O Corpo de Classes de Hilbert Absoluto de um Corpo Quadrático Imaginário

Luís Renato Abib Finotti

DISSERTAÇÃO APRESENTADA AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA UNIVERSIDADE DE SÃO PAULO
PARA A OBTENÇÃO DO GRAU DE
MESTRE EM MATEMÁTICA

Área de Concentração: Álgebra
Orientador: Prof. Dr. Paulo Agozzini Martin

Durante a elaboração deste trabalho o autor recebeu apoio financeiro da FAPESP.

—São Paulo, fevereiro de 1997—

O Corpo de Classes de Hilbert Absoluto de um Corpo Quadrático Imaginário

Este exemplar corresponde à redação
final da dissertação devidamente corrigida
e defendida por Luís Renato Abib Finotti
e aprovada pela comissão julgadora.

São Paulo, 03 de Março de 1997.

Banca examinadora:

- Prof. Dr. Paulo Agozzini Martin (orientador) - IME-USP
- Prof. Dr. Daniel Levcovitz - IME-USP
- Prof. Dr. Luiz Manuel S. Figueiredo - IM-UFF

Agradecimentos

Aos meus pais, maiores incentivadores deste trabalho, aos quais jamais poderei agradecer o suficiente.

Ao meu orientador, Prof. Dr. Paulo Agozzini Martin, pela dedicação, estímulo, colaboração, apoio, exemplo, paciência e amizade inestimáveis.

Ao Prof. Dr. Daniel Levcovitz, pela constante e espontânea ajuda e pelos excelentes cursos e seminários, que têm sido de grande valia para a minha formação.

Aos colegas Raul A. Ferraz, Pedro de P. L. Teixeira, Patrícia H. A. Nogueira, Paul Krause e Carlos J. Watanabe, cuja amizade e amparo tornaram bem mais agradáveis estes últimos seis anos de dedicação à matemática.

À FAPESP, pelo apoio financeiro durante a elaboração desta dissertação.

Luís Renato Abib Finotti

Resumo

É um resultado clássico de Kronecker que toda extensão abeliana do corpo $\mathbb{Q}$ dos números racionais está contida num corpo de raízes da unidade. Assim, certos valores da função exponencial geram a extensão abeliana maximal de $\mathbb{Q}$. Tal construção "explícita" também é possível para um corpo quadrático imaginário. Tem-se que usar os invariantes de classes ("valores singulares" da função modular j) e também valores de uma certa função relacionada com a função $\wp$ de Weierstrass. O objetivo principal deste texto é achar, o que foi originalmente feito por H. Weber, geradores explícitos da extensão abeliana *não ramificada* maximal de um corpo quadrático imaginário K, o assim chamado corpo de classes de Hilbert absoluto. Será provado que tais geradores são os invariantes de classes.

Abstract

It is a classical result of Kronecker that every abelian extension of the field $\mathbb{Q}$ of the rational numbers is contained in a field of roots of unity. So certain values of the exponential function generates the maximal abelian extension of $\mathbb{Q}$. Such an "explicit" construction is also possible for an imaginary quadratic field. One has to use the class invariants ("singular values" of the modular function j) and also values of a certain function related to the Weierstrass $\wp$-function. The main purpose of this text is to find, what was originaly done by H. Weber, explicit generators of the maximal *unramified* abelian extension of a imaginary quadratic field K, the so called absolute Hilbert class field. It will be proved that such generators are the class invariants.

Índice

Introdução

Um dos resultados mais fundamentais da teoria de extensões abelianas de corpos é o seguinte teorema:

Teorema (Kronecker-Weber). *Se $L/\mathbb{Q}$ é uma extensão abeliana finita do corpo dos racionais, então existe uma raiz da unidade ζ tal que $L \subset \mathbb{Q}(\zeta)$.*

Conseqüentemente, a extensão abeliana maximal de $\mathbb{Q}$, que denotaremos por $\mathbb{Q}^{ab}$, é dada por

$$\mathbb{Q}^{ab} = \mathbb{Q}(\{\zeta \in \mathbb{C} : \zeta^m = 1, \text{ para algum } m \in \mathbb{Z}, m > 1\}).$$

Assim, este teorema nos dá geradores explícitos de $\mathbb{Q}^{ab}$ por valores de uma função analítica, a saber $e^{2\pi iz}$, calculada nos pontos de torção de $\mathbb{R}/\mathbb{Z}$. Um resultado análogo, devido a H. Weber, é válido para um corpo quadrático imaginário K. Para podermos enunciá-lo, vamos introduzir alguns resultados da teoria de curvas elípticas[1].

Seja E uma curva elíptica, dada pelo quociente $\mathbb{C}/\Gamma$, onde Γ é um reticulado de $\mathbb{C}$. (Observamos aqui que, como curva algébrica, tal curva elíptica pode ser dada por zeros de uma equação da forma

$$y^2 = 4x^3 - g_2(\Gamma)x - g_3(\Gamma).)$$

Como $\mathbb{C}/\Gamma$ é isomorfa a $\mathbb{C}/(\lambda\Gamma)$, podemos considerar que Γ é gerado por 1 e τ.

Um endomorfismo de E pode ser identificado com um endomorfismo de seu recobrimento universal $\mathbb{C}$ que mantém Γ fixo. Desta forma, tal endomorfismo deve ser a multiplicação por um complexo λ tal que $\lambda, \lambda\tau \in \Gamma$.

[1]Todos estes resutados serão devidamente enunciados e provados nos capítulos seguintes.

Portanto, o conjunto dos endomorfismos de E pode ser associado a um sub-anel $A(E)$ dos complexos que obviamente contém $\mathbb{Z}$. Se tal conjunto contém $\mathbb{Z}$ propriamente, então dizemos que E *admite multiplicação complexa*.

Temos ainda que, se E admite multiplicação complexa, τ pertence a um corpo quadrático imaginário K, e $A(E) \subset \mathcal{O}_K$, onde $\mathcal{O}_K$ denota o conjunto dos inteiros algébricos de K. Na verdade $A(E)$ é uma *ordem* de K (i.e., é um sub-anel de $\mathcal{O}_K$ que contém $\mathbb{Z}$ e de posto 2 como $\mathbb{Z}$-módulo).

Se $A(E) = \mathcal{O}_K$, então Γ é um ideal fracionário de K, e reciprocamente, dado Γ um ideal fracionário de um corpo quadrático imaginário K, então $E = \mathbb{C}/\Gamma$ é uma curva elíptica tal que $A(E) = \mathcal{O}_K$. Portanto, duas curvas E e E', tais que $A(E) = A(E') = \mathcal{O}_K$, são isomorfas se os ideais associados a elas são homotéticos, ou seja, estão na mesma *classe de ideais*.

Dada uma curva elíptica E definida por

$$y^2 = 4x^3 - g_2 x - g_3$$

definimos o seu *invariante modular*

$$j_E := 1728\frac{g_2^3}{\Delta} \quad (\Delta := g_2^3 - 27g_3^2).$$

Duas curvas elípticas complexas são isomorfas se, e somente se, seus invariantes modulares forem iguais. Desta forma, j nos dá uma função das classes de ideais $\mathsf{k}_1, \ldots, \mathsf{k}_h$ de um corpo quadrático imaginário K; os números $j(\mathsf{k}_i)$ são valores singulares da *função modular* j, são dois a dois distintos e são chamados de *invariantes de classes* de K.

Se $K = \mathbb{Q}(\sqrt{-D})$ é um corpo quadrático imaginário e E é uma curva elíptica com $A(E) = \mathcal{O}_K$ e invariante j_E, o grupo dos automorfismos de E, que denotamos por $\mathrm{Aut}(E)$, é igual ao grupo das unidades de $\mathcal{O}_K$. Tal grupo é cíclico de ordem 2 (resp. 4, resp. 6) quando $D \neq 1, 3$ (resp. $D = 1$, resp. $D = 3$). Dado um reticulado Γ de $\mathbb{C}$, definimos:

$$\tau(u, \Gamma) := (-1)^{e/2}\, \wp(u, \Gamma)^{e/2}\, g^{(e)}(\Gamma),$$

onde e é a ordem de $\mathrm{Aut}(E)$, $\wp$ é a função $\wp$ de Weierstrass e

$$g^{(2)} := 2^7 3^5 g_2 g_3/\Delta$$
$$g^{(3)} := 2^8 3^4 g_2^2/\Delta$$
$$g^{(6)} := 2^9 3^6 g_3/\Delta.$$

Podemos agora enunciar o resultado em questão:

Teorema (Weber-Fueter). *Sejam K um corpo quadrático imaginário e L/K uma extensão abeliana finita de K. Ainda mais, sejam (ω_1, ω_2) uma base de algum ideal Γ de K e $j(\mathfrak{k})$ um invariante de classes de K. Então:*

1. *se L/K for não ramificada, então $L \subset K(j(\mathfrak{k}))$;*
2. *se L/K for ramificada, então $L \subset K(j(\mathfrak{k}), \tau((a\omega_1 + b\omega_2)/n, \Gamma)$, para certos a, b e n inteiros, com $n \neq 0$.*

Conseqüentemente:

$$K^{\mathrm{ab}} = K(j(\mathfrak{k}), \{\tau((a\omega_1 + b\omega_2)/n, \Gamma) : a, b, n \in \mathbb{Z},\ n > 0\}).$$

Observação. Apesar do nome, o teorema como enunciado acima é em parte devido a H. Hasse, já que, embora Weber e Fueter tenham achado geradores para tal extensão maximal, ambos usaram funções mais complicadas que τ para gerá-la. Hasse foi o primeiro a provar que τ poderia dar tais geradores.

Observamos que os pontos $(a\omega_1 + b\omega_2)/n$ são os pontos de torção da curva elíptica $\mathbb{C}/\Gamma$. Desta forma temos um resultado bastante similar ao feito por Kronecker para o corpo $\mathbb{Q}$.

Uma outra maneira de obtermos K^{ab} é adicionarmos a K as raízes da unidade, os valores de $j(z)$ para $z \in K^*$, com $\mathrm{Im}(z) > 0$, e as raízes quadradas dos elementos do corpo assim obtido.

O objetivo desta dissertação é provar o *primeiro item* deste teorema, ou seja, provar que $K(j(\mathfrak{k}))$, para qualquer $\mathfrak{k}$ pertencente ao grupo de classes de ideais $\mathcal{C}(K)$ de K, é a extensão abeliana não ramificada maximal do corpo quadrático imaginário K (chamamos tal extensão de o *corpo de classes de Hilbert absoluto* de K). Os passos da prova são essencialmente:

1. Provar que os $j(\mathfrak{k}_i)$'s são inteiros algébricos.
2. Provar a congruência

$$j(\mathfrak{p}^{-1}\mathfrak{k}) \equiv j(\mathfrak{k})^{N(\mathfrak{p})} \pmod{\mathfrak{p}},$$

onde $\mathfrak{p}$ é um ideal primo de K, $\mathfrak{k}$ é uma classe de ideal, $N(\mathfrak{p})$ é a norma de $\mathfrak{p}$, valendo para todos os ideais primos $\mathfrak{p}$ de K com grau 1 em relação a $\mathbb{Q}$ (i.e., com $N(\mathfrak{p}) = p$, p primo de $\mathbb{Q}$), a menos de um número finito.

3. Provar, usando resultados da teoria de corpos de classes, que o grupo de classes de ideais $\mathcal{C}(K)$ de K é isomorfo ao grupo de Galois da maior extensão abeliana não ramificada de K sobre K. Além disso, se $\mathfrak{k} \in \mathcal{C}(K)$ e $\sigma_{\mathfrak{k}}$ é o elemento do grupo de Galois associado a $\mathfrak{k}$ pelo isomorfismo em questão, então

$$\sigma_{\mathfrak{k}}(j(\mathfrak{k}_i)) = j(\mathfrak{k}^{-1}\mathfrak{k}_i).$$

4. Provar, também usando resultados da teoria de corpos de classes, que $K(j(\mathfrak{k}_i))$ não depende de i e é o corpo de classes de Hilbert absoluto de K.

No capítulo 1, damos algumas idéias básicas de formas modulares, as quais servirão de ferramentas na busca do resultado principal. Nesse capítulo, seguimos basicamente [Ser73], capítulo VII, definindo formas e funções modulares, as funções j e Δ e demonstramos o princípio da q-expansão.

No capítulo 2, damos apenas algumas noções básicas da teoria de curvas elípticas, como parametrização (pela função $\wp$ de Weierstrass), isomorfismos e suas relações com toros, seguindo basicamente [Lan86] e [Sil85].

Nos três capítulos seguintes, seguimos respectivamente, os capítulos III, IV e V de [BCH+66]. O capítulo 3, basicamente contém o passo 1 e o capítulo 4 contém o passo 2. O capítulo 5 conclui o nosso objetivo, contendo os passos 3 e 4. Neste capítulo damos, inicialmente, as noções básicas de corpos de classes (da maneira clássica) e enunciamos diversos resultados desta teoria que são necessários para se obter o nosso objetivo final, sem nos preocuparmos com as provas dos mesmos. A última seção contém alguns cálculos dos invariantes de classes em casos simples.

Vamos assumir que o leitor tenha conhecimentos básicos de álgebra abstrata, principalmente de teoria de Galois, e de funções de variáveis complexas; assumiremos também, conhecimentos não tão básicos de teoria dos números, incluindo inteiros algébricos, teoria de ideais, valorizações, ramificações, decomposição de ideais primos, entre outros tópicos. (Uma possível referência seria [Gol71], capítulos 2 a 5.) Embora, em geral, sejam citadas referências para os resultados usados, supomos que haja uma certa familiaridade com o assunto, principalmente com suas definições. Ainda em teoria de números, como já mencionamos, vamos usar resultados da teoria de corpos de classes, para os quais não vamos supor tal familiaridade, i.e., vamos dar as definições necessárias e enunciar todos os resultados que usaremos. (Os teoremas citados podem ser encontrados em [Has26]; outras referências têm tais resultados,

como o próprio [Gol71], mas como usamos a teoria de corpos de classes em sua forma clássica, [Has26] é mais apropriado.) Também supomos conhecimentos básicos de superfícies de Riemann (capítulos 1 e 2 de [For81], por exemplo), mas, de uma forma geral, sua falta não chega a comprometer a compreensão do texto em si.

Capítulo 1

Formas Modulares

1.1 O Grupo Modular

1.1.1 Definições e Notações

Durante todo este texto usaremos as seguintes definições e notações:

Definição 1. 1. $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, i.e., $\mathbb{H}$ representa o semi-plano complexo superior.

2. $\mathbf{SL}_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ e } ad - bc = 1 \right\}$.

3. $\mathbb{P}^1 := \mathbb{C} \cup \{\infty\}$, i.e., denotaremos por $\mathbb{P}^1$ o plano complexo extendido, que pode ser identificado com a esfera de Riemann.

4. $\mathbf{SL}_2(\mathbb{R})$ age naturalmente em $\mathbb{P}^1$ da seguinte forma: dados $z \in \mathbb{P}^1$ e $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{R})$, então:

$$gz := \begin{cases} \dfrac{az+b}{cz+d} & \text{se } z \neq \infty \text{ e } z \neq -d/c, \\ a/c & \text{se } z = \infty \text{ e } c \neq 0, \\ \infty & \text{se } z = \infty \text{ e } c = 0 \text{ ou se } z = -d/c. \end{cases}$$

Um cálculo simples mostra que:

$$\mathrm{Im}(gz) = \frac{\mathrm{Im}(z)}{|cz+d|^2}. \tag{1.1}$$

Logo, $\mathbb{H}$ fica invariante por $\mathbf{SL}_2(\mathbb{R})$. Por outro lado, é claro também que as matrizes $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $-\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ agem da mesma forma. Assim, podemos identificar estas duas matrizes, ou seja, considerar o grupo $\mathbf{PSL}_2(\mathbb{R}) := \mathbf{SL}_2(\mathbb{R})/\{\pm 1\}$ quando quisermos apenas pensar em termos da ação do grupo $\mathbf{SL}_2(\mathbb{R})$ em $\mathbb{H}$. Na verdade, pode-se provar que $\mathbf{PSL}_2(\mathbb{R}) = \mathrm{Aut}(\mathbb{H})$, onde $\mathrm{Aut}(\mathbb{H})$ é o conjunto dos automorfismos de $\mathbb{H}$.

Definição 2. O grupo $\mathbf{G} := \mathbf{SL}_2(\mathbb{Z})/\{\pm 1\}$ é chamado de *grupo modular*.

No entanto, para não sobrecarregarmos a notação, vamos denotar pelos mesmos símbolos $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z})$ e sua imagem em $\mathbf{G}$.

1.1.2 Domínio Fundamental do Grupo Modular

Definição 3. Definimos $S, T \in \mathbf{G}$ como os elementos de $\mathbf{G}$ com representantes

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

respectivamente.

Assim, temos:

$$Sz = -\frac{1}{z}, \quad Tz = z+1$$

e

$$S^2 = 1, \quad (ST)^3 = 1.$$

Definimos também:

Definição 4. Seja $D := \{z \in \mathbb{C} : -1/2 \leq |z| \leq 1/2 \text{ e } |z| \geq 1\}$ (ver a figura 1.1 a seguir).

Mostraremos que D é o que chamamos de *domínio fundamental* da ação de $\mathbf{G}$ em $\mathbb{H}$, mais precisamente:

Teorema 1. *1. Para todo $z \in \mathbb{H}$, existe $g \in \mathbf{G}$ tal que $gz \in D$.*

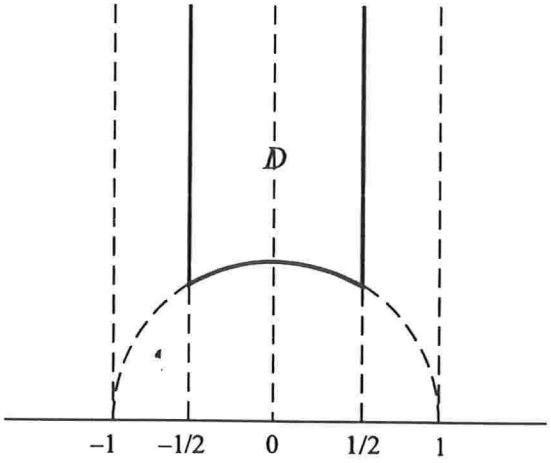

Figura 1.1: O Domínio Fundamental D de $\mathbf{G}$.

2. *Se* $z, z' \in D$ *e* $z \equiv z'$ (mod $\mathbf{G}$), *então* $\mathrm{Re}(z) = \pm 1/2$ *e* $z = z' \pm 1$, *ou* $|z| = 1$ *e* $z' = -1/z$.

3. *Seja* $z \in D$ *e* $I(z) := \{g \in \mathbf{G} : gz = z\}$ *(i.e., o estabilizador de* z *em* $\mathbf{G}$*). Temos que* $I(z) = \{1\}$, *exceto se:*

   (a) $z = i$, *e então* $I(z) = \langle S \rangle$ *(grupo de ordem 2);*

   (b) $z = \rho = e^{\frac{2\pi i}{3}}$, *e então* $I(z) = \langle S\,T \rangle$ *(grupo de ordem 3);*

   (c) $z = -\bar{\rho} = e^{\frac{\pi i}{3}}$, *e então* $I(z) = \langle T\,S \rangle$ *(grupo de ordem 3).*

Dos dois primeiros itens do teorema acima decorre, imediatamente, o seguinte corolário:

Corolário 1. *A projeção canônica de* D *em* $\mathbb{H}/\mathbf{G}$ *é sobrejetora e sua restrição ao interior de* D *é injetora.*

Temos ainda o seguinte teorema:

Teorema 2. *O grupo* $\mathbf{G}$ *é gerado por* S *e* T.

Demonstração dos teoremas 1 e 2. Seja $\mathbf{G}'$ o sub-grupo de $\mathbf{G}$ gerado por S e T. Tomemos $z \in \mathbb{H}$. Vamos mostrar agora que existe $g' \in \mathbf{G}'$ tal que $g'z \in D$, o que será suficiente para provarmos o item 1, do teorema 1. Se

$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ é um elemento de $\mathbf{G}'$, temos que vale a equação (1.1). Como $c, d \in \mathbb{Z}$, é *finito* o número de pares (c, d) tais que $|cz + d|$ é menor que um número qualquer fixado. Logo, existe $g \in \mathbf{G}'$ tal que $\mathrm{Im}(gz)$ é máximo. Seja n um inteiro tal que $T^n(gz)$ tenha parte real entre $-1/2$ e $1/2$. Assim, o elemento $z' = T^n(gz)$ estará em D se $|z'| \geq 1$. Mas, se $|z'| < 1$, temos que $\mathrm{Im}(-1/z')$ é estritamente maior que $\mathrm{Im}(z')$, o que é impossível por hipótese, já que $\mathrm{Im}(gz) = \mathrm{Im}(z')$. Logo $g' = T^n g$ leva este $z \in \mathbb{H}$ em D.

Provaremos agora os itens 2 e 3 do teorema 1. Seja $z \in D$ e tomemos $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{G}$ tal que $gz \in D$. Podemos supor que $\mathrm{Im}(gz) \geq \mathrm{Im}(z)$, já que podemos trocar z e g por gz e g^{-1}. Assim, devemos ter $|cz + d| \leq 1$. Se $c \geq 2$, isto é claramente impossível, restando-nos analisar os casos em que $c \in \{0, 1, -1\}$.

Se $c = 0$, temos que $d = \pm 1$ e assim g é uma translação por $\pm b$. Como $\mathrm{Re}(z)$ e $\mathrm{Re}(gz)$ estão ambos entre $-1/2$ e $1/2$, temos que ou $b = 0$, e então g é identidade, ou $b = \pm 1$ e então $\mathrm{Re}(z) = \mp 1/2$ e $\mathrm{Re}(gz) = \pm 1/2$.

Se $c = 1$, como $|z + d| \leq 1$, temos que $d = 0$ a menos que $z = \rho$ (resp. $z = -\bar{\rho}$), caso no qual $d \in \{0, 1\}$ (resp. $d \in \{0, -1\}$). Se $d = 0$, temos que $|z| \leq 1$, e como $z \in D$, vale que $|z| = 1$. Por outro lado, $ad - bc = 1$ implica que $b = -1$, e portanto $gz = a - 1/z$. Como vale $|z| = 1$, temos que $\mathrm{Re}(z) = -\mathrm{Re}(-1/z)$, e logo $\mathrm{Re}(gz) = a - \mathrm{Re}(z)$, e como já discutimos acima, devemos ter $a = 0$, a menos que $\mathrm{Re}(z) = \pm 1/2$ (e assim, $z = -\bar{\rho}$ ou $z = \rho$), quando a também pode ser ∓ 1. Assim, se $z \notin \{\rho, -\bar{\rho}\}$, temos que $gz = -1/z$. No caso $z = \rho$, $d = 1$ implica que $a - b = 1$ e $g\rho = a - 1/(1 + \rho) = a + \rho$, e então $a \in \{0, 1\}$. De maneira análoga podemos discutir o caso em que $z = -\bar{\rho}$.

O caso em que $c = -1$ é análogo ao caso $c = 1$, visto que podemos mudar os sinais de a, b, c e d sem alterar o elemento de $\mathbf{G}$ que esta nova matriz representa. Desta forma provamos os itens 2 e 3 do teorema 1.

Resta agora apenas provar o teorema 2, i.e., que $\mathbf{G} = \mathbf{G}'$. Seja $g \in \mathbf{G}$. Tomemos z_0 no *interior* de D (como por exemplo $z_0 = 2i$), e seja $z = gz_0$. Como já vimos acima, existe $g' \in \mathbf{G}'$ tal que $g'z \in D$. Temos que os pontos z_0 e $g'z = g'gz_0$ são equivalentes módulo $\mathbf{G}$ e z_0 está no interior de D. Logo, pelos itens 2 e 3 do teorema 1, provados acima, temos que $g'g = 1$, e então $g \in \mathbf{G}'$, o que conclui a prova. □

1.2 Formas Modulares

1.2.1 Definições

Definição 5. Seja $k \in \mathbb{Z}$. Uma função f é dita *fracamente modular* de peso $2k$ se f for meromorfa em $\mathbb{H}$ e verifica a relação[1]

$$f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right), \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}). \tag{1.2}$$

Uma equivalência desta definição é dada pela seguinte proposição:

Proposição 1. *Seja f uma função meromorfa em $\mathbb{H}$. A função f é fracamente modular de peso $2k$ se, e somente se, ela satisfizer as duas seguintes relações:*

$$f(z+1) = f(z) \tag{1.3}$$

e

$$f\left(-\frac{1}{z}\right) = z^{2k} f(z) \tag{1.4}$$

Demonstração. Suponha que f é fracamente modular de peso $2k$. Substituindo T e S na fórmula (1.2), obtemos as equações (1.3) e (1.4) respectivamente. Reciprocamente, como $\mathbf{G}$ é gerado por T e S e a fórmula (1.2) vale para estas duas, pode-se provar, indutivamente, que vale para todo $g \in \mathbf{G}$:
se vale para $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, temos:

$$f(T(z)) = (c(Tz)+d)^{-2k} f\left(\frac{a(Tz)+b}{c(Tz)+d}\right),$$

ou seja,

$$f(z+1) = (cz+(c+d))^{-2k} f\left(\frac{az+(b+a)}{cz+(c+d)}\right);$$

mas, pela equação (1.3), $f(z+1) = f(z)$, e conseqüentemente a fórmula (1.2) vale para a matriz $\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} T$. Analogamente, prova-se

[1] Alguns autores dizem de peso $-2k$ e outros de peso k, ao invés de $2k$.

que vale para $\begin{pmatrix} a & b \\ c & d \end{pmatrix} S$. Concluímos, assim, que vale para toda a matriz gerada por S e T. □

Suponha que a equação (1.3) seja verificada. Podemos então expressar f em termos de $q := e^{2\pi iz}$. A função de q que é igual a $f(z)$, para $q = e^{2\pi iz}$, denotaremos daqui em diante (como padrão de notação) por $\tilde{f}$; f meromorfa em $\mathbb{H}$ implica que $\tilde{f}$ é meromorfa para $0 < |q| < 1$. Se $\tilde{f}$ se extende meromorficamente (resp. holomorficamente) à origem, dizemos, por abuso de linguagem, que f é *meromorfa no infinito* (resp. *holomorfa no infinito*). Isto implica que $\tilde{f}$ admite uma expansão de Laurent em alguma vizinhança de $q = 0$ da forma

$$\tilde{f}(q) = \sum_{n=-N}^{\infty} a_n q^n \tag{1.5}$$

para algum $N \in \mathbb{N}$ (resp. $N = 0$).

Definição 6. Uma função fracamente modular é dita *modular* se é meromorfa no infinito. Quando f é holomorfa no infinito, definimos $f(\infty) := \tilde{f}(0)$ e chamamos este valor de *valor de f no infinito* .

Definição 7. Uma função modular holomorfa em $\mathbb{H} \cup \{\infty\}$ é chamada de *forma modular*; se tal função vale zero no infinito, é chamada *forma parabólica*.

Assim, uma forma modular de peso $2k$ admite uma expansão em série da forma:

$$f(z) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi inz} \tag{1.6}$$

que converge para $|q| < 1$ (i.e., para $\mathrm{Im}(z) > 0$) e que satisfaz a identidade (1.4). Ainda mais, será uma forma parabólica se $a_0 = 0$.

Exemplos 1. 1. Se f e f' são formas modulares de pesos $2k$ e $2k'$, o produto ff' é uma forma modular de peso $2k + 2k'$.

2. Pode-se provar que a função

$$q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \cdots$$

é uma forma parabólica de peso 12 ([Ser73], pg. 95).

1.2.2 Funções Modulares e Funções de Reticulados

Definição 8. Um *reticulado* é um subgrupo Γ de um $\mathbb{R}$-espaço vetorial V, verificando uma das seguintes condições (equivalentes entre si):

1. Γ é discreto e V/Γ é compacto;
2. Γ é discreto e gera o espaço V;
3. existe uma $\mathbb{R}$-base $\{e_1, \ldots, e_n\}$ de V que é uma $\mathbb{Z}$-base de Γ, i.e., $\Gamma = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n$.

Denotaremos por $\mathcal{R}$ os conjuntos dos reticulados de $\mathbb{C}$, considerando $\mathbb{C}$ um $\mathbb{R}$-espaço vetorial. Além disso, usaremos M para denotar o conjunto dos pares ordenados $(\omega_1, \omega_2) \in (\mathbb{C}^*)^2$, tais que $\mathrm{Im}(\omega_1/\omega_2) > 0$.

Assim, a um par $(\omega_1, \omega_2) \in M$ podemos associar um reticulado

$$\Gamma(\omega_1, \omega_2) := \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

com base $\{\omega_1, \omega_2\}$. Desta forma, obtemos uma aplicação de M em $\mathcal{R}$ que é claramente sobrejetora.

Seja $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z})$ e seja $(\omega_1, \omega_2) \in M$. Defimos então,

$$\omega_1' = a\omega_1 + b\omega_2 \quad \text{e} \quad \omega_2' = c\omega_1 + d\omega_2,$$

que nos dá uma ação de $\mathbf{SL}_2(\mathbb{Z})$ em M. Podemos ver facilmente que $\{\omega_1', \omega_2'\}$ também é uma base de $\Gamma(\omega_1, \omega_2)$ (pois $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ é inversível como matriz com entradas inteiras). Além disso, se $z = \omega_1/\omega_2$, e $z' = \omega_1'/\omega_2'$, temos

$$z' = \frac{az + b}{cz + d} = gz.$$

Logo $\mathrm{Im}(z') > 0$, e portanto $(\omega_1', \omega_2') \in M$.

Proposição 2. *Dois elementos de M definem o mesmo reticulado se, e somente se, são congruentes módulo* $\mathbf{SL}_2(\mathbb{Z})$.

Demonstração. Que a condição é suficiente, vimos acima. Reciprocamente, se (ω_1, ω_2) e (ω_1', ω_2') são dois elementos de M que definem o mesmo reticulado, existe uma matriz $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ com coeficientes inteiros que é inversível (com a inversa também inteira) tal que

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Logo $\det(g) = \pm 1$. Com um simples cálculo pode-se ver que se $\det(g) < 0$, o sinal de $\mathrm{Im}(\omega_1'/\omega_2')$ é oposto ao sinal de $\mathrm{Im}(\omega_1/\omega_2)$. Como ambos devem ser positivos, $\det(g) = 1$, o que deixa provada a proposição.

□

Assim, podemos identificar $\mathcal{R}$ com o quociente de M pela ação de $\mathbf{SL}_2(\mathbb{Z})$. Podemos definir também uma ação de $\mathbb{C}^*$ em $\mathcal{R}$ (resp. em M) por:

$$\Gamma \mapsto \lambda\Gamma \quad (\text{resp. } (\omega_1, \omega_2) \mapsto (\lambda\omega_1, \lambda\omega_2))$$

com $\lambda \in \mathbb{C}^*$. O quociente $M/\mathbb{C}^*$ é identificado com $\mathbb{H}$ via $(\omega_1, \omega_2) \mapsto z = \omega_1/\omega_2$, e por esta identificação, a ação de $\mathbf{SL}_2(\mathbb{Z})$ em M e a ação de $\mathbf{G} = \mathbf{SL}_2(\mathbb{Z})/\pm 1$ em $\mathbb{H}$ são compatíveis. Assim:

Proposição 3. *A aplicação $(\omega_1, \omega_2) \mapsto \omega_1/\omega_2$ induz uma bijeção entre os conjuntos $\mathcal{R}/\mathbb{C}^*$ e $\mathbb{H}$. (E assim, um elemento de $\mathbb{H}/\mathbf{G}$ pode ser identifiacado com um reticulado definido a menos de homotetia.)*

Observação. Associando o reticulado Γ ao *toro* $\mathbb{C}/\Gamma$, temos que dois toros, associadas aos reticulados Γ e Γ', são isomorfos, como superfícies de Riemann, se, e somente se, tais reticulados são homotéticos ([For81], pg. 9). Isso nos dá uma descrição de $\mathbb{H}/\mathbf{G} = \mathcal{R}/\mathbb{C}^*$ como o *conjunto de classes de isomorfismo de toros*.

