente se, o número de classe h de* $\mathbb{Z}[\zeta]$ *é* 1.

Demonstração. Para a demonstração deste resultado, utilizaremos o Teorema 6.3.6, segundo o qual $\mathbb{Z}[\zeta]$ é um domínio de fatoração única se, e somente se, é um domínio de ideais principais.

Assim, utilizando as definições de grupo e número de classe, segue que:

$$\mathbb{Z}[\zeta] \text{ é um DFU} \Leftrightarrow \mathbb{Z}[\zeta] \text{ é um DIP} \Leftrightarrow \mathcal{F} = \mathcal{P} \Leftrightarrow N(\mathcal{H}) = h = 1$$

□

O teorema 6.4.2 nos fornece um método para verificar se o anel $\mathbb{Z}[\zeta]$ é um domínio fatorial ou não. Caso tal condição se verifique, a abordagem de Lamé torna-se válida e, consequentemente, o Último Teorema de Fermat é demonstrado para o primo p associado a tal anel.

No caso dos anéis de inteiros ciclotômicos para os quais o valor de p é inferior a 100, pode-se mostrar, por meio de métodos computacionais, que os únicos cujo número de classe é 1 são aqueles em que $p = 3, 5, 7, 11, 13, 17$ e 19 (para as demonstrações, sugerimos consultar o capítulo 10 de [18]). Assim, a ideia de Lamé nos permite demonstrar o UTF para os primeiros números primos.

A tabela 2 apresenta os números de classe para os anéis ciclotômicos com p menor que 100, possibilitando a identificação dos primeiros números regulares.

p	h_1	p	h_1
3	1	43	211
5	1	47	$5 \cdot 139$
7	1	53	4889
11	1	59	$3 \cdot \mathbf{59} \cdot 233$
13	1	61	$41 \cdot 1861$
17	1	67	$\mathbf{67} \cdot 12739$
19	1	71	$7^2 \cdot 79241$
23	3	73	$89 \cdot 134353$
29	2^3	79	$5 \cdot 53 \cdot 377911$
31	3^2	83	$3 \cdot 279405653$
37	**37**	89	$113 \cdot 118401449$
41	11^2	97	$577 \cdot 3457 \cdot 206209$

Tabela 2 – Números de classe para primos menores que 100 [18]

Contudo, apesar da validade da ideia de Lamé para esses primos, a abordagem feita por Kummer é mais abrangente, na medida em que demonstra o teorema para quaisquer primos regulares, ou seja, primos que não dividem o número de classe. Em particular, quando temos $h = 1$ (ou, equivalentemente, $\mathbb{Z}[\zeta]$ sendo um domínio fatorial), esta condição se verifica.

Mais precisamente, considerando ainda os primos menores que 100, os únicos casos do UTF que não são provados pelo Teorema de Kummer são aqueles em que o expoente primo é $37, 59, 67$ (primos irregulares) e 74 (o qual não é múltiplo de 4 nem de nenhum primo regular).

Observação 6.4.3. Destacamos que, no caso em que $p = 3$, temos a unicidade da fatoração no anel de inteiros de Eisenstein, resultado que foi utilizado na prova do Último Teorema de Fermat: Caso $n = 3$, a qual apresentamos no Capítulo 3.

6.5 O TEOREMA DE KUMMER

Seguindo a ideia de Sophie Germain, Kummer adotou a divisão do UTF nos dois casos: quando o primo p não divide nenhuma das variáveis x, y e z (Caso 1) e quando ele divide exatamente uma delas (Caso 2). Nessas circunstâncias, ele provou o Teorema para ambos os casos, sob a condição de p ser um primo regular.

No entanto, os conceitos e as propriedades vistos até o momento nos permitem demonstrar apenas o primeiro caso, o que será feito nesta última seção. Embora, ao final da demonstração deste, sua generalização para o segundo se mostre relativamente acessível, ainda que possivelmente mais longa e trabalhosa, a verificação de um dos resultados auxiliares torna-se complicada. Mais precisamente, teríamos que mostrar que, fixado um primo regular p, se uma unidade em $\mathbb{Q}(\zeta)$ é congruente a um inteiro racional módulo p, então ela é a p-ésima potência de outra unidade do corpo ciclotômico (conforme mostraremos no Lema 6.5.1). Porém, no caso geral, a prova desse fato envolve métodos complexos de Teoria de Ideais e Teoria dos Números Naturais, os quais se distanciam de nosso objetivo principal. A demonstração completa do UTF para os primos regulares sob essa abordagem é apresentada em [13] (Lema 3.4, p. 86) e em [5] (Prova do Caso *II*, p. 171).

Para a demonstração do Teorema de Kummer (Caso 1), utilizaremos um ideal específico do anel de inteiros ciclotômicos $\mathbb{Z}[\zeta]$, no caso, o ideal gerado pelo elemento $1 - \zeta$, dado por:

$$I := \langle 1 - \zeta \rangle$$

Nessas condições, estabeleceremos algumas propriedades deste ideal.

