Universidade Estadual de Campinas

Instituto de Matemática, Estatística
e Computação Científica
Departamento de Matemática

Formas Modulares Aplicadas à Teoria dos Números

Autor: Eduardo Luis Estrada[1]

Mestrado em Matemática

Orientador: Prof. Dr. José Plínio O. Santos

Co-orientadora: Profa. Dra. Sueli I. R. Costa

[1]Este trabalho contou com o apoio financeiro da CAPES.

Formas Modulares Aplicadas à Teoria dos Números

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por **Eduardo Luis Estrada**, e aprovada pela comissão julgadora.

Campinas, 7 de março de 2006

Prof. Dr. José Plínio O. Santos
Orientador

Profa. Dra. Sueli I. R. Costa
Co-orientadora

Banca examinadora:
1) Prof. Dr. José Plínio de Oliveira Santos;
2) Prof. Dr. Marcelo Firer;
3) Prof. Dr. Marcelo Muniz Silva Alves.

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da UNICAMP como requisito parcial para obtenção do título de **Mestre em Matemática**.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecário: Miriam Cristina Alves – CRB8a / 5094

Estrada, Eduardo Luis

Es88f Formas modulares aplicadas à teoria dos números / Eduardo Luis Estrada -- Campinas, [S.P. :s.n.], 2006.

Orientador : José Plínio de Oliveira Santos

Co-orientadora: Sueli Irene Rodrigues Costa

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Formas modulares. 2. Teoria dos números. 3. Funções modulares. I. Santos, José Plínio de Oliveira. II. Costa, Sueli Irene Rodrigues. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Título em inglês: Modular forms applied in number theory

Palavras-chave em inglês (Keywords): 1. Modular forms. 2. Number theory. 3. Modular functions.

Área de concentração: Análise matemática

Titulação: Mestre em Matemática

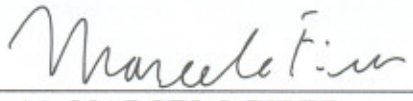
Banca examinadora: Prof. Dr. José Plínio de Oliveira Santos (IMECC-UNICAMP)
Prof. Dr. Marcelo Firer (IMECC-UNICAMP)
Prof. Dr. Marcelo Muniz Silva Alves (CM-UFPR)

Data da defesa: 07/03/2006

Dissertação de Mestrado defendida em 07 de março de 2006 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof. (a). Dr (a). JOSÉ PLINIO DE OLIVEIRA SANTOS



Prof. (a). Dr (a). MARCELO FIRER

Prof. (a). Dr (a). MARCELO MUNIZ SILVA ALVES

Agradecimentos

Primeiramente, um agradecimento ao Departamento de Matemática da Unicamp, extensivo a toda a universidade, pela infra-estrutura fornecida durante cada etapa do mestrado, e também à Capes, por seu apoio finaceiro. Explicitamente, um agradecimento à Secretaria de Pós-graduação do Instituto de Matemática.

Agradeço a todos aqueles que colaboraram, direta ou indiretamente, com a realização do meu mestrado, tanto na parte inicial, relativa às disciplinas cursadas, como na parte derradeira, referente à elaboração desta dissertação. De modo particularmente especial, agradeço ao meu orientador, o Prof. Dr. José Plínio O. Santos, que foi responsável por me oferecer apoio técnico e motivacional para que eu pudesse concluir as tarefas advindas da pós-graduação. Agradeço também à minha co-orientadora, a Profa. Dra. Sueli I. R. Costa, e aos outros componentes da banca examinadora da dissertação, os Profs. Drs. Marcelo Firer e Marcelo Muniz S. Alves, pelas sugestões e apontamentos relativos ao trabalho final. No tocante específico a este trabalho, registro gratidão também ao Prof. Dr. Paulo Mondek e ao mestrando em matemática Robson da Silva.

Resumo

Abordamos, de maneira elementar, as estruturas algébrica e topológica sobre a qual são construídas as formas modulares, objetos principais do nosso estudo. Após a definição de formas modulares, realizamos um estudo particular sobre duas funções específicas relacionadas à teoria dos números: $\eta(\tau)$ e $\vartheta(\tau)$. Trata-se de um texto introdutório, no qual apresentamos diversos conceitos e resultados extremamente importantes da teoria, tais como as demonstrações de que as duas funções supracitadas são formas modulares e a apresentação de uma fórmula explícita para seus sistemas multiplicadores.

Abstract

In an elemmentary way, we have dealt with the algebraic and topological structures in which the modular forms are constructed. After the definition of this important tool, we have made a particular study about two specific functions related to number theory: $\eta(\tau)$ and $\vartheta(\tau)$. It is an introductory text, in which we have presented many concepts and results extremely importants of the theory, such as the proofs of the fact that the functions $\eta(\tau)$ and $\vartheta(\tau)$ are modular forms and the presentation of exact formulas for their multiplier systems.

Introdução

O tema *Formas modulares* é bastante amplo e vem ganhando cada vez mais aplicações, dentre as quais à teoria dos números. Neste trabalho, todavia, essas aplicações não serão discutidas, reservando-se-as ao leitor que deseje aprofundar-se no assunto. Assim, procuramos apresentar um material que possa fornecer o arcabouço teórico necessário à compreensão dessas aplicações. Embora o entendimento deste trabalho exija, como evidencia o Capítulo 1, noções dos mais variados campos da matemática, dentre as quais conceitos topológicos, variáveis complexas, teoria dos números e teoria de grupos, assumimos que o leitor não tenha nenhum conhecimento prévio acerca de formas modulares.

O Capítulo 1, então, destina-se a revisar alguns assuntos importantes para o entendimento do texto, bem como a apresentar alguns teoremas e definições que não possuem uma única versão na literatura, a fim de adequá-los aos nossos objetivos. Exemplos disso são o *Teorema da identidade de funções analíticas*, o *Princípio do módulo máximo* e a fórmula do resto na *Série de Taylor*. Também neste capítulo apresentamos resultados cujos enunciados são facilmente compreensíveis, mas cujas demonstrações fugiriam aos nossos propósitos, tais como a expansão de uma função complexa em *Série de Laurent*, a *Fórmula de transformação theta* e a *Lei da reciprocidade quadrática*. Dedicamos, ainda, uma seção à teoria de *Produtos infinitos*, tema de difícil obtenção na literatura.

Os dois capítulos seguintes são interdependentes, pois que, enquanto o Capítulo 2 tem por objetivo o estudo da estrutura sobre a qual se constrói uma forma modular, o Capítulo 3 as constrói dentro de tal estrutura. Assim, no Capítulo 2, definimos o *Grupo modular* $\Gamma(1)$, para o qual exibimos um conjunto gerador bastante simples, e trabalhamos com alguns de seus subgrupos, dentre os quais Γ_ϑ, obtendo decomposições daquele em classes de equivalência destes. Embora já tenha sido dito no texto, enfatizamos que os subgrupos com que trabalhamos neste capítulo e nos demais possuem índice finito no grupo modular. Topologicamente, as formas modulares apresentam, como domínio, o

semiplano complexo superior estendido $\mathscr{H}$, de sorte que, para completar a estrutura algébrica necessária às formas modulares, definimos, entre os elementos de $\mathscr{H}$, uma relação de equivalência segundo o subgrupo de $\Gamma(1)$ considerado. Desse modo, definimos o importante conceito de *Região fundamental* segundo subgrupos, aproveitando para exibir a região fundamental $\mathscr{R}(\Gamma(1))$ segundo $\Gamma(1)$, que é utilizada ao longo do texto. Além disso, mediante decomposições do grupo modular em classes laterais, também definimos regiões fundamentais padronizadas. O Capítulo 3 não começa com a definição de forma modular, pois, além da estrutura exposta no capítulo anterior, são necessários mais alguns conceitos para que se as definam, tais como o de *Ponto parabólico* e algumas grandezas a ele associadas, o de *Grau* de uma forma modular e o de *Sistema multiplicador* associado a uma forma modular. Apresentamos também o Teorema 5, parte essencial da teoria, com demonstração tão detalhada quanto possível, para, finalmente, definir uma *Forma modular* e alguns casos particulares, tais como forma cúspide e função modular. A maioria dos estudos sobre formas modulares trata, segundo nossas definições, de casos específicos de formas modulares, como formas de grau par ou funções modulares. Desse modo, o estudo aqui apresentado é bastante geral, tendo [11] como referência básica. Com isso, por um lado, ganhamos por obter resultados mais gerais, porém os cálculos envolvidos se tornam mais trabalhosos, fazendo com que a teoria ganhe uma dimensão bastante analítica. Após apresentar a definição de forma modular, com objetivo de entender como as definições funcionam na prática, provamos alguns resultados que têm parentesco com resultados da teoria de variáveis complexas, como o Teorema de Liouville, dentre os quais os fatos de que *toda função modular inteira é constante* e *toda forma cúspide de grau positivo é identicamente nula.*

Se o objetivo do leitor é apenas entender o que são formas modulares, a leitura não deve prosseguir. Todavia, se o leitor acredita que, sem exemplos, não se entende uma teoria, ou quer ter uma noção de como as formas modulares podem ter relação com a teoria dos números, então os dois últimos capítulos podem ser bastante interessantes. Basicamente, o Capítulo 4 se presta à exibição de duas funções específicas, $\eta(\tau)$ e $\vartheta(\tau)$, que são formas modulares segundo $\Gamma(1)$ e Γ_ϑ, respectivamente, e se relacionam à teoria dos números. Enquanto a primeira possui relação com a função $p(n)$, que associa a cada inteiro não negativo n o número de partições desse inteiro, a segunda possui relação com $r_s(m)$, função que associa a cada inteiro positivo m o número de maneiras de se escrevê-lo como soma de exatamente s quadrados. Na verdade, essas relações são facilmente

verificáveis, de modo que este capítulo se dedica às demonstrações de que as duas funções exibidas são, de fato, formas modulares. Para tanto, será necessário apresentar diversos resultados auxiliares, como a fórmula do *Produto triplo de Jacobi*. Finalizando, o Capítulo 5 trata dos sistemas multiplicadores υ_η e υ_ϑ, associados às formas modulares tratadas no capítulo anterior. Neste capítulo, exibimos fórmulas explícitas para o cálculo dessas funções, cujos parâmetros são os coeficientes das matrizes dos subgrupos considerados. Para se provar tais fórmulas, embora os cálculos envolvidos sejam elementares, utilizando-se muito congruência entre inteiros e propriedades do símbolo de Legendre/Jacobi, eles são bastante trabalhosos.

Sumário

Capítulo 1

Pré-requisitos

1.1 Análise

1.1.1 Variáveis complexas

Transformações lineares fracionárias

Denominamos transformações lineares fracionárias as funções complexas

$$\begin{aligned} V : \mathbb{C} &\to \mathbb{C} \\ \tau &\mapsto \frac{a\tau + b}{c\tau + d}, \end{aligned}$$

sendo $a, b, c, d \in \mathbb{C}$, com $ad - bc \neq 0$. Essas transformações também são chamadas *transformações de Möbius*.

Se V, como acima, é uma transformação de Möbius, então é claro que

$$\begin{aligned} V^{-1} : \mathbb{C} &\to \mathbb{C} \\ \tau &\mapsto \frac{d\tau - b}{-c\tau + a} \end{aligned}$$

é também uma transformação de Möbius. Além disso, $V \circ V^{-1} = V^{-1} \circ V = I$, sendo I a aplicação identidade, que é também transformação linear fracionária. Logo, V^{-1} é a aplicação inversa de V, donde V é uma bijeção. Além disso, V é contínua, com inversa também contínua, ou seja, V é um homeomorfismo. Para que o que dissemos acima seja verdade, é importante ressaltar que o plano complexo ora considerado é o estendido, ou seja, o conjunto dos pontos finitos unido ao ponto ∞. Por isso, também definimos $V(\infty) = \frac{a}{c}$ e $V\left(\frac{-d}{c}\right) = \infty$ (note que não podemos ter $a = 0 = c$ nem $d = 0 = c$, pois

isso contradiz a hipótese de que $ad - bc \neq 0$, de modo que os quocientes a/c e $-d/c$ são sempre bem definidos considerando-se, ainda, $1/0 = \infty$).

Funções analíticas

Seja $f : U \to \mathbb{C}$ uma função complexa, para $U \subset \mathbb{C}$. Dizemos que f é *diferenciável* em $z_0 \in U$ se existe o seguinte limite

$$\lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0}.$$

Neste caso, tal limite é dito derivada ou diferencial de f em z_0, e denotado $f'(z_0)$. Quando f é diferenciável em cada $z_0 \in U$, dizemos que f é diferenciável em U.

Quando, além de f ser diferenciável em z_0, pudermos obter uma vizinhança de z_0 em cujos pontos f é diferenciável, diremos que f é *analítica* em z_0. Finalmente, se f é analítica em todos os pontos do domínio U, diremos que f é analítica em U. Muitas vezes, os termos função *regular* e função *holomorfa* são utilizados em lugar de função analítica. Se uma função é analítica em todo o plano complexo $\mathbb{C}$, dizemos que tal função é *inteira*.

Na seqüência, um importante teorema, que será bastante utilizado no Capítulo 4:

Teorema 1 (Teorema da Identidade de Funções Analíticas). *Suponha que $f(x)$ e $g(x)$ sejam duas funções analíticas nos domínios D_1 e D_2, respectivamente. Se $D = D_1 \cap D_2$ e existe uma seqüência de pontos distintos $(x_k)_{k=1}^{\infty} \subset D$, tendo pelo menos um limite em D, e tal que, para cada inteiro positivo k, $f(x_k) = g(x_k)$, então $f(x) = g(x)$ em D.*

Apresentamos mais um resultado relacionado à funções analíticas, ora apresentado de uma maneira bastante geral:

Teorema 2 (Princípio do Módulo Máximo).

1. *Se $f(z)$ é analítica em um domínio D, então $|f(z)|$ não pode assumir seu valor máximo em D, a menos que $f(z)$ seja constante;*

2. *Se $f(z)$ é analítica em um domínio limitado D e $|f(z)|$ é contínua em $\overline{D}$ (fecho de D), então $|f(z)|$ assume seu valor máximo em ∂D (fronteira de D).*

1.1.2 Série de Laurent

Se uma função é analítica em todo um domínio simplesmente conexo D, uma das maneiras mais eficientes de se representá-la como série de potências em torno de um ponto de D consiste no emprego das chamadas séries de Taylor. Todavia, nem sempre o domínio em que se aplica a função obedece àquela propriedade topológica. Por exemplo, podemos desejar representar uma dada função num anel, ou numa região da qual se exclui um ou mais pontos isolados. Nestes casos, uma das expansões para as quais se encontra utilidade são as chamadas séries de Laurent, expressas no seguinte teorema:

Teorema 3. *Se $f(z)$ é analítica no anel*

$$0 \leq R_1 < |z-a| < R_2 \leq \infty,$$

então

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z-a)^n, \quad a_n = \frac{1}{2\pi i} \int_C \frac{f(t)}{(t-a)^{n+1}} \mathrm{d}t,$$

onde $C = \{t \in \mathbb{C} \mid |t-a| = r, R_1 < r < R_2\}$, e a série é absolutamente convergente no anel. Ademais, se $f(z)$ é analítica no interior do círculo de raio R_2 e sobre ele, excetuando-se apenas o centro a, podemos tomar R_1 arbitrariamente pequeno, de tal maneira que o desenvolvimento anterior se torna válido para $0 < |z-a| < R_2$.

No caso previsto ao final do enunciado desse teorema, dizemos que a é uma singularidade *isolada* de $f(z)$, e podemos submetê-la à seguinte classificação:

Pólo Se existe $m > 0$ tal que $a_{-m} \neq 0$ e $a_{-n} = 0$ para cada $n > m$, dizemos que a é um pólo de ordem m de $f(z)$ na região considerada. Por exemplo, $f(z) = 1/(z-1)^2$, definida em $\mathbb{C}$, possui um pólo de ordem 2 em $z = 1$;

Singularidade essencial Contrariamente à definição anterior, se existem infinitos termos a_{-n} não nulos, para $n > 0$, dizemos que a é uma singularidade essencial de $f(z)$ na região considerada. Por exemplo, $f(z) = e^{1/z}$, definida em $\mathbb{C}$, apresenta uma singularidade essencial em $z = 0$;

Singularidade removível Ocorre quando há uma singularidade que pode ser removida. Por exemplo, $f(z) = z^2/z$, definida em $\mathbb{C}$, possui uma singularidade removível em $z = 0$.

Dizemos, ainda, que uma função é *meromorfa* num certo domínio se ela não possui, nesse domínio, singularidades que não pólos.

1.1.3 Produtos infinitos

No que vamos estudar, particularmente no Capítulo 4, serão comuns produtos e somas infinitos. Quanto a somas infinitas, denominadas *séries*, não faremos aqui nenhuma revisão, pois julgamos ser um assunto mais familiar dentro da matemática e, ademais, de fácil obtenção de fontes. De qualquer modo, indicamos a referência bibliográfica [16] para os interessados.

O desenvolvimento que aqui faremos sobre o assunto desta subseção pode ser encontrado com mais detalhes em [10]. Dada uma seqüência de números reais $(u_n)_{n=1}^{\infty}$, denotamos o produto infinito de seus termos por

$$U = \prod_{n=1}^{\infty} u_n. \tag{1.1}$$

Dizemos que uma série é convergente se, e somente se, suas somas parciais convergem para um número finito. Seria razoável, então, adotar essa mesma definição envolvendo produtos infinitos e parciais. Entretanto, isso seria inadequado, de modo que temos a seguinte definição:

Definição 1. *O produto infinito U exibido em (1.1) será dito* convergente *se existir um inteiro positivo m tal que, para cada $n > m$, $u_n \neq 0$, e os produtos parciais $p_n = u_{m+1} \cdot u_{m+2} \cdots u_n$ convirjam para um número finito e diferente de zero. Neste caso, denotando-se $\lim_{n\to\infty} p_n = U_m$, temos que $U = u_1 \cdot u_2 \cdots u_m \cdot U_m$.*

Não é difícil ver, com base na definição anterior, que, embora o valor U seja exibido em termos de m, ele não depende deste inteiro. Além disso, é conseqüência imediata da definição o seguinte

Teorema 4. *Em (1.1), $U = 0$ se, e somente se, existe $n \geq 1$ tal que $u_n = 0$.*

Basicamente, isto é decorrência do fato de que $U_m \neq 0$. O teorema e a definição anteriores nos garantem, por exemplo, que, se tomarmos $u_n = \frac{1}{n}$ em (1.1), temos que U *diverge* para 0. Outro resultado que exibimos é o seguinte

Teorema 5. *Se, em (1.1), U é convergente, então $u_n \to 1$ à medida que $n \to \infty$.*

A partir deste teorema, introduzindo a notação $u_n = 1 + a_n$, para cada $n \geq 1$, temos que

$$U = \prod_{n=1}^{\infty}(1 + a_n),$$

donde $a_n \to 0$ conforme $n \to \infty$ é condição necessária à convergência de U, e temos o seguinte fato, cuja demonstração omitiremos:

Teorema 6. *Um produto infinito da forma* $\prod_{n=1}^{\infty}(1+a_n)$ *ou* $\prod_{n=1}^{\infty}(1-a_n)$*, com* $a_n \geq 0$ *para todo* n*, é convergente se, e somente se, a série* $\sum_{n=1}^{\infty} a_n$ *é convergente.*

Finalizamos com uma definição e dois teoremas que, em conjunto, serão bastante utilizados em situações posteriores. Não são resultados de difícil demonstração, valendo inclusive para números complexos nos lugares dos termos u_n e a_n, seguindo a notação anterior.