Consideremos agora uma função $F : \mathcal{R} \to \mathbb{C}$, e seja $k \in \mathbb{Z}$. Dizemos que F tem peso $2k$ se

$$F(\lambda\Gamma) = \lambda^{-2k} F(\Gamma) \tag{1.7}$$

para todos $\Gamma \in \mathcal{R}$ e todos $\lambda \in \mathbb{C}^*$.

Seja F uma função de reticulados como acima. Se $(\omega_1, \omega_2) \in M$, vamos denotar por $F(\omega_1, \omega_2)$ o valor de F no reticulado $\Gamma(\omega_1, \omega_2)$. Assim, a fórmula (1.7) pode ser escrita como:

$$F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-2k} F(\omega_1, \omega_2). \tag{1.8}$$

Além disso, temos que F é invariante pela ação de $\mathbf{SL}_2(\mathbb{Z})$.

Esta fórmula (1.8) mostra que o produto $\omega_2^{2k} F(\omega_1, \omega_2)$ depende apenas de $z = \omega_1/\omega_2$, pois

$$\omega_2^{2k} F(\omega_1, \omega_2) = F\left(\frac{\omega_1}{\omega_2}, 1\right).$$

Assim, existe uma função f, definida em $\mathbb{H}$, dada por

$$f(z) := F(z, 1),$$

tal que

$$\omega_2^{-2k} f(\omega_1/\omega_2) = F(\omega_1, \omega_2). \tag{1.9}$$

Como F é invariante pela ação de $\mathbf{SL}_2(\mathbb{Z})$, temos que f satisfaz a identidade (1.2). E, reciprocamente, se temos uma f que satisfaz a identidade (1.2), a fórmula (1.9) dá-nos uma função F definida em $\mathcal{R}$ com peso $2k$. Assim, podemos associar funções modulares de peso $2k$ a funções de reticulados de peso $2k$.

1.2.3 Séries de Eisenstein

Lema 1. *Seja Γ um reticulado em $\mathbb{C}$. As séries*

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

convergem para $\sigma > 2$, onde o símbolo $\sum'$ indica que a somatória percorre todos elementos de Γ exceto o zero[2].

[2]Em geral vamos usar o símbolo $\sum'$ para indicar que a somatória está definida *"onde faz sentido"*.

Demonstração. Suponhamos que $\Gamma = \Gamma(\omega_1, \omega_2)$. Temos que

$$\mathrm{Im}(\omega_1/\omega_2).\,\mathrm{Im}(\omega_2/\omega_1) \neq 0,$$

pois caso contrário Γ não seria um reticulado. Assim, para todo par $(n_1, n_2) \in \mathbb{Z}^2$, vale:

$$|n_1\omega_1 + n_2\omega_2| = |\omega_2| \left| n_1 \frac{\omega_1}{\omega_2} + n_2 \right| \geq |n_1| \left| \mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) \right| |\omega_2|$$

e, analogamente,

$$|n_1\omega_1 + n_2\omega_2| \geq |n_2| \left| \mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right) \right| |\omega_1|.$$

Seja, então $m := \frac{1}{2} \min\left\{ |\omega_2| \left| \mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right) \right|, |\omega_1| \left| \mathrm{Im}\left(\frac{\omega_2}{\omega_1}\right) \right| \right\}$, e portanto $m > 0$. Assim, as duas equações acima resultam

$$|n_1\omega_1 + n_2\omega_2| \geq m\,(|n_1| + |n_2|)$$

para todo par $(n_1, n_2) \in \mathbb{Z}^2$. Por outro lado, temos $4n$ pares tais que $|n_1| + |n_2| = n$, para um n inteiro positivo fixado. Como

$$\sum_{\gamma \in \Gamma}{}' \frac{1}{|\gamma|^\sigma} = \sum_{n_1, n_2 \in \mathbb{Z}}{}' \frac{1}{|n_1\omega_1 + n_2\omega_2|^\sigma},$$

onde $\sum'$ indica, neste caso, a soma em todos os pares $(n_1, n_2) \in \mathbb{Z}^2$, exceto o $(0, 0)$, temos

$$\begin{aligned} \sum_{\gamma \in \Gamma}{}' \frac{1}{|\gamma|^\sigma} &\leq \sum_{n_1, n_2 \in \mathbb{Z}}{}' \frac{1}{m^\sigma\,(|n_1| + |n_2|)^\sigma} \\ &= m^{-\sigma} \sum_{n=1}^{\infty} 4n \frac{1}{n^\sigma} \\ &= 4m^{-\sigma} \sum_{n=1}^{\infty} \frac{1}{n^{\sigma-1}}. \end{aligned}$$

Se $\sigma > 2$, a última série à direita da desigualdade acima é convergente, e logo a primeira também o é, o que finaliza a prova. □

Definição 9. Seja k um inteiro maior que 1. Se Γ é um reticulado de $\mathcal{R}$, definimos

$$G_k(\Gamma) := \sum_{\gamma \in \Gamma}{}' \frac{1}{\gamma^{2k}} \tag{1.10}$$

(que sabemos que converge absolutamente pelo lema 1). Esta é chamada *série de Eisenstein* de índice k (ou índice $2k$ segundo alguns autores).

Claramente temos que G_k tem peso $2k$, e como vimos na sub-seção anterior, podemos considerar G_k como função em M, dada por:

$$G_k(\omega_1, \omega_2) := \sum_{m,n \in \mathbb{Z}}{}' \frac{1}{(m\omega_1 + n\omega_2)^{2k}}, \tag{1.11}$$

e como função em $\mathbb{H}$, que pelas equações (1.9) e (1.11), é dada por:

$$G_k(z) := \sum_{m,n \in \mathbb{Z}}{}' \frac{1}{(mz + n)^{2k}}. \tag{1.12}$$

Proposição 4. *Seja k um inteiro maior que 1. A série de Eisenstein $G_k(z)$ é uma forma modular de peso $2k$. Além disso, temos $G_k(\infty) = 2\zeta(2k)$, onde ζ denota a função zeta de Riemann.*

Observação. Lembramos que a função ζ é definida por:

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}$$

onde $\mathcal{P}$ representa o conjunto de todos os inteiros positivos primos. Além disso, temos que esta função é holomorfa e não nula em $\{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$ ([Ser73], pg. 69).

Demonstração. Pelos argumentos anteriores, sabemos que G_k satisfaz a fórmula (1.2). Resta então mostrar que f é holomorfa em $\mathbb{H} \cup \{\infty\}$. Suponhamos, inicialmente, que z está no domínio fundamental D. Assim:

$$|mz+n|^2 = m^2 z\bar{z} + 2mn\,\mathrm{Re}(z) + n^2.$$

e se $mn \geq 0$, temos:

$$|mz+n|^2 \geq m^2 - mn + n^2 = |m\rho - n|^2,$$

ou, se $mn < 0$, temos:

$$|mz+n|^2 \geq m^2 + mn + n^2 = |m(-\bar{\rho}) - n|^2.$$

Pelo lema 1, as séries

$$\sum_{m,n\in\mathbb{Z}}{}' \frac{1}{|m\rho - n|^{2k}} \quad \text{e} \quad \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{|m(-\bar{\rho}) - n|^{2k}}$$

são convergentes. Isto mostra que a série G_k converge *normalmente* em D, i.e., uniformemente em seus compactos. Assim G_k é holomorfa em D ([Ahl66], pg. 217). Mas, aplicando o mesmo resultado a $G_k(g^{-1}z)$, temos que G_k é holomorfa em cada um dos gD, para $g \in \mathbf{G}$. Como pelo teorema 1 estes conjuntos cobrem $\mathbb{H}$, temos que G_k é holomorfa em $\mathbb{H}$.

Resta ainda mostrar que é holomorfa no infinito e calcular seu valor neste ponto. Para isto, basta mostrar que G_k tem limite para $\mathrm{Im}(z) \to \infty$. Para isso, podemos supor que z permanece em D. Como temos a convergência uniforme em D, podemos comutar o limite com a somatória. Desta forma, os termos correspondentes a $m \neq 0$ vão para zero e os outros vão para $1/n^{2k}$. Assim:

$$\lim_{\mathrm{Im}(z)\to\infty} G_k(z) = \sum_{n\in\mathbb{Z}}{}' \frac{1}{n^{2k}} = 2\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = 2\zeta(2k).$$

□

Exemplos 2. As séries de Eisenstein de menores pesos são G_2 e G_3, que têm pesos 4 e 6 respectivamente. É usual, devido à teoria de curvas elípticas (como veremos no capítulo 2), substituí-las por múltiplos, dados por:

$$g_2 := 60G_2, \quad g_3 := 140G_3. \tag{1.13}$$

Assim, $g_2(\infty) = 120\zeta(4)$ e $g_3(\infty) = 280\zeta(6)$. Usando os valores conhecidos da função ζ, temos que:

$$g_2(\infty) = \frac{4}{3}\pi^4, \quad g_3(\infty) = \frac{8}{27}\pi^6. \tag{1.14}$$

Portanto, definindo

$$\Delta := g_2^3 - 27g_3^2, \tag{1.15}$$

temos que $\Delta(\infty) = 0$, ou seja, Δ é uma forma parabólica de peso 12. Na verdade, podemos escrever, por um teorema devido a Jacobi, Δ da seguinte forma:

$$\Delta = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}. \tag{1.16}$$

Este teorema pode ser encontrado em [Ser73], pg. 95.

1.3 O Espaço das Formas Modulares

1.3.1 Zeros e Polos de uma Função Modular

Definição 10. Sejam f uma função meromorfa em $\mathbb{H}$, não identicamente nula, e p um ponto em $\mathbb{H}$. O inteiro n tal que $f(z)/(z-p)^n$ é holomorfa e não nula em p, é chamado *ordem de f em p* e é denotado por $v_p(f)$. Além disso, para $p = \infty$, definimos $v_p(f)$ como a ordem de $\tilde{f}$ em $q = 0$.

Quando f é uma função modular de peso $2k$, a identidade (1.2) mostra que $v_p(f) = v_{g(p)}(f)$, para todo $g \in \mathbf{G}$. Em outras palavras, $v_p(f)$ depende apenas da imagem de p em $\mathbb{H}/\mathbf{G}$.

Finalmente, denotamos por e_p a ordem do estabilizador do ponto p em $\mathbf{G}$. Assim, temos $e_p = 2$ (resp. $e_p = 3$) se $p \equiv i \pmod{\mathbf{G}}$ (resp. $p \equiv \rho \pmod{\mathbf{G}}$), nos outros casos, temos $e_p = 1$.

Teorema 3. *Seja f uma função modular de peso $2k$, não identicamente nula. Então:*

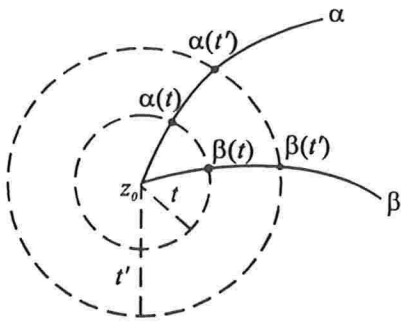

Figura 1.2: Curvas α e β.

$$v_\infty(f) + \sum_{p \in \mathbb{H}/\mathbf{G}} \frac{1}{e_p} v_p(f) = \frac{k}{6}. \tag{1.17}$$

Observação. Podemos reescrever a fórmula acima da seguinte forma:

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{p \in \mathbb{H}/\mathbf{G}}^{*} v_p(f) = \frac{k}{6}, \tag{1.18}$$

onde o símbolo $\sum^*$ indica a soma em todos os elementos de $\mathbb{H}/\mathbf{G}$ distintos das classes do i e do ρ.

No entanto, para mostrarmos o teorema acima, usaremos o seguinte lema:

Lema 2. *Seja f uma função meromorfa em uma vizinhança de um ponto $z_0 \in \mathbb{C}$, com z_0 seu único possível polo nesta vizinhança. Sejam também α e β duas curvas tais que $\alpha(0) = \beta(0) = z_0$ e $|\alpha(t) - z_0| = |\beta(t) - z_0| = t$, para $t \in [0, \epsilon]$ (ver figura 1.2), com $\epsilon > 0$. Se o ângulo entre β e α em z_0 é $2\pi/m$, então:*

$$\lim_{t \to 0} \frac{1}{2\pi i} \int_{\beta(t)}^{\alpha(t)} \frac{f'(z)}{f(z)}\, dz = \frac{v_{z_0}(f)}{m},$$

onde a integral acima é calculada no arco de circunferência (com orientação positiva) de centro em z_0 e que vai de $\beta(t)$ a $\alpha(t)$.

Demonstração do lema 2. Seja $v_{z_0}(f) = n$. Assim, $f(z) = (z - z_0)^n g(z)$, com $g(z)$ holomorfa em z_0 e $g(z_0) \neq 0$. Portanto:

$$f'(z) = n(z - z_0)^{n-1} g(z) + (z - z_0)^n g'(z),$$

e logo,

$$\frac{f'(z)}{f(z)} = \frac{n}{z - z_0} + \frac{g'(z)}{g(z)}.$$

Integrando, temos:

$$\begin{aligned} \frac{1}{2\pi i} \int_{\beta(t)}^{\alpha(t)} \frac{f'(z)}{f(z)}\, dz &= \frac{1}{2\pi i} \int_{\beta(t)}^{\alpha(t)} \frac{n}{z - z_0}\, dz + \frac{1}{2\pi i} \int_{\beta(t)}^{\alpha(t)} \frac{g'(z)}{g(z)}\, dz \\ &= \frac{1}{2\pi i} \int_{\beta(t)-z_0}^{\alpha(t)-z_0} \frac{n}{z}\, dz + \frac{1}{2\pi i} \int_{\beta(t)}^{\alpha(t)} \frac{g'(z)}{g(z)}\, dz \\ &= \frac{n}{2\pi i}(\log(\alpha(t) - z_0) - \log(\beta(t) - z_0)) \\ &\quad + \frac{1}{2\pi i}(\log(g(\alpha(t))) - \log(g(\beta(t)))). \end{aligned} \tag{1.19}$$

Como $g(z_0) \neq 0$ e g é holomorfa em uma vizinhança de z_0, temos que:

$$\lim_{t \to 0} \log(g(\alpha(t))) = \lim_{t \to 0} \log(g(\beta(t))) = \log(g(z_0)),$$

o que implica que levando a fórmula (1.19) ao limite de t tendendo a zero, temos:

$$\begin{aligned} \lim_{t \to 0} \frac{1}{2\pi i} \int_{\beta(t)}^{\alpha(t)} \frac{f'(z)}{f(z)}\, dz &= \lim_{t \to 0} \frac{n}{2\pi i}(i \arg(\alpha(t) - z_0) - i \arg(\beta(t) - z_0)) \\ &= \frac{n}{2\pi} \cdot \frac{2\pi}{m} = \frac{n}{m}, \end{aligned}$$

lembrando que $\log(z) := \log|z| + i \arg(z)$, onde $\arg(z)$ é a função *argumento*, que dá a medida do ângulo de vértice na origem passando por z e 1 (ver figura 1.3). □

Vamos agora à prova do teorema:

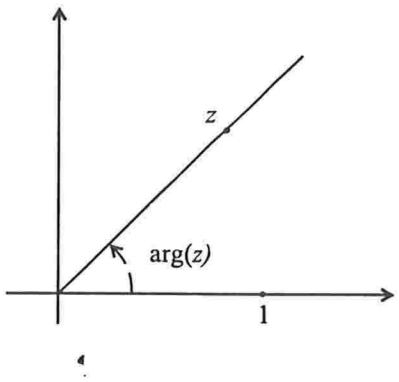

Figura 1.3: A função $\arg(z)$.

Demonstração do teorema 3. Como $\tilde{f}$ é meromorfa, existe $r > 0$ tal que $\tilde{f}$ não tem zeros ou polos para $0 < q < r$, pois, caso contrário, teríamos uma seqüência de polos convergindo para a origem, o que implicaria num absurdo, já que por definição, os polos de uma função meromorfa são isolados. Assim, f não tem zeros ou polos para $\mathrm{Im}(z) > e^{2\pi r}$. Logo, a parte do domínio fundamental limitada por $\mathrm{Im}(z) \leq e^{2\pi r}$, que denotaremos por D_r, é *compacta*, e portanto, temos apenas um número finito de zeros ou polos em D_r, e por conseguinte, em $\mathbb{H}/\mathbf{G}$. Portanto a somatória em questão faz sentido.

Suponhamos inicialmente que f não tem zeros ou polos na fronteira de D, exceto, possivelmente, i, ρ e $-\bar{\rho}$. Existe um caminho α, como está representado na figura 1.4, cujo interior contém todos os zeros e polos de f não congruentes a i e a ρ. Pelo teorema dos resíduos, temos:

$$\frac{1}{2\pi i}\int_{\alpha}\frac{f'(z)}{f(z)}\,dz = \sum_{p\in\mathbb{H}/\mathbf{G}}^{*} v_p(f).$$

Por outro lado,

1. A mudança de variáveis $q = e^{2\pi i z}$ leva o arco EA em um círculo ω centrado em $q = 0$, com orientação negativa, não contendo nenhum zero ou polo de $\tilde{f}$, exceto talvez o zero. Assim:

$$\frac{1}{2\pi i}\int_{E}^{A}\frac{f'(z)}{f(z)}\,dz = \frac{1}{2\pi i}\int_{\omega}\frac{\tilde{f}'(q)}{\tilde{f}(q)}\,dq = -v_{\infty}(f)$$

2. A integral de $\frac{1}{2\pi i}\frac{f'(z)}{f(z)}$ no círculo que contém o arco BB', orientado negativamente, vale $-v_{\rho}(f)$. Quando o raio deste círculo tende a zero, o ângulo

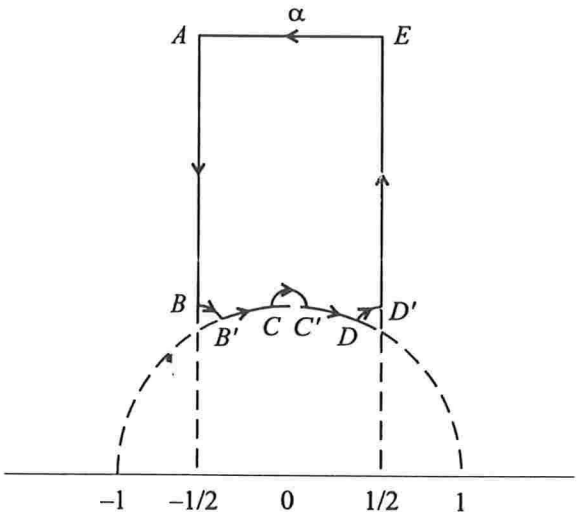

Figura 1.4: Curva α.

$\widehat{B\rho B'}$ tende a $2\pi/6$, e assim, pelo lema 2, temos:

$$\frac{1}{2\pi i}\int_B^{B'} \frac{f'(z)}{f(z)} \to -\frac{1}{6}v_\rho(f).$$

Analogamente, quando os raios dos arcos CC' e DD' tendem a zero, temos:

$$\frac{1}{2\pi i}\int_C^{C'} \frac{f'(z)}{f(z)} \to -\frac{1}{2}v_i(f)$$

e

$$\frac{1}{2\pi i}\int_D^{D'} \frac{f'(z)}{f(z)} \to -\frac{1}{6}v_\rho(f).$$

3. T leva o arco AB no arco ED'. Como $f(Tz) = f(z)$, temos:

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

4. S leva o arco $B'C$ no arco DC'. Como $f(Sz) = z^{2k}f(z)$, temos:

$$\frac{d(f(Sz))}{f(Sz)} = 2k\frac{dz}{z} + \frac{d(f(z))}{f(z)},$$

e assim:

$$\begin{aligned}\frac{1}{2\pi i}\left(\int_{B'}^{C}\frac{f'(z)}{f(z)}\,dz+\int_{C'}^{D}\frac{f'(z)}{f(z)}\,dz\right) &= \frac{1}{2\pi i}\int_{B'}^{C}\left(\frac{f'(z)}{f(z)}-\frac{(f\circ S)'(z)}{(f\circ S)(z)}\right)dz\\ &= \frac{1}{2\pi i}\int_{B'}^{C}\frac{-2k}{z}\,dz\\ &\to -2k\left(-\frac{1}{12}\right)=\frac{k}{6}\end{aligned}$$

quando o raio dos arcos BB', CC' e DD' tendem a zero.

Das duas expressões que obtivemos para $\frac{1}{2\pi i}\int_{\alpha}\frac{f'(z)}{f(z)}\,dz$, e passando ao limite, conseguimos a fórmula (1.18).

Suponhamos agora que temos um polo ou zero de f, que indicaremos por λ, em

$$\left\{z\in\mathbb{C}:\mathrm{Re}(z)=-\frac{1}{2}\ \text{e}\ \mathrm{Im}(z)>\frac{\sqrt{3}}{2}\right\}.$$

Repetimos a prova anterior, com o contorno α modificado em uma vizinhança de λ e de $T\lambda$, como o ilustrado na figura 1.5, e observamos que o arco em volta de λ é levado por T no arco em volta de $T\lambda$ com a orientação invertida (e, portanto, as integrais nestes arcos anulam-se).

Se tal zero ou polo estiver em $|z|=1$, procedemos da mesma forma, mas usando S no lugar de T; se houver mais de um zero ou polo, basta repetir o procedimento para cada ponto.

□

Observação. Uma prova mais simples é possível se definirmos uma estrutura analítica complexa no compactificado de $\mathbb{H}/\mathbf{G}$, como em [BCH+66], capítulo II.

1.3.2 A Álgebra das Formas Modulares

Definição 11. Se k é um inteiro, denotaremos por M_{2k} (resp. M_{2k}^0) o $\mathbb{C}$-espaço vetorial das formas modulares (resp. das formas parabólicas) de peso $2k$.

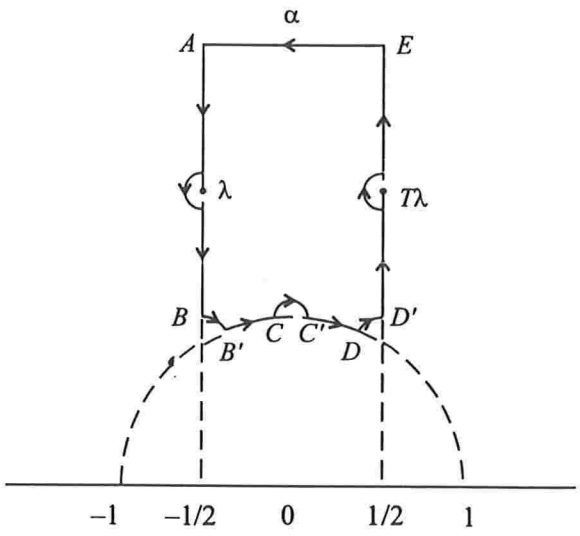

Figura 1.5: Curva α.

Por definição, M_{2k}^0 é o núcleo do homomorfismo de $\mathbb{C}$-espaços vetorias, de M_{2k} em $\mathbb{C}$, definido por $f \mapsto f(\infty)$. Assim, $\dim(M_{2k}/M_{2k}^0) \leq 1$. Ainda mais, para $k \geq 2$, a série de Eisenstein G_k é um elemento de M_{2k} tal que $G_k(\infty) \neq 0$, como vemos na proposição 4. Assim:

$$M_{2k} = M_{2k}^0 \oplus \mathbb{C} \cdot G_k \quad (\text{para } k \geq 2)$$

Finalmente recordamos que denotamos por Δ o elemento $g_2^3 - 27g_3^2$ de M_{12}^0, onde $g_2 = 60G_2$ e $g_3 = 140G_3$.

Teorema 4. *1. Temos $M_{2k} = \{0\}$ para $k < 0$ e $k = 1$.*

2. Para $k = 0, 2, 3, 4, 5$, M_{2k} é um espaço vetorial de dimensão 1, com bases $1, G_2, G_3, G_4, G_5$, respectivamente, e, além disso, $M_{2k}^0 = \{0\}$.

3. A multiplicação por Δ define um isomorfismo entre M_{2k-12} e M_{2k}^0.

Demonstração. Seja f um elemento não nulo de M_{2k}. Usando a fórmula (1.18) para este caso, temos que o primeiro membro contém apenas termos maiores ou iguais a zero, pois f não tem polos, e logo, teremos $k \geq 0$. Deste modo, temos que se $k < 0$, $f = 0$, e portanto, $M_{2k} = \{0\}$. Como $1/6$ não pode ser escrito na forma $n + n'/2 + n''/3$, com $n, n', n'' \geq 0$, temos que

$k \neq 1$, e, como anteriormente, isto implica que $M_2 = \{0\}$. Provamos então o *primeiro* item.

Vamos agora provar o *terceiro* item: apliquemos agora a fórmula (1.18) para $f = G_k$, com $k = 2$. Podemos escrever $2/6$ na forma $n + n'/2 + n''/3$, com $n, n', n'' \geq 0$, somente se $n, n' = 0$ e $n'' = 1$. Isto mostra que devemos ter $v_\rho(G_2) = 1$, e, para $p \not\equiv \rho \pmod{\mathbf{G}}$, $v_p(G_2) = 0$. Usando o mesmo argumento para G_3, chegamos à conclusão que $v_i(G_3) = 1$, e para os outros pontos não congruentes a i, $v_p(G_3) = 0$. Logo Δ não tem zero em i (pois $g_3(i) = 0$ e $g_2(i) \neq 0$), e assim, não é identicamente nula. Como o peso de Δ é 12 e $v_\infty(\Delta) \geq 1$, como vimos anteriormente, temos novamente pela fórmula (1.18) que $v_\infty(\Delta) = 1$ e $v_p(\Delta) = 0$ para $p \neq \infty$. Em outras palavras, Δ *não se anula em* $\mathbb{H}$ *e tem um zero simples no infinito*. Consideremos então $\phi : M_{2k-12} \to M_{2k}^0$ a multiplicação por Δ, ou seja, $\phi(f) := f \cdot \Delta$. Tal função é claramente um homomorfismo de espaços vetoriais. Se $f \cdot \Delta$ é nula em D, então f é necessariamente nula em D, pois Δ não se anula. Portanto, ϕ é injetora. Tomemos agora $f \in M_{2k}^0$. Como Δ não se anula em $\mathbb{H}$, então f/Δ é holomorfa em $\mathbb{H}$. Mas como $f \in M_{2k}^0$, temos $v_\infty(f) \geq 1$ e sabemos que $v_\infty(\Delta) = 1$, e logo $v_\infty(f/\Delta) = v_\infty(f) - 1 \geq 0$, i.e., f/Δ é holomorfa no infinito. Como f/Δ claramente tem peso $2k-12 = 2(k-6)$, $f/\Delta \in M_{2k-12}$, e $\phi(f/\Delta) = f$, ou seja ϕ é sobrejetora e portanto um isomorfismo de $\mathbb{C}$-espaços vetoriais.

Para provarmos o *segundo* item, seja $k \leq 5$. Assim, temos que $k - 6 < 0$, e logo, $M_{2k}^0 = \{0\}$ pelos itens já provados. Logo $\dim(M_{2k}) \leq 1$. Como 1, G_2, G_3, G_4 e G_5 são elementos não nulos de M_0, M_4, M_6, M_8 e M_{10}, respectivamente, temos que $\dim(M_{2k}) = 1$, para $k = 0, 2, 3, 4, 5$, o que conclui a prova.

□

Corolário 2. *Temos:*

$$\dim(M_{2k}) = \begin{cases} [k/6] & \text{se } k \equiv 1 \pmod 6,\ k \geq 0 \\ [k/6] + 1 & \text{se } k \not\equiv 1 \pmod 6,\ k \geq 0 \end{cases}, \tag{1.20}$$

onde $[x]$ *denota a parte inteira de* x, *i.e., o maior inteiro* n *tal que* $n \leq x$.

Demonstração. A fórmula vale para $0 \leq k < 6$, pelos itens 1 e 2 do teorema 4. Além disso, $[k/6]$ e $[k/6] + 1$ aumentam em uma unidade quando trocamos k por $k + 6$, pelo item 3. Logo, a fórmula vale para $k \geq 0$. □

Corolário 3. *O espaço M_{2k} tem como base a família de monômios da forma $G_2^{\alpha}G_3^{\beta}$, com α e β inteiros positivos tais que $2\alpha + 3\beta = k$.*

Demonstração. Mostraremos inicialmente que tais monômios geram M_{2k}. O caso em que $k \leq 3$. é uma conseqüência imediata dos itens 1 e 2 do teorema 4. Para $k \geq 4$, provaremos por indução sobre k. Sejam γ e δ inteiros positivos com $2\gamma + 3\delta = k$ (que é possível para todo $k \geq 2$). A forma modular $g = G_2^{\gamma}G_3^{\delta}$ é não nula no infinito. Se $f \in M_{2k}$, existe $\lambda \in \mathbb{C}$ tal que $f - \lambda g$ é uma forma parabólica, e assim, é igual a Δh para $h \in M_{2k-12}$, pelo item 3 do teorema anterior. Aplicando a hipótese de indução para h, temos que

$$\begin{aligned} f =& \lambda g + \Delta \sum_{2c+3d=k-6} \lambda_{cd} G_2^c G_3^d \\ =& \lambda G_2^{\gamma} G_3^{\delta} + \sum_{2c+3d=k-6} (60)^3 \lambda_{cd} G_2^{c+3} G_3^d - \sum_{2c+3d=k-6} 27 \cdot (140)^2 \lambda_{cd} G_2^c G_3^{d+2}, \end{aligned}$$

com $2c + 3d = k - 6$ e $\lambda_{cd} \in \mathbb{C}$. Como $2(c+3) + 3d = 2c + 3(d+2) = k$, provamos que os monômios em questão geram M_{2k}.

Resta mostrar que são linearmente independentes. Se não fossem, teríamos que existiriam $\lambda_{ab} \in \mathbb{C}$, não todos nulos, tais que:

$$\sum_{2a+3b=k} \lambda_{ab} G_2^a G_3^b = 0.$$

Mas, como $b = (k - 2a)/3$, teríamos que

$$\sum_{2a+3b=k} \left[\lambda_{ab} G_3^{k/3} \left(\frac{G_2^3}{G_3^2} \right)^{a/3} \right] = 0,$$

e como $G_3 \not\equiv 0$,

$$\sum_{2a+3b=k} \left[\lambda_{ab} \left(\frac{G_2^3}{G_3^2} \right)^{a/3} \right] = 0.$$

Portanto $(G_2^3/G_3^2)^{1/3}$ seria constante (pois um polinômio tem somente um número finito de raízes), i.e., existiria $\lambda \in \mathbb{C}$ tal que $G_2^3 = \lambda G_3^2$. Mas isto é um absurdo, pois G_2 se anula em ρ e G_3 não.