Proposição 6.5.1. *Sejam $I = \langle 1 - \zeta \rangle$ e p um primo ímpar. Então, são válidas as relações:*

$$I^{p-1} = \langle p \rangle \quad e \quad N(I) = p$$

Em particular, I é um ideal primo.

Demonstração. Pelo Lema 6.2.1, sabemos que $1 - \zeta$ e $1 - \zeta^j$ são associados sempre que $j = 1, \cdots, p - 1$. Assim, utilizando a definição de norma de um elemento para $1 - \zeta$,

obtemos:

$$N(1-\zeta) = \prod_{j=1}^{p-1}(1-\zeta^j) = 1 + 1^2 + \cdots + 1^{p-1} = p$$

Dessa forma, obtemos:

$$\langle p \rangle = \prod_{j=1}^{p-1} \left\langle 1-\zeta^j \right\rangle$$

Além disso, sabemos que, fixado j, temos $I := \langle 1-\zeta \rangle = \left\langle 1-\zeta^j \right\rangle$.

Logo, segue que

$$\langle p \rangle = I^{p-1}$$

A demonstração de que $N(I) = p$, segue diretamente da definição do ideal I e do Lema 6.4.1. Sob tal condição, o fato de I ser um ideal primo decorre do Corolário 6.4.1. □

Lema 6.5.1. *Dado $\alpha \in \mathbb{Z}[\zeta]$, existe $a \in \mathbb{Z}$ tal que:*

$$\alpha^p \equiv a \pmod{I^p}$$

Demonstração. Seja $\alpha \in \mathbb{Z}[\zeta]$. Então, temos que $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, em que $a_j \in \mathbb{Z}$ para todo $j = 0, \cdots, p-2$.

Consideremos o polinômio $p(x) = a_0 + a_1 x + \cdots + a_{p-2}x^{p-2} \in \mathbb{Z}[x]$. Pelo Algoritmo da Divisão, existem $q(x), r(x) \in \mathbb{Z}[x]$, com $\deg r(x) = 0$ ou $r(x) \equiv 0$, tais que

$$p(x) = (1-x)q(x) + r(x)$$

Nessas condições, podemos escrever $r(x) = r \in \mathbb{Z}$ e, assim,

$$\alpha = p(\zeta) = (1-\zeta)q(\zeta) + r,$$

resultando que

$$\alpha \equiv r \pmod{I}$$

Além disso, temos que [6]:

$$\alpha^p - r^p = \prod_{j=0}^{p-1}(\alpha - r\zeta^j)$$

Agora, como $1-\zeta \in I$, temos $\zeta \equiv 1 \pmod{I}$ e, consequentemente, $\zeta^j \equiv 1 \pmod{I}$) para qualquer inteiro j, implicando que:

$$\alpha - r\zeta^j \equiv \alpha - r \equiv 0 \pmod{I},$$

[6] A igualdade segue da análise feita na seção 5.1; mais precisamente, da equação (6.1).

ou seja, $\alpha - r\zeta^j \in I$.

Assim, segue que

$$\alpha^p - r^p = \prod_{j=0}^{p-1}(\alpha - r\zeta^j) \in I^p$$

Logo, $\alpha^p - r^p \equiv 0 \pmod{I^p}$, donde $\alpha^p \equiv r^p \pmod{I^p}$. E, portanto, tomando $a = r^p$ obtemos o resultado esperado: $\alpha^p \equiv a \pmod{I^p}$. □

Por fim, apresentamos alguns resultados auxiliares a fim de enunciar e demonstrar o Teorema de Kummer.

Lema 6.5.2. *As únicas raízes da unidade em* $\mathbb{Q}(\zeta)$ *são da forma* $\pm\zeta^s$, *em que* $s \in \mathbb{Z}$.

Demonstração. A prova deste Lema envolve resultados específicos da Teoria Algébrica dos Números e, então, iremos apenas utilizar o resultado por ele estabelecido, sem demonstrá-lo. Uma demonstração completa é feita em [18] (Teorema 10.1, p. 170). □

Lema 6.5.3. *Seja* $p(x) \in \mathbb{Z}[x]$ *um polinômio mônico cujas raízes possuam valor absoluto* 1. *Então, cada raiz é uma raiz da unidade.*

Demonstração. Sejam $\alpha_1, \ldots, \alpha_n$ as raízes do polinômio mônico $p(x) \in \mathbb{Z}[x]$. Assim, temos que $p(x)$ tem a forma:

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

Para cada $k \in \mathbb{N}$, definimos o seguinte polinômio:

$$p_k(x) = (x - \alpha_1^k) \cdots (x - \alpha_n^k) \in \mathbb{Z}[x]$$

Fixado k, sabemos, por definição, que as funções simétricas elementares[7] de $p(x)$ são dadas por:

$$\begin{aligned} v_1 &= \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k \\ v_2 &= \alpha_1^k\alpha_2^k + \alpha_1^k\alpha_3^k + \cdots + \alpha_{n-1}^k\alpha_n^k \\ &\vdots \\ v_n &= \alpha_1 \cdot \alpha_2 \cdots \alpha_n \end{aligned}$$

Ou seja, de modo geral, temos que v_i consiste da soma com $\binom{n}{i}$ parcelas de produtos das raízes de $p_k(x)$. Mais ainda, sabemos que cada função simétrica é um

[7] Para uma maior explicação sobre as funções simétricas de um polinômio e suas propriedades, sugerimos consultar Martinez [10] (Seção 6.3, p. 265 – 267).

polinômio da forma $f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$, donde segue que $f(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$, isto é, $v_i \in \mathbb{Z}$ para todo $i = 1, \ldots, n$.