Definição 2. *O produto infinito* $\prod_{n=1}^{\infty}(1+a_n)$ *é dito* absolutamente convergente *se o produto* $\prod_{n=1}^{\infty}(1+|a_n|)$*, com termos não negativos* $|a_n|$*, é convergente.*

Teorema 7. *A convergência de* $\prod_{n=1}^{\infty}(1+|a_n|)$ *implica na convergência de* $\prod_{n=1}^{\infty}(1+a_n)$.

Teorema 8. *O produto* $\prod_{n=1}^{\infty}(1+a_n)$ *é absolutamente convergente se, e somente se,* $\sum_{n=1}^{\infty} a_n$ *é absolutamente convergente.*

1.1.4 Série de Taylor

Suponha que $f(x)$ seja uma função real de uma variável real, continuamente diferenciável até a n-ésima ordem, para $x \in [a, a+h]$. Se $0 \leq t \leq 1$, então $f(a+h)$ é expresso por

$$f(a+h) = f(a) + \frac{f'(a)h}{1!} + \cdots + \frac{f^{(n-1)}(a)h^{n-1}}{(n-1)!} + \underbrace{\frac{h^n}{(n-1)!}\int_0^1 (1-t)^{n-1} f^{(n)}(a+th)dt}_{R_n}.$$

A expressão acima é denominada *expansão de Taylor de* $f(x)$ *em* $x = a$*, com resto integral* R_n. Como $f^{(n)}(a+th)$ é contínua para $0 \leq t \leq 1$, o Teorema do Valor Intermediário implica que existe $\theta \in [0,1]$ tal que

$$\int_0^1 (1-t)^{n-1} f^{(n)}(a+th)dt = f^{(n)}(a+\theta h)\int_0^1 (1-t)^{n-1}dt = \frac{1}{n}f^{(n)}(a+\theta h).$$

Logo, segue que

$$R_n = \frac{h^n}{(n-1)!}\cdot\frac{1}{n}f^{(n)}(a+\theta h) = \frac{h^n}{n!}f^{(n)}(a+\theta h),$$

que é a denominada *forma de Lagrange do resto* R_n. Finalmente, podemos escrever

$$f(a+h) = f(a) + \frac{f'(a)h}{1!} + \cdots + \frac{f^{(n-1)}(a)h^{n-1}}{(n-1)!} + \frac{h^n}{n!}f^{(n)}(a+\theta h), \tag{1.2}$$

para algum θ compreendido entre 0 e 1.

1.1.5 Fórmula de transformação theta

Nesta subseção, apresentaremos uma importante fórmula de transformação de variáveis, que faz parte da Análise. Não será nosso objetivo, aqui, apresentar uma demonstração da mesma, pois que para ela seria necessário o desenvolvimento prévio de temas tais como séries Cèsaro-somáveis, Teorema de Fejér, Fórmula da soma de Poisson, séries de Fourier e Teorema de Cauchy (variáveis complexas), ocorrendo uma digressão desnecessária aos objetivos desta dissertação. Sendo assim, optamos por somente apresentar seu enunciado, que é bastante claro, e indicar ao leitor interessado as referências [11] e [27].

Teorema 9 (Fórmula de transformação theta). *Para todo complexo z e todo complexo t tal que $\mathfrak{Re}(t) > 0$, tem-se que*

$$\sum_{n=-\infty}^{\infty} e^{-\pi t(n+z)^2} = \frac{1}{\sqrt{t}} \sum_{n=-\infty}^{\infty} e^{-\pi n^2/t + 2\pi i n z},$$

onde $\sqrt{t}$ é determinado de acordo com a convenção $|\arg(t)| < \pi/2$.

1.2 Álgebra

1.2.1 Teoria de grupos

Conceitos Básicos

Um *grupo* é, por definição, um conjunto G sobre o qual definimos uma operação $*$ que satisfaz as seguintes propriedades:

1. Se $g_1, g_2 \in G$, então $g_1 * g_2 \in G$ (fechamento);
2. Se $g_1, g_2, g_3 \in G$, então $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ (associativa);
3. Se $g \in G$ então existe $1_G \in G$ tal que $g * 1_G = 1_G * g = g$ (elemento neutro);
4. Se $g \in G$ então existe $h \in G$ tal que $g * h = h * g = 1_G$ (elemento inverso).

O elemento h dado pelo item 4 acima é usualmente denotado por g^{-1}, e denominado inverso de g. Finalmente, denotamos $(G, *)$ o grupo G segundo a operação $*$.

Seja G um grupo segundo a operação $*$ e H um subconjunto não vazio de G. Dizemos que H é *subgrupo* de G, denotando $H \leqslant G$, se H é um grupo segundo $*$. Todavia, as

seguintes duas propriedades são equivalentes à definição de subgrupo, fazendo-se muito úteis quando se quer provar que um certo subconjunto não vazio H de G é subgrupo de $(G, *)$:

1. Se $g_1, g_2 \in H$ então $g_1 * g_2 \in H$;
2. Se $g \in H$ então $g^{-1} \in H$.

Seja G um grupo e S um subconjunto não vazio de G. Então define-se

$$\langle S \rangle = \{g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_k^{\varepsilon_k} \mid k > 0,\, g_i \in S,\, \varepsilon_i = \pm 1,\, 1 \leq i \leq k\},$$

que é o menor subgrupo de G que contém S, sendo por isso denominado *subgrupo de G gerado por S*. Dizemos que um grupo é *cíclico* quando ele é gerado por um único elemento. Por exemplo, $(\mathbb{Z}, +)$ é cíclico com gerador igual a 1. Seguindo a notação anterior, podemos escrever $\mathbb{Z} = \langle 1 \rangle$.

Para cada grupo G, definimos a *ordem de G* como o número de elementos de G, isto é, a cardinalidade de G como conjunto. Definimos, ainda, para $g \in G$, a *ordem de g* como sendo a cardinalidade do grupo gerado por g. Assim, utilizando o símbolo $|X|$ para denotar a cardinalidade do conjunto X, temos que a ordem de G é igual a $|G|$, e a ordem de g é dada por $|\langle g \rangle|$.

Classes laterais

Seja G um grupo e $H \leqslant G$. Dados dois elementos x, y de G, definimos a seguinte relação entre eles:

$$x \sim y \Leftrightarrow xy^{-1} \in H.$$

É muito simples a prova de que a relação $\sim$ assim definida é, de fato, uma relação de equivalência, isto é, verifica as propriedades reflexiva, simétrica e transitiva. É importante observar, também, que esta relação depende de H. Com isso, podemos agrupar os elementos de G em classes de equivalência dadas por $C = \{y \in G \mid y \sim x\} = \{hx \mid h \in H\} = Hx$. De fato,

$$y \in C \Leftrightarrow y \sim x \Leftrightarrow yx^{-1} \in H \Leftrightarrow \exists h \in H : yx^{-1} = h \Leftrightarrow y = hx \Leftrightarrow y \in Hx.$$

Neste caso, os elementos x são chamados representantes das classes de equivalência, ou classes laterais à direita de H em G. Sempre podemos agrupar os elementos de G em

classes laterais disjuntas de H em G, tomando os representantes distintos que as definem. Ou seja, se T for um conjunto de representantes de classes laterais distintas de H em G (ou seja, elementos distintos de G módulo H), então podemos sempre escrever

$$G = \bigcup_{x \in T} Hx,$$

tal que $Hx_1 \cap Hx_2 = \emptyset$ sempre que $x_1 \neq x_2$, sendo $x_1, x_2 \in T$. O número de elementos de T, isto é, o número de classes laterais distintas determinadas pelo subgrupo H de G, é usualmente denominado índice do subgrupo H em G, e denotado $[G : H]$. Este valor é invariante no sentido de que não depende da decomposição realizada, mas apenas do subgrupo em questão. É importante observar, ainda, que o desenvolvimento que aqui se encontra poderia também ter sido feito para classes laterais à esquerda de H em G.

A partir da mesma notação anterior, desejamos agora definir uma operação produto entre duas classes laterais Hg_1 e Hg_2 por $(Hg_1)(Hg_2) = Hg_1g_2$. Se $x_1 \neq y_1$ e $x_2 \neq y_2$ são tais que $Hx_1 = Hy_1$ e $Hx_2 = Hy_2$, nem sempre ocorre que $Hx_1x_2 = Hy_1y_2$. Se, para um certo $H \leqslant G$, isso sempre ocorre, dizemos que a operação produto entre classes laterais é bem definida, e H é um subgrupo *normal* em G, denotando-se $H \triangleleft G$. A verificação de que a operação produto entre classes laterais é bem definida, todavia, nem sempre é tão prática para se concluir que um dado subgrupo é normal em outro. Assim, existe uma série de equivalências nesse sentido. Neste material, utilizaremos o fato de que $H \triangleleft G$ se $gHg^{-1} \subset H$, para todo $g \in G$ (é possível provar que, se isto ocorre, então a operação produto entre classes laterais é bem definida).

1.3 Topologia

1.3.1 Conceitos básicos

Seja X um conjunto. Chamamos de *topologia* em X uma família τ de subconjuntos de X com as seguintes propriedades:

1. $\emptyset$ e X pertencem a τ;

2. a união de uma família arbitrária de membros de τ pertence a τ;

3. a intersecção de qualquer família finita de membros de τ pertence a τ.

Denominamos *abertos* os membros de τ. Agora, podemos definir conjuntos *fechados* como sendo aqueles cujo complemento é um conjunto aberto. O *fecho* de um conjunto A, denotado por $\overline{A}$, e definido por

$$\overline{A} = \bigcap \{F \subset X \mid F \text{ é fechado e contém } A\}.$$

O fecho de um conjunto é, pela própria definição, o menor conjunto fechado que o contém. Analogamente, definimos o *interior* de um conjunto A, denotado por $int(A)$, como

$$\text{int}(A) = \bigcup \{U \subset X \mid U \text{ é aberto e está contido } A\},$$

sendo o maior subconjunto aberto de A.

Seja $f : A \to B$ uma função entre os espaços topológicos A e B. Quando f é contínua e possui inversa também contínua, dizemos que f é um *homeomorfismo*. Neste caso, para cada $A_0 \subset A$, vale que $f\left(\overline{A_0}\right) = \overline{f(A_0)}$. Outra propriedade que será utilizada envolvendo o fecho de conjuntos é o fato de que o fecho de uma união finita de subespaços de um certo espaço topológico X é igual à união dos fechos de cada um dos subespaços em questão.

Seja $x \in X$. Dizemos que $U \subset X$ é uma *vizinhança* de x se $x \in \text{int}(U)$. Denotamos $\mathcal{U}_x$ o conjunto de todas as vizinhanças de x. A seguinte proposição é importante e será por nós utilizada em ocasiões futuras:

Proposição 10. *Valem os seguintes resultados:*

1. *A é aberto se, e somente se, para cada $x \in A$, existe $U \in \mathcal{U}_x$ tal que $U \subset A$;*
2. *A é fechado se, e somente se, para cada $x \notin A$, existe $U \in \mathcal{U}_x$ tal que $U \cap A = \emptyset$;*
3. *$\overline{A} = \{x \in X \mid U \cap A \neq \emptyset \text{ para cada } U \in \mathcal{U}_x\}$;*
4. *$\text{int}(A) = \{x \in X \mid U \subset A \text{ para algum } U \in \mathcal{U}_x\}$.*

Sendo X um conjunto e τ uma topologia em X, podemos definir, para um certo $S \subset X$, a topologia de S induzida pela de X por

$$\tau_S = \{S \cap U \mid U \in \tau\}.$$

Neste caso, dizemos que S é um subespaço de X. Nessas condições, segue mais uma proposição, também importante:

Proposição 11. *Valem os seguintes resultados:*

1. *U é aberto em S se, e somente se, $U = S \cap U_1$, sendo U_1 aberto em X;*
2. *F é fechado em S se, e somente se, $F = S \cap F_1$, sendo F_1 fechado em X.*

1.3.2 Esfera de Riemann

Refere-se à compactificação do plano complexo $\mathbb{C}$, através da adição do ponto ∞, sendo por isso denotada $\mathbb{C} \cup \{\infty\} = \mathbb{C}^*$ (plano complexo estendido). Neste caso, o sistema de vizinhanças dos pontos de $\mathbb{C}$ são herdados da topologia induzida pela métrica euclideana em $\mathbb{R}^2$, e o sistema de vizinhanças de ∞ se define como o conjunto das faixas $\mathfrak{Im}(z) > r$ unidas a ∞, para $r \in \mathbb{R}$.

Sendo $S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$ (casca esférica centrada na origem e de raio igual a 1), podemos obter um homeomorfismo entre $S^2 \setminus \{(0, 0, 1)\}$ e $\mathbb{C}$ (projeções estereográficas). Ademais, o ponto $(0, 0, 1)$ pode ser identificado com ∞, de tal maneira que podemos entender que há uma identificação homeomórfica entre S^2 e $\mathbb{C}^*$, donde se justifica a denominação usual deste conjunto como "esfera" de Riemann.

A esfera de Riemann é uma variedade complexa unidimensional, podendo ser descrita através de dois sistemas de coordenadas locais. Para os pontos de $\mathbb{C}$, a carta é dada pela aplicação identidade entre $\mathbb{C}^* \setminus \{\infty\} = \mathbb{C}$ e $\mathbb{C}$ e, para o ponto ∞, a carta é dada pela aplicação entre $\mathbb{C}^* \setminus \{0\}$ e $\mathbb{C}$ que envia ∞ para 0 e todos os outros pontos z para $1/z$.

1.4 Teoria dos números

Começamos com uma definição:

Definição 3. *1. Se p é um número primo e a é um inteiro, dizemos que a é um* resíduo quadrático módulo p *se existe um inteiro x tal que $x^2 \equiv a \pmod{p}$. Em particular, se $p \neq 2$ e $(a, p) = 1$, definimos o* símbolo de Legendre $\left(\frac{a}{p}\right)$ *por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é um resíduo quadrático módulo } p, \\ -1, & \text{caso contrário.} \end{cases}$$

2. Sejam b um inteiro positivo ímpar e a um inteiro tal que $(a, b) = 1$. Se $b \neq 1$, escreva $b = p_1 p_2 \cdots p_s$, onde os números p_i, $1 \leq i \leq s$, são primos não necessariamente distintos. Então definimos o símbolo de Jacobi $\left(\frac{a}{b}\right)$ *por*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right),$$

sendo os fatores do membro direito símbolos de Legendre. Ademais, por convenção, $\left(\frac{a}{1}\right) = 1$, e $\left(\frac{p}{p}\right) = 0$, para cada a inteiro e p primo.

Observe que, se b é um primo ímpar, então o símbolo de Jacobi se reduz ao símbolo de Legendre. Portanto, justifica-se a prática usual de se utilizar o mesmo símbolo para ambos os conceitos.

Apresentamos agora um lema que reúne diversos resultados conhecidos a respeito do tema de que tratamos. Alguns deles são triviais, mas outros nem tanto, como por exemplo a lei da reciprocidade quadrática e sua posterior generalização. De qualquer modo, não provaremos esse lema, indicando ao leitor interessado a referência [22].

Lema 12. *1. Se m é um inteiro positivo ímpar, $(n,m)=1$, e $n' \equiv n \pmod m$, então $\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right)$;*

2. Se m e m' são inteiros positivos ímpares e $(n,m)=1=(n,m')$, então $\left(\frac{n}{m}\right)\left(\frac{n}{m'}\right) = \left(\frac{n}{mm'}\right)$;

3. Se m é um inteiro positivo ímpar e $(n,m)=1=(n',m)$, então $\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right) = \left(\frac{nn'}{m}\right)$;

4. Se m é um inteiro positivo ímpar, então $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$;

5. Se m é um inteiro positivo ímpar, então $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$;

6. (Lei da Reciprocidade Quadrática). Se m e n são inteiros positivos ímpares e $(m,n)=1$, então

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}};$$

7. (Lei da Reciprocidade Quadrática - generalização). Se m e n são ímpares e $(m,n)=1$, então

$$\begin{aligned}\left(\frac{n}{|m|}\right)\left(\frac{m}{|n|}\right) &= \begin{cases} -(-1)^{\frac{n-1}{2}\frac{m-1}{2}}, & \text{se } n,m<0, \\ (-1)^{\frac{n-1}{2}\frac{m-1}{2}}, & \text{caso contrário} \end{cases} \\ &= (-1)^{\frac{\operatorname{sign}(n)-1}{2}\frac{\operatorname{sign}(m)-1}{2}}(-1)^{\frac{n-1}{2}\frac{m-1}{2}},\end{aligned}$$

onde

$$\operatorname{sign}(x) = \frac{x}{|x|} = \begin{cases} 1, & \text{se } x>0, \\ -1, & \text{se } x<0. \end{cases}$$

Segue, enfim, uma última definição, que se destina tão somente a introduzir uma notação, a fim de tornar mais claros os nossos cálculos, no Capítulo 5.

Definição 4. *Suponha que c e d sejam inteiros não nulos tais que $(c,d)=1$ e d é ímpar. Definimos $\left(\frac{c}{d}\right)^* = \left(\frac{c}{|d|}\right)$ e $\left(\frac{c}{d}\right)_* = \left(\frac{c}{|d|}\right)(-1)^{\frac{\text{sign}(c)-1}{2}\frac{\text{sign}(d)-1}{2}}$. Ademais, definimos $\left(\frac{0}{\pm 1}\right)^* = 1$, $\left(\frac{0}{1}\right)_* = 1$, e $\left(\frac{0}{-1}\right)_* = -1$.*

Capítulo 2

O grupo modular e certos subgrupos

2.1 O grupo modular

O grupo modular é, por definição, o conjunto das transformações lineares fracionárias

$$\begin{aligned} V : \mathbb{C} &\rightarrow \mathbb{C} \\ \tau &\mapsto \frac{a\tau + b}{c\tau + d} \end{aligned} \tag{2.1}$$

para as quais a, b, c e d são inteiros e $ad - bc = 1$. Este conjunto é usualmente denotado por $\Gamma(1)$, e é importante ressaltar que o plano complexo considerado aqui e ao longo deste material é o estendido (esfera de Riemann[1]), definindo-se $V(-d/c) = \infty$ e $V(\infty) = a/c$. A seguir, provaremos que $\Gamma(1)$ é, de fato, um grupo via composição de funções, provando as propriedades exibidas no Capítulo 1:

1. Se $V_1, V_2 \in \Gamma(1)$, então $V_1 \circ V_2 \in \Gamma(1)$ (fechamento);

[1]Para mais esclarecimentos, consulte o Capítulo 1.

