UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

JOÃO GABRIEL OLIVEIRA DE JESUS

Propriedades Aritméticas do j-invariante

Campinas

2023

João Gabriel Oliveira de Jesus

Propriedades Aritméticas do j-invariante

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática.

Orientador: Tiago Jardim da Fonseca

Este trabalho corresponde à versão final da Dissertação defendida pelo aluno João Gabriel Oliveira de Jesus e orientada pelo Prof. Dr. Tiago Jardim da Fonseca.

Campinas

2023

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

J499p

Jesus, João Gabriel Oliveira de, 1998-
Propriedades aritméticas do j-invariante / João Gabriel Oliveira de Jesus. – Campinas, SP : [s.n.], 2023.

Orientador: Tiago Jardim da Fonseca.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Formas modulares. 2. Singular moduli. 3. Teoria dos números. 4. Invariante modular (Matemática). 5. j-Invariante. I. Fonseca, Tiago Jardim da, 1990-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações Complementares

Título em outro idioma: Arithmetic properties of the j-invariant
Palavras-chave em inglês:
Modular forms
Singular moduli
Number theory
Modular invariant
j-Invariant
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Tiago Jardim da Fonseca [Orientador]
Roberto Carlos Alvarenga da Silva Júnior
Sahibzada Waleed Noor
Data de defesa: 31-08-2023
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0009-0002-1970-1264
- Currículo Lattes do autor: http://lattes.cnpq.br/8672515384152520

Dissertação de Mestrado defendida em 31 de agosto de 2023 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). TIAGO JARDIM DA FONSECA

Prof(a). Dr(a). SAHIBZADA WALEED NOOR

Prof(a). Dr(a). ROBERTO CARLOS ALVARENGA DA SILVA JÚNIOR

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

Primeiramente, agradeço aos meus pais, que me acompanharam durante toda minha trajetória desde minha graduação, que me apoiaram e me deram todo suporte para que este trabalho fosse possível.

Agradeço ao meu orientador, Dr. Tiago Jardim da Fonseca, pelos ensinamentos, pela disponibilidade e pelas ideias que me deu ao longo da elaboração desta dissertação. Nossas reuniões foram fundamentais para o meu amadurecimento enquanto matemático e pesquisador.

Também agradeço aos meus amigos e colegas que estiveram ao meu lado, em especial, à Marina, pelo apoio, carinho e momentos de descontração, bem como a todos os professores que tive durante a graduação e a pós-graduação, pelo incentivo e pelos conselhos. Este trabalho existe por causa de vocês.

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

"God created the integers; all the rest is the work of Man".
(Leopold Kronecker)

Resumo

Formas modulares são funções no semiplano superior complexo que se transformam de uma forma especial sob a ação de um subgrupo discreto de $\mathrm{SL}(2,\mathbb{R})$. O objetivo desta dissertação é estudar a teoria de formas modulares e suas interações com a teoria dos números através das propriedades aritméticas de valores especiais da função j-invariante. O principal resultado deste trabalho nos diz que estes valores especiais são inteiros algébricos. Estes números possuem propriedades extraordinárias. Por exemplo, como aplicação à teoria algébrica dos números, podemos obter uma teoria de corpos de classe explícita para corpos quadráticos imaginários, isto é, os valores especiais de j descrevem as extensões abelianas finitas dos corpos quadráticos imaginários. Por fim, estudaremos o artigo [1] de Gross e Zagier, dedicado ao estudo da fatoração em primos da diferença entre dois valores especiais de j, que continua servindo de base para uma série de avanços à teoria de números e à geometria aritmética até os dias de hoje.

Palavras-chave: Formas Modulares; Singular Moduli; Teoria dos Números; Invariante Modular; j-invariante.

Abstract

Modular forms are functions in the complex upper half-plane which transform in a special way under the action of a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$. The aim of this work is to study the theory of modular forms and its interactions with number theory through the arithmetic properties of some special values of the j-invariant function. The main result of this work tells us that the singular moduli are algebraic integers. These numbers have extraordinary properties, that gives meaning to many concepts in different areas of mathematics. For example, as an application to the algebraic number theory, we can obtain a explicit class field theory for imaginary quadratic fields. At last, we will study the paper [1] of Gross and Zagier, dedicated to the study of the prime factorization of the difference between two singular moduli, that keep serving as a base to a series of advances to number theory and to arithmetic geometry up to the present day.

Keywords: Modular Forms; Singular Moduli; Number Theory; Modular Invariant; j-invariant;

Lista de ilustrações

Figura 1 – O domínio fundamental para a ação de Γ_1 em $\mathfrak{H}$ 19
Figura 2 – Domínio fundamental *estrito* e alguns transladados de $\mathcal{F}_1$ 20
Figura 3 – A curva $\mathcal{C}$ 37
Figura 4 – Uma variação da curva $\mathcal{C}$ 39
Figura 5 – Relações para o Teorema 11 90
Figura 6 – O Toro Complexo 102

Lista de tabelas

Tabela 1 – Números de Bernoulli e valores das séries de Eisenstein normalizadas . 32
Tabela 2 – Valores especiais de j em função do discriminante D 67

Sumário

Introdução **13**

I Teoria Básica de Formas Modulares **16**

1 Ação do Grupo $\mathrm{SL}(2,\mathbb{R})$ no Semiplano Superior Complexo **17**

1.1 Domínio Fundamental do Grupo Modular Completo 18

2 Formas Modulares **21**

2.1 Reticulados e Funções Modulares 24

2.2 Séries de Eisenstein 28

2.2.1 Os Números de Bernoulli e as Séries de Eisenstein Normalizadas . . 29

2.2.2 Séries de Eisenstein de Peso 2 32

3 Estrutura e Dimensão do Espaço das Formas Modulares **34**

3.1 Aplicação: Expansão da Forma Cuspidal Discriminante Δ e Função τ de Ramanujan 43

II O Invariante Modular j **47**

4 O Invariante Modular j **48**

4.1 Definições Básicas 48

4.2 Multiplicação Complexa 51

4.3 Matrizes Inteiras de um Dado Determinante 53

4.4 Subgrupos de Congruência de Γ_1 55

4.5 Algebricidade dos Valores Especiais de j 56

5 Valores Especiais de j e Discriminantes de Formas Quadráticas Binárias . . **68**

5.1 Discriminantes e a Finitude do Número de Classes 68

5.1.1 O Problema do Número de Classe de Gauss 72

5.2 O Polinômio de Classes H_D 76

5.3 Aplicação: Teoria de Corpos de Classe Explícita para Corpos Quadráticos Imaginários 82

6 Fatoração Prima de Valores Especiais de j **84**

REFERÊNCIAS **91**

Apêndices **92**

APÊNDICE A Pré-requisitos de Teoria Algébrica dos Números 93

A.1 Inteiros Algébricos 93

A.2 Ideais de $\mathcal{O}_K$ e Ramificação 96

A.3 O Corpo de Classe de Hilbert 99

APÊNDICE B Curvas Elípticas Complexas 102

B.1 Toro Complexo 102

B.2 Curvas Elípticas 104

Introdução

As formas modulares são funções definidas no semiplano superior complexo que satisfazem alguma condição de modularidade com respeito à ação de um subgrupo discreto de $\mathrm{SL}(2,\mathbb{R})$, juntamente com uma condição de crescimento no infinito. A princípio, estes são objetos da Análise Complexa e, embora tenham significado e aplicações em diversas áreas da matemática, geralmente são mais estudados por sua conexão com a Teoria dos Números. Neste trabalho, vamos estudar a interação entre estas áreas através das propriedades aritméticas dos valores especiais da função invariante modular j.

Este trabalho está estruturado em duas partes, sendo a primeira sobre a Teoria Básica de Formas Modulares, que compreende os capítulos 1 a 3, e a segunda sobre o Invariante Modular j, que abrange os capítulos 4 a 6. As principais referências utilizadas para a elaboração da primeira parte do trabalho foram [2], [3], [4], [5] e [6]. Para a segunda parte do trabalho, as principais referências utilizadas foram [2], [4], [5], [1], [7] e [8].

Essencialmente, no capítulo 1 introduziremos os objetos básicos do ambiente em que serão definidas as formas modulares. Consideraremos a ação de $\mathrm{SL}(2,\mathbb{R})$ no semiplano superior complexo $\mathfrak{H}$ via transformações de Möbius, com principal interesse no subgrupo $\Gamma_1 := \mathrm{SL}(2,\mathbb{Z})$, chamado de *grupo modular completo*, com respeito ao qual definiremos as formas modulares, e caracterizaremos um domínio fundamental para o grupo modular completo.

Iniciaremos o capítulo 2 estudando noções gerais de *funções modulares com respeito à* Γ_1 como um objeto com várias noções equivalentes. Entre elas, estamos particularmente interessados em duas:

- Uma função $f : \mathfrak{H} \to \mathbb{C}$ que é Γ_1-invariante, ou seja, uma função satisfazendo $f(\gamma z) = f(z)$, para todo $z \in \mathfrak{H}$ e todo $\gamma \in \Gamma_1$;
- Uma função de reticulados em $\mathbb{C}$, satisfazendo $f(\lambda\Lambda) = f(\Lambda)$, para todo reticulado Λ e $\lambda \in \mathbb{C}$ não nulo.

Veremos também uma forma explícita de relacionar essas duas noções. No entanto, para obter propriedades aritméticas interessantes, as funções modulares como definidas não são suficientes e precisaremos considerar uma classe mais geral de funções: as *formas modulares*, que são funções $f\colon \mathfrak{H} \to \mathbb{C}$ holomorfas em $\mathfrak{H}$, inclusive no infinito, satisfazendo a condição:

$$f(\gamma z) = (cz + d)^k f(z),$$

para algum $k \in \mathbb{N}$ e para toda matriz $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$, $z \in \mathfrak{H}$. Neste caso, diremos que f é uma forma modular de peso k. Além disso, temos as *formas cuspidais*, que são formas modulares cujo valor no infinito é zero. Ao decorrer do capítulo 2, descreveremos o primeiro exemplo não-trivial de formas modulares, as chamadas *séries de Eisenstein de peso k*, que são formas modulares de peso k, para todo $k > 2$, e estudaremos suas principais propriedades. Ao final do capítulo, mencionaremos brevemente o caso das séries de Eisenstein de peso 2.

Para encerrar a primeira parte, veremos no capítulo 3 que o conjunto das formas modulares de peso k é um $\mathbb{C}$-espaço vetorial de dimensão finita, denotado por M_k. O primeiro resultado fundamental que veremos afirma que $M_k = \mathbb{C}G_k \oplus S_k$, isto é, toda forma modular pode ser escrita unicamente como combinações de séries de Eisenstein e formas cuspidais. Além disso, obteremos propriedades fundamentais no que concerne à estrutura e dimensão dos espaços M_k, tais como: uma fórmula explícita para calcular zeros e polos de funções modulares — chamada *fórmula de valência* —, uma fórmula explícita para calcular a dimensão dos espaços M_k e uma base para M_k em função das séries de Eisenstein (normalizadas) de pesos 4 e 6. Em particular, veremos que o espaço das formas modulares M_k é unidimensional para $k = 0, 4, 6, 8$ e 10, cujas bases são as respectivas séries de Eisenstein (normalizadas) de peso k. Tendo em vista a caracterização $M_k = \mathbb{C}G_k \oplus S_k$, não podem existir formas cuspidais em M_k para estes valores de k. Neste contexto, finalizamos apresentando o primeiro exemplo de forma cuspidal, que se dá em M_{12}, com a *forma cuspidal discriminante* Δ, que será amplamente estudada neste capítulo — principalmente por ser um ingrediente fundamental na definição do invariante modular j.

A segunda parte deste trabalho se inicia no capítulo 4, com a definição e principais propriedades do invariante modular j como a função em $\mathfrak{H}$ que é o quociente de duas formas modulares de peso 12:

$$j = \frac{E_4^3}{\Delta}.$$

Essa terminologia é devida ao fato de que j é uma função modular de peso 0, por construção, e portanto é, simplesmente, Γ_1-invariante. No decorrer deste capítulo, estudaremos a noção de *multiplicação complexa* no âmbito geral, para curvas elípticas. É neste ambiente que iremos deduzir pontos com propriedades especiais, chamados de pontos CM, que são pontos quadráticos imaginários no semiplano superior $\mathfrak{H}$. A propriedade fundamental destes pontos é que os valores de j nestes pontos — chamados de *valores especiais de j* — são inteiros algébricos, que é o principal resultado deste trabalho. O restante deste capítulo trabalhará ferramentas para demonstrar este resultado.

Em seguida, no capítulo 5, seguiremos naturalmente para o estudo do grau destes valores especiais, que está intrinsicamente relacionado com o discriminante dos pontos CM correspondentes. Mais especificamente, veremos que para todo ponto CM de discriminante D, o valor especial de j associado é um inteiro algébrico de grau $h(D)$,

em que $h(D)$ é o o *número de classes* de D no contexto de discriminantes de formas quadráticas binárias. O caso $h(D) = 1$ recebe um tratamento especial, já que neste caso os valores especiais serão números inteiros, além de se tratar de um caso especial do *problema do número de classes de Gauss*, um problema clássico na matemática.

Finalmente, o capítulo 6 é dedicado ao aspecto da fatoração prima dos valores especiais de j, baseado no artigo [1] de Gross e Zagier. No trabalho em questão, veremos que é possível obter a fatoração prima de valores especiais de j realizando operações aritméticas que podem ser feitas algoritmicamente, o que é um resultado interessantíssimo, principalmente por se tratar de uma das raras ocasiões na matemática em que é possível obter a fatoração prima de um número inteiro de forma fechada.

Os apêndices discorrem brevemente sobre alguns aspectos básicos de Teoria Algébrica dos Números e conceitos a respeito de curvas elípticas complexas, assuntos que aparecem naturalmente no escopo deste trabalho.

Parte I

Teoria Básica de Formas Modulares

1 Ação do Grupo $\mathrm{SL}(2,\mathbb{R})$ no Semiplano Superior Complexo

Neste capítulo, introduziremos os objetos básicos do ambiente em que estudaremos as formas modulares: o grupo $\mathrm{SL}(2,\mathbb{R})$, sua ação no semiplano superior complexo via *transformações de Möbius*, o grupo modular completo $\mathrm{SL}(2,\mathbb{Z})$ e seu domínio fundamental.

O subconjunto de $\mathbb{C}$ dos números complexos cuja parte imaginária é estritamente positiva, denotado por $\mathfrak{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, é chamado de *semiplano superior complexo*. O *grupo linear especial* $\mathrm{SL}(2,\mathbb{R})$ é o grupo das matrizes 2×2 com entradas reais e determinante igual a 1, que age naturalmente em $\mathfrak{H}$ via *transformações de Möbius*:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathfrak{H} \to \mathfrak{H}, \qquad z \mapsto \gamma z = \frac{az+b}{cz+d}. \tag{1.1}$$

Verifiquemos que essa aplicação de fato induz uma ação de grupo $\mathrm{SL}(2,\mathbb{R}) \times \mathfrak{H} \to \mathfrak{H}$. Para isso, será útil a seguinte propriedade:

Lema 1. *Sejam* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{R})$ *e* $z \in \mathfrak{H}$. *Então,*

$$\mathrm{Im}(\gamma z) = \frac{\mathrm{Im}(z)}{|cz+d|^2}.$$

Demonstração. Por definição,

$$\gamma z = \frac{az+b}{cz+d}.\frac{\overline{cz+d}}{\overline{cz+d}} = \frac{(az+b)(\overline{cz+d})}{|cz+d|^2} = \frac{(a\,\mathrm{Re}(z)+b+ia\,\mathrm{Im}(z))(c\,\mathrm{Re}(z)+d-ic\,\mathrm{Im}(z))}{|cz+d|^2}.$$

Desenvolvendo apenas os termos que acompanham a unidade imaginária i na expressão acima, obtemos

$$\mathrm{Im}(\gamma z) = \frac{\mathrm{Im}(z)(ac\,\mathrm{Re}(z)+ad-ac\,\mathrm{Re}(z)-bc)}{|cz+d|^2} = \frac{\mathrm{Im}(z)(ad-bc)}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2}.$$

□

Proposição 1. *As transformações de Möbius induzem uma ação do grupo* $\mathrm{SL}(2,\mathbb{R})$ *em* $\mathfrak{H}$.

Demonstração. A aplicação está bem definida, visto que dado $z \in \mathfrak{H}$ temos $\mathrm{Im}(z) > 0$ e, portanto, para qualquer $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{R})$, segue do Lema 1 que

$$\mathrm{Im}(\gamma z) = \frac{\mathrm{Im}(z)}{|cz+d|^2} > 0,$$

ou seja, $\gamma z \in \mathfrak{H}$. Trivialmente, $1_{2\times 2} \cdot z = z$, para todo $z \in \mathfrak{H}$. Resta verificarmos a transitividade da ação. Para todo $\gamma, \delta \in \mathrm{SL}(2,\mathbb{R})$ e $z \in \mathfrak{H}$, temos $\gamma(\delta z) = (\gamma\delta)z$. Sejam $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ e $\delta = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$. Então,

$$\begin{aligned}\gamma(\delta z) = \gamma\left(\frac{a'z+b'}{c'z+d'}\right) &= \frac{a\left(\frac{a'z+b'}{c'z+d'}\right)+b}{c\left(\frac{a'z+b'}{c'z+d'}\right)+d} = \frac{(aa'+bc')z+ab'+bd'}{(ca'+dc')z+cb'+dd'} \\ &= \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cv'+dd' \end{pmatrix} z = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\right] z = (\gamma\delta)z.\end{aligned}$$

□

Observação 1. Dado $\gamma \in \mathrm{SL}(2,\mathbb{R})$, as matrizes $\pm\gamma$ agem de mesma forma em $\mathfrak{H}$, no sentido de que o valor de γz e $(-\gamma)z$ coincidem, para todo $z \in \mathfrak{H}$. Por tal motivo, eventualmente será conveninente trabalhar com o grupo quociente $\mathrm{PSL}(2,\mathbb{R}) = \dfrac{\mathrm{SL}(2,\mathbb{R})}{\{\pm 1_{2\times 2}\}}$. Além disso, vamos utilizar o mesmo símbolo para denotar a imagem de um elemento de $\mathrm{SL}(2,\mathbb{R})$ em $\mathrm{PSL}(2,\mathbb{R})$.

O estudo das formas modulares envolve a ação de um subgrupo discreto de $\mathrm{SL}(2,\mathbb{R})$. A princípio, estamos interessados no subgrupo discreto $\Gamma_1 = \mathrm{SL}(2,\mathbb{Z})$ de $\mathrm{SL}(2,\mathbb{R})$, chamado de *grupo modular completo*, e no respectivo grupo quociente $\mathrm{PSL}(2,\mathbb{Z})$, chamado de *grupo modular*. No entanto, mais posteriormente trabalharemos com outros subgrupos discretos de $\mathrm{SL}(2,\mathbb{R})$, como os *subgrupos de congruência*.

1.1 Domínio Fundamental do Grupo Modular Completo

Nesta seção, caracterizaremos um *Domínio Fundamental* para a ação do grupo modular completo Γ_1 em $\mathfrak{H}$, isto é, um subconjunto aberto $\mathcal{F} \subset \mathfrak{H}$ com as propriedades de que não existem dois pontos distintos em $\mathcal{F}$ que são equivalentes sob a ação de Γ_1 e todo ponto de $\mathfrak{H}$ é Γ_1-equivalente a algum ponto do fecho $\overline{\mathcal{F}}$ de $\mathcal{F}$. Para isso, considere os elementos de Γ_1

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{e} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

que satisfazem, para todo $z \in \mathfrak{H}$:

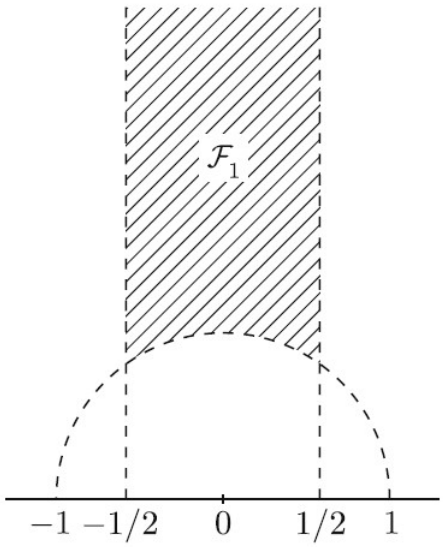
- $S \cdot z = -1/z$;
- $T \cdot z = z + 1$.

Teorema 1. *O conjunto*

$$\mathcal{F}_1 = \{z \in \mathfrak{H} : |z| > 1 \ e\ |\operatorname{Re}(z)| < 1/2\}$$

é um domínio fundamental para a ação de Γ_1 *em* $\mathfrak{H}$.

Figura 1 – O domínio fundamental para a ação de Γ_1 em $\mathfrak{H}$



Fonte: [3, p. 6]

Demonstração. Seja $z \in \mathfrak{H}$. O subconjunto $\{mz + n : m, n \in \mathbb{Z}\} \subset \mathbb{C}$ é discreto, e portanto admite um ponto $cz+d$ diferente da origem com módulo mínimo. Observe que $\mathrm{mdc}(c, d) = 1$, pois caso contrário seria possível dividir o ponto $cz + d$ e obter um outro ponto de módulo ainda menor. Pela Identidade de Bézout, existem $a, b \in \mathbb{Z}$ tais que $ad + bc = 1$. Podemos assumir que $\gamma_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$. Pelo Lema 1, segue que

$$\mathrm{Im}(\gamma_1 z) = \frac{\mathrm{Im}(z)}{|cz + d|^2}.$$

Como $cz + d$ tem módulo mínimo, a expressão acima garante que $\mathrm{Im}(\gamma_1 z)$ é um máximo de $\{\mathrm{Im}(\gamma z) : \gamma \in \Gamma_1\} \subset \mathbb{R}$. Tome $z^* = T^n \gamma_1 z = \gamma_1 z + n$, onde n é escolhido de forma que $|\,\mathrm{Re}(z^*)| \leqslant 1/2$. Observe $\mathrm{Im}(z^*) = \mathrm{Im}(z)$, e portanto $|z^*|$ não pode ser estritamente menor do que 1, pois caso contrário seguiria novamente do Lema 1 que

$$\mathrm{Im}(-1/z^*) = \frac{\mathrm{Im}(z^*)}{|z^*|^2} > \mathrm{Im}(z^*),$$

contradizendo a maximalidade de $\mathrm{Im}(z^*)$ em $\{\mathrm{Im}(\gamma z) : \gamma \in \Gamma_1\}$. Portanto, $z^* \in \overline{\mathcal{F}_1}$ e z é Γ_1-equivalente ao ponto z^*.

Agora, seja $z_1 \in \mathcal{F}_1$ e considere $z_2 = \gamma z_1 \in \mathcal{F}_1$, com $\gamma \neq \pm 1_{2\times 2} \in \Gamma_1$, pontos Γ_1-equivalentes. Note que γ não pode ser escrito na forma T^n, já que isso seria uma contradição com a condição $|\,\mathrm{Re}(z_1)|, |\,\mathrm{Re}(z_2)| < 1/2$. Logo, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$ com $c \neq 0$. Note que (por exemplo, pela figuras 6 e 2) temos $\mathrm{Im}(z) > \sqrt{3}/2$, para todo $z \in \mathcal{F}_1$. Portanto,

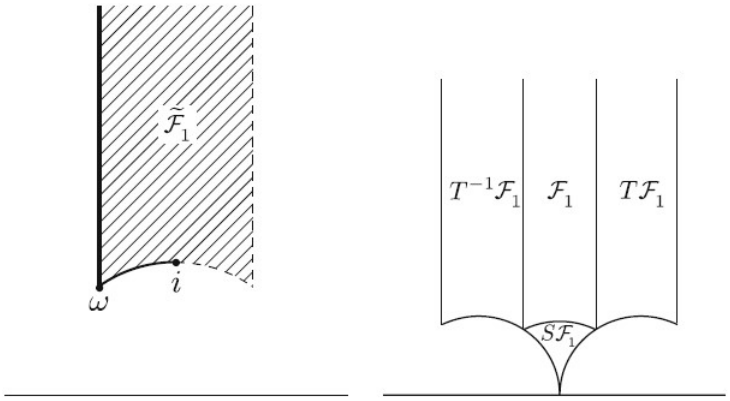
pelo Lema 1 temos que a desigualdade

$$\frac{\sqrt{3}}{2} < \mathrm{Im}(z_2) = \frac{\mathrm{Im}(z_1)}{|cz_1 + d|^2} \leqslant \frac{\mathrm{Im}(z_1)}{c^2\,\mathrm{Im}(z_1)} < \frac{2}{c^2\sqrt{3}}$$

é apenas satisfeita se $c = \pm 1$. Sem perda de generalidade, podemos supor que $\mathrm{Im}(z_1) \leqslant \mathrm{Im}(z_2)$. No entanto, $|\pm z_1 + d| > |z_1| > 1$ fornece uma contradição com o Lema 1. □

Observação 2. Os pontos no bordo de $\mathcal{F}_1$ são Γ_1-equivalentes. De fato, os pontos nas linhas $\mathrm{Re}(z) = \pm 1/2$ são Γ_1-equivalentes pela ação $T : z \mapsto z + 1$, enquanto que os pontos nas metades laterais do arco $|z| = 1$ são Γ_1-equivalentes pela ação $S : z \mapsto -1/z$. Na realidade, essas são as únicas equivalências possíveis para pontos no bordo de $\mathcal{F}_1$. Por essa razão, definimos $\widetilde{\mathcal{F}_1}$ como o conjunto dos pontos de $\mathcal{F}_1$ adicionado aos pontos do bordo com parte real não positiva, chamado de *semifecho* de $\mathcal{F}_1$. Então, todo ponto de $\mathfrak{H}$ é Γ_1-equivalente a um único ponto de $\widetilde{\mathcal{F}_1}$. Frequentemente, $\widetilde{\mathcal{F}_1}$ é referido como *Domínio Fundamental Estrito* para ação de Γ_1 em $\mathfrak{H}$.

Figura 2 – Domínio fundamental *estrito* e alguns transladados de $\mathcal{F}_1$



Fonte: [3, p. 6]

Corolário 1. Γ_1 *é gerado por* S *e* T.

Demonstração. Segue do Teorema 1 que $\overline{\mathcal{F}_1}$ e seus transladados $\gamma\overline{\mathcal{F}_1}$ cobrem $\mathfrak{H}$ de forma disjunta, com possível sobreposição no bordo. Os transladados vizinhos de $\mathcal{F}_1$ são $T^{-1}\mathcal{F}_1, S\mathcal{F}_1$ e $T\mathcal{F}_1$ (Figura 2). Logo, qualquer transladado $\gamma\mathcal{F}_1$ pode ser levado em algum desses conjuntos vizinhos via uma aplicação por elementos da forma $\gamma S\gamma^{-1}$ ou $\gamma T^{\pm 1}\gamma^{-1}$. Em particular, se $\gamma \in \Gamma_1$ que descreve a passagem do domínio fundamental $\mathcal{F}_1$ para algum transladado $\gamma\mathcal{F}_1$ pode ser escrito como um produto de matrizes envolvendo S e T, então todos os elementos de Γ_1 que descrevem a passagem de $\mathcal{F}_1$ para qualquer um dos vizinhos de $\gamma\mathcal{F}_1$ também podem ser escritos em função de S e T. Indutivamente, podemos ver que isto é válido para todo $\gamma \in \Gamma_1$. □

2 Formas Modulares

O nome grupo modular tem relação com o fato de que os pontos do espaço quociente $\Gamma_1\backslash\mathfrak{H}$ são *moduli* — parâmetros — para as classes de isomorfismo de curvas elípticas sobre $\mathbb{C}$[1]. Como veremos mais adiante, para cada ponto $z \in \mathfrak{H}$ podemos associar ao reticulado $\Lambda_z = \mathbb{Z}.z + \mathbb{Z}.1 \subset \mathbb{C}$ o espaço quociente $E_z = \mathbb{C}/\Lambda_z$, que é uma curva elíptica, ou seja: é uma superfície de Riemann compacta. Reciprocamente, toda curva elíptica sobre $\mathbb{C}$ pode ser obtida dessa forma, embora não unicamente. Mais especificamente, se E é uma curva elíptica sobre $\mathbb{C}$, então podemos escrevê-la como o quociente $\mathbb{C}/\Lambda$, para algum reticulado $\Lambda \subset \mathbb{C}$ que é único a menos de homotetias $\Lambda \mapsto \lambda\Lambda$, com $\lambda \in \mathbb{C}^*$. Escolhendo uma base (ω_1, ω_2) de Λ com $\mathrm{Im}(\omega_1/\omega_2) > 0$ e tomando $\lambda = \omega_2^{-1}$, temos que $E \cong E_z$ para algum $z \in \mathfrak{H}$.

Uma função complexa em $\Gamma_1\backslash\mathfrak{H}$ é chamada de uma *função modular*. Uma função modular pode ser então compreendida como um dos seguintes objetos equivalentes:

- Uma função $f : \Gamma_1\backslash\mathfrak{H} \to \mathbb{C}$;
- Uma função $f : \mathfrak{H} \to \mathbb{C}$, satisfazendo $f(\gamma z) = f(z)$, para todo $z \in \mathfrak{H}$ e todo $\gamma \in \Gamma_1$;
- Uma função que associa a cada curva elíptica E sobre $\mathbb{C}$ um número complexo dependendo do tipo de isomorfismo de E;
- Uma função de reticulados em $\mathbb{C}$, satisfazendo $f(\lambda\Lambda) = f(\Lambda)$, para todo reticulado Λ e $\lambda \in \mathbb{C}$ não nulo.

Veremos posteriormente uma forma explícita de relacionar funções modulares do tipo $f : \mathfrak{H} \to \mathbb{C}$ a funções modulares de reticulados.

Geralmente, se tratando de funções modulares com respeito à Γ_1 ou algum outro subgrupo discreto Γ de $\mathrm{SL}(2, \mathbb{R})$, trabalhamos com funções modulares meromorfas, isto é, funções meromorfas Γ-invariantes em $\mathfrak{H}$ com crescimento exponencial no infinito. Para desenvolver resultados e propriedades interessantes, as funções modulares não são suficientes e precisamos de uma classe mais geral de funções: as *formas modulares*. Nosso objetivo nessa seção é definir e abordar as principais propriedades das formas modulares.

Definição 1. Seja k um número inteiro. Uma função meromorfa $f\colon \mathfrak{H} \to \mathbb{C}$ é dita *fracamente modular de peso k* se

$$f(\gamma z) = (cz + d)^k f(z), \tag{2.1}$$

[1] O Apêndice B discute brevemente a teoria básica de curvas elípticas complexas.

para toda matriz $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$ e $z \in \mathfrak{H}$. A condição 2.1 é chamada de *condição de automorfia.*

Observação 3. (1) Se $f\colon \mathfrak{H} \to \mathbb{C}$ é uma função fracamente modular de peso 0, então f é simplesmente Γ_1-invariante, visto que a definição 1 implica que $f(\gamma z) = f(z)$ para todo $\gamma \in \Gamma_1$ e $z \in \mathfrak{H}$.

(2) Seja $f\colon \mathfrak{H} \to \mathbb{C}$ uma função fracamente modular de peso k e considere $\gamma = -1_{2\times 2} \in \Gamma_1$. Se k é um número ímpar, a definição 1 nos diz que $f(z) = (-1)^k f(z) = -f(z)$ para todo $z \in \mathfrak{H}$, isto é, que f é identicamente nula. Por essa razão, trabalharemos com valores pares de k.

Seja $f\colon \mathfrak{H} \to \mathbb{C}$ uma função meromorfa. Sabemos pelo Corolário 1 que Γ_1 é gerado pelos elementos S e T. Dessa forma, para que f seja fracamente modular de peso k basta verificarmos sua invariância de pelos elementos geradores de Γ_1, ou seja, verificar que f satisfaça as equações

$$f(z+1) = f(z), \tag{2.2}$$
$$f(-1/z) = z^k f(z), \tag{2.3}$$

para todo $z \in \mathfrak{H}$.

O fato de uma função $f : \mathfrak{H} \to \mathbb{C}$ meromorfa satisfazer a equação (2.2) nos diz que funções fracamente modulares são $\mathbb{Z}$-periódicas. Seja $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ o disco aberto unitário e seja $\mathbb{D}^\times = \mathbb{D}\backslash\{0\}$ o disco unitário furado. A aplicação holomorfa e $\mathbb{Z}$-periódica $z \mapsto e^{2\pi i z}$ leva o semiplano superior $\mathfrak{H}$ em $\mathbb{D}^\times$, e portanto fica bem definida a função

$$\begin{aligned} \tilde{f}\colon \mathbb{D}^\times &\to \mathbb{C} \\ q &\mapsto \tilde{f}(q) = f\left(\frac{\log q}{2\pi i}\right), \end{aligned}$$

de modo que $f(z) = \tilde{f}\left(e^{2\pi i z}\right)$, para todo $z \in \mathfrak{H}$, como no seguinte diagrama:

$$\begin{array}{ccc} \mathfrak{H} & & \\ {\scriptstyle q}\downarrow & \searrow^{f} & \\ \mathbb{D}^\times & \xrightarrow[\tilde{f}]{} & \mathbb{C} \end{array}$$

Se f for holomorfa em $\mathfrak{H}$, então $\tilde{f}$ será holomorfa em $\mathbb{D}^\times$ e admitirá expansão de Fourier $\tilde{f}(q) = \sum_{n\in\mathbb{Z}} a_n q^n$, com $q \in \mathbb{D}^\times$. Tomando $q = e^{2\pi i z}$, para $z \in \mathfrak{H}$, a expressão $|q| = e^{-2\pi \operatorname{Im}(z)}$ garante que $q \to 0$ se, e somente se, $\operatorname{Im}(z) \to \infty$. Nesse sentido, dizemos que f é *homolorfa (resp. meromorfa) no infinito* se $\tilde{f}$ se estende a uma função holomorfa (resp. meromorfa) na origem. Isso significa que f admite uma expansão de Fourier

$$f(z) = \sum_{n=0}^{\infty} a_n q^n,$$

se for holomorfa no infinito, e admite expansão de Laurent

$$f(z) = \sum_{n=n_0}^{\infty} a_n q^n,$$

se for meromorfa no infinito, onde $q = e^{2\pi iz}$, com $z \in \mathfrak{H}$ e $n_0 \in \mathbb{Z}$.

Observação 4. Para fins práticos, mostrar que uma função $f\colon \mathfrak{H} \to \mathbb{C}$ fracamente modular de peso k é holomorfa (meromorfa) no infinito não exige que calculemos a sua q-expansão. De fato, vimos que f é holomorfa (resp. meromorfa) no infinito se a correspondente função $\tilde{f}$ no disco furado $\mathbb{D}^\times$ se estende holomorficamente (resp. meromorficamente) em 0. No entanto, o Teorema de Riemann nos garante que $\tilde{f}$ se extende holomorficamente em 0 se, e somente se, $\tilde{f}$ é limitada numa vizinhança $U\backslash\{0\}$. Equivalentemente, para mostrar que $f(z)$ é holomorfa no infinito é suficiente verificar que $\tilde{f}(q) = O(1)$ [2], quando $q \to 0$, ou seja, $f(z) = \tilde{f}(q) = O(1),$ quando $\operatorname{Im}(z) \to +\infty$. Similarmente, $f(z)$ é meromorfa no infinito se, e somente se, existe $n \in \mathbb{Z}$ tal que $q^n \tilde{f}(q) = O(1)$, quando $q \to 0$, ou que $e^{2\pi inz} f(z) = O(1)$, quando $\operatorname{Im}(z) \to \infty$. Nesse sentido, para mostrar que f é meromorfa no infinito basta exibir $C > 0$ tal que $|e^{2\pi inz} f(z)| = e^{-2\pi n \operatorname{Im}(z)} < C$, para $\operatorname{Im}(z)$ suficientemente grande.

Definição 2. Uma função fracamente modular de peso k é chamada de *modular de peso* k se é meromorfa no infinito.

Definição 3. Seja k um inteiro. Uma função $f\colon \mathfrak{H} \to \mathbb{C}$ é chamada de *forma modular de peso* k se

(1) f é holomorfa em $\mathfrak{H}$,

(2) f é fracamente modular de peso k,

(3) f é holomorfa no infinito.

Se f vale zero no infinito dizemos que f é uma *forma cuspidal*.

Conforme vimos, se uma função é holomorfa no infinito, os coeficientes a_n da sua expansão de Laurent numa vizinhança da origem são nulos para $n < 0$. Então, uma forma modular f pode então ser escrita como a série

$$f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi inz},$$

que converge para $|q| < 1$, isto é, para $\operatorname{Im}(z) > 0$. Equivalentemente, converge para todo $z \in \mathfrak{H}$. Além disso, f é uma forma cuspidal se, e somente se, $a_0 = 0$.