□

Observação. Seja $M = \bigoplus_{k=0}^{\infty} M_{2k}$ a álgebra graduada dada pela soma direta dos M_k's e seja $\epsilon : \mathbb{C}[X,Y] \to M$ o homomorfismo que leva X em G_2 e Y em G_3. O corolário 3 é equivalente a dizer que ϵ é um isomorfismo. Assim, podemos identificar M com a álgebra polinomial $\mathbb{C}[G_2, G_3]$.

1.3.3 O Invariante Modular

Definição 12. Seja j, chamada de *invariante modular*, a função dada por:

$$j := \frac{1728 g_2^3}{\Delta}. \tag{1.21}$$

Proposição 5. *1. A função j é uma função modular de peso 0.*

2. j é holomorfa em $\mathbb{H}$ e tem um polo simples no infinito.

3. j induz uma bijeção entre $\mathbb{H}/\mathbf{G}$ e $\mathbb{C}$.

Demonstração. O *primeiro* item é conseqüência imediata do fato que g_2^3 e Δ são ambas funções modulares de peso 12.

O *segundo* item decorre de que $\Delta \neq 0$ em $\mathbb{H}$ e tem um zero simples no infinito, enquanto g_2 é não nula no infinito.

Para provarmos o *terceiro* item, basta mostrarmos que se $\lambda \in \mathbb{C}$, a forma modular $f_\lambda := 1728 g_2^3 - \lambda\Delta$ tem um único zero módulo $\mathbf{G}$. Aplicando a fórmula (1.18) para $f = f_\lambda$ e $k = 6$, temos $n + n'/2 + n''/3 = 1$, com n, n' e n'' inteiros não negativos, e as únicas possibilidades são:

$$(n, n', n'') = (1,0,0) \text{ ou } (0,2,0) \text{ ou } (0,0,3)$$

e como $f_\lambda(\infty) \neq 0$, temos que f_λ tem um único zero em $\mathbb{H}/\mathbf{G}$. □

Proposição 6. *Seja f uma função meromorfa em $\mathbb{H}$. As seguintes propriedades são equivalentes:*

1. f é uma função modular de peso 0;

2. f é o quociente de duas funções modulares de mesmo peso;

3. f é uma função racional de j.

Demonstração. Que 3 implica 2, e que 2 implica 1 é imediato. Assim, precisamos apenas mostrar que 1 implica 3. Seja, então, f função modular de peso 0. Como para esta prova podemos multiplicar tal f por um polinômio qualquer em j, podemos supor que f é holomorfa em $\mathbb{H}$, pois se $z_0 \in \mathbb{H}$ é polo de ordem m de f, então $(j(z)-j(z_0))^m f(z)$ é holomorfa em z_0, e f só pode ter um número finito de polos módulo $\mathbf{G}$, como vimos na demonstração do teorema 3. Além disso, como $\Delta(\infty) = 0$, existe n tal que $g := \Delta^n f$ é holomorfa no infinito. Logo, g é uma forma modular de peso $12n$, e pelo corolário 3, podemos escrevê-la como combinação linear de monômios da forma $G_2^\alpha G_3^\beta$ com $2\alpha + 3\beta = 6n$. Por linearidade, basta provarmos que $G_2^\alpha G_3^\beta/\Delta^n$ é uma função racional de j. Mas a relação $2\alpha + 3\beta = 6n$ implica que $p := \alpha/3$ e $q := \beta/2$ são inteiros, e assim, podemos escrever $G_2^\alpha G_3^\beta/\Delta^n = G_2^{3p} G_3^{2q}/\Delta^{p+q}$. Conseqüentemente, reduzimos a prova a mostrar que G_2^3/Δ e G_3^2/Δ são funções racionais de j. Mas, pelas equações (1.13) e (1.21),

$$\frac{G_2^3}{\Delta} = \frac{j}{1728 \cdot 60^3}.$$

Para a segunda, usando as equações (1.13) e (1.15), temos que

$$G_3^2 = \frac{g_2^3 - \Delta}{140^2 \cdot 27}$$

e logo,

$$\frac{G_3^2}{\Delta} = \frac{1}{140^2 \cdot 27}(j - 1).$$

□

Observações. 1. Como já mencionamos acima, é possível definir de maneira natural uma estrutura de variedade complexa analítica no compactificado $\overline{\mathbb{H}/\mathbf{G}}$ de $\mathbb{H}/\mathbf{G}$. A proposição 5 nos diz então que j define uma bijeção entre $\overline{\mathbb{H}/\mathbf{G}}$ e a esfera de Riemann $\mathbb{P}^1$. Da mesma forma, a proposição 6 representa o fato bem conhecido que as únicas funções meromorfas na esfera são as funções racionais.

2. O coeficiente $1728 = 2^6 3^3$ foi introduzido para que j tenha resíduo 1 no infinito. Além disso, este fator garante que a expansão de j como série de potências em $q = e^{2\pi i z}$ tenha apenas coeficientes inteiros. Na verdade temos:

$$j(z) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n. \tag{1.22}$$

com $c_n \in \mathbb{Z}$, conforme veremos na proposição 9.

1.4 Expansões no Infinito

1.4.1 Os Números de Bernoulli B_k

Definição 13. Definimos os *números de Bernoulli*, denotados por B_k, dados pela série de potências:

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{x^{2k}}{(2k)!}. \tag{1.23}$$

Uma tabela de valores dos números de Bernoulli para k de 1 a 14 pode ser encontrada em [Ser73], pg. 91. Além disso, os B_k's dão-nos os valores da função zeta de Riemann para inteiros positivos pares:

Proposição 7. *Se k é um inteiro maior que 1, temos:*

$$\zeta(2k) = \frac{2^{2k-1}}{(2k)!} B_k \pi^{2k}. \tag{1.24}$$

Demonstração. Colocando $2iz$ no lugar de x na fórmula (1.23), obtemos:

$$\frac{2iz}{e^{2iz} - 1} = 1 - iz + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{(2iz)^{2k}}{(2k)!},$$

ou seja,

$$\frac{2iz}{e^{2iz} - 1} + iz = 1 - \sum_{k=1}^{\infty} B_k \frac{(2z)^{2k}}{(2k)!}.$$

Desenvolvendo o primeiro membro, temos:

$$\frac{2iz}{e^{2iz}-1}+iz=\frac{2iz}{e^{iz}(e^{iz}-e^{-iz})}+iz=\frac{z}{e^{iz}\sin(z)}+iz$$
$$=z\left(\frac{e^{-iz}+i\sin(z)}{\sin(z)}\right)=z\cot(z).$$

Portanto:

$$z\cot(z)=1-\sum_{k=1}^{\infty}B_k\frac{2^{2k}z^{2k}}{(2k)!}. \tag{1.25}$$

Derivando, membro a membro, o logarítmo da fórmula bem conhecida ([Ahl66], pg. 195):

$$\sin(z)=z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{n^2\pi^2}\right), \tag{1.26}$$

obtemos para o primeiro membro

$$\frac{d}{dz}\log(\sin(z))=\cot(z),$$

e para o segundo

$$\frac{d}{dz}\left(\log(z)+\sum_{n=1}^{\infty}\log\left(1-\frac{z^2}{n^2\pi^2}\right)\right)=\frac{1}{z}+\sum_{n=1}^{\infty}\left[\frac{n^2\pi^2}{n^2\pi^2-z^2}\cdot\left(\frac{-2z}{n^2\pi^2}\right)\right]$$
$$=\frac{1}{z}-2\sum_{n=1}^{\infty}\frac{z}{n^2\pi^2-z^2}.$$

Assim, multiplicando por z e igualando as equação anteriores temos

$$z\cot(z)=1-2\sum_{n=1}^{\infty}\frac{z^2}{n^2\pi^2-z^2};$$

mas como

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

obtemos

$$z\cot(z) = 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\frac{z^{2k}}{n^{2k}\pi^{2k}}. \tag{1.27}$$

Comparando as equações (1.25) e (1.27), temos a equação (1.24).

□

1.4.2 Expansão em Série das Funções G_k

O objetivo desta seção é dar a expanção das séries de Eisenstein G_k em relação a $q = e^{2\pi iz}$. Para isto, começaremos com o seguinte lema:

Lema 3. *Para $k \geq 2$, temos:*

$$\sum_{m\in\mathbb{Z}}\frac{1}{(m+z)^k} = \frac{1}{(k-1)!}(-2\pi i)^k\sum_{n=1}^{\infty}n^{k-1}q^n. \tag{1.28}$$

Demonstração. Podemos obter de (1.26) a fórmula

$$\begin{aligned}\pi\cot(\pi z) &= \frac{1}{z} + \sum_{m=1}^{\infty}\frac{2z}{z^2-m^2}\\ &= \frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m}+\frac{1}{z-m}\right),\end{aligned} \tag{1.29}$$

(ou podemos simplesmente verificar em [Ahl66], pg. 187).

Por outro lado:

$$\pi\cot(\pi z) = \pi i\frac{q+1}{q-1} = \pi i - \frac{2\pi i}{1-q} = \pi i - 2\pi i\sum_{n=0}^{\infty}q^n. \tag{1.30}$$

Comparando estas duas últimas equações, obtemos:

$$\frac{1}{z} + \sum_{m=1}^{\infty}\left(\frac{1}{z+m}+\frac{1}{z-m}\right) = \pi i - 2\pi i\sum_{n=0}^{\infty}q^n. \tag{1.31}$$

Derivando a equação (1.31) sucessivamente, temos a equação (1.28).

□

Definição 14. Denotaremos por $\sigma_k(n)$ a somatória:

$$\sigma_k(n) = \sum_{d|n} d^k.$$

isto é, a soma das k-ésimas potências dos divisores positivos de n.

Com esta definição:

Proposição 8. *Para todo inteiro $k \geq 2$, temos:*

$$G_k(z) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n. \tag{1.32}$$

Demonstração. Temos:

$$\begin{aligned} G_k(z) &= \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{(nz+m)^{2k}} \\ &= \sum_{n=-\infty}^{-1}\sum_{m\in\mathbb{Z}}\frac{1}{(nz+m)^{2k}} + \sum_{m=-\infty}^{-1}\frac{1}{m^{2k}} \\ &\quad + \sum_{m=1}^{\infty}\frac{1}{m^{2k}} + \sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}}\frac{1}{(nz+m)^{2k}} \\ &= 2\zeta(2k) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}}\frac{1}{(nz+m)^{2k}} \end{aligned}$$

Aplicando a fórmula (1.28), colocando nz onde tínhamos z e $2k$ onde tínhamos k, obtemos:

$$\begin{aligned} G_k(z) &= 2\zeta(2k) + 2\frac{(-2\pi i)^{2k}}{(2k-1)!}\sum_{d=1}^{\infty}\sum_{a=1}^{\infty} d^{2k-1}q^{ad} \\ &= 2\zeta(2k) + 2\frac{(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n. \end{aligned}$$

□

1.4.3 O Princípio da q-Expansão

O objetivo desta sub-seção é provar o *"Princípio da q-Expansão"*, que será freqüentemente usado nos capítulos seguintes. Para tal, precisaremos da seguinte proposição:

Proposição 9. *Temos:*

$$\Delta = (2\pi)^{12} q \left(1 + \sum_{n=1}^{\infty} a_n q^n\right) \quad e \quad j = q^{-1} + \sum_{n=0}^{\infty} c_n q^n, \tag{1.33}$$

com os a_n's e c_n's inteiros.

Demonstração. Sejam

$$U := \sum_{n=1}^{\infty} \sigma_3(n) q^n$$

e

$$V := \sum_{n=1}^{\infty} \sigma_5(n) q^n.$$

Temos, aplicando a proposição 8 e lembrando que $\zeta(4) = \pi^4/(2 \cdot 3^2 \cdot 5)$:

$$\begin{aligned} g_2 = 60G_2 &= 60\left(2\zeta(4) + 2\frac{(2\pi i)^4}{3!}U\right) \\ &= (2\pi)^4 \frac{1}{2^2\, 3}(1 + 240\, U), \end{aligned} \tag{1.34}$$

e, analogamente,

$$g_3 = 140G_3 = (2\pi)^6 \frac{1}{2^3\, 3^3}(1 - 504\, V). \tag{1.35}$$

Assim:

$$\Delta = (2\pi)^{12} \frac{1}{2^6\, 3^3}\left[(1 + 240\, U)^3 - (1 - 504\, V)^2\right]. \tag{1.36}$$

Mas

$$\begin{aligned}(1+240\,U)^3-(1-504\,V)^2 &= 1+2^4\,3^3\,5\,U+2^8\,3^3\,5^2\,U^2+2^{12}\,3^3\,5^2\,U^3\\ &\quad -1+2^4\,3^2\,7\,V-2^6\,3^4\,7^2\,V^2\\ &= 2^4\,3^2\,5\,U+2^4\,3^3\,7\,V+2^8\,3^3\,5^2\,U^2\\ &\quad -2^6\,3^4\,7^2\,V^2+2^{12}\,3^3\,5^2\,U^3\end{aligned} \tag{1.37}$$

Como U e V não têm termos livres de q, Δ também não tem (refletindo o fato que $\Delta(\infty)=0$). O termo de Δ em q só pode vir de $(2^4\,3^2\,5\,U+2^4\,3^3\,7\,V)$, e expandindo vemos que $(2\pi)^{12}$ é tal coeficiente de q. Deste modo, podemos escrever

$$\Delta=(2\pi)^{12}\frac{1}{2^6\,3^3}q\left[2^6\,3^3+\sum_{n=1}^{\infty}a'_n q\right],$$

ou

$$\Delta=(2\pi)^{12}q\left[1+\sum_{n=1}^{\infty}a_n q^n\right]\quad\left(\text{onde } a_n=\frac{a'_n}{2^6\,3^3}\right).$$

Os a_n's serão inteiros se $(2^6\,3^3)|a'_n$ para todo $n\geq 1$. Mas, pela fórmula (1.37), basta que $2^2\,3$ divida os coeficientes de $(5U+7V)$. Se convencionarmos que duas séries de potências são congruentes módulo n se seus coeficientes de mesmo grau o forem, a afirmação anterior é equivalente a:

$$5\sigma_3(n)\equiv -7\sigma_5(n)\pmod{2^2 3}.$$

Como $-7\equiv 5\pmod{2^2 3}$, e[3] $(5,2^2 3)=1$, basta provarmos que

$$\sigma_3(n)\equiv\sigma_5(n)\pmod{2^2 3}. \tag{1.38}$$

Mas, se $d\in\mathbb{N}$ e 2 divide d, temos que 4 divide (d^5-d^3). Se 2 não divide d, este pode ser escrito na forma $d=2q+1$. Mas:

$$d^5-d^3\equiv(5(2q)+1)-(3(2q)+1)\equiv 4q\equiv 0\pmod 4.$$

Logo, sempre temos que 4 divide d^5-d^3.

[3]Usaremos a notação (n,m) para o máximo divisor comum dos inteiros n e m, como é usual.

Analogamente, 3 divide $d^5 - d^3$ para qualquer $d \in \mathbb{N}$, e como $(3,4) = 1$, temos que 12 divide $d^5 - d^3$ para todo $d \in \mathbb{N}$; disto resulta a fórmula (1.38). Assim, os a_i's são inteiros.

Agora, temos:

$$j(z) = 2^6 3^3 \frac{g_2^3}{\Delta} = \frac{(1 + 240\,U)^3}{q(1 + a_1 q + a_2 q^2 + \cdots)}$$

Mas como o termo livre de q de $(1 + a_1 q + a_2 q^2 + \cdots)$ é inversível em $\mathbb{Z}$, a série de potências em questão é inversível como série de potências com coeficientes *inteiros* e seu primeiro termo é 1. Assim:

$$j(z) = \frac{1}{q}(1 + 240\,U)^3(1 + a_1' q + a_2' q^2 + \cdots),$$

o que nos dá que os coeficientes da expansão em q de j estão em $\mathbb{Z}$, e o coeficiente de q^{-1} é 1.

□

Teorema 5 (Princípio da q-Expansão). *Seja $f = \sum_{n \geq -N} a_n q^n$ uma função modular de peso zero, holomorfa em $\mathbb{H}$ e com um polo de ordem N no infinito. Então f é um polinômio em j de grau N:*

$$f = \sum_{n=0}^{N} b_n j^n,$$

com $a_{-N} = b_N$. Ainda mais, o sub-grupo (de $\mathbb{C}$) aditivo $A(f)$ gerado por $\{a_{-N}, a_{-N+1}, \ldots\}$ coincide com o sub-grupo $B(f)$ gerado por $\{b_0, \ldots, b_N\}$.

Demonstração. Provaremos por indução em N. Se $N = 0$, f é uma forma modular, pois é holomorfa em $\mathbb{H} \cup \{\infty\}$ e de peso zero, i.e., $f \in M_0$. Pelo teorema 4, item 2, temos que $f \equiv a_0$, onde o princípio é trivialmente verdadeiro. Suponhamos que o teorema seja verdadeiro para todo inteiro menor que N. Assim, seja $g := f - a_{-N} j^N$, e logo, g tem um polo de, no máximo, ordem $(N - 1)$ no infinito. Então, pela hipótese de indução, temos:

$$g(z) = \sum_{n=0}^{N-1} b_n j^n,$$

o que implica que

$$f(z) = a_{-N} j^N + \sum_{n=0}^{N-1} b_n j^n. \tag{1.39}$$

Resta-nos apenas mostrar que $A(f) = B(f)$. Mas a fórmula (1.39) mostra que $B(f)$ é o grupo gerado por $B(g)$ e a_{-N}. Pela proposição 9, temos que os coeficientes de j são inteiros, e logo, $A(f)$ é gerado por $A(g) = B(g)$ e a_{-N}, o que nos dá a igualdade desejada. □

Capítulo 2

Curvas Elípticas

2.1 A Função $\wp$ de Weirstrass

Seja $\Gamma := \Gamma(\omega_1, \omega_2)$ um reticulado de $\mathbb{C}$, e seja

$$\wp(z;\Gamma) := \frac{1}{z^2} + \sum_{\omega\in\Gamma}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \tag{2.1}$$

a função $\wp$ de Weirstrass associada. Sabemos que esta função é uma função elíptica, i.e., uma função meromorfa, duplamente periódica (relativamente a Γ) e que tem seus polos (todos de ordem dois) nos pontos de Γ ([Ahl66], pg. 264). Ainda temos:

$$\wp'(z;\Gamma) = -2 \sum_{\omega\in\Gamma}{}' \frac{1}{(z-\omega)^3}. \tag{2.2}$$

Vamos agora calcular o desenvolvimento de Laurent de $\wp(z;\Gamma)$ em $0 < |z| < r$, onde $r := \min(|\omega_1|, |\omega_2|)$. As igualdades:

$$\frac{1}{(z-\omega)^2} = \left[\sum_{n=0}^{\infty} \left(\frac{z}{\omega} \right)^n \right]^2 \frac{1}{\omega^2}, \tag{2.3}$$

para $|z| < r$ e $\omega \in \Gamma$, e

$$\left[\sum_{n=0}^{\infty} x^n\right]^2 = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} x^{n+m} = \sum_{n=0}^{\infty}(n+1)x^n \tag{2.4}$$

resultam em

$$\begin{aligned}
\wp(z;\Gamma) &= \frac{1}{z^2} + \sum_{\omega\in\Gamma}{}' \left[\frac{1}{\omega^2}\cdot\left(\sum_{n=0}^{\infty}\left(\frac{z}{\omega}\right)^n\right)^2 - \frac{1}{\omega^2}\right] \\
&= \frac{1}{z^2} + \sum_{\omega\in\Gamma}{}' \left[\frac{1}{\omega^2}\cdot\left(\sum_{n=0}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n\right) - \frac{1}{\omega^2}\right] \\
&= \frac{1}{z^2} + \sum_{\omega\in\Gamma}{}' \sum_{n=1}^{\infty}\frac{(n+1)z^n}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}\left[(n+1)z^n \sum_{\omega\in\Gamma}{}' \frac{1}{\omega^{n+2}}\right];
\end{aligned}$$

se n é ímpar,

$$\sum_{\omega\in\Gamma}{}' \frac{1}{\omega^{n+2}} = 0.$$

Portanto,

$$\wp(z;\Gamma) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{k+1}(\Gamma)z^{2k}, \tag{2.5}$$

que é o desenvolvimento de Laurent procurado.

Logo[1],

$$\wp(z) = \frac{1}{z^2} + 3G_2 z^2 + 5G_3 z^4 + 7G_4 z^6 + \cdots$$

e, derivando,

$$\wp'(z) = -\frac{2}{z^3} + 6G_2 z + 20G_3 z^3 + 42G_4 z^5 + \cdots .$$

[1]Deixando o reticulado Γ subentendido.

Com isso, vamos tentar estabelecer uma equação algébrica relacionando $\wp$ e $\wp'$. Como $\wp'$ é impar e $\wp$ é par, uma tentativa seria escrever $(\wp')^2$ como um polinômio em $\mathbb{C}[\wp]$. Como

$$(\wp')^2 = \frac{4}{z^6} - \frac{24G_2}{z^2} - 80G_3 - 142G_4 z^2 + \cdots,$$

este polinômio teria de ser de grau 3. Vamos, inicialmente, tentar tirar a singularidade e o termo constante da expansão de $(\wp')^2$ em $0 < |z| < r$. Mas como

$$(\wp)^2 = \frac{1}{z^4} + 6G_2 + 10G_3 z^2 + \cdots$$

e

$$(\wp)^3 = \frac{1}{z^6} + \frac{9G_2}{z^2} + 15G_3 + \cdots,$$

alguns cálculos mostram que

$$\varphi(z) = (\wp'(z))^2 - \left[4(\wp(z))^3 - 60G_2\wp(z) - 140G_3\right]$$

é o resultado procurado, ou seja, $\varphi(z)$ é holomorfa em $|z| < r$, e $\varphi(0) = 0$. Por outro lado, a expressão acima nos garante que φ é uma função elíptica em relação a Γ e holomorfa para $z \notin \Gamma$. Como φ é holomorfa em $z = 0$, ela é holomorfa em $z \in \Gamma$. Assim, φ é uma função elíptica holomorfa, e portanto, constante ([For81], pg. 13). Desta forma $\varphi \equiv 0$. Como $g_2 = 60G_2$ e $g_3 = 140G_3$, temos:

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3. \tag{2.6}$$

2.2 Parametrização de Curvas Elípticas

Definição 15. Uma *curva elíptica complexa* é um par (E, O), onde E é uma curva algébrica plana em $\mathbb{P}^2(\mathbb{C})$, não singular e de gênero 1, e $O \in E$. O é chamado de *ponto base* ou *origem* de E.

Muitas vezes nos referimos a E como a curva elíptica, deixando o ponto O subentendido. Como vemos em [Lan86], pg. 15, tal curva elíptica sobre $\mathbb{C}$ sempre pode ser dada por uma cúbica da forma:

$$y^2 = 4x^3 - Ax - B \tag{2.7}$$

mais o ponto base [0:1:0] (o único ponto da curva na reta no infinito). Reciprocamente, a extensão a $\mathbb{P}^2(\mathbb{C})$ de uma curva dada pela equação acima, com $A^3 - 27B^2 \neq 0$ (para que seja não singular), sempre será uma curva elíptica. Assim, sempre pensaremos em curvas elípticas como curvas definidas pela equação acima.

Portanto, como nos mostra a equação (2.6) o par $(\wp, \wp')$ satisfaz a equação que define uma curva elíptica (equação (2.7)).

Se $z = a\omega_1 + b\omega_2$, com $a, b \in [0,1[$ e $z \equiv -z \pmod{\Gamma}$, então $2a, 2b \in \{0,1\}$, e logo $z \in \{0, \omega_1/2, \omega_2/2, (\omega_1+\omega_2)/2\}$. Desta maneira, se definirmos $w_1 := \omega_1/2$, $w_2 := \omega_2/2$ e $w_3 := (\omega_1+\omega_2)/2$, teremos que a função $[\wp(z) - \wp(w_i)]$, $i \in \{1,2,3\}$, possui um polo duplo em $z = 0$ e um zero em $z = w_i$. Como $w_i \equiv -w_i$ e $\wp'$ é ímpar, temos $\wp'(w_i) = \wp'(-w_i) = -\wp'(w_i)$, e isto implica que $\wp'(w_i) = 0$. Assim, w_i é zero duplo de $[\wp(z) - \wp(w_i)]$. Como $\wp$ é uma função meromorfa definida no toro $\mathbb{C}/\Gamma$, que é uma superfície de Riemann compacta, então o número de zeros e polos, contados com multiplicidades, são iguais ([For81], pg. 80). Desta forma w_i é o único zero de $[\wp(z) - \wp(w_i)]$, e logo, $\wp(w_i) \neq \wp(w_j)$ se $i \neq j$. Como $\wp'$ tem um único polo de ordem 3 em $\mathbb{C}/\Gamma$ e os w_i's são dois a dois não congruentes módulo Γ, temos que os w_i's são os únicos zeros de $\wp'$, pelo mesmo argumento acima. Assim, em $\mathbb{C}[\wp(z)]$, temos:

$$\left(\wp'(z)\right)^2 = 4(\wp(z) - \wp(w_1))(\wp(z) - \wp(w_2))(\wp(z) - \wp(w_3)),$$

e, como tal polinômio só tem raizes simples, seu discriminante deve ser não nulo, ou seja:

$$2^6(g_2^3 - 27g_3^2) = 2^6\Delta \neq 0.$$

Proposição 10. *A função*

$$\phi : \mathbb{C}/\Gamma - \{\Gamma\} \to E_\Gamma = \left\{(x,y) \in \mathbb{C}^2 : y^2 = 4x^3 - g_2(\Gamma)x - g_3(\Gamma)\right\},$$

dada por $\phi(z+\Gamma) = (\wp(z;\Gamma), \wp'(z;\Gamma))$ *é bijetora.*

Demonstração. Seja[2] $(a,b) \in E$. Como a função $(\wp(z) - a)$ tem um polo duplo em $z = 0$, ela deve ter pelo menos um zero (novamente, pelo mesmo argumento sobre superfícies de Riemann compactas), i.e., existe z_0 tal que $\wp(z_0) = a$. Logo $(\wp'(z_0))^2 = b^2$, pois $(\wp, \wp')$ satisfaz a equação em questão,

[2]Novamente deixando o reticulado Γ implícito, afim de não sobrecarregarmos a notação.

e podemos supor que $\wp'(z_0) = b$, pois senão trocaríamos z_0 por $-z_0$. Conseqüentemente $\phi(z_0 + \Gamma) = (a, b)$, e portanto, ϕ é sobrejetora.

Sejam agora z_1 e z_2 tais que $\phi(z_1) = \phi(z_2)$. Logo $\wp(z_1) = \wp(z_2)$ e $\wp'(z_1) = \wp'(z_2)$. Consideremos a função $g(z) := \wp(z) - \wp(z_1)$. Se $z_1 \equiv -z_1 \pmod{\Gamma}$, temos que $z_1 \in \{w_1, w_2, w_3\}$, e assim, $z_1 + \Gamma$ é o único zero de g, como vimos acima, que resulta em $z_1 \equiv z_2 \pmod{\Gamma}$. Se $z_1 \not\equiv -z_1 \pmod{\Gamma}$, temos que $z_1 + \Gamma$ e $-z_1 + \Gamma$ são zeros distintos de g. Como g tem no máximo dois zeros módulo Γ e $g(z_2) = 0$, temos que ou $z_2 \equiv z_1 \pmod{\Gamma}$ ou $z_2 \equiv -z_1 \pmod{\Gamma}$. Se valesse a segunda congruência, teríamos

$$\wp'(z_1) = \wp'(z_2) = \wp'(-z_1) = -\wp'(z_1),$$

que implicaria que $\wp'(z_1) = 0$, o que é um absurdo, pois z_1 tem que ser zero simples. Logo $z_2 \equiv z_1 \pmod{\Gamma}$, e assim, ϕ é injetora.

□

Observação. Se acrescentarmos o ponto $0 + \Gamma$ a $\mathbb{C}/\Gamma - \{\Gamma\}$, e um ponto O à curva E_Γ no infinito, teremos uma bijeção entre o toro $\mathbb{C}/\Gamma$ e a curva elíptica $E_\Gamma \cup \{O\}$ em $\mathbb{P}^2(\mathbb{C})$.

2.3 Toros e Curvas Elípticas

Consideremos agora um isomorfismo entre $\mathbb{C}/\Gamma$ e $\mathbb{C}/\Gamma'$, como superfícies de Riemann, dado então pela multiplicação por um certo $\lambda \in \mathbb{C}$ tal que $\Gamma' = \lambda\Gamma$ ([For81] pg. 9). As funções $\phi = (\wp_\Gamma, \wp'_\Gamma)$ e $\psi = (\wp_{\Gamma'}, \wp'_{\Gamma'})$ associam tais toros às curvas elípticas:

$$E : y^2 = 4x^3 - g_2 x - g_3 \qquad E' : y^2 = 4x^3 - g'_2 x - g'_3, \tag{2.8}$$

onde $E = E_\Gamma$, $E' = E_{\Gamma'}$, $g_2 = g_2(\Gamma)$, $g_3 = g_3(\Gamma)$, $g'_2 = g_2(\Gamma')$ e $g'_3 = g_3(\Gamma')$.

Definimos $\gamma = \psi \circ \lambda \circ \phi^{-1}$, ou seja, definimos γ de tal forma que o diagrama

$$\begin{array}{ccc} \mathbb{C}/\Gamma & \xrightarrow{\lambda} & \mathbb{C}/\Gamma' \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ E & \xrightarrow[\gamma]{} & E' \end{array}$$

comute. Sabemos que a função $\wp$ satisafaz

$$\wp(\lambda z;\lambda\Gamma) = \lambda^{-2}\wp(z;\Gamma) \qquad \wp'(\lambda z;\lambda\Gamma) = \lambda^{-3}\wp'(z;\Gamma),$$

e que

$$g_2(\lambda\Gamma) = \lambda^{-4}g_2(\Gamma) \qquad g_3(\lambda\Gamma) = \lambda^{-6}g_3(\Gamma).$$

Por conseguinte, se $(x,y) \in E$ e $z+\Gamma = \phi^{-1}(x,y)$ (i.e., $x = \wp(z)$ e $y = \wp'(z)$), o isomorfismo entre os toros leva tal classe em $\lambda z + \lambda\Gamma$, e $\psi(\lambda z + \lambda\Gamma) = (\wp(\lambda z;\lambda\Gamma), \wp'(\lambda z;\lambda\Gamma))$; portanto, as equações acima nos dizem que $\gamma(x,y) = (\lambda^{-2}x, \lambda^{-3}y)$, que é um isomorfismo de curvas algébricas. Logo, o isomorfismo entre toros *induz* um isomorfismo entre as curvas elípticas associadas.

A recíproca deste resultado também é válida, como vemos em [Sil85], pg. 161, i.e., se temos duas curvas elípticas, definidas por reticulados Γ e Γ', isomorfas, então tais reticulados são homotéticos. Isto nos dá o resultado enunciado em [Lan86], pg. 17:

Proposição 11. *Se E e E' são duas curvas elípticas (sobre $\mathbb{C}$), definidas por reticulados Γ e Γ', como na equação (2.8), isomorfas via γ, então existe $\lambda \in \mathbb{C}$ tal que $\Gamma' = \lambda\Gamma$,*

$$g_2' = \lambda^{-4}g_2, \qquad g_3' = \lambda^{-6}g_3,$$

e $\gamma(x,y) = (\lambda^{-2}x, \lambda^{-3}y)$, para todo par $(x,y) \in E$.