Consideremos $V_1(\tau) = \frac{a_1\tau+b_1}{c_1\tau+d_1} \in \Gamma(1)$ e $V_2(\tau) = \frac{a_2\tau+b_2}{c_2\tau+d_2} \in \Gamma(1)$. Logo

$$\begin{aligned} V_1 \circ V_2(\tau) &= V_1(V_2(\tau)) \\ &= V_1\left(\frac{a_2\tau+b_2}{c_2\tau+d_2}\right) \\ &= \frac{a_1\left(\frac{a_2\tau+b_2}{c_2\tau+d_2}\right)+b_1}{c_1\left(\frac{a_2\tau+b_2}{c_2\tau+d_2}\right)+d_1} \\ &= \frac{\frac{(a_1a_2+b_1c_2)\tau+(a_1b_2+b_1d_2)}{c_2\tau+d_2}}{\frac{(c_1a_2+d_1c_2)\tau+(c_1b_2+d_1d_2)}{c_2\tau+d_2}} \\ &= \frac{(a_1a_2+b_1c_2)\tau+(a_1b_2+b_1d_2)}{(c_1a_2+d_1c_2)\tau+(c_1b_2+d_1d_2)} \end{aligned}$$

Agora, comparando-se com (2.1), basta observarmos que

$$\begin{aligned} &(a_1a_2+b_1c_2)(c_1b_2+d_1d_2)-(a_1b_2+b_1d_2)(c_1a_2+d_1c_2) = \\ &\quad = a_1a_2c_1b_2 + a_1a_2d_1d_2 + b_1c_2c_1b_2 + b_1c_2d_1d_2 \\ &\qquad - a_1b_2c_1a_2 - a_1b_2d_1c_2 - b_1d_2c_1a_2 - b_1d_2d_1c_2 \\ &\quad = a_1a_2d_1d_2 + b_1c_2c_1b_2 - a_1b_2d_1c_2 - b_1d_2c_1a_2 \\ &\quad = a_1d_1(a_2d_2-b_2c_2) - b_1c_1(a_2d_2-b_2c_2) \\ &\quad = (a_1d_1-b_1c_1)(a_2d_2-b_2c_2) = 1\cdot 1 = 1, \end{aligned}$$

utilizando-se o fato de que V_1 e V_2 são elementos de $\Gamma(1)$.

2. Se $V_1, V_2, V_3 \in \Gamma(1)$, então $(V_1 \circ V_2) \circ V_3 = V_1 \circ (V_2 \circ V_3)$ (associativa);
   Esta propriedade segue diretamente do fato de que a composição de funções é, em geral, associativa.

3. Se $V \in \Gamma(1)$ então existe $1_{\Gamma(1)} \in \Gamma(1)$ tal que $V \circ 1_{\Gamma(1)} = 1_{\Gamma(1)} \circ V = V$ (elemento neutro);
   Para cada $V \in \Gamma(1)$, definamos $1_{\Gamma(1)}(\tau) = \tau = \frac{1\tau+0}{0\tau+1}$. Note que $1_{\Gamma(1)}$ realmente pertence a $\Gamma(1)$, pois $1\cdot 1 - 0\cdot 0 = 1$, sendo 0 e 1 inteiros. Além disso,

$$(V \circ 1_{\Gamma(1)})(\tau) = V(1_{\Gamma(1)}(\tau)) = V(\tau) = 1_{\Gamma(1)}(V(\tau)) = (1_{\Gamma(1)} \circ V)(\tau),$$

   donde segue o que queríamos mostrar.

4. Se $V \in \Gamma(1)$ então existe $V^{-1} \in \Gamma(1)$ tal que $V \circ V^{-1} = V^{-1} \circ V = 1_{\Gamma(1)}$ (elemento inverso).
   Para cada $V(\tau) = \frac{a\tau+b}{c\tau+d} \in \Gamma(1)$, definamos $V^{-1}(\tau) = \frac{d\tau-b}{-c\tau+a}$. É claro que $V^{-1} \in \Gamma(1)$, pois d, $-b$, $-c$ e a são inteiros e $da-(-b)(-c) = ad-bc = 1$. Além disso, por um lado,

$$\begin{aligned} V \circ V^{-1}(\tau) &= V(V^{-1}(\tau)) = V\left(\frac{d\tau-b}{-c\tau+a}\right) = \frac{a\left(\frac{d\tau-b}{-c\tau+a}\right)+b}{c\left(\frac{d\tau-b}{-c\tau+a}\right)+d} \\ &= \frac{\frac{(ad-bc)\tau+(ab-ab)}{-c\tau+a}}{\frac{(cd-cd)\tau+(ad-bc))}{-c\tau+a}} = \frac{\tau}{-c\tau+a}\cdot\frac{-c\tau+a}{1} = 1_{\Gamma(1)}(\tau) \end{aligned}$$

   e, por outro,

$$\begin{aligned} V^{-1} \circ V(\tau) &= V^{-1}(V(\tau)) = V^{-1}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{d\left(\frac{a\tau+b}{c\tau+d}\right)-b}{-c\left(\frac{a\tau+b}{c\tau+d}\right)+a} \\ &= \frac{\frac{(ad-bc)\tau+(bd-bd)}{c\tau+d}}{\frac{(ac-ac)\tau+(ad-bc))}{c\tau+d}} = \frac{\tau}{c\tau+d}\cdot\frac{c\tau+d}{1} = 1_{\Gamma(1)}(\tau), \end{aligned}$$

donde segue que $\Gamma(1)$ é, de fato, um grupo via composição de funções.

Outra propriedade interessante relativa aos elementos de $\Gamma(1)$ é o fato de que eles preservam os semiplanos complexos superior e inferior e também o eixo real. Para constatá-lo, dado um número complexo τ, denotemos $\mathfrak{Re}(\tau)$ e $\mathfrak{Im}(\tau)$, respectivamente, suas partes real e imaginária. Desse modo, temos que, se $V \in \Gamma(1)$ for definida como em (2.1), então

$$V(\tau) = \frac{a\tau+b}{c\tau+d} = \frac{a\tau+b}{c\tau+d}\cdot\frac{c\overline{\tau}+d}{c\overline{\tau}+d} = \frac{ac|\tau|^2+bd+ad\tau+bc\overline{\tau}}{|c\tau+d|^2},$$

sendo $\overline{\tau}$ o complexo conjugado de τ, ou seja, se $\tau = x+iy$, então $\overline{\tau} = x-iy$, para $x, y \in \mathbb{R}$. Nesse caso, continuando a partir da expressão anteriormente obtida, temos

$$\begin{aligned} V(\tau) &= \frac{ac|\tau|^2+bd+ad(x+iy)+bc(x-iy)}{|c\tau+d|^2} \\ &= \frac{ac|\tau|^2+bd+(ad+bc)x}{|c\tau+d|^2} + i\frac{y}{|c\tau+d|^2}, \end{aligned}$$

de forma que

$$\mathfrak{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \mathfrak{Im}(V(\tau)) = \frac{y}{|c\tau+d|^2} = \frac{\mathfrak{Im}(\tau)}{|c\tau+d|^2}. \tag{2.2}$$

Agora, como $|c\tau + d|^2 > 0$ sempre que $ad - bc = 1$, segue o que queríamos mostrar. Ao longo deste texto, merecerá especial destaque o semiplano complexo superior, o qual denotaremos $\mathscr{H}$.

Quando da demonstração de que $\Gamma(1)$ é grupo via composição de funções, pudemos observar que nem sempre é tão conveniente manipular os elementos do grupo modular, uma vez que as contas podem se estender demais. Deste modo, torna-se muito interessante o fato de podermos associar cada elemento de $\Gamma(1)$ com uma matriz 2×2 de coeficientes inteiros e determinante igual a 1, isto é, um elemento de $SL_2(\mathbb{Z})$. Explicitamente, podemos associar um dado $V(\tau) = \frac{a\tau+b}{c\tau+d} \in \Gamma(1)$ a $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, lembrando, obviamente, de identificar matrizes opostas, uma vez que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ são matrizes que se referem à mesma transformação linear fracionária. Assim, rigorosamente, existe um isomorfismo entre $\Gamma(1)$ e $SL_2(\mathbb{Z})/\{\pm I\}$, sendo I a matriz identidade de $SL_2(\mathbb{Z})$. Dependendo da conveniência, utilizaremos esse fato ao longo deste texto.

Suponha agora que Γ seja subgrupo de $\Gamma(1)$ ($\Gamma \leqslant \Gamma(1)$). Dizemos que os números complexos τ_1 e τ_2 são *equivalentes* com relação a Γ se existir $V \in \Gamma$ tal que $V(\tau_1) = \tau_2$ e, neste caso, denotamos $\tau_1 \sim_\Gamma \tau_2$. Esta relação é, de fato, uma relação de equivalência, isto é, satisfaz as propriedades reflexiva, simétrica e transitiva. Segue agora uma definição muito importante, que será utilizada com freqüência em outras partes do texto:

Definição 1. *Seja $\Gamma \leqslant \Gamma(1)$. Uma* região fundamental segundo Γ *é um subconjunto aberto $\mathscr{R}$ de $\mathscr{H}$ que satisfaz*

1. *Se $\tau_1, \tau_2 \in \mathscr{R}$ e $\tau_1 \neq \tau_2$ então $\tau_1 \nsim_\Gamma \tau_2$;*
2. *Se $\tau \in \mathscr{H}$ então existe $\tau' \in \overline{\mathscr{R}}$ tal que $\tau \sim_\Gamma \tau'$.*

Na definição acima, $\overline{\mathscr{R}}$ denota o fecho do conjunto aberto $\mathscr{R}$ segundo a topologia usual da esfera de Riemann (consulte o Capítulo 1). É interessante observar, também, que Γ, como subgrupo de $\Gamma(1)$, é essencial na definição de região fundamental, uma vez que a relação de equivalência que a define depende do subgrupo.

Segundo a Definição 1, não há unicidade em relação à existência de uma região fundamental. De fato, supondo que $\mathscr{R}$ seja uma região fundamental segundo Γ como na Definição 1, tomemos $F \subset \mathscr{R}$ tal que $\overline{F} = F$ e $\text{int}(F) = \emptyset$ (F é fechado em $\mathscr{H}$ e possui interior vazio). Como $F = \mathscr{R} \cap F$, vem que F é fechado também em $\mathscr{R}$, donde $\mathscr{R} \setminus F$ é

aberto em $\mathscr{R}$. Logo existe um conjunto A, aberto em $\mathscr{H}$, tal que $\mathscr{R} \setminus F = \mathscr{R} \cap A$ e, como $\mathscr{R}$ é aberto em $\mathscr{H}$, segue que $\mathscr{R} \setminus F$ é aberto em $\mathscr{H}$. Além disso, se $x \in \overline{\mathscr{R} \setminus F}$, então, dado $U \in \mathcal{U}_x$, tem-se que $U \cap (\mathscr{R} \setminus F) \neq \emptyset$, donde $(U \cap \mathscr{R}) \setminus F \neq \emptyset$ e, portanto, $U \cap \mathscr{R} \neq \emptyset$. Logo $x \in \overline{\mathscr{R}}$, donde $\overline{\mathscr{R} \setminus F} \subset \overline{\mathscr{R}}$. Reciprocamente, se $x \in \overline{\mathscr{R}}$, então, dado $U \in \mathcal{U}_x$, tem-se que $U \cap \mathscr{R} \neq \emptyset$. Agora, se existir $U \in \mathcal{U}_x$ tal que $(U \cap \mathscr{R}) \setminus F = \emptyset$, então $U \cap \mathscr{R} \subset F$, donde $\mathrm{int}(U) \cap \mathscr{R} = \mathrm{int}(U \cap \mathscr{R}) = \emptyset$. Entretanto, $\mathrm{int}(U) \in \mathcal{U}_x$, gerando uma contradição. Logo, para cada $U \in \mathcal{U}_x$, vale que $U \cap (\mathscr{R} \setminus F) = (U \cap \mathscr{R}) \setminus F \neq \emptyset$, donde $x \in \overline{\mathscr{R} \setminus F}$, ou seja, $\overline{\mathscr{R}} \subset \overline{\mathscr{R} \setminus F}$. Portanto, $\overline{\mathscr{R}} = \overline{\mathscr{R} \setminus F}$. Assim, $\mathscr{R} \setminus F \subset \mathscr{R}$ é um subconjunto aberto de $\mathscr{H}$ que possui fecho igual ao de $\mathscr{R}$. Agora, é imediato o fato de que $\mathscr{R} \setminus F$ também satisfaz a condição de ser região fundamental segundo Γ. Isso mostra que uma região fundamental segundo um certo subrupo Γ de $\Gamma(1)$, pela Definição 1, não é única. Como outra evidência a esse respeito, ainda utilizando a mesma notação da definição, sejam $A \subset \mathscr{R}$ e $V' \in \Gamma$. Sem maiores dificuldades, podemos provar que $\mathscr{R}' = \mathrm{int}(\mathscr{R} \setminus A) \cup \mathrm{int}(V'(A))$ é também uma região fundamental segundo Γ. Outra observação que fazemos é que, se $\Gamma_2 \leqslant \Gamma_1 \leqslant \Gamma(1)$ e $\mathscr{R}_1$ e $\mathscr{R}_2$ são regiões fundamentais, respectivamente, segundo Γ_1 e Γ_2, então $\mathscr{R}_1 \subset \mathscr{R}_2$, ou seja, o subgrupo maior possui a região fundamental menor. Este fato é conseqüência direta, em particular, da Propriedade 1 da definição de região fundamental: se o grupo é "menor", o número de pontos não equivalentes deve "aumentar".

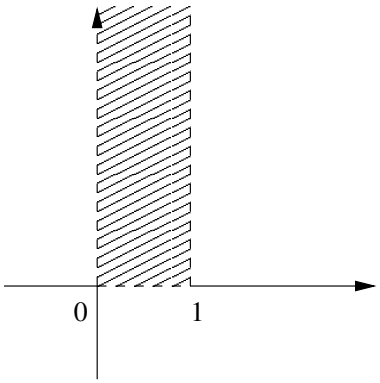
Já sabemos que dois elementos de $\mathscr{H}$ são equivalentes se um puder ser levado ao outro por meio de uma transformação de Γ, adotando-se a mesma notação anterior. Assim, resulta que os elementos de $\mathscr{H}$ podem ser agrupados em classes de equivalência e, desta maneira, uma região fundamental pode ser vista como um sistema completo de representantes de classes de equivalência de $\mathscr{H}$ segundo Γ.

Neste material, não consideraremos questões sobre existência de regiões fundamentais de subgrupos Γ arbitrários, restringindo-nos a subgrupos Γ de índice finito em $\Gamma(1)$, isto é, tais que $[\Gamma : \Gamma(1)] < \infty$. Isto resultará, como veremos, na construção de certas regiões fundamentais em termos da decomposição dos grupos em classes laterais. Os exemplos seguintes visam a tornar um pouco mais concreta a nossa definição de região fundamental, e devem ser bem compreendidos para que se dê continuidade ao estudo ora iniciado.

Exemplos

1. Consideremos as transformações lineares fracionárias S dadas por $S(\tau) = \tau + 1$. Também podemos escrever S em sua forma matricial como $S =$

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Seja $\Gamma = \langle S \rangle$ o subgrupo de $\Gamma(1)$ gerado por essas transformações. Então Γ consiste em todas as translações $S^n(\tau) = \tau + n$, $n \in \mathbb{Z}$. Uma escolha para uma região fundamental segundo Γ é o conjunto dado por $\mathfrak{Im}(\tau) > 0$ e $|\mathfrak{Re}(\tau)| < 1/2$. Outra opção é o conjunto dos elementos $\tau \in \mathscr{H}$ tais que $0 < \mathfrak{Re}(\tau) < 1$, cujo esboço segue abaixo:



Através da definição de Γ e da Definição 1, é fácil concluir que as regiões consideradas são, de fato, regiões fundamentais. Na verdade, podemos concluir, ainda, que qualquer faixa de largura 1 como as já citadas satisfazem a definição de região fundamental. Após a Definição 1, comentamos que, retirando-se um subconjunto fechado de uma região fundamental ou transformando, por um elemento de Γ, uma parte da região original, obtemos, novamente, uma região fundamental segundo Γ. Como exemplos, a partir de $\mathscr{R} = \{\tau \in \mathscr{H} \mid 0 < \mathfrak{Re}(\tau) < 1\}$, temos, como regiões fundamentais alternativas segundo Γ, os conjuntos

$$\{\tau \in \mathscr{H} \mid 0 < \mathfrak{Re}(\tau) < 1/2\} \cup \{\tau \in \mathscr{H} \mid 1/2 < \mathfrak{Re}(\tau) < 1\},$$

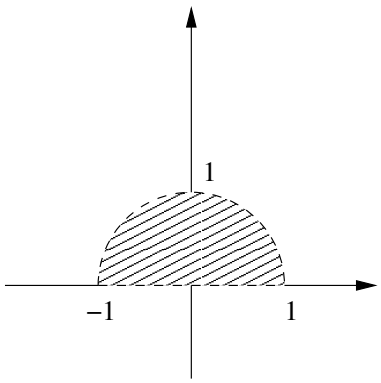
tomando-se $F = \{\tau \in \mathscr{H} \mid \mathfrak{Re}(\tau) = 1/2\}$, e

$$\{\tau \in \mathscr{H} \mid 0 < \mathfrak{Re}(\tau) < 1/2\} \cup \{\tau \in \mathscr{H} \mid 7/2 < \mathfrak{Re}(\tau) < 4\},$$

tomando-se $A = \{\tau \in \mathscr{H} \mid 1/2 < \mathfrak{Re}(\tau) < 1\}$ e $V' = S^3$.

2. Consideremos as transformações lineares fracionárias T, dadas por $T(\tau) = \frac{-1}{\tau}$, ou $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, em sua forma matricial. Seja $\Gamma = \langle T \rangle$. Observemos que $T^2 =$

$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$, donde $T^2(\tau) = \frac{-\tau}{-1} = \tau$. Logo Γ é um subgrupo de $\Gamma(1)$ de ordem 2. Neste caso, dentre as várias regiões fundamentais possíveis, elencamos $\{\tau \in \mathscr{H} \mid |\tau| < 1\}$, $\{\tau \in \mathscr{H} \mid |\tau| > 1\}$ e $\{\tau \in \mathscr{H} \mid |\mathfrak{Re}(\tau)| > 0\}$, das quais esboçamos a primeira:



Observe que sempre que tomamos um ponto interior ao semi-círculo esboçado, aplicando elementos de Γ, obtemos como imagem um elemento de seu exterior ou o próprio ponto de partida (no caso de tomarmos $I \in \Gamma$). Além disso, qualquer ponto de $\mathscr{H}$, via ação de algum elemento de Γ, é levado ao fecho da região delimitada.

A partir de agora, utilizaremos S e T segundo as definições desses dois exemplos.