[2] A notação $f(z) = O(g)$, quando $z \to a$, indica que existe $C > 0$ tal que $f(z) \leqslant Cg(z)$, quando $z \to a$.

2.1 Reticulados e Funções Modulares

Definição 4. Dado V um $\mathbb{R}$-espaço vetorial de dimensão finita, dizemos que um subgrupo $\Gamma \subseteq V$ é um reticulado se satisfaz alguma das seguintes condições equivalentes:

(i) Γ é discreto e V/Γ é compacto;

(ii) Γ é discreto e gera o $\mathbb{R}$-espaço vetorial V;

(iii) Existe uma $\mathbb{R}$-base $\{e_1, \cdots, e_n\}$ de V que é uma $\mathbb{Z}$-base de Γ, isto é: $\Gamma = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$.

Denote por $\mathcal{R}$ o conjunto de todos os reticulados em $\mathbb{C}$ como $\mathbb{R}$-espaço vetorial e considere

$$M = \left\{(w_1, w_2) \in \mathbb{C}^2 \backslash \{(0,0)\} : \operatorname{Im}(w_1/w_2) > 0\right\}.$$

Para cada par $(w_1, w_2) \in M$, associamos o reticulado

$$\Gamma(w_1, w_2) = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2, \tag{2.4}$$

com base $\{w_1, w_2\}$. Note que essa associação caracteriza um mapa sobrejetivo

$$\begin{aligned} H\colon M &\to \mathcal{R} \\ (w_1, w_2) &\mapsto \Gamma(w_1, w_2) := \mathbb{Z}w_1 \oplus \mathbb{Z}w_2. \end{aligned}$$

Considere a aplicação:

$$\begin{aligned} \Gamma_1 \times M &\to M \\ (\gamma, (w_1, w_2)) &\mapsto \gamma \cdot (w_1, w_2) = (aw_1 + bw_2, cw_1 + dw_2), \end{aligned} \tag{2.5}$$

onde $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$ e $(w_1, w_2) \in M$. Essa aplicação está bem definida, já que, para todo $\gamma \in \Gamma_1$ e $(w_1, w_2) \in M$,

$$\operatorname{Im}\left(\frac{aw_1 + bw_2}{cw_1 + dw_2}\right) = \operatorname{Im}\left(\frac{a\frac{w_1}{w_2} + b}{c\frac{w_1}{w_2} + d}\right) = \operatorname{Im}\left(\gamma\left(\frac{w_1}{w_2}\right)\right) = \frac{\operatorname{Im}(\frac{w_1}{w_2})}{|cz + d|^2} > 0, \tag{2.6}$$

pois, como $(w_1, w_2) \in M$, temos $\operatorname{Im}(w_1/w_2) > 0$. Mostrando que $\gamma \cdot (w_1, w_2) \in M$, como queríamos. Mais ainda, a proposição a seguir nos mostra que essa aplicação é na verdade uma ação de Γ_1 em M.

Proposição 2. *A aplicação (2.5) é uma ação do grupo Γ_1 em M.*

Demonstração. A parte não trivial da demonstração é associatividade da ação. Sejam $(w_1, w_2) \in M$ e $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in \Gamma_1$ quaisquer. Então,

$$\begin{aligned} \gamma \cdot (\gamma' \cdot (w_1, w_2)) &= \gamma \cdot (a'w_1 + b'w_2, c'w_1 + d'w_2) \\ &= (a(a'w_1 + b'w_2) + b(c'w_1 + d'w_2), c(a'w_1 + b'w_2) + d(c'w_1 + d'w_2)) \\ &= ((aa' + bc')w_1 + (ab' + bd')w_2, (ca' + dc')w_1 + (cb' + dd')w_2 \\ &= (\gamma\gamma') \cdot (w_1, w_2). \end{aligned}$$

□

Proposição 3. *Dois elementos em M definem o mesmo reticulado se, e somente se, são congruentes módulo Γ_1.*

Demonstração. Suponha que $(w_1, w_2), (w_1', w_2') \in M$ definam o mesmo reticulado, digamos

$$\Gamma = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2 = \mathbb{Z}w_1' \oplus \mathbb{Z}w_2',$$

isto é, $\beta = \{w_1, w_2\}$ e $\beta' = \{w_1', w_2'\}$ são duas bases para o reticulado Γ. Assim, existe matriz mudança de base $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M(2, \mathbb{Z})$ que leva β em β' com $\det(\gamma) = \pm 1$, mais especificamente:

$$\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\gamma} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} w_1' \\ w_2' \end{pmatrix} \iff \begin{pmatrix} aw_1 + bw_2 \\ cw_1 + dw_2 \end{pmatrix} = \begin{pmatrix} w_1' \\ w_2' \end{pmatrix}$$

$$\iff w_1' = aw_1 + bw_2 \ \text{ e } \ w_2' = cw_1 + bw_2.$$

Assim, temos:

$$\frac{w_1'}{w_2'} = \frac{aw_1 + bw_2}{cw_1 + dw_2} = \frac{a\frac{w_1}{w_2} + b}{c\frac{w_1}{w_2} + d} = \gamma\left(\frac{w_1}{w_2}\right).$$

Como, para todo $z \in \mathbb{C}$, vale $\mathrm{Im}(\gamma z) = \dfrac{(ad - bc)\,\mathrm{Im}(z)}{|cz + d|^2}$ (expressão vista na demonstração do Lema 1), segue que

$$\mathrm{Im}\left(\frac{w_1'}{w_2'}\right) = \frac{(ad - bc)\,\mathrm{Im}(w_1/w_2)}{|c(w_1/w_2) + d|^2} = \frac{det(\gamma)\,\mathrm{Im}(w_1/w_2)}{|c(w_1/w_2) + d|^2}.$$

Tendo em vista a expressão acima, se $det(\gamma) = -1$, o sinal de $\mathrm{Im}(w_1'/w_2')$ seria o oposto do sinal de $\mathrm{Im}(w_1/w_2)$, o que não pode ocorrer, visto que $(w_1, w_2), (w_1', w_2') \in M$ implica $\mathrm{Im}(w_1/w_2), \mathrm{Im}(w_1'/w_2') > 0$. Logo, $det(\gamma) = 1$ e portanto $\gamma \in \Gamma_1$. Sendo assim, existe $\gamma \in \Gamma_1$ tal que $\gamma \cdot (w_1, w_2) = (w_1', w_2')$, ou seja: (w_1, w_2) e (w_1', w_2') são congruentes módulo Γ_1.

Reciprocamente, suponha que os elementos $(w_1, w_2), (w_1', w_2') \in M$ sejam congruentes módulo Γ_1, isto é, que exista $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$ tal que

$$\gamma \cdot (w_1, w_2) = (w_1', w_2') \iff w_1' = aw_1 + bw_2 \ \text{ e } \ w_2' = cw_1 + dw_2.$$

A expressão acima nos mostra que w_1' e w_2' são combinações lineares dos elementos w_1 e w_2. Logo, $\Gamma(w_1', w_2') \subset \Gamma(w_1, w_2)$. Utilizando a mesma argumentação para γ^{-1}, concluímos. □

Na introdução deste capítulo, mencionamos que é possível relacionar explicitamente funções modulares do tipo $\mathfrak{H} \to \mathbb{C}$ à funções modulares de reticulados. Essa relação é de extrema importância para começarmos a estudar os primeiros exemplos não-triviais de formas modulares. Neste momento, temos as ferramentas necessárias para descrever esse processo.

Definição 5. Dada uma função $F\colon \mathcal{R} \to \mathbb{C}$ e $k \in \mathbb{Z}$, dizemos que F é de peso k se para todo reticulado $\Gamma \in \mathcal{R}$ e todo $\lambda \in \mathbb{C}^\times$ vale

$$F(\lambda\Gamma) = \lambda^{-k}F(\Gamma).$$

Seja F uma função de peso k. Dado $(w_1, w_2) \in M$, denotamos por $\widetilde{F}(w_1, w_2)$ o valor de F no reticulado $\Gamma(w_1, w_2)$, isto é:

$$\widetilde{F}(w_1, w_2) := F(\Gamma(w_1, w_2)).$$

Note que temos a seguinte relação:

$$\begin{array}{ccc} M & \xrightarrow{H} & \mathcal{R} \\ & \searrow^{\widetilde{F}} & \downarrow F \\ & & \mathbb{C} \end{array}$$

Sendo F de peso k, escrevemos:

$$\widetilde{F}(\lambda w_1, \lambda w_2) = \lambda^{-k}\widetilde{F}(w_1, w_2), \qquad \text{para todo } \lambda \in \mathbb{C}^\times. \tag{2.7}$$

Além disso, da Proposição 3 temos que dois elementos de M definem o mesmo reticulado se, e somente se, são congruentes módulo Γ_1. Dessa forma, segue que F é invariante pela ação de Γ_1 em M.

Tendo a expressão (2.7) em vista, e dado $(w_1, w_2) \in M$, temos $w_2 \neq 0$ e portanto, para $\lambda = w_2^{-1}$,

$$\widetilde{F}(w_1 w_2^{-1}, w_2 w_2^{-1}) = w_2^k \widetilde{F}(w_1, w_2) \implies \widetilde{F}(w_1/w_2, 1) = w_2^k \widetilde{F}(w_1, w_2),$$

mostrando que $w_2^k \widetilde{F}(w_1, w_2)$ depende apenas de $z = w_1/w_2$. Logo, existe função $f : \mathfrak{H} \to \mathbb{C}$ tal que

$$F(\Gamma(w_1, w_2)) = \widetilde{F}(w_1, w_2) = w_2^{-k} f\left(\frac{w_1}{w_2}\right). \tag{2.8}$$

Uma vez que F é Γ_1-invariante, temos que f satisfaz, para todo $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$, a identidade:

$$f(z) = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right), \tag{2.9}$$

isto é, f é uma função fracamente modular de peso k. De fato, basta observar que, para todo $z = w_1/w_2$, obtivemos $f(z) = \widetilde{F}(z, 1) := F(\Gamma_1(z, 1)) = F(\mathbb{Z}z + \mathbb{Z})$. Então, para todo $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$, concluímos que

$$\begin{aligned} f(\gamma z) = f\left(\frac{az + b}{cz + d}\right) &= F\left(\mathbb{Z}\left(\frac{az + b}{cz + d}\right) + \mathbb{Z}\right) = F\left(\frac{1}{cz + d}\left(\mathbb{Z}(az + b) + \mathbb{Z}(cz + d)\right)\right) \\ &= (cz + d)^k \widetilde{F}(z, 1) = (cz + d)^k f(z). \end{aligned}$$

O caminho reverso também é possível: se f é uma função fracamente modular de peso k, a expressão (2.8) associa f a uma função de reticulado F em $\mathcal{R}$ de peso k. De fato, note primeiramente que para cada par $(w_1, w_2) \in M$, podemos associar um ponto $z \in \mathfrak{H}$ e vice-versa, via as aplicações:

$$\begin{aligned} M &\to \mathfrak{H} & \mathfrak{H} &\to M \\ (w_1, w_2) &\mapsto z := \frac{w_1}{w_2} & z &\mapsto (z, 1) \end{aligned}$$

Evidentemente, elas estão bem definidas: se (w_1, w_2) é um ponto de M, então $\mathrm{Im}(w_1/w_2) > 0$. Isso mostra que $z := w_1/w_2$ é um ponto de $\mathfrak{H}$. Da mesma forma, se $z \in \mathfrak{H}$, temos $\mathrm{Im}(z) > 0$, e portanto $(z, 1) \in M$.

Agora, seja $f : \mathfrak{H} \to \mathbb{C}$ uma função modular de peso k. Então, para cada $z \in \mathfrak{H}$ existe ponto correspondente $(w_1, w_2) \in M$. Assim, a expressão 2.8 nos fornece função $F : \mathcal{R} \to \mathbb{C}$ dada por

$$F(\Gamma(w_1, w_2)) = w_2^{-k} f\left(\frac{w_1}{w_2}\right).$$

Da modularidade de f, segue que, para todo $\lambda \in \mathbb{C}^\times$:

$$\begin{aligned} F(\lambda\Gamma(w_1, w_2)) = F(\Gamma(\lambda w_1, \lambda w_2)) &= (\lambda w_2)^{-k} f\left(\frac{\lambda w_1}{\lambda w_2}\right) = \lambda^{-k}\left(w_2^{-k} f\left(\frac{\lambda w_1}{\lambda w_2}\right)\right) \\ &= \lambda^{-k} F(\Gamma(w_1, w_2)), \end{aligned}$$

mostrando que F é uma função modular de peso k. Dessa forma, existe uma identificação:

$$\{\text{funções modulares de peso } k\} \longleftrightarrow \{\text{funções modulares de reticulados de peso } k\}.$$

2.2 Séries de Eisenstein

A função nula em $\mathfrak{H}$ é uma forma modular de peso k, para todo k inteiro, e funções constantes em $\mathfrak{H}$ são formas modulares de peso 0. Um primeiro exemplo não-trivial de formas modulares são as chamadas *séries de Eisenstein*, que discutiremos a seguir.

Lema 2. *Seja Γ um reticulado em $\mathbb{C}$. A série*

$$\sum_{\gamma\in\Gamma}{}' \frac{1}{|\gamma|^\sigma} \tag{2.10}$$

é convergente para todo $\sigma > 2$. (O símbolo $\sum'$ representa a soma sobre todos os elementos não nulos de Γ).

Uma prova para este resultado pode ser encontrado em [2], pg. 82-83.

Definição 6. Sejam $k > 2$ um inteiro e Γ um reticulado em $\mathbb{C}$. A série

$$G_k(\Gamma) = \sum_{\gamma\in\Gamma}{}' \frac{1}{\gamma^k} \tag{2.11}$$

é chamada *série de Eisenstein de peso k.*

O Lema 2 garante que a série de Eisenstein converge absolutamente. Além disso, a função G_k é uma função de reticulado de peso k, pois satisfaz a identidade

$$G_k(\lambda\Gamma) = \sum_{\gamma\in\Gamma}{}' \frac{1}{(\lambda\gamma)^k} = \frac{1}{\lambda^k}\sum_{\gamma\in\Gamma}{}' \frac{1}{\gamma^k} = \lambda^{-k}G_k(\Gamma) \quad \text{, para todo } \lambda \in \mathbb{C}^\times.$$

Conforme visto na seção anterior, dado $(w_1, w_2) \in M$, podemos considerar o reticulado $\Gamma(w_1, w_2) = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ e ver G_k como função de M:

$$\widetilde{G}_k(w_1, w_2) := G_k(\Gamma(w_1, w_2)) = \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(mw_1 + nw_2)^k}. \tag{2.12}$$

Mais ainda, vimos que existe uma identificação entre funções de reticulados e funções modulares de mesmo peso. Dessa forma, a função fracamente modular de peso k em $\mathfrak{H}$ que corresponde a função de reticulados (2.12) é obtida aplicando a equação (2.8). Portanto, a série de Eisenstein de peso k como função de $\mathfrak{H}$ é dada por:

$$G_k(z) = \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(mz + n)^k}. \tag{2.13}$$

Proposição 4. *Seja $k > 2$ inteiro. A série de Eisenstein $G_k(z)$ é uma forma modular de peso k. Além disso, $G_k(\infty) = 2\zeta(k)$, onde ζ denota a função zeta de Riemann.*

Demonstração. Já vimos que $G_k(z)$ é uma função fracamente modular de peso k. Resta verificar que $G_k(z)$ é holomorfa (inclusive no infinito). Como $\mathcal{F}_1$ é um domínio fundamental para ação de Γ_1 em $\mathfrak{H}$, podemos supor $z \in \overline{\mathcal{F}_1}$, isto é, $|z| \geqslant 1$ e $|\operatorname{Re}(z)| \leqslant 1/2$. Logo,

$$|mz+n|^2 = m^2|z|^2+2mn\operatorname{Re}(z)+n^2 \geqslant m^2-mn\operatorname{Re}(z)+n^2 = |m\omega-n|^2 \ , \qquad \text{onde } \omega = e^{2\pi i/3}.$$

Pelo Lema 2, a série $\sum' \dfrac{1}{|m\omega+n|^k}$ é convergente, pois $k > 2$. A desigualdade acima nos mostra que $G_k(z)$ converge normalmente[3] em $\mathcal{F}_1$. Como $\mathcal{F}_1$ é um domínio fundamental para a ação de Γ_1 em $\mathfrak{H}$, temos $G_k(z)$ convergente em cada um dos transladados $\gamma\mathcal{F}_1$, com $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$, pois

$$G_k(z) = G_k(\gamma\gamma^{-1}z) = (cz+d)^{-k}G_k(\gamma^{-1}z),$$

e $G_k(\gamma^{-1}z)$ converge normalmente em $\mathcal{F}_1$. Uma vez que essas regiões cobrem $\mathfrak{H}$, segue que $G_k(z)$ é holomorfa em $\mathfrak{H}$. Por fim, falta ver que $G_k(z)$ é holomorfa no infinito; para tal, vamos usar a convergência uniforme de $G_k(z)$ em $\mathcal{F}_1$ para calcular o limite de $G_k(z)$ quando $\operatorname{Im}(z) \to \infty$ termo a termo. De fato, os limites $\dfrac{1}{(mz+n)^k}$ se anulam para os pares (m,n) com $m \neq 0$ e valem $\dfrac{1}{n^k}$ para os pares (m,n) com $m = 0$. Logo,

$$G_k(\infty) = \lim_{\operatorname{Im}(z)\to\infty} G_k(z) = \sum{}' \frac{1}{n^k} = 2\sum_{n=1}^{\infty} \frac{1}{n^k} = 2\zeta(k). \qquad \square$$

Observação 5. Na Observação 3, item (2), vimos que funções fracamente modulares de peso ímpar são identicamente nulas. Logo, as séries de Eisenstein de peso ímpar são identicamente nulas. Nesse sentido, estamos interessados em trabalhar com as séries de Eisenstein G_k para $k > 2$ par.

2.2.1 Os Números de Bernoulli e as Séries de Eisenstein Normalizadas

As séries de Eisenstein são formas modulares de peso k, e portanto admitem q-expansão de Fourier. Introduzimos os *números de Bernoulli* com o propósito de encontrar essa expansão.

Definição 7. Seja $k \geqslant 0$ um número inteiro. O k-ésimo *número de Bernoulli*, B_k, é dado pela expressão:

$$\sum_{k=0}^{\infty} \frac{B_k}{k!}x^k = \frac{x}{e^x-1}. \tag{2.14}$$

[3] Dizemos que a convergência de uma série $\sum_{n=0}^{\infty} f_n$ de funções $f_n : S \to \mathbb{C}$ é *normal* se a série de normas uniformes $\sum_{n=0}^{\infty} \sup_{x\in S} |f_n(x)|$ converge. Além disso, séries normalmente convergentes de funções holomorfas são holomorfas.

Exemplo 1. Os primeiros números de Bernoulli são dados por:

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0, \ldots$$

O resultado a seguir nos mostra que se $k \neq 1$ é um número ímpar, então os números de Bernoulli B_k são nulos.

Lema 3. *Se $k \geqslant 3$ é um inteiro ímpar, então $B_k = 0$.*

Demonstração. Extraindo o termo correspondente a $k = 1$ da soma que define o número de Bernoulli B_k, obtemos

$$\frac{x}{e^x - 1} + \frac{x}{2} = \sum_{k=0, k\neq 1}^{\infty} \frac{B_k}{k!} x^k.$$

Note que

$$\frac{x}{e^x - 1} + \frac{x}{2} = \frac{2x + x(e^x - 1)}{2(e^x - 1)} = \frac{x}{2} \cdot \frac{e^x + 1}{e^x - 1} = \frac{x}{2} \cdot \frac{e^{x/2} + e^{-x/2}}{e^{x/2} - e^{-x/2}},$$

e, portanto,

$$\sum_{k=0, k\neq 1}^{\infty} \frac{B_k}{k!} x^k = \frac{x}{2} \cdot \frac{e^{x/2} + e^{-x/2}}{e^{x/2} - e^{-x/2}}.$$

Se trocarmos x por $-x$ na identidade acima, ela se mantém inalterada. Isso implica que $B_k = (-1)^k B_k$, para $k \neq 1$. Logo, se $k \geqslant 3$ é ímpar, concluímos que $B_k = 0$. □

Teorema 2 (Teorema de Euler)**.** *Os números de Bernoulli determinam os valores da função zeta de Riemann para entradas pares, isto é: se $k \geqslant 1$ é um inteiro, então*

$$\zeta(2k) = \frac{2^{2k-1}}{(2k)!} B_{2k} \pi^{2k}. \tag{2.15}$$

Demonstração. Por um lado, tomando $x = 2iz$ na equação (2.14) obtemos a identidade

$$zcotg(z) = 1 - \sum_{k=1}^{\infty} B_{2k} \frac{2^{2k} z^{2k}}{(2k)!}. \tag{2.16}$$

Por outro lado, tomando a derivada logarítmica da expressão

$$sin(z) = z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2 \pi^2}\right),$$

obtemos

$$zcotg(z) = 1 + 2 \sum_{n=1}^{\infty} \frac{z^2}{z^2 - n^2 \pi^2} = 1 - 2 \sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \frac{z^{2k}}{n^{2k} \pi^{2k}}. \tag{2.17}$$

Igualando as equações (2.16) e (2.17) obtemos (2.15). □

Proposição 5. *Para $k \geqslant 2$, vale*

$$G_{2k}(z) = 2\zeta(2k) + 2 \frac{(2i\pi)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n,$$

onde $\sigma_k(n)$ denota a soma $\sum_{d|n} d^k$.

Demonstração. De fato, por um lado temos a fórmula

$$\pi cotg(\pi z) = \frac{1}{z} + \sum_{m=1}^{\infty} \left(\frac{1}{z+m} - \frac{1}{z-m} \right).$$

Por outro, sabemos que

$$\pi cotg(\pi z) = \pi \frac{\cos(\pi z)}{\text{sen}(\pi z)} = i\pi \frac{q+1}{q-1} = i\pi - 2i\pi \sum_{n=0}^{\infty} q^n.$$

Igualando as duas equações acima e derivando-a sucessivas vezes, segue que, para $k \geqslant 2$,

$$\sum_{m \in \mathbb{Z}} \frac{1}{(m+z)^k} = \frac{1}{(k+1)!}(-2i\pi)^k \sum_{n=1}^{\infty} n^{k-1} q^n. \tag{2.18}$$

Da definição, expandimos

$$G_{2k} = \sum_{(n,m) \neq (0,0)} \frac{1}{(nz+m)^{2k}} = 2\zeta(2k) + 2 \sum_{n=1}^{\infty} \sum_{m \in \mathbb{Z}} \frac{1}{(nz+m)^{2k}}.$$

Substituindo a equação (2.18) para $n = nz$ na expressão acima obtemos

$$G_{2k} = 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!} \sum_{d=1}^{\infty} \sum_{a=1}^{\infty} d^{2k-1} q^{ad} = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n \qquad \square$$

Tendo em vista a proposição acima e o fato de que o coeficiente inicial da série de Eisenstein $2\zeta(2k)$ é sempre não nulo para todo $k > 1$, podemos normalizar a série de Eisenstein de modo que seu coeficiente inicial seja 1. Mais especificamente, denotamos por

$$E_{2k} = \frac{G_{2k}}{2\zeta(2k)}$$

a *série de Eisenstein normalizada*, onde

$$E_{2k}(z) = 1 + \gamma_{2k} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n \quad \text{e} \quad \gamma_{2k} = (-1)^k \frac{4k}{B_{2k}}.$$

Observação 6. O coeficiente γ_{2k} pode ser calculado utilizando a Proposição 2 da seguinte forma:

$$\gamma_{2k} = \frac{(2\pi i)^{2k}}{(2k-1)!\zeta(2k)} = \frac{(2\pi)^{2k}(-1)^k(2k)!}{(2k-1)!2^{2k-1}B_{2k}\pi^{2k}} = (-1)^k \frac{4k}{B_{2k}}.$$

Essencialmente, as proposições apresentadas podem ser também utilizadas como ferramentas de cálculo. Para ilustrar, considere a seguinte tabela, que relaciona um número inteiro par $2k$ aos seus respectivos valores do número de Bernoulli B_{2k}, da função zeta de Riemann $\zeta(2k)$ e da série de Eisenstein normalizada E_{2k}.

Tabela 1 – Números de Bernoulli e valores das séries de Eisenstein normalizadas.

$2k$	B_{2k}	$\zeta(2k)$	E_{2k}
4	$B_4 = -\frac{1}{30}$	$\zeta(4) = \frac{\pi^4}{2 \cdot 3^2 \cdot 5}$	$E_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n$
6	$B_6 = \frac{1}{42}$	$\zeta(6) = \frac{\pi^6}{3^3 \cdot 5 \cdot 7}$	$E_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n$
8	$B_8 = -\frac{1}{30}$	$\zeta(8) = \frac{\pi^8}{2 \cdot 3^2 \cdot 5^2 \cdot 7}$	$E_8 = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n$
10	$B_{10} = \frac{5}{66}$	$\zeta(10) = \frac{\pi^{10}}{3^5 \cdot 5 \cdot 7 \cdot 11}$	$E_{10} = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n) q^n$
12	$B_{12} = -\frac{691}{2730}$	$\zeta(12) = \frac{691\pi^{12}}{3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13}$	$E_{12} = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n$
14	$B_{14} = \frac{7}{6}$	$\zeta(14) = \frac{2\pi^{14}}{3^6 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13}$	$E_{14} = 1 - 24 \sum_{n=1}^{\infty} \sigma_{13}(n) q^n$

Fonte: [2, p. 91, p.93]

Observe que, a princípio, as séries de Eisenstein são objetos puramente analíticos, mas os coeficientes de suas séries de Fourier possuem natureza aritmética, visto que dependem da função aritmética σ_k multiplicados por coeficientes racionais. Este é um primeiro indicativo de que existe uma relação direta do estudo dessas funções com a Teoria dos Números. Em certo sentido, as séries de Eisenstein são séries geradoras de funções aritméticas.

2.2.2 Séries de Eisenstein de Peso 2

As séries de Eisenstein são formas modulares de peso k, para todo $k > 2$. Este fato se deve essencialmente ao Lema 2, que garante a convergência das séries

$$\sum_{\gamma \in \Gamma}{}' \frac{1}{|\gamma|^\sigma},$$

para $\sigma > 2$, em que Γ é um reticulado em $\mathbb{C}$. No entanto, para $k = 2$ podemos definir

$$G_2(z) = \sum_n \sum_m{}' \frac{1}{(m + nz)^2}$$

como a *série de Eisenstein de peso 2*. Observe que não ter a garantia da convergência absoluta da série implica que a ordem em que a soma é feita é relevante e, neste caso, convencionamos que a soma seja feita primeiramente em $n \in \mathbb{Z}$, e depois em $m \in \mathbb{Z}$. Uma consequência imediata disto é que não podemos obter a equação de modularidade para o elemento $S \in \Gamma_1$, ou seja:

$$G_2(-1/z) = z^2 G_2(z).$$

No entanto, podemos obter uma equação similar, adicionando um termo de correção.

Lema 4. *Seja G_2 a série de Eisenstein de peso 2. Então, para todo $z \in \mathfrak{H}$,*

$$G_2(-1/z) = z^2 G_2(z) - 2\pi i z.$$

Demonstração. Considere as séries duplas

$$G_2(z) = \sum_n \sum_m{}' \frac{1}{(m+nz)^2} \;;\; G(z) = \sum_m \sum_n{}' \frac{1}{(m+nz)^2};$$
$$H_2(z) = \sum_n \sum_m{}' \frac{1}{(m-1+nz)(m+nz)} \;;\; H(z) = \sum_m \sum_n{}' \frac{1}{(m-1+nz)(m+nz)}.$$

Utilizando a fórmula

$$\frac{1}{(m-1+nz)(m+nz)} = \frac{1}{m-1+nz} + \frac{1}{m+nz}, \tag{2.19}$$

é possível calcular explicitamente as séries H_2 e H, e ver que elas convergem para $H_2 = 2$ e $H = 2 - \dfrac{2\pi i}{z}$. Note que:

$$G_2 - H_2 = \sum_n \sum_m{}' \frac{1}{(m+nz)^2} - \frac{1}{(m-1+nz)(m+nz)},$$
$$G - H = \sum_m \sum_n{}' \frac{1}{(m+nz)^2} - \frac{1}{(m-1+nz)(m+nz)},$$

isto é, o termo geral das duas séries duplas $G_2 - H_2$ e $G - H$ coincidem, apenas trocam a ordem da soma. Então, pela equação (2.19), a série de termo geral

$$\frac{1}{(m+nz)^2} - \frac{1}{(m-1+nz)(m+nz)} = \frac{1}{(m+nz)^2(m-1+nz)}$$

é absolutamente somável, e , portanto, as séries $G_2 - H_2$ e $G - H$ coincidem, e as séries G e G_2 convergem. Logo,

$$G_2(z) - G(z) = H_2(z) - H(z) = \frac{2\pi i}{z}.$$

Como $G_2(-1/z) = z^2 G(z)$, segue que

$$G_2\left(-1/z\right) = z^2 G_2(z) - 2\pi i z. \tag{2.20}$$

□

A q-expansão de G_2 pode ser obtida com cálculos análogos aos feitos na Proposição 5, e obtemos a seguinte expressão:

$$G_1(z) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

Dividindo pelo termo $2\zeta(2) = \pi^2/6$, obtemos a série de Eisenstein normalizada de peso 2

$$E_2(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

3 Estrutura e Dimensão do Espaço das Formas Modulares

Seja k um número inteiro. Denotamos por M_k o conjunto das formas modulares de peso k. Neste capítulo, vamos descrever resultados e propriedades que concernem à estrutura de M_k - mais especificamente, vamos ver que M_k é, antes de tudo, um $\mathbb{C}$-espaço vetorial, e que $\bigoplus_{k\in\mathbb{Z}} M_k$ é um anel graduado.

Além disso, vamos provar que M_k é um espaço de dimensão finita e obter uma fórmula para calculá-la, bem como apresentar uma caracterização explícita deste espaço: se S_k denota o conjunto das formas cuspidais de peso k (*Spitzenform*), então toda forma modular $f \in M_k$ pode ser escrita unicamente como uma combinação linear de séries de Eisenstein G_k e formas cuspidais $g \in S_k$.

Lema 5. *Sejam $f, g \in M_k$, $c \in \mathbb{C}$ e $k \in \mathbb{Z}$. Então, $f + cg \in M_k$.*

Demonstração. A soma e multiplicação por escalar de funções holomorfas em $\mathfrak{H}$ (inclusive no infinito) continuam sendo funções holomorfas em $\mathfrak{H}$ (inclusive no infinito). Se $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$, temos, para todo $z \in \mathfrak{H}$:

$$(f + cg)(\gamma z) = f(\gamma z) + cg(\gamma z) = (cz + d)^k (f(z) + cg(z)) = (cz + d)^k (f + cg)(z).$$

Portanto, $f + cg \in M_k$. □

O Lema 5 nos mostra que combinações lineares sobre $\mathbb{C}$ de formas modulares de peso k são formas modulares de peso k, e portanto nos mostra que M_k possui estrutura de $\mathbb{C}$-espaço vetorial.

Lema 6. *Sejam $k, l \in \mathbb{Z}$ e considere $f \in M_k$ e $g \in M_l$. Então, $fg \in M_{k+l}$.*

Demonstração. O produto de funções holomorfas em $\mathfrak{H}$ (inclusive no infinito) é uma função holomorfa em $\mathfrak{H}$ (inclusive no infinito). Além disso, para todo $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$, temos:

$$(fg)(\gamma z) = f(\gamma z)g(\gamma z) = (cz + d)^k f(z)(cz + d)^l g(z) = (cz + d)^{k+l}(fg)(z),$$

visto que $f \in M_k$ e $g \in M_l$ são de pesos k e l, respectivamente. Portanto, fg é uma forma modular de peso $k + l$, isto é, $fg \in M_{k+l}$. □

O Lema 6 nos mostra que, para quaisquer $k, l \in \mathbb{Z}$, temos $M_k M_l \subseteq M_{k+l}$. Juntando isto ao fato de que cada M_k é um $\mathbb{C}$-espaço vetorial - em particular, um grupo abeliano aditivo - segue que $\bigoplus_{k\in\mathbb{Z}} M_k$ é um anel graduado.

Vimos, nas seções anteriores, primeiros exemplos não triviais de formas modulares, tais como as séries de Eisenstein G_k. Nosso objetivo agora é provar um teorema que nos mostra que qualquer forma modular de peso k é, na realidade, escrita unicamente como uma combinação linear de séries de Eisenstein G_k e formas cuspidais S_k.

Proposição 6. *Seja $k > 2$ um inteiro. Então, $M_k = \mathbb{C}.G_k \oplus S_k$.*

Demonstração. Primeiramente, vejamos que $M_k = \mathbb{C}.G_k + S_k$. A inclusão $\supseteq$ é imediata, visto que soma de formas modulares de peso k é uma forma modular de peso k, pelo Lema 5. Para a outra inclusão, seja $f(z) = \sum a_n(f)q^n$ a q-expansão de f. Em particular, $a_0 \colon M_k \to \mathbb{C}$ é um funcional linear não-nulo tal que $\ker(a_0) = S_k$. Se $a_0(f) = 0$, então $f \in S_k$ e não há o que provar. Suponha $a_0(f) \neq 0$ e tome $\lambda = \dfrac{a_0(f)}{a_0(G_k)}$, onde $a_0(G_k) = 2\zeta(k) \neq 0$, visto que $k > 2$, e $g = f - \lambda G_k$. Note que g é uma forma modular de peso k como soma de formas modulares de peso k. Mais ainda, como

$$a_0(g) = a_0(f) - \lambda a_0(G_k) = a_0(f) - \frac{a_0(f)}{a_0(G_k)} = 0,$$

segue que g é forma cuspidal. Portanto, $f = \lambda G_k + g \in \mathbb{C}.G_k + S_k$, como queríamos.

Resta mostrar que a soma é direta, isto é, que $\mathbb{C}.G_k \cap S_k = \{0\}$. Com efeito, suponha $f(z) = \sum a_n(f)q^n \in \mathbb{C}.G_k \cap S_k$; então, como $f \in S_k$, segue que f é forma cuspidal, ou seja, $a_0(f) = 0$. Por outro lado, como $f \in \mathbb{C}.G_k$, temos $f = \lambda G_k$, para algum $\lambda \in \mathbb{C}$, de onde temos $a_0(f) = \lambda a_0(G_k) = \lambda 2\zeta(k)$. A condição $a_0(f) = 0$ força $\lambda = 0$, e portanto $f \equiv 0$. □

Uma vez vistos os principais aspectos estruturais do espaço M_k, podemos estudar sua dimensionalidade. Para isso, comecemos com a seguinte definição e o seguinte teorema associado.

Definição 8. Dada uma função f não-nula e meromorfa em $\mathfrak{H}$ e dado ponto $p \in \mathfrak{H}$, dizemos que $n \in \mathbb{Z}$ é a ordem de f em p se $f/(z-p)^n$ é holomorfa e não nula em p. Neste caso, denotamos

$$\mathrm{ord}_p(f) := n.$$

Além disso, definimos $\mathrm{ord}_\infty(f)$ como a ordem da $q-$expansão de f em 0.

Seja f uma função modular de peso k. Em geral, f não é bem definida no quociente $\Gamma_1\backslash\mathfrak{H}$, pois, se

$$\begin{aligned} f \colon \frac{\Gamma_1}{\mathfrak{H}} &\to \mathbb{C} \\ [z] &\mapsto f([z]) := f(z), \end{aligned}$$

pode ocorrer que, para pontos distintos $z, z' \in \mathfrak{H}$ em uma mesma classe $[z]$, tenhamos $f(z) \neq f(z') := f([z])$. No entanto, a condição de automorfia de f, isto é, o fato de que, para todo $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$ e todo $z \in \mathfrak{H}$, temos $f(\gamma z) = (cz+d)^k f(z)$, nos permite concluir que, em um ponto $p \in \mathfrak{H}$, a ordem $\mathrm{ord}_p(f)$ depende apenas da órbita Γp. De fato, se $n = \mathrm{ord}_p(f)$, então a função $f(z)/(z-p)^n$ é não-nula em p e holomorfa em $\mathfrak{H}$. A condição de automorfia de f implica que

$$\frac{f(\gamma z)}{(cz+d)^k (z-p)^n} = \frac{f(z)}{(z-p)^n}$$

é não-nula em p e holomorfa em $\mathfrak{H}$, ou seja, $\mathrm{ord}_p(f(\gamma z)) = n = \mathrm{ord}_p(f)$. Em outros termos, isto mostra que $\mathrm{ord}_p(f)$ depende apenas da imagem de p no quociente $\Gamma_1 \backslash \mathfrak{H}$. Faz sentido então considerar $\mathrm{ord}_P(f)$, para cada $P = [p] \in \Gamma_1 \backslash \mathfrak{H}$. O principal resultado que veremos nos diz que a soma de todas essas ordens, isto é, a soma total dos zeros de f, depende apenas de k. Para tal, precisamos entender melhor a geometria do espaço quociente $\Gamma_1 \backslash \mathfrak{H}$, pois existem pontos singulares, isto é, pontos em $\mathfrak{H}$ que não possuem estabilizador trivial em $\overline{\Gamma}_1$. O Lema a seguir caracteriza os pontos singulares de $\Gamma_1 / \mathfrak{H}$ e os respectivos estabilizadores no domínio fundamental $\overline{\mathcal{F}_1}$.