Desta forma, se E é uma curva elíptica definida por uma equação como (2.8), então a não singularidade implica que seu discriminante deve ser não nulo, e logo, $\Delta \neq 0$. Assim podemos definir o número[3]

$$j_E := 1728\frac{g_2^3}{\Delta},$$

que, por analogia ao capítulo anterior, chamaremos de *invariante modular* da curva elíptica E, e, pela proposição 11, vemos claramente que se E' é isomorfa a E (no caso de curvas elípticas que são dadas por reticulados), então $j_{E'} = j_E$. Na verdade vale ainda mais:

Proposição 12. *Sejam E e E' duas curvas elípticas (dadas por reticulados) definidas por equações como em (2.8). Então, tais curvas são isomorfas se, e somente se, $j_E = j_{E'}$.*

[3]Introduzimos uma constante multiplicativa à definição natural, afim de manter a relação com o capítulo 1.

Mas antes de provarmos tal proposição, provaremos o seguinte lema:

Lema 4. *Se $z, w \in \mathbb{C}$ são tais que $z^2 = w^3$, então existe $\lambda \in \mathbb{C}$ tal que $\lambda^4 = w$ e $\lambda^6 = z$.*

Demonstração do lema 4. Seja $\xi := z^2 = w^3$. Tomemos uma raiz 12-ézima qualquer[4] $(\xi)^{1/12}$ de ξ. Assim, $(\xi^{1/12})^4 = \zeta w$, com ζ uma raiz terceira da unidade e $(\xi^{1/12})^6 = \zeta' z$, com $\zeta' \in \{-1, 1\}$. Se $\zeta' = 1$, seja $\zeta'' := 1$, e, se $\zeta' = -1$, seja $\zeta'' := i$. Desta forma, em qualquer caso $\zeta'(\zeta'')^2 = 1$. Definimos então $\lambda := (\zeta^{-1}\zeta''\xi^{1/12})$, que satisfaz a condição do lema. □

Demonstração da proposição 12. Que a condição é necessária, vimos acima. Reciprocamente, suponhamos que $j_E = j_{E'}$. Logo,

$$(g_3')^2 \, g_2^3 = (g_2')^3 \, g_3^2.$$

Queremos achar $\lambda \in \mathbb{C}$ tal que $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$ seja um isomorfismo entre E e E', ou seja, tal que $(\lambda^2 x, \lambda^3 y) \in E'$. Se $g_2 = 0$, pela fórmula acima $g_2' = 0$ e $g_3, g_3' \neq 0$ pela não-singularidade de E e E'. Então tomamos $\lambda := (g_3'/g_3)^{1/6}$. De maneira análoga, se $g_3 = 0$, tomamos $\lambda = (g_2'/g_2)^{1/4}$. Se $g_2, g_3 \neq 0$, como

$$\left(\frac{g_3'}{g_3}\right)^2 = \left(\frac{g_2'}{g_2}\right)^3$$

pelo lema 4, existe $\lambda \in \mathbb{C}$ tal que

$$\lambda^6 = \frac{g_3'}{g_3} \quad \text{e} \quad \lambda^4 = \frac{g_2'}{g_2};$$

e tal λ é o procurado.

□

Observação. Na demonstração da proposição acima, observamos que a recíproca foi provada para duas curvas elípticas *quaisquer* (i.e., não só para aquelas que são dadas por reticulados).

Teorema 6 (Uniformização Euclidiana). *Sejam $A, B \in \mathbb{C}$ verificando $A^3 - 27B^2 \neq 0$. Então, existe um único reticulado Γ de $\mathbb{C}$ tal que $g_2(\Gamma) = A$ e $g_3(\Gamma) = B$.*

[4] Denotaremos, em geral, por $z^{1/n}$ uma raiz n-ésima qualquer de z.

Demonstração. Dados A e B tais que $A^3 - 27B^2 \neq 0$, existe uma curva elíptica E tal que

$$j_E = \frac{A^3}{A^3 - 27B^2}.$$

De fato, se $j_E = 1$, tomamos $y^2 = 4x^3 - x$; se $j_E = 0$, tomamos $y^2 = 4x^3 - 1$; e se $j_E \neq 0, 1$, tomamos $y^2 = 4x^3 - gx - g$, com $g = 27j_E/(j_E - 1)$. Como a função modular $j(z)$ é sobrejetora e existe $z_0 \in \mathbb{H}$ tal que $j(z_0) = j_E$. Este $j(z_0)$ está associado à classe de homotetia do reticulado $\Gamma_0 := \Gamma(1, z_0)$, i.e.,

$$j(z_0) = j_E = \frac{g_2(\Gamma_0)^3}{g_2(\Gamma_0)^3 - 27g_3(\Gamma_0)^2} = \frac{g_2(\lambda\Gamma_0)^3}{g_2(\lambda\Gamma_0)^3 - 27g_3(\lambda\Gamma_0)^2}.$$

Desta forma, se existir tal reticulado que procuramos, ele será da forma $\lambda\Gamma_0$, pois, se não for, a curva elíptica associada a Γ é não isomorfa à curva elíptica associada a Γ_0, o que implica que seus invariantes modulares são diferentes, e, portanto, $g_2(\Gamma) \neq A$ ou $g_3(\Gamma) \neq B$.

Então a curva elíptica que é dada pela equação

$$y^2 = 4x^3 - g_2(\Gamma_0)x - g_3(\Gamma_0)$$

é isomorfa à curva elíptica dada por

$$y^2 = 4x^3 - Ax - B,$$

pela observação que segue a proposição 12 e, pela demonstração de tal proposição, temos que existe $\lambda \in \mathbb{C}$ tal que $A = \lambda^{-4}g_2(\Gamma_0) = g_2(\lambda\Gamma_0)$ e $B = \lambda^{-6}g_3(\Gamma_0) = g_3(\lambda\Gamma_0)$. Portanto, o reticulado $\Gamma := \lambda\Gamma_0$ é tal que $g_2(\Gamma) = A$ e $g_3(\Gamma) = B$.

Se temos um outro reticulado Γ' tal que $g_2(\Gamma') = g_2(\Gamma) = A$ e $g_3(\Gamma') = g_3(\Gamma) = B$, então Γ e Γ' estão associados a curvas elípticas isomorfas (pois os invariantes modulares coincidem), e logo deve existir $\lambda \in \mathbb{C}$ tal que $\Gamma' = \lambda\Gamma$. Mas isto implica, pelos pesos de g_2 e g_3, que $\lambda^{-4} = 1$ e $\lambda^{-6} = 1$, e então, $\lambda^2 = 1$. Portanto, $\lambda = 1$ ou $\lambda = -1$, mas, em qualquer caso, $\Gamma = \Gamma'$, o que nos dá a unicidade de Γ. □

Por conseguinte, temos que *toda* curva elíptica pode ser dada por reticulados, que nos permite concluir o seguinte corolário:

Corolário 4. *As proposições 11 e 12 valem para o caso geral, i.e., para* quaisquer *duas curvas elípticas.*

Com tais resultados obtidos, doravante não faremos mais distinção entre toros e curvas elípticas.

Capítulo 3

Invariantes de Classes I

3.1 Preliminares

Seja E uma curva elíptica dada pelo quociente $\mathbb{C}/\Gamma$, onde $\Gamma = \Gamma(\omega_1, \omega_2)$. Como tal curva é isomorfa à curva associada ao reticulado

$$\omega_2^{-1}\Gamma = \Gamma(\omega_1/\omega_2, 1),$$

podemos então assumir que Γ é gerado por 1 e τ, com $\mathrm{Im}(\tau) > 0$.

Um endomorfismo de E pode ser identificado a um endomorfismo de seu recobrimento universal $\mathbb{C}$, que fixa o reticulado Γ, i.e, uma multiplicação por algum $\lambda \in \mathbb{C}$, tal que $\lambda, \lambda\tau \in \Gamma$ ([For81], pg. 39). Pode-se ver facilmente que o conjunto dos λ's tais que $\lambda\Gamma \subset \Gamma$, é um sub-anel de $\mathbb{C}$ que contém $\mathbb{Z}$, e que pode ser identificado com o grupo dos endomorfismos de E, que denotaremos por $\mathrm{End}(E)$, de maneira natural. Os endomorfismos associados a números inteiros são chamados de *endomorfismos triviais*. Observamos que os endomorfismos não-triviais são sempre números complexos não reais: de fato, se existir $\lambda \in \mathbb{R}$ tal que $\lambda\Gamma \subset \Gamma$, para $\Gamma = \Gamma(\omega_1, \omega_2)$, então $\lambda\omega_1 \in \Gamma$; logo, existem inteiros a e b, tais que $\lambda\omega_1 = a\omega_1 + b\omega_2$ e como $\{\omega_1, \omega_2\}$ é uma base de $\mathbb{C}$ como $\mathbb{R}$-espaço vetorial, temos que $a = \lambda$ e $b = 0$, e assim $\lambda \in \mathbb{Z}$.

Denotaremos por $A(E)$ o sub-anel de $\mathbb{C}$ associado aos endomorfismos de E. Se $A \neq \mathbb{Z}$, dizemos que E *admite multiplicação complexa*. Em geral, uma curva elíptica não admite multiplicação complexa, como mostra a seguinte proposição:

Proposição 13. *Seja E uma curva elíptica definida pelo reticulado $\Gamma = \Gamma(1, \tau)$. Temos que se E admite multiplicação complexa, então τ pertence a*

um corpo quadrático imaginário K, e, ainda mais, $A(E) \subset \mathcal{O}_K$, onde $\mathcal{O}_K$ denota o anel dos inteiros algébricos de K.

Demonstração. Seja $\lambda \in A(E)$, não trivial. Assim, existem $a, b, c, d \in \mathbb{Z}$, com $b \neq 0$, tais que:

$$\lambda = a + b\tau \quad e \quad \lambda\tau = c + d\tau,$$

o que implica que

$$a\tau + b\tau^2 = c + d\tau.$$

Assim τ satisfaz uma equação de segundo grau com coeficientes inteiros; como $\tau \in (\mathbb{C} - \mathbb{R})$, como já observamos, temos que $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$. Logo τ pertence ao corpo quadrático imaginário $K := \mathbb{Q}(\tau)$.

Como $\lambda = a + b\tau$, temos que $\lambda \in K$, e logo satisfaz uma equação da forma

$$\lambda^2 + A\lambda + B = 0$$

com $A, B \in \mathbb{Q}$. Mas,

$$(a + b\tau)^2 + A(a + b\tau) + B = 0$$

implica que

$$\left(a^2 + bc + Aa + B\right) + \tau\left(ab + Ab + bd\right) = 0. \tag{3.1}$$

Como 1 e τ são linearmente independentes (sobre $\mathbb{R}$) seus coeficientes na equação (3.1) devem ser nulos. Portanto, como $b \neq 0$, $A = -(a + b) \in \mathbb{Z}$ e $B = -(a^2 + bc + Aa) \in \mathbb{Z}$. Assim, $\lambda \in \mathcal{O}_K$.

□

Vale, igualmente, a seguinte proposição:

Proposição 14. *Seja $E = \mathbb{C}/\Gamma$ uma curva elíptica que admite multiplicação complexa, com $\Gamma = \Gamma(\omega_1, \omega_2)$. Seja então $\lambda \in A(E)$, com $N_{K/\mathbb{Q}}(\lambda) = \lambda\bar{\lambda} = |\lambda|^2 = n$. Então $n \in \mathbb{N}$, e se*

$$\lambda \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}, \tag{3.2}$$

com $a, b, c, d \in \mathbb{Z}$, então $|ad - bc| = n$. Ainda mais, se $\lambda \notin mA(E)$, para qualquer $m \in \mathbb{Z}$, $m > 1$, temos que $(a, b, c, d) = 1$.

Demonstração. A área do paralelogramo definido pelos vetores $\lambda\omega_1$ e $\lambda\omega_2$, que denotaremos por $P(\lambda\omega_1, \lambda\omega_2)$, é dada por $|\lambda|^2 P(\omega_1, \omega_2)$, a qual, por outro lado, deve ser igual a $P(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$. Esta área, por sua vez, é igual a $|ad - bc| P(\omega_1, \omega_2)$. Logo $|\lambda|^2 = |ad - bc| \in \mathbb{N}$.

Se $m|a, b, c, d$, temos:

$$\lambda/m \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a/m & b/m \\ c/m & d/m \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

e logo, $\lambda/m \in A(E)$, i.e., $\lambda \in mA(E)$, o que conclui a prova. □

Definição 16. Uma *ordem* de um corpo quadrático imaginário K é um sub-anel de $\mathcal{O}_K$ que contém $\mathbb{Z}$ e de posto 2 como $\mathbb{Z}$-módulo.

Lema 5. *Seja K um corpo quadrático imaginário. Então todo $\mathbb{Z}$-sub-módulo de $\mathcal{O}_K$, livre e de posto 2, é um reticulado de $\mathbb{C}$. Em particular ordens e ideais fracionários de K são reticulados.*

Demosntração. Se M é tal sub-módulo e (ω_1, ω_2) é uma base de M, temos que (ω_1, ω_2) é linearmente independente sobre $\mathbb{Q}$, e portanto, uma $\mathbb{Q}$-base de K. Por outro lado, K contém números reais e números complexos não reais. Desta forma (ω_1, ω_2) é linearmente independente sobre $\mathbb{R}$.

O caso de ordens é imediato. Para o caso em que temos $\mathfrak{a}$ um ideal fracionário de K, basta observarmos que, como existe $\alpha \in \mathcal{O}_K$ tal que $\alpha\,\mathfrak{a}$ é ideal de $\mathcal{O}_K$ ([Gol71], pg. 14), $\mathcal{O}_K/(\alpha\,\mathfrak{a})$ é finito ([Gol71], pg. 27) e $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto 2 ([Gol71], pg. 12) então $\alpha\,\mathfrak{a}$ é $\mathbb{Z}$-módulo livre de posto 2 ([Ste79], pg. 32). Portanto, pelo que fizemos acima, $\alpha\,\mathfrak{a}$ é um reticulado e logo $\mathfrak{a}$ também o é. □

Proposição 15. *Se E é uma curva elíptica que adimite multiplicação complexa, então $A(E)$ é uma ordem do corpo quadrático imaginário K (dado pela proposição 13). Reciprocamente, dada uma ordem Γ de um corpo quadrático imaginário K, existe uma curva elíptica E tal que $A(E)$ é igual à ordem dada.*

Demonstração. Suponhamos que E admite multiplicação complexa. A proposição 13 nos diz que $\mathbb{Z} \subset A(E) \subset \mathcal{O}_K$. Temos que $1 \in A(E)$ e existe $\lambda \in A(E)$ não real. Logo, $A(E)$ contém $\{1, \lambda\}$, que é uma $\mathbb{Q}$-base de K. Além disso, $A(E)$ é trivialmente um sub-anel e um $\mathbb{Z}$ sub-módulo de $\mathcal{O}_K$ que

contém $\mathbb{Z}$; como $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto 2 ([Gol71] pg. 10), então $A(E)$ também é livre de posto menor ou igual a dois ([Ste79] pg. 31). Mas como $A(E)$ contém uma $\mathbb{Q}$-base de K, então o posto de $A(E)$ é maior ou igual a $[K : \mathbb{Q}] = 2$, e assim, $A(E)$ é livre de posto 2.

Para a recíproca, basta que tomemos a curva $E = \mathbb{C}/\Gamma$ (observe que podemos definir tal curva pelo lema 5). Como $1 \in \Gamma$, temos que $\lambda\Gamma \subset \Gamma$ implica que $\lambda \in \Gamma$. Por outro lado, se $\lambda \in \Gamma$, como Γ é uma anel, temos que $\lambda\Gamma \subset \Gamma$. Portanto, $A(E) = \Gamma$.

□

Ainda mais, temos:

Proposição 16. *Seja $E = \mathbb{C}/\Gamma$ uma curva elíptica que admite multiplicação complexa tal que $A(E) = \mathcal{O}_K$, para o corpo K correspondente. Então Γ é um ideal fracionário de K. Reciprocamente, qualquer ideal fracionário Γ de um corpo quadrático imaginário K, é um reticulado que nos dá uma curva $E = \mathbb{C}/\Gamma$ tal que $A(E) = \mathcal{O}_K$.*

Demonstração. Seja $\tau \in K$, tal que $\Gamma = \Gamma(1, \tau)$. Sabemos que existe $m \in \mathbb{N}^*$ tal que $m\tau \in \mathcal{O}_K$ ([Gol71], pg. 10). Logo, $m\Gamma \subset \mathcal{O}_K = A(E)$. Temos claramente que $m\Gamma$ é fechado para a soma. Tomemos então $x \in \mathcal{O}_K$ e $my \in m\Gamma$. Como $A(E) = \mathcal{O}_K$, $xy \in \Gamma$ e $x(my) \in m\Gamma$. Desta forma, $m\Gamma$ é um ideal de $\mathcal{O}_K$ e Γ um ideal fracionário de K.

Para recíproca, tomemos um ideal fracionário Γ de K. Sabemos, pelo lema 5, que Γ é um reticulado. Assim, podemos definir a curva elíptica $E = \mathbb{C}/\Gamma$. Sempre vale que $A(E) \subset \mathcal{O}_K$. Por outro lado, existe m tal que $m\Gamma$ é um ideal de $\mathcal{O}_K$, pois existe $\alpha \in \mathcal{O}_K$ tal que $\alpha\Gamma$ é um ideal de $\mathcal{O}_K$, e então, $m := |\alpha|^2 \in \mathbb{Z}$ serve. Se $z \in \mathcal{O}_K$, $z \cdot m\Gamma \subset m\Gamma$, o que implica que $z\Gamma \subset \Gamma$. Assim, $\mathcal{O}_K \subset A(E)$. Portanto, $\mathcal{O}_K = A(E)$.

□

Definição 17. Dado um corpo de números K definimos $\mathcal{I}(K)$ como o grupo multiplicativo formado pelos ideais fracionários de K. Definimos $\mathcal{J}(K)$ como o subgrupo de $\mathcal{I}(K)$ formado pelos ideais fracionários principais de K. O quociente $\mathcal{C}(K) := \mathcal{I}(K)/\mathcal{J}(K)$ é chamdado *grupo de classes de ideais de K*.

Fixemos agora um corpo quadrático imaginário K. Sejam então E e E' duas curvas elípticas tais que $A(E) = A(E') = \mathcal{O}_K$. Assim, nossa análise no capítulo 2 mostra que tais curvas elípticas são isomorfas se, e somente se,

os ideais (reticulados) associados a elas são homotéticos, i.e., pertencem à mesma classe de ideais.

Para a curva definida pela equação

$$y^2 = 4x^3 - g_2 x - g_3,$$

o invariante modular associado vale

$$j = 1728\frac{g_2^3}{\Delta}.$$

Como duas curvas elípticas são isomorfas se e somente se seus invariantes modulares são iguais, temos que j define uma função em $C(K)$, que é um conjunto finito ([Gol71], pg. 42), cuja ordem denotaremos por h_K, ou simplesmente por h quando não houver dúvida sobre o corpo em questão. Denotaremos tais classes de ideais por k_i, $i \in \{1, \ldots, h\}$. Os números $j(\mathsf{k}_i)$ são chamados *invariantes de classes*, e são, claramente, dois a dois distintos.

Temos assim uma bijeção entre $\{j(\mathsf{k}_1), \ldots, j(\mathsf{k}_h)\}$ e o conjunto das curvas elípticas E, módulo isomorfismos, tais que $A(E) = \mathcal{O}_K$.

3.2 O Conjunto H_n

Definição 18. Seja n um inteiro positivo. Denotaremos por H_n^* o conjunto de todos os automorfismos de $\mathbb{H}$ que podem ser representados na forma:

$$M : z \mapsto \frac{az+b}{cz+d}, \quad ad - bc = n,\ a, b, c, d \in \mathbb{Z}, \tag{3.3}$$

e por H_n o subconjunto de H_n^*, consistindo dos M que têm uma representação como em (3.3) e ainda com $(a, b, c, d) = 1$.

Observações.

1. Como observamos no capítulo 1, os automorfismos de $\mathbb{H}$ são dados pelo conjunto $\mathbf{PSL}_2(\mathbb{R})$, que é composto por matrizes que têm determinantes iguais a 1, o que não acontece com as matrizes de H_n. No entanto, dado um elemento de H_n, existe uma matriz em $\mathbf{PSL}_2(\mathbb{R})$ que é igual a tal elemento como *função* em $\mathbb{H}$ (basta dividir as entradas da matriz que representa o elemento de H_n por $\sqrt{n}$).

2. A proposição 14, juntamente com a prova do teorema 8 enunciado mais adiante, justificam em parte, a definição do H_n.

Daqui em diante, quando dissermos

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_n^*, \quad \text{ou} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_n,$$

estaremos nos referindo à transformação representada pela matriz em questão e vamos supor que tais matrizes já estão na representação especial mencionada na definição acima.

Proposição 17. *Com a notação acima temos* $\mathbf{G}H_n^* = H_n^*$, $(H_n^*)^{-1} = H_n^*$ *e* $H_n^*\mathbf{G} = H_n^*$; *e ainda* $\mathbf{G}H_n = H_n$, $(H_n)^{-1} = H_n$ *e* $H_n\mathbf{G} = H_n$.

Demonstração. Como podemos tomar os elementos de $\mathbf{G}$ e H_n^* como matrizes inteiras, o seu produto é uma matriz inteira; como o determinante de matrizes é uma função multiplicativa, temos claramente que $\mathbf{G}H_n^* \subset H_n^*$. Como a matriz identidade está em $\mathbf{G}$, vale a outra inclusão e, portanto, vale a igualdade.

Seja agora $M \in H_n^*$ com uma representação dada por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

como em (3.3). Logo,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d/n & -b/n \\ -c/n & a/n \end{pmatrix},$$

que possui uma representação

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Assim, $M^{-1} \in H_n^*$. Analogamente, temos a outra inclusão, o que prova a igualdade.

A terceira igualdade a ser provada segue das duas primeiras de maneira geral (e, portanto, a mesma prova valerá para H_n). Sejam $A \in \mathbf{G}$ e $N \in H_n^*$. Definimos $N' := NA$; precisamos mostrar que $N' \in H_n^*$. Temos $N^{-1} = A(N')^{-1}$. Como $N \in H_n^*$, $N^{-1} \in (H_n^*)^{-1} = H_n^*$ e portanto $A(N')^{-1} \in \mathbf{G}H_n^* = H_n^*$; assim $(N')^{-1} \in H_n^* = (H_n^*)^{-1}$, i.e., $N' \in H_n^*$.

Dada

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

uma representação de $M \in H_n$, temos que $M^{-1} \in H_n$, pois $(a,b,c,d) = (d,-b,-c,a)$. Desta forma, resta apenas mostrar que $\mathbf{G}H_n = H_n$. Como a inclusão $H_n \subset \mathbf{G}H_n$ é imediata, basta provarmos que $\mathbf{G}H_n \subset H_n$. Mas $\mathbf{G} = \langle S, T \rangle$, pelo teorema 2. É suficiente então mostrar que se $M \in H_n$, então $SM, TM \in H_n$. Isto segue de $\mathbf{G}H_n^* = H_n^*$ e de $(a,b,c,d) = (-c,-d,a,b) = (a+b, b+d, c, d)$, onde a primeira igualdade é imediata e, para a segunda igualdade, tomemos $p|(a+c), (b+d), c, d$; como $p|c$ e $p|(a+c)$, $p|a$, e analogamente $p|b$; por outro lado, se $p|a, b, c, d$, claramente $p|(a+c), (b+d), c, d$.

□

Proposição 18. *Um conjunto completo de representantes para as classes* $\mathbf{G}M$ *de* $H_n^*/\mathbf{G}$ *é obtida pelos automorfismos que podem ser representados pelas matrizes*

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad a > 0,\ d > 0,\ d > b \geq 0,\ ad = n. \tag{3.4}$$

Além disso, $[H_n^* : \mathbf{G}] = \sigma_1(n)$ *(conforme a definição 14).*

Demonstração. Precisamos mostrar que dada

$$M = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in H_n^*,$$

existe $N \in \mathbf{G}$ e

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

como em (3.4) tais que

$$N \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix},$$

ou, equivalentemente, que existe $N \in \mathbf{G}$ tal que

$$N \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Lembrando novamente que $\mathbf{G} = \langle S, T \rangle$, vamos tentar triangularizar a matriz dada. Como S troca as linhas e muda o sinal de uma delas, da matriz que multiplicarmos a esquerda por S, podemos supor $|x| \geq |z|$. Se $z = 0$, não há

nada a fazer. Se $z \neq 0$, pelo algoritmo da divisão, existem $q_1, r_1 \in \mathbb{Z}$ tais que $x = zq_1 + r_1$ e $0 \leq r_1 < |z|$. Logo,

$$T^{-q_1}M = \begin{pmatrix} r_1 & y - q_1 w \\ z & w \end{pmatrix}$$

e

$$M_1 := ST^{-q_1}M = \begin{pmatrix} z & w \\ -r_1 & -(y - q_1 w) \end{pmatrix}.$$

Se $r_1 = 0$, então já conseguimos. Caso contrário, novamente exsitem $q_2, r_2 \in \mathbb{Z}$ tais que $z = (-r_1)q_2 + r_2$ e $0 \leq r_2 < r_1$. Assim,

$$M_2 := ST^{-q_2}M_1 = \begin{pmatrix} r_1 & * \\ -r_2 & * \end{pmatrix},$$

e podemos prosseguir com este processo. Como os r_i's são inteiros positivos e decrescentes, este processo termina, chegando finalmente a $r_k = 0$. Portanto, existe $N \in \mathbf{G}$ tal que

$$NM = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}.$$

Observamos que este processo garante que $a = (x, z)$ (é equivalente ao algoritmo de Euclides), que $a > 0$ e $ad = n$ (e logo, $d > 0$). Se $b' \geq d$, temos, novamente pelo algoritmo da divisão, que $b' = qd + b$, com $0 \leq b < d$, e logo,

$$T^{-q}NM = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

com a, b, c e d como em (3.4). Se $b' < 0$, existe q tal que $b' + dq = b$, com $0 \leq b < d$, e

$$T^{q}NM = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

com a, b, c e d como em (3.4).

Vamos mostrar agora que tal representação é única: seja então

$$\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

como em (3.4), tal que exista $N' \in \mathbf{G}$, com

$$N'M = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}.$$

Temos então que $a'|x, z$, pois

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} = (N')^{-1} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

com $(N')^{-1} \in \mathbf{G}$, e $\mathbf{G} = \langle S, T \rangle$. Mas, se $(N')^{-1} = S$, ou $(N')^{-1} = T$, vemos claramente que $a'|x, y$, e, depois disso, basta usarmos indução. Como $a = (x, z)$, temos que $a'|a$, digamos $a = a'q$ (e logo $d' = dq$). Assim,

$$N \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \quad \text{e} \quad N' \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$$

implicam que

$$N'N^{-1}NM = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

com $N'N^{-1} \in \mathbf{G}$, i.e.,

$$N'N^{-1} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1}$$

$$= \frac{1}{n} \begin{pmatrix} a'd & ab' - a'b \\ 0 & ad' \end{pmatrix} \in \mathbf{G}.$$

Entretanto, a matriz acima deve ter coeficientes inteiros (pois o determinante é igual a 1). Porém $a'd = ad/q = n/q$, e logo o coeficiente na posição $(1,1)$ da matriz acima é $1/q$ e deve ser inteiro. Desta forma, $q = 1$ (já sabíamos que q era positivo), $a = a'$ e $d = d'$. Temos agora que $a(b' - b) \in \mathbb{Z}$, com $d > b, b' \geq 0$, e $n|a(b' - b)$. Mas $|b' - b| < d$; como $n = ad$, $|a(b' - b)| < n$, e assim $b = b'$, ou seja

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}.$$

Provamos então que para toda $M \in H_n^*$, existe uma única matriz

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in H_n^*$$

como em (3.4), tal que

$$M \in \mathbf{G} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

o que prova a primeira parte da proposição. Para a segunda parte, observamos que todo representante tem d como divisor de n. Fixado tal d, o $a = n/d$ está bem determinado e podemos escolher qualquer $b \in \{0, \ldots, d-1\}$, o que nos dá d possibilidades e mostra que

$$[H_n^* : \mathbf{G}] = \sum_{d|n} d = \sigma_1(n).$$

□

Sabemos, em particular, que se $M \in H_n$, M pode ser representada por uma matriz como em (3.4) e, como vimos acima, $(a, b, 0, d) = (a, b, d) = 1$. Queremos agora achar $\psi(n) := [H_n : \mathbf{G}]$. Vejamos inicialmente o caso em que $n = p$, primo. Para tal caso, as possibilidades são

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix},$$

com $b \in \{0, \ldots, p-1\}$, o que nos dá $(p+1)$ possibilidades.

Se $n = p^k$ com p primo, temos: $d = 1$ nos dá uma única possibilidade, a saber,

$$\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix};$$

se $d = n$, temos n possibilidades, da forma

$$\begin{pmatrix} 1 & b \\ 0 & n \end{pmatrix},$$

com $b \in \{0, \ldots, n-1\}$. Se $d = p^i$, com $1 \leq i \leq (k-1)$, o que nos dá todas as outras possibilidades para d, observamos que $(a, b, d) = 1$ se, e somente se, p não divide b, ou, equivalentemente, se $(b, d) = 1$. Logo, se $d = p^i$, temos $\varphi(p^i)$ possibilidades, onde φ é a função φ de Euler. Assim, neste caso,

$$\begin{aligned} [H_n : \mathbf{G}] &= 1 + \sum_{i=1}^{k-1} \varphi(p^i) + p^k \\ &= 1 + \sum_{i=1}^{k-1} (p^i - p^{i-1}) + p^k \\ &= 1 + (p^{k-1} - 1) + p^k \\ &= p^k + p^{k-1}. \end{aligned}$$

Para o caso geral, dado d um divisor de n, temos a bem definido por $a := n/d$. Seja então $e := (a, d)$. Temos que achar os possíveis b's. Mas $(a, b, d) = 1$ se, e somente se, $(b, e) = 1$. Além disso, $(b, e) = 1$ se, e somente se, $b = qe + r$, com $0 \leq r < e$, e $(r, e) = 1$. Como $0 \leq b < d$, as possibilidades para tais q's são $q \in \{0, \ldots, ((d/e) - 1)\}$. Logo, o número de possibilidades para b é $(d/e)\varphi(e)$. Portanto

$$\psi(n) = \sum_{d|n} \frac{d}{e}\varphi(e), \quad \text{com } e := (d, n/d). \tag{3.5}$$

Mas, tal função é multiplicativa no sentido usual em teoria dos números, i.e., se $n = n_1 n_2$, com $(n_1, n_2) = 1$, então $\psi(n_1 n_2) = \psi(n_1)\psi(n_2)$. De fato , se $d|n$, $d = d_1 d_2$, com $d_i|n_i$, e $(d, n/d) = e_1 e_2$, com $(d_i, n_i/d_i) = e_i$, para $i \in \{1, 2\}$. Desta forma[1]:

$$\psi(n_1 n_2) = \sum_{\substack{d_1|n_1 \\ d_2|n_2}} \frac{d_1 d_2}{e_1 e_2}\varphi(e_1)\varphi(e_2) = \psi(n_1)\psi(n_2).$$

Como ψ é multiplicativa, se $n = p_1^{k_1} \ldots p_t^{k_t}$ é a decomposição de n em primos, temos:

$$\begin{aligned} \psi(n) = \psi(p_1^{k_1}) \ldots \psi(p_t^{k_t}) &= \prod_{i=1}^{t} \left(p_i^{k_i} + p_i^{k_i - 1}\right) \\ &= \prod_{i=1}^{t} \left[p_i^{k_i}\left(1 + \frac{1}{p_i}\right)\right] \\ &= n \prod_{p|n} \left(1 + \frac{1}{p}\right). \end{aligned} \tag{3.6}$$

Conseqüentemente, obtivemos uma fórmula geral para $\psi(n) = [H_n : \mathbf{G}]$.