2.2 Uma região fundamental segundo $\Gamma(1)$

Antes de enunciar e demonstrar o teorema importante desta seção, provemos o seguinte lema:

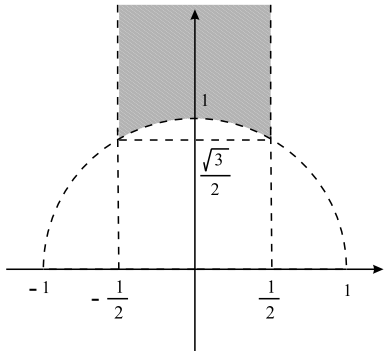
Lema 1. *Para $\tau \in \mathscr{H}$ e $N \in \mathbb{N}$ fixos, há somente um número finito de pares inteiros $c, d \in \mathbb{Z}$ tais que $|c\tau + d| \leq N$.*

Demonstração. Seja $\tau = x + iy \in \mathscr{H}$. Se $|c\tau + d| \leq N$, então $|c\tau + d|^2 \leq n$, ou $|(cx + d) + i(cy)|^2 \leq n$, donde $(cx + d)^2 + (cy)^2 \leq n$. Logo, $c^2y^2 \leq (cx + d)^2 + (cy)^2 \leq n$, donde $c^2 \leq \frac{n}{y^2}$ e, portanto, $|c| \leq \frac{\sqrt{n}}{y}$, uma vez que $y > 0$. Logo, há somente um número finito de possíveis soluções para $c \in \mathbb{Z}$. Por outro lado, para cada uma das soluções c, há também finitas possibilidades para $d \in \mathbb{Z}$, uma vez que $|c\tau + d| \leq N$. Isso conclui a prova. □

O seguinte Teorema estabelece uma importante região fundamental segundo $\Gamma(1)$, amplamente utilizada em estudos que envolvem formas modulares:

Teorema 2. *O seguinte conjunto, visualmente representado pela figura seguinte, é região fundamental segundo* $\Gamma(1)$*:*

$$\mathscr{R} = \mathscr{R}(\Gamma(1)) = \{\tau \in \mathscr{H} \mid |\tau| > 1 \text{ e } |\mathfrak{Re}(\tau)| < 1/2\}.$$



Demonstração. Seja

$$\mathscr{R}^* = \{\tau \in \mathscr{H} \mid |\mathfrak{Re}(\tau)| < 1/2 \text{ e } |c\tau + d| > 1 \text{ para todo par } c, d \in \mathbb{Z} \text{ tal que } (c,d) = 1 \text{ e } c \neq 0\}$$

Provaremos que $\mathscr{R}^* = \mathscr{R}$. Para $\tau \in \mathscr{R}^*$, tomando $c = 1$ e $d = 0$, temos que $|\tau| > 1$ e, portanto, $\tau \in \mathscr{R}$. Logo, $\mathscr{R}^* \subset \mathscr{R}$. Reciprocamente, seja $\tau = x + iy \in \mathscr{R}$, e sejam $c, d \in \mathbb{Z}$ tais que $(c,d) = 1$ e $c \neq 0$. Neste caso, temos

$$\begin{aligned} |c\tau + d|^2 &= |(cx+d) + i(cy)|^2 = (cx+d)^2 + (cy)^2 \\ &= c^2(x^2+y^2) + 2cdx + d^2 = c^2|\tau|^2 + 2cd\mathfrak{Re}(\tau) + d^2 \\ &> c^2 - 2|cd||\mathfrak{Re}(\tau)| + d^2 > c^2 - |cd| + d^2 \\ &= (|c| - |d|)^2 + |cd| \geq 1, \end{aligned}$$

uma vez que $c \neq 0$. Logo, $\tau \in \mathscr{R}^*$, donde $\mathscr{R} \subset \mathscr{R}^*$. Portanto, $\mathscr{R}^* = \mathscr{R}$. Agora, temos de provar que $\mathscr{R}$ é região fundamental segundo $\Gamma(1)$. Em primeiro lugar, é claro que $\mathscr{R}$ é um subconjunto aberto de $\mathscr{H}$. Dividamos a prova nos dois itens fornecidos pela Definição 1:

1. Se $\tau_1, \tau_2 \in \mathscr{R}$ e $\tau_1 \neq \tau_2$ então $\tau_1 \nsim_{\Gamma(1)} \tau_2$;
   Para este item, utilizaremos o fato de que $\mathscr{R}^* = \mathscr{R}$, provando o resultado acima para o primeiro conjunto. Seja $\tau_1 \in \mathscr{R}^*$ e considere $V = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, com $\tau_2 = \frac{a\tau_1+b}{c\tau_1+d}$, isto é, suponhamos que $\tau_1 \sim_{\Gamma(1)} \tau_2$. Neste caso,

$$|-c\tau_2 + a| = \left|-c\left(\frac{a\tau_1+b}{c\tau_1+d}\right) + a\right| = \frac{|ad-bc|}{|c\tau_1+d|} = \frac{1}{|c\tau_1+d|} < 1,$$

   pois $|c\tau_1 + d| > 1$. Entretanto, $(-c, a) = 1$, pois $ad - bc = 1$. Assim, se $c \neq 0$, então $\tau_2 \notin \mathscr{R}^*$. Por outro lado, se $c = 0$, então, como $ad - bc = 1$, temos $a = d = \pm 1$, donde $\tau_2 = \frac{\pm\tau_1+b}{\pm 1} = \tau_1 \pm b$. Agora, como $b \in \mathbb{Z}$ e $\tau_1 \sim_{\Gamma(1)} \tau_2$, segue que $b = 0$ ($\tau_2 \in \mathscr{R}^*$), isto é, $\tau_2 = \tau_1$, concluindo a demonstração deste item.

2. Se $\tau \in \mathscr{H}$ então existe $\tau' \in \overline{\mathscr{R}}$ tal que $\tau \sim_{\Gamma(1)} \tau'$.
   Seja $\tau \in \mathscr{H}$. Pelo Lema 1, podemos tomar $c, d \in \mathbb{Z}$ tais que $|c\tau + d|$ seja mínimo. Portanto, se $V = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, então, pela igualdade (2.2), $\mathfrak{Im}(V(\tau))$ é máximo dentre os elementos equivalentes a τ. Agora, consideremos $\tau' = V(\tau)+m$, e tomemos $m \in \mathbb{Z}$ tal que $|\mathfrak{Re}(\tau')| \leq 1/2$. Para que τ' corresponda ao número procurado, basta mostrarmos que $|\tau'| \geq 1$. De fato, se $|\tau'| < 1$, então, tomando $T \in \Gamma(1)$, temos

$$\mathfrak{Im}(T(\tau')) = \mathfrak{Im}\left(\frac{-1}{\tau'}\right) = \frac{\mathfrak{Im}(\tau')}{|\tau'|^2} > \mathfrak{Im}(\tau') = \mathfrak{Im}(V(\tau)),$$

   contradizendo a maximalidade de $\mathfrak{Im}(V(\tau))$. Assim, $\tau' \in \overline{\mathscr{R}}$, sendo $\tau \sim_{\Gamma(1)} \tau'$.

□

Ao longo deste texto, sempre denotaremos a região fundamental do teorema precedente por $\mathscr{R}(\Gamma(1))$.

2.3 Alguns subgrupos de $\Gamma(1)$

Definição 2. *Seja $n \in \mathbb{N}$. Define-se o* subgrupo principal de congruência de nível n de $\Gamma(1)$, *que se denota por $\Gamma(n)$, como o subconjunto dos elementos $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ tais que $a \equiv d \equiv \pm 1$ (mod n) e $b \equiv c \equiv 0$ (mod n). Em notação matricial, para cada matriz*

$M \in \Gamma(1)$, tem-se que $M \in \Gamma(n)$ se $M \equiv \pm I$ (mod n), sendo a congruência considerada em relação a cada um dos termos correspondentes das matrizes. Além disso, $\Gamma^0(n)$ é tido como o subgrupo de $\Gamma(1)$ sujeito a $b \equiv 0$ (mod n), e $\Gamma_0(n)$ o subgrupo de $\Gamma(1)$ ao qual impomos $c \equiv 0$ (mod n). Finalmente, Γ_ϑ é definido como o subgrupo de $\Gamma(1)$ gerado por S^2 e T, isto é $\Gamma_\vartheta = \langle S^2, T\rangle$ (ϑ: variante da letra grega θ).

São muito simples as demonstrações de que os subconjuntos de $\Gamma(1)$ definidos acima são, de fato, subgrupos de $\Gamma(1)$. Observemos também que, para $n = 1$, $\Gamma(n)$ coincide com o grupo modular.

Merece destaque, ainda, o fato de que $\Gamma(n)$ é subgrupo normal em $\Gamma(1)$, o mesmo não ocorrendo com os outros subgrupos da definição. De fato, dado $\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \in \Gamma(n)$ ($a_0 \equiv d_0 \equiv \pm 1 \pmod{n}$ e $b_0 \equiv c_0 \equiv 0 \pmod{n}$) e $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, temos

$$\begin{aligned}
&\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\
&= \begin{pmatrix} ada_0 + bdc_0 - acb_0 - bcd_0 & -aba_0 - b^2c_0 + a^2b_0 + abd_0 \\ cda_0 + d^2c_0 - c^2b_0 - cdd_0 & -bca_0 - bdc_0 + acb_0 + add_0 \end{pmatrix} \\
&\equiv \begin{pmatrix} ad(\pm 1) - bc(\pm 1) & -ab(\pm 1) + ab(\pm 1) \\ cd(\pm 1) - cd(\pm 1) & -bc(\pm 1) + ad(\pm 1) \end{pmatrix} \\
&= \begin{pmatrix} \pm(ad - bc) & 0 \\ 0 & \pm(-bc + ad) \end{pmatrix} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} = \pm I \pmod{n}.
\end{aligned}$$

Logo, para cada $V \in \Gamma(1)$, tem-se que $V\Gamma(n)V^{-1} \subset \Gamma(n)$, donde $\Gamma(n) \triangleleft \Gamma(1)$. Por outro lado, dado $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(n)$ ($c \equiv 0 \pmod{n}$), temos que

$$\begin{aligned}
T\begin{pmatrix} a & b \\ c & d \end{pmatrix}T^{-1} &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \in \Gamma^0(n),
\end{aligned}$$

o que prova que $T\Gamma_0(n)T^{-1} \subset \Gamma^0(n)$. Analogamente, dado $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^0(n)$, podemos tomar $\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \in \Gamma_0(n)$ e escrever $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = T \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} T^{-1}$, de modo que $\Gamma^0(n) \subset T\Gamma_0(n)T^{-1}$. Portanto, $T\Gamma_0(n)T^{-1} = \Gamma^0(n)$, ficando provado que nenhum desses dois subgrupos são normais em $\Gamma(1)$. A identidade anterior, envolvendo $\Gamma_0(n)$ e $\Gamma^0(n)$, é importante, e será utilizada em ocasiões futuras. Também provaremos, no Lema 9, que $S\Gamma_\vartheta S^{-1} = \Gamma^0(2)$, donde Γ_ϑ tampouco é normal em $\Gamma(1)$.

Uma vez estudados alguns dos subgrupos importantes de $\Gamma(1)$, vamos estudar decomposições do grupo modular em classes laterais desses subgrupos. Antes, porém, um resultado que será importante nesse sentido

Teorema 3. *Seja $n \in \{1, 2, 3, 4\}$, e considere Γ_1 o grupo gerado pelas transformações lineares fracionárias da forma $\tau \mapsto \tau + \sqrt{n}$ e $\tau \mapsto -1/\tau$ ou, em notação matricial, por $\begin{pmatrix} 1 & \sqrt{n} \\ 0 & 1 \end{pmatrix}$ e $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = T$. Seja Γ_2 o conjunto de todas as transformações lineares fracionárias dos dois seguintes tipos:*

1. *$\tau \mapsto \frac{a\tau + b\sqrt{n}}{c\sqrt{n}\tau + d}$, tal que $a, b, c, d \in \mathbb{Z}$ e $ad - nbc = 1$;*

2. *$\tau \mapsto \frac{a\sqrt{n}\tau + b}{c\tau + d\sqrt{n}}$, tal que $a, b, c, d \in \mathbb{Z}$ e $nad - bc = 1$.*

Então Γ_2 é grupo idêntico a Γ_1.

Demonstração. Primeiramente, notemos que os elementos de Γ_1 e Γ_2 pertencem ao grupo $SL_2(\mathbb{R})/\{\pm I\}$, de modo que Γ_1 é um subgrupo desse grupo, e não de $\Gamma(1) = SL_2(\mathbb{Z})/\{\pm I\}$ (caso $n = 1$).

Um elemento genérico de Γ_2 pode ser expresso por $\begin{pmatrix} a & b\sqrt{n} \\ c\sqrt{n} & d \end{pmatrix}$ (tipo especificado em 1.) ou $\begin{pmatrix} a\sqrt{n} & b \\ c & d\sqrt{n} \end{pmatrix}$ (tipo especificado em 2.). A demonstração de que este conjunto é um grupo é muito simples, consistindo apenas na verificação direta das propriedades definidoras de subgrupo estabelecidas no Capítulo 1, quais sejam, as de que, dados dois elementos de Γ_2, sua composição também se encontra em Γ_2, e cada elemento de Γ_2 possui inverso também neste conjunto (em seguida utilizando-se o fato de que $SL_2(\mathbb{R})/\{\pm I\}$ é grupo). Entretanto, mostrando-se diretamente que $\Gamma_1 = \Gamma_2$, a

conclusão anterior é imediata, uma vez que Γ_1 é grupo (seguir tal caminho é possível porque, na demonstração que faremos, o fato de que Γ_2 é grupo não será utilizado). Assim, ocuparemo-nos, nesta demonstração, de sua parte mais difícil, isto é, do fato de que $\Gamma_1 = \Gamma_2$. Em primeiro lugar, observe que os geradores de Γ_1 pertencem a Γ_2, donde $\Gamma_1 \subset \Gamma_2$.

Resta-nos, pois, provar, que $\Gamma_2 \subset \Gamma_1$. Para tanto, consideremos $\begin{pmatrix} a & b\sqrt{n} \\ c\sqrt{n} & d \end{pmatrix} \in \Gamma_2$. Se $a = 0$ então, como $ad - nbc = 1$, ou $-nbc = 1$, vem que $n = 1$ e b e c possuem sinais contrários, sendo ambos iguais a mais ou menos 1. Logo, a matriz original se reduz a

$$\pm \begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix} = \pm \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\in \Gamma_1} \underbrace{\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}}_{\in \Gamma_1} \in \Gamma_1,$$

uma vez que é igual ao produto de dois elementos de Γ_1, que é subgrupo de $SL_2(\mathbb{R})/\{\pm I\}$. Como veremos a seguir, este argumento será freqüente na demonstração. Se $b = 0$ então, como $ad - nbc = 1$, ou $ad = 1$, temos que $a = d = \pm 1$, e a matriz original se reduz a

$$\pm \begin{pmatrix} 1 & 0 \\ c\sqrt{n} & 1 \end{pmatrix} = \mp \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\in \Gamma_1} \underbrace{\begin{pmatrix} 1 & -c\sqrt{n} \\ 0 & 1 \end{pmatrix}}_{\in \Gamma_1} \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\in \Gamma_1} \in \Gamma_1.$$

Assim, podemos supor $a \neq 0$ e $b \neq 0$. Para $t \in \mathbb{Z}$, temos

$$\begin{pmatrix} a & b\sqrt{n} \\ c\sqrt{n} & d \end{pmatrix} \underbrace{\begin{pmatrix} 1 & t\sqrt{n} \\ 0 & 1 \end{pmatrix}}_{\in \Gamma_1} = \begin{pmatrix} a & b'\sqrt{n} \\ c\sqrt{n} & d' \end{pmatrix},$$

onde $b' = at + b$ e $d' = ctn + d$. Nosso objetivo, então, pode ser transferido para a prova de que $\begin{pmatrix} a & b'\sqrt{n} \\ c\sqrt{n} & d' \end{pmatrix} \in \Gamma_1$. Afirmamos, agora, que existe $t \in \mathbb{Z}$ tal que $|b'\sqrt{n}| < |a|$. Isto é equivalente a existir $t \in \mathbb{Z}$ tal que $-|a| < b'\sqrt{n} < |a|$, ou $-|a| - at\sqrt{n} < b\sqrt{n} < |a| - at\sqrt{n}$. Se $a > 0$ então $a = |a|$, donde $-|a|(1 + \sqrt{n}t) < b\sqrt{n} < |a|(1 - \sqrt{n}t)$, ou $|a|(\sqrt{n}t - 1) < b\sqrt{n} < |a|(\sqrt{n}t + 1)$, substituindo t por $-t$, uma vez que estamos interessados apenas em assegurar a existência do inteiro em questão. Analogamente, se $a < 0$ então $a = -|a|$, donde $|a|(\sqrt{n}t - 1) < b\sqrt{n} < |a|(\sqrt{n}t + 1)$. Assim, a existência de $t \in \mathbb{Z}$ tal que $|b'\sqrt{n}| < |a|$ é equivalente à existência de $t \in \mathbb{Z}$ tal que

$$|a|(\sqrt{n}t - 1) < b\sqrt{n} < |a|(\sqrt{n}t + 1). \tag{2.3}$$

Agora, afirmamos que sempre se pode escolher um inteiro t que satisfaça (2.3), desde que $1 \leq n \leq 4$. Para tanto, notemos que, para tais valores de n, os intervalos da forma $[|a|(\sqrt{n}t-1), |a|(\sqrt{n}t+1)]$ cobrem toda a reta à medida que t percorre $\mathbb{Z}$. De fato, para $1 \leq n \leq 3$, os interiores desses intervalos já cobrem $\mathbb{R}$. Para prová-lo, observemos que cada intervalo do tipo $(|a|(\sqrt{n}t-1), |a|(\sqrt{n}t+1))$ possui comprimento $2|a|$, que $|a|(\sqrt{n}t-1)$ é tão pequeno quanto se queira, que $|a|(\sqrt{n}t+1)$ é tão grande quanto se queira e, finalmente, que cada dois intervalos correspondentes a valores consecutivos de t possuem intersecção. De fato, observe que, dado $t \in \mathbb{Z}$, $|a|(\sqrt{n}(t+1)-1) < |a|(\sqrt{n}t+(\sqrt{n}-1)) < |a|(\sqrt{n}t+1)$, para $n = 1, 2, 3$. Logo, existe $t \in \mathbb{Z}$ satisfazendo (2.3) nesses casos. Para $n = 4$, a demonstração é análoga, exceto que a segunda das desigualdades da segunda linha anterior se torna $\leq$, garantindo-nos apenas a existência de $t \in \mathbb{Z}$ tal que $|a|(\sqrt{n}t-1) \leq b\sqrt{n} \leq |a|(\sqrt{n}t+1)$, ou

$$|a|(2t-1) \leq 2b \leq |a|(2t+1).$$

Entretanto, como $ad - nbc = 1$, ou $ad - 4bc = 1$, vem que ad é ímpar, donde a e d também são ímpares. Logo $|a|$ e $2t \pm 1$ são ímpares, enquanto $2b$ é par. Logo, não podem ocorrer igualdades na expressão acima. Desse modo, também para $n = 4$, sempre existe um inteiro t satisfazendo (2.3). Voltemos à prova de que $\begin{pmatrix} a & b'\sqrt{n} \\ c\sqrt{n} & d' \end{pmatrix} \in \Gamma_1$. Se $b' = 0$ então basta repetir o raciocínio que aplicamos no início da demonstração para a matriz original. Caso contrário, isto é, se $b' \neq 0$, então tomemos $t \in \mathbb{Z}$ que verifique (2.3), e consideremos um novo valor $q \in \mathbb{Z}$ satisfazendo

$$\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\in \Gamma_1} \begin{pmatrix} a & b'\sqrt{n} \\ c\sqrt{n} & d' \end{pmatrix} \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\in \Gamma_1} \underbrace{\begin{pmatrix} 1 & q\sqrt{n} \\ 0 & 1 \end{pmatrix}}_{\in \Gamma_1} = \begin{pmatrix} -d' & -c'\sqrt{n} \\ b'\sqrt{n} & -a' \end{pmatrix},$$

onde $c' = c - d'q$ e $a' = a - nb'q$.