Lema 7. *Seja $z \in \overline{\mathcal{F}_1}$ e considere $I(z) = \{\gamma \in \overline{\Gamma_1} : \gamma z = z\}$ o estabilizador de z em $\overline{\Gamma_1}$. Então, $I(z) = \{1_{2\times 2}\}$ para todo $z \in \overline{\mathcal{F}_1}$, exceto nos seguintes casos:*

- *$z = i$, e neste caso $I(z)$ é o grupo de ordem 2 gerado por S,*
- *$z = \omega = e^{2\pi i/3}$, e neste caso $I(z)$ é o grupo de ordem 3 gerado por ST,*
- *$z = -\overline{\omega} = e^{\pi i/3}$, e neste caso $I(z)$ é o grupo de ordem 2 gerado por TS.*

Uma demonstração para este resultado pode ser encontrada em [2], nas páginas 78 e 79.

Observação 7. Seja f uma função modular de peso k e $P \in \Gamma_1 \backslash \mathfrak{H}$. Vamos denotar por e_P a ordem do estabilizador de P. Por exemplo, $e_P = 2$, se $P = [i]$ módulo Γ_1, $e_P = 3$, se $P = [\omega]$ módulo Γ_1 e $e_P = 1$ para todos os outros casos, conforme vimos no Lema 7.

Teorema 3 (Fórmula de Valência)**.** *Seja f função modular de peso k não-nula. Então,*

$$ord_\infty(f) + \sum_{P \in \Gamma_1 \backslash \mathfrak{H}} \frac{1}{e_P} ord_P(f) = \frac{k}{12}. \tag{3.1}$$

Mais ainda, pelo Lema 7, a expressão acima pode ser escrita na forma:

$$ord_\infty(f) + \frac{1}{2} ord_i(f) + \frac{1}{3} ord_\omega(f) + \sum_{P \in \Gamma_1 \backslash \mathfrak{H}}^{*} ord_P(f) = \frac{k}{12}, \tag{3.2}$$

onde o símbolo $\sum^*$ indica a soma dos pontos $P \in \Gamma_1 \backslash \mathfrak{H}$ que são distintos das classes de i e ω módulo Γ_1.

Demonstração. Vejamos primeiramente que a equação 3.2 está bem definida, isto é, que f possui um número finito de zero e polos módulo Γ_1. De fato, como $f\colon \mathfrak{H} \to \mathbb{C}$ é meromorfa em $\mathfrak{H}$, vimos que a aplicação

$$\begin{aligned} g\colon \mathbb{D}^\times &\to \mathbb{C} \\ q \mapsto g(q) &= f\left(\frac{\log q}{2\pi i}\right), \qquad \text{onde } q = e^{2\pi i z} \text{ , e } z \in \mathfrak{H}, \end{aligned}$$

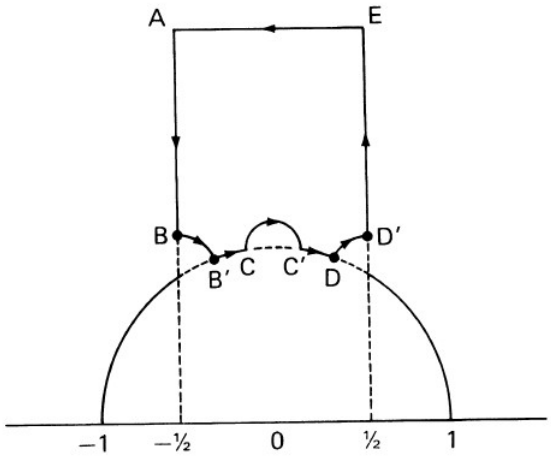
é uma função meromorfa em $\mathbb{D}^\times$ tal que $f(z) = g(q)$. Isso significa que existe $r > 0$ para o qual g não possui polos e zeros em $0 < |q| < r$. Logo, f não possui polos e zeros no conjunto $\{z : \mathrm{Im}(z) > (1/2\pi)\log(1/r)\}$. Como o subconjunto de $\overline{\mathcal{F}_1}$ dado por

$$\overline{\mathcal{F}_1}(r) = \{z \in \overline{\mathcal{F}_1} : \mathrm{Im}(z) \leqslant (1/2\pi)\log(1/r)\}$$

é compacto, a meromorficidade de f em $\mathfrak{H}$ garante que f possui apenas um número finito de polos e zeros em $\overline{\mathcal{F}_1}(r)$.

Em linhas gerais, a demonstração do Teorema consiste em integrar $1/2\pi i f$ no bordo $\partial\overline{\mathcal{F}_1}$. Para tanto, considere a curva $\mathcal{C}$ ilustrado na figura abaixo:

Figura 3 – A curva $\mathcal{C}$



Fonte: [2, p. 86]

A curva $\mathcal{C}$ é um contorno que contém em seu interior um representante de cada zero e polo de f que não está nas classes de equivalência $[i]$ e $[\omega]$ módulo Γ_1, e não passa por nenhum dos pontos singulares i, ω e $-\overline{\omega}$, que são os únicos no domínio fundamental $\overline{\mathcal{F}_1}$ com estabilizador não-trivial. O Teorema dos Resíduos nos dá:

$$\frac{1}{2\pi i}\int_{\mathcal{C}} \frac{df}{f} = \sum_{P \in \Gamma_1 \backslash \mathfrak{H}}^{*} \mathrm{ord}_P(f). \tag{3.3}$$

Por outro lado, podemos calcular separadamente a integral de $1/2\pi i f$ nos segmentos e arcos que formam a curva $\mathcal{C}$.

(i) Para o segmento EA, a mudança de variáveis $q = e^{2\pi iz}$ transforma a integral sobre EA na integral sobre um círculo centrado em $q = 0$ (com orientação negativa) que não passa nem contém no seu interior zeros e polos de g, exceto possivelmente por 0. Pelo Teorema de Cauchy,

$$\frac{1}{2\pi i}\int_E^A \frac{df}{f} = -\mathrm{ord}_\infty(f).$$

(ii) O elemento $T \in \Gamma_1$ leva o segmento AB no segmento ED'. Como f é uma função modular, temos f invariante por T, isto é, $f(Tz) = f(z)$, para todo $z \in \mathfrak{H}$. Logo,

$$\frac{1}{2\pi i}\int_A^B \frac{df}{f} + \frac{1}{2\pi i}\int_{D'}^E \frac{df}{f} = \frac{1}{2\pi i}\int_A^B \left(\frac{df(z)}{f(z)} - \frac{df(Tz)}{f(Tz)}\right) = 0.$$

(iii) O elemento $S \in \Gamma_1$ transforma o arco $B'C$ no arco DC'. Novamente, como f é uma função modular de peso k, f satisfaz a identidade $f(Sz) = z^k f(z)$, para todo $z \in \mathfrak{H}$. Temos,

$$\frac{df(Sz)}{f(Sz)} = k\frac{dz}{z} + \frac{df(z)}{f(z)}.$$

Logo,

$$\begin{aligned}\frac{1}{2\pi i}\int_{B'}^C \frac{df}{f} + \frac{1}{2\pi i}\int_{C'}^D \frac{df}{f} &= \frac{1}{2\pi i}\int_{B'}^C \left(\frac{df(z)}{f(z)} - \frac{df(Sz)}{f(Sz)}\right) \\ &= \frac{1}{2\pi i}\int_{B'}^C -k\frac{dz}{z} \longrightarrow -k\left(-\frac{1}{12}\right) = \frac{k}{12},\end{aligned}$$

quando o comprimento dos arcos BB', CC', DD' tende a 0.

(iv) Integrando $1/2\pi i f$ no círculo que contém o arco BB', orientado negativamente, obtemos $-\mathrm{ord}_\omega(f)$. Quando o raio deste círculo tende a zero, o ângulo entre B, B' tende a $2\pi/6$. Portanto,

$$\frac{1}{2\pi i}\int_{B'}^B \frac{df}{f} \longrightarrow -\frac{1}{6}\mathrm{ord}_\omega(f).$$

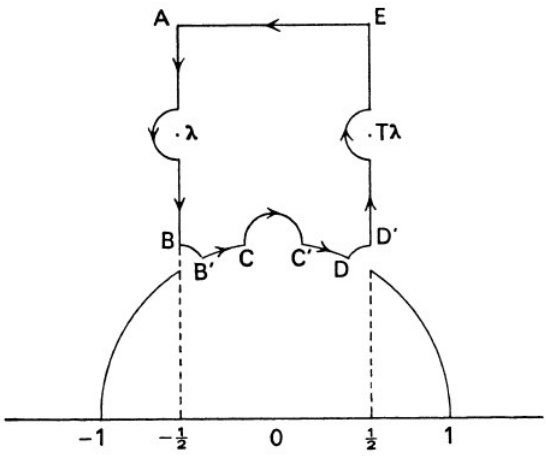
De modo análogo, quando tendemos o comprimento dos arcos CC' e DD' a zero, obtemos

$$\frac{1}{2\pi i}\int_C^{C'} \frac{df}{f} \longrightarrow -\frac{1}{2}\mathrm{ord}_i(f) \qquad \text{e} \qquad \frac{1}{2\pi i}\int_{D'}^D \frac{df}{f} \longrightarrow -\frac{1}{6}\mathrm{ord}_\omega(f).$$

Assim, basta igualar a expressão 3.3 com a integral separada em todos os segmentos que formam o contorno $\mathcal{C}$, e tomar o limite para obter a expressão 3.2.

No entanto, observamos que f pode possuir outros zeros e polos no bordo de $\overline{\mathcal{F}_1}$. Para estes casos, basta repetir a demonstração considerando um contorno muito similar à $\mathcal{C}$, mas realizando pequenos desvios nas vizinhanças dos zeros e polos de f. Por exemplo, suponha que f possua um zero ou polo λ na semi-reta $\{z : \mathrm{Re}(z) = -1/2, \mathrm{Im}(z) > \sqrt{3}/2\}$. Então, podemos considerar o contorno similar a $\mathcal{C}$, mas com um arco contornando λ e com o respectivo arco contornando $T\lambda$, que é a transformação do arco em λ por T:

Figura 4 – Uma variação da curva $\mathcal{C}$



Fonte: [2, p. 87]

□

Em geral, a principal aplicação da fórmula de valência é permitir o estudo dos zeros e polos de funções modulares aritmeticamente, conforme faremos no exemplo a seguir. Além disso, vamos utilizar a fórmula de valência para caracterizar explicitamente a dimensão dos espaços de formas modulares M_k.

Exemplo 2 (A Forma Cuspidal *Discriminante*). As séries de Eisenstein, conforme vimos, são exemplos de formas modulares de peso k. Uma particularidade dessas séries é a de que seu valor no infinito é dado por $2\zeta(k)$, e portanto, para $k > 1$, nunca se anula. Isso implica que nenhuma série de Eisenstein pode ser uma *forma cuspidal*, que são formas modulares cujo valor no infinito é zero. No entanto, vimos que o conjunto das formas modulares de peso k formam um $\mathbb{C}$-espaço vetorial e o que $\bigoplus_{k\in\mathbb{Z}} M_k$ é um anel graduado, de forma que soma, produto e combinações de formas modulares são, ainda, formas modulares. Sabendo disso, podemos construir um primeiro exemplo de forma cuspidal.

Considere as séries de Eisenstein normalizadas não-triviais de menores pesos, isto é, E_4 e E_6, de pesos 4 e 6, respectivamente. Em particular, E_4^3 e E_6^2 são formas modulares de peso 12 e ambas possuem coeficiente constante iguais a 1, pois os coeficientes contantes de E_4 e E_6 são 1. Considere:

$$\Delta = \frac{1}{1728}(E_4^3 - E_6^2). \tag{3.4}$$

Naturalmente, Δ é uma forma modular de peso 12, que possui coeficiente constante

$$\Delta(\infty) = \frac{1}{1728}(E_4^3(\infty) - E_6^2(\infty)) = \frac{1}{1728}1 - 1 = 0,$$

ou seja, é uma forma cuspidal de peso 12, denominada de *discriminante*. Note que Δ não possui polos, pois E_4 e E_6 são formas modulares, e portanto holomorfas em $\mathfrak{H}$. Vejamos

agora que Δ também não possui zeros em $\mathfrak{H}$. De fato, aplicando a fórmula de valência para E_4, vemos que a expressão

$$\mathrm{ord}_\infty(E_4) + \frac{1}{2}\mathrm{ord}_i(E_4) + \frac{1}{3}\mathrm{ord}_\omega(E_4) + \sum_{P\in\Gamma_1\backslash\mathfrak{H}}^{*} \mathrm{ord}_P(E_4) = \frac{4}{12} = \frac{1}{3}$$

é apenas satisfeita se $\mathrm{ord}_\omega(E_4) = 1$, e os restantes $\mathrm{ord}_z(E_4) = 0$, para todo $z \in \mathfrak{H}$ que não é congruente a ω módulo Γ_1, ou $z = \infty$. Isto mostra que, em $\mathfrak{H}$, E_4 se anula apenas em ω. Similarmente, aplicando a fórmula de valência para E_6, segue que a expressão

$$\mathrm{ord}_\infty(E_6) + \frac{1}{2}\mathrm{ord}_i(E_6) + \frac{1}{3}\mathrm{ord}_i(E_6) + \sum_{P\in\Gamma_1\backslash\mathfrak{H}}^{*} \mathrm{ord}_P(E_6) = \frac{6}{12} = \frac{1}{2}$$

é satisfeita apenas se $\mathrm{ord}_i(E_6) = 1$, e os restantes $\mathrm{ord}_z(E_6) = 0$, para todo $z \in \mathfrak{H}$ que não é congruente a i módulo Γ_1, ou $z = \infty$, isto é, E_6 se anula apenas em i, em $\mathfrak{H}$. Portanto, $\Delta = \dfrac{1}{1728}(E_4^3 - E_6^2)$ não se anula em nenhum ponto de $\mathfrak{H}$. Além disso, se aplicarmos a fórmula de valência para Δ, obtemos

$$\mathrm{ord}_\infty(\Delta) + \frac{1}{2}\mathrm{ord}_i(\Delta) + \frac{1}{3}\mathrm{ord}_i(\Delta) + \sum_{P\in\Gamma_1\backslash\mathfrak{H}}^{*} \mathrm{ord}_P(\Delta) = 1.$$

No entanto, sabemos que Δ não se anula em $\mathfrak{H}$, e portanto temos $\mathrm{ord}_z(\Delta) = 0$, para todo $z \neq \infty$, e $\mathrm{ord}_\infty(\Delta) = 1$, mostrando que Δ tem um zero simples no infinito.

Além disso, se considerarmos a q-expansão de Δ, dada por $\displaystyle\sum_{n=1}^{\infty} \tau(n)q^n$, temos que os coeficientes $\tau(n)$ são inteiros, para todo $n \in \mathbb{N}$. Para mostrar isto, como E_4 e E_6 possuem coeficientes inteiros, é suficiente verificarmos que $E_4^3 - E_6^2 \equiv 0 \mod 1728$, pela equação (3.4). De fato, como

$$E_4^3 = 1728\left[8000\left(\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3 + 100\left(\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^2\right] + 720\sum_{n=1}^{\infty}\sigma_3(n)q^n + 1,$$

$$E_6^2 = 1728\left(\sum_{n=1}^{\infty}\sigma_5(n)q^n\right)^2 - 1008\sum_{n=1}^{\infty}\sigma_5(n)q^n + 1,$$

e $1008 \equiv 720 \mod 1728$, segue que $E_4^3 - E_6^2 \equiv 720\displaystyle\sum_{n=1}^{\infty}(\sigma_3(n) - \sigma_5(n))q^n \mod 1728$. Usando o fato de que $d^3(d^2-1) \equiv 0 \mod 12$, para todo $d \in \mathbb{Z}$, e $12 \cdot 720 = 8640 \equiv 0 \mod 1728$, concluímos que

$$E_4^3 - E_6^2 \equiv 0 \mod 1728.$$

Teorema 4. *(a) $M_k = 0$ para $k < 0$ e $k = 2$.*

(b) M_k é espaço vetorial de dimensão 1 para $k = 0, 4, 6, 8, 10$, com base $1, E_4, E_6, E_8$ e E_{10}, respectivamente. Além disso, $S_k = 0$ para tais valores de k.

(c) A multiplicação por Δ induz isomorfismo $M_{k-12} \to S_k$.

Demonstração. Seja $f \in M_k$ não-nulo. Pela fórmula de valência (equação (3.2)), temos

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\omega(f) + \sum_{P \in \Gamma_1 \backslash \mathfrak{H}}^{*} \mathrm{ord}_P(f) = \frac{k}{12}. \tag{3.5}$$

Como f é uma forma modular, temos f holomorfa em $\mathfrak{H}$ e, portanto, não possui polos de nenhuma ordem. Logo, $\mathrm{ord}_z(f) \geqslant 0$, para todo $z \in \mathfrak{H}$, e $\mathrm{ord}_\infty(f) \geqslant 0$. Dessa forma, se $k < 0$, temos no lado esquerdo da igualdade (3.5) uma soma de números não-negativos, e do lado direito um número estritamente negativo, gerando uma contradição. Portanto, para $k < 0$, existe única forma modular de peso k e é a forma modular identicamente nula, de onde segue que $M_k = 0$, para todo $k < 0$. Similarmente, para o caso $k = 2$, basta analisar a fórmula de valência (3.5) para ver que não existem inteiros não-negativos n, n', n'' satisfazendo

$$n + \frac{1}{2}n' + \frac{1}{3}n'' = \frac{1}{6}$$

para o caso em que $f \in M_2$ seja não-nula. Portanto, temos outra contradição. De onde segue que $M_2 = 0$, finalizando a prova do item (a).

Conforme vimos no exemplo 2, Δ é sempre não-nula em $\mathfrak{H}$ e possui um zero simples no infinito. Se $f \in S_k$ e tomarmos $g = f/\Delta$, temos g de peso $k - 12$. Daí, a expressão

$$\mathrm{ord}_z(g) = \mathrm{ord}_z(f) - \mathrm{ord}_z(\Delta) = \begin{cases} \mathrm{ord}_z(f), \text{ se } z \neq \infty \\ \mathrm{ord}_z(f) - 1, \text{ se } z = \infty \end{cases}$$

mostra que $\mathrm{ord}_z(g) \geqslant 0$ para todo $z \in \mathfrak{H}$, ou seja, g não possui polos em $\mathfrak{H}$. Portanto, g é uma forma modular de peso $k - 12$, isto é, $g \in M_{k-12}$, o que prova (c).

Por fim, se $k = 0, 4, 6, 8, 10$, temos $k - 12 < 0$ e $S_k = 0$, por (a) e (c), mostrando que $dim(M_k) \leqslant 1$. Como $1, E_4, E_6, E_8$ e E_{10} são elementos não-nulos de M_0, M_4, M_6, M_8 e M_{10}, segue que $\dim(M_k) = 1$, para $k = 0, 4, 6, 8, 10$, provando (b). □

Corolário 2. *Seja $k \in \mathbb{Z}$. Então $\dim M_k = 0$ para $k < 0$ ou k ímpar, e para todo $k \geqslant 0$ par, temos*

$$\dim M_k = \begin{cases} [k/12], \text{ se } k \equiv 2 \bmod 12, k \geqslant 0 \\ [k/12] + 1, \text{ se } k \not\equiv 2 \bmod 12, k \geqslant 0 \end{cases} \tag{3.6}$$

onde $[k/12]$ denota a parte inteira de $k/12$.

Demonstração. Pelos itens (a) e (b) do Teorema 4, o resultado é imediato para $0 \leqslant k < 12$. Usando o isomorfismo entre M_{k-12} e S_k discutido no item (c) do mesmo teorema, podemos notar que a dimensão de M_k aumenta uma unidade quando trocamos k por $k + 12$, de onde segue a validade da fórmula para todo $k \geqslant 0$. □

Corolário 3. *A família* $\{E_4^\alpha E_6^\beta : \alpha, \beta \in \mathbb{Z}_{\geqslant 0}, 4\alpha + 6\beta = k\}$ *é uma base de* M_k.

Demonstração. Vejamos primeiramente que essa família gera M_k. Pelo Teorema 4, é imediato que os monômios $E_4^\alpha E_6^\beta$ geram M_k, para $k \leqslant 6$. Para $k \geqslant 8$, prosseguimos por indução. Escolha (γ, δ) par de inteiros positivos satisfazendo $4\gamma + 6\delta = k$ — essa escolha sempre pode ser feita para todo $k \geqslant 2$. Observe agora que a forma modular $g = E_4^\gamma E_6^\delta$ é não-nula no infinito. Se $f \in M_k$, existe $\lambda \in \mathbb{C}$ tal que $f - \lambda g$ é uma forma cuspidal (este fato segue da Proposição 6). Então, podemos considerar o isomorfismo entre M_{k-12} e S_k discutido no item (c) do Teorema 4 para ver que existe $h \in M_{k-12}$ tal que

$$f = \lambda g = \Delta \cdot h.$$

Assim, o resultado segue ao aplicar a hipótese indutiva em h.

Para ver que a família $\{E_4^\alpha E_6^\beta : \alpha, \beta \in \mathbb{Z}_{\geqslant 0}, 4\alpha + 6\beta = k\}$ é linearmente independente, basta observar que, caso não fosse, teríamos em particular que a função E_4^3/E_6^2 satisfaria alguma equação algébrica não trivial com coeficientes em $\mathbb{C}$, e portanto seria constante. Mas isso não pode ocorrer, visto que $E_4(\omega) = 0$ (pois já vimos que $\mathrm{ord}_\omega(G_6) = 1$), e E_6 não zera em ω. □

Observação 8. O Corolário 3 nos fornece a seguinte interpretação para o anel graduado $M = \bigoplus_{k \in \mathbb{Z}} M_k$. A aplicação

$$\begin{aligned} \varphi \colon \mathbb{C}[X, Y] &\to M \\ X &\mapsto E_4 \\ Y &\mapsto E_6 \end{aligned}$$

é um homomorfismo de $\mathbb{C}$-álgebras. O Corolário 3 nos garante que φ é na realidade um isomorfismo, mostrando que é possível identificar o espaço $M = \bigoplus_{k \in \mathbb{Z}} M_k$ com a álgebra de polinômios $\mathbb{C}[E_4, E_6]$.

Os principais resultados desta seção também possuem versões racionais, que serão úteis mais adiante. Defina os seguintes conjuntos:

$$\begin{aligned} M_{k,\mathbb{Q}} &:= \{\text{formas modulares de peso } k \text{ com coeficientes de Fourier racionais}\}, \\ S_{k,\mathbb{Q}} &:= \{\text{formas cuspidais de peso } k \text{ com coeficientes de Fourier racionais}\}. \end{aligned}$$

De forma análoga ao que foi feito no Lema 5, podemos ver que os conjuntos $M_{k,\mathbb{Q}}$ e $S_{k,\mathbb{Q}}$ possuem estrutura de $\mathbb{Q}$-espaço vetorial. Estamos particularmente interessados na versão racional do Corolário 3, que afirma que a família $\{E_4^\alpha E_6^\beta : \alpha, \beta \in \mathbb{Z}_{\geqslant 0}, 4\alpha + 6\beta = k\}$ é uma base para o $\mathbb{Q}$-espaço vetorial $M_{k,\mathbb{Q}}$, pois isto significa que, se $f \in M_{k,\mathbb{Q}}$ é uma forma modular de peso k com coeficientes de Fourier racionais, podemos representar f por um polinômio em E_4 e E_6 com coeficientes racionais. Enunciamos a seguir mais precisamente as versões racionais dos resultados dessa seção.

Proposição 7 (Versão racional da Proposição 6)**.** *Seja $k > 2$ um inteiro. Então,*

$$M_{k,\mathbb{Q}} = \mathbb{Q}.G_k \oplus S_{k,\mathbb{Q}}.$$

Teorema 5 (Versão racional do Teorema 4)**.** *(a) $M_{k,\mathbb{Q}} = 0$ para $k < 0$ e $k = 2$.*

(b) $M_{k,\mathbb{Q}}$ é um $\mathbb{Q}$-espaço vetorial de dimensão 1 para $k = 0, 4, 6, 8, 10$, com base $1, E_4, E_6, E_8$ e E_{10}, respectivamente. Além disso, $S_{k,\mathbb{Q}} = 0$ para tais valores de k.

(c) A multiplicação por Δ induz isomorfismo $M_{k-12,\mathbb{Q}} \to S_{k,\mathbb{Q}}$.

As demonstrações destes resultados são essencialmente análogas às demonstrações dos resultados originais, com as devidas observações de que as séries de Eisenstein G_k possuem coeficientes racionais, e de que $M_{k,\mathbb{Q}}, S_{k,\mathbb{Q}}$ são $\mathbb{Q}$-espaços vetoriais.

Corolário 4 (Versão racional do Corolário 3)**.** *A família $\{E_4^\alpha E_6^\beta : \alpha, \beta \in \mathbb{Z}_{\geqslant 0}, 4\alpha + 6\beta = k\}$ é uma $\mathbb{Q}$-base de $M_{k,\mathbb{Q}}$.*

Demonstração. Pelo Teorema 5, os monômios $E_4^\alpha E_6^\beta$ geram $M_{k,\mathbb{Q}}$ para valores de $k \leqslant 6$. Analogamente à demonstração do resultado original, prosseguimos por indução para os valores de $k \geqslant 8$. Escolhendo (γ, δ) um par de inteiros positivos satisfazendo $4\gamma + 6\delta = k$, temos que a forma modular $g = E_4^\gamma E_6^\delta$ possui coeficientes racionais e é não-nula no infinito. Tomando $f \in M_{k,\mathbb{Q}}$, segue pela Proposição 7 que existe $\lambda \in \mathbb{Q}$ tal que $f - \lambda g \in S_{k,\mathbb{Q}}$. Então, podemos considerar o isomorfismo entre $M_{k-12,\mathbb{Q}}$ e $S_{k,\mathbb{Q}}$ garantido pelo Teorema 5 para obter $h \in M_{k-12,\mathbb{Q}}$ tal que $f = \lambda g = \Delta \cdot h$, e o resultado segue ao aplicar a hipótese indutiva em h. Para ver que a família $\{E_4^\alpha E_6^\beta : \alpha, \beta \in \mathbb{Z}_{\geqslant 0}, 4\alpha + 6\beta = k\}$ é linearmente independente sobre $\mathbb{Q}$, basta observar que, caso não fosse, teríamos em particular que a função E_4^3/E_6^2 satisfaria alguma equação algébrica não trivial com coeficientes em $\mathbb{Q}$, e portanto seria constante. Mas isso não pode ocorrer, visto que $E_4(\omega) = 0$ e E_6 não zera em ω. □

3.1 Aplicação: Expansão da Forma Cuspidal Discriminante Δ e Função τ de Ramanujan

Os resultados desenvolvidos neste capítulo nos permitem trabalhar de forma mais concreta com as formas modulares, visto que já obtivemos uma caracterização explícita para uma forma modular como combinação de séries de Eisenstein e formas cuspidais, bem como compreendemos mais profundamente a aritmética da dimensionalidade dos espaços envolvidos.

Uma aplicação destes resultados é obter a q-expansão da forma cuspidal discriminante Δ — o chamado *Teorema de Jacobi*. Nesse contexto, nos depararemos naturalmente

com uma função que descreve certas propriedades dos coeficientes da expansão de Δ: a *função τ de Ramanujan*. Nesta seção, vamos então provar o Teorema de Jacobi e estudar propriedades da função τ.

Recordemos do Exemplo 2 que a forma cuspidal Δ é dada por:

$$\Delta = \frac{1}{1728}(E_4^3 - E_6^3).$$

Utilizando as $q-$ expansões das séries de Eisenstein normalizadas dadas na Tabela 1, a saber,

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \quad \text{e} \quad E_6(z) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n,$$

podemos desenvolver os primeiros termos destas séries, obtendo

$$\Delta(z) = q - 24q^2 + 252q^3 - 1472q^4 + \dots$$

O Teorema de Jacobi fornece uma expressão para a q-expansão de Δ como um produto infinito.

Teorema 6 (Jacobi)**.** *Se $q = e^{2\pi iz}$, com $z \in \mathfrak{H}$, então*

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} \tag{3.7}$$

Demonstração. Defina $F(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$. Queremos mostrar que F e Δ são proporcionais. Para isto, é suficiente mostrar que F é uma forma cuspidal de peso 12, pois, por um lado, temos do Corolário 2 que dim $S_{12} = 1$, e por outro lado, sabemos que Δ é uma forma cuspidal de peso 12. Com efeito, mostemos que, para todo $z \in \mathfrak{H}$, valem as relações:

(i) $F(z+1) = F(z)$,

(ii) $F(-1/z) = z^{12}F(z)$.

A relação (i) segue imediatamente do fato que $q = e^{2\pi iz}$ é invariante por $z \mapsto z+1$. Para verificar a relação (ii), vamos provar que as funções $F(-1/z)$ e $z^{12}F(z)$ possuem a mesma diferencial logarítmica. Assim, existirá constante k tal que $F(-1/z) = kz^{12}F(z)$, para todo $z \in \mathfrak{H}$. Para $z = i$, temos $z^{12} = 1, -1/z = z$ e $F(z) \neq 0$, mostrando que $k = 1$. Portanto, a relação $F(-1/z) = z^{12}F(z)$ segue. Tomando a derivada logarítmica de F, segue que

$$\frac{dF}{F} = \frac{dq}{q}\left(1 - 24\sum_{n,m=1}^{\infty}nq^{nm}\right) = \frac{dq}{q}\left(1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n\right) = \frac{dq}{q}E_2(z).$$

Como $G_2(z) = 2\zeta(2)E_2(z) = \dfrac{\pi^2}{6}E_2(z)$, obtemos

$$\frac{dF}{F} = \frac{6i}{\pi}G_2(z)dz.$$

Agora, pelo Lema 4, sabemos que

$$G_2\left(-1/z\right) = z^2 G_2(z) - 2\pi i z.$$

Então, aplicando as duas últimas expressões em $-1/z$,

$$\frac{dF(-1/z)}{F(-1/z)} = \frac{6i}{\pi} G_2(-1/z)\frac{dz}{z^2} = \frac{6i}{\pi}\frac{dz}{z^2}(z^2 G_2(z) - 2\pi i z) = \frac{dF(z)}{F(z)} + 12\frac{dz}{z}.$$

Portanto, as funções $F(-1/z)$ e $z^{12}F(z)$ possuem a mesma diferencial logarítmica, como queríamos. □

Denote por $\tau(n)$ o n-ésimo coeficiente da forma cuspidal Δ. A função $n \mapsto \tau(n)$ é chamada de *função τ de Ramanujan*. Ramanujan calculou os primeiros 30 coeficientes $\tau(n)$ e observou que eles satisfaziam certas propriedades multiplicativas, por exemplo:

$$\tau(2)\tau(3) = -24 \cdot 252 = -6048 = \tau(6) = \tau(2 \cdot 3),$$
$$\tau(2)\tau(5) = -24 \cdot 4830 = -115920 = \tau(10) = \tau(2 \cdot 5).$$

Mais ainda, em 1916 conjecturou as seguintes propriedades da função τ:

1. $\tau(n) \cdot \tau(m) = \tau(mn)$, sempre que m e n são coprimos.
2. $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$, para todo p primo e $r > 0$.
3. $|\tau(p)| \leqslant 2p^{11/2}$, para todo p primo.

As propriedades 1. e 2. foram provadas por *Louis Mordell em 1917* e a propriedade 3. foi provada por *Pierre Deligne* em 1974.

Essas propriedades são úteis para calcular alguns valores $\tau(n)$, especialmente se n é primo. Mais especificamente, podemos calcular valores de $\tau(n)$ congruentes módulo m, para alguns valores de m inteiro. Sabemos que existem congruências para $\tau(n)$ módulo $2^{11}, 3^7, 5^3, 7, 23$ e 691 - mais informações sobre essas congruências e propriedades gerais da função τ podem ser encontradas em [9]. Faremos neste trabalho o caso da congruência módulo 691 no seguinte teorema.

Teorema 7. *Para todo primo p, $\tau(p) \equiv 1 + p^{11} \mod 691$.*

Demonstração. Considere as séries de Eisenstein normalizadas de pesos 6 e 12 (Tabela 1):

$$E_6(q) = 1 - 605\sum_{n=1}^{\infty}\sigma_5(n)q^n,$$
$$E_{12}(q) = 1 + \frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n,$$

onde $\sigma_r(n) = \sum_{d|n} d^r$. Segue do Teorema 4 que $M_{12} = \mathbb{C}E_{12} \oplus \mathbb{C}\Delta$. Então E_6^2 é combinação linear de E_{12} e Δ, digamos

$$E_6^2 = \lambda E_{12} + \mu\Delta, \qquad \text{para } \lambda, \mu \in \mathbb{C}.$$

Considere os funcionais lineares $a_n : M_{12} \to \mathbb{C}$ que associam uma forma modular em M_{12} ao n-ésimo coeficiente de sua q-expansão. Então, aplicando o funcional linear a_0, obtemos

$$a_0(E_6^2) = \lambda a_0(E_{12}) + \mu a_0(\Delta).$$

Como E_6 e E_{12} são séries de Eisenstein normalizadas, temos $a_0(E_6) = a_0(E_{12}) = 1$. Além disso, $a_0(\Delta) = 0$, pois Δ é uma forma cuspidal. Logo, $\lambda = 1$. Similarmente, aplicando o funcional linear a_1, obtemos:

$$a_1(E_6^2) = a_1(E_{12}) + \mu a_1(\Delta).$$

Como sabemos, $a_1(\Delta) = 1$. Resta então calcularmos os primeiros coeficientes de E_6^2 e E_{12}. Utilizando as q-expansões dadas no início da resolução, temos:

$$E_6(q) = 1 - 605 \sum_{n=1}^{\infty} \sigma_5(n) q^n = 1 - 504q + \ldots \implies E_6^2(q) = 1 - 2 \cdot 504 + \ldots$$
$$E_{12}(q) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n = 1 + \frac{65520}{691} + \ldots$$

Logo, $a_1(E_6^2) = -2 \cdot 504 = -1008$ e $a_1(E_{12}) = 65520/691$. Portanto,

$$-1008 = \frac{65520}{691} + \mu \implies \mu = -1008 - \frac{65520}{691} = -\frac{762048}{691}.$$

Dessa forma, obtemos a combinação linear desejada:

$$E_6^2 = E_{12} - \frac{762048}{691}\Delta,$$

onde $762048 \equiv 65520 \mod 691$. Multiplicando a expressão acima por 691, segue que

$$0 \equiv \left(65520 \sum_{n=1}^{\infty} \sigma_{11}(n) q^n - \sum_{n=1}^{\infty} \tau(n) q^n \right) \mod 691.$$

Mas isso implica que $\tau(n) \equiv \sigma_{11}(n) \bmod 691$. Como $n = p$ é primo, então $\sigma_{11}(p) = \sum_{d|p} d^{11} = 1^{11} + p^{11} = 1 + p^{11}$. Portanto, $\tau(n) \equiv 1 + p^{11} \bmod 691$. □

Parte II

O Invariante Modular j

4 O Invariante Modular j

No Capítulo 3, estudamos as principais propriedades do espaço M_k das formas modulares de peso k no que concerne à sua estrutura e dimensão. Em particular, o Teorema 4 nos mostra que o espaço das formas modulares de peso 0 é unidimensional. Juntando isto ao fato de que toda função constante é uma forma modular de peso 0, temos que $M_0 = \mathbb{C}$, ou seja: não podemos encontrar exemplos interessantes (não-constantes) de formas modulares de peso 0. No entanto, podemos encontrar *funções modulares* de peso 0, isto é, funções fracamente modulares de peso 0 que são meromorfas no infinito. Encontrar um tal exemplo é relevante, pois funções modulares de peso 0 são Γ_1-invariantes.