Definição 19. Sejam Γ e Γ' reticulados de $\mathbb{C}$ tais que $\Gamma' \subset \Gamma$ (i.e, um *sub-reticulado* de Γ). Suponhamos que $[\Gamma : \Gamma'] = n$. Γ' é chamado *primitivo* se Γ/Γ' for um grupo cíclico de ordem n.

[1] Lembrando que a função φ de Euler é multiplicativa.

Proposição 19. *Seja* $\Gamma = \Gamma(\omega_1, \omega_2)$ *e seja* $\Gamma' = \Gamma(\omega_1', \omega_2')$ *um sub-reticulado com* $[\Gamma : \Gamma'] = n$. *Temos então que existem* $a, b, c, d \in \mathbb{Z}$ *tais que:*

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Então Γ' *será primitivo de ordem* n *se, e somente se,*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_n.$$

Demonstração. Suponhamos inicialmente que Γ' é primitivo. Podemos supor que $\det M > 0$ (eventualmente trocando a ordem de ω_1' e ω_2'). Temos que[2] $P(\omega_1', \omega_2') = \det M \cdot P(\omega_1, \omega_2)$. Por outro lado, temos que $[\Gamma : \Gamma'] = P(\omega_1', \omega_2')/P(\omega_1, \omega_2)$. Logo, $\det M = n$, i.e., $M \in H_n^*$.

Suponhamos que $\Gamma/\Gamma' = \langle(\alpha\omega_1 + \beta\omega_2) + \Gamma'\rangle$. Portanto, para quaisquer $x, y \in \mathbb{Z}$, existe $m \in \{0, \ldots, n-1\}$ tal que

$$(x\omega_1 + y\omega_2) + \Gamma' = m(\alpha\omega_1 + \beta\omega_2) + \Gamma',$$

ou seja,

$$(x - m\alpha)\omega_1 + (y - m\beta)\omega_2 \in \Gamma'.$$

Deste modo, devem existir $u, v \in \mathbb{Z}$ que satisfazem o sistema:

$$\begin{cases} x - m\alpha = a\,u + c\,v \\ y - m\beta = b\,u + d\,v \end{cases}.$$

Como tal sistema tem solução inteira, $d_1 := (a, c)$ e $d_2 := (b, d)$ devem satisfazer $d_1 | (x - m\alpha)$ e $d_2 | (y - m\beta)$. Se $p | a, b, c, d$, com $p > 1$ primo, temos que $p | d_1, d_2$, e logo $p | (x - m\alpha)$ e $p | (y - m\beta)$. Mas, lembramos que x e y foram tomados quaisquer, i.e., deve valer para todos $x, y \in \mathbb{Z}$,

$$\begin{cases} m\alpha \equiv x \pmod{p} \\ m\beta \equiv y \pmod{p} \end{cases}.$$

Se $\alpha \equiv 0 \pmod{p}$, então $x \equiv 0 \pmod{p}$, o que seria um absurdo, pois x é qualquer. Analogamente $\beta \not\equiv 0$. Como p é primo, as α e β são inversíveis em

[2] Lembrando que $P(\omega_1, \omega_2)$ denota a área do paralelogramo definido por ω_1 e ω_2.

$\mathbb{Z}/p\mathbb{Z}$. Sejam $\widetilde{\alpha}, \widetilde{\beta}$ inteiros que representam as classes dos inversos de α e β, respectivamente. Logo,

$$x\widetilde{\alpha} \equiv y\widetilde{\beta} \pmod{p}.$$

que é absurdo (basta tomarmos $x \equiv 0 \pmod{p}$ e $y \equiv 1 \pmod{p}$). Por conseguinte, não existe primo que divida ao mesmo tempo a, b, c e d, i.e., $(a, b, c, d) = 1$. Assim $M \in H_n$.

Reciprocamente, dada

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_n$$

tomemos $\omega_1, \omega_2 \in \mathbb{C}$, com $\mathrm{Im}(\omega_1/\omega_2) > 0$, e definamos $\Gamma := \Gamma(\omega_1, \omega_2)$ e $\Gamma' := \Gamma(\omega_1', \omega_2')$, onde

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w_1 \\ \omega_2 \end{pmatrix}.$$

Novamente temos $[\Gamma : \Gamma'] = P(\omega_1', \omega_2')/P(\omega_1, \omega_2) = ad - bc = n$. Resta-nos então mostrar que Γ/Γ' tem um elemento de ordem n. Usando o *Teorema do Divisor Elementar*, como vemos em [Gol71] pg. 276, existem bases (τ_1, τ_2) e (τ_1', τ_2') de Γ e Γ', respectivamente, tais que $\tau_1' = a_1\tau_1$ e $\tau_2' = a_2\tau_2$, com $a_1, a_2 \in \mathbb{Z}$, e com $a_1 | a_2$. Assim, existem $N_1, N_2 \in \mathbf{SL}_2(\mathbb{Z})$, tais que:

$$N_1 \begin{pmatrix} \tau_1 \\ \tau_2 \end{pmatrix} = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \quad \text{e} \quad N_2 \begin{pmatrix} \tau_1' \\ \tau_2' \end{pmatrix} = \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}.$$

Portanto,

$$N_2^{-1} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} N_1^{-1} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix},$$

o que implica que

$$N_2 \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} N_1^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Desta forma, como $N_1, N_2 \in \mathbf{SL}_2(\mathbb{Z})$, temos que $(a, b, c, d) = 1$ implica $(a_1, a_2) = 1$, e como $a_1 | a_2$, então $a_1 = 1$ e $a_2 = n$. Conseqüentemente, $\Gamma' = \Gamma(\tau_1, n\tau_2)$ e a classe do elemento τ_2 tem ordem n, ou seja, $\Gamma/\Gamma' = \langle \tau_2 + \Gamma' \rangle$.

□

Desta forma, se $\Gamma = \Gamma(1, \tau)$, a aplicação definida por

$$\Gamma \mapsto \Gamma_M = \Gamma(1, M(\tau)),$$

para $M \in H_n$, associa a Γ reticulados homotéticos a sub-reticulados primitivos de índices n em Γ. Analogamente, se $M \in H_n^*$, associará a Γ sub-reticulados de índice n em Γ.

Se Γ' é sub-reticulado primitivo de ordem n de Γ, o fato de Γ e Γ' terem bases das formas $\{\tau_1, \tau_2\}$ e $\{n\tau_1, \tau_2\}$, respectivamente, implica que tomando

$$M_0 := \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix},$$

teremos $H_n = \mathbf{G}M_0\mathbf{G}$, pois dada uma M qualquer em H_n, existem $N_1, N_2 \in \mathbf{G}$ tais que $N_2 M N_1^{-1} = M_0$, como vemos na demonstração da proposição acima (a outra inclusão é conseqüência da proposição 17). Desta forma, a multiplicação à direita por $\mathbf{G}$ age *transitivamente* em $H_n/\mathbf{G}$, i.e., dadas $\mathbf{G}M$ e $\mathbf{G}M'$ duas classes de $H_n/\mathbf{G}$, existe $N \in \mathbf{G}$ tal que $\mathbf{G}MN = \mathbf{G}M'$. De fato, sabemos que existem $N_1, N_2, N_1', N_2' \in \mathbf{G}$ tais que $N_1 M N_2 = M_0 = N_1' M' N_2'$. Logo, se $N = N_2(N_2')^{-1}$, então $N_1 MN = N_1' M'$, o que equivale a $\mathbf{G}MN = \mathbf{G}M'$. Tal fato, em geral, não vale para H_n^*.

3.3 As Equações Modulares

Doravante $\psi(n)$ será denotado simplesmente por N. Sejam $M_1, \ldots, M_N$ representantes das classes de $H_n/\mathbf{G}$ dados por matrizes como em (3.4), com $(a, b, d) = 1$. Definimos $j_s(z) = j(M_s(z))$, para $s \in \{1, \ldots, N\}$. onde j é a função modular (como no capítulo 1).

Dada qualquer $A \in \mathbf{G}$, a associação $j_s(z) \mapsto j_s(A(z))$ é uma permutação dos $j_1, \ldots, j_N$, pois, se supusermos que $M_r A = BM_t$ e $M_s A = B'M_t$, com $B, B' \in \mathbf{G}$, então $M_s A = B'B^{-1}BM_t = B'B^{-1}M_r A$, e, logo, $M_s = B'B^{-1}M_r$, o que implica que M_r e M_s estão na mesma classe, pois $B'B^{-1} \in \mathbf{G}$, e, desta forma, $r = s$. Portanto, funções simétricas em $j_1, \ldots, j_N$ são invariantes por $z \mapsto A(z)$, para qualquer $A \in \mathbf{G}$.

Teorema 7. *1. $F_n(t, j) := \prod_{s=1}^{N}(t - j_s(z))$ é um polinômio em t e $j = j(z)$ com coeficientes inteiros.*

2. Se n não é um quadrado, o coeficiente de maior grau em j de $F_n(j, j)$ é ± 1.

3. *$F_n(t,j)$ como polinômio em $\mathbb{C}(j)[t]$ é irredutível.*

4. *$F_n(t,j) = F_n(j,t)$, para todo $n > 1$.*

Demonstração. Uma função simétrica elementar dos j_s's,

$$\sigma_\nu(j_1(z), \ldots, j_N(z))$$

é invariante por $\mathbf{G}$, como observamos acima, e claramente holomorfa em $\mathbb{H}$. Verifiquemos agora o comportamento de σ_ν no infinito. Para tal, seja $q = e^{2\pi i z}$. Como vemos em (1.22) e na proposição 9, podemos escrever j na forma

$$j(z) = q^{-1}(1 + A(q)),$$

onde $A(q)$ é uma série de potências em q com coeficientes inteiros e $A(0) = 0$. Se representarmos:

$$M_s = \begin{pmatrix} a_s & b_s \\ 0 & d_s \end{pmatrix},$$

então,

$$\exp(2\pi i M_s(z)) = \zeta_{d_s}^{b_s} q^{a_s/d_s}$$

onde $\zeta_{d_s} := \exp((2\pi i)/d_s)$, o que implica

$$\begin{aligned} j_s(z) &= j(M_s(z)) = (\exp(2\pi i M_s(z)))^{-1}(1 - A(\exp(2\pi i M_s(z)))) \\ &= \zeta_{d_s}^{-b_s} q^{-a_s/d_s} \left(1 + A\left(\zeta_{d_s}^{b_s} q^{a_s/d_s}\right)\right). \end{aligned} \tag{3.7}$$

Assim, podemos ver que σ_ν pode ter apenas um polo no infinito, e conseqüentemente, pelo princípio da q-Expansão (sub-seção 1.4.3, teorema 5), é um polinômio (sobre $\mathbb{C}$) em j. Como os coeficientes de j_s estão em $\mathbb{Z}[\zeta_{d_s}] \subset \mathbb{Z}[\zeta_n]$ ($\zeta_n := \exp((2\pi i)/n)$), os coeficientes de σ_ν estão em $\mathbb{Z}[\zeta_n]$. Seja então τ um automorfismo de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Logo $\tau(\zeta_n) = \zeta_n^r$, para algum r tal que $(n,r) = 1$, e podemos escrever

$$\tau(\zeta_{d_s}^{b_s}) = \tau(\zeta_n^{a_s b_s}) = \zeta_n^{r a_s b_s} = \zeta_{d_s}^{r b_s} = \zeta_{d_t}^{b_t},$$

onde $a_t = a_s$, $d_t = d_s$ e $0 \leq b_t < d_t$, com $b_t \equiv r b_s \pmod{d_s}$. Logo, a matriz

$$\begin{pmatrix} a_t & b_t \\ 0 & d_t \end{pmatrix}$$

é como em (3.4), e está unicamente determinada por M_s e τ. Portanto, também denotando por τ o automorfismo das séries de potências com coeficientes em $\mathbb{Q}(\zeta_n)$, que é induzido por τ (i.e., aplicando τ coeficiente a coeficiente), temos

$$\begin{aligned}\tau(j_s) &= \tau(\zeta_{d_s}^{-b_s})q^{-a_s/d_s}\left(\tau(1) + A(\tau(\zeta_{d_s}^{b_s})q^{a_s/d_s})\right)\\ &= \zeta_{d_t}^{-b_t}q^{-a_t/d_t}\left(1 + A(\zeta_{d_t}^{b_t}q^{a_t/d_t})\right)\\ &= j_t.\end{aligned}$$

Por conseguinte, τ permuta as funções $j_1, \ldots, j_N$, e desta forma, $\tau(\sigma_\nu) = \sigma_\nu$, para todo $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Por outro lado, como os coeficientes de σ_ν estão em $\mathbb{Z}[\zeta_n]$ e são fixos por τ, temos que tais coeficientes estão em $\mathbb{Z}$. Pelo princípio da q-expansão os coeficientes de σ_ν como polinômio em j também são inteiros. Assim, provamos o item 1.

Para provarmos 2, suponhamos que n não é um quadrado, e logo, $a_s/d_s \neq 1$ para todo $s \in \{1, \ldots, N\}$. Desta maneira, o coeficiente do menor exponte de q, para $j - j_s$, será $\zeta_{d_s}^{-b_s}$, se $a_s/d_s > 1$, e 1, se $a_s/d_s < 1$. Portanto, em ambos os casos será uma raiz da unidade. Portanto o coeficiente do menor expoente de q em $F_n(j, j) = \prod_{s=1}^{N}(j - j_s)$ será um produto de raízes da unidade, e conseqüentemente uma raiz da unidade. Assim, o princípio da q-expansão nos diz que $F_n(j, j)$, como polinômio em j, terá por coeficiente dominante tal raiz da unidade. Mas, como tal polinômio tem coeficientes inteiros, esse coeficiente dominante deve ser ± 1.

Provemos agora o item 3: o corpo $\mathbb{C}(j, j_1, \ldots, j_N)$ é o corpo de raízes de $F_n(t, j)$ (como polinômio em $\mathbb{C}(j)[t]$). Se o polinômio $F_n(t, j)$ fosse redutível, existiria um corpo de raízes entre $\mathbb{C}(j, j_1, \ldots, j_N)$ e $\mathbb{C}(j)$. Mas, dada $A \in \mathbf{G}$, a aplicação $j_s \mapsto j_s \circ A$ é um $\mathbb{C}(j)$-automorfismo de $\mathbb{C}(j, j_1, \ldots, j_N)$, e tais isomorfismos agem transitivamente nos j_s's. Desta forma, a extensão $\mathbb{C}(j, j_1, \ldots, j_N)/\mathbb{C}(j))$ não possui nenhum corpo de raízes intermediário não trivial, e logo, $F_n(t, j)$ é irredutível.

Resta apenas o item 4: como $z \mapsto nz$ e $z \mapsto z/n$ estão ambas em H_n, $F_n(j(nz), j(z)) = 0$ e $F_n(j(z/n), j(z)) = 0$ para $z \in \mathbb{H}$. Substituindo z por nz no segundo caso (observe que $nz \in \mathbb{H}$), obtemos $F_n(j(z), j(nz)) = 0$. Segue que, como polinômios em $\mathbb{C}(j)[t]$, $F_n(t, j(z))$ e $F_n(j(z), t)$ têm um zero comum, a saber $t = j(nz)$. Como $F_n(t, j)$ é irredutível, pelo item 3, e o coeficiente de maior grau em t é 1, obtemos:

$$F_n(j, t) = P(t, j)\, F_n(t, j),$$

com $P(t,j) \in \mathbb{Z}[j,t]$, pois os coeficientes de $F_n(t,j)$ estão em $\mathbb{Z}[j]$ (como polinômio em t) e o fato do coeficiente de maior grau em t ser 1 (inversível) permite-nos fazer a divisão de polinômios no anel $\mathbb{Z}[j]$. Assim:

$$F_n(t,j) = P(j,t)\,F_n(j,t) = P(j,t)\,P(t,j)\,F_n(t,j).$$

que implica em $P(j,t)\,P(t,j) = 1$. Como $P(t,j) \in \mathbb{Z}[t,j]$, $P(t,j) = P(j,t) = \pm 1$. Se $P(t,j) = -1$, então $F_n(t,j) = -F_n(j,t)$ e, conseqüentemente, $F_n(j,j) = 0$. Desta forma, $F_n(t,j)$ é divisível por $(t-j)$, o que é um absurdo, pois pelo item 3, $F_n(t,j)$ é irredutível. Portanto, $P(t,j) = 1$ e $F_n(t,j) = F_n(j,t)$.

□

Definição 20. A equação $F_n(t,j) = 0$ é chamada *equação modular* de grau n.

Para um dado $j(z)$, que é o invariante de modular da curva elíptica dada por $E = \mathbb{C}/\Gamma(1,z)$, as raízes de $F_n(t,j)$ são os invariantes modulares das curvas E_s, $1 \leq s \leq N$, que são associadas a E pelas aplicações $M_s : \Gamma(1,z) \mapsto \Gamma(1, M_s(z))$, onde $E_s := \mathbb{C}/\Gamma(1, M_s(z))$. Em outras palavras, as raízes de $F_n(t,j)$ são os invariantes das curvas definidas pelos reticulados primitivos de índice n em Γ. O item 4 do teorema 7 nos diz que E está entre as imagens dos E_s (por estas mesmas aplicações), i.e., que existe r tal que $E \cong (E_s)_r$. Tal fato também pode ser visto geometricamente da seguinte forma: se Γ' é um sub-reticulado primitivo de índice n em Γ, então $n\Gamma$ é primitivo de índice n em Γ', e curvas definidas por Γ e $n\Gamma$ são isomorfas, ou seja, a curva $\mathbb{C}/\Gamma \cong \mathbb{C}/(n\Gamma)$ esta entre as curvas dadas por reticulados primitivos de índice n de Γ', que, por sua vez, é um reticulado primitivo de índice n de Γ.

3.4 Invariantes de Classes

Teorema 8. *Uma curva elíptica E tem multiplicação complexa se, e somente se, o invariante modular $j(E)$ satisfaz $F_n(j(E), j(E)) = 0$ para algum $n > 1$.*

Demonstração. Sejam $E = \mathbb{C}/\Gamma$, $\Gamma = \Gamma(\omega_1, \omega_2)$ e $\omega := \omega_1/\omega_2$. Então, $j(E) = j(\omega)$. Suponhamos inicialmente que $F_n(j(\omega), j(\omega)) = 0$ para algum $n > 1$. Assim, existe $s \in \{1, \ldots, N\}$ tal que $j(\omega) = j_s(\omega)$. Logo, existe $\mathbf{G}M_s \in H_n/\mathbf{G}$ tal que $j(\mathbf{G}M_s(\omega)) = j(M_s(\omega)) = j(w)$. mas como j é uma bijeção

entre $\mathbb{H}/\mathbf{G}$ e $\mathbb{C}$, existe $A \in \mathbf{G}$ tal que $A\omega = M_s\omega$. Assim, existe $M := A^{-1}M_s \in \mathbf{G}M_s$ (conseqüentemente $M \in H_n$), tal que $M\omega = \omega$.

Se tal M é dada pela matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

então

$$\frac{a\omega + b}{c\omega + d} = \omega,$$

ou seja,

$$\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{\omega_1}{\omega_2}.$$

Isto implica que existe $\lambda \in \mathbb{C}$ tal que:

$$\lambda \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = M \begin{pmatrix} w_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{pmatrix}.$$

Se $\lambda \in \mathbb{Z}$, como (ω_1, ω_2) é base do reticulado Γ, então $a = d = \lambda$ e $b = c = 0$, o que é absurdo, pois esta matriz não pertence a H_n. Logo, $\lambda \notin \mathbb{Z}$ e a curva E tem multiplicação complexa.

Reciprocamente, suponhamos que E tem multiplicação complexa. Já sabemos que $A(E)$ é uma ordem de um corpo quadrático imaginário K. Podemos achar $\lambda \in A(E)$ tal que $N_{K/\mathbb{Q}}(\lambda) = |\lambda|^2 = n > 1$ e $\lambda \notin mA(E)$, para qualquer $m > 1$ inteiro. De fato: seja $A(E) = \Gamma(\tau_1, \tau_2)$. Se $|\tau_1|^2 \leq 1$, seja $t \in \mathbb{N}$ tal que

$$t > \frac{1 + |\tau_1|}{|\tau_2|}.$$

Temos $\Gamma(\tau_1 + t\tau_2, \tau_2) = \Gamma(\tau_1, \tau_2) = A(E)$ e

$$|\tau_1 + t\tau_2|^2 \geq (t\,|\tau_2| - |\tau_1|)^2 > 1.$$

Desta forma, podemos supor que $|\tau_1|^2 > 1$, e como $A(E) \subset \mathcal{O}_K$, temos que $\tau_1 \in \mathcal{O}_K$, e então, $N_{K/\mathbb{Q}}(\tau_1) = |\tau_1|^2 \in \mathbb{N}$. Se, por outro lado, $\tau_1 \in mA(E) = m\Gamma(\tau_1, \tau_2)$, temos que existem $a, b \in \mathbb{Z}$, tais que $\tau_1 = am\tau_1 + bm\tau_2$, e logo, $am = 1$ (pois $am \in \mathbb{Z}$), o que leva a $m = 1$. Assim, tomamos $\lambda := \tau_1$.

Como $\lambda \in A(E)$ e $\lambda \notin mA(E)$ para qualquer $m > 1$, a proposição 14 nos diz que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_n,$$

onde $n := |\lambda|^2$. Logo,

$$\frac{a\omega + b}{c\omega + d} = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{\lambda\omega_1}{\lambda\omega_2} = \omega, \tag{3.8}$$

e assim, existe $s \in \{1, \ldots, N\}$ tal que $j_s(\omega) = j(\mathbf{G}M_s(\omega)) = j(\omega)$, onde

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{G}M_s.$$

□

Teorema 9. *Os invariantes de classes $j(\mathsf{k}_i)$, $i \in \{1, \ldots, h\}$, de um corpo quadrático imaginário K são inteiros algébricos.*

Demonstração. Fixado um corpo quadrático imaginário K, consideremos os invariantes de classes $j(\mathsf{k}_i)$, $i \in \{1, \ldots, h\}$, de K, i.e., os invariantes $j(E)$ das curvas elípticas E tais que $A(E) = \mathcal{O}_K$. Seja $\lambda \in \mathcal{O}_K$ tal que $n = N_{K/\mathbb{Q}}(\lambda)$ seja um inteiro livre de quadrados (e logo, $\lambda \notin \mathbb{Z}$) maior que 1. Tal λ sempre existe pois: se $K = \mathbb{Q}(\sqrt{-1})$, tomamos $\lambda := 1 + \sqrt{-1}$, e se $K = \mathbb{Q}(\sqrt{-m})$, com $m > 1$, livre de quadrados, tomamos $\lambda := \sqrt{-m}$.

Seja (ω_1, ω_2) base de um ideal em uma classe de ideais k de K, e seja também

$$\lambda \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{pmatrix},$$

com $a, b, c, d \in \mathbb{Z}$. Como vimos anteriormente, $ad - bc = n = N_{K/\mathbb{Q}}(\lambda)$, e como n é livre de quadrados, $(a, b, c, d) = 1$. De fato, se existisse $p | a, b, c, d$, então $\lambda/p \in A(E) = \mathcal{O}_K$ e $N_{K/\mathbb{Q}}(\lambda/p) = p^{-2} N_{K/\mathbb{Q}}(\lambda) = p^{-2} n \in \mathbb{Z}$, o que vai contra a hipótese que n é livre de quadrados. Logo,

$$M : z \mapsto \frac{az + b}{cz + d} \in H_n.$$

Como $j(M(\omega)) = j(\omega)$ (como vemos na equação (3.8)), $j(\mathsf{k}) = j(\omega)$ satisfaz $F_n(j(\mathsf{k}), j(\mathsf{k})) = 0$. Pelo teorema 7, temos que $F_n(j, j)$ tem coeficientes inteiros e, como n é livre de quadrados, seu coeficiente dominante é ± 1. Então, $j(\mathsf{k})$ satisfaz um polinômio mônico de coeficientes inteiros e, portanto, é um inteiro algébrico.

□

Capítulo 4

Invariantes de Classes II

4.1 Introdução

Neste capítulo vamos analisar propriedades de certas funções obtidas com o discriminante Δ. Seguiremos aqui uma convenção usual em teoria algébrica dos números, na qual não se faz distinção explícita entre um ideal $\mathfrak{a}$ em um corpo de números K e o ideal $\mathfrak{a}\mathcal{O}_L$ gerado por ele em uma extensão finita L. Em particular, se $\mathfrak{a}_1$ e $\mathfrak{a}_2$ são ideais em K_1 e K_2, respectivamente, e se L é uma extensão finita de ambos os corpos K_1 e K_2, dizemos que $\mathfrak{a}_1$ divide $\mathfrak{a}_2$ (resp. $\mathfrak{a}_1$ e $\mathfrak{a}_2$ são primos entre si) se $\mathfrak{a}_1\mathcal{O}_L$ divide $\mathfrak{a}_2\mathcal{O}_L$ (resp. $\mathfrak{a}_1\mathcal{O}_L$ e $\mathfrak{a}_2\mathcal{O}_L$ são primos entre si). Na verdade temos:

Proposição 20. *Sejam $\mathfrak{a}_1$, $\mathfrak{a}_2$, K_1, K_2 e L como acima. Se $\mathfrak{a}_1\mathcal{O}_L$ divide $\mathfrak{a}_2\mathcal{O}_L$ (resp. $\mathfrak{a}_1\mathcal{O}_L$ e $\mathfrak{a}_2\mathcal{O}_L$ são primos entre si), então $\mathfrak{a}_1\mathcal{O}_{L'}$ divide $\mathfrak{a}_2\mathcal{O}_{L'}$ (resp. $\mathfrak{a}_1\mathcal{O}_{L'}$ e $\mathfrak{a}_2\mathcal{O}_{L'}$ são primos entre si), para qualquer extensão L' de K_1 e K_2.*

Demonstração. Seja $K = K_1 K_2$ o menor corpo que contém K_1 e K_2. Sabemos que $\mathfrak{a}_1\mathcal{O}_L$ divide $\mathfrak{a}_2\mathcal{O}_L$ se, e somente se, $\mathfrak{a}_2\mathcal{O}_L \subset \mathfrak{a}_1\mathcal{O}_L$. Logo $(\mathfrak{a}_2\mathcal{O}_L) \cap \mathcal{O}_K \subset (\mathfrak{a}_1\mathcal{O}_L) \cap \mathcal{O}_K$. Como $(\mathfrak{a}_i\mathcal{O}_L) \cap \mathcal{O}_K = \mathfrak{a}_i\mathcal{O}_K$, temos que $\mathfrak{a}_1\mathcal{O}_K$ divide $\mathfrak{a}_2\mathcal{O}_K$. Mas L' é uma extensão de K, e isto implica que $(\mathfrak{a}_i\mathcal{O}_K)\mathcal{O}_{L'} = \mathfrak{a}_i\mathcal{O}_{L'}$. Conseqüentemente $\mathfrak{a}_2\mathcal{O}_{L'} \subset \mathfrak{a}_1\mathcal{O}_{L'}$, i.e., $\mathfrak{a}_1\mathcal{O}_{L'}$ divide $\mathfrak{a}_2\mathcal{O}_{L'}$. Quando $\mathfrak{a}_1$ e $\mathfrak{a}_2$ forem primos entre si, a demonstração é análoga.

□

4.2 As Funções ϕ_M

Para analisar Δ, será conveniente usarmos a formulação homogênea para funções modulares dada na sub-seção 1.2.2. Assim Δ pode ser vista como uma função homogênea de grau -12 dada por:

$$\Delta(\omega_1, \omega_2) = \omega_2^{-12} \Delta\left(\frac{\omega_1}{\omega_2}\right), \tag{4.1}$$

e temos

$$\Delta(\omega_1, \omega_2) = \left(\frac{2\pi}{\omega_2}\right)^{12} q(1 + B(q)), \quad q := \exp\left(2\pi i \frac{\omega_1}{\omega_2}\right), \tag{4.2}$$

onde $B(q)$ é uma série de potências em q com coeficientes inteiros, satisfazendo $B(0) = 0$, de acordo com a proposição 9 e com a equação (1.33).

Definição 21. Dada $M \in H_n$, definimos

$$\phi_M(\omega_1, \omega_2) := n^{12} \frac{\Delta(M(\omega_1, \omega_2))}{\Delta(\omega_1, \omega_2)}. \tag{4.3}$$

Desta forma, ϕ_M depende apenas da classe $\mathbf{G}M$ de $H_n/\mathbf{G}$, e, a partir das $N = \psi(n)$ classes de $H_n/\mathbf{G}$, obtemos N funções homogêneas de ω_1 e ω_2 de graus iguais a zero:

$$\phi_s(\omega_1, \omega_2) := \phi_{M_s}(\omega_1, \omega_2), \quad 1 \leq s \leq N.$$

Tais funções são regulares para $\mathrm{Im}(\omega_1/\omega_2) > 0$ e são permutadas entre si pela composição com um elemento qualquer de $\mathbf{G}$.

Segue imediatamente de (4.2) que:

$$\phi_s(\omega_1, \omega_2) = a_s^{12} \zeta_{d_s}^{b_s} q^{a_s/d_s - 1} \left(1 + B\left(\zeta_{d_s}^{b_s} q\right)\right) (1 + B(q))^{-1}, \tag{4.4}$$

(observe que como o coeficiente livre de q em $(1 + B(q))$ é 1, e, portanto, inversível em $\mathbb{Z}$, então tal série de potências é inversível como série com coeficientes inteiros) onde $\zeta_d := \exp(2\pi i/d)$, e vemos por argumentos análogos aos usados na prova do teorema 7, que

$$\Phi_n(t,j) := \prod_{s=1}^{N} (t - \phi_s(\omega_1.\omega_2)) \tag{4.5}$$

é um polinômio em t e j com coeficientes inteiros.

Lema 6. *Se $n = p$ é primo, então*

$$\prod_{s=1}^{N} \phi_s(\omega_1.\omega_2) = (-1)^{p-1} p^{12}.$$

Demonstração. Para p primo temos $N = \psi(p) = p + 1$ e as matrizes representantes de H_n podem ser dadas por:

$$M_s := \begin{pmatrix} 1 & s \\ 0 & p \end{pmatrix}, \text{ para } 1 \leq s \leq p; \quad M_{p+1} := \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Portanto,

$$\phi_s(\omega_1,\omega_2) = \zeta_p^s q^{1/p-1} \left(1 + B\left(\zeta_p^s q^{1/p}\right)\right) (1 + B(q))^{-1}, \ (1 \leq s \leq p), \tag{4.6}$$

$$\phi_{p+1}(\omega_1,\omega_2) = p^{12} q^{p-1} (1 + B(q^p)) (1 + B(q))^{-1}, \ (s = p+1), \tag{4.7}$$

e a q-expansão de $\prod_{s=1}^{N} \phi_s(\omega_1,\omega_2)$ se inicia com um termo constante igual a $(-1)^{p-1}p^{12}$. Como tal produtória é uma função modular de peso 0 e holomorfa em $\mathbb{H} \cup \{\infty\}$, já que Δ e $\Delta \circ M_s$ são holomorfas e não nulas em $\mathbb{H}$, e com zeros simples no infinito, pelo princípio da q-expansão tem que ser um polinômio (em j) de grau 0 (portanto constante), e logo, tal função deve ser constante e igual a $(-1)^{p-1}p^{12}$.