De maneira análoga à prova da existência de $t \in \mathbb{Z}$ que verifica (2.3), podemos provar que existe $q \in \mathbb{Z}$ que verifica a relação $|a'| < |b'\sqrt{n}|$, ou

$$|b'\sqrt{n}|(\sqrt{n}q-1) < a < |b'\sqrt{n}|(\sqrt{n}q+1).$$

Uma vez provado este fato, tomemos um inteiro q verificando $|a'| < |b'\sqrt{n}|$. Para este q e

aquele t que tomamos acima, segue que $|a'| < |a|$. Além disso, temos:

$$\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\in \Gamma_1} \begin{pmatrix} -d' & -c'\sqrt{n} \\ b'\sqrt{n} & -a' \end{pmatrix} \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\in \Gamma_1} = \begin{pmatrix} a' & b'\sqrt{n} \\ c'\sqrt{n} & d' \end{pmatrix} \in \Gamma_2. \tag{2.4}$$

Agora, se $a' = 0$, então repetimos o raciocínio inicial, concluindo que $\begin{pmatrix} a' & b'\sqrt{n} \\ c'\sqrt{n} & d' \end{pmatrix} \in \Gamma_1$, donde $\begin{pmatrix} -d' & -c'\sqrt{n} \\ b'\sqrt{n} & -a' \end{pmatrix} \in \Gamma_1$ e, finalmente, $\begin{pmatrix} a & b'\sqrt{n} \\ c\sqrt{n} & d' \end{pmatrix} \in \Gamma_1$. Por outro lado, se $a' \neq 0$, então repetimos todo o processo da demonstração, obtendo, em (2.4), uma matriz $\begin{pmatrix} a'' & b''\sqrt{n} \\ c''\sqrt{n} & d'' \end{pmatrix} \in \Gamma_2$ tal que $|a''| < |a'| < |a|$ ou $b'' = 0$. Este raciocínio pode prosseguir, mas é finito, uma vez que a, a', a'' são inteiros e decrescem a cada passo realizado. Assim, obtemos em (2.4), após um número finito de repetições do processo considerado, uma matriz de uma das duas formas: $\begin{pmatrix} 0 & \beta\sqrt{n} \\ \gamma\sqrt{n} & \delta \end{pmatrix}$ ou $\begin{pmatrix} \alpha & 0 \\ \gamma\sqrt{n} & \delta \end{pmatrix}$, que pertencem a Γ_1. Assim, os elementos de Γ_2 da forma $\begin{pmatrix} a & b\sqrt{n} \\ c\sqrt{n} & d \end{pmatrix}$ (tipo 1.) pertencem a Γ_1.

Para mostrar que os elementos especificados em 2. também fazem parte de Γ_1, poderíamos adotar uma estratégia semelhante, mas há uma maneira mais simples, que aproveita as conclusões anteriores. Dado um elemento de Γ_2 da forma $\begin{pmatrix} a\sqrt{n} & b \\ c & d\sqrt{n} \end{pmatrix}$, temos

$$\begin{pmatrix} a\sqrt{n} & b \\ c & d\sqrt{n} \end{pmatrix} \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\in \Gamma_1} = \underbrace{\begin{pmatrix} b & -a\sqrt{n} \\ d\sqrt{n} & -c \end{pmatrix}}_{\in \Gamma_1(\text{ tipo 1.})},$$

donde $\begin{pmatrix} a\sqrt{n} & b \\ c & d\sqrt{n} \end{pmatrix} \in \Gamma_1$. Assim, $\Gamma_2 \subset \Gamma_1$, concluindo a demonstração. □

Corolário 4. *O grupo modular é gerado por S e T, ou seja, $\Gamma(1) = \langle S, T \rangle$.*

Demonstração. Tomando $n = 1$ no Teorema 3, temos, por um lado, $\Gamma_1 = \langle S, T \rangle$ e, por outro, $\Gamma_2 = \Gamma(1)$. Como foi provado no teorema, $\Gamma_1 = \Gamma_2$, donde segue o resultado. □

Corolário 5. *Γ_ϑ consiste no conjunto de todas as transformações lineares fracionárias de $\Gamma(1)$ da forma $\tau \mapsto \frac{a\tau+b}{c\tau+d}$ tais que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (mod 2) ou $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (mod 2).*

Demonstração. Este caso corresponde a se tomar $n = 4$ no Teorema 3. Por um lado, $\Gamma_1 = \langle S^2, T\rangle = \Gamma_\vartheta$ e, por outro, Γ_2 corresponde justamente às transformações lineares fracionárias da forma especificada no enunciado do corolário. Assim, pelo resultado do teorema precedente, segue o resultado. □

A partir de agora, nesta seção, apresentaremos alguns resultados referentes a decomposições de $\Gamma(1)$ em classes laterais (à direita) de alguns de seus subgrupos de índice finito. O seguinte teorema exibe uma decomposição em classes laterais módulo $\Gamma^0(p)$, para p primo:

Teorema 6. *$\Gamma(1)$ pode ser decomposto numa união de $p+1$ classes laterais (à direita) de $\Gamma^0(p)$, para p primo. Especificamente, podemos tomar as classes laterais dos elementos S^j $(0 \leq j \leq p-1)$ e a de T, de modo que*

$$\Gamma(1) = \left(\bigcup_{j=0}^{p-1} \Gamma^0(p)S^j\right) \cup \Gamma^0(p)T.$$

Demonstração. É claro que as classes $\Gamma^0(p)S^j$ são distintas entre si, para $0 \leq j \leq p-1$. Além disso, para cada j, temos que $\Gamma^0(p)S^j \neq \Gamma^0(p)T$. De fato, observe que

$$S^jT^{-1} = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -j & 1 \\ -1 & 0 \end{pmatrix} \notin \Gamma^0(p).$$

Portanto, as $p+1$ classes laterais são distintas, restando-nos provar a igualdade do enunciado do teorema. Para tanto, a inclusão não óbvia a ser provada é $\Gamma(1) \subset \left(\bigcup_{j=0}^{p-1} \Gamma^0(p)S^j\right) \cup \Gamma^0(p)T$. Assim, consideremos $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$. Temos dois casos:

1. $p \mid a$;

   Se $p \mid a$ então $a \equiv 0 \pmod{p}$, e podemos escrever

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \underbrace{\begin{pmatrix} -b & a \\ -d & c \end{pmatrix}}_{\in \Gamma^0(p)} \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{T} \in \Gamma^0(p)T.$$

2. $p \nmid a$.

   Neste caso, existe solução j $(0 \leq j \leq p-1)$ para a congruência linear $aj \equiv b \pmod{p}$, uma vez que $(a,p) = 1 \mid b$, para todo $b \in \mathbb{Z}$. Logo, para tal solução j, tem-se que $b - aj \equiv 0 \pmod{p}$, donde

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \underbrace{\begin{pmatrix} a & b-aj \\ c & d-cj \end{pmatrix}}_{\in \Gamma^0(p)} \underbrace{\begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}}_{S^j} \in \Gamma^0(p)S^j.$$

Assim, de 1. e 2., vale a inclusão e, portanto, o teorema. □

A seguir, um lema técnico da teoria de grupos, que terá como corolário (Corolário 8) um resultado análogo ao do Teorema 6 para $\Gamma_0(p)$, sendo p um número primo:

Lema 7. *Se Γ_1 e Γ_2 são subgrupos conjugados de $\Gamma(1)$ (i.e., se existe $B \in \Gamma(1)$ tal que $B\Gamma_1 B^{-1} = \Gamma_2$), então $[\Gamma(1) : \Gamma_1] = [\Gamma(1) : \Gamma_2]$, ou seja, subgrupos conjugados de $\Gamma(1)$ possuem o mesmo índice nesse grupo.*

Demonstração. Seja $\Gamma(1) = \Gamma_1 A_1 \cup \ldots \cup \Gamma_1 A_\mu$ uma decomposição de $\Gamma(1)$ em μ classes laterais disjuntas de Γ_1, de tal modo que $[\Gamma(1) : \Gamma_1] = \mu$. Como Γ_1 e Γ_2 são conjugados, podemos assegurar a existência do elemento $B \in \Gamma(1)$ do enunciado. Afirmamos, então, que $BA_1, \ldots, BA_\mu$ é um conjunto completo de representantes distintos de $\Gamma(1)$ módulo Γ_2. De fato, primeiramente observemos que

$$\begin{aligned} \Gamma(1) &= \Gamma_1 A_1 \cup \ldots \cup \Gamma_1 A_\mu \\ &= B^{-1}\Gamma_2 B A_1 \cup \ldots \cup B^{-1}\Gamma_2 B A_\mu \\ &= B^{-1}(\Gamma_2 B A_1 \cup \ldots \cup \Gamma_2 B A_\mu), \end{aligned}$$

donde, multiplicando ambos os membros por $B \in \Gamma(1)$, temos

$$\Gamma(1) = \Gamma_2 B A_1 \cup \ldots \cup \Gamma_2 B A_\mu.$$

Resta-nos, agora, provar que estas μ classes laterais de Γ_2 são distintas. De fato, se i e j estão entre 1 e μ e $BA_i(BA_j)^{-1} = BA_iA_j^{-1}B^{-1} \in \Gamma_2$, então $A_iA_j^{-1} \in B^{-1}\Gamma_2 B = \Gamma_1$, donde $i = j$, uma vez que as classes laterais de Γ_1 são distintas. Portanto, as classes laterais de Γ_2 também são distintas, donde $[\Gamma(1) : \Gamma_2] = \mu = [\Gamma(1) : \Gamma_1]$. □

Pela demonstração, fica claro que o resultado deste lema é válido em geral. De fato, para prová-lo, não nos utilizamos, em nenhum momento, de propriedades específicas do grupo modular e de seus subgrupos.

Corolário 8. *$\Gamma(1)$ pode ser decomposto numa união de $p+1$ classes laterais de $\Gamma_0(p)$, para p primo. Especificamente, podemos tomar as classes laterais dos elementos TS^j $(0 \leq j \leq p-1)$ e a de I.*

Demonstração. Vimos anteriormente que $\Gamma^0(n) = T\Gamma_0(n)T^{-1}$, para todo $n \in \mathbb{N}$. Em particular, tomemos $n = p$. Então, pelo Teorema 6, vem:

$$\begin{aligned}\Gamma(1) &= \bigcup_{j=0}^{p-1} \Gamma^0(p)S^j \cup \Gamma^0(p)T \\ &= \bigcup_{j=0}^{p-1} T\Gamma_0(p)T^{-1}S^j \cup T\Gamma_0(p)T^{-1}T \\ &= T\left(\bigcup_{j=0}^{p-1} \Gamma_0(p)T^{-1}S^j \cup \Gamma_0(p)I\right).\end{aligned}$$

Multiplicando ambos os membros da igualdade acima por $T^{-1} \in \Gamma(1)$, e observando que $T^{-1} = T$, temos

$$\Gamma(1) = \bigcup_{j=0}^{p-1} \Gamma_0(p)TS^j \cup \Gamma_0(p)I. \tag{2.5}$$

Agora, como $\Gamma^0(p) = T\Gamma_0(p)T^{-1}$, vem que $\Gamma^0(p)$ e $\Gamma_0(p)$ são subgrupos conjugados de $\Gamma(1)$, donde, pelo Lema 7, possuem o mesmo índice em $\Gamma(1)$. Pelo Teorema 6, $[\Gamma(1) : \Gamma^0(p)] = p+1$, donde segue que (2.5) é a decomposição procurada. □

Na seqüência, o lema que justifica o fato de Γ_ϑ não ser normal em $\Gamma(1)$:

Lema 9. $\Gamma_\vartheta = S^{-1}\Gamma^0(2)S$.

Demonstração. Para provar que $\Gamma_\vartheta \subset S^{-1}\Gamma^0(2)S$, ou seja, que $S\Gamma_\vartheta S^{-1} \subset \Gamma^0(2)$, basta provar que $STS^{-1} \in \Gamma^0(2)$ e que $SS^2S^{-1} \in \Gamma^0(2)$, isto é, que a inclusão é satisfeita para para os geradores de Γ_ϑ. Ora, de fato,

$$STS^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix} \in \Gamma^0(2),$$

e

$$SS^2S^{-1} = S^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in \Gamma^0(2).$$

Agora, para provar que $S^{-1}\Gamma^0(2)S \subset \Gamma_\vartheta$, seja $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^0(2)$. Neste caso, $ad - bc = 1$ e $b \equiv 0 \pmod 2$, com $a, b, c, d \in \mathbb{Z}$, donde $ad \equiv 1 \pmod 2$, ou seja, $a \equiv d \equiv 1 \pmod 2$ e $c \equiv 0 \pmod 2$ ou $c \equiv 1 \pmod 2$. Assim,

$$\begin{aligned} S^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix} S &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a-c & a-c+b-d \\ c & c+d \end{pmatrix} = M. \end{aligned}$$

Se $c \equiv 0 \pmod 2$, então $M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2$ e, se $c \equiv 1 \pmod 2$, então $M \equiv \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \pmod 2$. Em todo o caso, pelo Corolário 5, $M \in \Gamma_\vartheta$, donde segue o resultado.

□

Utilizando-se o lema anterior, podemos obter o seguinte resultado:

Corolário 10. $\Gamma(1)$ *pode ser decomposto numa união disjunta de três classes laterais de* Γ_ϑ*, a saber, as classes de* I*,* S^{-1} *e* $S^{-1}T$*.*

Demonstração. Pelo Lema 9, sabemos que $\Gamma^0(2) = S\Gamma_\vartheta S^{-1}$. Assim, aplicando-se o Teorema 6 para $p = 2$, segue que:

$$\begin{aligned} \Gamma(1) &= \bigcup_{j=0}^{2-1} \Gamma^0(2)S^j \cup \Gamma^0(2)T \\ &= \Gamma^0(2)I \cup \Gamma^0(2)S \cup \Gamma^0(2)T \\ &= S\Gamma_\vartheta S^{-1} \cup S\Gamma_\vartheta S^{-1}S \cup S\Gamma_\vartheta S^{-1}T \\ &= S(\Gamma_\vartheta S^{-1} \cup \Gamma_\vartheta I \cup \Gamma_\vartheta S^{-1}T) \end{aligned}$$

Agora, multiplicando-se ambos os membros da última igualdade por $S^{-1} \in \Gamma(1)$, obtemos que

$$\Gamma(1) = \Gamma_\vartheta I \cup \Gamma_\vartheta S^{-1} \cup \Gamma_\vartheta S^{-1}T.$$

Finalmente, como $[\Gamma(1) : \Gamma^0(2)] = 2 + 1 = 3$, e $\Gamma^0(2)$ e Γ_ϑ são conjugados (Lema 9), segue, pelo Lema 7, que I, S^{-1} e $S^{-1}T$ compõem, de fato, um conjunto completo de representantes distintos de $\Gamma(1)$ módulo Γ_ϑ. □

É interessante observar que, pelo corolário anterior, segue que Γ_ϑ é um subgrupo de índice 3 em $\Gamma(1)$. O subgrupo Γ_ϑ será útil no estudo das formas modulares de que trataremos neste material. Finalizamos esta seção com o seguinte resultado:

Teorema 11. *Seja p um número primo. Então $[\Gamma_0(p) : \Gamma_0(p^2)] = p$ e, como decomposição de $\Gamma_0(p)$ módulo $\Gamma_0(p^2)$, podemos tomar*

$$\Gamma_0(p) = \bigcup_{k=0}^{p-1} \Gamma_0(p^2) \begin{pmatrix} 1 & 0 \\ -pk & 1 \end{pmatrix}.$$

Demonstração. Primeiramente, notemos que, se $0 \leq k_1 < k_2 \leq p-1$, então

$$\begin{aligned} \begin{pmatrix} 1 & 0 \\ -pk_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -pk_2 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & 0 \\ -pk_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ pk_2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ p(k_2 - k_1) & 1 \end{pmatrix} \notin \Gamma_0(p^2), \end{aligned}$$

pois $p^2 \nmid p(k_2 - k_1)$. Logo, as p classes laterais de $\Gamma_0(p^2)$ são distintas, donde $[\Gamma_0(p) : \Gamma_0(p^2)] \geq p$. Deste modo, para provar a igualdade em questão, resta-nos fazê-lo com a inclusão $\Gamma_0(p) \subset \bigcup_{k=0}^{p-1} \Gamma_0(p^2) \begin{pmatrix} 1 & 0 \\ -pk & 1 \end{pmatrix}$, uma vez que a inclusão contrária é evidente. Assim, seja $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p)$, de modo que $p \mid c$. Logo, existe $\alpha \in \mathbb{Z}$ tal que $c = \alpha p$. Dividindo-se α por p, obtemos $\alpha = pt + u$, com $0 \leq u \leq |p| - 1 = p - 1$, aplicando-se o algoritmo de Euclides. Assim, $c = p(pt + u)$, com $0 \leq u \leq p - 1$. Como $ad - bc = 1$, vem que $(c, d) = 1$ (Teorema de Bèzout), donde $(p, d) = 1$, uma vez que $p \mid c$. Agora, observe que

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -pk & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} a & b \\ p(pt+u) & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ pk & 1 \end{pmatrix} \\ &= \begin{pmatrix} * & * \\ p(pt+u+dk) & * \end{pmatrix}. \end{aligned}$$

Sabemos que existe k compreendido entre 0 e $p-1$ tal que $dk \equiv -u \pmod{p}$, pois $(p,d) = 1|(-u)$, qualquer que seja u. Logo $p \mid u+dk$, donde $p(pt+u+dk) \equiv 0 \pmod{p^2}$. Neste caso, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -pk & 1 \end{pmatrix}^{-1} \in \Gamma_0(p^2)$, donde $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^2)\begin{pmatrix} 1 & 0 \\ -pk & 1 \end{pmatrix}^{-1} \subset \bigcup_{k=0}^{p-1}\Gamma_0(p^2)\begin{pmatrix} 1 & 0 \\ -pk & 1 \end{pmatrix}$, ficando provado o teorema. □

2.4 Regiões fundamentais segundo subgrupos

Lema 12. *Seja $V \in \Gamma(1)$. Se existe $\tau_0 \in \mathscr{R}(\Gamma(1))$ tal que $V(\tau_0) = \tau_0$, então $V = I$.*

Demonstração. Como V é contínua em $\mathscr{H}$, temos que V é contínua em τ_0. Portanto, dada uma vizinhança N_2 de $V(\tau_0) = \tau_0$ contida em $\mathscr{R}(\Gamma(1))$ (subconjunto aberto de $\mathscr{H}$), existe uma vizinhança N_1' de τ_0 tal que $V(N_1') \subset N_2 \subset \mathscr{R}(\Gamma(1))$. Por mera formalidade, podemos tomar $N_1 \subset N_1'$, sendo N_1 também vizinhança de τ_0 satisfazendo às condições $N_1 \subset N_2 \subset \mathscr{R}(\Gamma(1))$ e $V(N_1) \subset N_2 \subset \mathscr{R}(\Gamma(1))$. Neste caso, $V(\tau) = \tau$ para cada $\tau \in N_1$, uma vez que $\mathscr{R}(\Gamma(1))$ é região fundamental segundo $\Gamma(1)$, ou seja, $V = I$ para cada elemento da vizinhança N_1. Como V é regular em $\mathscr{H}$, segue que o mesmo é válido em todo esse domínio. □

Utilizando-se o lema anterior, podemos provar o seguinte teorema, um dos mais importantes deste capítulo:

Teorema 13. *Seja $\Gamma \leqslant \Gamma(1)$ tal que $\Gamma(1) = \bigcup_{i=1}^{\mu}\Gamma A_i$ é uma decomposição de $\Gamma(1)$ em classes laterais à direita de Γ. Então, como região fundamental segundo Γ, podemos tomar $\mathscr{R} = \bigcup_{i=1}^{\mu} A_i\{\mathscr{R}(\Gamma(1))\}$.*

Demonstração. Primeiro vamos provar que, em $\mathscr{R}$, não existem dois pontos distintos equivalentes em relação a Γ. Para tanto, consideremos $\tau_1, \tau_2 \in \mathscr{R}$ tais que $\tau_1 \sim_\Gamma \tau_2$. Como $\tau_1, \tau_2 \in \mathscr{R}$, podemos tomar $\tau_1 = A_i x$ e $\tau_2 = A_j y$, com $x, y \in \mathscr{R}(\Gamma(1))$ e $1 \leq i, j \leq \mu$. Além disso, como τ_1 e τ_2 são equivalentes com respeito a Γ, existe $M \in \Gamma$ tal que $\tau_2 = M\tau_1$, donde $A_j y = M(A_i x)$, ou $y = (A_j^{-1}MA_i)x$. Como $A_j^{-1}MA_i \in \Gamma(1)$ e $x, y \in \mathscr{R}(\Gamma(1))$, que é região fundamental de $\Gamma(1)$, devemos ter $x = y$ donde, pelo Lema 12, $A_j^{-1}MA_i = I$, ou $A_j A_i^{-1} = M \in \Gamma$. Finalmente, como os A's são distintos módulo Γ, segue que $i = j$, donde $\tau_1 = A_i x = A_j y = \tau_2$.