Uma maneira natural de obter uma função modular de peso 0 seria considerar o quociente de duas funções modulares de mesmo peso. No entanto, não podemos considerar quaisquer duas funções modulares de peso k em M_k. Por exemplo, caso M_k seja unidimensional, o quociente de quaisquer $f, g \in M_k$ não-nulas seria constante, o que não fornece um exemplo não-trivial. Para contornar esse problema, basta considerarmos o primeiro espaço M_k com dimensão maior do que 1, já que o Teorema 4 garante que existe pelo menos uma série de Eisenstein e uma forma cuspidal neste espaço, de modo que o quociente de tais funções seria um exemplo de função modular não constante de peso 0. O primeiro espaço M_k de dimensão maior que 1 é o espaço M_{12}, e o *invariante modular* j aparece neste contexto.

4.1 Definições Básicas

Definição 9. O *Invariante Modular* j é a função em $\mathfrak{H}$ definida por:

$$j = \frac{E_4^3}{\Delta} = 1728 \cdot \frac{E_4^3}{E_4^3 - E_6^2} \tag{4.1}$$

Conforme já comentado, a propriedade fundamental da função j é ser Γ_1-invariante, haja vista que é uma função modular de peso 0 como quociente de duas formas modulares de peso 12. Utilizando propriedades já discutidas das formas modulares E_4^3 e Δ podemos provar as seguintes propriedades da função j.

Proposição 8. *(a) A função j é holomorfa em $\mathfrak{H}$ e possui um polo simples no infinito.*

(b) A função j induz uma bijeção $\Gamma_1\backslash\mathfrak{H} \to \mathbb{C}$.

Demonstração. (a) Como E_4^3 é uma forma modular (portanto holomorfa em $\mathfrak{H}$), e vimos no Exemplo 2 que Δ é uma forma cuspidal que não se anula em nenhum ponto de $\mathfrak{H}$,

segue que j é holomorfa em $\mathfrak{H}$. Uma vez que Δ possui um zero simples no infinito (Exemplo 2) e $E_4(\infty) \neq 0$, concluímos que j possui polo simples no infinito.

(b) É suficiente mostrar que, no domínio fundamental, j alcança todo valor em $\mathbb{C}$ uma única vez, ou, equivalentemente, mostrar que, dado $\lambda \in \mathbb{C}$, a forma modular $f_\lambda = E_4^3 - \lambda\Delta$ possui um único zero módulo Γ_1. Analisando a fórmula de valência para f_λ em $k = 12$, vemos que

$$\mathrm{ord}_\infty(f_\lambda) + \frac{1}{2}\mathrm{ord}_i(f_\lambda) + \frac{1}{3}\mathrm{ord}_\omega(f_\lambda) + \sum_{P\in\Gamma_1\backslash\mathfrak{H}}^{*} \mathrm{ord}_P(f_\lambda) = 1.$$

Como $E_4(\infty) \neq 0$ e Δ possui zero simples no infinito, segue que o $\mathrm{ord}_\infty(f_\lambda) = 0$. Logo, basta analisarmos para quais triplas (n, n', n'') de números inteiros não-negativos temos a equação

$$\frac{1}{2}\mathrm{ord}_i(f_\lambda) + \frac{1}{3}\mathrm{ord}_\omega(f_\lambda) + \sum_{P\in\Gamma_1\backslash\mathfrak{H}}^{*} \mathrm{ord}_P(f_\lambda) = \frac{1}{2}n + \frac{1}{3}n' + n'' = 1$$

satisfeita. Podemos concluir que essas triplas são $(0, 0, 1), (2, 0, 0)$ ou $(0, 3, 0)$. Em todo caso, f_λ possui zero em apenas um ponto de $\Gamma_1\backslash\mathfrak{H}$.

□

Proposição 9. *Seja f meromorfa em $\mathfrak{H}$. As seguintes afirmações são equivalentes:*

(i) f é uma função modular de peso 0.

(ii) f é quociente de duas formas modulares de mesmo peso.

(iii) f é uma função racional de j.

Demonstração. A implicação $(ii) \implies (i)$ é imediata. Para a implicação $(iii) \implies (ii)$, suponha

$$f = \frac{P(j)}{Q(j)},$$

onde P, Q são polinômios complexos. Então, $P(j)$ e $Q(j)$ são ambas funções modulares de peso 0 e holomorfas em $\mathfrak{H}$. Note que $P(j)$ e $Q(j)$ podem possuir, no máximo, um polo no infinito, que podem ser controlados multiplicando por alguma potência de Δ, isto é, existe k tal que $\Delta^k P(j)$ e $\Delta^k Q(j)$ são holomorfas no infinito. Logo,

$$f = \frac{P(j)\Delta^k}{Q(j)\Delta^k}$$

é quociente de formas modulares de mesmo peso. Para provar $(i) \implies (iii)$, suponha f função modular de peso 0 e considere

$$g(z) = f(z) \prod_{P\in\Gamma_1\backslash\mathfrak{H}, \mathrm{ord}_P(f)<0} (j(z) - j(P))^{-\mathrm{ord}_P(f)}, \tag{4.2}$$

que cancela todos os polos de f em $\mathfrak{H}$. Evidentemente, g é uma função modular de peso 0 e meromorfa no infinito, e portanto existe um inteiro $k > 0$ para o qual $g\Delta^k$ é uma forma modular de peso $12k$. O Corolário 3 garante que podemos escrever

$$g(z)\Delta^k(z) = \sum_{4\alpha+6\beta=12k} c_{\alpha\beta} E_4^\alpha(z) E_6^\beta(z),$$

onde os coeficientes $c_{\alpha\beta}$ são complexos. Como estamos percorrendo as combinações lineares sobre os índices α e β satisfazendo $4\alpha + 6\beta = 12k$, segue que $12 \mid 4\alpha + 6\beta$ e, em particular, $3 \mid \alpha$ e $2 \mid \beta$. Portanto, a expressão

$$\begin{aligned} g(z) &= \sum_{4\alpha+6\beta=12k} c_{\alpha\beta} \left(\frac{E_4^3(z)}{\Delta(z)}\right)^{\frac{\alpha}{3}} \left(\frac{E_6^2(z)}{\Delta(z)}\right)^{\frac{\beta}{2}} = \sum_{4\alpha+6\beta=12k} c_{\alpha\beta} \left(j(z)\right)^{\frac{\alpha}{3}} \left(j(z) - 1728\right)^{\frac{\beta}{2}} \\ &= \sum_{4\alpha+6\beta=12k} c_{\alpha\beta} \left(j(z)\right)^{\frac{\alpha}{3}} \left(j(z) - j(i)\right)^{\frac{\beta}{2}} \end{aligned}$$

mostra que g é um polinômio em j. Logo, f é uma função racional em j. □

Observação 9. A demonstração da Proposição 9 mostra que se f é uma função modular de peso 0 holomorfa em $\mathfrak{H}$, então f é na verdade um polinômio em j. De fato, neste caso, temos que f não possui polos em $\mathfrak{H}$, ou seja, não existem pontos $P \in \Gamma_1\backslash\mathfrak{H}$ com $\mathrm{ord}_P(f) < 0$, e portanto a equação (4.2) garante que $f = g$. Além disso, se f possui coeficientes de Fourier racionais, então f é um polinômio em j com coeficientes racionais. De fato, pelo item anterior, $f = g$ e a expressão

$$f(z)\Delta^k(z) = \sum_{4\alpha+6\beta=12k} c_{\alpha\beta} E_4^\alpha(z) E_6^\beta(z),$$

garante que $f\Delta^k$ é uma forma modular com coeficientes de Fourier em $\mathbb{Q}$, pois Δ possui coeficientes em $\mathbb{Z}$. Logo, $f\Delta^k \in M_{12k,\mathbb{Q}}$ e, pelo Corolário 4, temos que $f\Delta^k \in \mathbb{Q}[E_4, E_6]$, mostrando que os coeficientes $c_{\alpha\beta}$ são racionais, para todo α, β satisfazendo $4\alpha + 6\beta = 12k$. Logo, segue que da expressão

$$f(z) = \sum_{4\alpha+6\beta=12k} c_{\alpha\beta} \left(j(z)\right)^{\frac{\alpha}{3}} \left(j(z) - j(i)\right)^{\frac{\beta}{2}}$$

que os coeficientes de f como um polinômio em j são racionais.

Observação 10. No espírito da observação anterior, temos um resultado ainda mais preciso, que será útil mais adiante: Se f é uma função holomorfa em $\mathfrak{H}$ e modular de peso 0 com coeficientes de Fourier inteiros, então os coeficientes de f como um polinômio em j são inteiros. De fato, seja $Q(Y) \in \mathbb{C}[Y]$ e $f(z) = Q(j(z))$. Sendo f uma função modular de peso 0, f admite expansão de Fourier

$$f(z) = \sum a_n q^n \in \mathbb{C}[[q]][q^{-1}].$$

Escrevendo $Q(Y) = \sum_{i=0}^{d} Q_i Y^i$, com $Q_i \in \mathbb{C}$, $Q_d \neq 0$, temos:

$$f(z) = Q(j(z)) = \sum_{i=0}^{d} Q_i Y^i = \sum_{i=0}^{d} Q_i \left(\frac{1}{q} + 744 + 196844q + \cdots \right) = \sum_{i=0}^{d} Q_i \left(\frac{1}{q^i} + \frac{744i}{q^{i-1}} + \cdots \right)$$
$$= \frac{Q_q}{q^d} + \frac{Q_{d-1} + 744dQ_d}{q^{d-1}} + \cdots = \sum a_n q^n$$

Logo, $a_n = 0$ se $n < -d$ e $a_{-d} = Q_d$. Agora, basta considerar

$$Q(Y) - Q_d Y^d = \sum_{i=0}^{d-1} Q_i Y^i$$

e aplicar indução no grau, pois

$$Q(j(z)) - Q_d j(z)^d = f(z) - Q_d j(z)^d \in \mathbb{Z}[[q]][q^{-1}].$$

Observação 11. Na expressão $j = 1728 \cdot \dfrac{E_4^3}{E_4^3 - E_6^2}$ temos o coeficiente $1728 = 2^6 3^3$. Ele foi introduzido de modo a garantir que j possua resíduo igual a 1 no infinito. Mais precisamente, utilizando a q-expansão dada na seção 2.2.1 podemos obter

$$j(z) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n) q^n, \qquad z \in \mathfrak{H} \text{ e } q = e^{2\pi i z},$$

onde os coeficientes $c(n)$ são inteiros, por exemplo:

$$c(1) = 2^2 \cdot 3^3 \cdot 1823 = 196884 \text{ e } c(2) = 2^{11} \cdot 5 \cdot 2099 = 21493760.$$

De fato, vimos no Exemplo 2 que os coeficientes $\tau(n)$ da q-expansão de Δ são inteiros e $\tau(1) = 1$. Isso significa que os coeficientes da q-expansão de $1/\Delta$ são inteiros, e, portanto, a q-expansão de $j = E_4^3/\Delta$ terá coeficientes inteiros, tendo em vista que os coeficientes de E_4^3 também são inteiros.

4.2 Multiplicação Complexa

Uma *curva elíptica* é representada pelo quociente $E = \mathbb{C}/\Lambda$, onde Λ é um reticulado em $\mathbb{C}$. Se $E' = \mathbb{C}/\Lambda'$ é outra curva elíptica com $\lambda\Lambda \subseteq \Lambda'$ para algum $\lambda \in \mathbb{C}$, fica bem definido um endomorfismo

$$\begin{aligned} E &\to E' \\ [z] &\mapsto [\lambda z]. \end{aligned} \tag{4.3}$$

Uma vez que um reticulado é um $\mathbb{Z}$-módulo, se temos $\Lambda = \Lambda'$, então sempre podemos obter este mapa para $\lambda \in \mathbb{Z}$ (este é o único caso para λ real). No entanto, é possível que λ seja um número complexo.

Definição 10. Dizemos que uma curva elíptica $E = \mathbb{C}/\Lambda$ admite *multiplicação complexa* se existe $\lambda \in \mathbb{C}\backslash\mathbb{R}$ tal que $\lambda\Lambda \subseteq \Lambda$.

Cada $z \in \mathfrak{H}$ pode ser associado à uma curva elíptica da forma:

$$E = \frac{\mathbb{C}}{\Lambda_z}, \qquad \text{onde } \Lambda_z := \mathbb{Z}z + \mathbb{Z}. \tag{4.4}$$

Os pontos $z \in \mathfrak{H}$ tais que a curva elíptica $E = \mathbb{C}/\Lambda_z$ admite multiplicação complexa são chamados de *pontos CM*(*Complex Multiplication*, em inglês). A Proposição a seguir apresenta suas principais propriedades e equivalências.

Proposição 10. *Seja $z \in \mathfrak{H}$. As seguintes afirmações são equivalentes:*

(i) z é um ponto CM.

(ii) Existem inteiros a, b, c, com $a \neq 0$, tais que $az^2 + bz + c = 0$, ou, equivalentemente, $z = (-b + \sqrt{D})/2a$, com $D = b^2 - 4ac$.

(iii) Existe um inteiro positivo n e uma matriz $M \in M(2, \mathbb{Z})$ não proporcional à identidade e com determinante n que fixa z.

Demonstração. Vejamos que (i) $\iff$ (ii). Supondo $z \in \mathfrak{H}$ um ponto CM, existe $\lambda \in \mathbb{C}\backslash\mathbb{R}$ tal que $\lambda(\mathbb{Z}z+\mathbb{Z}) \subseteq \mathbb{Z}z+\mathbb{Z}$. Em particular, existem inteiros A, B, C, D tais que $\lambda = Az+B$ e $\lambda z = Cz + D$. Evidentemente, $A \neq 0$, pois $\lambda \in \mathbb{C}\backslash\mathbb{R}$. Como $\lambda \neq 0$,

$$z = \frac{Cz + D}{Az + B},$$

de onde segue que $Az^2 + (B - C)z - D = 0$. Tomando $A = a \neq 0$, $b = B - C$ e $d = -D$, concluímos. Reciprocamente, se z satisfaz $az^2 + bz + c = 0$, para inteiros a, b, c com $a \neq 0$, tomando $\lambda = az$, segue que

$$\lambda(\mathbb{Z}z + \mathbb{Z}) = \mathbb{Z}(a - b)z + \mathbb{Z}c \subseteq \mathbb{Z}z + \mathbb{Z}.$$

Logo, z é ponto CM.

Para (ii) $\iff$ (iii), suponha $az^2 + bz + c = 0$, para inteiros a, b, c com $a \neq 0$. Então, tomando $n = ac$ — o qual é positivo pois sabemos que $z \in \mathfrak{H}$ implica $D = b^2 - 4ac < 0$, temos:

$$z = \frac{bz + c}{-az + 0} = \begin{pmatrix} b & c \\ -a & 0 \end{pmatrix} z = Mz.$$

Evidentemente, $M \in M(2, \mathbb{Z})$ não é proporcional à identidade, pois $a \neq 0$ e fixa z, pela expressão acima. Além disso, $\det M = ac = n$, concluíndo a implicação. Reciprocamente,

suponha que exista um inteiro positivo n e uma matriz $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in M(2,\mathbb{Z})$ não proporcional à identidade e com determinante n que fixa z. Então,

$$Mz = z \implies \frac{Az+B}{Cz+D} = z \implies Az + B = Cz^2 + Dz \implies Cz^2 + (D-A)z - B = 0.$$

Tomando $a = C \neq 0$ (pois M não é proporcional à identidade), $b = D - A$ e $c = -B$, segue o resultado. □

A teoria de multiplicação complexa é muito vasta e entrelaça conceitos de teoria algébrica dos números, curvas elípticas e formas modulares. Nesta seção, mencionamos brevemente apenas os seus principais aspectos básicos. Essencialmente, vimos a definição de multiplicação complexa no contexto de curvas elípticas e deduzimos pontos com um comportamento especial: os pontos quadrático imaginários no semiplano superior, chamados de pontos CM. Esses pontos são de especial interesse, pois provaremos neste capítulo que $j(\mathfrak{z})$ é um número algébrico — na realidade, é um inteiro algébrico — sempre que $\mathfrak{z}$ é um ponto CM. No entanto, para que possamos abordar esse resultado, serão necessários alguns conceitos e resultados envolvolvendo matrizes de um dado determinante e subgrupos de congruência de Γ_1, temas das próximas duas seções.

4.3 Matrizes Inteiras de um Dado Determinante

Considere m um inteiro positivo não nulo e denote por $\mathcal{M}_m$ o subconjunto de $M(2,\mathbb{Z})$ de matrizes 2×2 com entradas inteiras e determinante m. Note que o grupo Γ_1 age em $\mathcal{M}_m$ via multiplicação de matrizes à direita e à esquerda.

Proposição 11. *O conjunto finito*

$$\mathcal{M}_m^* = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z}, ad = m \ e \ 0 \leqslant b < d \right\} \subseteq \mathcal{M}_m$$

é um sistema completo de representantes para o quociente à esquerda $\Gamma_1 \backslash \mathcal{M}_m = \{[M] : M \in \mathcal{M}_m\}$.

Demonstração. Seja $[M] \in \Gamma_1 \backslash \mathcal{M}_m$ e mostremos que existe único $M' \in \mathcal{M}_m^*$ e $\gamma \in \Gamma_1$ tais que $M = \gamma M'$. Digamos que $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, com $\det M = AD - BC = m$, e considere $g = \mathrm{mdc}(A, C)$. A Identidade de Bézout nos garante a existência de $u_0, v_0 \in \mathbb{Z}$ satisfazendo $u_0 A + v_0 C = g$. Denotando $b_0 = u_0 B + v_0 D$, vamos provar primeiramente a seguinte afirmação: existem $u, v \in \mathbb{Z}$, com $uA + vC = g$, tais que $b = uB + vD$ satisfaz $0 \leqslant b < \dfrac{\det M}{g}$. De fato, verificamos imediatamente que

$$(u, v) = (u_0, v_0) + k\left(\frac{-C}{g}, \frac{A}{g}\right), \qquad k \in \mathbb{Z}$$

são soluções de $xA + yC = g$:

$$uA+vC = \left(u_0 - k\frac{C}{g}\right)A+\left(V_0 + k\frac{A}{g}\right)C = u_0A+v_0C+\frac{k}{g}(AC-AC) = u_0A+v_0C = g.$$

Além disso,

$$\begin{aligned} b = uB + vD &= \left(u_0 - k\frac{C}{g}\right)B + \left(V_0 + k\frac{A}{g}\right)D = u_0B + v_0D + k\frac{(AD-BC)}{g} \\ &= b_0 + k\left(\frac{\det M}{g}\right) \end{aligned}$$

pode sempre ser escolhido de forma a satisfazer $0 \leqslant b < \det M/g$, e cada escolha é única módulo $\det M/g$, provando a afirmação.

Escolhendo $u, v \in \mathbb{Z}$ tais que $uA + vC = g$ e $b = uB + vD$ satisfazendo $0 \leqslant b < \det M/g$, defina:

$$\gamma = \begin{pmatrix} \frac{A}{g} & -v \\ \frac{C}{g} & u \end{pmatrix} \text{ e } M' = \begin{pmatrix} g & b \\ 0 & \frac{\det M}{g} \end{pmatrix}.$$

Note primeiramente que $\gamma \in \Gamma_1$: de fato, como $g = \text{mdc}(A, C) \mid A, C$, temos que A/g e C/g são números inteiros, de modo que $\gamma \in M(2, \mathbb{Z})$. Uma vez que $\det\gamma = (uA + vC)/g = g/g = 1$, segue que $\gamma \in \Gamma_1$. Além disso, $M' \in \mathcal{M}_m^*$: similarmente, como $g = \text{mdc}(A, C) \mid A, C$, temos que g divide qualquer combinação inteira de A e C. Em particular, $g \mid AD - BC = \det M$, de onde obtemos que $\det M/g \in \mathbb{Z}$ e portanto que $M' \in M(2, \mathbb{Z})$. Como $\det M' = \det M = m$, e a escolha de b (única módulo $\det M/g$) foi foita de modo a satisfazer $0 \leqslant b < \det M/g$, segue que M' é um elemento de $\mathcal{M}_m^*$. Por fim, basta mostrarmos a relação $M = \gamma M'$:

$$\begin{aligned} \gamma M' &= \begin{pmatrix} \frac{A}{g} & -v \\ \frac{C}{g} & u \end{pmatrix}\begin{pmatrix} g & b \\ 0 & \frac{\det M}{g} \end{pmatrix} = \begin{pmatrix} A & \frac{A(uB+vD)-v(AD-BC)}{g} \\ C & \frac{C(uB+vD)+u(AD-BC)}{g} \end{pmatrix} \\ &= \begin{pmatrix} A & \frac{Bg}{g} \\ C & \frac{Dg}{g} \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = M. \end{aligned}$$

□

Lema 8. *Seja $M = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in M_m^*$. A q-expansão de $j(Mz)$ é dada por*

$$j(Mz) = \sum_{n=-1}^{\infty} c_n \zeta_d^{bn} q^{\frac{an}{d}}, \tag{4.5}$$

em que $\zeta_d = e^{\frac{2\pi i}{d}}$ e os coeficientes c_n são os coeficientes da q-expansão de $j(z)$. Além disso, $j(Mz)$ é uma função holomorfa em $\mathfrak{H}$ e meromorfa no infinito.

Demonstração. Para obter a q-expansão de $j(Mz)$, basta substituir z por Mz na q-expansão de j:

$$j(Mz) = j\left(\frac{az+b}{d}\right) = \frac{1}{e^{2\pi i\frac{b}{d}}}\frac{1}{q^{\frac{a}{d}}} + c_0 + c_1 e^{2\pi i\frac{b}{d}} q^{\frac{a}{d}} + \ldots = \sum_{n=-1}^{\infty} c_n \zeta_d^{bn} q^{\frac{an}{d}}. \tag{4.6}$$

Além disso, $j(Mz)$ é holomorfa em $\mathfrak{H}$ como a composição das aplicações $z \mapsto Mz$ e $j(z)$, que são holomorfas em $\mathfrak{H}$ — pois $\det M = m > 0$. Por fim, escolha $n_i \in \mathbb{Z}$ tal que $n_i - a > 0$ e considere

$$q^{\frac{n_i}{d}} j(Mz) = \sum_{n=-1}^{\infty} c_n \zeta_d^{bn} q^{\frac{n_i + an}{d}}.$$

Como $\dfrac{n_i - a}{d} > 0$ e $\dfrac{n_i + an}{d} > 0$, para todo $n \geqslant 1$ inteiro, segue da expressão acima que $q^{\frac{n_i}{d}} j(Mz) \longrightarrow 0$, quando $z \longrightarrow +i\infty$, mostrando que $j(Mz)$ é meromorfa no infinito. (menos formalmente, poderíamos ter observado simplesmente que a parte negativa da expansão de $j(Mz)$ é finita). □

4.4 Subgrupos de Congruência de Γ_1

Dado $N \in \mathbb{N}$, o subgrupo $\Gamma_N := \{\gamma \in \Gamma_1 : \gamma \equiv 1 \mod N\}$ de Γ_1 é chamado de *subgrupo de congruência principal de nível N*.

Definição 11. Um subgrupo Γ' de Γ_1 é dito *subgrupo de congruência* de Γ_1 se Γ' contém algum subgrupo de congruência principal de nível N, para algum $N \in \mathbb{N}$.

Lema 9. *Todo subgrupo de congruência de Γ_1 possui índice finito.*

Demonstração. Seja Γ' subgrupo de congruência de Γ_1. Então, existe $N \in \mathbb{Z}$ para o qual $\Gamma_N \subseteq \Gamma'$. Considerando o homomorfismo de grupos $\varphi_N : \Gamma_1 \to \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$, dado por $\varphi_N(\gamma) = \gamma \mod N$, temos que $\Gamma_N = \{\gamma \in \Gamma_1 : \gamma \equiv 1 \mod N\} = \ker \varphi_N$. Pelo Primeiro Teorema do Isomorfismo,

$$\frac{\Gamma_1}{\ker \varphi_N} \simeq Im\varphi_N \implies \frac{\Gamma_1}{\Gamma_N} \simeq Im\varphi_N \subset \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z}).$$

Como $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ é um conjunto finito, segue que $Im\varphi_N$ é um conjunto finito. Logo, $[\Gamma_1 : \Gamma_N] = \#\Gamma_1/\Gamma_N = \#Im\varphi_N < \infty$. Como $\Gamma_N \subseteq \Gamma' \subseteq \Gamma_1$, segue que $[\Gamma_1 : \Gamma'] < \infty$. □

Lema 10. *Seja $M \in M(2, \mathbb{Z})$ com determinante não-nulo. Então, $\Gamma_1 \cap M^{-1}\Gamma_1 M$ é um subgrupo de congruência de Γ_1.*

Demonstração. Seja $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M(2, \mathbb{Z})$. Como, por hipótese, temos $\det M \neq 0$, tome $N = \det M$. Por definição, $\Gamma_N \subseteq \Gamma_1$. Resta ver que $\Gamma_N \subseteq M^{-1}\Gamma_1 M$, ou, equivalentemente, que dado $\gamma \in \Gamma_N$ temos $M\gamma M^{-1} \in \Gamma_1$.

(i) $M\gamma M^{-1}$ possui coeficientes inteiros: de fato, note que $\gamma \in \Gamma_N$ implica que $\gamma = 1_{2\times 2} + N\delta$, onde $\delta = \left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{smallmatrix}\right) \in M(2,\mathbb{Z})$. Logo,

$$\begin{aligned} M\gamma M^{-1} &= M(1_{2\times 2} + N\delta)M^{-1} = (M + MN\delta)M^{-1} = MM^{-1} + MN\delta M^{-1} \\ &= 1_{2\times 2} + MN\delta M^{-1} = 1_{2\times 2} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \det M \cdot \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \cdot \frac{1}{\det M} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= 1_{2\times 2} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M(2,\mathbb{Z}). \end{aligned}$$

(ii) $\det M\gamma M^{-1} = 1$: De fato, como $\gamma \in \Gamma_1$, temos $\det \gamma = 1$. Logo,

$$\det(M\gamma M^{-1}) = \det M \det \gamma \det M^{-1} = \det M \det M^{-1} = \det(MM^{-1}) = \det(1) = 1.$$

Dos itens (i) e (ii) segue o resultado. □

Corolário 5. *Seja $M \in M(2,\mathbb{Z})$ com determinante não-nulo. O subgrupo $\Gamma_1 \cap M^{-1}\Gamma_1 M$ possui índice finito em Γ_1.*

Demonstração. A demonstração segue imediatamente dos dois últimos lemas. □

4.5 Algebricidade dos Valores Especiais de j

Definição 12. Seja $\mathfrak{z} \in \mathfrak{H}$ um ponto CM. O número complexo $j(\mathfrak{z})$ é chamado de *valor especial*[1] de j.

O principal teorema deste trabalho afirma que valores especiais de j são números algébricos. Sabemos que, se $\mathfrak{z} \in \mathfrak{H}$ é um ponto CM, a Proposição 10 garante a existência de uma matriz $M \in M(2,\mathbb{Z})$ não proporcional à identidade fixando $\mathfrak{z}$. O ponto chave da demonstração deste teorema é a dependência algébrica das funções $j(z)$ e $j(Mz)$ sobre $\mathbb{Q}$, que fornecerá um polinômio $R(X,Y) \in \mathbb{Q}[X,Y]\backslash\{0\}$ satisfazendo

$$R\left(j(Mz), j(z)\right) \equiv 0. \tag{4.7}$$

Ao considerar a restrição deste polinômio à diagonal $X = Y$, obtemos polinômio $R(X,X) \in \mathbb{Q}[X]$ não identicamente nulo satisfazendo a relação (4.7). A conclusão segue utilizando o fato de que a matriz M fixa o ponto CM $\mathfrak{z}$.

Proposição 12. *Para toda matriz $M \in M(2,\mathbb{Z})$ com determinante não nulo, existe um polinômio $R \in \mathbb{Q}[X,Y]\backslash\{0\}$, tal que $R(j(Mz), j(z)) \equiv 0$.*

[1] Em inglês, estes valores são conhecidos como *singular moduli*. A terminologia *valor especial* vem do fato de que os pontos CM são pontos especiais do semiplano superior no contexto de variedades de Shimura.

Demonstração. Seja $M \in M(2,\mathbb{Z})$ uma matriz com determinante positivo. As funções $j(z)$ e $j(Mz)$ são ambas funções modulares com respeito ao subgrupo $\Gamma' := \Gamma_1 \cap M^{-1}\Gamma_1 M$ e, pelo Corolário 5, sabemos que Γ' possui índice finito em Γ_1, digamos $(\Gamma_1 : \Gamma') = m$. Então, $\Gamma_1 = \Gamma'\gamma_1 \cup \ldots \cup \Gamma'\gamma_m$, para representantes $\gamma_1, \ldots, \gamma_m \in \Gamma_1$. A fim de facilitar a notação, considere:

$$j'(z) = j(Mz) \qquad \text{e} \qquad j'_{|_\gamma}(z) = j'(\gamma z) = j(M\gamma z),$$

para $\gamma \in \Gamma_1$ e $z \in \mathfrak{H}$, e defina o polinômio

$$\begin{aligned} P(X) &:= \prod_{i=1}^{m} \left(X - j'_{|_{\gamma_i}}(z)\right) = \left(X - j'_{|_{\gamma_1}}(z)\right) \ldots \left(X - j'_{|_{\gamma_m}}(z)\right) \\ &= P_0 + P_1 X + \ldots + P_{m-1}X^{m-1} + X^m, \end{aligned} \tag{4.8}$$

cujos coeficientes são os *polinômios simétricos elementares*:

$$P_i(z) = (-1)^m \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant m} j'_{|_{\gamma_{i_1}}}(z) \ldots j'_{|_{\gamma_{i_m}}}(z), \qquad \text{para } i = 1, \ldots, m.$$

Note que P é um polinômio mônico, e portanto não identicamente nulo, que anula $j(Mz)$, pois podemos supor $\gamma_k = 1_{2\times 2} \in \Gamma_1$, para algum $k \in I = \{1, \ldots, m\}$. Vamos provar que $P_i \in \mathbb{Q}[j]$, para cada $i \in J = \{0, \ldots, m-1\}$, ou seja, que cada coeficiente de P é um polinômio em j com coeficientes racionais. Primeiramente, vejamos que $P_i \in \mathbb{C}[j]$ e, para isto, é suficiente provar que cada coeficiente de P é uma função holomorfa em $\mathfrak{H}$ e modular de peso 0, pois seguirá da Proposição 9 (Observação 9) que cada coeficiente de P é um polinômio em j. Mais precisamente, vamos provar os seguintes itens: para cada $i \in J$,

(i) P_i é Γ_1 - invariante,

(ii) P_i é uma função meromorfa em $\mathfrak{H}$, inclusive no infinito.

Para o item (i), note que a ação de Γ_1 em $\Gamma'\backslash\Gamma_1$ pela direita via um elemento $\gamma \in \Gamma_1$ apenas permuta os representantes γ_i, e portanto existe uma permutação σ nos índices $I = \{1, \cdots, m\}$ tal que $\Gamma'\gamma_i\gamma = \Gamma'\gamma_{\sigma(i)}$, para cada $i \in I$. Assim, para cada $i \in I$, existe γ'_i dependendo de γ para o qual $\gamma_i\gamma = \gamma'_i\gamma_{\sigma(i)}$. Sendo j' uma função Γ'-invariante, temos

$$j'_{|_{\gamma_i\gamma}}(z) = j'(\gamma_i\gamma z) = j'(\gamma'_i\gamma_{\sigma(i)}z) = j'_{|_{\gamma_{\sigma(i)}}}(z), \qquad \text{para cada } i \in I \text{ e } z \in \mathfrak{H}.$$

Agindo com $\gamma \in \Gamma_1$ em P, segue que

$$P_{|_\gamma}(X) = \left(X - j'_{|_{\gamma_1\gamma}}\right) \ldots \left(X - j'_{|_{\gamma_m\gamma}}\right) = \left(X - j'_{|_{\gamma_{\sigma(1)}}}\right) \ldots \left(X - j'_{|_{\gamma_{\sigma(m)}}}\right) = P(X),$$

uma vez que a permutação nos índices apenas altera a ordem dos fatores $\left(X - j'_{|_{\gamma_i}}\right)$, para cada $i \in I$. Logo, $P_{i|_\gamma} = P_i$, para todo $i \in J$, o que prova a afirmação (i).

Para o item (ii), como os coeficientes P_i são somas de produtos das funções $j'_{|\gamma_k}$, com $1 \leqslant k \leqslant i$, basta provarmos, para um $i \in I$ fixo, que $j'_{|\gamma_i}$ é holomorfa em $\mathfrak{H}$ e meromorfa no infinito. De fato, como $j'_{|\gamma_i}(z) = j'(\gamma_i z) = j(M\gamma_i z)$, podemos ver $j'_{|\gamma_i}$ como a composição de j com as aplicações $z \mapsto Mz$ e $z \mapsto \gamma_i z$, que são holomorfas em $\mathfrak{H}$, visto que $\det M, \det \gamma_i > 0$. Logo $j'_{|\gamma_i}$ é holomorfa em $\mathfrak{H}$. Também, considere $M' = M\gamma_i$, que possui determinante positivo, pois $\det \gamma_i = 1$ e $\det M > 0$. Pela Proposição 11, existem matrizes $\delta_i \in \Gamma_1$ e $N_i \in \mathcal{M}^*_{\det M}$ com $\det M' = \det M$, digamos $N_i = \left(\begin{smallmatrix} a_i & b_i \\ 0 & d_i \end{smallmatrix}\right)$, tais que $M' = \delta_i N_i$. Como j é Γ_1 - invariante, obtemos que

$$j'_{|\gamma_i}(z) = j'(\gamma_i z) = j(M\gamma_i z) = j(M'z) = j(\delta_i N_i z) = j(N_i z).$$

Pelo Lema 8, $j(N_i z)$ é meromorfa no infinito e, portanto, concluímos o item (ii).

Por fim, vejamos que os coeficientes de P são racionais. De fato, pelo Lema 8, podemos substituir a q-expansão de $j'_{|\gamma_i}(z) = j(N_i z)$ na expressão de P:

$$P(X) = \prod_{i=1}^{m} \left(X - j'_{|\gamma_i}(z)\right) = \prod_{i=1}^{m} \left(X - \sum_{n=-1}^{\infty} c_n \zeta_{d_i}^{b_i n} q^{\frac{a_i n}{d_i}}\right),$$

e notar que o termo geral no produto é um elemento do anel $\mathbb{Z}[\zeta_{d_i}][X][q^{-1/d_i}, q^{1/d_i}]$ das séries de Laurent em q^{1/d_i} com coeficientes em $\mathbb{Z}[\zeta_{d_i}]$. Aplicar uma conjugação galoisiana $\zeta_{d_i} \mapsto \zeta_{d_i}^r$, em que $r \in (\mathbb{Z}/d_i\mathbb{Z})^*$ — o conjunto dos elementos inversíveis em $\mathbb{Z}/d_i\mathbb{Z}$ — apenas altera a potência b_i de ζ_{d_i} por $b_i r$, a qual acaba percorrendo novamente o mesmo conjunto de possíveis potências $(\mathbb{Z}/d_i\mathbb{Z})^*$, que é um grupo finito. Isto significa que aplicar qualquer $\mathbb{Q}$-automorfismo em P vai apenas permutar a ordem dos produtos $\left(X - j'_{|\gamma_i}\right)$, de modo que os valores dos coeficientes de P permanecem inalterados. Portanto, os coeficientes da expansão de Laurent de P são racionais. A conclusão segue da Observação 9, pois, como cada coeficiente de P é uma função modular de peso 0 e holomorfa em $\mathcal{H}$ com coeficientes da série de Laurent racionais, temos que cada coeficiente de P é um polinômio em j com coeficientes racionais, ou seja, $P_i \in \mathbb{Q}[j]$, para todo $i \in J$.