Calculando o módulo de v_1 e lembrando que, por hipótese, cada raiz tem valor absoluto igual a 1, obtemos:

$$|v_1| = \left|\alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k\right| \leq |\alpha_1|^k + \cdots + |\alpha_n|^k = \binom{n}{1} = n$$

De modo semelhante, mostra-se que, para todo $i = 1, \ldots, n$, temos:

$$|v_i| \leq \binom{n}{i} \tag{6.8}$$

Agora, utilizando as relações entre tais funções e os coeficientes de $p_k(x)$ (denominadas *Relações de Girard*), obtemos:

$$p_k(x) = x_n - v_1 x^{n-1} + v_2 x^{n-2} - \cdots + (-1)^{n-1} v_{n-1} x + (-1)^n v_n \in \mathbb{Z}[x]$$

E, como para cada i, temos que v_j é inteiro, só pode existir uma quantidade finita de polinômios do formato acima satisfazendo as desigualdades representadas em (6.8). Dessa forma, existe $m \in \mathbb{N}$ com $m \neq k$ satisfazendo:

$$p_m(x) = p_k(x)$$

Logo, existe uma permultação τ dos índices $\{1, \ldots, k\}$ tal que as funções simétricas destes polinômios verificam a relação:

$$\alpha_j^k = \alpha_{\tau(j)}^m \text{ , em que } j = 1, \ldots n$$

Assim, segue que:

$$\alpha_j^{k^2} = \left(\alpha_j^k\right)^k = \left(\alpha_{\tau(j)}^m\right)^k = \left(\alpha_{\tau((\tau(j))}^m\right)^m = \alpha_{\tau^2(j)}^{m^2}$$

Indutivamente, dado $r \in \mathbb{N}$, prova-se que:

$$\alpha_j^{k^r} = \alpha_{\tau^r(j)}^{m^r}$$

Por fim, como τ é uma permutação no conjunto de valores para o índice i, temos que $\tau^{n!}(j) = j$, implicando, pela equação anterior, que:

$$\alpha_j^{k^{n!}} = \alpha_j^{m^{n!}}$$

Portanto,

$$\alpha_j^{k^{n!} - m^{n!}} = 1$$

E, como $k \neq m$, garantindo que $k^{n!} \neq m^{n!}$, concluímos que, de fato, α_i é uma raiz da unidade para todo $i = 1, \ldots, n$. □

Lema 6.5.4 (**Lema de Kummer**). *Toda unidade de $\mathbb{Z}[\zeta]$ é da forma $r\zeta^g$, em que r é um número real e g, um inteiro.*

Demonstração. Seja $\epsilon \in \mathbb{Z}[\zeta]$ uma unidade. Como ϵ é um inteiro algébrico, temos que o mesmo é da forma:

$$\epsilon = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} =: f(\zeta)$$

em que $a_i \in \mathbb{Z}$ para todo $i = 0, \ldots, p-2$.

Agora, lembrando que $N(\zeta) = N(\zeta^j) = -1$ para todo $j = 1, \ldots, p-2$, além das propriedades da norma vistas na Proposição 6.2.3, obtemos:

$$N(\epsilon) = \prod_{i=1}^{p-1} [a_0 - a_1 - \cdots - a_{p-2}]$$

Como ϵ é uma unidade, existe $\delta \in \mathbb{Z}[\zeta]$ tal que $\epsilon\delta = 1$, donde resulta:

$$1 = N(1) = N(\epsilon\delta) = N(\epsilon)N(\delta) \therefore N(\epsilon) = \pm 1$$

Por outro lado, calculando a norma de ϵ em função dos monomorfismos σ_i de $\mathbb{Q}(\zeta)$ em $\mathbb{C}$, temos ainda que:

$$\begin{aligned} N(\epsilon) &= N(f(\zeta)) \\ &= \prod_{i=1}^{p-1} \sigma_i(a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}) \\ &= \prod_{i=1}^{p-1} a_0 + a_1 \cdot \sigma_i(\zeta) + \cdots + a_{p-2} \cdot \sigma_i(\zeta^{p-2}) \\ &= \prod_{i=1}^{p-1} a_0 + a_1\zeta^i + \cdots + a_{p-2}\zeta^{i(p-2)} \\ &= \prod_{i=1}^{p-1} f(\zeta^i) \end{aligned}$$

Ou seja, os conjugados de ϵ são da forma $\epsilon_s = f(\zeta^s)$, em que $s = 1, \ldots, p-1$.