Agora, dado $\tau \in \mathscr{H}$, desejamos provar a existência de $\tau' \in \overline{\mathscr{R}}$ satisfazendo $\tau \sim_\Gamma \tau'$. Se $\tau \in \mathscr{H}$, então existe $x \in \overline{\mathscr{R}(\Gamma(1))}$ satisfazendo $\tau \sim_{\Gamma(1)} x$, isto é, existe $V \in \Gamma(1)$ tal que $\tau = Vx$. Além disso, como $\Gamma(1) = \bigcup_{i=1}^{\mu} \Gamma A_i$, existem $M \in \Gamma$ e i $(1 \leq i \leq \mu)$ tais que $V = MA_i$. Portanto $\tau = (MA_i)x$, ou $M^{-1}\tau = A_i x \in A_i \left\{\overline{\mathscr{R}(\Gamma(1))}\right\}$. Agora, como os A_i's são homeomorfismos, segue que $M^{-1}\tau = A_i x \in A_i \left\{\overline{\mathscr{R}(\Gamma(1))}\right\} = \overline{A_i\{\mathscr{R}(\Gamma(1))\}} \subset \bigcup_{i=1}^{\mu} \overline{A_i\{\mathscr{R}(\Gamma(1))\}} = \overline{\bigcup_{i=1}^{\mu} A_i\{\mathscr{R}(\Gamma(1))\}} = \overline{\mathscr{R}}$. Logo, existe $\tau' \in \overline{\mathscr{R}}$ tal que $M^{-1}\tau = \tau'$, donde $\tau = M\tau'$, com $M \in \Gamma$. Isto prova que $\tau \sim_\Gamma \tau'$, terminando a demonstração. □

Definição 3. *Uma região fundamental $\mathscr{R}$ segundo Γ como a estabelecida no teorema precedente, determinada a partir de $\mathscr{R}(\Gamma(1))$ e dos representantes das classes de equivalência da decomposição de $\Gamma(1)$ módulo Γ, recebe a denominação de* região fundamental padronizada *segundo Γ.*

É interessante observar que, de acordo com a definição, regiões fundamentais padronizadas segundo um determinado subgrupo Γ de $\Gamma(1)$ também não são únicas, uma vez que dependem dos representantes escolhidos para a decomposição de $\Gamma(1)$ módulo Γ. Sendo assim, a terminologia *padronizada* refere-se apenas à forma como essas regiões são construídas.

Os três corolários que vêm a seguir são interessantes aplicações do Teorema 13 a resultados anteriormente obtidos:

Corolário 14. *Como região fundamental de $\Gamma^0(p)$, p primo, podemos tomar*

$$\bigcup_{j=0}^{p-1} S^j\{\mathscr{R}(\Gamma(1))\} \cup T\{\mathscr{R}(\Gamma(1))\}.$$

Demonstração. Pelo Teorema 6, sabemos que

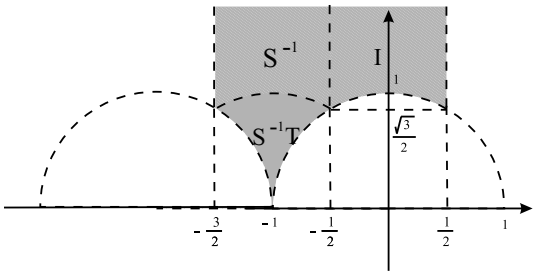
$$\Gamma(1) = \left(\bigcup_{j=0}^{p-1} \Gamma^0(p) S^j\right) \cup \Gamma^0(p) T.$$

Logo, o resultado desejado segue diretamente do Teorema 13. □

Corolário 15. *Como região fundamental segundo Γ_ϑ, podemos tomar*

$$\mathscr{R}(\Gamma(1)) \cup S^{-1}\{\mathscr{R}(\Gamma(1))\} \cup S^{-1}T\{\mathscr{R}(\Gamma(1))\},$$

representada por:



onde I, S^{-1} e $S^{-1}T$ representam as regiões obtidas ao se aplicar tais elementos no conjunto $\mathscr{R}(\Gamma(1))$.

Demonstração. Pelo Corolário 10, I, S^{-1} e $S^{-1}T$ representam três classes laterais distintas de Γ_ϑ cuja união resulta $\Gamma(1)$. Logo, o resultado segue do Teorema 13. □

Corolário 16. *Sejam Γ_1 e Γ_2 subgrupos conjugados de $\Gamma(1)$, com $B\Gamma_1 B^{-1} = \Gamma_2$, $B \in \Gamma(1)$. Se $\mathscr{R}_1$ é uma região fundamental padronizada segundo Γ_1, então $\mathscr{R}_2 = B(\mathscr{R}_1)$ é região fundamental padronizada segundo Γ_2.*

Demonstração. Na demonstração do Lema 7, concluímos que, se $A_1, A_2, \ldots, A_\mu$ é um conjunto completo de representantes distintos de $\Gamma(1)$ módulo Γ_1, então $BA_1, BA_2, \ldots, BA_\mu$ é um conjunto completo de representantes distintos de $\Gamma(1)$ módulo Γ_2, dado que Γ_1 e Γ_2 são conjugados. Desta maneira, suponhamos que os representantes acima sejam aqueles para os quais $\mathscr{R}_1 = \bigcup_{i=1}^{\mu} A_i\{\mathscr{R}(\Gamma(1))\}$. Então, uma possível região fundamental padronizada segundo Γ_2 é

$$\bigcup_{i=1}^{\mu}(BA_i)\{\mathscr{R}(\Gamma(1))\} = B\left(\bigcup_{i=1}^{\mu} A_i\{\mathscr{R}(\Gamma(1))\}\right) = B(\mathscr{R}_1) = \mathscr{R}_2,$$

como queríamos demonstrar. □

Finalizamos este capítulo com um importante teorema, o qual, de certa forma, generaliza a idéia de região fundamental padronizada segundo subgrupos:

Teorema 17. *Sejam $\Gamma_2 \leqslant \Gamma_1 \leqslant \Gamma(1)$. Se $\mathscr{R}_1$ é uma região fundamental padronizada segundo Γ_1 e se $\Gamma_1 = \bigcup_{i=1}^{\mu} \Gamma_2 A_i$ é uma decomposição de Γ_1 em classes laterais distintas de Γ_2, então $\mathscr{R}_2 = \bigcup_{i=1}^{\mu} A_i(\mathscr{R}_1)$ é uma região fundamental padronizada segundo Γ_2.*

Demonstração. Repetindo-se os argumentos utilizados na demonstração do Teorema 13 para Γ_1 no lugar de $\Gamma(1)$ e Γ_2 no lugar de Γ, concluimos que $\mathscr{R}_2$ é uma região fundamental segundo Γ_2. Resta-nos, pois, provar que ela é padronizada. Como $\mathscr{R}_1$ é região

fundamental padronizada segundo Γ_1, podemos supor $\mathscr{R}_1 = \bigcup_{j=1}^{\nu} B_j\{\mathscr{R}(\Gamma(1))\}$, sendo $\Gamma(1) = \bigcup_{j=1}^{\nu} \Gamma_1 B_j$ a decomposição que torna $\mathscr{R}_1$ padronizada. Portanto, temos

$$\mathscr{R}_2 = \bigcup_{i=1}^{\mu} A_i(\mathscr{R}_1) = \bigcup_{i=1}^{\mu} A_i \left(\bigcup_{j=1}^{\nu} B_j\{\mathscr{R}(\Gamma(1))\} \right) = \bigcup_{i=1}^{\mu}\bigcup_{j=1}^{\nu} (A_iB_j)\{\mathscr{R}(\Gamma(1))\}.$$

Agora, afirmamos que $\Gamma(1) = \bigcup_{i=1}^{\mu}\bigcup_{j=1}^{\nu} \Gamma_2(A_iB_j)$ é uma decomposição de $\Gamma(1)$ em $\mu\nu$ classes laterais distintas módulo Γ_2. De fato,

$$\Gamma(1) = \bigcup_{j=1}^{\nu} \Gamma_1 B_j = \bigcup_{j=1}^{\nu} \left(\bigcup_{i=1}^{\mu} \Gamma_2 A_i \right) B_j = \bigcup_{i=1}^{\mu}\bigcup_{j=1}^{\nu} \Gamma_2(A_iB_j),$$

de modo que vale a igualdade. Deste modo, só nos resta provar que os $\mu\nu$ elementos do conjunto $C = \{A_iB_j \mid 1 \leq i \leq \mu, 1 \leq j \leq \nu\}$ são distintos módulo Γ_2. Para tanto, suponhamos que A_iB_j e A_kB_l estejam na mesma classe lateral de Γ_2. Neste caso, $A_iB_j(A_kB_l)^{-1} = A_iB_jB_l^{-1}A_k^{-1} \in \Gamma_2$, donde $B_jB_l^{-1} \in A_i^{-1}\Gamma_2A_k \subset \Gamma_1$. Como os B's são distintos módulo Γ_1, segue que $j = l$, donde $A_iA_k^{-1} \in \Gamma_2$. Agora, como os A's são distintos módulo Γ_2, tem-se que $i = k$. Portanto, $A_iB_j = A_kB_l$, donde os elementos do conjunto C são distintos módulo Γ_2, ficando provado o teorema. □

Capítulo 3

Formas e funções modulares

3.1 Sistema multiplicador

Para bem compreendermos as definições não triviais de forma modular e de função modular (tipo específico de forma modular), alguns conceitos prévios deverão ser esclarecidos. Para o desenvolvimento que segue, Γ denotará um subgrupo de índice finito em $\Gamma(1)$, o grupo modular.

Para que uma função F seja considerada forma modular de grau $-r$ (ou de peso/dimensão r, $r \in \mathbb{R}$), com respeito a Γ, ela deve ser definida e meromorfa em $\mathscr{H}$, e satisfazer a seguinte equação funcional

$$F(M\tau) = \upsilon(M)(c\tau + d)^r F(\tau), \qquad \tau \in \mathscr{H}, \tag{3.1}$$

para cada $M = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma$, sendo υ uma função que associa a cada M (visto como matriz) um número complexo que possui módulo igual a 1, ou seja, $|\upsilon(M)| = 1$ para cada $M \in \Gamma$ (os coeficientes de M indicados por * são irrelevantes para os nossos atuais objetivos). Na equação (3.1), aparece o termo complexo $(c\tau + d)^r$. Como usual em variáveis complexas, para $z \in \mathbb{C}$, adotaremos a convenção de que

$$z^r = |z|^r e^{ir\arg(z)}, \qquad -\pi \leq \arg(z) < \pi. \tag{3.2}$$

Agora, estabeleceremos uma importante condição de consistência para a função υ. Para tanto, suponhamos que exista $\tau \in \mathscr{H}$ tal que $F(\tau) \neq 0$, e definamos $M_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in$

Γ, para $i = 1, 2, 3$ e $M_3 = M_1 M_2$. Desse modo,

$$\begin{aligned} \upsilon(M_3)(c_3\tau + d_3)^r F(\tau) &= F(M_3\tau) \\ &= F(M_1(M_2\tau)) \\ &= \upsilon(M_1)(c_1(M_2\tau) + d_1)^r F(M_2\tau) \\ &= \upsilon(M_1)(c_1 M_2\tau + d_1)^r \upsilon(M_2)(c_2\tau + d_2)^r F(\tau), \end{aligned}$$

de tal maneira que, se $F(\tau) \neq 0$, tem-se que

$$\upsilon(M_3)(c_3\tau + d_3)^r = \upsilon(M_1)\upsilon(M_2)(c_1 M_2\tau + d_1)^r (c_2\tau + d_2)^r. \tag{3.3}$$

Note, ainda, que

$$M_3 = M_1 M_2 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix},$$

de modo que $c_3 = c_1 a_2 + d_1 c_2$ e $d_3 = c_1 b_2 + d_1 d_2$. Portanto,

$$c_3\tau + d_3 = (c_1 a_2 + d_1 c_2)\tau + c_1 b_2 + d_1 d_2,$$

donde, caso r seja inteiro,

$$\begin{aligned} (c_1 M_2\tau + d_1)^r (c_2\tau + d_2)^r &= \left(c_1 \left(\frac{a_2\tau + b_2}{c_2\tau + d_2} \right) + d_1 \right)^r (c_2\tau + d_2)^r \\ &= \left(\frac{(c_1 a_2 + d_1 c_2)\tau + c_1 b_2 + d_1 d_2}{c_2\tau + d_2} \right)^r (c_2\tau + d_2)^r \\ &= \frac{((c_1 a_2 + d_1 c_2)\tau + c_1 b_2 + d_1 d_2)^r}{(c_2\tau + d_2)^r} (c_2\tau + d_2)^r \\ &= (c_3\tau + d_3)^r. \end{aligned}$$

Em geral,

$$\left(\frac{z_1}{z_2} \right)^r = \frac{z_1^r}{z_2^r} e^{2\pi i n r},$$

para algum inteiro n. Torna-se evidente, desta forma, que, quando r é inteiro, o expoente da fração é igual à fração dos expoentes, ou seja, $\left(\frac{z_1}{z_2}\right)^r = \frac{{z_1}^r}{{z_2}^r}$, fato que utilizamos na penúltima das passagens acima. Logo, nesse caso, o cancelamento na igualdade (3.3) conduz à identidade $\upsilon(M_1 M_2) = \upsilon(M_1)\upsilon(M_2)$ (os termos cancelados serem não nulos segue do fato de que as matrizes consideradas são elementos de $\Gamma(1)$). Entre outras conseqüências disso, temos que, quando r é inteiro, então υ é um caráter associado ao subgrupo Γ.

Existem diversos estudos sobre formas modulares de grau inteiro e, mesmo nesse caso, elas são subdivididas nos graus par e ímpar. Obviamente, nesses casos particulares, existem mais propriedades do que no caso geral. Entretanto, pelos nossos objetivos, faremos uma abordagem tão geral quanto possível de formas modulares.

Voltando ao assunto principal desta seção, estamos em condições de compreender a seguinte definição:

Definição 1. *A função complexa υ que aparece em (3.1) e satisfaz a condição de consistência explicitada por (3.3) recebe o nome de* sistema multiplicador *de grau $-r$ para o subgrupo Γ.*

Observações:

1. Após a equação (3.1), comentamos que υ é uma função do grupo de matrizes associado a Γ. Com isso, queremos dizer que, embora as matrizes $M \in \Gamma$ e $-M \in \Gamma$, como transformações lineares fracionárias, sejam o mesmo elemento, podemos ter $\upsilon(M) \neq \upsilon(-M)$. Isto pode ser facilmente verificado aplicando-se a relação (3.3) para $M_1 = M_2 = I$ e, em seguida, para $M_1 = M_2 = -I$. No primeiro caso, temos

$$\upsilon(I \cdot I)(0\tau + 1)^r = \upsilon(I)\upsilon(I)(0\tau + 1)^r(0\tau + 1)^r,$$

donde $\upsilon(I) = [\upsilon(I)]^2$ e, portanto, $\upsilon(I) = 1$, uma vez que $\upsilon(I) \neq 0$. No segundo, temos

$$\upsilon((-I) \cdot (-I))(0\tau + 1)^r = \upsilon(-I)\upsilon(-I)(0\tau - 1)^r(0\tau - 1)^r,$$

donde $\upsilon(I) = (-1)^{2r}[\upsilon(-I)]^2 = (e^{-\pi i})^{2r}[\upsilon(-I)]^2$, ou $[\upsilon(-I)]^2 = e^{2\pi ir}$. Logo, se r não for inteiro, então $\upsilon(-I) \neq 1 = \upsilon(I)$.

2. Se existir τ tal que $F(\tau) \neq 0$, para alguma função F como a exibida em (3.1), então $\upsilon(I) = 1$ e $\upsilon(-I) = e^{\pi ir}$. De fato, basta que apliquemos (3.1) para $M = I$ e também para $M = -I$, supondo que $F(\tau) \neq 0$. No primeiro caso, $F(\tau) = F(I\tau) = \upsilon(I)(0\tau + 1)^r F(\tau)$, donde $\upsilon(I) = 1$ e, no segundo, $F(\tau) = F(-I\tau) = \upsilon(-I)(0\tau - 1)^r F(\tau)$, donde $\upsilon(-I) = e^{\pi ir}$.
   Agora, utilizando-se (3.3) para $M_1 = -I$ e $M_2 = M \in \Gamma$, obtemos a seguinte

relação:

$$\begin{aligned} \upsilon(-M)(-c\tau-d)^r &= \upsilon(-IM)(-c\tau-d)^r \\ &= \upsilon(-I)\upsilon(M)(0\tau-1)^r(c\tau+d)^r \\ &= e^{\pi ir}\upsilon(M)e^{-\pi ir}(c\tau+d)^r \\ &= \upsilon(M)(c\tau+d)^r. \end{aligned}$$

3.2 Pontos parabólicos

Iniciamos com a definição do importante conceito que dá nome a esta seção:

Definição 2. *Seja $\mathscr{R}$ uma região fundamental segundo Γ. Um* ponto parabólico *(ou vértice parabólico, ou cúspide parabólica) de Γ em $\mathscr{R}$ é qualquer ponto de $\mathbb{R}\cup\{\infty\}$ pertencente a $\overline{\mathscr{R}}$.*

Observações:

1. Na definição acima, $\mathbb{R}$ é o eixo real, isto é, o conjunto dos complexos $z = x + iy$ tais que $y = 0$, e ∞ deve ser visto como um ponto no infinito em relação ao eixo imaginário positivo, sendo usualmente denotado por $i\infty$.