Em suma, encontramos polinômio P em uma variável X que anula $j(Mz)$ e cujos coeficientes $P_i \in \mathbb{Q}[j]$ são polinômios em j com coeficientes racionais. Digamos que $P_i = Q_i(j)$, em que $Q_i(Y) \in \mathbb{Q}[Y]$ é um polinômio em uma variável Y com coeficientes racionais, e defina

$$R(X, Y) = Q_0(Y) + Q_1(Y)X + \ldots + X^m \in \mathbb{Q}[X, Y] \backslash \{0\}.$$

Como $P(j(Mz)) \equiv 0$ e cada coeficiente de P é um polinômio em j, segue que

$$R(j(Mz), j(z)) \equiv 0,$$

concluindo a demonstração. □

Teorema 8. *Seja $\mathfrak{z} \in \mathfrak{H}$ um ponto CM. Então, $j(\mathfrak{z})$ é um número algébrico.*

Demonstração. Seja $\mathfrak{z} \in \mathfrak{H}$ um ponto CM. Pela Proposição 10, existe matriz $M \in M(2,\mathbb{Z})$ não proporcional à identidade que fixa $\mathfrak{z}$. O Lema 12 garante a existência de um polinômio $R \in \mathbb{Q}[X,Y]\backslash\{0\}$ satisfazendo $R(j(Mz), j(z)) \equiv 0$. Podemos considerar a restrição de R à diagonal $X = Y$, visto que possíveis potências de $X - Y$ dividindo R podem ser removidas sem afetar a validade da relação $R(j(Mz), j(z)) \equiv 0$, já que $j(Mz)$ não é identicamente igual a $j(z)$, e isto garante que $R(X,X)$ não é identicamente nulo. Desta forma, obtemos polinômio $R[X,X] \in \mathbb{Q}[X]\backslash\{0\}$ satisfazendo

$$R(j(M\mathfrak{z}), j(\mathfrak{z})) = R(j(\mathfrak{z}), j(\mathfrak{z})) = 0,$$

pois M fixa o ponto CM $\mathfrak{z}$. Portanto, o valor especial $j(\mathfrak{z})$ é um número algébrico. □

Observação 12. Dado $\mathfrak{z} \in \mathfrak{H}$ um ponto CM e dada uma correspondente matriz $M \in M(2,\mathbb{Z})$ que fixa este ponto, provamos que o valor especial $j(\mathfrak{z})$ é um número algébrico utilizando a dependência algébrica das funções $j(Mz)$ e $j(z)$ para obter um polinômio mônico com coeficientes racionais que admita o valor especial $j(\mathfrak{z})$ como raíz. No entanto, é possível escolher este polinômio de forma que ele possua coeficientes inteiros. Na realidade, a proposição a seguir nos fornece um resultado ainda mais preciso: este polinômio pode ser escolhido de forma a possuir coeficientes inteiros e dependendo apenas do determinante da matriz M.

Proposição 13. *Para cada $m \in \mathbb{N}$, existe um polinômio $\Psi_m(X,Y) \in \mathbb{Z}[X,Y]$, simétrico a menos de sinal e de grau $\sigma_1(m)$ em ambas as entradas tal que $\Psi_m(j(Mz), j(z)) \equiv 0$, para toda matriz $M \in M(2,\mathbb{Z})$ de determinante m.*

Demonstração. Seja $\mathcal{M}_m$ o conjunto das matrizes em $M(2,\mathbb{Z})$ de determinante m. Pela Proposição 11, o conjunto $\mathcal{M}_m^*$ é um sistema completo de representantes para o quociente $\Gamma_1\backslash\mathcal{M}_m$ e, portanto, podemos nos restringir a trabalhar com matrizes de $\mathcal{M}_m^*$, já que j é Γ_1-invariante. Considere o polinômio

$$P(X) := \prod_{M \in \mathcal{M}_m^*} (X - j(Mz)) = \sum_i P_i(z) X^i,$$

que é Γ_1-invariante, pois $\mathcal{M}_m$ é invariante sob a multiplicação à esquerda e à direita por matrizes de Γ_1, e é de grau $\sigma_1(m) = \sum_{d|m} d$, pois

$$|\Gamma_1\backslash\mathcal{M}_m| = |\mathcal{M}_m^*| = \sum_{ad=m} d = \sigma_1(m).$$

Pelo Lema 8, temos que $j(Mz)$ é uma função holomorfa em $\mathfrak{H}$ e meromorfa no infinito, para toda matriz $M \in \mathcal{M}_m^*$. Logo, os coeficientes P_i deste polinômio são funções holomorfas em $\mathfrak{H}$ e meromorfas no infinito, de onde segue que são funções modular de peso 0. Pela

Observação 9, cada coeficiente P_i é um polinômio em j, digamos $P_i = Q_i(j)$. Para $\Psi_m(X,Y) = \sum_i Q_i(Y)X^i$, temos que

$$\Psi_m(X, j(z)) = \sum_i Q_i(j(z))X^i = \prod_{M\in\mathcal{M}_m^*} (X - j(Mz)).$$

Queremos mostrar que $\Psi_m(X,Y) \in \mathbb{Z}[X,Y]$. Como $\Psi_m(X,Y) = \sum_i Q_i(Y)X^i$, basta mostrarmos que cada $Q_i \in \mathbb{Z}[Y]$. Agora, sabemos que cada $Q_i(j(z)) = P_i(z)$ é uma função modular de peso 0, e portanto admite expansão de Fourier. Como o Lema 8 nos fornece a q-expansão de $j(Mz)$, para toda matriz $M \in \mathcal{M}_m^*$, e podemos expandir o polinômio $\Psi_m(X, j(z))$ na forma

$$\begin{aligned}\Psi_m(X, j(z)) &= \prod_{M\in\mathcal{M}_m^*} (X - j(Mz)) = \prod_{ad=m}\prod_{b=0}^{d-1}\left(X - j\left(\frac{az+b}{d}\right)\right)\\ &= \prod_{ad=m}\prod_{b=0}^{d-1}\left(X - \sum_{n=-1}^{\infty} c_n\zeta_d^{bn}q^{an/d}\right), \qquad \text{onde } \zeta_d = e^{2\pi i/d},\end{aligned}$$

segue que os coeficiente de Fourier de P_i são racionais (pela mesma argumentação apresentada na demonstração da Proposição 12). Mais ainda, eles são inteiros, pois os coeficientes de $\Psi_m(X, j(z))$ são inteiros algébricos, já que são combinações dos coeficientes c_n de j (que são inteiros) e das raízes da unidade ζ_d (que são inteiros algébricos), e $\overline{\mathbb{Z}}$ é um subanel de $\mathbb{C}$ (pelo Lema 12). O Lema 14 nos diz que inteiros algébricos racionais são simplesmente números inteiros, e concluímos. Em suma, temos que cada $Q_i(j(z)) = P_i(z)$ possui coeficientes da expansão de Fourier inteiros. Pela Observação 10, segue então que os coeficientes de Q_i como um polinômio em j são inteiros, isto é $Q_i(Y) \in \mathbb{Z}[Y]$. Portanto, $\Psi_m(X,Y) \in \mathbb{Z}[X,Y]$. Para finalizar a demonstração, basta notar que

$$\Psi_m(j(Mz), j(z)) = \prod_{M\in\mathcal{M}_m^*} (j(Mz) - j(Mz)) \equiv 0, \qquad \text{para toda matriz } M \in \mathcal{M}_m^*,$$

e que a simetria de $\Psi_m(X,Y)$ a menos de sinal segue do fato de que $z' = Mz$ para $M = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$ é equivalente a $z = M'z'$, para $M' = \left(\begin{smallmatrix} d & -b \\ -a & c\end{smallmatrix}\right)$. □

Observação 13. $\Psi_m(X,Y)$ é chamado de *polinômio modular*.

Exemplo 3 (Polinômio Modular para o caso $m = 2$). Observe que o sistema completo de representantes para o quociente $\Gamma_1\backslash\mathcal{M}_2$ é o conjunto

$$\mathcal{M}_2^* = \left\{\begin{pmatrix} a & b \\ 0 & d\end{pmatrix}; a,b,d \in \mathbb{Z}, ad = 2, 0 \leqslant b < d\right\} = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 2\end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2\end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1\end{pmatrix}\right\},$$

e, portanto, o polinômio modular é dado por

$$\Psi_2(X, j(z)) := \prod_{M\in\mathcal{M}_2^*} (X - j(Mz)) = \left(X - j\left(\frac{z}{2}\right)\right)\left(X - j\left(\frac{z+1}{2}\right)\right)(X - j(2z)).$$

Desenvolvendo o produto, escrevemos o polinômio na forma $X^3 - A(z)X^2 + B(z)X - C(z)$, onde

$$\begin{aligned}
A(z) &= j\left(\frac{z}{2}\right) + j\left(\frac{z+1}{2}\right) + j(2z),\\
B(z) &= j\left(\frac{z}{2}\right) j\left(\frac{z+1}{2}\right) + j\left(\frac{z}{2}\right) j(2z) + j\left(\frac{z+1}{2}\right) j(2z),\\
C(z) &= j\left(\frac{z}{2}\right) j\left(\frac{z+1}{2}\right) j(2z).
\end{aligned}$$

Vamos escrever os termos $j(Mz)$, com $M \in M_2^*$, em função de $j(z)$, já que a Proposição 13 nos garante que os coeficientes do polinômio modular são polinômios em j. Lembrando que a q-expansão de $j(Mz)$ é dada por

$$j(Mz) = \sum_{n=-1}^{\infty} c_n \zeta_d^{bn} q^{\frac{an}{d}} \text{ , em que } M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

temos, para o nosso caso,

$$\begin{aligned}
j\left(\frac{z}{2}\right) &= \sum_{n=-1}^{\infty} c_n \zeta_2^{0.n} q^{\frac{n}{2}}\\
&= q^{-\frac{1}{2}} + 744 + 196884q^{\frac{1}{2}} + 21493760q + 864299970q^{\frac{3}{2}}\\
&\quad + 20245856256q^2 + O(q^{\frac{5}{2}}), \qquad (4.9)\\
j\left(\frac{z+1}{2}\right) &= \sum_{n=-1}^{\infty} c_n \zeta_2^{n} q^{\frac{n}{2}}\\
&= -q^{-\frac{1}{2}} + 744 - 196884q^{\frac{1}{2}} + 21493760q - 864299970q^{\frac{3}{2}}\\
&\quad + 20245856256q^2 + O(q^{\frac{5}{2}}), \qquad (4.10)\\
j(2z) &= \sum_{n=-1}^{\infty} c_n \zeta_2^{0.n} q^{2n}\\
&= q^{-2} + 744 + 196884q^2 + O(q^4). \qquad (4.11)
\end{aligned}$$

Além disso, serão úteis as seguintes identidades:

$$\begin{aligned}
q^{-1} &= j(z) - c_0 + O(q) = j(z) - 744 + O(q), \qquad (4.12)\\
q^{-2} &= j(z)^2 - 2c_0 q^{-1} - (2c_1 + c_0^2) + O(q) = j(z)^2 - 1488q^{-1} - 947304 + O(q), \qquad (4.13)\\
q^{-3} &= j(z)^3 - 3c_0 q^{-2} - (3c_0^2 + 3c_1)q^{-1} - (c_0^3 + 6c_0c_1 + 3c_2) + O(q)\\
&= j(z)^3 - 2232q^{-2} - 2251260q^{-1} - 1355202240 + O(q). \qquad (4.14)
\end{aligned}$$

Nas equações acima, utilizamos a notação $O(q^n)$ para ocultar os termos com as potências

maiores ou iguais a n. Substituindo-as na expressão de $A(z)$, obtemos:

$$\begin{aligned} A(z) &= j\left(\frac{z}{2}\right) + j\left(\frac{z+1}{2}\right) + j(2z) \\ &= (q^{-\frac{1}{2}} + c_0 + O(q^{\frac{1}{2}})) + (-q^{-\frac{1}{2}} + c_0 + O(q^{\frac{1}{2}})) + (q^{-2} + c_0 + O(q^4)) \\ &= q^{-2} + 3c_0 + O(q) = j(z)^2 - 2c_0(j(z) - c_0) - c_0^2 - 2c_1 + 3c_0 + o(1) \\ &= j(z)^2 - 1488j(z) + 162000 + O(q^{\frac{1}{2}}). \end{aligned} \tag{4.15}$$

Para o cálculo de $B(z)$, calculemos os produtos envolvidos separadamente:

$$\begin{aligned} j\left(\frac{z}{2}\right) j\left(\frac{z+1}{2}\right) &= (q^{-\frac{1}{2}} + 744 + 196884q^{\frac{1}{2}} + O(q))(-q^{-\frac{1}{2}} + 744 - 196884q^{\frac{1}{2}} + O(q)) \\ &= -q^{-1} + 159768 + O(q^{\frac{1}{2}}), \end{aligned}$$

$$\begin{aligned} j\left(\frac{z}{2}\right) j(2z) &= (q^{-\frac{1}{2}} + 744 + 196844q^{\frac{1}{2}} + 21493760q \\ &\quad + 8642999970q^{\frac{3}{2}} + 20245856256q^2 + O(q^{\frac{5}{2}})) \\ &\quad (q^{-2} + 744 + O(q^4)) \\ &= q^{-\frac{5}{2}} + 744q^{-2} + 196844q^{-\frac{3}{2}} + 21493760q^{-1} + 862499970q^{-\frac{1}{2}} + \\ &\quad 20245856256 + 744q^{-\frac{1}{2}} + 744.744 + O(q^{\frac{1}{2}}) \\ &= q^{-\frac{5}{2}} + 744q^{-2} + 196844q^{-\frac{3}{2}} + 21493760q^{-1} + 864300714q^{-\frac{1}{2}} \\ &\quad + 20246409792 + O(q^{\frac{1}{2}}), \end{aligned}$$

$$\begin{aligned} j\left(\frac{z+1}{2}\right) j(2z) &= (-q^{-\frac{1}{2}} + 744 - 196844q^{\frac{1}{2}} + 21493760q - 8642999970q^{\frac{3}{2}} \\ &\quad + 20245856256q^2 + O(q^{\frac{5}{2}}))(q^{-2} + 744 + O(q^4)) \\ &= -q^{-\frac{5}{2}} + 744q^{-2} - 196844q^{-\frac{3}{2}} + 21493760q^{-1} - 864300714q^{-\frac{1}{2}} \\ &\quad + 20246409792 + O(q^{\frac{1}{2}}). \end{aligned}$$

Somando $j\left(\frac{z}{2}\right) j(2z)$ e $j\left(\frac{z+1}{2}\right) j(2z)$, obtemos

$$\begin{aligned} j\left(\frac{z}{2}\right) j(2z) + j\left(\frac{z+1}{2}\right) j(2z) &= 2(744q^{-2} + 21493760q^{-1} + 20246409792 + O(q)) \\ &= 1488q^{-2} + 42987520q^{-1} + 40492819584 + O(q). \end{aligned}$$

Portanto,

$$\begin{aligned}
B(z) &= j\left(\frac{z}{2}\right) j\left(\frac{z+1}{2}\right) + j\left(\frac{z}{2}\right) j(2z) + j\left(\frac{z+1}{2}\right) j(2z) \\
&= (-q^{-1} + 159768 + O(q^{\frac{1}{2}})) + (1488q^{-2} + 42987520q^{-1} + 40492819584 + O(q)) \\
&= 1488q^{-2} + 42987519q^{-1} + 40492979352 + O(q^{\frac{1}{2}}) \\
&= 1488(j(z)^2 - 1488q^{-1} - 947304 + O(q)) + 42987519q^{-1} + 40492979352 + O(q^{\frac{1}{2}}) \\
&= 1488j(z)^2 + 40773375q^{-1} + 39083391000 + O(q^{\frac{1}{2}}) \\
&= 1488j(z)^2 + 40773375(j(z) - 744 + O(q)) + 39083391000 + O(q^{\frac{1}{2}}) \\
&= 1488j(z)^2 + 40773375j(z) + 8748000000 + O(q^{\frac{1}{2}}). \qquad (4.16)
\end{aligned}$$

Por fim, para o cálculo de $C(z) = j\left(\frac{z}{2}\right) j\left(\frac{z+1}{2}\right) j(2z)$, calculemos $j\left(\frac{z}{2}\right) j\left(\frac{z+1}{2}\right)$ até a segunda potência:

$$\begin{aligned}
j\left(\frac{z}{2}\right) j\left(\frac{z+1}{2}\right) &= (q^{-\frac{1}{2}} + c_0 + c_1 q^{\frac{1}{2}} + c_2 q + c_3 q^{\frac{3}{2}} + c_4 q^2 + c_5 q^{\frac{5}{2}} + O(q^3)) \\
&\quad (-q^{-\frac{1}{2}} + c_0 - c_1 q^{\frac{1}{2}} + c_2 q - c_3 q^{\frac{3}{2}} + c_4 q^2 - c_5 q^{\frac{5}{2}} + O(q^3)) \\
&= -q^{-1} + (c_0^2 - 2c_1) + (2c_0c_2 - 2c_3 - c_1^2)q \\
&+ (2c_0c_4 - 2c_1c_3 - 2c_5 + c_2^2)q^2 + O(q^3) \\
&= -q^{-1} + 159768 - 8509194516q + 151107477178368q^2 + O(q^3).
\end{aligned}$$

Multiplicando por $j(2z)$, obtemos

$$\begin{aligned}
C(z) &= j\left(\frac{z}{2}\right) j\left(\frac{z+1}{2}\right) j(2z) \\
&= (-q^{-1} + 159768 - 8509194516q + 151107477178368q^2 + O(q^3)) \\
&(q^{-2} + 744 + 196884q2 + O(q^4)) \\
&= -q^{-3} + 159768q^{-2} - 8509195260q^{-1} + 151107596045760 + O(q) \\
&= -(j(z)^3 - 2232q^{-2} - 2251260q^{-1} - 1355202240 + O(q)) + 159768q^{-2} \\
&- 8509195260q^{-1} + 151107596045760 + O(q) \\
&= -j(z)^3 + 162000q^{-2} - 8506944000q^{-1} + 151108951248000 + O(q) \\
&= -j(z)^3 + 162000(j(z)^2 - 1488q^{-1} - 947304 + O(q)) - 8506944000q^{-1} + \\
&\qquad 151108951248000 + O(q) \\
&= -j(z)^3 + 162000j(z)^2 - 8748000000q^{-1} + 150955488000000 + O(q) \\
&= -j(z)^3 + 162000j(z)^2 - 8748000000(j(z) - 744 + O(q)) \\
&+ 150955488000000 + O(q) \\
&= -j(z)^3 + 162000j(z)^2 - 8748000000j(z) + 157464000000000 + O(q). \qquad (4.17)
\end{aligned}$$

Escrevendo

$$\begin{aligned}
&A(z) - (j(z)^2 - 1488j(z) + 162000) = O(q^{\frac{1}{2}}),\\
&B(z) - (1488j(z)^2 + 40773375j(z) + 8748000000) = O(q^{\frac{1}{2}}),\\
&C(z) - (-j(z)^3 + 162000j(z)^2 - 8748000000j(z) + 157464000000000) = O(q),
\end{aligned}$$

notamos que o lado esquerdo das igualdades acima são funções modulares, visto que a Proposição 13 nos garante que os coeficientes de polinômio modular são funções modulares, e $j(z)$ é uma função modular. Mas o fato de que $O(q^n) \to 0$ quando $z \to +i\infty$ para valores positivos de n nos diz que as expressões do lado esquerdo das igualdades são formas cuspidais de peso 0. Como $\dim S_0 = 0$, a única forma cuspidal de peso 0 é a função constante igual a zero, e portanto

$$\begin{aligned}
A(z) &= j(z)^2 - 1488j(z) + 162000,\\
B(z) &= 1488j(z)^2 + 40773375j(z) + 8748000000,\\
C(z) &= -j(z)^3 + 162000j(z)^2 - 8748000000j(z) + 157464000000000.
\end{aligned}$$

Considerando $Y = j(z)$, temos que o polinômio modular é dado por:

$$\begin{aligned}
\Psi_2(X,Y) = &-X^2Y^2 + X^3 + 1488X^2Y + Y^3 - 162000X^2 + 40773375 - 162000Y^2\\
&+ 8748000000X + 8748000000Y - 157464000000000.
\end{aligned}$$

No Teorema 8 obtemos a algebricidade do valor especial $j(\mathfrak{z})$ encontrando o polinômio $P(X,X) \in \mathbb{Q}[X]$ satisfeito por $j(\mathfrak{z})$. Revisitando este resultado, agora sob a perspectiva da Proposição 13, poderíamos restringir o polinômio $\Psi_m(X,Y)$ à diagonal $X = Y$ e obter dessa vez um polinômio com coeficientes inteiros satisfeito por $j(\mathfrak{z})$. No entanto, para concluirmos que os valores especiais da função j são *inteiros algébricos*, precisamos da garantia de que a restrição desse polinômio à diagonal $X = Y$ continua sendo um polinômio mônico. A proposição a seguir nos assegura deste fato.

Proposição 14. *Se m não é um quadrado perfeito, o polinômio $\Psi_m(X,X)$ é, a menos de sinal, um polinômio mônico de grau $\sigma_1^+(m) := \sum_{d|m} \max(d, m/d)$.*

Demonstração. Primeiramente, observe que a condição de m não ser um quadrado perfeito nos garante que Ψ_m não é identicamente nulo, pois, caso contrário, $\Psi_m(X,Y)$ conteria algum fator $(X-Y)$, de modo que a restrição do polinômio $\Psi_m(X,Y)$ a diagonal $X = Y$ seria identicamente nula. Agora, restingindo

$$\Psi_m(X, j(z)) = \prod_{ad=m} \prod_{b=0}^{d-1} \left(X - j\left(\frac{az+b}{d}\right)\right)$$

à diagonal $X = j(z)$ e já considerando as q-expansões de $j(z)$ e $j\left(\frac{az+b}{d}\right)$, obtemos:

$$\begin{aligned}\Psi_m(j(z), j(z)) &= \prod_{ad=m}\prod_{b=0}^{d-1}\left(j(z) - j\left(\frac{az+b}{d}\right)\right) = \prod_{ad=m}\prod_{b=0}^{d-1}\left(\sum_{n=-1}^{\infty} c_n q^n - \sum_{n=-1}^{\infty} c_n \zeta_d^{bn} q^{an/d}\right)\\ &= \prod_{ad=m}\prod_{b=0}^{d-1}(q^{-1} + c_0 + O(1)) - \left(\zeta_d^{-b} q^{-a/d} + c_0 + O(1)\right)\\ &= \prod_{ad=m}\prod_{b=0}^{d-1}\left(q^{-1} - \zeta_d^{-b} q^{-a/d} + O(1)\right).\end{aligned}$$

Utilizando a identidade $\prod_{b=0}^{d-1}\left(x - \zeta_d^b y\right) = x^d - y^d$, segue que

$$\prod_{b=0}^{d-1}\left(q^{-1} + O(1) - \zeta_d^{-b} q^{-1/d}\right) = q^{-d} - q^{-a} + O(1).$$

Logo,

$$\Psi_m(j(z), j(z)) = \prod_{ad=m}\left(q^{-d} - q^{-a} + O(1)\right).$$

A expressão nos parênteses é uma série de Laurent de ordem negativa, dependendo dos valores de a e d. Mais especificamente, a ordem dessa série é $\max\{d, a\} = \max\{d, m/d\}$. Dessa forma, o coeficiente líder dessa série será ± 1, a depender dos valores de a e d. Por outro lado, sabemos que o polinômio $\Psi_m(X, Y)$ é mônico, e assim sua restrição à diagonal $X = j(z)$ vai possuir coeficiente líder ± 1, ou seja, é mônico a menos de sinal. Por fim, a ordem de $\Psi_m(j(z), j(z))$ é $\sum_{d|m} \max\{d, m/d\} = \sigma_1^+(m)$. Tomando $z \to +i\infty$, temos $O(1) \to 0$ e, portanto,

$$\Psi_m(j(z), j(z)) = \prod_{ad=m}\left(q^{-d} - q^{-a} + O(1)\right) \sim \pm q^{-\sigma_1^+(m)}.$$

□

Corolário 6. *Os valores especiais da função j são inteiros algébricos.*

Demonstração. Seja $\mathfrak{z} \in \mathfrak{H}$ um ponto CM. Então, existe alguma matriz em $\mathcal{M}_m$ que fixa j. Seja M^* a matriz em $\mathcal{M}_m^*$ correspondente. A proposição 13 nos fornece o polinômio $\Psi_m(X, j(z)) \in \mathbb{Z}[X, Y]$, e a proposição 14 garante que sua restrição à diagonal $X = j(z)$ é ainda um polinômio mônico com coeficientes inteiros $\Psi_m(j(z), j(z)) = \prod_{M \in \mathcal{M}_m^*}(j(z) - j(Mz))$. Avaliando em $j(\mathfrak{z})$,

$$\begin{aligned}\Psi_m(j(\mathfrak{z}), j(\mathfrak{z})) &= (j(\mathfrak{z}) - j(M^*\mathfrak{z})) \prod_{M \neq M^* \in \mathcal{M}_m^*}(j(z) - j(Mz))\\ &= (\underbrace{j(\mathfrak{z}) - j(\mathfrak{z})}_{0}) \prod_{M \neq M^* \in \mathcal{M}_m^*}(j(z) - j(Mz)) = 0.\end{aligned}$$

Portanto, o valor especial $j(\mathfrak{z})$ é um inteiro algébrico. □

Revisitando o exemplo 3 sob a perspectiva da Proposição 14, restringimos o polinômio $\Psi_2(X, Y)$ à diagonal $X = Y$ e obtemos

$$\begin{aligned}\Psi_2(X, X) &= -X^4 + 2978X^3 + 40449375X^2 + 17496000000X - 157464000000000 \\ &= -(X - 8000)(X + 3375)^2(X - 1728). \end{aligned} \tag{4.18}$$

Logo,

$$\Psi_2(j(z), j(z)) = -(j(z) - 8000)(j(z) + 3375)^2(j(z) - 1728).$$

Naturalmente, os zeros do polinômio modular $\Psi_2(j(z), j(z))$ são valores especiais de j. Isso significa que cada número complexo $\mathfrak{z} \in \mathfrak{H}$ que é fixo por uma matriz de $\mathcal{M}_2$ tem $j(\mathfrak{z})$ como raíz de Ψ_2. Por exemplo, os números complexos i, $(1 + 1\sqrt{7})/2$ e $i\sqrt{2}$ são pontos CM fixos, respectivamente, pelas seguintes matrizes:

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -2 \\ 1 & 0 \end{pmatrix} \text{ e } \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix}.$$

Logo, $j(i)$, $j((1 + 1\sqrt{7})/2)$ e $j(i\sqrt{2})$ são raízes de $\Psi_2(j(z), j(z))$, e portanto o valor de j nestes pontos CM pertence ao conjunto $\{8000, -3375, 1728\}$. Para distinguir as raízes, podemos calcular numéricamente alguns termos das q-expansões de $j(i)$, $j((1 + 1\sqrt{7})/2)$ e $j(i\sqrt{2})$ para concluir que

$$j(i) = 1728\ , \qquad j\left(\frac{1 + i\sqrt{7}}{2}\right) = -3375 \qquad \text{e} \qquad j(i\sqrt{2}) = 8000.$$

Em resumo, obter polinômios modulares Ψ_m nos fornece os valores especiais de j. Para ilustrar, se $\mathfrak{z}_D$ é o ponto CM da forma

$$\mathfrak{z}_D = \begin{cases} \dfrac{1}{2}\sqrt{D}\ , \text{ se } D \text{ é par} \\ \dfrac{1}{2}(1 + \sqrt{D})\ , \text{ se } D \text{ é ímpar} \end{cases},$$

em que D é um discriminante negativo, isto é, um número inteiro negativo congruente a 0 ou 1 módulo 4, temos a seguinte Tabela para os valores especiais $j(\mathfrak{z}_D)$:

Observação 14. Se $\mathfrak{z}_D \in \mathfrak{H}$ é um ponto CM, dizemos que D é o discriminante de $\mathfrak{z}_D$ se é o discriminante do polinômio minimal satisfeito por $\mathfrak{z}_D$. Neste caso, D é um inteiro negativo congruente a 0 ou 1 módulo 4, já que $\mathfrak{z}_D$ é um ponto quadrático imaginário em $\mathfrak{H}$.

Tabela 2 – Valores especiais de j em função do discriminante D.

D	$j(\mathfrak{z}_D)$
-3	0
-4	1728
-7	-3375
-8	8000
-11	-32768
-12	54000
-15	$-\frac{191025+85995\sqrt{5}}{2}$
-16	287496
-19	-884736

Fonte: [3, p. 71]

5 Valores Especiais de j e Discriminantes de Formas Quadráticas Binárias

O resultado fundamental do Capítulo 4 afirma que valores especiais de j são inteiros algébricos. Naturalmente, o próximo passo é estudar o grau destes valores, e, para isto, veremos que este grau está intrinsicamente relacionado com o discriminante dos valores especiais. Provaremos que, se $\mathfrak{z}, \mathfrak{z}' \in \mathfrak{H}$ são pontos CM com mesmo discriminante, então os conjuntos de determinantes de matrizes em $M(2, \mathbb{Z})$ que fixam os valores especiais $j(\mathfrak{z})$ e $j(\mathfrak{z}')$ coincidem. Então, veremos que se $\mathfrak{z}_D \in \mathfrak{H}$ é um ponto CM de discriminante D, o valor especial $j(\mathfrak{z}_D)$ é um inteiro algébrico de grau $h(D)$, ou seja, o *número de classes* de D, que definiremos neste capítulo no contexto de discriminantes de formas quadráticas binárias. O caso $h(D) = 1$ será tratado mais especificamente na Seção 5.1.1, já que neste caso os valores especiais serão inteiros (inteiros algébricos de grau 1), e também por se tratar de um caso especial de um problema clássico na matemática, o *problema do número de classes de Gauss*. De modo geral, este capítulo é dedicado à classificação dos valores especiais de acordo com seu grau e o discriminante do ponto CM associado, bem como descrever mais precisamente o processo de calcular os valores especiais de j discutido na Seção 4.5.

5.1 Discriminantes e a Finitude do Número de Classes

Considere as formas quadráticas binárias da forma:

$$Q(x, y) = Ax^2 + Bxy + Cy^2 := [A, B, C], \tag{5.1}$$

onde $A, B, C \in \mathbb{Z}$ e $D = B^2 - 4AC < 0$.

Lema 11. *A forma quadrática $Q(x, y)$ é definida, isto é, $Q(x, y) \neq 0$ para todo $(x, y) \neq (0, 0) \in \mathbb{R}^2$.*

Demonstração. Suponha que exista $(x, y) \neq (0, 0)$ tal que $Q(x, y) = 0$. Sem perda de generalidade, assuma $y \neq 0$ (o caso $x \neq 0$ se trata analogamente). Dividindo por y a equação (5.1), obtemos

$$A\left(\frac{x}{y}\right)^2 + B\left(\frac{x}{y}\right) + C = 0,$$

mostrando que x/y é raíz real de um polinômio quadrático cujo discriminante D é negativo, gerando uma contradição. □

Pelo lema provado acima, como as formas quadráticas $Q(x,y)$ são definidas, segue que elas possuem sinal fixo, isto é: o sinal de $Q(x,y)$ é sempre positivo, ou sempre negativo, para todo $(x,y) \in \mathbb{R}^2$. Convencionamos que seja positivo, ou, equivalentemente, basta supor $A > 0$. Além disso, vamos assumir que a forma quadrática $Q(x,y) = Ax^2 + Bxy + Cy^2$ seja *primitiva*, isto é, que $\text{mdc}(A,B,C) = 1$. Fica então definido o conjunto das formas quadráticas que trabalharemos:

$$\mathfrak{Q}_D = \{Q(x,y) = Ax^2 + Bxy + Cy^2 : A > 0, \text{mdc}(A,B,C) = 1 \text{ e } D = B^2 - 4AC < 0\}. \tag{5.2}$$

Proposição 15. *Se* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$ *e* $Q \in \mathfrak{Q}_D$*, a aplicação:*

$$\begin{aligned} \mathfrak{Q}_D \times \Gamma_1 &\to \mathfrak{Q}_D \\ (Q, \gamma) &\mapsto Q \circ \gamma, \end{aligned}$$

definida por $(Q \circ \gamma)(x,y) = Q(ax+by, cx+dy)$ *configura uma ação de grupo à direta de* Γ_1 *em* $\mathfrak{Q}_D$*.*

Demonstração. Sejam $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \gamma' = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in \Gamma_1$ e $Q \in \mathfrak{Q}_D$ quaisquer. Veja que a aplicação está bem definida, pois

$$\begin{aligned} (Q \circ \gamma)(x,y) &= Q(ax+by, cx+dy) = A(ax+by)^2 + B(ax+by)(cx+dy) + C(cx+dy)^2 \\ &= \underbrace{(Aa^2 + Bac + Cc^2)}_{\tilde{A}} x^2 + \underbrace{(2Aab + B(ad+bc) + 2Ccd)}_{\tilde{B}} xy \\ &+ \underbrace{(Ab^2 + Bbd + Cd^2)}_{\tilde{C}} y^2 \\ &= \tilde{A}x^2 + \tilde{B}xy + \tilde{C}y^2 \in \mathfrak{Q}_D. \end{aligned}$$

Além disso, como $(Q \circ 1_{2\times 2})(x,y) = Q(1x+0y, 0x+1y) = Q(x,y)$ e $(Q\circ\gamma)\circ\gamma' = Q\circ(\gamma\circ\gamma')$, segue o resultado. □

Observação 15. Podemos enxergar uma forma quadrática $Q(x,y) = Ax^2 + Bxy + Cy^2$ na forma matricial:

$$Q(x,y) = Ax^2 + Bxy + Cy^2 = \begin{pmatrix} x & y \end{pmatrix} \underbrace{\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix}}_{M} \underbrace{\begin{pmatrix} x \\ y \end{pmatrix}}_{X} = X^t M X. \tag{5.3}$$

Neste caso, se $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1$, a ação de γ em Q pode ser entendida matricialmente:

$$\begin{aligned} (Q \circ \gamma)(x,y) = Q(ax+by, cx+dy) &= \begin{pmatrix} ax+by & cx+dy \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} \\ &= \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} \gamma^t M \gamma \begin{pmatrix} x \\ y \end{pmatrix} \\ &= X^t \gamma^t M \gamma X = (\gamma X)^t M (\gamma X). \end{aligned} \tag{5.4}$$

Nesse sentido, para entender a ação de Γ_1 em $\mathfrak{Q}_D$ em determinados casos é conveniente utilizar a notação matricial descrita acima, como veremos mais adiante.

Definição 13. O número de classes de equivalência da ação de Γ_1 em $\mathfrak{Q}_D$, para um determinante fixo D, é chamado de *número de classes de* D, e denotado por $h(D)$.

Agora, a ideia é mostrar que, fixado um discriminante D, $h(D)$ é finito. Para isso, considere a aplicação $\mathfrak{Q}_D \to \mathfrak{H}$ que associa a cada forma quadrática $Q \in \mathfrak{Q}_D$ a única raíz

$$\mathfrak{z}_Q = \frac{-B + \sqrt{D}}{2A}$$

de $Q(\mathfrak{z}, 1) = 0$ no semi-plano superior $\mathfrak{H}$ (pois $A > 0$ e $\sqrt{D} = +i\sqrt{|D|}$). O Lema a seguir mostra a relação da aplicação definida acima com a ação de Γ_1 em $\mathfrak{Q}_D$.

Lema 12. *Para toda forma quadrática $Q \in \mathfrak{Q}_D$ e $\gamma \in \Gamma_1$ vale:*

$$\mathfrak{z}_{Q\circ\gamma} = \gamma^{-1}\mathfrak{z}_Q. \tag{5.5}$$

Demonstração. Por definição, $\mathfrak{z}_{Q\circ\gamma}$ é o único zero de $(Q \circ \gamma)(z, 1)$ em $\mathfrak{H}$. Portanto, é suficiente mostrar que temos $(Q \circ \gamma)(\gamma^{-1}\mathfrak{z}_Q, 1) = 0$. Observe que, se $\gamma^{-1} = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$, então

$$\gamma^{-1}\begin{pmatrix}\mathfrak{z}_Q \\ 1\end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix}\mathfrak{z}_Q \\ 1\end{pmatrix} = \begin{pmatrix} a'\mathfrak{z}_Q + b' \\ c'\mathfrak{z}_Q + d' \end{pmatrix} = \underbrace{\frac{1}{c'\mathfrak{z}_Q + d'}}_{\delta(\gamma^{-1},\mathfrak{z}_Q)}\begin{pmatrix}\frac{a'\mathfrak{z}_Q + b'}{c'\mathfrak{z}_Q + d'} \\ 1\end{pmatrix}$$

$$= \frac{1}{\delta(\gamma^{-1}, \mathfrak{z}_Q)}\begin{pmatrix}\gamma^{-1}\mathfrak{z}_Q \\ 1\end{pmatrix}. \tag{5.6}$$

Então, pelas equações (5.4) e (5.6), segue que

$$\begin{aligned}(Q \circ \gamma)(\gamma^{-1}\mathfrak{z}_Q, 1) &= \begin{pmatrix}\gamma^{-1}\mathfrak{z}_Q \\ 1\end{pmatrix}^t \gamma^t M \gamma \begin{pmatrix}\gamma^{-1}\mathfrak{z}_Q \\ 1\end{pmatrix} \\ &= \delta(\gamma^{-1}, \mathfrak{z}_Q)^2 \begin{pmatrix}\mathfrak{z}_Q \\ 1\end{pmatrix}^t {\gamma^{-1}}^t \gamma^t M \gamma\gamma^{-1} \begin{pmatrix}\mathfrak{z}_Q \\ 1\end{pmatrix} \\ &= \delta(\gamma^{-1}, \mathfrak{z}_Q)^2 \begin{pmatrix}\mathfrak{z}_Q \\ 1\end{pmatrix}^t M \begin{pmatrix}\mathfrak{z}_Q \\ 1\end{pmatrix} \\ &= \delta(\gamma^{-1}, \mathfrak{z}_Q)^2 \underbrace{Q(\mathfrak{z}_Q, 1)}_{0} = 0.\end{aligned}$$

□

Sabemos que $\widetilde{\mathcal{F}_1}$ é domínio fundamental estrito para a ação de Γ_1 no semiplano superior $\mathfrak{H}$. O Lema anterior mostra que cada classe de equivalência de $\Gamma_1\backslash\mathfrak{Q}_D$ possui único representante Q no conjunto

$$\mathfrak{Q}_D^{\text{red}} = \{[A, B, C] \in \mathfrak{Q}_D : -A < B \leqslant A < C \text{ ou } 0 \leqslant B \leqslant A = C\} \tag{5.7}$$

para o qual $\mathfrak{z}_Q \in \widetilde{\mathcal{F}_1}$. Um elemento deste conjunto é chamado de *forma quadrática reduzida de discriminante* D.