□

4.3 Propriedades dos Valores Singulares das ϕ_M's

Fixaremos para esta seção um corpo quadrático imaginário K.

Lema 7. *Sejam* $\mathfrak{a} \in \mathcal{I}(K)$ *e* (α_1, α_2) *uma base*[1] *de* $\mathfrak{a}$ *tal que* $\mathrm{Im}(\alpha_1/\alpha_2) > 0$. *Então, para toda* $M \in H_n$, $\phi_M(\alpha_1, \alpha_2)$ *é um inteiro algébrico e, se* $n = p$ *é primo, o ideal principal* $(\varphi_M(\alpha_1, \alpha_2))$ *é um divisor de* (p^{12}).

Demonstração. Pela definição de Φ_n, temos:

$$\Phi_n(t, j(\mathfrak{a})) = \prod_{s=1}^{N} (t - \phi_s(\alpha_1, \alpha_2)).$$

Mas, pelo teorema 9, $j(\mathfrak{a})$ é um inteiro algébrico, e então, o primeiro membro da igualdade acima é um polinômio (em t) mônico com coeficientes inteiros algébricos. Como $\phi_M = \phi_s$, para algum $s \in \{1, \ldots, N\}$, ϕ_M é raiz de $\Phi_n(t, j(\mathfrak{a}))$, e logo, é um inteiro algébrico ([Ste79], pg. 47). A segunda parte deste lema é conseqüência imediata do lema 6.

□

Seja $\mathfrak{a}$ um ideal integral de K, i.e., um ideal de $\mathcal{O}_K$. Então, para qualquer ideal, integral ou fracionário, $\mathfrak{b}$ de K, $\mathfrak{ab}$ é um sub-grupo aditivo de $\mathfrak{b}$ de índice igual a $N(\mathfrak{a})$. De fato, se $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2^{-1}$, com $\mathfrak{b}_1$ e $\mathfrak{b}_2$ ideais integrais e primos entre si, temos que existe $t \in \mathbb{N}^*$ tal que $\mathfrak{b}_2^t = (\xi)$, pois a ordem do grupo de classes é finita. Logo $(\xi)\mathfrak{b}$ é um ideal integral. Assim:

$$[\mathcal{O}_K : \mathfrak{a}(\xi)\mathfrak{b}] = [\mathcal{O}_K : (\xi)\mathfrak{b}][(\xi)\mathfrak{b} : \mathfrak{a}(\xi)\mathfrak{b}],$$

e então:

$$[(\xi)\mathfrak{b} : \mathfrak{a}(\xi)\mathfrak{b}] = \frac{[\mathcal{O}_K : \mathfrak{a}(\xi)\mathfrak{b}]}{[\mathcal{O}_K : (\xi)\mathfrak{b}]} = \frac{N(\mathfrak{a})N((\xi)\mathfrak{b})}{N((\xi)\mathfrak{b})} = N(\mathfrak{a})$$

(lembrando que a norma de ideais N é multiplicativa). Por outro lado temos que $\mathfrak{b}/(\mathfrak{ab})$ é isomorfo a $((\xi)\mathfrak{b})/((\xi)\mathfrak{ab})$, pelo homomorfismo dado por $a + \mathfrak{ab} \mapsto \xi a + (\xi)\mathfrak{ab}$ $(a \in \mathfrak{b})$. Logo $[\mathfrak{b} : \mathfrak{ab}] = [(\xi)\mathfrak{b} : (\xi)\mathfrak{ab}] = N(\mathfrak{a})$.

Assim, se (β_1, β_2) é uma base de $\mathfrak{b}$, e $(a\beta_1 + b\beta_2, c\beta_1 + d\beta_2)$, $a, b, c, d \in \mathbb{Z}$, é uma base de $\mathfrak{ab}$ (lembramos que $\mathfrak{ab}$ é um sub-reticulado de $\mathfrak{b}$), devemos ter $|ad - bc| = N(\mathfrak{a})$, pois, como ideais, o índice é $N(\mathfrak{a})$, como observamos acima, e, como reticulados, tal índice é o quociente entre as áreas dos respectivos domínios fundamentais. Se temos que $\mathfrak{a}$ não é divisível por nenhum inteiro maior que 1, por exemplo se $\mathfrak{a}$ é primo, então $(a, b, c, d) = 1$. De fato, suponha

[1] Lembramos que, pela proposição 16, tal ideal é um reticulado de $\mathbb{C}$.

que $p|a,b,c,d$. Temos que $(p) = \mathfrak{p}_1\mathfrak{p}_2$ com $\mathfrak{p}_1$ e $\mathfrak{p}_2$ ideais primos de K, ou que (p) é primo em K ([Gol71] pg. 74). No primeiro caso, sejam ϵ_1 e ϵ_2 tais que ϵ_i é o inteiro que aparece como expoente de $\mathfrak{p}_i$ na decomposição em primos de $\mathfrak{b}$ ($i = 1,2$), e assim, $\mathfrak{p}_i$ aparece com expoente maior ou igual a ϵ_i em (β_1) e (β_2). Além disso, como $p|a,b,c,d$, temos $\mathfrak{p}_i|a,b,c,d$, e logo, $\mathfrak{p}_i$ aparece como fator de $(a\beta_1 + b\beta_2)$ e de $(c\beta_1 + d\beta_2)$ com expoente maior ou igual a $(\epsilon_i + 1)$, i.e., $\mathfrak{p}_i$ aparece como fator de $(a\beta_1 + b\beta_2, c\beta_1 + d\beta_2) = \mathfrak{ab}$ com expoente maior ou igual a $(e_i + 1)$. Assim, necessariamente, $\mathfrak{p}_i$ aparece na decomposição em primos de $\mathfrak{a}$ com expoente pelo menos 1. Para o caso que (p) é primo, podemos proceder de maneira análoga.

Definição 22. Dada K_2 uma extensão finita de um corpo de números K_1, e dados $\mathfrak{P}$ e $\mathfrak{p}$ ideais primos de K_2 e K_1 respectivamente, tais que $\mathfrak{P}$ divide $\mathfrak{p}$, definimos $f(\mathfrak{P}/\mathfrak{p})$ como o grau da extensão de corpos[2] $(\mathcal{O}_{K_2}/\mathfrak{P})/(\mathcal{O}_{K_1}/\mathfrak{p})$.

Tal $f(\mathfrak{P}/\mathfrak{p})$ tem diversas propriedades notáveis, como por exemplo: se $\mathfrak{p}$ é um ideal primo de K_1 que se decompõe em primos em K_2 como

$$\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{e(\mathfrak{P}_i/\mathfrak{p})}, \tag{4.8}$$

então

$$\sum_{i=1}^{g} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) = [K_2 : K_1], \tag{4.9}$$

como vemos em [Gol71], pg. 73. Além disso, se K_2/K_1 é galoisiana, temos que os $e(\mathfrak{P}_i/\mathfrak{p})$ e os $f(\mathfrak{P}_i/\mathfrak{p})$ na fórmula (4.8) não dependem de i, i.e., existem inteiros positivos $e_\mathfrak{p}$ e $f_\mathfrak{p}$ tais que $e(\mathfrak{P}_i/\mathfrak{p}) = e_\mathfrak{p}$ e $f(\mathfrak{P}_i/\mathfrak{p}) = f_\mathfrak{p}$ para todo $i \in \{1,\ldots,g\}$, e então, a fórmula (4.9) torna-se $[K_2 : K_1] = e_\mathfrak{p} f_\mathfrak{p} g$ ([Gol71], pg. 84).

Definição 23. Dizemos que um ideal primo $\mathfrak{p}$ de K é de *grau um* se $f(\mathfrak{p}/p) = 1$, onde p é o inteiro primo tal que $(p) = \mathfrak{p} \cap \mathbb{Z}$.

Deduz-se da definição do *homomorfismo norma*, que $N_{K/\mathbb{Q}}(\mathfrak{p}) = (p)^{f(\mathfrak{p}/p)}$. Por outro lado, como vemos em [Gol71], pg. 79, $N_{K/\mathbb{Q}}(\mathfrak{p}) = N(\mathfrak{p})\mathbb{Z}$. Logo,

[2]Lembramos que os ideais primos dos corpos de números são também maximais ([Gol71], pg. 14).

temos que $N(\mathfrak{p}) = p^{f(\mathfrak{p}/p)}$, com p primo. Desta forma, $\mathfrak{p}$ tem grau 1, se, e só se, $N(\mathfrak{p}) = p$, com p primo.

Temos que $\mathfrak{p}$ é *não ramificado* em $K/\mathbb{Q}$ se seu quadrado não divide um inteiro primo, i.e., se o *índice de ramificação* $e(\mathfrak{p}/p)$ for igual a um. Sabemos que $\mathfrak{p}$ é não ramificado se, e somente se, $\mathfrak{p} \cap \mathbb{Z}$ não divide o discriminante $d_{K/\mathbb{Q}}$ ([Gol71], pg. 81).

Portanto, se $\mathfrak{p}$ é um ideal primo de K de grau um e não ramificado, então $\mathfrak{p} \neq \bar{\mathfrak{p}}$ (onde a barra denota a conjugação complexa) e $(p) = \mathfrak{p}\bar{\mathfrak{p}}$. De fato, como $K/\mathbb{Q}$ é galoisiana, pois é de grau 2, temos que os elementos do grupo de Galois permuta os primos de K sobre um dado p inteiro primo ([Gol71], pg. 83). Como o grau da extensão é 2, temos no máximo dois primos sobre $(p) = \mathfrak{p} \cap \mathbb{Z}$. Já que $\mathfrak{p}$ é de grau 1, temos que ou existem exatamente dois primos distintos sobre p ou existe apenas o quadrado de um primo. A segunda hipótese é descartada, já que $\mathfrak{p}$ é não ramificado. Logo, o outro primo sobre p é dado pela conjugação complexa de $\mathfrak{p}$, pois este é o único elemento não trivial de $\mathrm{Gal}(K/\mathbb{Q})$. Assim: $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, com $\mathfrak{p} \neq \bar{\mathfrak{p}}$.

Teorema 10. *Sejam (α_1, α_2) uma base de um ideal $\mathfrak{a}$ de K, $\mathfrak{p}$ ideal primo de grau um de K não ramificado para $K/\mathbb{Q}$ e $p = N(\mathfrak{p})$. Existe $P \in H_p$ (resp. $\bar{P} \in H_p$) tal que $P(\alpha_1, \alpha_2)$ (resp. $\bar{P}(\alpha_1, \alpha_2)$) é uma base de $\mathfrak{p}\mathfrak{a}$ (resp. $\bar{\mathfrak{p}}\mathfrak{a}$). Além disso, temos:*

$$(\phi_P(\alpha_1, \alpha_2)) = \bar{\mathfrak{p}}^{12}, \ (\phi_{\bar{P}}(\alpha_1, \alpha_2)) = \mathfrak{p}^{12},$$

e se $M \in H_p$, com $M \notin \mathbf{G}P, \mathbf{G}\bar{P}$, então $\phi_M(\alpha_1, \alpha_2)$ é uma unidade (i.e., é um inteiro algébrico com inverso também inteiro algébrico).

Demonstração. Seja $t \in \mathbb{N}^*$ tal que $\mathfrak{p}^t$ é um ideal principal em K. Assim, $\mathfrak{p}^t = (\xi)$, com $\xi \in \mathcal{O}_K$, e $\xi\bar{\xi} = N_{K/\mathbb{Q}}(\xi) = N(\xi\mathcal{O}_K) = N(\mathfrak{p}^t) = N(\mathfrak{p})^t = p^t$.

Se $P(\alpha_1, \alpha_2)$ é base de $\mathfrak{a}\mathfrak{p}$, temos pela discussão anterior que $\det P = N(\mathfrak{p}) = p$, e, como $\mathfrak{p}$ é primo, $(a, b, c, d) = 1$; então $P \in H_p$.

Além disso, podemos achar $P = P_1, P_2, \ldots, P_t \in H_p$ de tal forma que $P_i \cdot P_{i-1} \ldots P_1(\alpha_1, \alpha_2)$ é uma base de $\mathfrak{p}^i\mathfrak{a}$, para $1 \leq i \leq t$, e com $P_t \ldots P_1(\alpha_1, \alpha_2) = (\xi\alpha_1, \xi\alpha_2)$. Seja

$$\lambda_i := \phi_{P_i}(P_{i-1} \ldots P_1(\alpha_1, \alpha_2)) = p^{12} \frac{\Delta(P_i \ldots P_1(\alpha_1, \alpha_2))}{\Delta(P_{i-1} \ldots P_1(\alpha_1, \alpha_2))},$$

para $1 \leq i \leq t$. Então,

$$\prod_{i=1}^{t} \lambda_i = p^{12t} \frac{\Delta(P_t \dots P_1(\alpha_1, \alpha_2))}{\Delta(\alpha_1, \alpha_2)}$$
$$= p^{12t} \frac{\Delta(\xi\alpha_1, \xi\alpha_2)}{\Delta(\alpha_1, \alpha_2)}$$
$$= p^{12t} \xi^{-12}$$

Mas como $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, temos que $(p)^t = \mathfrak{p}^t\bar{\mathfrak{p}}^t = (\xi)(\bar{\xi})$, e assim,

$$\prod_{i=1}^{t}(\lambda_i) = (p)^{12t}(\xi)^{-12} = \overline{(\xi)}^{12}.$$

Como os λ_i's são inteiros algébricos, pelo lema 7, o ideal (λ_i) divide $(\bar{\xi}^{12}) = \bar{\mathfrak{p}}^{12t}$. Mas, pelo mesmo lema, (λ_i) também divide $(p^{12}) = \mathfrak{p}^{12}\bar{\mathfrak{p}}^{12}$. Assim, (λ_i) é um divisor de $\bar{\mathfrak{p}}^{12}$. Como $\prod_{i=1}^{t}(\lambda_i) = (\bar{\xi})^{12} = \bar{\mathfrak{p}}^{12t}$, temos que $(\lambda_i) = \bar{\mathfrak{p}}^{i2}$, para todo $i \in \{1, \dots, t\}$, e, em particular, $(\phi_P(\alpha_1, \alpha_2)) = (\lambda_1) = \bar{\mathfrak{p}}^{12}$. Analogamente, $(\phi_{\bar{P}}(\alpha_1, \alpha_2)) = \mathfrak{p}^{12}$. Como $\mathfrak{p} \neq \bar{\mathfrak{p}}$, temos que $\mathbf{G}P \neq \mathbf{G}\bar{P}$. Além disso,

$$\prod_{i=1}^{N}(\phi_i(\alpha_1, \alpha_2)) = (p^{12}) = \mathfrak{p}^{12}\bar{\mathfrak{p}}^{12}$$

implica que $(\phi_M(\alpha_1, \alpha_2)) = \mathcal{O}_K$ se $\mathbf{G}M \neq \mathbf{G}P$ e $\mathbf{G}M \neq \mathbf{G}\bar{P}$, i.e., $\phi_M(\alpha_1, \alpha_2)$ é uma unidade. □

4.4 Uma Congruência Formal

Sejam ξ e η séries de potências em determinadas variáveis, com coeficientes inteiros algébricos, e seja $\mathfrak{a}$ um ideal integral. Como é usual, escreveremos:

$$\xi \equiv \eta \pmod{\mathfrak{a}}$$

se todos os coeficientes de $(\xi - \eta)$ estão em $\mathfrak{a}$.

Consideremos as q séries $\xi_k(q)$ e $\eta_k(q)$, para $1 \leq k \leq (p+1)$, com p inteiro primo, e satisfazendo as seguintes propriedades:

1. seus coeficientes são inteiros algébricos de $\mathbb{Q}(\zeta_p)$ (i.e., em $\mathbb{Z}(\zeta_p)$); ξ_p, ξ_{p+1}, η_p e η_{p+1} têm coeficientes inteiros. Os ξ_k's (resp. η_k's), para $1 \leq$

$k \leq (p-1)$, são permutados pelos automorfismos do grupo de Galois de $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, e

$$\xi_k \equiv \xi_l, \quad \eta_k \equiv \eta_l \pmod{(1-\zeta_p)},$$

para $1 \leq k, l \leq p$.

2. Tais séries representam funções holomorfas em $\mathbb{H}$ que são permutadas entre si por $\mathbf{G}$.

Temos que as ϕ_k's, com $n \neq p$, satisfazem tais condições, como vemos em (4.6) e (4.7). O mesmo vale para os j_k's, pois:

$$j_k(q) = \zeta_p^{-k} q^{-1/p} \left(1 + A(\zeta_p^k q^{1/p})\right) \tag{4.10}$$

$$j_{p+1}(q) = q^{-p}\left(1 + A(q^p)\right), \tag{4.11}$$

onde A tem coeficientes inteiros. Tais funções serão as únicas funções satisfazendo 1 e 2 que usaremos aqui. Na verdade elas motivam tais definições e as usaremos para provar propriedades comuns às ϕ_k's e j_k's.

Deixando t e u como indeterminadas, definimos:

$$G_p(t, u, \xi_k, \eta_l) := \sum_{k=1}^{p+1} \left[(t - \xi_k) \prod_{\substack{l=1 \\ l \neq k}}^{p+1} (u - \eta_l) \right].$$

Lema 8. *1. $G_p(t, u, \xi_k, \eta_l) = \tilde{G}_p(t, u, j)$ é um polinômio em t, u e j com coeficientes inteiros.*

2. $G_p(t, u, \xi_k(q), \eta_l(q)) \equiv (t - \xi_{p+1}(q))(u^p - \eta_p(q)^p) \pmod{p}$.

Demonstração. O *primeiro* item é provado exatamente tal como no item 1 do teorema 7.

Vamos agora ao *segundo* item; vejamos como (p) se fatora em $\mathbb{Q}(\zeta_p)$: temos que

$$X^{p-1} + X^{p-2} + \cdots + X + 1 = \prod_{i=1}^{p-1} (X - \zeta_p^i),$$

e logo,

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

Mas $(1-\zeta_p^i) = (1-\zeta_p)(1+\zeta_p+\cdots+\zeta_p^{i-1})$, o que implica que $(1-\zeta_p^i)$ pertence ao ideal $(1-\zeta_p)$, para $1 \leq i \leq (p-1)$. Portanto, $(1-\zeta_p)^{p-1}|(p)$. Como $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = (p-1)$, temos que o maior expoente de um divisor de (p) em $\mathbb{Q}(\zeta_p)$ é $(p-1)$, e logo, $(1-\zeta_p)$ é primo e $(1-\zeta_p)^{p-1} = (p)$.

Temos que ambos os lados da congruência do segundo item do teorema têm coeficientes inteiros: o lado esquerdo pelo primeiro item e pelo princípio da q-expansão, e o lado direito porque ξ_{p+1} e η_p têm coeficientes inteiros pela hipótese 1. Desta forma, este fato e a decomposição de (p) em $\mathbb{Q}(\zeta_p)$ implicam que basta provar a congruência módulo $(1-\zeta_p)$. Pela hipótese 1, temos:

$$\begin{aligned} G_p(t,u,\xi_k,\eta_l) \equiv & (t-\xi_{p+1})(u-\eta_p)^p \\ & + p(u-\eta_{p+1})(t-\xi_p)(u-\eta_p)^{p-1} \pmod{(1-\zeta_p)}. \end{aligned}$$

Como $(u-\eta_p)^p \equiv u^p - \eta_p^p \pmod{p}$, temos o procurado. □

4.5 Aplicações

A equação modular de grau p é dada por $F_p(j,j) = 0$, onde $F_p(t,j) = \prod_{k=1}^{p+1}(t-j_k)$ é um polinômio em t e j como coeficientes inteiros, como nos diz o teorema 7. A seguinte propriedade de F_p é um resultado clássico devido a H. Weber:

Teorema 11. $F_p(t,j) \equiv (t-j^p)(t^p-j) \pmod{p}$, *para p primo.*

Demonstração. Pelas equações (4.10) e (4.11) e pelo "Pequeno Teorema de Fermat", temos:

$$j_{p+1}(q) \equiv j(q)^p \pmod{p} \tag{4.12}$$

$$j_p(q)^p \equiv j(q) \pmod{p}. \tag{4.13}$$

Usando esse resultado e aplicando o lema 8 para $t = u$ e $\xi_k = \eta_k = j_k$, com $1 \leq k \leq (p+1)$, i.e.,

$$G_p(t, t, j_k, j_l) = \sum_{k=1}^{p+1} \left[(t - j_k) \prod_{\substack{l=1 \\ l \neq k}}^{p+1} (t - j_l) \right]$$
$$= (p+1) \prod_{k=1}^{p+1} (t - j_k) = (p+1)\, F_p(t, j);$$

observando que

$$\tilde{G}_p(t, t, j) = (p+1) F_p(t, j) \equiv F_p(t, j) \pmod{p},$$

conseguimos

$$F_p(t, j) \equiv (t - j_{p+1})(t^p - j_p^p) \pmod{p}.$$

Mas as congruências dadas pelas fórmulas (4.12) e (4.13) nos dão

$$F_p(t, j) \equiv (t - j^p)(t^p - j) \pmod{p}.$$

Assim, como *série de potências* em t e q, a diferença entre os dois lados da equação acima tem coeficientes em $p\mathbb{Z}$. Pelo princípio da q-expansão, o mesmo é verdade para a tal diferença como polinômio em t e j.

□

Teorema 12. *Sejam K um corpo quadrático imaginário, $\mathfrak{p}$ um ideal primo de K de grau um e não ramificado para $K/\mathbb{Q}$, e $\mathsf{k}_\mathfrak{p}$ a classes de ideais que contém $\mathfrak{p}$. Então, para toda classe de ideais k de K, temos:*

$$j(\mathsf{k}_\mathfrak{p}^{-1}\mathsf{k}) \equiv j(\mathsf{k})^{N(\mathfrak{p})} \pmod{\mathfrak{p}}.$$

Demonstração. Seja $\mathfrak{a}$ um ideal pertencente à classe k. Seja p o inteiro primo tal que $N(\mathfrak{p}) = \mathfrak{p}\bar{\mathfrak{p}} = (p)$. Assim, a classe de ideais $\mathsf{k}_\mathfrak{p}^{-1}$ contém o ideal $\bar{\mathfrak{p}}$, e logo, basta mostrar que

$$j(\bar{\mathfrak{p}}\mathfrak{a}) \equiv j(\mathfrak{a})^p \pmod{\mathfrak{p}}.$$

Seja (α_1, α_2) uma base de $\mathfrak{a}$. Pelo teorema 10, existem $P, \bar{P} \in H_p$ tais que $P(\alpha_1, \alpha_2)$ é base de $\mathfrak{p}\mathfrak{a}$ e $\bar{P}(\alpha_1, \alpha_2)$ é base de $\bar{\mathfrak{p}}\mathfrak{a}$. Sejam também $c, d \leq (p+1)$ índices tais que $P \in \mathbf{G}M_c$ e $\bar{P} \in \mathbf{G}M_d$. Como $\mathfrak{p} \neq \bar{\mathfrak{p}}$, $c \neq d$, e temos também

$$j(\bar{\mathfrak{p}}\mathfrak{a}) = j_{\bar{P}}(\mathfrak{a}) = j_d(\mathfrak{a}) = j_d(\alpha_1, \alpha_2).$$

Aplicando o lema 8 para o caso $\xi_k = j_k$, $\eta_l = \phi_l$, e $t = j^p$, conseguimos

$$G_p(j^p(q), u, j_k(q), \phi_l(q)) \equiv (j^p(q) - j_{p+1}(q))(u^p - \phi_p^p(q)) \pmod{p},$$

que juntamente com as equações (4.12) e (4.13), resulta em

$$G_p(j(q)^p, u, j_k(q), \phi_l(q)) \equiv 0 \pmod{p}$$

(como série de potências em u e q). Pelo princípio de q-expansão, temos:

$$\tilde{G}_p(j^p, u, j) \equiv 0 \pmod{p},$$

onde, como no lema 8, $\tilde{G}_p$ é G_p como polinômio em j e u.

Seja agora $q_0 := \exp(2\pi i\alpha_1/\alpha_2)$. Então, $j(q_0)$, $j_k(q_0)$, $\phi_l(q_0)$ são inteiros algébricos. Como $G_p(j^p, u, j_k, \phi_l)$ pode ser escrita como *polinômio* em u e j com coeficientes em $p\mathbb{Z}$, seu valor para $q = q_0$ é um polinômio em u com coeficientes inteiros algébricos divisíveis por p. Assim,

$$G_p(j(\mathfrak{a})^p, u, j_k(\mathfrak{a}), \phi_l(\alpha_1, \alpha_2)) \equiv 0 \pmod{p}.$$

Coloquemos agora $u = \phi_{\bar{p}}(\alpha_1, \alpha_2) = \phi_d(\alpha_1, \alpha_2)$. Portanto, pela equação acima e pela definição de G_p, temos:

$$(j(\mathfrak{a})^p - j_d(\mathfrak{a})) \prod_{\substack{k=1 \\ k\neq d}}^{p+1} (\phi_d(\alpha_1, \alpha_2) - \phi_k(\alpha_1, \alpha_2)) \equiv 0 \pmod{p}.$$

Como $\mathfrak{p}|(p)$, a equação acima nos dá:

$$(j(\mathfrak{a})^p - j_d(\mathfrak{a})) \prod_{\substack{k=1 \\ k\neq d}}^{p+1} (\phi_d(\alpha_1, \alpha_2) - \phi_k(\alpha_1, \alpha_2)) \equiv 0 \pmod{\mathfrak{p}}.$$

Pelo teorema 10 sabemos que $\phi_d(\alpha_1, \alpha_2) \equiv 0 \pmod{\mathfrak{p}}$, e assim:

$$\prod_{\substack{k=1 \\ k\neq d}}^{p+1} (\phi_d(\alpha_1, \alpha_2) - \phi_k(\alpha_1, \alpha_2)) \equiv (-1)^p \prod_{\substack{k=1 \\ k\neq d}}^{p+1} \phi_k(\alpha_1, \alpha_2) \pmod{\mathfrak{p}}.$$

Além disso, pelo mesmo teorema, o ideal gerado pelo segundo membro da equação acima é o ideal $\bar{\mathfrak{p}}^{12}$, que é primo com $\mathfrak{p}$. Logo,

$$j(\mathfrak{a})^p - j_d(\mathfrak{a}) \equiv 0 \pmod{\mathfrak{p}}.$$

Como $j_d(\mathfrak{a}) = j(\bar{\mathfrak{p}}\mathfrak{a})$, temos o resultado procurado.

□

Capítulo 5

Corpos de Classes

5.1 Introdução

Como ficou provado no capítulo 4, os invariantes de classes $j(\mathfrak{k})$'s de um corpo quadrático imaginário K satisfazem certas congruências formais. A seguir, daremos inicialmente uma visão geral da teoria de corpos de classes em sua forma clássica e, usando tal teoria, mostraremos como deduzir de tais congruências propriedades aritméticas dos invariantes de classes $j(\mathfrak{k})$'s e da extensão $K(j(\mathfrak{k}))/K$.

5.2 Grupos de Ideais

Neste capítulo, salvo menção contrária, consideraremos K um corpo de números qualquer, não necessariamente um corpo quadrático imaginário.

Inicialmente, precisamos definir *K-primos finitos* e *infinitos*. Os *K-primos finitos* representam simplesmente os ideais primos de $\mathcal{O}_K$, aos quais associamos um valor absoluto não-arquimediano da seguinte forma: dado $\alpha \in K$ e um primo $\mathfrak{p}$ finito de K, então $|\alpha|_{\mathfrak{p}} := N(\mathfrak{p})^{-\nu_{\mathfrak{p}}(\alpha)}$, onde $\nu_{\mathfrak{p}}(\alpha)$ é, por definição, o inteiro que aparece como expoente de $\mathfrak{p}$ na decomposição em ideais primos do ideal principal (α). Os *K-primos infinitos* são símbolos associados aos morfismos de K em $\bar{\mathbb{Q}}$ sobre $\mathbb{Q}$, a partir dos quais definimos valores absolutos arquimedianos: se $[K : \mathbb{Q}] = n$, teremos n morfismos; tal n pode ser escrito como $n = r_1 + 2r_2$, com r_1 representando o número de morfismos *reais* (i.e., com imagem em $\mathbb{R}$) e r_2 representando o número de morfismos *complexos* (i.e., com a imagem em $\mathbb{C}$, mas não em $\mathbb{R}$) não conjugados; dado

então um morfismo σ dentre estes $r_1 + r_2$ morfismos *não conjugados*, associamos a ele um primo infinito $\mathfrak{p}_\sigma$ e definimos um valor absoluto (arquimediano) dado por $|\alpha|_\sigma := |\sigma(\alpha)|$.

Definição 24. Um *divisor* $\mathfrak{m}$ do corpo K é um produto formal de um número finito de K-primos (finitos e infinitos):

$$\mathfrak{m} = \prod \mathfrak{p}_i^{e_i}.$$

Dado tal divisor, denotaremos por $\mathfrak{m}_0$ o produto dos primos finitos de $\mathfrak{m}$ e por $\mathfrak{m}_\infty$ o produto dos primos infinitos de $\mathfrak{m}$ (e então, $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$).

Consideraremos aqui sempre divisores $\mathfrak{m}$ tais que $\mathfrak{m}_0$ é um ideal *integral* de K e $\mathfrak{m}_\infty$ é um produto de K-primos infinitos *reais* e *distintos*. Desta forma, para $\xi \in K$, vamos então escrever:

$$\xi \equiv 1 \pmod{\mathfrak{m}}$$

se, e somente se, $\nu_{\mathfrak{p}_i}(\xi - 1) \geq e_i$ e $\sigma_{\mathfrak{p}_j}(\xi) > 0$, para todo $\mathfrak{p}_j | \mathfrak{m}_\infty$, onde $\nu_{\mathfrak{p}_i}(\mathfrak{a})$ é a potência de $\mathfrak{p}_i$ que aparece na fatoração do ideal $\mathfrak{a}$ e $\sigma_{\mathfrak{p}_j}$ é o morfismo de K no corpo dos reais $\mathbb{R}$ correspondente ao ideal infinito $\mathfrak{p}_j$.

Dado um divisor $\mathfrak{m}$ de K, denotaremos por $\mathcal{I}_\mathfrak{m}(K)$ o grupo multiplicativo de todos os ideais não nulos de K primos com $\mathfrak{m}_0$, e por $\mathcal{S}_\mathfrak{m}(K)$ o sub-grupo de $\mathcal{I}_\mathfrak{m}(K)$ dos ideais principais (ξ) tais que $\xi \equiv 1 \pmod{\mathfrak{m}}$. Como pode ser visto em [Gol71], pg. 42, $\mathcal{I}_\mathfrak{m}(K)/\mathcal{S}_\mathfrak{m}(K)$ é finito.