2. A partir de agora, adotaremos a convenção de que $\infty = 1/0$ é um ponto racional. Se $\mathscr{R}$ for uma região fundamental padronizada de Γ, como a construída no Teorema 13 do Capítulo 2, então todos os pontos parabólicos de Γ em $\mathscr{R}$ são números racionais. De fato, pela observação anterior e pelo Teorema 2 do Capítulo 2, o único ponto de $\mathbb{R}\cup\{\infty\}$ pertencente a $\overline{\mathscr{R}(\Gamma(1))}$ é o ponto ∞. Além disso,

$$\overline{\mathscr{R}} = \overline{\bigcup_{i=1}^{\mu} A_i\{\mathscr{R}(\Gamma(1))\}} = \bigcup_{i=1}^{\mu} A_i\left\{\overline{\mathscr{R}(\Gamma(1))}\right\}.$$

   No Capítulo 2, pela igualdade (2.2), concluimos que os elementos de $\Gamma(1)$ preservam os semiplanos superior e inferior e o eixo real $\mathbb{R}$. Pela mesma igualdade, podemos concluir que os elementos de $\Gamma(1)$ também preservam o elemento ∞. Logo, os únicos pontos parabólicos de Γ em $\mathscr{R}$ são os pontos $A_i(\infty)$, para $1 \leq i \leq \mu$, que são números racionais, dado que os A's são transformações lineares fracionárias de coeficientes inteiros. Evidencia-se nesta propriedade um bom motivo para se trabalhar com regiões fundamentais padronizadas.

3. Na observação anterior, vimos que os únicos pontos parabólicos de Γ em $\mathscr{R}$ são os pontos $A_1(\infty), A_2(\infty), \ldots, A_\mu(\infty)$, os quais denotaremos freqüentemente $q_i = A_i(\infty)$, para $1 \leq i \leq \mu$. Como veremos em exemplos futuros, estes pontos não são necessariamente distintos, isto é, pode ocorrer que existam $i \neq j$ $(1 \leq i, j \leq \mu)$ tais que $q_i = q_j$. Neste caso, $A_i(\infty) = A_j(\infty)$, ou $A_j^{-1}A_i(\infty) = \infty$. Como já vimos no Capítulo 2, $\Gamma(1)$ é gerado por S e T, donde $A_j^{-1}A_i \in \Gamma(1)$ deve se expressar como um produto finito de termos da forma T^ε e S^δ, sendo $\varepsilon = \pm 1$ e $\delta = \pm 1$. Para que $A_j^{-1}A_i(\infty) = \infty$, não deve aparecer, na expressão de $A_j^{-1}A_i$, nenhum termo da forma T^ε, pois $T(\infty) = -1/\infty = 0$ e $T^{-1}(\infty) = 1/(-\infty) = 0$. Logo, $A_j^{-1}A_i = S^n$, para algum inteiro n, donde segue que $A_i = A_j S^n$. Embora trivial, este resultado será utilizado para demonstrar o Lema 1, que nos será de grande utilidade.

Para se fixar o seguinte lema, procure interpretá-lo geometricamente:

Lema 1. *Seja $\mathscr{R} = \bigcup_{i=1}^{\mu} A_i\{\mathscr{R}(\Gamma(1))\}$ uma região fundamental padronizada segundo Γ e $q_i = A_i(\infty)$ $(1 \leq i \leq \mu)$ os pontos parabólicos de Γ em tal região. Se $\tau \to q_i$ a partir de pontos de $\mathscr{R}$, então $A_i^{-1}(\tau) \to \infty$ a partir de pontos de uma faixa vertical da forma $\mathfrak{Im}(z) > 0$, $a_i < \mathfrak{Re}(z) < b_i$, onde $a_i, b_i \in \mathbb{R}$.*

Demonstração. Como $\tau \to q_i = A_i(\infty)$, então $A_i^{-1}(\tau) \to A_i^{-1}(A_i(\infty)) = \infty$, uma vez que A_i é contínua. Resta-nos, então, provar que tal convergência ocorre da maneira determinada pelo enunciado do lema. Para tanto, suponhamos que $\tau \to q_i$ de dentro de $\mathscr{R}$ e, num primeiro momento, suponhamos $q_i \neq \infty$. Na topologia que consideramos (a saber, a topologia da esfera de Riemann), as vizinhanças dos pontos $q_i \neq \infty$ são discos abertos D centrados em q_i. Como $\tau \to q_i$ de dentro de $\mathscr{R}$ e $q_i \in \overline{\mathscr{R}}$, podemos tomar D pequeno o bastante de modo que

$$D \cap \mathscr{R} = D \cap \left(\bigcup_{\nu \in \sigma(i)} A_\nu\{\mathscr{R}(\Gamma(1))\} \right),$$

sendo $\sigma(i) = \{\nu \mid 1 \leq \nu \leq \mu \text{ e } A_\nu(\infty) = A_i(\infty), \text{ i.e., } q_\nu = q_i\}$. Agora, pela Observação 3 que precede este lema, para cada $\nu \in \sigma(i)$, existe um inteiro $n(\nu)$ tal que $A_\nu = A_i S^{n(\nu)}$, donde, a partir do momento que os elementos τ se encontrarem dentro de $D \cap \mathscr{R}$, os

elementos $A_i^{-1}(\tau)$ se encontrarão em

$$\begin{aligned} A_i^{-1}(D \cap \mathscr{R}) &= A_i^{-1}(D) \cap A_i^{-1}\left(\bigcup_{\nu\in\sigma(i)} A_i S^{n(\nu)}\{\mathscr{R}(\Gamma(1))\}\right) \\ &= A_i^{-1}(D) \cap \left(\bigcup_{\nu\in\sigma(i)} S^{n(\nu)}\{\mathscr{R}(\Gamma(1))\}\right), \end{aligned}$$

conjunto este que pode ser sempre delimitado numa faixa da forma considerada no enunciado. O caso $q_i = \infty$ possui tratamento análogo, sendo a única diferença os tipos de vizinhança considerados. Neste caso, de acordo com a topologia usual da esfera de Riemann, as vizinhanças D serão semiplanos da forma $\mathfrak{Im}(z) > y_0$ unidos a ∞, com $y_0 > 0$, e a prova segue da mesma forma. □

Exemplos

Nos seguintes exemplos, veremos como se encontram, na prática, os pontos parabólicos associados a uma certa região fundamental padronizada.

1. Pelo Corolário 10 do Capítulo 2, I, S^{-1} e $S^{-1}T$ são os representantes distintos da decomposição de $\Gamma(1)$ em classes laterais de Γ_ϑ. Logo, os pontos parabólicos de Γ_ϑ na região fundamental padronizada relativa a essa decomposição são $I(\infty) = \infty$, $S^{-1}(\infty) = \infty - 1 = \infty$ e $S^{-1}T(\infty) = S^{-1}(-1/\infty) = S^{-1}(0) = 0 - 1 = -1$. Logo, os pontos parabólicos são ∞ e -1. Este exemplo também ilustra o fato que comentamos na Observação 3 precedente ao Lema 1, qual seja, o de existirem dois representantes distintos na decomposição que conduzam ao mesmo ponto parabólico. Neste caso, $I(\infty) = S^{-1}(\infty)$.

2. Pelo Corolário 8 do Capítulo 2, os pontos parabólicos de $\Gamma_0(p)$ referentes à região fundamental padronizada associada à tal decomposição, são os pontos $TS^j(\infty) = T(\infty) = 0$ e $I(\infty) = \infty$.

O próximo lema é importante porque dá sentido à definição de *largura* de pontos parabólicos:

Lema 2. *Seja q um ponto racional e considere $\Gamma_q = \{M \in \Gamma \mid M(q) = q\}$, sendo $\Gamma \leqslant \Gamma(1)$. Então Γ_q é um subgrupo cíclico não trivial de Γ e, ademais, todo elemento $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_q$ é tal que $\alpha + \delta = 2$.*

Demonstração. Para mostrarmos que $\Gamma_q \leqslant \Gamma$, basta mostrarmos as duas seguintes propriedades:

1. Se $M_1, M_2 \in \Gamma_q$, então $M_1 \circ M_2 \in \Gamma_q$;
   Se $M_1, M_2 \in \Gamma_q$, é claro que $M_1 \circ M_2 \in \Gamma$ e, além disso, $M_1 \circ M_2(q) = M_1(M_2(q)) = M_1(q) = q$, donde $M_1 \circ M_2 \in \Gamma_q$.

2. Se $M \in \Gamma_q$, então $M^{-1} \in \Gamma_q$.
   Se $M \in \Gamma_q$, é claro que $M^{-1} \in \Gamma$ e, além disso, $M(q) = q$, donde $M^{-1}(M(q)) = M^{-1}(q)$. Logo, $M^{-1}(q) = M^{-1} \circ M(q) = I(q) = q$, donde $M^{-1} \in \Gamma_q$.

Já sabemos, então, que Γ_q é subgrupo de Γ. Agora, afirmamos que existe um inteiro positivo n tal que $S^n \in \Gamma$. De fato, caso isso não ocorresse para nenhum inteiro positivo n, os elementos $S, S^2, S^3, \ldots$, constituiriam infinitos elementos distintos módulo Γ, donde Γ possuiria índice infinito em $\Gamma(1)$, contradizendo nossa convenção.

Para $q = \infty$, temos de mostrar que Γ_∞ é cíclico não trivial. Como vimos no parágrafo anterior, existe um inteiro positivo n tal que $S^n \in \Gamma$. Afirmamos que $S^n \in \Gamma_\infty$ e que $\Gamma_\infty = \langle S^n \rangle$. De fato, em primeiro lugar, $S^n(\infty) = \infty + n = \infty$, donde Γ_∞ é não trivial. Em segundo lugar, suponhamos $M \in \Gamma_\infty$. Neste caso, $M(\infty) = \infty$, donde $M = S^\lambda$ (reveja a Observação 3 que precede o Lema 1). Se $\lambda = 0$, então $M = S^0 = I \in \langle S^n \rangle$. Se $\lambda > 0$, então podemos dividir λ por n, obtendo $\lambda = nt + r$, sendo $0 \leq r < n$ (Algoritmo de Euclides). Neste caso,

$$S^\lambda = S^{nt+r} = (S^n)^t S^r.$$

Como $S^\lambda, S^n \in \Gamma_\infty$, segue que $S^r \in \Gamma_\infty \leqslant \Gamma$ e, pela definição de n, temos $r = 0$, donde $S^\lambda = (S^n)^t \in \langle S^n \rangle$. Agora, se $\lambda < 0$, então $M^{-1} = S^{-\lambda}$, com $-\lambda > 0$ e $M^{-1} \in \Gamma_\infty$. Pelo caso $\lambda > 0$, temos $M^{-1} = (S^n)^t$, ou $M = (S^n)^{-t}$, como queríamos. Logo, Γ_∞ é, de fato, cíclico.

Agora, suponhamos $q \neq \infty$, ou seja, $q = a/b$, com a e b inteiros coprimos e $b \neq 0$. Pelo Teorema de Bèzout, existem $x, y \in \mathbb{Z}$ tais que $-ax - by = 1$ e, portanto, $V = \begin{pmatrix} x & y \\ b & -a \end{pmatrix} \in \Gamma(1)$ é tal que

$$V(q) = V(a/b) = \frac{x(a/b) + y}{b(a/b) - a} = \frac{(ax + by)/b}{0} = \frac{-1/b}{0} = \infty.$$

Agora, temos $V\Gamma_q V^{-1} = \{VMV^{-1} \in V\Gamma V^{-1} \mid M(q) = q\}$ e, como $V(q) = \infty$,

$$VMV^{-1}(\infty) = V(M(V^{-1}(\infty))) = V(M(q)) = V(q) = \infty,$$

donde

$$V\Gamma_q V^{-1} = \{VMV^{-1} \in V\Gamma V^{-1} \mid VMV^{-1}(\infty) = \infty\},$$

ou seja, $V\Gamma_q V^{-1}$ é o subgrupo de $V\Gamma V^{-1}$ que possui ∞ como ponto fixo. Pelo mesmo raciocínio do caso Γ_∞, segue que $V\Gamma_q V^{-1}$ é subgrupo cíclico não trivial de $V\Gamma V^{-1}$, isto é, existe um inteiro positivo $n(q)$ tal que $V\Gamma_q V^{-1} = \left\langle S^{n(q)} \right\rangle$ (a notação $n(q)$ para o determinado inteiro se justifica pelo fato dele variar de acordo com o racional $q \neq \infty$). Agora, observamos que Γ_q é também não trivial pois, caso contrário, $V\Gamma_q V^{-1}$ seria trivial. Finalmente, para cada $M \in \Gamma_q$, existe $t \in \mathbb{Z}$ tal que $VMV^{-1} = \left(S^{n(q)}\right)^t$. Logo,

$$M = V^{-1}\left(S^{n(q)}\right)^t V = \left(V^{-1}S^{n(q)}V\right)^t,$$

ou seja, $\Gamma_q = \left\langle V^{-1}S^{n(q)}V \right\rangle$ é cíclico.

Com relação à asserção do lema segundo a qual cada elemento de Γ_q, como matriz, possui traço igual a 2, se $q = \infty$, então cada elemento de Γ_∞ é da forma

$$M = (S^n)^t = S^{nt} = \begin{pmatrix} 1 & nt \\ 0 & 1 \end{pmatrix},$$

e $1 + 1 = 2$. Por outro lado, se $q \neq \infty$, cada elemento de Γ_q é da forma

$$\begin{aligned} M &= V^{-1}S^{n(q)t}V \\ &= \begin{pmatrix} -a & -y \\ -b & x \end{pmatrix}\begin{pmatrix} 1 & n(q)t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & y \\ b & -a \end{pmatrix} \\ &= \begin{pmatrix} -a & -an(q)t - y \\ -b & -bn(q)t + x \end{pmatrix}\begin{pmatrix} x & y \\ b & -a \end{pmatrix} \\ &= \begin{pmatrix} -ax - abn(q)t - by & -ay + a^2n(q)t + ay \\ -bx - b^2n(q)t + bx & -by + abn(q)t - ax \end{pmatrix} \\ &= \begin{pmatrix} 1 - abn(q)t & a^2n(q)t \\ -b^2n(q)t & 1 + abn(q)t \end{pmatrix}, \end{aligned}$$

e $(1 - abn(q)t) + (1 + abn(q)t) = 2$, finalizando a demonstração.

De modo mais simples, a última conclusão poderia também ter sido obtida observando-se que

$$\mathrm{tr}(V^{-1}S^{n(q)t}V) = \mathrm{tr}(S^{n(q)t}VV^{-1}) = \mathrm{tr}(S^{n(q)t}) = 1 + 1 = 2,$$

onde $\mathrm{tr}(A)$ denota o *traço* da matriz quadrada A, ou seja, a soma dos elementos de sua diagonal principal, operador este que obedece à seguinte propriedade, para cada par de matrizes A e B: $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. □

Observações:

1. Uma matriz ou transformação linear fracionária $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ tal que $\alpha+\delta = \pm 2$ recebe o nome de parabólica. Na Observação 2 precedente ao Lema 1, vimos que todo ponto parabólico de Γ em $\mathscr{R}$, sendo $\Gamma \leqslant \Gamma(1)$ e $\mathscr{R}$ uma região fundamental padronizada segundo Γ, é ponto racional e, pelo lema anterior, associado a cada ponto racional q, temos um subgrupo cíclico infinito Γ_q (infinito porque $S^\lambda \neq I$ para cada inteiro não nulo λ). Assim, todo ponto parabólico de Γ segundo $\mathscr{R}$ é mantido fixo por um subgrupo cíclico infinito cujos elementos são também parabólicos.

2. Na demonstração do lema anterior, utilizamos a notação $n(q)$ $(q \neq \infty)$ para indicar o menor inteiro positivo tal que $S^{n(q)} \in V\Gamma V^{-1}$, e $n = n(\infty)$ para indicar o menor inteiro positivo tal que $S^{n(\infty)} \in \Gamma$. No caso $n(\infty)$, fica evidente que tal valor depende apenas de Γ, mas no caso $n(q)$, $q \neq \infty$, poder-se-ia perguntar se tal valor não depende do elemento $V \in \Gamma(1)$ satisfazendo $V(q) = \infty$. Para responder esta questão, suponhamos $V_1, V_2 \in \Gamma(1)$ tais que $V_1(q) = \infty = V_2(q)$. Neste caso, $V_2V_1^{-1}(\infty) = V_2(q) = \infty$, donde $V_2V_1^{-1} = S^\lambda$, ou $V_2 = S^\lambda V_1$, para algum inteiro λ. Logo, $V_2\Gamma V_2^{-1} = S^\lambda V_1 \Gamma V_1^{-1} S^{-\lambda}$, donde, se $M \in \Gamma_q$, $V_1 M V_1^{-1}(\infty) = \infty$ se, e somente se, $V_2 M V_2^{-1}(\infty) = \infty$. Logo, $V_1\Gamma_q V_1^{-1} = V_2\Gamma_q V_2^{-1}$, donde, pela demonstração do lema, $n(q)$ independe de $V \in \Gamma(1)$, desde que $V(q) = \infty$.

   Pelo que comentamos no parágrafo anterior, podemos definir, para todo racional q (incluindo-se o caso $q = \infty$), $n(q)$ como sendo o menor inteiro positivo tal que $S^{n(q)} \in V\Gamma V^{-1}$, para $V(q) = q$ (no caso $q = \infty$, podemos tomar $V = I$, por exemplo).

3. Se $\Gamma(1) = \bigcup_{j=1}^{\mu} \Gamma A_j$ é a decomposição de $\Gamma(1)$ em μ classes laterais distintas de Γ, sabemos que os pontos parabólicos de Γ na região fundamental padronizada associada a essa decomposição são os pontos racionais $q_j = A_j(\infty)$, $1 \leq j \leq \mu$. Ora, neste caso, $A_j^{-1} \in \Gamma(1)$ é tal que $A_j^{-1}(q_j) = \infty$.

As observações anteriores motivam a seguinte definição:

Definição 3. *Se $q_j = A_j(\infty)$, $1 \leq j \leq \mu$, são os pontos parabólicos de Γ numa região fundamental padronizada segundo Γ, consideremos $n(q_j) = \lambda_j$ como os menores inteiros positivos tais que $S^{\lambda_j} \in A_j^{-1}\Gamma A_j$. Denominamos λ_j a* largura *do ponto parabólico q_j.*

De acordo com as observações precedentes a essa definição, o conceito de largura de um ponto parabólico está bem definido, dependendo unicamente do ponto em questão, de tal maneira que, se $q_i = q_j$, então $\lambda_i = \lambda_j$.

Exemplo: Como exemplo de aplicação da definição acima, consideremos o subgrupo Γ_ϑ de $\Gamma(1)$. Pelo Exemplo 2 que vem após o Lema 1, os pontos parabólicos de Γ_ϑ na região fundamental padronizada lá considerada são $q_1 = q_2 = \infty$ e $q_3 = -1$. Os representantes associados aos pontos q_1 e q_2 são, respectivamente, I e S^{-1}. Pela definição anterior, λ_1 é o menor inteiro positivo tal que $S^{\lambda_1} \in I^{-1}\Gamma_\vartheta I = \Gamma_\vartheta$. Como $S \notin \Gamma_\vartheta$ e $S^2 \in \Gamma_\vartheta$, temos $\lambda_1 = 2$. Pelo que comentamos antes deste exemplo, $\lambda_2 = \lambda_1 = 2$. Finalmente, como o representante associado ao ponto q_3 é $S^{-1}T$, temos que λ_3 é o menor inteiro positivo tal que

$$\begin{aligned} S^{\lambda_3} \in (S^{-1}T)^{-1}\Gamma_\vartheta(S^{-1}T) &= T^{-1}(S\Gamma_\vartheta S^{-1})T \\ &= T^{-1}\Gamma^0(2)T \\ &= \Gamma_0(2), \end{aligned}$$

utilizando, respectivamente, o Lema 9 do Capítulo 2 e a relação que também lá comentamos após a Definição 2, qual seja, o fato de que, para n inteiro positivo, $T^{-1}\Gamma^0(n)T = \Gamma_0(n)$. Agora, como $S \in \Gamma_0(2)$, vem que $\lambda_3 = 1$.