Proposição 16. *$\mathfrak{Q}_D^{red}$ é um conjunto finito.*

Demonstração. Note que dado $Q = [A, B, C] \in \mathfrak{Q}_D^{\text{red}}$, temos que $C \geqslant A \geqslant |B|$. Uma vez que $D < 0$, segue que

$$|D| = |B^2 - 4AC| = -(B^2 - 4AC) = 4AC - B^2 \geqslant 4AA - A^2 = 3A^2 \implies A \leqslant \sqrt{\frac{|D|}{3}}.$$

Agora, uma vez que $A \geqslant |B|$, o número $\sqrt{\dfrac{|D|}{3}}$ é uma cota superior para ambos A e B. Sendo $C = \dfrac{B^2 - D}{4A}$, vemos que C é limitado também. Como A, B, C são inteiros limitados superiormente, segue que $\mathfrak{Q}_D^{\text{red}}$ é um conjunto finito. □

Observamos que a cota superior $\sqrt{|D|/3}$ dada na demonstração da proposição anterior é extremamente útil para calcular $h(D)$, como faremos no exemplo numérico a seguir:

Exemplo 4. Para ilustrar a construção feita na demonstração da Proposição 16 considere $D = -47$ e seja $[A, B, C] \in \mathfrak{Q}_{-47}^{\text{red}}$ qualquer. Conforme observado anteriormente,

$$|B| \leqslant A \leqslant \sqrt{\frac{|D|}{3}} = \sqrt{\frac{47}{3}} < 4.$$

Em resumo, A, B, C são inteiros tais que

$$|B| \leqslant A < 4 \text{ e } C = \frac{B^2 + 47}{4A}.$$

Com a restrição feita, basta analisarmos os possíveis seguintes casos:

1. Se $A = 3$, então $|B| \leqslant 3$. Se $B = \pm 1$, então

   $$C = \frac{B^2 + 47}{4A} = \frac{1 + 47}{12} = \frac{48}{12} = 4 \in \mathbb{Z}$$

   e, neste caso, $[A, B, C] = [3, \pm 1, 4]$. Por outro lado, se $B = 0$, $B = \pm 2$ ou $B = \pm 3$, temos respectivamente $C = 47/12$, $C = 51/12$ ou $C = 56/12$, os quais não são inteiros. Portanto, as únicas possibilidades para o caso $A = 3$ são $[A, B, C] = [3, \pm 1, 4]$.

2. Se $A = 2$, então $|B| \leqslant 2$. Se $B = \pm 1$, então

   $$C = \frac{B^2 + 47}{4A} = \frac{1 + 47}{8} = \frac{48}{8} = 6 \in \mathbb{Z}$$

   e, neste caso, $[A, B, C] = [2, \pm 1, 6]$. Por outro lado, se $B = 0$ ou $B = \pm 2$, temos respectivamente $C = 47/8$ e $C = 51/8$ que não são inteiros. Portanto, as únicas possibilidades para o caso $A = 2$ são $[A, B, C] = [2, \pm 1, 6]$.

3. Se $A = 1$, então $B = 1$ ou $B = 0$. Se $B = 1$,

$$C = \frac{B^2 + 47}{4A} = \frac{1 + 47}{4} = \frac{48}{4} = 12 \in \mathbb{Z}.$$

Neste caso $[A, B, C] = [1, 1, 12]$. Agora se $B = 0$, então $C = 47/4 \notin \mathbb{Z}$, e este caso não ocorre.

Portanto, $\mathfrak{Q}_{-47}^{\text{red}} = \{[1, 1, 12], [2, \pm 1, 6], [3, \pm 1, 4]\}$ e consequentemente $h(-47) = 5$.

5.1.1 O Problema do Número de Classe de Gauss

O Problema do Número de Classe de Gauss se trata de exibir para cada inteiro $n \geqslant 1$ uma lista completa de corpos quadráticos imaginários $\mathbb{Q}(\sqrt{D})$, onde D é um número inteiro negativo que possui número de classe $h(D) = n$. Originalmente, *Carl Friedrich Gauss* conjecturou em 1801 que $h(D) \to \infty$ conforme $D \to -\infty$. Essa conjectura foi provada por *Heilbronn(1934)* e *Siegel(1936).*

Para o caso do número de classe 1, temos o Teorema de Baker-Heegner-Stark, que estabelece uma lista completa de corpos quadráticos imaginários $\mathbb{Q}(\sqrt{D})$ para os quais $h(D) = 1$, ou seja, todos os corpos quadráticos imaginários para os quais o correspondente anel dos inteiros é um domínio de fatoração única. Os números desta lista são chamados de *números de Heegner* e, neste sentido, determiná-los é um caso particular do problema do número de classe de Gauss. Esta terminologia é devida a Heegner, que essencialmente provou o resultado em 1952, apesar de sua demonstração não ter sido aceita devido à algumas falhas. Em 1971, *Baker* e *Stark* fornerceram uma demontração apresentando a lista completa de discriminantes D tais que $h(D) = 1$. Os números de Heegner são, precisamente:

$$-3, -4, -7, -8, -11, -19, -43, -67 \text{ e } -163.$$

Embora a demonstração deste resultado envolva muitos conceitos da teoria de formas modulares, ela foge do escopo deste trabalho e, por isto, não será feita. Nesta seção, vamos verificar que esses números possuem número de classe igual a 1 utilizando a construção dada na demonstração da proposição 16.

No contexto dos valores especiais de j, veremos que se $\mathfrak{z} \in \mathfrak{H}$ é um ponto CM de discriminante D, então o valor especial $j(\mathfrak{z})$ é um inteiro algébrico de grau $h(D)$. O Teorema de Baker-Heegner-Stark nos garante que $j(\mathfrak{z})$ é um número inteiro, para todo ponto CM $\mathfrak{z} \in \mathfrak{H}$ de discriminante igual a algum dos números de Heegner, pois será um inteiro algébrico de grau 1.

- $D = -3$

  Sabemos que se $[A, B, C] \in \mathfrak{Q}_{-3}^{\text{red}}$, então $|B| \leqslant A \leqslant \sqrt{|D|/3} = 1$. Uma vez que $A > 0$,

a única possibilidade seria $A = 1$. Agora, $B = 0$ ou $B = 1$. O primeiro caso não ocorre, pois teríamos $C = -D/4A = 3/4 \notin \mathbb{Z}$. Para o segundo caso,

$$C = \frac{B^2 - D}{4A} = \frac{4}{4} = 1 \in \mathbb{Z},$$

e temos $\mathfrak{Q}_{-3}^{\text{red}} = \{[1, 1, 1]\}$. Portanto, $h(-3) = 1$.

- $D = -4$
  Se $[A, B, C] \in \mathfrak{Q}_{-4}^{\text{red}}$, segue que $|B| \leqslant A \leqslant \sqrt{|-4|/3} < 2$. Como $0 < A < 2$, devemos ter necessariamente $A = 1$. Uma vez que $|B| \leqslant A = 1$, temos que $B = 1$ ou $B = 0$. Veja que este primeiro caso não ocorre, pois teríamos

  $$C = \frac{B^2 - D}{4A} = \frac{1 + 4}{4} = \frac{5}{4} \notin \mathbb{Z}.$$

  Portanto, $B = 0$ e $C = -D/4A = 1$. Dessa forma, $\mathfrak{Q}_{-4}^{\text{red}} = \{[1, 0, 1]\}$ e $h(-4) = 1$.

- $D = -7$
  Tomando $[A, B, C] \in \mathfrak{Q}_{-7}^{\text{red}}$, temos $|B| \leqslant A \leqslant \sqrt{|D|/3} = \sqrt{7/3} < 2$. Sendo $A > 0$, temos $A = 1$. Agora, se $B = 0$, então $C = -D/4A = 7/4 \notin \mathbb{Z}$, e portanto este caso não ocorre. Se $B = 1$, então $C = (B^2 - D)/4A = (1 + 7)/4 = 2 \in \mathbb{Z}$. Portanto, $\mathfrak{Q}_{-7}^{\text{red}} = \{[1, 1, 2]\}$ e $h(-7) = 1$.

- $D = -8$
  Se $[A, B, C] \in \mathfrak{Q}_{-8}^{\text{red}}$, temos $|B| \leqslant A < \sqrt{|-8|/3} < 3$. Temos dois casos a considerar:

  – Se $A = 1$, então $|B| \leqslant A$ implica $B = 1$ ou $B = 0$. Daí, se $B = 1$

  $$C = \frac{B^2 - D}{4A} = \frac{9}{4} \notin \mathbb{Z},$$

  e, portanto, este caso não ocorre. Se $B = 0$, então

  $$C = \frac{B^2 - D}{4A} = \frac{8}{4} = 2 \in \mathbb{Z},$$

  e temos $[1, 0, 2] \in \mathfrak{Q}_{-8}^{\text{red}}$.

  – Se $A = 2$, então $|B| \leqslant A$ implica $B = 1$, $B = 2$ ou $B = 0$. Similarmente, vemos que o primeiro caso não ocorre, pois teríamos $C = 9/8 \notin \mathbb{Z}$. Para o segundo caso, teríamos $C = 12/8 \notin \mathbb{Z}$. Por fim, para o terceiro caso, teríamos

  $$C = \frac{B^2 - D}{4A} = \frac{8}{8} = 1 \in \mathbb{Z},$$

  e logo $[2, 0, 1] \in \mathfrak{Q}_{-8}^{\text{red}}$. No entanto, as formas quadráticas reduzidas devem respeitar $C \geqslant A$, e consequentemente este caso não ocorre.

  Portanto, $\mathfrak{Q}_{-8}^{\text{red}} = \{[1, 0, 2]\}$ e $h(-8) = 1$.

- $D = -11$
  Tomando $[A, B, C] \in \mathfrak{Q}_{-11}^{\text{red}}$, temos $|B| \leqslant A \leqslant \sqrt{|D|/3} = \sqrt{11/3} < 2$. Sendo $A > 0$, temos $A = 1$. Agora, se $B = 0$ então $C = -D/4A = 11/4 \notin \mathbb{Z}$, e portanto este caso não ocorre. Se $B = 1$, então $C = (B^2 - D)/4A = (1 + 11)/4 = 3 \in \mathbb{Z}$. Portanto, $\mathfrak{Q}_{-11}^{\text{red}} = \{[1, 1, 3]\}$ e $h(-11) = 1$.

- $D = -19$
  Tomando $[A, B, C] \in \mathfrak{Q}_{-19}^{\text{red}}$, temos $|B| \leqslant A \leqslant \sqrt{|D|/3} = \sqrt{19/3} < 3$. Sendo $A > 0$, temos $A = 1$ ou $A = 2$.

  – Se $A = 1$, então $|B| \leqslant A$ implica $B = 0$ ou $B = 1$. Daí, se $B = 0$

  $$C = \frac{B^2 - D}{4A} = \frac{19}{4} \notin \mathbb{Z},$$

  e, portanto, este caso não ocorre. Se $B = 1$, então

  $$C = \frac{B^2 - D}{4A} = \frac{1 + 19}{4} = 5 \in \mathbb{Z},$$

  e temos $[1, 1, 5] \in \mathfrak{Q}_{-19}^{\text{red}}$.

  – Se $A = 2$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$ ou $B = 2$. Similarmente, vemos que o primeiro caso não ocorre, pois teríamos $C = 19/8 \notin \mathbb{Z}$. Para o segundo caso, teríamos $C = 20/8 \notin \mathbb{Z}$. Por fim, o terceiro caso também não ocorre, pois

  $$C = \frac{B^2 - D}{4A} = \frac{4 + 19}{8} = \frac{23}{8} \notin \mathbb{Z}.$$

  Portanto, $\mathfrak{Q}_{-19}^{\text{red}} = \{[1, 1, 5]\}$ e $h(-19) = 1$.

- $D = -43$
  Tomando $[A, B, C] \in \mathfrak{Q}_{-43}^{\text{red}}$, temos $|B| \leqslant A \leqslant \sqrt{|D|/3} = \sqrt{43/3} < 4$. Sendo $A > 0$, temos $A = 1$, $A = 2$ ou $A = 3$.

  – Se $A = 1$, então $|B| \leqslant A$ implica $B = 0$ ou $B = 1$. Daí, se $B = 0$,

  $$C = \frac{B^2 - D}{4A} = \frac{43}{4} \notin \mathbb{Z},$$

  e, portanto, este caso não ocorre. Se $B = 1$, então

  $$C = \frac{B^2 - D}{4A} = \frac{1 + 43}{4} = 11 \in \mathbb{Z},$$

  e temos $[1, 1, 11] \in \mathfrak{Q}_{-43}^{\text{red}}$.

  – Se $A = 2$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$ ou $B = 2$. Similarmente, vemos que o primeiro caso não ocorre pois teríamos $C = 43/8 \notin \mathbb{Z}$. Para o segundo caso, teríamos $C = 44/8 \notin \mathbb{Z}$. Por fim, o terceiro caso também não ocorre, pois

  $$C = \frac{B^2 - D}{4A} = \frac{4 + 43}{8} = \frac{47}{8} \notin \mathbb{Z}.$$

– Se $A = 3$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$, $B = 2$ ou $B = 3$. Nenhum destes casos ocorrem, pois teríamos, respectivamente, $C = 43/12 \notin \mathbb{Z}$, $C = 44/12$, $C = 47/12$ e $C = 52/12$, e nenhum destes números é inteiro.

Portanto, $\mathfrak{Q}_{-43}^{\text{red}} = \{[1, 1, 11]\}$ e $h(-19) = 1$.

- $D = -67$
  Tomando $[A, B, C] \in \mathfrak{Q}_{-67}^{\text{red}}$, temos $|B| \leqslant A \leqslant \sqrt{|D|/3} = \sqrt{67/3} < 5$. Sendo $A > 0$, temos $A = 1$, $A = 2$, $A = 3$ ou $A = 4$.

  – Se $A = 1$, então $|B| \leqslant A$ implica $B = 0$ ou $B = 1$. Daí, se $B = 0$, temos $C = 67/4 \notin \mathbb{Z}$ e, portanto, este caso não ocorre. Se $B = 1$, então
  $$C = \frac{B^2 - D}{4A} = \frac{1 + 67}{4} = 17 \in \mathbb{Z},$$
  e temos $[1, 1, 17] \in \mathfrak{Q}_{-67}^{\text{red}}$.

  – Se $A = 2$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$ ou $B = 2$. Similarmente, vemos que o primeiro caso não ocorre, pois teríamos $C = 67/8 \notin \mathbb{Z}$. Para o segundo caso, teríamos $C = 68/8 \notin \mathbb{Z}$. Por fim, o terceiro caso também não ocorre, pois $C = 71/8 \notin \mathbb{Z}$. Logo, A não pode ser 2.

  – Se $A = 3$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$, $B = 2$ ou $B = 3$. Nenhum destes casos ocorrem, pois teríamos, respectivamente, $C = 67/12 \notin \mathbb{Z}$, $C = 68/12$, $C = 71/12$ e $C = 76/12$, e nenhum destes números é inteiro.

  – Se $A = 4$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$, $B = 2$, $B = 3$ ou $B = 4$. Nenhum destes casos ocorrem, pois teríamos, respectivamente, $C = 67/16 \notin \mathbb{Z}$, $C = 68/16$, $C = 71/16$, $C = 76/16$ e $C = 83/16$, mas nenhum destes números é inteiro.

  Portanto, $\mathfrak{Q}_{-67}^{\text{red}} = \{[1, 1, 17]\}$ e $h(-67) = 1$.

- $D = -163$
  Tomando $[A, B, C] \in \mathfrak{Q}_{-163}^{\text{red}}$, temos $|B| \leqslant A \leqslant \sqrt{|D|/3} = \sqrt{163/3} < 8$. Sendo $A > 0$, temos $A = 1, 2, 3, 4, 5, 6$ ou 7.

  – Se $A = 1$, então $|B| \leqslant A$ implica $B = 0$ ou $B = 1$. Daí, se $B = 0$, temos $C = 163/4 \notin \mathbb{Z}$ e, portanto, este caso não ocorre. Se $B = 1$, então
  $$C = \frac{B^2 - D}{4A} = \frac{1 + 163}{4} = 41 \in \mathbb{Z},$$
  e temos $[1, 1, 41] \in \mathfrak{Q}_{-163}^{\text{red}}$.

  – Se $A = 2$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$ ou $B = 2$. Similarmente, vemos que o primeiro caso não ocorre, pois teríamos $C = 163/8 \notin \mathbb{Z}$. Para o segundo caso, teríamos $C = 164/8 \notin \mathbb{Z}$. Por fim, o terceiro caso também não ocorre, pois $C = 167/8 \notin \mathbb{Z}$. Logo, A não pode ser 2.

– Se $A = 3$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$, $B = 2$ ou $B = 3$. Nenhum destes casos ocorrem, pois teríamos, respectivamente, $C = 163/12$, $C = 164/12$, $C = 167/12$ e $C = 172/12$, e nenhum destes números é inteiro.

– Se $A = 4$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$, $B = 2$, $B = 3$ ou $B = 4$. Nenhum destes casos ocorrem, pois teríamos, respectivamente, $C = 163/16$, $C = 164/16$, $C = 167/16$, $C = 172/16$ e $C = 179/16$, mas nenhum destes números é inteiro.

– Se $A = 5$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$, $B = 2$, $B = 3$, $B = 4$ ou $B = 5$. Nenhum destes casos ocorrem, pois teríamos, respectivamente, $C = 163/20$, $C = 164/20$, $C = 167/20$, $C = 172/20$, $C = 179/20$ e $C = 188/20$, mas nenhum destes números é inteiro.

– Se $A = 6$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$, $B = 2$, $B = 3$, $B = 4$, $B = 5$ ou $B = 6$. Nenhum destes casos ocorrem, pois teríamos, respectivamente, $C = 163/24$, $C = 164/24$, $C = 167/24$, $C = 172/24$, $C = 179/24$, $C = 188/24$ e $C = 199/24$, mas nenhum destes números é inteiro.

– Se $A = 7$, então $|B| \leqslant A$ implica $B = 0$, $B = 1$, $B = 2$, $B = 3$, $B = 4$, $B = 5$, $B = 6$ ou $B = 7$. Nenhum destes casos ocorrem, pois teríamos, respectivamente, $C = 163/28$, $C = 164/28$, $C = 167/28$, $C = 172/28$, $C = 179/28$, $C = 188/28$, $C = 199/28$ e $C = 212/28$, mas nenhum destes números é inteiro.

Portanto, $\mathfrak{Q}_{-163}^{\text{red}} = \{[1, 1, 41]\}$ e $h(-163) = 1$.

5.2 O Polinômio de Classes H_D

Na Seção 5.1, associamos a cada discriminante $D < 0$ o conjunto $\mathfrak{Q}_D$ das formas quadráticas binárias positivas definidas de discriminante D, e a cada forma quadrática $Q \in \mathfrak{Q}_D$ associamos o único zero $\mathfrak{z}_Q$ de $Q(z, 1) = 0$ no semiplano superior $\mathfrak{H}$. Denotando por $\mathfrak{Z}_D \subset \mathfrak{H}$ o subconjunto de $\mathfrak{H}$ dos pontos CM com discriminante D, fica bem definido o mapa:

$$\begin{aligned} \varphi_D \colon \mathfrak{Q}_D &\to \mathfrak{Z}_D \subset \mathfrak{H} \\ Q &\mapsto \mathfrak{z}_Q \end{aligned}$$

Este mapa é uma bijeção: de fato, a injetividade segue por definição, já que para toda forma quadrática $Q \in \mathfrak{Q}_D$ associamos um único ponto $\mathfrak{z}_Q$ em $\mathfrak{Z}_D \subset \mathfrak{H}$. Para a sobrejetividade, basta observar que um ponto CM $\mathfrak{z} \in \mathfrak{Z}_D$ de discriminante D satisfaz uma equação quadrática $A\mathfrak{z}^2 + B\mathfrak{z} + C = 0$ de discriminante D, em que $A > 0$ e $D < 0$, pois $\mathfrak{z}$ é um ponto quadrático no semiplano superior. Considerando a forma quadrática $Q(x, y) = Ax^2 + Bxy + Cy^2$, que podemos assumir ser primitiva (caso não for, basta dividi-la por

$\mathrm{mdc}(A,B,C)$), segue que $\mathfrak{z}$ é o único zero de $Q(z,1)=0$, e, portanto, $\varphi_D(Q)=\mathfrak{z}$, como queríamos. Mais ainda, φ_D é Γ_1-equivariante. De fato, recorde que Γ_1 age em $\mathfrak{Q}_D$ via a aplicação

$$\begin{aligned}\mathfrak{Q}_D\times\Gamma_1&\to\mathfrak{Q}_D\\(Q,\gamma)&\mapsto Q\circ\gamma\end{aligned}$$

Então, dados $\gamma\in\Gamma_1$ e $Q\in\mathfrak{Q}_D$, temos, pelo Lema 12:

$$\varphi_D(Q\circ\gamma)=\mathfrak{z}_{Q\circ\gamma}=\gamma^{-1}\mathfrak{z}_Q=\gamma^{-1}\varphi_D(Q),$$

mostrando a Γ_1-equivariância da aplicação φ_D.

O fato de que a aplicação $\varphi_D\colon\mathfrak{Q}_D\to\mathfrak{Z}_D\subset\mathfrak{H}$ é uma bijeção Γ_1-equivariante nos permite dizer qual é a cardinalidade do quociente $\Gamma_1\backslash\mathfrak{Z}_D$. Vimos na Seção 5.1 que $\mathfrak{Q}_D^{\mathrm{red}}$ é um sistema de representantes para $\Gamma_1\backslash\mathfrak{Q}_D$ e possui cardinalidade $h(D)$. Logo,

$$|\Gamma_1\backslash\mathfrak{Z}_D|=|\Gamma_1\backslash\mathfrak{Q}_D|=|\mathfrak{Q}_D^{\mathrm{red}}|=h(D).$$

Em particular, podemos escolher um conjunto de representantes $\{\mathfrak{z}_{D,i}\}_{1\leqslant i\leqslant h(D)}$ para o quociente $\Gamma_1\backslash\mathfrak{Z}_D$, onde $\mathfrak{z}_{D,1}=\mathfrak{z}_D$. Na realidade, estes pontos pertecem ao subconjunto $\mathfrak{Z}_D\cap\widetilde{\mathcal{F}_1}$ do domínio fundamental estrito $\widetilde{\mathcal{F}_1}$ para a ação de Γ_1 em $\mathfrak{H}$, e as respectivas formas quadráticas associadas aos zeros $\mathfrak{z}_{D,i}$ são elementos de $\mathfrak{Q}_D^{\mathrm{red}}$. Neste contexo, dado um discriminante $D<0$, definimos o *Polinômio de Classe* H_D:

$$H_D(X)=\prod_{\mathfrak{z}\in\Gamma_1\backslash\mathfrak{Z}_D}(X-j(\mathfrak{z}))=\prod_{1\leqslant i\leqslant h(D)}(X-j(\mathfrak{z}_{D,i}))\,. \tag{5.8}$$

Vamos provar que o polinômio de classes H_D possui coeficientes inteiros e é irredutível. Isto mostra que o número $j(\mathfrak{z}_D)$ é algébrico de grau $h(D)$ sobre $\mathbb{Q}$, com conjugados $j(\mathfrak{z}_{D,i})$, para $1<i\leqslant h(D)$. Para tanto, vamos provar alguns resultados auxiliares.

Sabemos que, se $\mathfrak{z}_D\in\mathfrak{H}$ é um ponto CM de discriminante D, existe $m\in\mathbb{N}$ e uma matriz $M\in M(2,\mathbb{Z})$ de determinante m tal que $M\mathfrak{z}_D=\mathfrak{z}_D$. A Proposição 13 garante $j(\mathfrak{z}_D)$ é raíz do polinômio $\Psi_m(X,X)\in\mathbb{Z}[X]$. Associamos a cada ponto CM $\mathfrak{z}_D\in\mathfrak{H}$ o conjunto dos determinantes $m=\det M$ das matrizes $M\in M(2,\mathbb{Z})$ que fixam $\mathfrak{z}_D$:

$$m(\mathfrak{z}_D)=\{m\in\mathbb{Z}:m=\det M,\ \text{onde } M\in M(2,\mathbb{Z}) \text{ satisfaz } M\mathfrak{z}_D=\mathfrak{z}_D\}.$$

Por exemplo, vamos calcular $m(i)$. Seja $M=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in M(2,\mathbb{Z})$ fixando i. Então,

$$\begin{aligned}Mi=i&\iff\frac{ai+b}{ci+d}=i\iff ai+b=di-c\iff a=d\text{ e }b=-c\\&\iff M=\begin{pmatrix}a&b\\-b&a\end{pmatrix}.\end{aligned}$$

Logo, $\det M = a^2 + b^2$ e, portanto, $m(i) = \{m \in \mathbb{Z} : m = a^2 + b^2\}$.

O fato é que, se $\mathfrak{z}_D$ é um ponto CM, o conjunto $m(\mathfrak{z}_D)$ depende apenas do discriminante D, e não do ponto $\mathfrak{z}_D$. Provaremos isto no seguinte lema.

Lema 13. *Seja $\mathfrak{z}_D$ um ponto CM de discriminante D. Então, o conjunto $m(\mathfrak{z}_D)$ depende apenas de D. Mais precisamente,*

$$m(\mathfrak{z}_D) = \left\{ \frac{1}{4}(t^2 - Du^2) : t, u \in \mathbb{Z} \text{ e } t \equiv Du \bmod 2 \right\}.$$

Demonstração. Seja $m \in m(\mathfrak{z}_D)$ e $M \in M(2, \mathbb{Z})$ a respectiva matriz de determinante m que fixa $\mathfrak{z}_D$. Isso implica que podemos obter uma equação quadrática satisfeita por $\mathfrak{z}_D$, a saber:

$$M \cdot \mathfrak{z}_D = \mathfrak{z}_D \implies \frac{a\mathfrak{z}_D + b}{c\mathfrak{z}_D + d} = \mathfrak{z}_D \implies c\mathfrak{z}_D^2 + (d-a)\mathfrak{z}_D - b = 0.$$

Por outro lado, $\mathfrak{z}_D$ satisfaz seu polinômio minimal $Az^2 + Bz + C$ de discriminante D. Logo, o polinômio minimal de $\mathfrak{z}_D$ divide o polinômio $cz^2 + (d-a)z - b$, isto é, existe $u \in \mathbb{Z}$ tal que $(c, d-a, -b) = u(A, B, C)$. Dessa forma, podemos reescrever a matriz M em função dos coeficientes A, B e C:

$$M = \begin{pmatrix} \frac{1}{2}(t - Bu) & -Cu \\ Au & \frac{1}{2}(t + Bu) \end{pmatrix}, \text{ onde } t = trM = a + d. \tag{5.9}$$

De fato, veja que vale a igualdade dos coeficientes:

- $\frac{1}{2}(t - Bu) = \frac{1}{2}\left(a + d - \left(\frac{d-a}{u}\right)u\right) = a.$
- $-Cu = -(-b/u)u = b.$
- $Au = (c/u)u = c$
- $\frac{1}{2}(t + Bu) = \frac{1}{2}\left(a + d + \left(\frac{d-a}{u}\right)u\right) = d.$

E, além disso, como $D = B^2 - 4AC$, temos

$$\det M = \frac{t^2 - Du}{4} = \frac{(a+d)^2 - \left(\left(\frac{d-a}{u}\right)^2 - 4\frac{c(-b)}{u^2}u^2\right)}{4} = ad - bc.$$

A recíproca deste fato também é verdadeira, isto é, se temos $t, u \in \mathbb{Z}$ satisfazendo $t^2 - Du^2 = 4m$, a expressão 5.9 nos fornece uma matriz $M \in M(2, \mathbb{Z})$ de determinante m fixando $\mathfrak{z}_D$. De fato, vejamos primeiramente que as entradas da matriz são inteiras. Imediatamente, temos $Au, -Cu \in \mathbb{Z}$. Para as outras duas entradas, considere $x = t - Bu$ e $y = t + Bu$. Por um lado, a expressão

$$\begin{aligned} xy &= (t - Bu)(t + Bu) = t^2 - B^2u^2 = t^2 - (D + 4AC)u^2 = (t^2 - Du^2) - 4ACu^2 \\ &= 4m - 4ACu^2 = 4(m - ACu^2) \end{aligned}$$

nos mostra que x é par ou y é par. Por outro lado, a expressão $x - y = -2Bu$ nos mostra que x e y possuem a mesma paridade. Logo, x e y são pares, e portanto os coeficientes $\frac{1}{2}(t - Bu)$ e $\frac{1}{2}(t + Bu)$ são inteiros. Além disso, já sabemos que M fixa $\mathfrak{z}_D$ e, por fim,

$$\det M = \frac{t^2 - Du^2}{4} = \frac{4m}{4} = m.$$

Portanto,

$$m(\mathfrak{z}_D) = \left\{ \frac{1}{4}(t^2 - Du^2) : t, u \in \mathbb{Z} \text{ e } t \equiv Du \bmod 2 \right\}.$$

A igualdade entre esses conjuntos garante que o conjunto $m(\mathfrak{z}_D)$ depende apenas do discriminante D. □

Observação 16. Na realidade, o conjunto $m(\mathfrak{z}_D)$ é igual ao conjunto das normas de elementos da ordem quadrática

$$\mathcal{O}_D = \left\{ \frac{t + u\sqrt{D}}{2} : t, u \in \mathbb{Z} \text{ e } t \equiv Du \bmod 2 \right\}.$$

De fato, se $\dfrac{t + u\sqrt{D}}{2}$ é um elemento qualquer de $\mathcal{O}_D$, então

$$\left| \frac{t + u\sqrt{D}}{2} \right| = \left(\frac{t + u\sqrt{D}}{2} \right) \left(\frac{t - u\sqrt{D}}{2} \right) = \frac{1}{4}(t^2 - Du^2) \in m(\mathfrak{z}_D).$$

Corolário 7. *Sejam $\mathfrak{z}, \mathfrak{z}' \in \mathfrak{H}$ pontos CM de um mesmo discriminante D. Então, $m(\mathfrak{z}) = m(\mathfrak{z}')$.*

O Corolário acima nos mostra que pontos CM de mesmo discriminante D possuem o mesmo conjunto de possíveis determinantes de matrizes que os fixam. Neste sentido, podemos denotar $m(D)$ para nos referir ao conjunto $m(\mathfrak{z}_D)$, em que $\mathfrak{z}_D$ é qualquer ponto CM de discriminante D.

Proposição 17. *O polinômio de classes H_D possui coeficientes inteiros e é irredutível. Em particular, o número $j(\mathfrak{z}_D)$ é algébrico de grau $h(D)$ sobre $\mathbb{Q}$, com conjugados $j(\mathfrak{z}_{D,i})$, para $1 \leqslant i \leqslant h(D)$.*

Demonstração. A versão da demonstração que apresentaremos aqui apenas indica os principais passos da construção deste resultado, conforme apresentado em [3], na página 72. A razão para isto é que uma prova completa — como em [7], na página 286 — envolve conceitos que fogem ao escopo deste trabalho, como, por exemplo, uma quantidade relevante de pré-requisitos a respeito da aritmética de curvas elípticas com multiplicação complexa e teoria de corpos de classes de aneis de inteiros quadráticos. Desta forma, omitiremos detalhes mais específicos da demonstração desta proposição.

A Proposição 13 nos diz que $j(\mathfrak{z})$ é raíz da equação modular $\Psi_m(X, X) = 0$, para todo m que é o determinante de uma matriz $M \in M(2, \mathbb{Z})$ fixando o ponto CM $\mathfrak{z}$, ou seja, a princípio, $j(\mathfrak{z})$ é raíz de uma infinidade de polinômios $\Psi_m(X, X)$. No entanto, note que se α é uma raíz de Ψ_m, então α é necessariamente igual a algum $j(\mathfrak{z})$, em que $\mathfrak{z}$ é fixo por uma matrix $M \in M(2, \mathbb{Z})$ de determinante m. De fato, se α é uma raíz de $\Psi(X, X)$, então $\alpha = j(\mathfrak{z})$, para um único $\mathfrak{z}$ no domínio fundamental $\widetilde{\mathcal{F}_1}$. Daí,

$$\Psi(j(\mathfrak{z}), j(\mathfrak{z})) = \prod_{M \in \mathcal{M}_m^*} j(\mathfrak{z}) - j(M\mathfrak{z}) = 0 \iff \exists M \in \mathcal{M}_m^* : j(\mathfrak{z}) = j(M\mathfrak{z}).$$

Como $j \colon \Gamma_1 \backslash \mathfrak{H} \to \mathbb{C}$ é uma bijeção, segue que existe $\gamma \in \Gamma_1$ para o qual $\mathfrak{z} = \gamma M \mathfrak{z}$. De toda forma, γM ainda é uma matrix de determinante m fixando o ponto $\mathfrak{z}$.

O ponto principal dessa demonstração é que m depende apenas do discriminante de $\mathfrak{z}$, e não do ponto $\mathfrak{z}$ em si, fato que provamos no Lema 13. Desta forma, como os pontos $\{\mathfrak{z}_{D,i}\}$, para $1 \leqslant i \leqslant h(D)$, são todos pontos CM de discriminante D, sabemos que os conjuntos $m(\mathfrak{z}_{D,i})$ são iguais e, portanto, os valores especiais $j(\mathfrak{z}_{D,i})$ são raízes comuns de todos os polinômios $\Psi_m(X, X)$, em que $m \in m(D)$, isto é, o conjunto de normas de elementos da ordem quadrática $\mathcal{O}_D$. Desta forma, a ideia para obter o polinômio $H_D(X)$ é considerar o mdc de finitos polinômios $\Psi_m(X, X)$, para $m \in m(D)$.

Observamos que este argumento apenas mostra que $H_D(X)$ tem coeficientes racionais. A irredutibilidade deste polinômio é provada usualmente utilizando a aritmética das correspondentes curvas elípticas com multiplicação complexa, no sentido de que a condição de uma curva elíptica admitir multiplicação complexa é puramente algébrica e é, portanto, preservada por conjugações de Galois. Mas, conforme mencionamos inicialmente, nossa ênfase está nos métodos aritméticos do polinômio $H_D(X)$, e portanto omitiremos estes detalhes. □

A intuição da demonstração da proposição anterior nos mostra que os polinômios $H_D(X)$ são fatores dos polinômios $\Psi_m(X, X)$, para $m \in m(D)$. A fórmula explícita que descreve essa relação é devida a *Kronecker*, e é dada por:

$$\Psi_m(X, X) = \pm \prod_{D<0} H_D(X)^{r_D(m)/\omega(D)} \text{ , } m \in \mathbb{N} \text{ e } m \neq a^2 \text{ , para todo } a \in \mathbb{Z}, \tag{5.10}$$

onde $r_D(m) = \left|\{(t, u) \in \mathbb{Z}^2 : t^2 - Du^2 = 4m\}\right| = |\{\lambda \in \mathcal{O}_D : N(\lambda) = m\}|$, e $\omega(D)$ é o número de unidades na ordem quadrática $\mathcal{O}_D$.