Definição 25. Um grupo qualquer H tal que $\mathcal{S}_\mathfrak{m}(K) \subset H \subset \mathcal{I}_\mathfrak{m}(K)$ é chamado de um *grupo de ideais de K definido módulo* $\mathfrak{m}$.

5.3 Densidade de um Conjunto de Ideais Primos

Sejam $\mathcal{P}(K)$ o conjunto de todos os ideais primos de K e $M \subset \mathcal{P}(K)$. Definimos então:

$$\mu(s; M) := \sum_{\mathfrak{p} \in M} N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}.$$

Tal soma converge absolutamente para $\mathrm{Re}(s) > 1$. De fato, seja $n = [K : \mathbb{Q}]$, e $\mathfrak{p} \in \mathcal{P}(K)$. Logo, $\mathfrak{p} \cap \mathbb{Q} = (p)$, com p inteiro primo; podemos escrever

$(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$, supondo $\mathfrak{p}_1 = \mathfrak{p}$, e também $N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_i}$, de tal forma que $\sum_{i=1}^{g} e_i f_i = n$. Assim, no pior caso (relativamente à convergência) teríamos $g = n$ e $e_i = f_i = 1$, para $i \in \{1, \dots, g\}$. Como $|X^s| = X^{\mathrm{Re}(s)}$, para $X \in \mathbb{Q}_+$ (onde $\mathbb{Q}_+$ denota o conjunto dos racionais não negativos), temos:

$$\begin{aligned}
\sum_{\mathfrak{p} \in M} \left| N_{K/\mathbb{Q}}(\mathfrak{p})^{-s} \right| &\leq \sum_{\mathfrak{p} \in \mathcal{P}(K)} \left| N_{K/\mathbb{Q}}(\mathfrak{p})^{-s} \right| \\
&= \sum_{\mathfrak{p} \in \mathcal{P}(K)} N_{K/\mathbb{Q}}(\mathfrak{p})^{-\mathrm{Re}(s)} \\
&\leq \sum_{\substack{p \in \mathcal{P}(\mathbb{Q}) \\ p > 0}} n p^{-\mathrm{Re}(s)} \\
&\leq n \sum_{k=1}^{\infty} k^{-\mathrm{Re}(s)},
\end{aligned}$$

que converge se $\mathrm{Re}(s) > 1$.

Definição 26. Se o limite

$$\delta(M) := \lim_{s \to 1_+} \frac{\mu(s; M)}{\mu(s; \mathcal{P}(K))}$$

existir, chamaremos seu valor de *densidade de Dirichlet* de $M \subset \mathcal{P}(K)$.

Lembramos da definição da função zeta de Riemann para um corpo de números K:

$$\zeta_K(s) := \prod_{\mathfrak{p} \in \mathcal{P}(K)} \left(1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}\right)^{-1}.$$

Temos:

$$\mu(s; \mathcal{P}(K)) \sim \log(\zeta_K(s)) \sim \log\left(\frac{1}{s-1}\right),$$

onde o símbolo $\sim$ indica que a diferença entre os dois lados de $\sim$ é limitada em $s = 1$. De fato: usando que

$$\log\left(\frac{1}{1-z}\right) = \sum_{m=1}^{\infty} \frac{1}{m} z^m$$

temos

$$\log \prod_{\mathfrak{p}\in\mathcal{P}(K)} \left(1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}\right)^{-1} = \sum_{\mathfrak{p}\in\mathcal{P}(K)} \log\left(1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}\right)^{-1}$$
$$= \sum_{\mathfrak{p}\in\mathcal{P}(K)} \sum_{m=1}^{\infty} \frac{1}{m} N_{K/\mathbb{Q}}(\mathfrak{p})^{-sm}$$
$$= \mu(s;\mathcal{P}(K)) + \sum_{\mathfrak{p}\in\mathcal{P}(K)} \sum_{m=2}^{\infty} \frac{1}{m} N_{K/\mathbb{Q}}(\mathfrak{p})^{-sm}.$$

Mas, se $[K:\mathbb{Q}] = n$, e tomando $s = 1$,

$$\sum_{\mathfrak{p}\in\mathcal{P}(K)} \sum_{m=2}^{\infty} \frac{1}{m} N_{K/\mathbb{Q}}(\mathfrak{p})^{-m} \leq \sum_{p\in\mathcal{P}(\mathbb{Q})} \sum_{m=2}^{\infty} n \frac{1}{mp^m}$$
$$\leq n \sum_{p\in\mathcal{P}(\mathbb{Q})} \sum_{m=2}^{\infty} \frac{1}{p^m}$$
$$= n \sum_{p\in\mathcal{P}(\mathbb{Q})} \frac{1}{p(p-1)}$$
$$\leq n \sum_{k=2}^{\infty} \frac{1}{k(k-1)} < \infty,$$

o que justifica o primeiro $\sim$. O segundo é justificado pelo fato que $\zeta_K(s)$ tem um polo *simples* em $s = 1$ ([Ser73], pg. 72).

É claro então que

$$\mu(s;\mathcal{P}(K)) \sim \log\left(\frac{1}{s-1}\right),$$

o que implica

$$\lim_{s\to 1_+} \frac{\mu(s;\mathcal{P}(K))}{\log\left(\frac{1}{s-1}\right)} = 1.$$

Desta forma poderíamos definir a densidade de Dirichlet também por:

$$\delta(M) = \lim_{s\to 1_+} \frac{\mu(s;M)}{\log\left(\frac{1}{s-1}\right)}.$$

Exemplo 3. Seja $\mathcal{P}'(K)$ o conjunto dos ideais primos de K com grau um, e seja $\mathcal{P}''(K)$ o seu complementar em $\mathcal{P}(K)$. Logo, para todo $\mathfrak{p} \in \mathcal{P}''(K)$, $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^f \geq p^2$, onde p é o primo tal que $\mathfrak{p} \cap \mathbb{Z} = (p)$. Assim

$$\mu(1; \mathcal{P}''(K)) \leq n \sum_{m=2}^{\infty} \frac{1}{m^2} \leq \infty,$$

e logo $\delta(\mathcal{P}''(K)) = 0$ e $\delta(\mathcal{P}'(K)) = 1$. Na verdade, de maneira mais geral, se $M' = M \cap \mathcal{P}'(K)$ e $M'' = M \cap \mathcal{P}''(K)$, temos $\delta(M') = \delta(M)$ e $\delta(M'') = 0$.

Teorema 13 (Teorema da Progressão Aritmética). *Seja H um grupo de ideais definido módulo $\mathfrak{m}$ e seja k uma classe de de $\mathcal{I}_{\mathfrak{m}}(K)/H$. Então*

$$\delta(\mathsf{k} \cap \mathcal{P}(K)) = \delta(\mathsf{k} \cap \mathcal{P}'(K)) = \frac{1}{h},$$

onde $h = [\mathcal{I}_{\mathfrak{m}}(K) : H]$.

Observação. Tal teorema é uma generalização do teorema de Dirichlet, onde $K = \mathbb{Q}$. Uma prova detalhada deste teorema pode ser encontrada em [Ser73].

5.4 A Desigualdade $h \leq n$

Seja L uma extensão galoisiana de grau n de K. Um ideal primo $\mathfrak{p}$ de K *decompõe-se completamente* em L se $\mathfrak{p}$ se escreve como um produto de n primos de L distintos, ou, equivalentemente, se $\mathfrak{p}$ é não ramificado em L e $\mathfrak{p} = N_{L/K}(\mathfrak{P})$, para algum ideal primo $\mathfrak{P}$ de L. De fato, temos que $\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_1 \ldots \mathfrak{P}_g$, com os $\mathfrak{P}_i$'s distintos entre si, e com $\mathfrak{P} = \mathfrak{P}_1$, por exemplo. Logo $f_1 = f(\mathfrak{P}_1/\mathfrak{p}) = 1$, e como a extensão L/K é galoisiana (e portanto, normal), $f_i = f(\mathfrak{P}_i/\mathfrak{p}) = f_1 = 1$ para todo $i \in \{1, \ldots, g\}$ ([Gol71], pg. 84), e logo, $g = n$.

Seja $\mathcal{W}$ o conjunto dos ideais primos $\mathfrak{p}$ de K que se decompõem completamente em L, e seja $\mathcal{P}'''(L)$ o conjunto dos ideais primos $\mathfrak{P}$ de L de grau um (sobre $\mathbb{Q}$, e portanto, sobre K) e tais que $\mathfrak{p} = N_{L/K}(\mathfrak{P})$ é não ramificado em L. Desta forma, a aplicação $\mathfrak{P} \mapsto \mathfrak{p} = N_{L/K}(\mathfrak{P})$ é n a 1 entre $\mathcal{P}'''(L)$ e $\mathcal{W}' = \mathcal{W} \cap \mathcal{P}'(K)$, i.e., para cada elemento de $\mathcal{W}'$ existem exatamente n elementos de $\mathcal{P}'''(L)$ que são levados nele por tal aplicação. Como $N_{L/\mathbb{Q}}(\mathfrak{P}) = N_{K/\mathbb{Q}}(\mathfrak{p})$, então $\mu(s; \mathcal{P}'''(L)) = n\mu(s; \mathcal{W}')$. No entanto, a diferença entre $\mathcal{P}'(L)$ e $\mathcal{P}'''(L)$ é um conjunto finito, pois existem apenas finitos

$\mathfrak{p} \in \mathcal{P}(K)$ tais que $\mathfrak{p}|d_{L/K}$ e existem finitos $\mathfrak{P} \in \mathcal{P}(L)$ tais que $N_{L/K}(\mathfrak{P}) = \mathfrak{p}$; desta forma $\delta(\mathcal{P}'''(L)) = \delta(\mathcal{P}'(L)) = \delta(\mathcal{P}(L)) = 1$. Por outro lado:

$$\delta(\mathcal{P}'''(L)) = \lim_{s \to 1_+} \frac{\mu(s; \mathcal{P}'''(L))}{\log\left(\frac{1}{s-1}\right)}$$

$$= \lim_{s \to 1_+} \frac{n\,\mu(s; \mathcal{W}')}{\log\left(\frac{1}{s-1}\right)}$$

$$= n\,\delta(\mathcal{W}') = n\,\delta(\mathcal{W}).$$

Logo $\delta(\mathcal{W}) = 1/n$.

Definição 27. Seja $\mathfrak{m}$ um divisor de K. Definimos o grupo

$$\mathcal{N}_{\mathfrak{m}} = \mathcal{N}_{\mathfrak{m}}(L/K) := \mathcal{S}_{\mathfrak{m}}(K)\, N_{L/K}(\mathcal{I}_{\mathfrak{m}}(L)).$$

Como $\mathcal{O}_L \in \mathcal{I}_{\mathfrak{m}}(L)$ e $N_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$, temos que $\mathcal{S}_{\mathfrak{m}}(K) \subset \mathcal{N}_{\mathfrak{m}}$, e claramente $\mathcal{N}_{\mathfrak{m}} \subset \mathcal{I}_{\mathfrak{m}}(K)$. Segue então que $\mathcal{N}_{\mathfrak{m}}$ é um grupo de ideais de K definido módulo $\mathfrak{m}$. Usaremos como notação:

$$h_{\mathfrak{m}} = h_{\mathfrak{m}}(L/K) := [\mathcal{I}_{\mathfrak{m}}(K) : \mathcal{N}_{\mathfrak{m}}].$$

Pela definição de $\mathcal{W}$, $\mathcal{W}_{\mathfrak{m}} = \mathcal{W} \cap \mathcal{I}_{\mathfrak{m}}(K)$ está contido em $N_{L/K}(\mathcal{I}_{\mathfrak{m}}(L))$. Portanto, $\mathcal{W}_{\mathfrak{m}} \subset \mathcal{N}_{\mathfrak{m}}$, e como $\mathcal{W}_{\mathfrak{m}} \subset \mathcal{P}(K)$, deduz-se que $\mathcal{W}_{\mathfrak{m}} \subset \mathcal{P}(K) \cap \mathcal{N}_{\mathfrak{m}}$. Como a diferença entre $\mathcal{W}$ e $\mathcal{W}_{\mathfrak{m}}$ é um conjunto finito, temos pelo teorema da progressão aritmética que:

$$\frac{1}{n} = \delta(\mathcal{W}) = \delta(\mathcal{W}_{\mathfrak{m}}) \leq \delta(\mathcal{N}_{\mathfrak{m}} \cap \mathcal{P}(K)) = \frac{1}{h_{\mathfrak{m}}},$$

i.e.,

$$h_{\mathfrak{m}} \leq n, \quad \text{ou seja} \quad [\mathcal{I}_{\mathfrak{m}}(K) : \mathcal{N}_{\mathfrak{m}}(L/K)] \leq [L : K]. \tag{5.1}$$

A desigualdade acima é chamada *segunda desigualdade fundamental* da teoria de corpos de classes[1] e é valida para qualquer $\mathfrak{m}$ e para qualquer extensão galoisiana finita L de K.

[1] Observe que a primeira desigualdade fundamental ainda não foi mencionada.

5.5 A Definição de Corpo de Classes

Definição 28. Uma extensão galoisiana finita L/K de um corpo de números K é chamada de *corpo de classes* sobre K se, com a notação acima, $h_{\mathfrak{m}} = n$ para algum divisor $\mathfrak{m}$ de K.

Se L/K é um corpo de classes, existe um único divisor $\mathfrak{f} = \mathfrak{f}(L/K)$ tal que a igualdade $h_{\mathfrak{m}} = n$ vale para algum divisor se, e somente se, $\mathfrak{m}$ é um múltiplo de $\mathfrak{f}$. Tal divisor $\mathfrak{f}$ é chamado *condutor* de L/K.

Critério. *Se L/K é um corpo de classes, existe um divisor $\mathfrak{m}$ de K e um grupo de ideais H de K definido módulo $\mathfrak{m}$ tais que*

1. $N_{L/K}(\mathcal{I}_{\mathfrak{m}}(L)) \subset H$;
2. $H \cap \mathcal{P}(K)$ *está contido em* $\mathcal{W}$ *a menos de um conjunto de densidade nula.*

Reciprocamente, se existem tais $\mathfrak{m}$ e H, então L/K é um corpo de classes e $h_{\mathfrak{m}} = n$, $H = \mathcal{N}_{\mathfrak{m}}$.

Demonstração. Se L/K é um corpo de classes, tomemos $H = \mathcal{N}_{\mathfrak{m}}$ para $\mathfrak{m}$ um divisor de K tal que $h_{\mathfrak{m}} = n$. Então, 1 vale trivialmente. A condição 2 segue de $\mathcal{W}_{\mathfrak{m}} \subset (N_{L/K}(\mathcal{I}_{\mathfrak{m}}(L)) \cap \mathcal{P}(K)) \subset (\mathcal{N}_{\mathfrak{m}} \cap \mathcal{P}(K))$ e de $\delta(\mathcal{W}) = \delta(\mathcal{W}_{\mathfrak{m}}) = 1/n = 1/h_{\mathfrak{m}} = \delta(\mathcal{N}_{\mathfrak{m}} \cap \mathcal{P}(K))$.

Vejamos agora a recíproca: suponhamos que tais $\mathfrak{m}$ e H existam. Pela condição 1, temos $\mathcal{S}_{\mathfrak{m}}(K) \subset \mathcal{N}_{\mathfrak{m}} \subset H \subset \mathcal{I}_{\mathfrak{m}}(K)$. Definimos $a := [H : \mathcal{N}_{\mathfrak{m}}]$. Então, pelo teorema da progressão aritmética, $\delta(H \cap \mathcal{P}(K)) = a/h_{\mathfrak{m}}$. No entanto, a condição 2 nos diz que $\delta(H \cap \mathcal{P}(K)) \leq \delta(\mathcal{W}) = 1/n$. Desta forma, $a/h_{\mathfrak{m}} \leq 1/n$, ou seja, $an \leq h_{\mathfrak{m}}$. Pela segunda desigualdade fundamental da teoria de corpos de classes, temos que $a = 1$ e $h_{\mathfrak{m}} = n$.

□

Uma primeira aplicação deste critério é a seguinte proposição:

Proposição 21. *Sejam L_1/K, L_2/K corpos de classes. Então $L := L_1L_2$ (o menor corpo que contém L_1 e L_2) também é um corpo de classes.*

Demonstração. Seja $\mathfrak{m}$ um divisor de L tal que $\mathfrak{m}$ é divisível por $\mathfrak{f}_1 = \mathfrak{f}(L_1/K)$ e $\mathfrak{f}_2 = \mathfrak{f}(L_2/K)$. Provaremos que $\mathfrak{m}$ e $H = \mathcal{N}_{\mathfrak{m}}(L_1/K) \cap \mathcal{N}_{\mathfrak{m}}(L_2/K)$ satisfazem

as condições 1 e 2 do critério acima para a extensão L/K. De fato, como $N_{L/L_i}(\mathcal{I}_{\mathfrak{m}}(L)) \subset \mathcal{I}_{\mathfrak{m}}(L_i)$, para $i = 1, 2$, temos:

$$N_{L/K}(\mathcal{I}_{\mathfrak{m}}(L)) = N_{L_i/K}(N_{L/L_i}(\mathcal{I}_{\mathfrak{m}}(L))) \subset N_{L_i/K}(\mathcal{I}_{\mathfrak{m}}(L_i)) \subset \mathcal{N}_{\mathfrak{m}}(L_i/K),$$

para $i = 1, 2$. Isto implica que

$$N_{L/K}(\mathcal{I}_{\mathfrak{m}}(L)) \subset \mathcal{N}_{\mathfrak{m}}(L_1/K) \cap \mathcal{N}_{\mathfrak{m}}(L_2/K) = H,$$

e então, a condição 1 é satisfeita.

Para a condição 2, basta observarmos:

$$\begin{aligned}
&\delta(H \cap \mathcal{P}(K) - \mathcal{W}) \\
&\qquad = \delta(\mathcal{N}_{\mathfrak{m}}(L_1/K) \cap \mathcal{N}_{\mathfrak{m}}(L_2/K) \cap \mathcal{P}(K) - \mathcal{W}) \\
&\qquad = \delta((\mathcal{N}_{\mathfrak{m}}(L_1/K) \cap \mathcal{P}(K) - \mathcal{W}) \cap (\mathcal{N}_{\mathfrak{m}}(L_2/K) \cap \mathcal{P}(K) - \mathcal{W})) \\
&\qquad \leq \delta((\mathcal{N}_{\mathfrak{m}}(L_1/K) \cap \mathcal{P}(K) - \mathcal{W}) \cup (\mathcal{N}_{\mathfrak{m}}(L_2/K) \cap \mathcal{P}(K) - \mathcal{W})) \\
&\qquad \leq \delta(\mathcal{N}_{\mathfrak{m}}(L_1/K) \cap \mathcal{P}(K) - \mathcal{W}) + \delta(\mathcal{N}_{\mathfrak{m}}(L_2/K) \cap \mathcal{P}(K) - \mathcal{W}) \\
&\qquad = 0 + 0 = 0,
\end{aligned}$$

o que é suficiente para provar tal condição. □

Usando o critério, segue da demonstração acima, o seguinte corolário:

Corolário 5. *Se L_1/K e L_2/K são corpos de classes como na proposição 21, então para qualquer divisor $\mathfrak{m}$ de L, múltiplo de $\mathfrak{f}_1$ e $\mathfrak{f}_2$, temos $h_{\mathfrak{m}}(L/K) = [L : K]$, $\mathcal{N}_{\mathfrak{m}}(L/K) = \mathcal{N}_{\mathfrak{m}}(L_1/K) \cap \mathcal{N}_{\mathfrak{m}}(L_2/K)$. Ainda mais, $L_1 \supset L_2$ se, e somente se, $\mathcal{N}_{\mathfrak{m}}(L_1/K) \subset \mathcal{N}_{\mathfrak{m}}(L_2/K)$.*

Demonstração. A primeira parte é conseqüência imediata do critério. Para a segunda, basta observar que $\mathcal{N}_{\mathfrak{m}}(L_1) \subset \mathcal{N}_{\mathfrak{m}}(L_2)$ é equivalente a $\mathcal{N}_{\mathfrak{m}}(L/K) = \mathcal{N}_{\mathfrak{m}}(L_1/K)$, pela primeira parte, que também é equivalente a $h_{\mathfrak{m}}(L/K) = h_{\mathfrak{m}}(L_1/K)$, i.e., $[L : K] = [L_1 : K]$, ou seja $L = L_1$, ou $L_1 \supset L_2$. □

5.6 Teoremas Fundamentais

Vamos enunciar alguns teoremas fundamentais da teoria de corpos de classes que usaremos em seguida.

Teorema 14. *Uma extensão finita L de K é um corpo de classes sobre K se, e somente se, L/K é uma extensão abeliana (i.e., uma extensão galoisiana, com o grupo de Galois abeliano).*

O passo essencial da prova de tal teorema é provar que $n \leq h_{\mathfrak{m}}$ para algum divisor $\mathfrak{m}$ de K, onde L/K é uma extensão *cíclica*. Esta é chamada de *primeira desigualdade fundamental* da teoria de corpos de classes.

Teorema 15. *Dado um grupo de ideais H de K definido módulo $\mathfrak{m}$, existe um único corpo de classes sobre L tal que $[\mathcal{I}_{\mathfrak{m}}(K) : \mathcal{N}_{\mathfrak{m}}(L/K)] = [L : K]$ e $H = \mathcal{N}_{\mathfrak{m}}(L/K)$.*

Teorema 16. *Um ideal primo $\mathfrak{p}$ de K é ramificado em um corpo de classes L sobre K se, e somente se, $\mathfrak{p}$ divide o condutor $\mathfrak{f}(L/K)$.*

Antes de enunciarmos o próximo teorema, consideraremos algumas preliminares. Seja L/K uma extensão galoisiana arbitrária de grau n e com o grupo de Galois $G := \mathrm{Gal}(L/K)$. Seja $\mathfrak{p}$ um ideal primo de K não ramificado em L, e $\mathfrak{P}$ um ideal primo de L que divide $\mathfrak{p}$. Temos então que existe um único elemento $\sigma \in G$ tal que

$$\sigma(\alpha) \equiv \alpha^{N_{K/\mathbb{Q}}(\mathfrak{p})} \pmod{\mathfrak{P}}, \text{ para todo } \alpha \in \mathcal{O}_L. \tag{5.2}$$

Este elemento σ é chamado *substituição de Frobenius* de $\mathfrak{P}$ para a extensão L/K, e é denotado por $\sigma_{\mathfrak{P}}$. O grupo $D_{\mathfrak{P}}$ gerado por tal elemento é chamado *grupo de decomposição* do ideal primo $\mathfrak{P}$. Como vemos em [Gol71], pgs. 82 a 84, tal grupo tem a seguinte propriedade:

$$D_{\mathfrak{P}} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\};$$

além disso, como $\mathfrak{p}$ é não ramificado em L, a ordem de $D_{\mathfrak{P}}$ é $f(\mathfrak{P}/\mathfrak{p})$ e $D_{\sigma(\mathfrak{P})} = \sigma D_{\mathfrak{P}} \sigma^{-1}$, para qualquer $\sigma \in G$.

Vamos assumir agora que L/K é um corpo de classes (i.e., uma extensão abeliana) e

$$\mathfrak{p} = \mathfrak{P}_1 \ldots \mathfrak{P}_g$$

é a decomposição de $\mathfrak{p}$ em primos de L e, como $\mathfrak{p}$ é não ramificado, $\mathfrak{P}_i \neq \mathfrak{P}_j$ se $i \neq j$. Então, como o grupo de Galois de L/K age transitivamente sobre os primos sobre $\mathfrak{p}$, existe $\sigma \in G$ tal que $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$, para $i \neq j$, fixados. Logo $D_{\mathfrak{P}_j} = D_{\sigma(\mathfrak{P}_i)} = \sigma D_{\mathfrak{P}_i} \sigma^{-1} = D_{\mathfrak{P}_i}$, i.e., $\sigma_{\mathfrak{P}_i} = \sigma_{\mathfrak{P}_j}$, pela unicidade da

substituição de Frobenius. Assim, podemos denotar tal elemento do grupo de Galois simplesmente por $\sigma_{\mathfrak{p}}$.

Seja então $\mathfrak{m}$ um divisor de K tal que $h_{\mathfrak{m}} = n$, e seja $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{s_i}$ a decomposição em ideais primos em K de $\mathfrak{a} \in \mathcal{I}_{\mathfrak{m}}(K)$. Pelo teorema 16, cada $\mathfrak{p}_i$ é não ramificado e podemos definir $\sigma_{\mathfrak{p}_i}$ como acima. Logo, podemos definir também:

$$\sigma_{\mathfrak{a}} := \prod_{i=1}^{r} \sigma_{\mathfrak{p}_i}^{s_i}.$$

Temos claramente que $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}}$ é um homomorfismo de $\mathcal{I}_{\mathfrak{m}}(K)$ em G.

Teorema 17. *Seja L um corpo de classes sobre K e $\mathfrak{m}$ um divisor de K tal que $h_{\mathfrak{m}} = n$. O homomorfismo $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}}$ induz um isomorfismo entre $\mathcal{I}_{\mathfrak{m}}(K)/\mathcal{N}_{\mathfrak{m}}(L/K)$ e G, i.e., tal homomorfismo é sobrejetor e seu núcleo é $\mathcal{N}_{\mathfrak{m}}(L/K)$.*

Corolário 6. *Nas mesmas condições do teorema acima, ideais primos de K que pertencem à mesma classe de $\mathcal{I}_{\mathfrak{m}}(K)/\mathcal{N}_{\mathfrak{m}}(L/K)$ decompõem-se da mesma forma em L, i.e., em um mesmo número de fatores primos, com expoentes iguais a 1 (pois são não ramificados) e com os mesmos $f_{\mathfrak{p}}$'s. Em particular, todo elemento primo de $\mathcal{N}_{\mathfrak{m}}(L/K)$ decompõe-se completamente em L.*

Demonstração. Se $\mathfrak{p}$ e $\mathfrak{p}'$ pertencem à mesma classe de $\mathcal{I}_{\mathfrak{m}}(K)/\mathcal{N}_{\mathfrak{m}}(L/K)$, então são levados pelo homomorfismo em questão no mesmo $\sigma \in G$. Sejam:

$$\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_g, \quad \mathfrak{p}' = \mathfrak{P}_1' \dots \mathfrak{P}_{g'}'$$

as decomposições de $\mathfrak{p}$ e $\mathfrak{p}'$ em L. Como ambos são não ramificados em L, temos que $\mathfrak{P}_i \neq \mathfrak{P}_j$ se $i \neq j$, e analogamente, $\mathfrak{P}_i' \neq \mathfrak{P}_j'$. Além disso, $f = f(\mathfrak{P}_i/\mathfrak{p})$ (note que é independente de i) é a ordem de σ, e então, $f = f' = f(\mathfrak{P}_i'/\mathfrak{p}')$. Logo $n = fg = f'g' = fg'$, que implica que $g = g'$, e temos a primeira parte. Para a segunda, basta observarmos que

$$\mathcal{W}_{\mathfrak{m}} = \mathcal{W} \cap \mathcal{I}_{\mathfrak{m}}(K) \subset N_{L/K}(\mathcal{I}_{\mathfrak{m}}(L)) \subset \mathcal{N}_{\mathfrak{m}}(L/K),$$

e logo, como $\delta(\mathcal{W}_{\mathfrak{m}}) \neq 0$, segue que $\mathcal{W}_{\mathfrak{m}}$ é não vazio e existe um ideal em $\mathcal{N}_{\mathfrak{m}}(L/K)$ que se decompõe completamente; pela primeira parte, todos os ideais de $\mathcal{N}_{\mathfrak{m}}(L/K)$ decompõem-se completamente.

□

Observação. Este corolário dá-nos uma das mais impotantes propriedades dos corpos de classes.

Finalmente, seja L uma extensão galoisiana de K (não necessariamente um corpo de classes), e σ um elemento qualquer de $G = \mathrm{Gal}(L/K)$. Denotamos por $\mathcal{P}_\sigma$ o conjunto dos ideais primos $\mathfrak{p}$ de K não ramificados em L e tais que $\sigma = \sigma_{\mathfrak{P}}$, para algum ideal primo $\mathfrak{P}$ de L que divide $\mathfrak{p}$. Então:

Teorema 18. *Se c é o número de elementos na classe de conjugados de σ em G, então*

$$\delta(\mathcal{P}_\sigma) = \frac{c}{n}.$$

Observação. Se L/K é um corpo de classes, o teorema 18 pode ser facilmente deduzido do teorema 17 e do teorema da progressão aritmética, pois nesse caso, o tal número de conjugados é 1, pois L/K é abeliana e dado $\sigma \in G$, se $\mathfrak{k} \in \mathcal{I}_{\mathfrak{m}}(K)/\mathcal{N}_{\mathfrak{m}}(L/K)$ é a classe de ideais levada em σ pelo isomorfismo do teorema 17, então $\mathcal{P}_\sigma$ é a interseção de $\mathfrak{k}$ com o conjunto dos primos não ramificados de L, que difere de todos os primos de L por um número finito de ideais primos (os que dividem o discriminante de L/K). Logo

$$\delta(\mathcal{P}_\sigma) = \delta(\mathfrak{k} \cap \mathcal{P}(K)) = \frac{1}{[\mathcal{I}_{\mathfrak{m}}(K) : \mathcal{N}_{\mathfrak{m}}(L/K)]} = \frac{1}{n}.$$

5.7 O Corpo de Classes de Hilbert Absoluto

Denotemos por 1 o divisor unidade de K. Então, $\mathcal{I}_1(K) = \mathcal{I}(K)$ e $\mathcal{S}_1(K) = \mathcal{J}(K)$, lembrando que $\mathcal{J}(K)$ denota o sub-grupo de todos os ideais principais de K. Portanto, o quociente $\mathcal{I}_1(K)/\mathcal{S}_1(K)$ é igual ao grupo de classes de ideais de K, que denotamos por $\mathcal{C}(K)$ e supomos ter ordem h.

Pelo teorema 15, temos a existência de um corpo de classes L_0 sobre K tal que:

$$h = [\mathcal{I}(K) : \mathcal{J}(K)] = [L_0 : K], \quad \mathcal{J}(K) = \mathcal{N}_1(L_0/K).$$

Desta forma, o condutor $\mathfrak{f}(L_0/K) = 1$ e, pelo teorema 16, L_0/K é uma extensão não ramificada. Se tomamos L outra extensão abeliana e finita não ramificada de K, então L é um corpo de classes e novamente pelo teorema 16, temos que $\mathfrak{f}(L/K) = 1$. Logo, $\mathcal{N}_1(L/K)$ é um grupo de ideais definidos módulo 1; portanto, $\mathcal{S}_1(K) \subset \mathcal{N}_1(L/K)$, e como $\mathcal{J}(K) = \mathcal{S}_1(K) =$

$\mathcal{N}_1(L_0/K) \subset \mathcal{N}_1(L/K)$, $L \subset L_0$, pelo corolário 5. Então L_0 é a *única* extensão abeliana não ramificada maximal de K e é chamada de *corpo de classes de Hilbert absoluto* sobre K. Pelo teorema 17, o grupo de Galois de L_0/K é canonicamente isomorfo ao grupo de classes de ideais $\mathcal{C}(K)$ de K.