Desse modo, temos que $\pm 1 = N(\epsilon) = \epsilon_1 \cdots \epsilon_{p-1}$.

Além disso, o conjugado complexo de ϵ_s é dado por:

$$\overline{\epsilon_s} = \overline{f(\zeta^s)} = f(\overline{\zeta^s}) = f(\zeta^{p-s}) = \epsilon_{p-s}$$

Assim, $\epsilon_s \cdot \epsilon_{p-s} = |\epsilon_s|^2 > 0$ para todo $s = 1, \ldots, p-2$ e, pelo fato de p ser primo ímpar, teremos que $N(\epsilon)$ se expressa como a multiplicação de um número par de fatores do tipo $|\epsilon_s|^2$. Consequentemente, $N(\epsilon)$ é positivo, donde $N(\epsilon) = 1$.

Ainda, temos que $\dfrac{\epsilon_s}{\epsilon_{p-s}}$ é uma unidade de $\mathbb{Z}[\zeta]$, sendo seu inverso multiplicativo correspondente ao seu próprio conjugado, o qual é dado por:

$$\overline{\frac{\epsilon_s}{\epsilon_{p-s}}} = \overline{\epsilon_s(\epsilon_{p-s})^{-1}} = \overline{\epsilon_s}\,\overline{\epsilon_{p-s}^{-1}} = \epsilon_{p-s}\cdot\epsilon_s^{-1} = \frac{\epsilon_{p-s}}{\epsilon_s}$$

Desta forma, temos que o valor absoluto de $\dfrac{\epsilon_s}{\epsilon_{p-s}}$ é igual a 1:

$$\left|\frac{\epsilon_s}{\epsilon_{p-s}}\right| = \frac{\epsilon_s}{\epsilon_{p-s}}\cdot\frac{\epsilon_{p-s}}{\epsilon_s} = 1$$

Por outro lado, consideremos o polinômio:

$$g(x) = \prod_{s=1}^{p-1}\left(x - \frac{\epsilon_s}{\epsilon_{p-s}}\right)$$

Utilizando a noção de funções simétricas, temos que $g(x) \in \mathbb{Z}[x]$ e, assim, pelo Lema 6.5.3, segue que as raízes de $g(x)$ são também raízes da unidade. Então, em particular, pelo Lema 6.5.2, devemos ter:

$$\frac{\epsilon}{\epsilon_{p-1}} = \pm\zeta^u$$

para algum $u \in \mathbb{Z}$.

Notemos agora que, como p é um primo ímpar segue que u ou $u + p$ é par e, consequentemente, obtemos:

$$\frac{\epsilon}{\epsilon_{p-1}} = \pm\zeta^u = \pm\zeta^u\cdot\zeta^p = \pm\zeta^{2g} \tag{6.9}$$

para algum inteiro g.

Precisamos, então, definir o sinal da igualdade acima. Para tanto, utilizaremos o Algoritmo da Divisão.

Consideremos a divisão do polinômio $t^g f(t^{p-1})$ por $1-\zeta$. Então, existe um polinômio $q(x) \in \mathbb{Q}[x]$ e um resto $v \in \mathbb{R}$ satisfazendo:

$$t^g f(t^{p-1}) = (1-\zeta)q(t) + v$$

Tomemos, em particular, $t = \zeta$. Assim:

$$\zeta^g\epsilon_{p-1} = (1-\zeta)q(\zeta) + v$$

ou seja,

$$\zeta^g\epsilon_{p-1} \equiv v \pmod{I}$$

Tomando o conjugado nesta equivalência e utilizando que o conjugado de ϵ_{p-s} é igual a ϵ_s, para qualquer $s \in \{1, \ldots, p-1\}$, temos:

$$\overline{\zeta^g \epsilon_{p-1}} = \zeta^{-g}\epsilon \equiv v \pmod{I} \tag{6.10}$$

Assim, obtemos a seguinte relação:

$$\zeta^g \epsilon_{p-1} \equiv \zeta^{-g}\epsilon \pmod{I}$$

E, utilizando que ϵ_{p-1} é invertível, segue:

$$\frac{\epsilon}{\epsilon_{p-1}} \equiv \zeta^{2g} \pmod{I}$$

Neste momento, podemos avaliar qual o sinal da equação (6.9).

Consideremos que o sinal seja negativo. Então, comparando a congruência acima com a referida equação, e usando (6.9), obtemos:

$$\zeta^{2g} \equiv -\zeta^u = -\zeta^{2g} \pmod{I},$$

resultando que

$$2\zeta^{2g} \equiv 0 \pmod{I}$$

Desse modo, $2\zeta^{2g} \in I$, donde $\langle 2\zeta^{2g} \rangle \subseteq I$ e, pelo Corolário 6.3.3, I divide $\langle 2\zeta^{2g} \rangle$. Aplicando Proposição 6.4.2, temos que $N(I)$ divide $N(\langle 2\zeta^{2g} \rangle)$, isto é,

$$p = N(I) \text{ divide } N\left(\left\langle 2\zeta^{2g} \right\rangle\right) = 2^{p-1}$$

No entanto, isso contradiz o fato de que p é um primo ímpar.