Veja que o produto em 5.10 está bem definido (é finito), pois se $r_D(m)$ for não nulo, como m não é um quadrado, temos $4m = t^2 - u^2 D \geqslant |D|$, ou seja, $|D| \leqslant 4m$ implica que $r_D(m) = 0$, para todo $|D| > 4m$ e, portanto, teremos um número finito de parcelas no produto em 5.10. Observamos que a cota superior $|D| \leqslant 4m$ é extremamente útil para o cálculo dos polinômios modulares. Além disso, com respeito ao número de unidades na

ordem quadrática $\mathcal{O}_{\mathcal{D}}$, temos a seguinte caracterização:

$$\omega(D) = \begin{cases} 6 \text{ , se } D = -3 \\ 4 \text{ , se } D = -4 \\ 2 \text{ , caso contrário} \end{cases} \tag{5.11}$$

Observação 17. O caso mais simples para determinar os polinômios de classes $H_D(X)$ é quando o discriminante $D < 0$ possui número de classe $h(D) = 1$, já que nestes casos existe apenas um ponto $\mathfrak{z}_D$ em $\mathfrak{Z}_D \cap \widetilde{\mathcal{F}_1}$. Nestes casos, $H_D(X)$ é o monômio

$$H_D(X) = X - j(\mathfrak{z}_D).$$

Na seção 5.1.1 vimos todos os valores de $D < 0$ com $h(D) = 1$, como, por exemplo: $-3, -4, -7, -8, -11$ e -12. Podemos então considerar a Tabela 2 e já obter alguns polinômios $H_D(X)$:

$$\begin{aligned} H_{-3}(X) &= X - \mathfrak{z}_{-3} = X, \\ H_{-4}(X) &= X - \mathfrak{z}_{-4} = X - 1728, \\ H_{-7}(X) &= X - \mathfrak{z}_{-7} = X + 3375, \\ H_{-8}(X) &= X - \mathfrak{z}_{-8} = X - 8000, \\ H_{-11}(X) &= X - \mathfrak{z}_{-11} = X + 32768, \\ H_{-12}(X) &= X - \mathfrak{z}_{-12} = X - 54000. \end{aligned}$$

Exemplo 5. Vamos obter os polinômios modulares Ψ_2 e Ψ_3 através da fórmula de Kronecker dada em 5.10. Para Ψ_2, temos $|D| \leqslant 4m = 8$. Então, o conjunto de possíveis valores para o discriminante D é $\{-3, -4, -7, -8\}$, já que estamos considerando os discriminantes fundamentais negativos, isto é, inteiros negativos congruentes a 0 e 1 módulo 4. Calculemos primeiramente os valores $r_D(m)$:

$$\begin{aligned} r_{-3}(2) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 3u^2 = 8\}\right| = 0, \\ r_{-4}(2) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 4u^2 = 8\}\right| = |\{(\pm 2, \pm 1)\}| = 4, \\ r_{-7}(2) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 7u^2 = 8\}\right| = |\{(\pm 1, \pm 1)\}| = 4, \\ r_{-8}(2) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 8u^2 = 8\}\right| = |\{(0, \pm 1)\}| = 2. \end{aligned}$$

Além disso, como $\omega(-3) = 6, \omega(-4) = 4$ e $\omega(-7) = \omega(-8) = 2$, segue que

$$\begin{aligned} \Psi_2(X, X) &= \pm \left(H_{-4}(X)^{\frac{r_{-4}(2)}{\omega(-4)}}\right)\left(H_{-7}(X)^{\frac{r_{-7}(2)}{\omega(-7)}}\right)\left(H_{-8}(X)^{\frac{r_{-8}(2)}{\omega(-8)}}\right) \\ &= \pm H_{-4}(X) H_{-7}(X)^2 H_{-8}(X). \end{aligned}$$

Note que, substituindo os valores de $H_D(X)$ obtidos na Observação 17, vemos que

$$\Psi_2(X, X) = -(X - 8000)(X + 3375)^2(X - 1728),$$

confirmando o valor obtido na equação (4.18).

Agora, para Ψ_3, temos $|D| \leqslant 4m = 12$ e, portanto, o conjunto dos discriminantes fundamentais possíveis é $\{-3, -4, -7, -8, -11, -12\}$. Logo,

$$\begin{aligned}
r_{-3}(3) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 3u^2 = 12\}\right| = |\{(\pm 3, \pm 1), (0, \pm 2)\}| = 6,\\
r_{-4}(3) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 4u^2 = 12\}\right| = 0,\\
r_{-7}(3) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 7u^2 = 12\}\right| = 0,\\
r_{-8}(3) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 8u^2 = 12\}\right| = |\{(\pm 2, \pm 1)\}| = 4,\\
r_{-11}(3) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 11u^2 = 12\}\right| = |\{(\pm 1, \pm 1)\}| = 4,\\
r_{-12}(3) &= \left|\{(t,u) \in \mathbb{Z}^2 : t^2 + 12u^2 = 12\}\right| = |\{(0, \pm 1)\}| = 2.
\end{aligned}$$

Sabendo que $\omega(-11) = \omega(-12) = 2$, segue que

$$\begin{aligned}
\Psi_3(X,X) &= \pm \left(H_{-3}(X)^{\frac{r_{-3}(3)}{\omega(-3)}}\right)\left(H_{-8}(X)^{\frac{r_{-8}(3)}{\omega(-8)}}\right)\left(H_{-11}(X)^{\frac{r_{-11}(3)}{\omega(-11)}}\right)\left(H_{-12}(X)^{\frac{r_{-12}(3)}{\omega(-12)}}\right)\\
&= \pm H_{-3}(X)H_{-8}(X)^2H_{-11}(X)^2H_{-12}(X).
\end{aligned}$$

Substituindo os valores de $H_D(X)$ vistos na Observação 17, vemos que

$$\Psi_3(X,X) = -X(X - 8000)^2(X + 32768)^2(X - 54000).$$

Este valor confirma o valor obtido em [7], na página 291.

5.3 Aplicação: Teoria de Corpos de Classe Explícita para Corpos Quadráticos Imaginários

A Teoria de Corpos de Classe é um dos temas mais relevantes da Teoria Algébrica dos Números. Essencialmente, ela se concentra em fornecer uma classificação completa de todas as extensões abelianas de um dado corpo de números K. Em particular, ela mostra que as extensões abelianas não-ramificadas de K serão subcorpos de uma extensão finita H/K, chamada de *Corpo de Classe de Hilbert*, em que o grau da extensão do corpo de classe de Hilbert é o número de classe de K. Mais ainda, o *Teorema da Reciprocidade de Artin* nos garante que o grupo de Galois $\mathrm{Gal}(H/K)$ é isomorfo ao grupo de classes de ideais de $\mathcal{O}_K$ — estes resultados são tratados em maiores detalhes no Apêndice A.1.

Em geral, a Teoria de Corpos de Classe não fornece um metodo explícito para construir as extensões abelianas de um dado corpo de números K. Na realidade, até o momento sabemos que existem apenas dois casos em que é possível fazer esta descrição. O primeiro caso é para $K = \mathbb{Q}$, em que temos o *Teorema de Kronecker-Weber*, que garante que todas as extensões abelianas de $\mathbb{Q}$ são os corpos ciclotômicos $\mathbb{Q}(\zeta_n)$, gerados por

uma raíz da unidade $\zeta_n = e^{2\pi i/n}$, $n \in \mathbb{N}$. O segundo caso é para os corpos quadráticos imaginários, isto é, para corpos da forma $K = \mathbb{Q}(\sqrt{D})$, em que D é um discriminante negativo. Neste caso, os valores especiais de j desempenham um papel análogo às raízes da unidade para o caso $K = \mathbb{Q}$, no sentido de que as extensões abelianas de $\mathbb{Q}(\sqrt{D})$ são da forma $K(j(\mathfrak{z}_D))$, em que $\mathfrak{z}_D$ é um ponto CM de discriminante D. Mais precisamente, temos o seguinte teorema:

Teorema 9. *Seja K um corpo quadrático imaginário com discriminante D e seja H o correspondente corpo de classe de Hilbert. Então, os valores especiais $j(\mathfrak{z}_{D,i})$, com $1 \leqslant i \leqslant h(D)$, são conjugados sobre K e qualquer um destes valores gera a extensão H/K.*

Este teorema é um resultado de muita relevância para a Teoria Algébrica dos Números, e para a matemática em geral. Deixamos indicado a referência [7], na qual a Seção 11 do Capítulo 3 é inteiramente dedicada a provar este resultado.

6 Fatoração Prima de Valores Especiais de j

Uma propriedade excepcional dos valores especiais de j é a de que eles são números com muitos divisores — ou muitas potências de divisores. Pela Tabela 2 temos, por exemplo:

$$j(\mathfrak{z}_{-11}) = -32768 = -2^{15},$$
$$j(\mathfrak{z}_{-19}) = -884736 = -2^{15} \cdot 3^3.$$

Na realidade, estamos interessados em estudar a fatoração prima da diferença entre dois valores especiais de j. Isto se deve ao fato de que a função modular j possui as mesmas propriedades, sejam elas analíticas ou aritméticas, da função $j + C$, para qualquer constante $C \in \mathbb{C}$, e fazer esta alteração não modifica o resultado da diferença entre dois valores especiais. Além disso, trabalhar com essa diferença não nos impede, por exemplo, de obter a fatoração prima de um único valor especial, e isto porque dado qualquer ponto CM $\mathfrak{z}$, o fato de que $j(\mathfrak{z}_{-3}) = 0$ garante que a diferença $j(\mathfrak{z}) - j(\mathfrak{z}_{-3})$ nos forneça a fatoração prima de $j(\mathfrak{z})$. No entanto, como em geral os valores especiais de j são inteiros algébricos — e não necessariamente inteiros — vamos estudar a norma da diferença entre dois valores especiais. Mais especificamente, dados discriminantes fundamentais, coprimos e negativos D_1 e D_2, a norma de $j(\mathfrak{z}_{D_1}) - j(\mathfrak{z}_{D_2})$ depende apenas do valor dos discriminantes associados e é dada, por definição[1], pelo produto de todos os conjugados nos domínios fundamentais $\Gamma_1\backslash\mathfrak{Z}_{D_1}$ e $\Gamma_1\backslash\mathfrak{Z}_{D_2}$:

$$J(D_1, D_2) := \prod_{\mathfrak{z}_1 \in \Gamma_1\backslash\mathfrak{Z}_{D_1}} \prod_{\mathfrak{z}_2 \in \Gamma_1\backslash\mathfrak{Z}_{D_2}} (j(\mathfrak{z}_1) - j(\mathfrak{z}_2)).$$

Este capítulo é focado em descrever a construção e propriedades de $J(D_1, D_2)$, bem como apresentar um teorema que caracteriza completamente sua fatoração prima, proposto no artigo [1] de Gross e Zagier. Mais precisamente, este resultado permite calcular $J(D_1, D_2)$ utilizando uma função aritmética, ou seja, podemos obter a fatoração prima de valores especiais de j realizando operações com números inteiros que podem ser feitas algoritmicamente. Este é um resultado interessantíssimo, já que, dentre várias razões, se trata de uma das raras ocasiões na matemática em que é possível obter a fatoração prima de um número inteiro de forma fechada.

Considere D_1 e D_2 dois discriminantes fundamentais, coprimos e negativos e sejam $j(\mathfrak{z}_1), j(\mathfrak{z}_2)$ valores especiais associados a D_1 e D_2, respectivamente. Conforme vimos na demonstração da Proposição 17, o conjunto dos números $m \in \mathbb{N}$ que são determinante de matrizes em $M(2, \mathbb{Z})$ fixando um dado ponto CM depende apenas do discriminante

[1] Apêndice A.1, Definição 17.

associado a este ponto. Isto significa que a norma de $j(\mathfrak{z}_1) - j(\mathfrak{z}_2)$ depende apenas dos discriminantes D_1 e D_2. Por definição, a norma deste número algébrico é o produto de todos os seus conjugados nos subconjuntos $\mathfrak{Z}_{D_1} \cap \widetilde{\mathcal{F}_1}$ e $\mathfrak{Z}_{D_2} \cap \widetilde{\mathcal{F}_1}$, que são domínios fundamentais para $\Gamma_1\backslash\mathfrak{Z}_{D_1}$ e $\Gamma_1\backslash\mathfrak{Z}_{D_2}$, respectivamente. Desta forma, a *norma da diferença entre os valores especiais* $j(\mathfrak{z}_1)$ *e* $j(\mathfrak{z}_2)$ é dada por:

$$J(D_1, D_2) := \prod_{\mathfrak{z}_1 \in \Gamma_1\backslash\mathfrak{Z}_{D_1}} \prod_{\mathfrak{z}_2 \in \Gamma_1\backslash\mathfrak{Z}_{D_2}} (j(\mathfrak{z}_1) - j(\mathfrak{z}_2)) = \prod_{1 \leqslant i \leqslant h(D_1)} \prod_{1 \leqslant j \leqslant h(D_2)} (j(\mathfrak{z}_{D_1,i}) - j(\mathfrak{z}_{D_2,j})). \quad (6.1)$$

Observação 18. Sejam $\mathfrak{z}_{D_1}, \mathfrak{z}_{D_2} \in \mathfrak{H}$ pontos CM com discriminantes D_1 e D_2 e suponha que $h(D_1) = 1$. Então, $|\Gamma_1\backslash\mathfrak{Z}_{D_1}| = h(D_1) = 1$ implica que $\mathfrak{z}_1$ é o único representante no domínio fundamental $\mathfrak{Z}_{D_1} \cap \widetilde{\mathcal{F}_1}$ de $\Gamma_1\backslash\mathfrak{Z}_{D_1}$. Portanto, a norma de $j(\mathfrak{z}_{D_1}) - j(\mathfrak{z}_{D_2})$ fica dada por

$$J(D_1, D_2) = \prod_{\mathfrak{z}_1 \in \Gamma_1\backslash\mathfrak{Z}_{D_1}} \prod_{\mathfrak{z}_2 \in \Gamma_1\backslash\mathfrak{Z}_{D_2}} (j(\mathfrak{z}_1) - j(\mathfrak{z}_2)) = \prod_{\mathfrak{z}_2 \in \Gamma_1\backslash\mathfrak{Z}_{D_2}} (j(\mathfrak{z}_{D_1}) - j(\mathfrak{z}_2)) = H_{D_2}(\mathfrak{z}_{D_1}).$$

Note também que, se $h(D_2) = 1$, então

$$J(D_1, D_2) = j(\mathfrak{z}_{D_1}) - j(\mathfrak{z}_{D_2})$$

é simplesmente a diferença entre os valores especiais $j(\mathfrak{z}_{D_1})$ e $j(\mathfrak{z}_{D_2})$.

Em [1], Gross e Zagier apresentaram o resultado seguinte, que caracteriza os fatores primos de $J(D_1, D_2)$ para o caso em que os discriminantes são coprimos.

Teorema 10. *Sejam D_1 e D_2 discriminantes fundamentais, negativos e coprimos e seja $D = D_1D_2$. Então, todos os fatores primos de $J(D_1, D_2)$ são limitados superiormente por $D/4$. Mais precisamente, todo fator primo de $J(D_1, D_2)$ divide $(D - x^2)/4$, para algum $x \in \mathbb{Z}$ satisfazendo $|x| < \sqrt{D}$ e $x^2 \equiv D \mod 4$.*

O Teorema 10 é uma versão qualitativa de um resultado ainda mais preciso, que fornece uma fórmula completa para a fatoração prima de $J(D_1, D_2)$. Para enunciar este resultado, precisaremos definir duas funções, $\varepsilon(m)$ e $F(m)$, que serão construídas a seguir.

Para cada $n \in \mathbb{Z}$ positivo denote por $\mathrm{div}(n)$ o conjunto dos divisores de n. Vamos definir a função $\varepsilon : \mathrm{div}(n) \to \{-1, 1\}$ pelas seguintes propriedades:

(i) ε é completamente multiplicativa, isto é, para quaisquer divisores $p_1^{r_1}, \ldots, p_s^{r_s} \in \mathrm{div}(n)$,

$$\varepsilon(p_1^{r_1} \ldots p_s^{r_s}) = \varepsilon(p_1)^{r_1} \ldots \varepsilon(p_s)^{r_s}.$$

(ii) Para todo primo $p \in \mathrm{div}(n)$,

$$\varepsilon(p) = \begin{cases} \chi_{D_1}(p) \text{ , se } p \nmid D_1 \\ \chi_{D_2}(p) \text{ , se } p \nmid D_2 \end{cases}.$$

onde χ_D é a *função característica módulo D de Dirichlet*, dada por $\chi_D(p) = \left(\frac{D}{p}\right)$, em que $\left(\frac{D}{p}\right)$ denota o *símbolo de Legendre*, definido por:

$$\left(\frac{D}{p}\right) = \begin{cases} 0 \text{ , se } p \mid D \\ 1 \text{ , se } D \text{ é um resíduo quadrático módulo } p \\ -1 \text{ , se } D \text{ é um resíduo não-quadrático módulo } p \end{cases}.$$

Vejamos que ε está bem definida. De fato, como $\text{mdc}(D_1, D_2) = 1$ e p é primo, então pelo menos uma das condições $p \nmid D_1$ ou $p \nmid D_2$ vale, e se ambas valem ao mesmo tempo, então os valores $\chi_{D_1}(p)$ e $\chi_{D_2}(p)$ coincidem, já que neste caso $D_1 D_2$ seria congruente a um quadrado não-nulo módulo p, se p é ímpar, e congruente a um quadrado ímpar módulo 8 se $p = 2$. Em todo caso, $\chi_{D_1}(p)\chi_{D_2}(p) = 1$. Isto mostra que, necessariamente, $\chi_{D_1} = \chi_{D_2} = 1$ ou $\chi_{D_1} = \chi_{D_2} = -1$. No entanto, para fins práticos, podemos reformular a definição de ε da seguinte forma:

Definição 14. Sejam D_1, D_2 discriminantes fundamentais, negativos e coprimos e seja $D = D_1 D_2$. Para primos p com símbolo de Legendre $\left(\frac{D}{p}\right) \neq -1$, definimos:

$$\varepsilon(p) = \begin{cases} \left(\frac{D_1}{p}\right) \text{ , se } \text{mdc}(p, D_1) = 1 \\ \left(\frac{D_2}{p}\right) \text{ , se } \text{mdc}(p, D_2) = 1 \end{cases}. \tag{6.2}$$

Para um número inteiro $m = \prod_i p_i^{a_i}$, com p_i primos, a_i inteiros positivos e $\left(\frac{D}{p_i}\right) \neq -1$, para todo i, definimos ε como a função completamente multiplicativa satisfazendo (6.2):

$$\varepsilon(m) = \prod_i \varepsilon(p_i)^{a_i}. \tag{6.3}$$

Definição 15. Defnimos, para $m \in \mathbb{Z}$ na forma $(D - x^2)/4$, para algum $x \in \mathbb{Z}$, a função:

$$F(m) = \prod_{n \mid m} n^{\varepsilon(m/n)} = \prod_{\substack{nn' = m \\ n, n' > 0}} n^{\varepsilon(n')}.$$

Observação 19. A princípio, a função F assume valores racionais, já que $\varepsilon(n') \in \{-1, 1\}$, mas, na realidade, F sempre assume valores inteiros. No artigo [1], consta a caracterização explícita da função F dependendo do valor de m, onde, de forma geral, temos que $F(m) = 1$ ou $F(m)$ é sempre uma potência de um único número primo. Mais precisamente, se m é um inteiro positivo na forma $(D - x^2)/4$, temos $F(m) = 1$, exceto no caso em que m pode ser escrito na forma:

$$m = p^{2a+1} p_1^{2a_1} \cdots p_r^{2a_r} q_1^{b_1} \cdots q_s^{b_s},$$

em que $\varepsilon(p) = \varepsilon(p_1) = \ldots = \varepsilon(p_r) = -1$ e $\varepsilon(q_1) = \ldots = \varepsilon(q_s) = 1$. Neste caso,

$$F(m) = p^{(a+1)(b_1+1)\cdots(b_s+1)}.$$

Em particular, se p é um divisor primo de $F(m)$, então p é o único primo dividindo m com um expoente negativo e $\varepsilon(p) = -1$.

Esta caracterização, apesar de ser um fato curioso sobre a função F, não é necessária para a demonstração, nem para efetuar cálculos com a fórmula completa para $J(D_1, D_2)$ e, por esta razão, omitiremos sua prova — que pode ser encontrada em [7], na página 301.

Agora, podemos enunciar o resultado que fornece a fórmula completa para $J(D_1, D_2)$.

Teorema 11. *Sejam D_1 e D_2 discriminantes fundamentais, negativos e coprimos e seja $D = D_1 D_2$. Então,*

$$J(D_1, D_2)^{8/\omega(D_1)\omega(D_2)} = \prod_{\substack{x^2<D \\ x^2 \equiv D \mod 4}} F\left(\frac{D-x^2}{4}\right) = \prod_{\substack{x,n,n' \in \mathbb{Z} \\ n,n'>0 \\ x^2+4nn'=D}} n^{\varepsilon(n')}, \tag{6.4}$$

em que $\omega(D_1)$ e $\omega(D_2)$ denotam o número de unidades nas ordens quadráticas $\mathcal{O}_{D_1}$ e $\mathcal{O}_{D_2}$, respectivamente.

O artigo [1] de Gross e Zagier fornece duas demonstrações para este teorema: uma algébrica e outra analítica. A demonstração algébrica usa a teoria de redução de curvas elípticas, e é dada apenas para o caso em que os discriminantes são primos. Já na demonstração analítica, os autores se baseiam no cálculo dos coeficientes de Fourier das séries de Eisenstein no grupo modular de Hilbert $\mathbb{Q}(\sqrt{D})$ na restrição à diagonal $\mathfrak{H} \subset \mathfrak{H} \times \mathfrak{H}$.

Observação 20. Faremos uma série de observações à respeito do Teorema 11.

1. A fórmula dada pelo Teorema 11 está bem definida: de fato, o produto em (6.4) é finito, visto que $D = D_1 D_2$ é dado e temos finitos números inteiros x, n, n', com $n, n' > 0$, capazes de satisfazer $x^2 + 4nn' = D$. Além disso, a função $\varepsilon(n')$ está bem definida, já que para todo primo p_i dividindo $\dfrac{D-x^2}{4}$ temos por definição que $\left(\dfrac{D}{p_i}\right) \neq -1$.
2. Podemos trocar $\varepsilon(n')$ por $-\varepsilon(n)$. A expressão $x^2 + 4nn' = D$ nos mostra que $\varepsilon\left(\dfrac{D-x^2}{4}\right) = -1$, e como ε é completamente multiplicativa, obtemos

$$x^2 + 4nn' = D \implies nn' = \frac{D-x^2}{4} \implies \varepsilon(n)\varepsilon(n') = \varepsilon\left(\frac{D-x^2}{4}\right) = -1,$$

mostrando que $\varepsilon(n') = -\varepsilon(n)$.

3. Para os casos em que $D_1, D_2 \neq -3, -4$, a fórmula para $J(D_1, D_2)$ não depende do número de unidades nas respectivas formas quadráticas $\mathcal{O}_{D_1}$ e $\mathcal{O}_{D_2}$, já que a potência $8/\omega(D_1)\omega(D_2)$ em $J(D_1, D_2)$ será igual a 2, uma vez que nestes casos temos $\omega(D_1) = \omega(D_2) = 2$. Desta forma, obtemos a seguinte expressão para $J(D_1, D_2)$:

$$J(D_1, D_2)^2 = \prod_{\substack{x^2<D \\ x^2 \equiv D \mod 4}} F\left(\frac{D-x^2}{4}\right) = \prod_{\substack{x,n,n' \in \mathbb{Z} \\ n,n'>0 \\ x^2+4nn'=D}} n^{\varepsilon(n')}. \tag{6.5}$$

A seguir, daremos dois exemplos aplicando o Teorema 11 para obter a fatoração prima de valores especiais de j.

Exemplo 6. Considere $D_1 = -7$ e $D_2 = -43$. Estes discriminantes possuem números de classe $h(D_1) = h(D_2) = 1$, conforme calculamos na Seção 5.1.1. Na Observação 18, vimos que no caso em que os discriminantes D_1 e D_2 possuem números de classe igual a um, $J(D_1, D_2)$ é simplesmente a diferença entre os valores especiais $j(\mathfrak{z}_{D_1})$ e $j(\mathfrak{z}_{D_2})$. Então, pela fórmula (6.5), obtemos

$$J(-7, -43)^2 = (j(\mathfrak{z}_{-7}) - j(\mathfrak{z}_{-43}))^2.$$

Agora, tendo em mente o Teorema 11, basta calcularmos o produto

$$\prod_{\substack{x^2<D \\ x^2 \equiv D \mod 4}} F\left(\frac{D-x^2}{4}\right).$$

Com efeito, vamos encontrar primeiramente os possíveis valores de $x \in \mathbb{Z}$. Como $x^2 < D_1D_2 = D = 301$, temos $|x| \leqslant 17$. Além disso, apenas os valores ímpares de x satisfazem a condição $x^2 \equiv D \mod 4$. Portanto,

$$(j(\mathfrak{z}_{-7}) - j(\mathfrak{z}_{-43}))^2 = \prod_{\substack{|x|\leqslant 17 \\ x \text{ ímpar}}} F\left(\frac{301-x^2}{4}\right) = \prod_{\substack{1\leqslant x\leqslant 17 \\ x \text{ ímpar}}} F\left(\frac{301-x^2}{4}\right)^2$$

Logo,

$$\begin{aligned} j(\mathfrak{z}_{-7}) - j(\mathfrak{z}_{-43}) &= \pm F(75)F(73)F(69)F(63)F(55)F(45)F(33)F(19)F(3) \\ &= \pm 3 \cdot 73 \cdot 3^2 \cdot 7 \cdot 5^2 \cdot 5 \cdot 3^2 \cdot 19 \cdot 3 \\ &= \pm 3^6 \cdot 5^3 \cdot 7 \cdot 19 \cdot 73 \end{aligned}$$

Neste exemplo, omitimos o cálculo explícito dos valores $F(m)$, pela quantidade de valores a calcular ser extensa. A fim de ilustrar como é feita a aritmética desta função, calculemos $F(33)$.

$$F(33) = \prod_{d|33} d^{\varepsilon(33/d)} = 1^{\varepsilon(33)} \cdot 3^{\varepsilon(11)} \cdot 11^{\varepsilon(3)} \cdot 33^{\varepsilon(1)} = 3^{\varepsilon(11)} \cdot 11^{\varepsilon(3)} \cdot 33.$$

Como $11 \nmid D_1 = -7$, temos

$$\varepsilon(11) = \left(\frac{-7}{11}\right) = 1,$$

pois -7 é um resíduo quadrático módulo 11. Similarmente,

$$\varepsilon(3) = \left(\frac{-7}{3}\right) = -1,$$

pois -7 é um resíduo não-quadrático módulo 3. Portanto, $F(33) = 3 \cdot 11^{-1} \cdot 33 = 3^2$.

Exemplo 7. Mencionamos na introdução deste capítulo que o fato curioso de que $j(\mathfrak{z}_{-3}) = 0$ nos permite calcular a fatoração prima de um único valor especial de $j(\mathfrak{z})$. Utilizando a fórmula fechada para a diferença de dois valores especiais de j fornecida pelo Teorema 11, isto se torna possível. Para ilustrar, vamos obter a fatoração prima de $\mathfrak{z}_{-7}$.

Considere $D_1 = -7$ e $D_2 = -3$. Conforme calculamos na Seção 5.1.1, estamos tratando de dois discriminantes de número de classe um. Logo, $J(D_1, D_2)$ é simplesmente a diferença $j(\mathfrak{z}_{-7}) - j(\mathfrak{z}_{-3})$, ou seja, na realidade, $J(D_1, D_2) = j(\mathfrak{z}_{-7})$. Por (5.11), sabemos que $\omega(D_1) = 2$ e $\omega(D_2) = 6$. Logo, o Teorema 11 nos dá:

$$j(\mathfrak{z}_{-7})^{2/3} = \prod_{\substack{x^2<21 \\ x^2 \equiv 21 \mod 4}} F\left(\frac{21-x^2}{4}\right).$$

Por um lado, a condição $x^2 < 21$ implica que $|x| \leqslant 4$. Por outro, a condição $x^2 \equiv 21 \mod 4$ só é satisfeita para os valores ímpares de x. Portanto,

$$\prod_{\substack{x^2<21 \\ x^2 \equiv 21 \mod 4}} F\left(\frac{21-x^2}{4}\right) = \prod_{\substack{|x|\leqslant 4 \\ x \text{ ímpar}}} F\left(\frac{21-x^2}{4}\right) = \prod_{\substack{1\leqslant x\leqslant 4 \\ x \text{ ímpar}}} F\left(\frac{21-x^2}{4}\right)^2 = (F(5)F(3))^2.$$

Nosso problema se resume a calcular os valores $F(m)$. Obtemos:

$$F(5) = \prod_{d|5} d^{\varepsilon(5/d)} = 1^{\varepsilon(5)} \cdot 5^{\varepsilon(1)} = 5,$$
$$F(3) = \prod_{d|3} d^{\varepsilon(3/d)} = 1^{\varepsilon(3)} \cdot 3^{\varepsilon(1)} = 3.$$

Portanto,

$$j(\mathfrak{z}_{-7})^{2/3} = (F(5)F(3))^2 = (3 \cdot 5)^2 \implies j(\mathfrak{z}_{-7}) = \pm 3^3 \cdot 5^3,$$

e de fato este valor se confirma: pela tabela 2, $j(\mathfrak{z}_{-7}) = -3^3 \cdot 5^3 = -3375$.

Conforme mencionamos, a principal contribuição do Teorema 11 é fornecer uma forma algorítmica de calcular e obter a fatoração prima de valores especiais de j. A imagem a seguir apresenta uma tabela com o propósito de auxiliar em cálculos utilizando este teorema: para cada $|x|$, com x ímpar, estão representados os valores $\dfrac{D-x^2}{4}$ e $F\left(\dfrac{D-x^2}{4}\right)$.

Figura 5 – Relações para o Teorema 11

$\lvert x\rvert$	$\frac{D-x^2}{4}$	$F\left(\frac{D-x^2}{4}\right)$
1	$2\cdot 3\cdot 5\cdot 7\cdot 13$	1
3	$2^3\cdot 11\cdot 31$	1
5	$2^2\cdot 3\cdot 227$	3^2
7	$2\cdot 3^2\cdot 151$	2^2
9	$2\cdot 5\cdot 271$	1
11	$2^2\cdot 3^3\cdot 5^2$	3^2
13	$2^7\cdot 3\cdot 7$	1
15	$2\cdot 7\cdot 191$	1
17	$2\cdot 3\cdot 443$	1
19	$2^4\cdot 3\cdot 5\cdot 11$	1
21	$2^2\cdot 5\cdot 131$	5^2
23	$2\cdot 3\cdot 433$	1
25	$2\cdot 3^2\cdot 11\cdot 13$	1
27	$2^2\cdot 7^2\cdot 13$	13
29	$2^3\cdot 3^2\cdot 5\cdot 7$	1
31	$2\cdot 3\cdot 5\cdot 83$	1
33	$2\cdot 1229$	2^2
35	$2^3\cdot 3\cdot 101$	1
37	$2^2\cdot 3\cdot 199$	3^2
39	$2\cdot 5^2\cdot 47$	2^2
41	$2\cdot 3\cdot 5\cdot 7\cdot 11$	1
43	$2^2\cdot 3^4\cdot 7$	7
45	$2^4\cdot 139$	139
47	$2\cdot 3^2\cdot 11$	2
49	$2\cdot 3\cdot 5\cdot 71$	1
51	$2^2\cdot 5\cdot 13$	1
53	$2^2\cdot 3\cdot 13^2$	3
55	$2\cdot 3\cdot 329$	1
57	$2\cdot 7\cdot 137$	1
59	$2^2\cdot 3\cdot 5\cdot 31$	1
61	$2^3\cdot 3^2\cdot 5^2$	2^2
63	$2\cdot 11\cdot 79$	1
65	$2\cdot 3^3\cdot 31$	1
67	$2^3\cdot 3\cdot 67$	1
69	$2^2\cdot 5\cdot 7\cdot 11$	1
71	$2\cdot 3\cdot 5\cdot 7^2$	1
73	$2\cdot 3\cdot 233$	1
75	$2^2\cdot 331$	331
77	$2^5\cdot 3\cdot 13$	1
79	$2\cdot 3^2\cdot 5\cdot 13$	1
81	$2\cdot 5\cdot 109$	1
83	$2^4\cdot 3^2\cdot 7$	7
85	$2^2\cdot 3\cdot 7\cdot 11$	1
87	$2\cdot 419$	2^2
89	$2\cdot 3\cdot 5^3$	1
91	$2^2\cdot 3\cdot 5\cdot 11$	1
93	$2^3\cdot 71$	2^4
95	$2\cdot 3\cdot 79$	1
97	$2\cdot 3^3\cdot 7$	1
99	$2^3\cdot 5\cdot 7$	1
101	$2^2\cdot 3^2\cdot 5$	5
103	$2\cdot 3\cdot 13$	1

Fonte: [1, p. 193]

Referências

[1] GROSS, B. H.; ZAGIER, D. B. On singular moduli. *Journal für die reine und angewandte Mathematik*, n. 355, p. 191–220, 1984. Citado 9 vezes nas páginas 7, 8, 13, 15, 84, 85, 86, 87 e 90.

[2] SERRE, J.-P. *A Course in Arithmetic*. 1. ed. New York: Springer-Verlag, 1973. Citado 6 vezes nas páginas 13, 28, 32, 36, 37 e 39.

[3] ZAGIER, D. et al. *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*. 1. ed. Berlin: Springer-Verlag, 2008. Citado 5 vezes nas páginas 13, 19, 20, 67 e 79.

[4] COHEN, H.; STRöMBERG, F. *Modular Forms: A Classical Approach*. 1. ed. Providence, Rhode Island: American Mathematical Society, 2017. Citado na página 13.

[5] DIAMOND, F.; SHURMAN, J. *A First Course in Modular Forms*. 1. ed. New York: Springer-Verlag, 2005. Citado 4 vezes nas páginas 13, 102, 103 e 105.

[6] COHEN, H. *An Introduction to Modular Forms*. 1. ed. New York: Springer-Verlag, 2019. Citado na página 13.

[7] COX, D. A. *Primes of The Form $x^2 + ny^2$*. 1. ed. New York: John Wiley & Sons, 1989. Citado 6 vezes nas páginas 13, 79, 82, 83, 87 e 96.

[8] SILVERMAN, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves*. 1. ed. New York: Springer-Verlag, 1994. Citado na página 13.

[9] SERRE, J.-P. Une interprétation des congruences relatives à la fonction τ de ramanujan. *Séminaire Delange-Pisot-Poitou*, v. 9, n. 14, p. 1–17, 1968. Citado na página 45.

[10] STEWART, D. T. I. *Algebraic Number Theory and Fermat's Last Theorem*. 3. ed. University of Warwick: A.K. Peters, 2019. Citado na página 93.

Apêndices

APÊNDICE A – Pré-requisitos de Teoria Algébrica dos Números

A.1 Inteiros Algébricos

Inteiros algébricos são soluções de polinômios mônicos com coeficientes em $\mathbb{Z}$. Nosso objetivo é estudar a fatoração destes números, que a princípio é muito semelhante à fatoração de números inteiros, mas que difere em um ponto fundamental: a unicidade da fatoração. Em geral, a fatoração de um número depende do anel considerado. Estamos particularmente interessados no anel dos inteiros $\mathcal{O}_K$ de um corpo de números K, na possibilidade de obter a fatoração de um elemento em produto de elementos irredutíveis e na sua unicidade. Os resultados apresentados nesta seção do apêndice são resultados clássicos da Teoria dos Números e foram baseados na referência [10].

Definição 16. Dizemos que um número $\alpha \in \mathbb{C}$ é *algébrico* se é a raiz de um polinômio

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

com coeficientes $a_i \in \mathbb{Q}$, para $i = 1, \ldots, n-1$. Denotamos o conjunto dos números algébricos por $\overline{\mathbb{Q}}$. Se os coeficientes a_i forem inteiros, dizemos que α é um *inteiro algébrico*. Neste caso, denotamos o conjunto dos inteiros algébricos por $\overline{\mathbb{Z}}$.

Exemplo 8. As raízes da unidade $\zeta_n = e^{2\pi i/n}$ são inteiros algébricos, para todo $n \in \mathbb{N}$, já que por definição satisfazem o polinômio $x^n - 1$ em $\mathbb{Z}[X]$.

Definição 17. Seja $\alpha \in \overline{\mathbb{Q}}$ um número algébrico. Definimos a *norma* de α como o produto de todos os seus conjugados galoisianos:

$$N(\alpha) = \prod_{\sigma \in Gal(\mathbb{C}/\mathbb{Q})} \sigma(\alpha).$$

Definição 18. Um *corpo de números* K é um subcorpo de $\mathbb{C}$ de grau finito sobre $\mathbb{Q}$. Denotamos o grau de K sobre $\mathbb{Q}$ por $[K : \mathbb{Q}]$.