5.8 Conjugação dos Invariantes de Classes

Vamos assumir novamente que K é um corpo quadrático imaginário e

$$\mathcal{C}(K) = \{\mathfrak{k}_1, \ldots, \mathfrak{k}_h\}.$$

Os invariantes de classes $j(\mathfrak{k}_i)$, para $i \in \{1, \ldots, h\}$ são então inteiros algébricos dois a dois distintos. Seja L uma extensão galoisiana contendo tais $j(\mathfrak{k}_i)$'s e denotemos por $\xi_1, \ldots, \xi_s$ os elementos distintos em

$$\{\sigma(j(\mathfrak{k}_i)) : \sigma \in G = \mathrm{Gal}(L/K) \text{ e } i \in \{1, \ldots, h\}\}.$$

Definimos então,

$$\eta := \prod_{a<b}(\xi_a - \xi_b),$$

e denotemos por $\mathcal{P}^*$ o conjunto de todos os ideais primos de K de grau 1 que não ramificam em L e são primos com η. Como os ideais primos que não ramificam em L e os ideais primos que não são primos com η formam um conjunto finito, então $\delta(\mathcal{P}^*) = \delta(\mathcal{P}'(K)) = 1$. Desta forma, para qualquer conjunto $M \subset \mathcal{P}(K)$ com $\delta(M) > 0$, $\delta(M \cap \mathcal{P}^*) = \delta(M) > 0$, e então, a interseção de M com $\mathcal{P}^*$ é não vazia (e infinita).

Seja $\mathfrak{p}$ um ideal primo de $\mathcal{P}^*$ e $\mathfrak{k}_\mathfrak{p} \in \mathcal{C}(K)$ a classe de ideais que contém o ideal $\mathfrak{p}$. Seja p o inteiro primo tal que $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$. Pelo teorema 12 do capítulo 4, sabemos que

$$j(\mathfrak{k}_\mathfrak{p}^{-1}\mathfrak{k}) \equiv j(\mathfrak{k})^p \pmod{\mathfrak{p}},$$

para qualquer classe de ideais $\mathfrak{k}$. Por outro lado, se $\mathfrak{P}$ é um ideal primo de L dividindo $\mathfrak{p}$ e $\sigma_\mathfrak{P}$ é a substituição de Frobenius de $\mathfrak{P}$ para L/K, então, pela equação (5.2),

$$\sigma_\mathfrak{P}(j(\mathfrak{k})) \equiv j(\mathfrak{k})^p \pmod{\mathfrak{P}},$$

e segue que

$$\sigma_\mathfrak{P}(j(\mathfrak{k})) \equiv j(\mathfrak{k}_\mathfrak{p}^{-1}\mathfrak{k}) \pmod{\mathfrak{P}}.$$

No entanto, ambos os lados da congruência acima são elementos do conjunto $\{\xi_1, \ldots, \xi_s\}$, e $\mathfrak{p}$ é primo com η (e logo, $\mathfrak{P}$ também o é) implica então que

$$\sigma_{\mathfrak{P}}(j(\mathfrak{k})) = j(\mathfrak{k}_{\mathfrak{p}}^{-1}\mathfrak{k}).$$

Assim provamos a seguinte proposição:

Proposição 22. *Se $\mathfrak{p} \in \mathcal{P}^*$ e $\mathfrak{k}_{\mathfrak{p}}$ é a classe de ideais que contém $\mathfrak{p}$, então para qualquer $\mathfrak{k} \in \mathcal{C}(K)$ e qualquer $\mathfrak{P}$ ideal primo de L que divide $\mathfrak{p}$, a substituição de Frobenius de $\mathfrak{P}$ tem a seguinte propriedade:*

$$\sigma_{\mathfrak{P}}(j(\mathfrak{k})) = j(\mathfrak{k}_{\mathfrak{p}}^{-1}\mathfrak{k}).$$

Sejam agora $\mathfrak{k}$ e $\mathfrak{k}'$ duas classes de ideais quaisquer de $\mathcal{C}(K)$. Pelo teorema da progressão aritmética (pg. 79), $\delta(\mathfrak{k}(\mathfrak{k}')^{-1} \cap \mathcal{P}^*) = \delta(\mathfrak{k}(\mathfrak{k}')^{-1} \cap \mathcal{P}(K)) > 0$, i.e., a classe $\mathfrak{k}(\mathfrak{k}')^{-1}$ contém um ideal primo $\mathfrak{p}$ em $\mathcal{P}^*$, e então, $\mathfrak{k}' = \mathfrak{k}_{\mathfrak{p}}^{-1}\mathfrak{k}$. Segue da proposição 22 que os $j(\mathfrak{k})$ e $j(\mathfrak{k}')$ são conjugados em relação à extensão L/K. Por outro lado, dado qualquer $\sigma \in G$, pelo teorema 18, $\delta(\mathcal{P}_\sigma \cap \mathcal{P}^*) = \delta(\mathcal{P}_\sigma) > 0$, e assim existe $\mathfrak{p} \in \mathcal{P}^*$ tal que $\sigma = \sigma_{\mathfrak{P}}$ para algum $\mathfrak{P}$ ideal primo de L dividindo $\mathfrak{p}$. Novamente pela proposição 22, todo conjugado $\sigma(j(\mathfrak{k}))$ de um invariante de classes $j(\mathfrak{k})$ é um outro invariante de classes $j(\mathfrak{k}')$. Temos então:

Teorema 19. *Os invariantes de classes $j(\mathfrak{k}_i)$, $i = 1, \ldots, h$, de um corpo quadrático imaginário K formam um conjunto completo de conjugados sobre K.*

5.9 A Extensão $K(j(\mathfrak{k}))/K$

A partir de agora, consideraremos $L := K(j(\mathfrak{k}_1), \ldots, j(\mathfrak{k}_h))$, que, pelo teorema 19, é uma extensão galoisiana.

Lema 9. *Um ideal primo $\mathfrak{p} \in \mathcal{P}^*$ decompõe-se completamente em L se, e somente se, $\mathfrak{p} \in \mathcal{S}_1(K) = \mathcal{J}(K)$.*

Demonstração. Seja $\mathfrak{P}$ ideal primo de L que divide $\mathfrak{p}$. Como L/K é galoisiana e a ordem de $\sigma_{\mathfrak{P}}$ é $f = f(\mathfrak{P}/\mathfrak{p})$, $\mathfrak{p}$ decompõe-se completamente se, e somente se, $\sigma_{\mathfrak{P}} = 1$. Como $L = K(j(\mathfrak{k}_1), \ldots, j(\mathfrak{k}_h))$, segue da proposição 22 que $\sigma_{\mathfrak{P}} = 1$ se, e somente se, $j(\mathfrak{k}_{\mathfrak{p}}^{-1}\mathfrak{k}) = j(\mathfrak{k})$, i.e., $\mathfrak{k}_{\mathfrak{p}} = 1$, o que significa que $\mathfrak{p} \in \mathcal{J}(K)$.

□

Vamos agora verificar que as duas condições do critério dado na seção 5.5 são satisfeitas para $\mathfrak{m} = 1$ e $H = \mathcal{S}_1(K) = \mathcal{J}(K)$ e para a extensão L/K. Seja $\mathfrak{A}$ um ideal de L. Pelo teorema da progressão aritmética, existe um ideal primo $\mathfrak{P}$ de L de grau um (sobre $\mathbb{Q}$, e portanto, também sobre K) tal que $\mathfrak{A} = (\alpha)\mathfrak{P}$, pois se $\mathsf{k}_{\mathfrak{A}} \in \mathcal{C}(K)$ é classe que contém $\mathfrak{A}$, então $\delta(\mathsf{k}_{\mathfrak{A}} \cap \mathcal{P}'(L)) = \delta(\mathsf{k}_{\mathfrak{A}} \cap \mathcal{P}(L)) > 0$, e assim existe um $\mathfrak{P} \in \mathsf{k}_{\mathfrak{A}}$ como o procurado.

Ainda mais, como existem apenas finitos ideais primos de K que não são primos com η e são ramificados, e apenas finitos primos de L dividindo cada um destes primos de K, podemos assumir que $N_{L/K}(\mathfrak{P}) = \mathfrak{p}$ é primo com η e não ramificado. Logo $\mathfrak{p} \in \mathcal{P}^*$ (pois $\mathfrak{P}$ ter grau um implica que $\mathfrak{p}$ tem grau um) e decompõe-se completamente em L, pois L/K é galoisiana. Pelo lema 9, $\mathfrak{p} \in \mathcal{S}_1(K)$, e portanto, $N_{L/K}(\mathfrak{A}) = N_{L/K}(\alpha)\mathfrak{p} \in \mathcal{S}_1(K)$, e então $N_{L/K}(\mathcal{I}_1(L)) \subset \mathcal{S}_1(K)$, i.e., vale a condição 1 do critério. Como

$$\delta((\mathcal{S}_1(K) \cap \mathcal{P}(K)) \cap \mathcal{W}) = \delta(\mathcal{S}_1(K) \cap \mathcal{P}^*) = \delta(\mathcal{S}_1(K) \cap \mathcal{P}(K)),$$

também vale a condição 2 do critério.

Desta forma L/K é um corpo de classes e

$$h = [L : K], \quad \mathcal{S}_1(K) = \mathcal{N}_1(L/K).$$

Assim, pelos comentários da seção 5.7, L é o corpo de classes de Hilbert absoluto sobre K, i.e., a extensão abeliana não ramificada maximal de K.

Como agora sabemos que L/K é abeliana, para uma classe qualquer $\mathsf{k} \in \mathcal{C}(K)$, a extensão $K(j(\mathsf{k}))/K$ é normal. Por outro lado, dada outra classe k', existe $\sigma \in G$ tal que $\sigma(j(\mathsf{k})) = j(\mathsf{k}')$. Temos então que $j(\mathsf{k}')$ também é raiz do polinômio minimal de $j(\mathsf{k})$ (sobre K), e como $K(j(\mathsf{k}))/K$ é normal, $j(\mathsf{k}') \in K(j(\mathsf{k}))$. Desta forma, $K(j(\mathsf{k})) = L$. Portanto, provamos o seguinte teorema:

Teorema 20. *Seja $j(\mathsf{k})$ um invariante de classes qualquer de um corpo quadrático imaginário K. Então $K(j(\mathsf{k}))$ é a extensão abeliana não ramificada maximal de K.*

Como mencionamos na seção 5.7, temos um isomorfismo canônico entre $\mathcal{C}(K)$ e $G = \mathrm{Gal}(L/K)$. Seja então σ_{k} o elemento de G associado à classe de ideais k por tal isomorfismo. Se $\mathfrak{p}$ é um ideal primo de $\mathcal{P}^*$ pertencente à classe k, então $\sigma_{\mathsf{k}} = \sigma_{\mathfrak{p}}$ pela definição de tal isomorfismo. Então, a proposição 22 nos dá a seguinte fórmula explícita para o automorfismo σ_{k} de L/K:

$$\sigma_{\mathfrak{k}}(j(\mathfrak{k}')) = j(\mathfrak{k}^{-1}\mathfrak{k}'), \quad \mathfrak{k}, \mathfrak{k}' \in \mathcal{C}(K). \tag{5.3}$$

Seja agora τ um automorfismo de $\bar{\mathbb{Q}}$ (onde $\bar{\mathbb{Q}}$ é o corpo de todos os números algébricos) sobre $\mathbb{Q}$. Claramente $\tau(L)$ é a extensão abeliana não ramificada maximal de $\tau(K)$. Como K é um corpo quadrático imaginário, digamos $K = \mathbb{Q}(\sqrt{-D})$ com $D \in \mathbb{N}^*$ livre de quadrados, então $\tau(K) = \mathbb{Q}(\pm\sqrt{-D}) = K$. Logo $\tau(L)$ deve coincidir com L, pela unicidade do corpo de classes de Hilbert absoluto, e assim, L é uma extensão galoisiana de $\mathbb{Q}$. Sejam $\mathcal{G} := \mathrm{Gal}(L/\mathbb{Q})$ e ϱ o elemento de $\mathcal{G}$ que representa a conjugação complexa. Desta forma ϱ é o único automorfismo não trivial de K, i.e., $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \varrho\}$. Pela teoria de Galois, temos $\{1, \varrho\} = \mathcal{G}/G$. Seja $\mathfrak{a}$ um ideal de K na classe de ideais $\mathfrak{k}$. Então $\varrho(j(\mathfrak{k})) = \overline{j(\mathfrak{k})} = \overline{j(\mathfrak{a})}$. Como $\mathfrak{a}$ é um reticulado de $\mathbb{C}$, seja $\Gamma(\omega_1, \omega_2) = \mathfrak{a}$, com $\omega := \omega_1/\omega_2 \in \mathbb{H}$. Assim, $j(\mathfrak{a}) = j(\omega)$. Mas $\bar{\mathfrak{a}} = \overline{\Gamma(\omega_1, \omega_2)} = \Gamma(\bar{\omega}_1, \bar{\omega}_2) = \Gamma(-\bar{\omega}_1, \bar{\omega}_2)$, com $-\bar{\omega} \in \mathbb{H}$. Portanto $j(\bar{\mathfrak{a}}) = j(-\bar{\omega})$. Como $\exp(2\pi i(-\bar{\omega})) = \overline{\exp(2\pi i\omega)}$ e os coeficientes da q-expansão de j são inteiros, temos que $j(\bar{\mathfrak{a}}) = \overline{j(\mathfrak{a})}$, ou seja, $\varrho(j(\mathfrak{a})) = j(\bar{\mathfrak{a}})$. Como $\mathfrak{a}\bar{\mathfrak{a}} = N_{K/\mathbb{Q}}(\mathfrak{a})\mathcal{O}_K$ é um ideal principal, $\bar{\mathfrak{a}}$ está na classe $\mathfrak{k}^{-1}$, e logo,

$$\varrho(j(\mathfrak{k})) = j(\mathfrak{k}^{-1}). \tag{5.4}$$

Esta fórmula, juntamente com $\{1, \varrho\} = \mathcal{G}/G$ e o teorema 19 resultam no seguinte teorema:

Teorema 21. *Os invariantes de classes $j(\mathfrak{k}_i)$, $i = 1, \ldots, h$, de um corpo quadrático imaginário K formam um conjunto completo de conjugados sobre $\mathbb{Q}$.*

Dado $\sigma \in G$, pela proposição 22 e pelos comentários que a seguem, e mais o fato que L é um corpo de classes sobre K, sabemos que existe $\mathfrak{p} \in \mathcal{P}^*$ tal que $\sigma = \sigma_{\mathfrak{p}}$, e então $\sigma(j(\mathfrak{k})) = \sigma_{\mathfrak{p}}(j(\mathfrak{k})) = j(\mathfrak{k}_{\mathfrak{p}}^{-1}\mathfrak{k})$; assim σ permuta os $j(\mathfrak{k})$'s. Da mesma forma, como $\varrho(j(\mathfrak{k})) = j(\mathfrak{k}^{-1})$, ϱ também permuta os $j(\mathfrak{k})$'s, e conseqüentemente o mesmo fazem todos os elementos de $\mathcal{G}$. Desta forma, o polinômio $f(X) := \prod_{i=1}^{h}(X - j(\mathfrak{k}_i))$ é invariante pela ação de $\mathcal{G}$, resultando que tal polinômio é irredutível (e claramente mônico) e com coeficientes racionais. Mas como os $j(\mathfrak{k})$'s são inteiros algébricos, suas funções simétricas também o são, e logo, os coeficientes de tal polinômio estão em $\mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}$. Em suma, $f \in \mathbb{Z}[X]$ é mônico e irredutível.

Outra conseqüência da fórmula (5.4) é a seguinte: seja $\sigma \in G$ qualquer. Temos que existe $\mathsf{k} \in \mathcal{C}(K)$ tal que $\sigma = \sigma_{\mathsf{k}}$, e então, $\sigma^{-1} = \sigma_{\mathsf{k}^{-1}}$. Como G é normal em $\mathcal{G}$ (pois tem índice 2), $\varrho\sigma\varrho^{-1}$ também está em G, e segue das equações (5.3) e (5.4) que

$$(\varrho\sigma\varrho^{-1})(j(\mathsf{k}')) = (\varrho\sigma)(j((\mathsf{k}')^{-1})) = \varrho(j(\mathsf{k}^{-1}(\mathsf{k}')^{-1})) = j(\mathsf{k}\mathsf{k}') = \sigma^{-1}(j(\mathsf{k}')).$$

para qualquer invariante de classes $j(\mathsf{k}')$. Logo,

$$\varrho\sigma\varrho^{-1} = \sigma^{-1}, \quad \sigma \in G.$$

Uma conseqüência da fórmula acima é que a extensão $L/\mathbb{Q}$ é abeliana se, e somente se, todo $\tau \in \mathcal{G}$ é tal que $\tau^2 = 1$. Além disso, tal fórmula juntamente com o fato que $\{1, \varrho\} = \mathcal{G}/G$ mostra que a estrutura do grupo de Galois $\mathcal{G}$ é completamente determinada pela estrutura de $\mathcal{C}(K) \cong G$.

5.10 Alguns Exemplos

Vamos calcular o valor de j para alguns casos simples. Inicialmente, introduzimos a q-expansão de j com coeficientes calculados até ordem 6:

$$\begin{aligned} j(z) = 1/q + 744 + 196.884q + 21.493.760q^2 \\ + 864.299.970q^3 + 20.245.856.256q^4 \\ + 333.202.640.600q^5 + 4.252.023.300.096q^6 + \cdots . \end{aligned} \quad (5.5)$$

Tal expressão pode ser calculada usando-se as equações (1.16) e (1.32). Para $\mathrm{Im}(z) \geq \sqrt{3}/2$, ou seja, para $|q| \leq 0,04333\ldots$, pode-se mostrar que o truncamento acima (até q^6) é suficientemente preciso para o cálculo dos invariantes de classes em alguns casos simples ([Coh85], pg. 157).

Vamos aplicar tal aproximação aos casos em que o número de classes h é igual a um. Em tais casos, como $f(X) = \prod_{i=1}^{h}(X - j(\mathsf{k}_i))$ tem coeficientes inteiros (conseqüência já observada do teorema 21), temos que o único invariante de classes, que é dado por $j(\tau)$, onde[2] $\mathcal{O}_K = [1, \tau]$, deve ser inteiro.

Para aplicarmos a fórmula (5.5), observamos que um corpo quadrático imaginário K sempre pode ser escrito como $\mathbb{Q}(\sqrt{-D})$ com D livre de quadrados. Como vemos em [Gol71], pg. 12, se $-D \equiv 1 \pmod 4$, então $\mathcal{O}_K =$

[2]Denotaremos por $[\alpha_1, \alpha_2]$ o $\mathbb{Z}$-módulo livre gerado por α_1 e α_2.

K	$d_{K/\mathbb{Q}}$	$j(\mathsf{k})$	$erro$
$\mathbb{Q}(\sqrt{-3})$	-3	0	0
$\mathbb{Q}(\sqrt{-1})$	-4	12^3	0
$\mathbb{Q}(\sqrt{-7})$	-7	-15^3	10^{-11}
$\mathbb{Q}(\sqrt{-2})$	-8	20^3	10^{-13}
$\mathbb{Q}(\sqrt{-11})$	-11	-32^3	10^{-18}
$\mathbb{Q}(\sqrt{-19})$	-19	-96^3	10^{-30}
$\mathbb{Q}(\sqrt{-43})$	-43	-960^3	10^{-30}
$\mathbb{Q}(\sqrt{-67})$	-67	-5280^3	10^{-30}
$\mathbb{Q}(\sqrt{-163})$	-163	-640.320^3	10^{-30}

Tabela 5.1: Exemplos de Invariantes de Classes

$[1,(1+\sqrt{-D})/2]$ e o discriminante de K é dado por $d_{K/\mathbb{Q}} = -D$; se $-D \equiv 2,3 \pmod 4$, então $\mathcal{O}_K = [1,\sqrt{-D}]$ e $d_{K/\mathbb{Q}} = -4D$. Portanto, temos que aplicar a fórmula (5.5) para $z = (1+\sqrt{-D})/2$ se $K = \mathbb{Q}(\sqrt{-D})$ com $-D \equiv 1 \pmod 4$, e para $z = \sqrt{-D}$ nos demais casos.

Sabe-se que existem exatamente nove corpos quadráticos imaginários tais que $h = 1$ ([Coh85], pg. 183). Estes são dados pelos corpos K da tabela 5.1, onde também colocamos o respectivo discriminante $d_{K/\mathbb{Q}}$, o valor do único invariante de classes $j(\mathsf{k})$ e a ordem do erro feito pela aproximação dada pela fórmula (5.5)[3], exceto nos dois primeiros casos que são imediatos da definição de j (pois $g_2(\rho) = 0$ e $g_3(i) = 0$, como vimos na demonstração do teorema 4).

Um próximo caso seria quando K é tal que o número de classes é $h = 2$, por exemplo, para $K = \mathbb{Q}(\sqrt{-5})$ (onde $d_{K/\mathbb{Q}} = -20$). Neste caso, para a classe k_1 que contém $\mathcal{O}_K$, i.e., a unidade de $\mathcal{C}(K)$, usando a aproximação (5.5) temos

$$j(\mathsf{k}_1) = j(\sqrt{-5}) \approx 1.264.538,909475140509320227 0474.$$

Vamos achar agora um ideal $\mathfrak{a}$ tal que $\mathfrak{a} \notin \mathsf{k}_1$. Uma possível escolha é $\mathfrak{a} = [2, 1+\sqrt{-5}]$. De fato, um cálculo simples mostra que $\mathfrak{a}$ é um ideal de $\mathcal{O}_K$, e temos

$$\begin{aligned} j(\mathfrak{a}) &= j((1+\sqrt{-5})/2) \\ &\approx -538,909475120985766563618335 4. \end{aligned}$$

[3]Observamos que os cálculos foram feitos com precisão de 30 casas decimais.

Então, $j(\mathfrak{a}) \neq j(\mathfrak{k}_1)$, e assim, $\mathfrak{a} \notin \mathfrak{k}_1$, e portanto, $j(\mathfrak{a}) = j(\mathfrak{k}_2)$. Como $(X - j(\mathfrak{k}_1))(X - j(\mathfrak{k}_2))$ tem coeficientes inteiros, $j(\mathfrak{k}_1)\,j(\mathfrak{k}_2), j(\mathfrak{k}_1) + j(\mathfrak{k}_2) \in \mathbb{Z}$. Pelas nossas aproximações temos

$$j(\mathfrak{k}_1)\,j(\mathfrak{k}_2) = -681.472.000 = -880^3 \quad \text{e} \quad j(\mathfrak{k}_1) + j(\mathfrak{k}_2) = 1.264.000. \quad (5.6)$$

Para obtermos os valores exatos, basta resolvermos a equação

$$X^2 - 1.264.000\,X - 681.472.000 = 0.$$

Assim:

$$j(\mathfrak{k}_1) = 632.000 + 282.880\sqrt{5} = (50 + 26\sqrt{5})^3$$

e

$$j(\mathfrak{k}_2) = 632.000 - 282.880\sqrt{5} = (50 - 26\sqrt{5})^3,$$

e o erro de aproximação é da ordem inferior a 10^{-30} para a primeira e de ordem 10^{-8} para a segunda.

De maneira análoga, para o caso $K = \mathbb{Q}(\sqrt{-6})$ $(d_{K/\mathbb{Q}} = -24)$, onde também $h = 2$, temos

$$j(\mathfrak{k}_1) = 12^3(1 + \sqrt{2})^2(5 + 2\sqrt{2})^3 \quad \text{e} \quad j(\mathfrak{k}_2) = 12^3(1 - \sqrt{2})^2(5 - 2\sqrt{2})^3,$$

onde $\mathfrak{k}_1$ é a classe de ideais que contém $\mathcal{O}_K$ e $\mathfrak{k}_2$ é a classe de ideais remanescente, à qual o ideal $\mathfrak{a} = [2, \sqrt{-6}]$ pertence. Neste caso, os erros de aproximação são de ordens inferiores a 10^{-30} e igual a 10^{-10}, respectivamente.

Um outro caso em que $h = 2$ é $K = \mathbb{Q}(\sqrt{-15})$ $(d_{K/\mathbb{Q}} = -15)$. Neste caso $\mathfrak{a} = [2, (1 + \sqrt{-15})/2] \in \mathfrak{k}_2$,

$$j(\mathfrak{k}_1) = -135\sqrt{5}((3 + \sqrt{5})/2)(4 + \sqrt{5})^3$$

e

$$j(\mathfrak{k}_2) = 135\sqrt{5}((3 - \sqrt{5})/2)(4 - \sqrt{5})^3,$$

com erros de aproximação de ordens 10^{-24} e 10^{-5}, respectivamente.

Índice de Notações

$a := b$	a é definido como b
$a \mid b$	a divide b
$\mathbb{N}$	conjunto dos números naturais
$\mathbb{Z}$	conjunto dos números inteiros
$\mathbb{R}$	conjunto dos números reais
$\mathbb{C}$	conjunto dos números complexos
K^*	conjunto $K - \{0\}$
K, L	corpos de números
L/K	L é uma extensão de K
KL	menor corpo que contém os corpos K e L
$\bar{K}$	fecho algébrico de K
$\mathcal{O}_K$	inteiros algébricos de K
$d_{L/K}$	discriminante da extensão L/K
k	classe de ideais
$\mathcal{C}(K)$	grupo de classes ideais do corpo K
$\mathcal{I}(K)$	grupo dos ideais fracionários de K
$\mathcal{J}(K)$	sub-grupo dos ideais fracionários principais de K
K^{ab}	maior extensão abeliana do corpo K
$\mathbb{H}$	semi-plano complexo superior
$\mathbb{P}^1$	esfera de Riemann

$\mathbf{G}$	grupo modular
D	domínio fundamental
q	$e^{2\pi iz}$
$\tilde{f}$	$f(z)$ como função de q
Γ	reticulado de $\mathbb{C}$
$\Gamma(\omega_1, \omega_2)$	reticulado gerado por ω_1 e ω_2
$\mathcal{R}$	conjunto dos reticulados de $\mathbb{C}$
G_k	série de Eisenstein de índice k
g_2	$60\,G_2$
g_3	$140\,G_3$
Δ	$g_2^3 - 27g_3^2$
$v_p(f)$	ordem da função f no ponto p
M_{2k}	espaço vetorial das formas modulares de peso $2k$
M_{2k}^0	espaço vetorial das formas parabólicas de peso $2k$
j	invariante modular $(1728\,g_2^3/\Delta)$
B_k	números de Bernoulli
$\sigma_k(n)$	soma das k-ésimas potências dos divisores de n
(n, m)	máximo divisor comum de n e m
$\wp(z;\Gamma)$	função $\wp$ de Weirstrass
E	curva elíptica
j_E	invariante modular da curva elíptica E
$A(E)$	sub-anel de $\mathbb{C}$ associado aos endomorfismos de E
$\mathfrak{a}, \mathfrak{b}, \mathfrak{A}$	ideais fracionários
$\mathfrak{p}, \mathfrak{P}$	ideais primos
(ξ)	ideal principal gerado por ξ
h	ordem do grupo de classes de ideais

$j(\mathfrak{k})$	invariante de classes
ζ	raiz da unidade
ζ_n	raiz n-ézima primitiva da unidade
$\zeta(s)$	função zeta de Riemann
$\zeta_K(s)$	função zeta de Riemann para o corpo K
H_n^*	sub-conjunto de $\mathbf{G}$ que pode ser representado por uma matriz inteira de determinante n
H_n	sub-conjunto de H_n^* que pode ser representado por uma matriz inteira de determinante n e com entradas primas entre si
$\psi(n)$	$[H_n : \mathbf{G}]$
φ	função φ de Euler
N	$\psi(n)$
j_s	$j \circ M_s$, onde M_s é um representante de classe de $H_n/\mathbf{G}$
$F_n(t,j)$	$\prod_{s=1}^{N}(t - j_s)$
$f(\mathfrak{P}/\mathfrak{p})$	$[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$, onde L é uma extensão de K, $\mathfrak{P}$ e $\mathfrak{p}$ são primos de L e K, respectivamente, e $\mathfrak{P}\|\mathfrak{p}$
$e(\mathfrak{P}/\mathfrak{p})$	expoente de $\mathfrak{P}$ na decomposição de $\mathfrak{p}$ em primos
$\mathfrak{m}$	divisor de um corpo K
$\mathfrak{m}_0$	parte finita de $\mathfrak{m}$
$\mathfrak{m}_\infty$	parte infinita de $\mathfrak{m}$
$\mathcal{I}_\mathfrak{m}(K)$	grupo dos ideais de K primos com $\mathfrak{m}_0$
$\mathcal{S}_\mathfrak{m}(K)$	sub-grupo de $\mathcal{I}_\mathfrak{m}(K)$ dos ideais principais congruentes a 1 módulo $\mathfrak{m}$
$\mathcal{P}(K)$	conjunto dos ideais primos de K
$\mathcal{P}'(K)$	conjunto dos ideais primos de K de grau um
$\mathcal{P}''(K)$	complementar de $\mathcal{P}'(K)$ em $\mathcal{P}(K)$

$\mathcal{P}'''(L)$	ideais primos de L de grau um e tais que a restrição a K é não ramificada em L
$\mathcal{W}$	conjunto dos ideais primos de K que se decompõem completamente em L
$\delta(M)$	densidade de Dirichlet de $M \subset \mathcal{P}(K)$
$f(s) \sim g(s)$	$f(s) - g(s)$ é limitado em $s = 1$
$\mathcal{N}_{\mathfrak{m}}$	$\mathcal{S}_{\mathfrak{m}}(K)\, N_{L/K}(\mathcal{I}_{\mathfrak{m}}(L))$
$h_{\mathfrak{m}}$	$[\mathcal{I}_{\mathfrak{m}}(K) : \mathcal{N}_{\mathfrak{m}}]$
$\mathfrak{f}(L/K)$	condutor de L/K
$\sigma_{\mathfrak{P}}$	substituição de Frobenius de $\mathfrak{P}$
$D_{\mathfrak{P}}$	grupo de decomposição de $\mathfrak{P}$
$\mathcal{P}_{\sigma}(K)$	ideais primos $\mathfrak{p}$ de K não ramificados em L, com $\sigma = \sigma_{\mathfrak{P}}$ para algum ideal $\mathfrak{P}$ de L sobre $\mathfrak{p}$
ϱ	conjugação complexa

Índice Remissivo

Bibliografia

[Ahl66] Lars V. Ahlfors. *Complex Analysis*. McGraw-Hill Book Company, second edition, 1966.

[BCH+66] A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, and J-P. Serre. *Seminar on Complex Multiplication*, volume 21 of *Lecture Notes in Mathematics*. Springer-Verlag, 1966.

[Coh85] Harvey Cohn. *Introduction to the Construction of Class Fields*, volume 6 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1985.

[For81] Otto Forster. *Lectures on Riemann Surfaces*, volume 81 of *Graduate Texts in Mathematics*. Springer-Verlag, 1981.

[Gol71] Larry Joel Goldstein. *Analytic Number Theory*. Prentice-Hall, Inc., 1971.

[Has26] H. Hasse. Klassenkörper bericht. *Jahr. Ber. D.M.V.*, 35:1–55, 1926.

[Lan86] Serge Lang. *Elliptic Functions*, volume 112 of *Garduate Texts in Mathematics*. Springer-Verlag, second edition, 1986.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Spinger-Verlag, 1973.

[Sil85] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1985.

[Ste79] Ian Stewart. *Algebraic Number Theory*. Chapman and Hall Ltd, 1979.