Logo, na equação (6.9), devemos ter o sinal positivo, ou seja,

$$\frac{\epsilon}{\epsilon_{p-1}} = \zeta^{2g}$$

Mas tal equação equivale a $\zeta^{-g}\epsilon = \zeta^g \epsilon_{p-1}$, implicando pela equação (6.10), que $\zeta^{-g}\epsilon$ e seu conjugado são iguais. Como consequência, temos que os mesmos são números reais, ou seja, existe $r \in \mathbb{R}$ satisfazendo:

$$\zeta^{-g}\epsilon = \zeta^g \epsilon_{p-1} = r$$

Portanto, $\epsilon = r\zeta^g$, como queríamos provar. □

Teorema 6.5.1 (Teorema de Kummer). *Seja p primo ímpar e regular. Então a equação*

$$x^p + y^p = z^p$$

não possui solução inteira (x, y, z) tal que $p \nmid x$, $p \nmid y$ e $p \nmid z$.

Demonstração. Conforme já visto no estudo feito por Lamé, como p é um número primo ímpar, para demonstrar o Teorema, basta mostrarmos que a equação:

$$x^p + y^p + z^p = 0 \tag{6.11}$$

não possui soluções inteiras não triviais.

Para tanto, utilizaremos uma demonstração por redução ao absurdo.

Suponhamos que a tripla (x, y, z) seja uma solução inteira e não trivial para a equação (6.11). Sem perda de generalidade, podemos considerar que x, y e z são primos entre si. Além disso, por hipótese, sabemos que $p \nmid xyz$.

Reescrevendo a equação acima e utilizando a fatoração em $\mathbb{Q}(\zeta)$, obtemos:

$$-z^p = x^p + y^p = \prod_{i=0}^{p-1} \left(x + \zeta^i y\right)$$

Consequentemente, segue a seguinte igualdade de ideais:

$$\langle z^p \rangle = \left\langle \prod_{i=0}^{p-1} \left(x + \zeta^i y\right) \right\rangle = \prod_{i=0}^{p-1} \left\langle x + \zeta^i y \right\rangle \tag{6.12}$$

Afirmamos que os ideais $\left\langle x + \zeta^i y \right\rangle$ são dois a dois primos entre si.

Com efeito, suponhamos que exista um ideal primo P em $\mathbb{Z}[\zeta]$ que divida $\left\langle x + \zeta^k y \right\rangle$ e $\left\langle x + \zeta^l y \right\rangle$, em que $k, l \in \{1, \ldots, p-1\}$ e $l < k$. Dessa forma, temos que:

$$\left\langle x + \zeta^k y \right\rangle \subseteq P \text{ e } \left\langle x + \zeta^l y \right\rangle \subseteq P$$

donde resulta:

$$\left(x + \zeta^l y\right) - \left(x + \zeta^k y\right) = y\zeta^l \left(1 - \zeta^{k-l}\right) \in P$$

Sabemos ainda que $1 - \zeta^{k-l}$ e $1 - \zeta$ são associados em $\mathbb{Z}[\zeta]$ (Lema 6.2.1); além disso, temos que ζ^l é inversível, pois como $l < p$, podemos tomar[8] $\zeta^{-i} := \zeta^{p-l} \in \mathbb{Q}[\zeta]$, sendo que $\zeta^l \zeta^{p-l} = 1$. Assim, segue que $y(1 - \zeta) \in P$. Agora, como P é ideal primo, temos que $y \in P$ ou $1 - \zeta \in P$.

Por outro lado, pela equação (6.12), temos que P divide o ideal $\langle z^p \rangle = \langle z \rangle^p$, donde pela primalidade de P, obtemos que P divide $\langle z \rangle$. Assim, segue que $z \in P$. Ainda, como consideramos que y e z são relativamente primos, pela Identidade de Bézout, existem $a, b \in \mathbb{Z}$ tais que $ay + bz = 1$. Dessa forma, caso tenhamos $y \in P$, como $z \in P$, seguiria

[8] No caso em que $j \in \mathbb{N}$ com $j > p$, teríamos igualmente que ζ^j é inversível. De fato, pelo algoritmo da divisão, temos que existem $q, r \in \mathbb{Z}$ tais que $i = pq + q$ e, assim, seu inverso multiplicativo seria dado por $\zeta^{-j} := \zeta^{pq-r}$.

que $1 \in P$ e, consequentemente, $P = \mathbb{Z}[\zeta]$, contrariando o fato de que P é ideal primo de $\mathbb{Z}[\zeta]$.