Teorema 12 (Estrutura e Propriedades dos Números Algébricos)**.**

(i) $\overline{\mathbb{Q}}$ *é um subcorpo de* $\mathbb{C}$ *e* $\overline{\mathbb{Z}}$ *é um subanel de* $\overline{\mathbb{Q}}$*.*

(ii) Se $\alpha \in \mathbb{C}$ *é raíz de um polinômio mônico cujos coeficientes são números algébricos (resp. inteiros algébricos), então* α *é um número algébrico (resp. inteiro algébrico).*

O Teorema anterior nos permite construir uma infinidade de números algébricos. Por exemplo, sabemos que $\sqrt{2}$ e $\sqrt{5}$ são inteiros algébricos. Então, qualquer combinação inteira destes dois números será um inteiro algébrico, como $\sqrt{2} + 3\sqrt{5}$. Da mesma forma, qualquer raíz de um polinômio mônico com coeficientes em $\mathbb{Z}[\sqrt{2}, \sqrt{5}]$ será um inteiro algébrico, como as raízes do polinômio $x^5 + (\sqrt{2})^3 x - 17\sqrt{5}$.

Lema 14. *Se $\alpha \in \mathbb{Q}$ é um inteiro algébrico, então $\alpha \in \mathbb{Z}$. Equivalentemente, $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.*

Demonstração. A inclusão $\mathbb{Z} \subset \overline{\mathbb{Z}} \cap \mathbb{Q}$ é imediata. Para a inclusão contrária, suponha que

$$\alpha = \frac{p}{q}, \qquad \text{mdc}(p, q) = 1,$$

é um inteiro algébrico, raíz de

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_i \in \mathbb{Z}, i = 1, \ldots, n-1.$$

Então,

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0.$$

Multiplicando a equação acima por q^n, obtemos

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0.$$

Logo, $q \mid p^n$. Como $\text{mdc}(p, q) = 1$, isso ocorre somente se $q = \pm 1$, ou seja, $\alpha \in \mathbb{Z}$. □

Definição 19. Seja K um corpo de números. O *anel dos inteiros* de K é definido por

$$\mathcal{O}_K = \{\alpha \in K : \alpha \text{ é um inteiro algébrico}\} = K \cap \overline{\mathbb{Z}}.$$

Exemplo 9. O Lema 14 nos diz que $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

A estrutura básica do anel dos inteiros de um corpo de números K é descrita no teorema abaixo.

Teorema 13. *Seja K um corpo de números.*

(i) $\mathcal{O}_K$ é um subanel de $\mathbb{C}$, cujo corpo de frações é K.

(ii) $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto $[K : \mathbb{Q}]$.

Historicamente, o fato de a fatoração de polinômios e números inteiros em fatores irredutíveis (primos) ser única levou à intuição de que o mesmo deveria o ocorrer com números no conjunto dos inteiros algébricos. No entanto, isto não é verdade. Por exemplo, o número 6 no anel $\mathbb{Z}[\sqrt{-6}]$ não possui fatoração única, pois

$$6 = 2 \cdot 3 = \left(-\sqrt{-6}\right) \cdot \sqrt{-6}.$$

A razão disto tem origem na definição do que vem a ser um elemento ser *primo* ou *irredutível*.

Definição 20. Seja R um anel. Sejam $a, b \in R$ satisfazendo as condições:

(i) $p = ab \implies a$ ou b é uma unidade,

(ii) $p|ab \implies p|a$ ou $p|b$.

Um elemento $p \in R$ é dito *irredutível* se satisfaz a condição (i), e é dito *primo* se satisfaz a condição (ii).

Observação 21. Todo elemento primo é irredutível, mas a recíproca não é, em geral, verdadeira. Por exemplo, o elemento $\sqrt{-6}$ é irredutível em $\mathbb{Z}[\sqrt{-6}]$, mas não é primo, pois $\sqrt{-6}$ divide $6 = 2 \cdot 3$, mas não divide nem 2 e nem 3.

Em geral, estamos interessados em saber sob quais condições é possível fatorar um elemento do anel de inteiros $\mathcal{O}_K$ de um corpo K em produto de irredutíveis — e produto de primos — e quando essa maneira é única.

A princípio, estudaremos o caso da fatoração em irredutíveis. Para isso, vamos trabalhar a noção de anel *noetheriano* e veremos que a decomposição em fatores primos é sempre possível em um domínio noetheriano. O resultado segue concluíndo que $\mathcal{O}_K$ é noetheriano.

No entanto, essa decomposição não é única em geral. A fim de descobrir em quais casos a unicidade ocorre, veremos que toda decomposição em fatores primos é única. Sendo assim, o problema se resume a entender em quais aneis de inteiros um elemento irredutível é primo.

Definição 21. Seja D um domínio. Se, para todo $x \in D$ não nulo que não é uma unidade, podemos escrever $x = p_1 p_2 \cdots p_n$, para $p_i, i \in \{1, \cdots, n\}$ irredutíveis em D, dizemos que a *fatoração em irredutíveis é possível em* D.

Em geral, a fatoração em irredutíveis nem sempre é possível em um domínio D. Por exemplo, $\overline{\mathbb{Z}}$ não admite: se $\alpha \neq 0$ não é uma unidade, então $\sqrt{\alpha}$ também não é. Como $\alpha = \sqrt{\alpha}\sqrt{\alpha}$ e $\sqrt{\alpha}$ é um inteiro algébrico, pois α o é, α não é irredutível. No entanto, a fatoração em irredutíveis é sempre possível num domínio D noetheriano, embora não necessariamente única.

Definição 22. Seja D um domínio. Dizemos que D é *noetheriano* se todo ideal em D é finitamente gerado.

A proposição a seguir descreve duas propriedades equivalentes à condição noetheriana.

Proposição 18. *Seja D um domínio. São equivalentes:*

(i) D *é noetheriano.*

(ii) D *satisfaz a condição da cadeia ascendente: Toda cadeia ascendente de ideais de* D

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

se estabiliza, isto é, existe N *para o qual* $I_n = I_N$*, para todo* $n \geqslant N$*.*

(iii) Todo conjunto não vazio de ideais em D *tem um elemento maximal.*

Teorema 14. *Se* D *é um domínio noetheriano, então a fatoração em irredutíveis é possível em* D*.*

Teorema 15. *Seja* K *um corpo de números. O anel dos inteiros* $\mathcal{O}_K$ *é noetheriano.*

Corolário 8. *Se* K *é um corpo de números, a fatoração em irredutíveis é possivel no anel dos inteiros* $\mathcal{O}_K$*.*

Embora a fatoração em irredutíveis seja sempre possível no anel dos inteiros de um corpo de números, ela não é, em geral, única. Por exemplo, se $K = \mathbb{Q}(\sqrt{-6})$, temos $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$. Mas $6 = 2.3 = (-\sqrt{-6})\sqrt{-6}$ possui duas decomposições distintas em fatores irredutíveis. Neste caso, vimos na Observação 21, por exemplo, que $\sqrt{-6}$ é um irredutível que não é primo. A falha na unicidade está relacionada com a existência de elementos em irredutíveis em $\mathcal{O}_K$ que não são primos. Mais ainda, satisfazer essa condição é suficiente para garantir a unicidade da fatoração, como afirma o teorema seguinte.

Teorema 16. *Seja* D *um domínio em que a fatoração em irredutíveis seja possível. A fatoração é única se, e somente se, todo elemento irredutível é primo.*

Dizemos que um domínio D é um *Domínio de Fatoração Única (DFU)* se a fatoração em irredutíveis é possível e única. Evidentemente, isso ocorre se, e somente se, todo elemento irredutível em D é primo.

Corolário 9. *Seja* K *um corpo de números. O anel dos inteiros* $\mathcal{O}_K$ *é um DFU se, e somente se, todo elemento irredutível em* $\mathcal{O}_K$ *é primo.*

A.2 Ideais de $\mathcal{O}_K$ e Ramificação

Nesta seção caracterizaremos os ideais de $\mathcal{O}_K$ e introduziremos a ideia de ramificação de um ideal, conceito fundamental para o estudo da teoria de corpos de classe. Os resultados desta seção e da seção seguinte foram baseados na referência [7].

Teorema 17. *Seja* K *um corpo de números, e* $\mathfrak{a}$ *um ideal não-nulo de* $\mathcal{O}_K$*. Então, o anel quociente* $\mathcal{O}_K/\mathfrak{a}$ *é finito.*

Tendo em mente o teorema acima, podemos definir a *norma* de um ideal $\mathfrak{a}$ de $\mathcal{O}_K$ como a cardinalidade

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|. \tag{A.1}$$

Em geral, vimos que os aneis $\mathcal{O}_K$, onde K é um corpo de números, não são domínios de fatoração única. No entanto, estes aneis são *domínios de Dedekind*, isto é, são aneis noetherianos satisfazendo as propriedades:

(i) $\mathcal{O}_K$ é integralmente fechado: se $\alpha \in K$ é raíz de um polinômio mônico definido em $\mathcal{O}_K$, então $\alpha \in \mathcal{O}_K$,

(ii) Todo ideal primo não-nulo de $\mathcal{O}_K$ é maximal.

Esta caracterização é extremamente relevante, pois todo domínio de Dedekind admite fatoração única em ideais primos. Em particular, para $\mathcal{O}_K$, embora não possamos — em geral — obter fatoração única para seus elementos, sempre podemos decompor $\mathcal{O}_K$ unicamente como produto de ideais primos. Ademais, sendo $\mathcal{O}_K$ domínios de Dedekind, todo ideal primo $\mathfrak{p}$ não-nulo de $\mathcal{O}_K$ é maximal, e portanto o Teorema 17 nos garante que $\mathcal{O}_K/\mathfrak{p}$ é um corpo finito, denominado *corpo residual de* $\mathfrak{p}$.

Dentre os ideais de $\mathcal{O}_K$, estamos particularmente interessados nos *ideais fracionários*, ou seja, ideais que podem ser escritos na forma $\alpha\mathfrak{a}$, para algum $\alpha \in K$ e algum ideal $\mathfrak{a}$ de $\mathcal{O}_K$. Vale o seguinte resultado para ideais fracionários de $\mathcal{O}_K$:

Proposição 19. *Seja K um corpo de números e $\mathfrak{a}$ um ideal fracionário de $\mathcal{O}_K$. Então,*

(i) Existe ideal fracionário $\mathfrak{b}$ de $\mathcal{O}_K$ tal que $\mathfrak{ab} = K$. Neste caso, denotamos $\mathfrak{b} = \mathfrak{a}^{-1}$.

(ii) $\mathfrak{a}$ é escrito unicamente como o produto

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i},$$

em que $r_i \in \mathbb{Z}$ e $\mathfrak{p}_i$ são ideais primos distintos de $\mathcal{O}_K$, para todo $i = 1, \cdots, r$.

Seja K corpo de números e I_K o conjunto de todos os ideais fracionários de $\mathcal{O}_K$. A proposição acima garante que I_K é fechado com respeito à multiplicação e é um grupo. Para o nosso caso, o subgrupo de maior relevância de I_K é o subgrupo P_K dos *ideais fracionários principais*, ou seja, o subgrupo dos ideais da forma $\alpha\mathcal{O}_K$, para $\alpha \in K$ não-nulo.

Definição 23. Seja K um corpo de números. O quociente

$$Cl(\mathcal{O}_K) = \frac{I_K}{P_K}$$

é chamado de *Grupo de Classes de Ideais de* $\mathcal{O}_K$.

Um fato fundamental da Teoria Algébrica dos Números é que $Cl(\mathcal{O}_K)$ é um grupo finito. A ordem desse grupo é chamada de *número de classes de* $\mathcal{O}_K$, e é denotada por $h(\mathcal{O}_K)$.

Observação 22. Seja K um corpo de números. Então, $h(\mathcal{O}_K) = 1$ se, e somente se, $\mathcal{O}_K$ é um domínio de fatoração única. De fato, basta relembrar que domínios de Dedekind admitem fatoração única em ideais primos, isto é, em domínios de Dedekind, domínios de ideais principais (DIP) e domínios de fatoração única (DFU) são equivalentes. O anel $\mathcal{O}_K$ é um domínio de Dedekind, conforme mencionado anteriormente. Então, o fato de $h(\mathcal{O}_K) = 1 \iff \mathcal{O}_K$ é um DIP garante que $\mathcal{O}_K$ é um DFU. Em certo sentido, o grupo de classes é uma medida de quão longe o anel $\mathcal{O}_K$ está de ser um DFU.

A seguir, estudaremos a ideia de *Ramificação*. Considere K um corpo de números e L uma extensão finita de K. Seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ e $\mathfrak{p}\mathcal{O}_L$ o correspondente ideal em $\mathcal{O}_L$ com fatoração prima dada por

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

onde $\mathfrak{P}_i$ são os ideais primos de $\mathcal{O}_L$ contendo $\mathfrak{p}$, para $i = 1, \cdots, g$. Os números inteiros e_i são chamados de *índices de ramificação* de $\mathfrak{p}$ em $\mathfrak{P}_i$, com $i = 1, \ldots, g$. Nesse contexto, cada ideal primo $\mathfrak{P}_i$ contendo $\mathfrak{p}$ fornece uma extensão de corpos residuais $\mathcal{O}_K/\mathfrak{p} \subset \mathcal{O}_L/\mathfrak{P}_i$, cujo grau f_i é chamado de *grau de inércia* de $\mathfrak{p}$ em $\mathfrak{P}_i$. A relação entre os índices de ramificação e os graus inerciais é dada pelo seguinte resultado:

Proposição 20. *Sejam $K \subset L$ corpos de números e $\mathfrak{p}$ ideal primo de $\mathcal{O}_K$. Se e_i e f_i são os índices de ramificação e os graus inerciais, respectivamente, para $i = 1, \ldots, g$ então:*

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

Definição 24. Sejam $K \subset L$ corpos de números e $\mathfrak{p}$ ideal primo de $\mathcal{O}_K$. Dizemos que $\mathfrak{p}$ se *ramifica* em L se qualquer um dos índices de ramificação é maior do que 1.

Pode ser provado que apenas um número finito de ideais primos de $\mathcal{O}_K$ se ramifica em L. Uma outra observação a ser feita é a de que a definição dada acima pode ser mais explícita quando a extensão $K \subset L$ é galoisiana, devido ao seguinte resultado:

Proposição 21. *Sejam $K \subset L$ extensão galoisiana e $\mathfrak{p}$ ideal primo de $\mathcal{O}_K$. Então,*

(i) Se $\mathfrak{P}, \mathfrak{P}'$ são ideais primos de $\mathcal{O}_L$ contendo $\mathfrak{p}$, então existe $\sigma \in Gal(L/K)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$.

(ii) Os ideais primos $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ de $\mathcal{O}_L$ contendo $\mathfrak{p}$ possuem o mesmo índice de ramificação e mesmo grau inercial. Além disso,

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

A definição de ramificação para uma extensão $K \subset L$ Galoisiana de corpos de números pode ser reformulada da seguinte forma: se $\mathfrak{p}$ é um ideal primo de $\mathcal{O}_K$, dizemos que $\mathfrak{p}$ é *ramificado* em L se $e > 1$, e *não ramificado* em L se $e = 1$. Além disso, se $\mathfrak{p}$ satisfaz $e = f = 1$, dizemos que $\mathfrak{p}$ se *decompõe completamente* em L.

A.3 O Corpo de Classe de Hilbert

O *Corpo de Classe de Hilbert* de um corpo de números K é definido em função das extensões abelianas não ramificadas de K. Uma extensão $K \subset L$ é *Abeliana* quando é uma extensão de Galois e o grupo de Galois $Gal(L/K)$ é Abeliano. No entanto, precisamos entender o que é uma extensão *não ramificada*, e para isso devemos estudar a ramificação de ideais primos infinitos.

Os ideais primos de $\mathcal{O}_K$ são chamados de *primos finitos*, e os o *primos infinitos* são determinados por mergulhos de um corpo de números K em $\mathbb{C}$. Um *primo infinito real* é um mergulho $\sigma : K \to \mathbb{R}$, e um *primo infinito complexo* é um par de mergulhos conjugados distintos $\sigma, \overline{\sigma} : K \to \mathbb{C}$. Dada uma extensão $K \subset L$, dizemos que um primo infinito σ de K *ramifica* em L se σ é real mas existe uma extensão de σ em L que é complexa.

Definição 25. Seja $K \subset L$ uma extensão de corpos. Dizemos que ela é uma extensão *não ramificada* se todos os primos, finitos ou infinitos, são não ramificados.

Teorema 18. *Seja K um corpo de números. Então, existe uma extensão de Galois $K \subset L$ tal que L é uma extensão abeliana não ramificada de K e qualquer extensão abeliana não ramificada de K está em L. Dizemos que L é o Corpo de Classe de Hilbert de K.*

O principal resultado que veremos nessa seção é o *Teorema da Reciprocidade de Artin*, que relaciona o corpo de classe de Hilbert com o Grupo de Classes de Ideais de $Cl(\mathcal{O}_K)$. Para chegar neste ponto, veremos algumas propriedades que ligam o corpo de classe de Hilbert L de K à estrutura de ideal do anel dos inteiros $\mathcal{O}_K$. Mais especificamente, começamos definindo o *símbolo de Artin*.

Lema 15. *Seja $K \subset L$ uma extensão de Galois, e seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ não ramificado em L. Se $\mathfrak{P}$ é um ideal primo de $\mathcal{O}_L$ contendo $\mathfrak{p}$, então existe único $\sigma \in Gal(L/K)$ tal que*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \ mod\ \mathfrak{P} \ , \ para\ todo\ \alpha \in \mathcal{O}_L,$$

em que $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ é a norma do ideal $\mathfrak{p}$.

O único K-automorfismo σ garantido pelo Lema acima é chamado de *símbolo de Artin* e denotado por $((L/K)/\mathfrak{P})$. O símbolo de Artin satisfaz as seguintes proriedades úteis:

Corolário 10. *Seja $K \subset L$ uma extensão de Galois, e seja $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ não ramificado. Dado um ideal primo $\mathfrak{P}$ de $\mathcal{O}_L$ contendo $\mathfrak{p}$, valem as seguintes afirmações:*

(i) Se $\sigma \in Gal(L/K)$, então

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}.$$

(ii) A ordem de $((L/K)/\mathfrak{P})$ é o grau inercial $f = f_{\mathfrak{P}|\mathfrak{p}}$.

(iii) $\mathfrak{p}$ se decompõe em L se, e somente se, $((L/K)/\mathfrak{P}) = 1$.

Um caso especial a ser considerado é quando $K \subset L$ é uma extensão Abeliana. Nesta situação, o símbolo de Artin $((L/K)/\mathfrak{P})$ depende apenas do ideal primo $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. De fato, seja $\mathfrak{P}'$ outro ideal primo contendo $\mathfrak{p}$. Então, existe $\sigma \in Gal(L/K)$ para o qual $\mathfrak{P}' = \sigma(\mathfrak{P})$. Do Corolário 10, item (i), segue que

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1} = \sigma\sigma^{-1} \left(\frac{L/K}{\mathfrak{P}}\right) = \left(\frac{L/K}{\mathfrak{P}}\right),$$

haja vista que $Gal(L/K)$ é Abeliano. Nesse sentido, sempre que a extensão $K \subset L$ for Abeliana, escreveremos o símbolo de Artin como $((L/K)/\mathfrak{p})$. Indo além, um caso ainda mais especial é quando a extensão $K \subset L$ Abeliana é não ramificada, pois o símbolo de Artin estará definido para todo ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$. De fato, considere I_K o conjunto de todos ideais fracionários de $\mathcal{O}_K$. Pela Proposição 19, todo ideal fracionário $\mathfrak{a}$ admite fatoração prima na forma

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}.$$

Então, podemos definir o símbolo de Artin $((L/K)/\mathfrak{a})$ como o produto

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i},$$

que fornece um homomorfismo de grupos, chamado de *mapa de Artin*:

$$\left(\frac{L/K}{\cdot}\right) : I_K \to Gal(L/K).$$

Este mapa é sobrejetor e seu núcleo é exatamente o subgrupo P_K dos ideais fracionários principais. Logo, o Teorema do Isomorfismo nos garante que

$$Cl(\mathcal{O}_K) = \frac{I_K}{P_K} \simeq Gal(L/K).$$

Este é exatamente o enunciado do Teorema da Reciprocidade de Artin:

Teorema 19 (Teorema da Reciprocidade de Artin)**.** *Seja L o corpo de classe de Hilbert de um corpo de números K. O mapa de Artin*

$$\left(\frac{L/K}{\cdot}\right) : I_K \to Gal(L/K)$$

induz isomorfismo

$$Cl(\mathcal{O}_K) = \frac{I_K}{P_K} \simeq Gal(L/K).$$

O Teorema da Reciprocidade de Artin fornece uma *Teoria de Corpos de Classe* para extensões Abelianas não ramificadas, isto é, classifica extensões Abelianas não ramificadas de K em termos de subgrupos do grupo de classes de ideais de $\mathcal{O}_K$. Mais explicitamente, temos o seguinte corolário:

Corolário 11. *Seja K um corpo de números. Existe uma correspondência biunívoca entre as extensões Abelianas não ramificadas M de K e os subgrupos H do grupo de classes de ideais $Cl(\mathcal{O}_K)$. Além disso, se uma extensão Abeliana não ramificada $K \subset M$ corresponde ao subgrupo H de $Cl(\mathcal{O}_K)$, o mapa de Artin induz isomorfismo*

$$\frac{Cl(\mathcal{O}_K)}{H} \simeq Gal(M/K).$$

APÊNDICE B – Curvas Elípticas Complexas

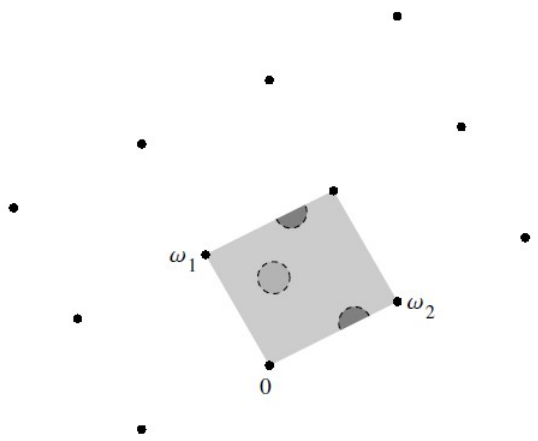
B.1 Toro Complexo

Na Seção 2.1, vimos que um reticulado é um subconjunto discreto de $\mathbb{C}$ dado por $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$, em que $\{w_1, w_2\}$ é uma base de $\mathbb{C}$ como $\mathbb{R}$-espaço vetorial. Um *toro complexo* é o quociente de $\mathbb{C}$ por um reticulado Λ:

$$\frac{C}{\Lambda} := \{z + \Lambda : z \in \mathbb{C}\}.$$

Algebricamente, um toro complexo possui a estrutura de um grupo abeliano sob a soma, herdada das propriedades de $\mathbb{C}$ como espaço vetorial. Topologicamente, um toro complexo é paralelogramo gerado pelos elementos $\{w_1, w_2\}$ em que seus lados opostos são identificados. Mais especificamente, um toro complexo é uma *superfície de Riemann*, isto é, uma variedade complexa conexa. A figura abaixo ilustra um toro complexo $\mathbb{C}/\Lambda$ gerado por $\{w_1, w_2\}$ e algumas vizinhanças:

Figura 6 – O Toro Complexo



Fonte: [5, p. 25]

A noção de funções holomorfas faz sentido quando definidas para toros complexos. De fato, mais geralmente temos o seguinte resultado para superfícies de Riemann:

Proposição 22. *Sejam X e Y superfícies de Riemann compactas. Se $f : X \to Y$ é holomorfa, então $f(X) = Y$ ou $f(X)$ é um conjunto unitário.*

Demonstração. Sendo f contínua e X compacto e conexo, temos $f(X)$ compacto e conexo. Isto mostra que $f(X)$ é fechado. O Teorema da Aplicação Aberta nos diz que f é constante

ou é aberta. Se f for constante, então $f(X)$ é unitário. Se f é aberta, então $f(X) \subset Y$ é aberto, fechado e conexo, ou seja, $f(X) = Y$. □

Como caso particular da proposição acima, segue que aplicações holomorfas não-constantes entre toros complexos são sobrejetoras.

Proposição 23. *Seja $\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ uma função holomorfa entre toros complexos. Então, existem $m, b \in \mathbb{C}$, com $m\Lambda \subset \Lambda'$, tais que $\varphi(z + \Lambda) = mz + b + \Lambda'$. Além disso, φ é invertível se, e somente se, $m\Lambda = \Lambda'$.*

Uma demonstração para esta proposição pode ser encontrada em [5], na página 26.

Corolário 12. *Seja $\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ uma função holomorfa entre toros complexos, e sejam $m, b \in \mathbb{C}$ com $m\Lambda \subset \Lambda'$. São equivalentes:*

(i) *φ é um homomorfismo de grupos abelianos,*

(ii) *$b \in \Lambda'$ e, portanto, $\varphi(z + \Lambda) = mz + \Lambda'$,*

(iii) *$\varphi(0) = 0$.*

Demonstração. Vamos provar que $(i) \implies (ii)$. Suponha φ homomorfismo de grupos. Então, para todo $z + \Lambda \in \mathbb{C}/\Lambda$, temos:

$$\begin{aligned} mz + b + \Lambda' = \varphi(z + \Lambda) &= \varphi((z + \Lambda) + (0 + \Lambda)) = \varphi(z + \Lambda) + \varphi(0 + \Lambda) \\ &= (mz + b + \Lambda') + (m0 + b + \Lambda') = mz + 2b + \Lambda'. \end{aligned}$$

A expressão acima implica que $b + \Lambda' = 0 + \Lambda'$, ou seja, $b \in \Lambda'$. Portanto, $\varphi(z + \Lambda) = mz + \Lambda'$. A implicação $(ii) \implies (iii)$ é imediata. De fato, se $b \in \Lambda'$, então

$$\varphi(0 + \Lambda) = m0 + b + \Lambda' = 0 + b + \Lambda' = 0 + \Lambda'.$$

Por fim, vamos mostrar a implicação $(iii) \implies (i)$. Sejam $z + \Lambda, w + \Lambda \in \mathbb{C}/\Lambda$. Então,

$$\begin{aligned} \varphi((z + \Lambda) + (w + \Lambda)) = \varphi((z + w) + \Lambda) &= m(z + w) + b + \Lambda' = mz + b + mw + 0 + \Lambda' \\ &= mz + b + mw + \varphi(0) + \Lambda' = mz + b + mw + (m0 + b + \Lambda') + \Lambda' \\ &= (mz + b + \Lambda') + (mw + b + \Lambda') = \varphi(z + \Lambda) + \varphi(w + \Lambda). \end{aligned}$$ □

Observação 23. Sejam $\mathbb{C}/\Lambda$ e $\mathbb{C}/\Lambda'$ toros complexos. O Corolário 12 nos mostra que existe um homomorfismo de grupos holomorfo $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ se, e somente se, existe $m \in \mathbb{C}$ não-nulo satisfazendo $m\Lambda \subset \Lambda'$. Além disso, para garantir que este homomorfismo seja um isomorfismo, é necessário e suficiente impor que $m\Lambda = \Lambda'$.

Exemplo 10. Vamos discutir um isomorfismo de particular interesse para este trabalho. Na Seção 2.1, consideramos reticulados da forma $\mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, em que o par (w_1, w_2) é um elemento de $M = \{(w_1, w_2) \in \mathbb{C}^2 \backslash \{(0,0)\} : \mathrm{Im}(w_1/w_2) > 0\}$. Observe que se $(w_1, w_2) \in M$, então $\tau = w_1/w_2$ é naturalmente um elemento do semiplano superior $\mathfrak{H}$. Dessa forma, faz sentido trabalharmos equivalentemente com reticulados da forma $\mathbb{Z}\tau \oplus \mathbb{Z}$ — conforme fizemos na Seção 4.2. Agora, sob a perspectiva do Corolário 12, se tomarmos $\Lambda = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$, em que $(w_1, w_2) \in M$, e considerarmos $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$, vemos que o fato de a condição $(1/w_2)\Lambda = \Lambda_\tau$ ser satisfeita nos garante que o mapa

$$\begin{aligned} \varphi_\tau \colon \mathbb{C}/\Lambda &\to \mathbb{C}/\Lambda_\tau \\ z + \Lambda &\mapsto \varphi_\tau(z + \Lambda) = \frac{z}{w_2} + \Lambda_\tau \end{aligned}$$

é um isomorfismo. Isto mostra que todo toro complexo é isomorfo a um toro complexo cujo reticulado é gerado por $\{\tau, 1\}$, em que $\tau \in \mathfrak{H}$. Evidentemente, este τ não é único. Embora possa existir τ' gerando o mesmo reticulado, sabemos pela Proposição 3 que τ' deve ser um elemento congruente módulo Γ_1 de τ, isto é, $\tau' = \gamma\tau$, para algum $\gamma \in \Gamma_1$. A moral é que cada toro complexo determina um ponto no semiplano superior módulo Γ_1.

Definição 26. Um homomorfismo holomorfo não-nulo entre toros complexos é chamado de *isogenia*.

B.2 Curvas Elípticas

Nesta seção vamos descrever uma forma de enxergar toros complexos como curvas cúbicas, chamadas de *curvas elípticas* [1]. Esta relação é feita através de funções meromorfas num toro complexo $\mathbb{C}/\Lambda$, que são naturalmente identificadas com funções meromorfas Λ-periódicas no plano complexo.

O exemplo fundamental de função meromorfa em um toro complexo $\mathbb{C}/\Lambda$ é a chamada *função $\wp$ de Weierstrass*, definida por

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda}{}' \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right), \qquad z \in \mathbb{C}, z \notin \Lambda.$$

Esta soma converge uniformemente em compactos de $\mathbb{C}$ fora do reticulado Λ. No entanto, não é imediato ver que $\wp$ é Λ-periódica. Mas sua derivada

$$\wp'(z) = -2 \sum_{w \in \Lambda} \frac{1}{(z-w)^3}$$

é claramente Λ-periódica. Juntanto isto ao fato de que $\wp$ é uma função par, pode-se concluir enfim que $\wp$ é Λ-periódica. Curiosamente, estes são os únicos exemplos de funções

[1] O nome curvas elípticas provém de uma relação entre as curvas cúbicas e o comprimento de arco de uma elipse.

meromorfas no toro complexo $\mathbb{C}/\Lambda$ essenciais, devido ao fato de que o corpo das funções meromorfas em $\mathbb{C}/\Lambda$ é $\mathbb{C}(\wp, \wp')$, ou seja, isto significa toda função meromorfa em $\mathbb{C}/\Lambda$ pode ser escrita como uma função racional em $\wp$ e $\wp'$. A Proposição a seguir descreve a expansão de Laurent da função $\wp$ de Weierstrass em termos das séries de Eisenstein G_k.

Proposição 24. *Seja $\wp$ a função de Weierstrass com respeito ao reticulado Λ. Então,*

(i) A expansão de Laurent de $\wp$ é dada por

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{n=2 \\ n \ par}}^{\infty} (n+1)G_{n+2}(\Lambda)z^n,$$

para todo z satisfazendo $0 < |z| < \inf\{|w| : w \in \Lambda \backslash \{0\}\}$.

(ii) $\wp$ e $\wp'$ satisfazem a relação

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda),$$

onde $g_2(\Lambda) = 60G_4(\Lambda)$ e $g_3(\Lambda) = 140G_6(\Lambda)$.

(iii) Seja $\Lambda = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$ e considere $w_3 = w_1 + w_2$. Então, a equação cúbica satisfeita por $\wp$ e $\wp'$, $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, é dada por

$$y^2 = 4(x - e_1)(x - e_2)(x - e_3), \qquad e_i = \wp(w_i/2) \text{ para } i = 1, 2, 3.$$

Além disso, essa equação é não-singular, ou seja, todas suas raízes são distintas.

Uma ideia para a demonstração desta Proposição pode ser encontrada em [5], na página 33.

Seja $\mathbb{C}/\Lambda$ um toro complexo. A Proposição 24 nos mostra que a aplicação $z \mapsto (\wp(z), \wp'(z))$ leva pontos de $\mathbb{C}$ fora do reticulado Λ em pontos (x, y) de $\mathbb{C}^2$ satisfazendo a relação $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$. Esta aplicação é uma bijeção, já que um valor $x \in \mathbb{C}$ fora do reticulado Λ é mapeado duas vezes em $\mathbb{C}/\Lambda$ via $\wp$, isto é, $x = \wp(\pm z + \Lambda)$, e os correspondentes valores y satisfazendo a equação cúbica são mapeados por $\wp'$, $y = \wp'(\pm z + \Lambda)$. Definindo o valor de pontos do reticulado Λ em um ponto no infinito conveniente, garantimos que a aplicação $z \mapsto (\wp(z), \wp'(z))$ é uma bijeção. Em suma, para cada reticulado em $\mathbb{C}$, as funções de Weirstrass associadas, $\wp$ e $\wp'$, fornecem uma bijeção

$$\{\text{toros complexos}\} \longrightarrow \{\text{curvas elípticas}\}.$$

Exemplo 11. No Exemplo 2 do Capítulo 3 utilizamos a fórmula de valência para calcular $\text{ord}_\omega E_4$ e $\text{ord}_i E_6$. Mais especificamente, vimos que, em $\mathfrak{H}$, E_4 — e portanto $g_2 = 60G_4$ — se anula apenas em ω e E_6 — e portanto $g_3 = 140G_6$ — se anula apenas em i. Em particular, o toro complexo $\mathbb{C}/\Lambda_i$ está associado bijetivamente com a curva elíptica de equação $y^2 = 4x^3 - g_2(i)x$, e o toro complexo $\mathbb{C}/\Lambda_\omega$ com a curva elíptica de equação $y^2 = 4x^3 - g_3(\omega)$.

Conforme vimos, a cada toro complexo $\mathbb{C}/\Lambda$ podemos associar uma curva elíptica via aplicações $(\wp, \wp')$. A recíproca deste resultado também é verdadeira. Mais precisamente, temos a seguinte proposição:

Proposição 25. *Seja*

$$y^2 = 4x^3 - a_2x - a_3, \qquad a_2^3 - 27a_3^2 \neq 0$$

uma curva elíptica. Então, existe um reticulado Λ *para o qual* $a_2 = g_2(\Lambda)$ *e* $a_3 = g_3(\Lambda)$.

Demonstração. Daremos uma ideia geral da demonstração. Primeiramente, vamos olhar para os casos $a_2 = 0$ e $a_3 = 0$. Nestes casos, as curvas elípticas em questão são $y^2 = 4x^3 - a_3$ e $y^2 = 4x^3 - a_2x$, respectivamente. No Exemplo 11, vimos que os toros complexos $\mathbb{C}/\Lambda_\omega$ e $\mathbb{C}/\Lambda_i$ estão associados bijetivamente com as curvas elípticas $y^2 = 4x^3 - g_3(\omega)$ e $y^2 = 4x^3 - g_2(i)x$, respectivamente. Dessa forma, podemos provar que os reticulados Λ_ω e Λ_i cumprem as condições desejadas para os casos $a_2 = 0$ e $a_3 = 0$, respectivamente. Agora, para o caso $a_2 \neq 0$ e $a_3 \neq 0$, como $j\colon \mathfrak{H} \to \mathbb{C}$ é sobrejetora, podemos encontrar $z \in \mathfrak{H}$ para o qual

$$j(z) = 1728\frac{a_2^3}{a_2^3 - 27a_3^2}.$$

Isso implica que devemos encontrar reticulado Λ satisfazendo

$$\frac{g_2^3(z)}{g_2^3(z) - 27g_3^2(z)} = \frac{a_2^3}{a_2^3 - 27a_3^2}$$

ou, equivalentemente,

$$\frac{a_2^3}{g_2^3(z)} = \frac{a_3^2}{g_3^2(z)}$$

Para qualquer $w_2 \in \mathbb{C}$ não-nulo, tome $w_1 = zw_2$ e considere o reticulado $\Lambda = \mathbb{Z}w_1 \oplus \mathbb{Z}w_2$. Então, $g_2(\Lambda) = w_2^{-4}g_2(z)$ e $g_3(\Lambda) = w_2^{-6}g_3(z)$. Escolha w_2 de modo a satisfazer a primeira condição, isto é, $w_2^{-12} = a_2^3/g_2^3(z)$. Então, a igualdade acima nos dá $w_2^{-6} = \pm a_3/g_3(z)$. Caso necessário, podemos trocar w_2 por iw_2, e isto completa a prova. □

As Proposições 24 e 25 nos mostram um fato extraordinário: os toros complexos, que são objetos analíticos (superfícies de Riemann), estão intrínsecamente relacionados com curvas elípticas, que são objetos algébricos (conjuntos soluções de equações cúbicas). Estes resultados justificam as situações em que os termos *curvas elípticas complexas* e *toros complexos* são tratados como sinônimos.