Logo, devemos ter que $1-\zeta \in P$. No entanto, isso implica que P divide $I = \langle 1-\zeta \rangle$, o qual é ideal primo, conforme visto na Proposição 6.5.1. Pela unicidade da fatoração em ideais primos, segue que $P = I = \langle 1-\zeta \rangle$ e, então I divide $\langle z \rangle$. Em outras palavras, existe um ideal N em $\mathbb{Z}[\zeta]$ tal que $\langle z \rangle = IN$, donde temos, pela Proposição 6.4.2, que:

$$p = N(I) \mid N(\langle z \rangle) = z^{p-1}$$

Desse modo, $p \mid z$, o que gera uma contradição com a hipótese inicial do Teorema. Assim, de fato, temos que os ideais $\left\langle x + \zeta^i \right\rangle$ são relativamente primos.

Além disso, notemos que a equação (6.12) representa a fatoração de $\langle z^p \rangle$ em ideais primos, a qual é única pois $\mathbb{Z}[\zeta]$ é um domínio de Dedekind. Então, utilizando que à direita temos o produto de ideais relativamente primos e, à esquerda, uma p-ésima potência, segue que todo ideal $\left\langle x + \zeta^i u \right\rangle$, com $i = 1, \ldots, p-1$, é uma p-ésima potência de um ideal de $\mathbb{Z}[\zeta]$. Em particular, existe um ideal J de $\mathbb{Z}[\zeta]$ satisfazendo:

$$\left\langle x + \zeta^i y \right\rangle = J^p$$

Dessa forma, segue que J^p é um ideal principal. Provaremos ainda que J é um ideal principal de $\mathbb{Z}[\zeta]$.

Utilizando a definição do grupo de classe $\mathcal{H}$ de $\mathbb{Z}[\zeta]$, temos, então, que J^p pertence à classe $1_{\mathcal{H}}$ (elemento neutro de $\mathcal{H}$), ou seja, $[J^p] = 1_{\mathcal{H}}$. Por outro lado, como p é primo regular, sabemos que $p \nmid h$, resultando que p e h são relativamente primos. Consequentemente, existem $r, s \in \mathbb{Z}$ tais que $rp + sh = 1$. Logo:

$$[J] = \left[J^{rp+sh}\right] = \left[J^{rp}\right]\left[J^{sh}\right] = \left[J^p\right]^r \left[J^h\right]^s = 1_{\mathcal{H}}^r \cdot 1_{\mathcal{H}}^s = 1_{\mathcal{H}}$$

donde J é um ideal principal.

Assim, existe $\alpha \in \mathbb{Z}[\zeta]$ tal que $J = \langle \alpha \rangle$. E, como $x + \zeta y \in J^p$, temos:

$$x + \zeta y = \epsilon \alpha^p$$

em que ϵ é uma unidade.

Usando que ϵ é uma unidade, temos, pelo Lema de Kummer, que existem $r \in \mathbb{R}$ e $g \in \mathbb{Z}$ tais que $\epsilon = r\zeta^g$. Além disso, pelo Lema 6.5.1, existe $a \in \mathbb{Z}$ tal que $\alpha^p \equiv a \pmod{I^p}$. Dessa forma, temos:

$$x + \zeta y = r\zeta^g \alpha^p \equiv r\zeta^g a \pmod{I^p}$$

Ainda, conforme visto na Proposição 6.5.1, sabemos que $I^p \subseteq \langle p \rangle = \langle 1-\zeta \rangle^{p-1}$ e, então,

$$x + \zeta y \equiv r\zeta^g a \pmod{\langle p \rangle}$$

Agora, utilizando que ζ^g é inversível com inversa ζ^{-g}, obtemos:

$$\zeta^{-g}(x + \zeta y) \equiv ra \pmod{\langle p \rangle}$$

Tomando o conjugado nesta equação e utilizando que $\overline{\zeta^j} = \zeta^j$ para todo $j \in \mathbb{Z}$, temos:

$$\zeta^g(x + \zeta^{-1}y) \equiv ra \pmod{\langle p \rangle}$$

Assim, segue que:

$$\zeta^{-g}(x + \zeta y) \equiv \zeta^g(x + \zeta^{-1}y) \pmod{\langle p \rangle}$$

e, consequentemente,

$$\zeta^{-g}x + \zeta^{1-g}y - \zeta^g x - \zeta^{g-1}y \equiv 0 \pmod{\langle p \rangle} \tag{6.13}$$

Analisaremos, agora, os possíveis valores de g na equação (6.13).

Primeiramente, suponhamos que $g \equiv 0 \pmod{\langle p \rangle}$. Então, temos que $\zeta^g = 1$, o que, aplicado na equação (6.13) nos fornece $y(\zeta - \zeta^{-1}) \equiv 0 \pmod{\langle p \rangle}$. Tomando o conjugado e multiplicando tal equivalência por ζ, obtemos:

$$0 \equiv y(\zeta - \zeta^{-1}) \equiv y\zeta(\zeta^{-1} - \zeta) \equiv y(1 - \zeta^2) \equiv y(1 + \zeta)(1 - \zeta) \pmod{\langle p \rangle} \tag{6.14}$$

Notemos ainda que $1 + \zeta$ é inversível, pois, ao fazer $x = 1$ em $P_\zeta(x)$, cuja fórmula foi apresentada na Observação 6.2.3, obtemos:

$$P_\zeta(-1) = 1 = (-1 - \zeta)(-1 - \zeta^2)\cdots(-1 - \zeta^{p-1})$$

Utilizando esse resultado na equação (6.14), temos, então,

$$y(1 - \zeta) \equiv 0 \pmod{\langle p \rangle}$$

Assim, $y(1 - \zeta) \in \langle p \rangle = \langle 1 - \zeta \rangle^{p-1}$, donde deve existir $q \in \mathbb{Z}[\zeta]$ satisfazendo $y(1 - \zeta) = q(1 - \zeta)^{p-1}$. E, como $p \geq 3$, tal relação pode ser reescrita da seguinte maneira:

$$(1 - \zeta)\left[y - q(1 - \zeta)^{p-2}\right] = 0$$

Logo, usando que $\mathbb{Z}[\zeta]$ é um domínio e que $1 \neq \zeta$, resulta que $y = q(1 - \zeta)^{p-2}$ e, então, $1 - \zeta$ divide y. E, utilizando que a norma é multiplicativa, obtemos ainda que:

$$\begin{aligned} N(y) &= N(q) \cdot N(1 - \zeta)^{p-2} \\ &= N(q) \cdot p^{p-2} \end{aligned}$$

E, como $y \in \mathbb{Z}$, temos $N(y) = y^{p-1}$, donde $y^{p-1} = N(q) \cdot p^{p-2}$ e, pela primalidade de p, segue que $p \mid y$, uma contradição com a hipótese inicial.

Analogamente, caso $g \equiv 1 \pmod{\langle p \rangle}$, teremos que os termos em y se anulam, reduzindo a equação (6.13) a:

$$\zeta^{-g}x - \zeta^{g}x \equiv x\zeta^{-1}(1-\zeta^{2}) \equiv x(1-\zeta^{2}) \equiv 0 \pmod{\langle p \rangle}$$

implicando que p divide x, uma contradição.

Logo, pelas contradições obtidas, concluímos que g não pode ser congruente a 0 nem a 1 módulo $\langle p \rangle$.

Por outro lado, analisando a equação (6.13), temos que existe $\beta \in \mathbb{Z}[\zeta]$ satisfazendo:

$$\zeta^{-g}x + \zeta^{1-g}y - \zeta^{g}x - \zeta^{g-1}y = \beta p$$

Dessa igualdade decorre que:

$$\zeta^{-g}\left(\frac{x}{p}\right) + \zeta^{1-g}\left(\frac{y}{p}\right) - \zeta^{g}\left(\frac{x}{p}\right) - \zeta^{g-1}\left(\frac{y}{p}\right) = \beta \tag{6.15}$$

sendo que p não divide nenhum dos expoentes de ζ, como mostrado acima.

Agora, sabemos que $\alpha \in \mathbb{Z}[\zeta]$; então, α se escreve como combinação linear de $\{1, \ldots, \zeta^{p-1}\}$, onde os escalares são inteiros. Mais ainda, como $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ e $\mathbb{Q}$ é um corpo, temos que tal conjunto constitui uma base para $\mathbb{Q}(\zeta)$, garantindo a unicidade desta combinação.

Nesse contexto, consideremos, por absurdo, que os expoentes de ζ na equação (6.15) sejam todos incongruentes módulo p. Pela unicidade da fatoração de β, teríamos que $\frac{x}{p}$ e $\frac{y}{p}$ seriam inteiros, uma contradição com a hipótese de que $p \nmid x$ e $p \nmid y$.

Dessa forma, ao menos dois dos expoentes de ζ na referida equação devem ser congruentes módulo p.

Vejamos todas as possibilidades (lembrando que g não pode ser congruente a 0 ou a 1 módulo p).

1. Caso $-g \equiv 1 - g \pmod{p}$ ou, equivalentemente, $g \equiv g - 1 \pmod{p}$, teríamos $0 \equiv 1 \pmod{p}$, o que só é possível se $p = \pm 1$, contradizendo o fato de que p é primo.

2. Caso $-g \equiv g \pmod{p}$, teríamos $2g \equiv 0 \pmod{p}$ e, como p é primo ímpar, resultaria que $g \equiv 0 \pmod{p}$, gerando uma contradição, como mostrado anteriormente.

3. Caso $1 - g \equiv g - 1 \pmod{p}$, teríamos $2g - 2 \equiv 2(g-1) \equiv 0 \pmod{p}$ e, utilizando novamente que p é primo ímpar, seguiria que $g \equiv 1 \pmod{p}$, igualmente uma contradição.

Assim, resta-nos apenas o caso em que $-g \equiv g-1 \pmod{p}$ (ou, equivalentemente, $g \equiv 1-g \pmod{p}$), o qual implica em $2g \equiv 1 \pmod{p}$. Utilizando este resultado na equação (6.15), obtemos:

$$\begin{aligned} \beta p\zeta^g &= x + \zeta y - \zeta^{2g}x - \zeta^{2g-1}y \\ &= x + \zeta y - \zeta x - y \\ &= (x-y)(1-\zeta) \end{aligned}$$

Aplicando a norma nessa igualdade, temos:

$$N(\beta p\zeta^g) = N(x-y)\cdot N(1-\zeta) = (x-y)^{p-1}p$$

Por outro lado, utilizando que a norma é multiplicativa, obtemos :

$$N(\beta p\zeta^g) = N(\beta)\cdot N(p)\cdot N(\zeta^g) = N(\beta)\cdot p^{p-1}\cdot 1$$

Assim, temos que:

$$N(\beta)\cdot p^{p-1} = (x-y)^{p-1}p$$

donde, pela primalidade de p, segue que p divide $x-y$, ou seja, $x \equiv y \pmod{p}$.

Agora, utilizando argumento de simetria na equação (6.11), isto é, que poderíamos ter procedido de forma semelhante isolando x^p em tal equação, temos que $x \equiv z \pmod{p}$. Como consequência:

$$0 \equiv x^p + y^p + z^p \equiv 3x^p \pmod{p}$$

Como $p \nmid x$ e p é primo, temos que p divide 3, resultando que $p = 3$.

Além disso, como o cubo de um inteiro que não é divisível por 3 só pode deixar restos ± 1 por 9, temos, pela congruência anterior,

$$0 \equiv \pm 1 \pm 1 \pm 1 \pmod{9},$$

o que é impossível.

Portanto, concluímos que a equação (6.11) não possui solução inteira não trivial quando p é um primo regular satisfazendo $p \nmid xyz$. □

REFERÊNCIAS

[1] ALKALAY-HOULIHAN, C. *Sophie Germain and Special Cases of Fermat's Last Theorem.* Disponível em `http://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Colleen-Alkalay-Houlihan.pdf`. Acesso em: 12 ago. 2018.

[2] ANDRADE, J. F. S. *Tópicos Especiais em Álgebra.* Rio de Janeiro: Sociedade Brasileira de Matemática, 2013.

[3] BOEING, F. K. *Fatoração Única em Corpos Ciclotômicos e o Último Teorema de Fermat.* Dissertação (Graduação) - UDESC, Joinville, 2013.

[4] DUMMIT, D.S.; FOOTE, R. M. *Abstract Algebra.* Wiley Hoboken, 2004.

[5] EDWARD, H. M. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory.* New York: Springer Verlag, 1977.

[6] GALLIAN, J. *Contemporary Abstract Algebra.* 8ed. Cengage Learning. 2012.

[7] GARCIA, A. e LEQUAIN, Y. *Elementos de Álgebra.* Rio de Janeiro: Instituto de Matemática Pura e Aplicada (Projeto Euclides), 2002.

[8] GONÇALVES, A. *Introdução à Álgebra.* Rio de Janeiro: Instituto de Matemática Pura e Aplicada (Projeto Euclides), 2003.

[9] HARDY, G. H.; WRIGHT, E. M.;HEATH-BROWN, D. R.; SILVERMAN, J.H. *An Introduction to the Theory of Numbers.* Posts & Telecom Press, 2009.

[10] MARTINEZ, F. B. ; MOREIRA, C.G.; SALDANHA, N.; TENGAN, E. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro.* Rio de Janeiro: Instituto de Matemática Pura e Aplicada (Projeto Euclides), 2015.

[11] OTTO, E. *Teoria dos Números Algébricos.* Rio de Janeiro: Instituto de Matemática Pura e Aplicada (Projeto Euclides), 2014.

[12] PERIC, V; VUKOVIC, M. Some Examples of Principal Ideal Domain which are not Euclidean and Some Other Counterexamples. *Novi Sad J. Math*, v. 38, n. 1, p. 137-154, mai. 2008.

[13] RIBENBOIM, P. *13 Lectures on Fermat's Last Theorem.* Springer Science & Business Media, 1979. Disponível em `http://staff.math.su.se/shapiro/ProblemSolving/13%20Lectures%20on%20Fermat's%20Last%20Theorem.pdf`. Acesso em: 14 ago. 2018.

[14] RIDDLE, L. Sophie Germain and Fermat's Last Theorem *Online*, jul. 2009. Disponível em `https://www.agnesscott.edu/lriddle/women/germain-FLT/SGandFLT.htm`. Acesso em: 23 set. 2018.

[15] ROTMAN, J.J. *Advanced Modern Algebra.* Prentice Hall, 2003.

[16] SILVA, P.R. *Tópicos de Teoria dos Números Algébricos e Aplicações em Reticulados e Equações Diofantinas.* Dissertação (Mestrado) - UEP, Rio Claro, 2015.

[17] SINGH, S. *O Último Teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos.* Rio de Janeiro: Record, 2011.

[18] STEWART, I.; TALL, D. *Algebraic Number Theory and Fermat's Last Theorem.* Massachussets: A K Peters, 2002.