Na seqüência, temos uma interessante proposição, que estabelece uma espécie de invariância da largura de pontos parabólicos:

Proposição 3. *Suponha que*

$$\mathscr{R} = \bigcup_{j=1}^{\mu} A_j\{\mathscr{R}(\Gamma(1))\} \text{ e } \mathscr{R}' = \bigcup_{j=1}^{\mu} A'_j\{\mathscr{R}(\Gamma(1))\}$$

sejam duas regiões fundamentais padronizadas segundo $\Gamma \leqslant \Gamma(1)$*, onde* A_j *e* A'_j *são representantes da mesma classe de equivalência de* Γ *em* $\Gamma(1)$*, para cada* j*,* $1 \leq j \leq \mu$*. Sejam* q_j *os pontos parabólicos de* Γ *em* $\mathscr{R}$*, cada um com largura* λ_j*. Se denotarmos* λ'_j *as larguras dos pontos parabólicos* q'_j*, de* Γ *em* $\mathscr{R}'$*, então* $\lambda_j = \lambda'_j$*, para cada* j*,* $1 \leq j \leq \mu$*.*

Demonstração. Para cada j, como $A'_j \in \Gamma A_j$, existe $W \in \Gamma$ tal que $A'_j = WA_j$, de modo que $(A'_j)^{-1}\Gamma(A'_j) = (WA_j)^{-1}\Gamma(WA_j) = A_j^{-1}(W^{-1}\Gamma W)A_j = A_j^{-1}\Gamma A_j$. Assim, pela própria definição de largura de um ponto parabólico, temos, imediatamente, que $\lambda_j = \lambda'_j$. □

A proposição acima implica que a largura de pontos parabólicos é invariante com relação a classes de equivalência, i.e., valendo-nos da demonstração acima, se q é um ponto parabólico de Γ em $\mathscr{R}$, então $q' = W(q)$ é ponto parabólico de Γ em $\mathscr{R}'$, sendo iguais as larguras de q e q'.

3.3 Expansões de Fourier

De agora em diante, fixemos uma região fundamental padronizada $\mathscr{R} = \bigcup_{i=1}^{\mu} A_i\{\mathscr{R}(\Gamma(1))\}$ segundo Γ, referente à decomposição $\Gamma(1) = \bigcup_{i=1}^{\mu} \Gamma A_i$. Além disso, sejam $q_j = A_j(\infty)$, $1 \leq j \leq \mu$, os pontos parabólicos de Γ em $\mathscr{R}$. O principal resultado que apresentaremos nesta seção é que, se $F(\tau)$ é meromorfa em $\mathscr{H}$, satisfaz a relação (3.1) para todo $M \in \Gamma$ e possui um número finito de pólos em $\overline{\mathscr{R}} \cap \mathscr{H}$, então $F(\tau)$ apresenta-se como uma série infinita nos pontos parabólicos de Γ em $\mathscr{R}$. Tais expansões serão chamadas "expansões de Fourier" que, como veremos, possuem estreita relação com as conhecidas séries de Laurent. Antes de enunciar e demonstrar esse importante resultado, porém, daremos uma definição e provaremos um lema, ambos imprescindíveis aos nossos objetivos:

Definição 4. *Seja υ um sistema multiplicador fixo de grau $-r$ para o grupo Γ (i.e., o sistema multiplicador associado a uma determinada forma modular $F(\tau)$). Para $1 \leq j \leq \mu = [\Gamma(1) : \Gamma]$, definimos κ_j como sendo o único número real que satisfaz*

$$\upsilon\left(A_j S^{\lambda_j} A_j^{-1}\right) = e^{2\pi i \kappa_j}, \qquad 0 \leq \kappa_j < 1. \tag{3.4}$$

Como λ_j é o menor inteiro que satisfaz $S^{\lambda_j} \in A_j^{-1}\Gamma A_j$, é claro que $A_j S^{\lambda_j} A_j^{-1} \in \Gamma$. Além disso, $e^{2\pi i \kappa_j}$, conforme κ_j varia entre 0 e 1, percorre bijetivamente o círculo unitário. Assim, como $A_j S^{\lambda_j} A_j^{-1} \in \Gamma$, segue que $\left|\upsilon\left(A_j S^{\lambda_j} A_j^{-1}\right)\right| = 1$, ou seja, $\upsilon\left(A_j S^{\lambda_j} A_j^{-1}\right)$ situa-se no círculo unitário, donde se asseguram existência e unicidade de κ_j. Portanto, a Definição 4 faz sentido. Além disso, pelo que comentamos após a Definição 3, se $q_i = q_j$ $(i \neq j)$, então $\lambda_i = \lambda_j$. Ademais, também já concluímos anteriormente que, nesse caso, $A_j = A_i S^t$, para algum inteiro t. Logo, $A_j S^{\lambda_j} A_j^{-1} = (A_i S^t) S^{\lambda_i} (A_i S^t)^{-1} = A_i S^{\lambda_i} A_i^{-1}$, donde $\kappa_i = \kappa_j$, ou seja, κ_j, assim como λ_j, é uma grandeza que depende unicamente do ponto parabólico em questão, o que é muito conveniente.

Lema 4. *Seja $q \neq \infty$ um ponto racional e $M = \begin{pmatrix} * & * \\ \gamma & \delta \end{pmatrix} \in \Gamma(1)$ tal que $Mq = q$. Então, para cada número real r, $(M\tau - q)^r = (\gamma\tau + \delta)^{-r}(\tau - q)^r$.*

Demonstração. Como $q \neq \infty$, podemos considerar $q = a/b$, com $a, b \in \mathbb{Z}$ tais que $(a, b) = 1$ e $b \neq 0$. Repetindo-se os argumentos utilizados na prova do Lema 2, M pode ser expresso da seguinte maneira:

$$M = \begin{pmatrix} 1 - ab\lambda & a^2\lambda \\ -b^2\lambda & 1 + ab\lambda \end{pmatrix},$$

sendo λ o inteiro igual ao produto $n(q)t$ daquele lema. Então, a igualdade que desejamos mostrar equivale a

$$\left(\frac{(1 - ab\lambda)\tau + a^2\lambda}{(-b^2\lambda)\tau + (1 + ab\lambda)} - \frac{a}{b}\right)^r = ((-b^2\lambda)\tau + (1 + ab\lambda))^{-r}(\tau - a/b)^r.$$

Por outro lado,

$$\begin{aligned}
\left(\frac{(1 - ab\lambda)\tau + a^2\lambda}{(-b^2\lambda)\tau + (1 + ab\lambda)} - \frac{a}{b}\right)^r &= \left(\frac{b[(1 - ab\lambda)\tau + a^2\lambda] - a[(-b^2\lambda)\tau + (1 + ab\lambda)]}{b[(-b^2\lambda)\tau + (1 + ab\lambda)]}\right)^r \\
&= \left(\frac{b\tau - ab^2\lambda\tau + a^2b\lambda + ab^2\lambda\tau - a - a^2b\lambda}{b[(-b^2\lambda)\tau + (1 + ab\lambda)]}\right)^r \\
&= \left(\frac{b\tau - a}{b[(-b^2\lambda)\tau + (1 + ab\lambda)]}\right)^r \\
&= \left(\frac{\tau - a/b}{(-b^2\lambda)\tau + (1 + ab\lambda)}\right)^r,
\end{aligned}$$

de modo que a igualdade que desejamos mostrar é a seguinte:

$$\left(\frac{\tau - a/b}{-b^2\lambda\tau + 1 + ab\lambda}\right)^r = (-b^2\lambda\tau + 1 + ab\lambda)^{-r}(\tau - a/b)^r. \tag{3.5}$$

É claro que os valores absolutos de ambos os membros acima são iguais. Resta-nos, portanto, provar que os dois membros possuem o mesmo argumento. Sabendo que

$$\arg \underbrace{\left(\frac{\tau - a/b}{-b^2\lambda\tau + 1 + ab\lambda}\right)}_{M\tau - q} = \arg(\tau - a/b) - \arg(-b^2\lambda\tau + 1 + ab\lambda) + 2n\pi, \tag{3.6}$$

vamos provar que $n = 0$. Como $M\tau - q \in \mathscr{H}$ ($\tau \in \mathscr{H}$ e $M \in \Gamma(1)$), vem que

$$0 < \arg\left(\frac{\tau - a/b}{-b^2\lambda\tau + 1 + ab\lambda}\right) < \pi.$$

Além disso, $0 < \arg(\tau - a/b) < \pi$, e $-\pi \leq \arg(-b^2\lambda\tau + 1 + ab\lambda) < \pi$, de modo que

$$2\pi|n| = \left|\arg\left(\frac{\tau - a/b}{-b^2\lambda\tau + 1 + ab\lambda}\right) - \arg(\tau - a/b) + \arg(-b^2\lambda\tau + 1 + ab\lambda)\right| < 2\pi,$$

donde $n = 0$ em (3.6) e, portanto,

$$r \arg\left(\frac{\tau - a/b}{-b^2\lambda\tau + 1 + ab\lambda}\right) = r\arg(\tau - a/b) - r\arg(-b^2\lambda\tau + 1 + ab\lambda),$$

ou seja,

$$\arg\left(\frac{\tau - a/b}{-b^2\lambda\tau + 1 + ab\lambda}\right)^r = \arg[(\tau - a/b)^r(-b^2\lambda\tau + 1 + ab\lambda)^{-r}],$$

o que completa a prova. □

Na seqüência, o importante teorema a que já nos referimos. Sua demonstração é bastante técnica e, talvez por esse motivo, difícil. Todavia, captar ao menos suas idéias centrais é fundamental para o desenvolvimento do assunto de que tratamos.

Teorema 5. *Suponha que $F(\tau)$ seja meromorfa em $\mathscr{H}$, satisfaça (3.1) para cada $M \in \Gamma$ e, ademais, que possua um número finito de pólos em $\overline{\mathscr{R}} \cap \mathscr{H}$. Então, para cada $j = 1, 2, \ldots, \mu$, existe um número real não negativo y_j tal que*

$$F(\tau) = \sigma_j(\tau) \sum_{n=-\infty}^{\infty} a_n(j) e^{2\pi i(n+\kappa_j)(A_j^{-1}\tau)/\lambda_j}, \tag{3.7}$$

expressão válida sempre que $\mathfrak{Im}\left(A_j^{-1}\tau\right) > y_j$. Na expansão (3.7), também denominada "expansão de Fourier de $F(\tau)$ em q_j", os termos são relativos ao ponto parabólico $q_j = A_j(\infty)$. Assim, κ_j é como na Definição 4, λ_j é a largura de q_j, os coeficientes $a_n(j)$ são números complexos que dependem de q_j, e

$$\sigma_j(\tau) = \begin{cases} 1, & \text{se } q_j = \infty \\ (\tau - q_j)^{-r}, & \text{se } q_j < \infty \end{cases}$$

Além disso, quando $F(\tau)$ é regular em $\mathscr{H}$, podemos tomar $y_j = 0$ para $1 \leq j \leq \mu$, de modo que a expansão (3.7) se torna válida em todo o semiplano $\mathscr{H}$, para cada ponto parabólico considerado.

Demonstração. Para simplificar a notação da prova, vamos considerar $q_j = q$, $\lambda_j = \lambda$, $\kappa_j = \kappa$ e $A_j = A$.

Observemos agora que a condição de $F(\tau)$ possuir um número finito de pólos em $\overline{\mathscr{R}} \cap \mathscr{H}$ independe da região fundamental padronizada $\mathscr{R}$. De fato, suponhamos que $\alpha \in \mathbb{C}$ seja um pólo de $F(\tau)$ em $\overline{\mathscr{R}} \cap \mathscr{H}$. Ademais, suponhamos que $\mathscr{R}$ e $\mathscr{R}'$ sejam duas regiões

fundamentais padronizadas segundo Γ, exatamente como as que aparecem na Proposição 3. Portanto, a expansão em série de Laurent de $F(\tau)$ em α corresponde a

$$F(\tau) = \sum_{n=-k}^{\infty} t_n(\tau - \alpha)^n,$$

sendo k um inteiro positivo, igual à ordem do pólo α. Agora, para cada $\tau \in \overline{\mathscr{R}} \cap \mathscr{H}$, existem $\tau' \in \overline{\mathscr{R}'} \cap \mathscr{H}$ e $M = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma$ tais que $\tau = M\tau'$, pois $\mathscr{R}$ e $\mathscr{R}'$ são regiões fundamentais segundo Γ. Desse modo, utilizando-se a relação (3.1), temos

$$\sum_{n=-k}^{\infty} t_n(\tau - \alpha)^n = F(\tau) = F(M\tau') = \upsilon(M)(c\tau' + d)^r F(\tau'),$$

donde

$$\begin{aligned} F(\tau') &= [\upsilon(M)]^{-1}(c\tau' + d)^{-r} \sum_{n=-k}^{\infty} t_n(\tau - \alpha)^n \\ &= [\upsilon(M)]^{-1}(c\tau' + d)^{-r} \sum_{n=-k}^{\infty} t_n(M\tau' - \alpha)^n \\ &= [\upsilon(M)]^{-1}(\underbrace{c\tau' + d}_{\neq 0})^{-r} \sum_{n=-k}^{\infty} t_n M^n(\tau' - M^{-1}\alpha)^n, \end{aligned}$$

Logo, $M^{-1}\alpha$ é um pólo de ordem menor do que ou igual a k de $F(\tau')$ em $\overline{\mathscr{R}'} \cap \mathscr{H}$. Este mesmo raciocínio mostra que, a cada pólo de $F(\tau')$ em $\overline{\mathscr{R}'} \cap \mathscr{H}$, corresponde um pólo de $F(\tau)$ em $\overline{\mathscr{R}} \cap \mathscr{H}$. Portanto, a asserção de que $F(\tau)$ possui um número finito de pólos em $\overline{\mathscr{R}} \cap \mathscr{H}$ é independente da região fundamental padronizada $\mathscr{R}$, sendo esse número de pólos, também, constante.

Pelo mesmo argumento utilizado na demonstração do Lema 2, existe um inteiro positivo λ tal que $S^\lambda \in \Gamma$ e $S^n \notin \Gamma$, para $1 \leq n \leq \lambda - 1$. Pelo que observamos no parágrafo anterior, podemos supor que $\mathscr{R}$ seja a região fundamental padronizada associada à decomposição $\Gamma(1) = \bigcup_{i=1}^{\mu} \Gamma A_i$ que satisfaça $A_i = S^{i-1}$, para $1 \leq i \leq \lambda$. Estes λ representantes de $\Gamma(1)$ serão distintos módulo Γ, pelo que comentamos no início deste parágrafo. Assim, notando-se que $\overline{\mathscr{R}(\Gamma(1))}$ contém a faixa $-1/2 \leq \mathfrak{Re}(\tau) \leq 1/2$, $\mathfrak{Im}(\tau) \geq 1$, concluimos que $\overline{\mathscr{R}} \cap \mathscr{H}$ contém a faixa $-1/2 \leq \mathfrak{Re}(\tau) \leq 1/2 + (\lambda - 1)$, ou $-1/2 \leq \mathfrak{Re}(\tau) \leq \lambda - 1/2$, $\mathfrak{Im}(\tau) \geq 1$. Por hipótese, $F(\tau)$ deve apresentar um número finito de pólos também nessa faixa.

Cientes do que já explicamos nos parágrafos anteriores, suponhamos inicialmente $q = \infty$. Neste caso, $A(\infty) = \infty$ e, portanto, $A = S^t$, para algum inteiro t. Logo, $M = AS^\lambda A^{-1} = S^\lambda \in \Gamma$, e podemos aplicar a relação (3.1) a M, obtendo

$$F(\tau + \lambda) = F(S^\lambda \tau) = \upsilon(S^\lambda)(0\tau + 1)^r F(\tau) = e^{2\pi i\kappa} F(\tau),$$

utilizando também a Definição 4. Atribuindo $g(\tau) = e^{-2\pi i\kappa\tau/\lambda} F(\tau)$, vem

$$\begin{aligned} g(\tau + \lambda) &= e^{-2\pi i\kappa(\tau+\lambda)/\lambda} F(\tau + \lambda) \\ &= e^{-2\pi i\kappa\tau/\lambda} e^{-2\pi i\kappa} e^{2\pi i\kappa} F(\tau) \\ &= e^{-2\pi i\kappa\tau/\lambda} F(\tau) = g(\tau), \end{aligned}$$

para todo $\tau \in \mathscr{H}$. Agora, denotando $w = e^{2\pi i\tau/\lambda}$, com $\tau = x + iy$, temos

$$w = e^{2\pi i(x+iy)/\lambda} = e^{-2\pi y/\lambda} e^{i(2\pi x/\lambda)}.$$

Definamos, então, a função $h(w) = h(e^{2\pi i\tau/\lambda}) = g(\tau)$, que está bem definida, uma vez que $g(\tau + \lambda) = g(\tau)$, para cada $\tau \in \mathscr{H}$. Como $|w| = e^{-2\pi y/\lambda}$, se $0 < |w| < 1$ (disco de raio 1 sem a origem), então $0 < e^{-2\pi y/\lambda} < 1$, donde $y > 0$, ou $\tau \in \mathscr{H}$. Logo, se $0 < |w| < 1$, então $\tau \in \mathscr{H}$, onde $F(\tau)$ é meromorfa e, pela construção anterior, $h(w)$ é meromorfa. Sabemos que $F(\tau)$ possui um número finito de pólos na faixa $-1/2 \leq \mathfrak{Re}(\tau) \leq \lambda - 1/2$, $\mathfrak{Im}(\tau) \geq 1$. Logo, se $y = \mathfrak{Im}(\tau) \geq 1$, então $|w| = e^{-2\pi y/\lambda} \leq e^{-2\pi/\lambda}$, donde $h(w)$ possui um número finito de pólos em $0 < |w| \leq e^{-2\pi/\lambda}$ e, por conseguinte, $h(w)$ é regular num disco da forma $0 < |w| < \rho$, para um certo $\rho \leq e^{-2\pi/\lambda}$. Portanto, $h(w)$ se expressa em série de Laurent em torno da origem como

$$h(w) = \sum_{n=-\infty}^{n=\infty} b_n w^n,$$

para $0 < |w| < \rho$. Neste caso, $0 < e^{-2\pi y/\lambda} < \rho$, donde $y > (\lambda/2\pi)\ln(1/\rho) = y_j \geq 0$. Assim, para $y = \mathfrak{Im}(\tau) > y_j$, temos $h(w) = \sum_{n=-\infty}^{\infty} b_n w^n$ ou, em termos de τ,

$$g(\tau) = \sum_{n=-\infty}^{\infty} b_n \left(e^{2\pi i\tau/\lambda}\right)^n,$$

ou

$$e^{-2\pi i\kappa\tau/\lambda} F(\tau) = \sum_{n=-\infty}^{\infty} b_n e^{2\pi in\tau/\lambda},$$

donde

$$\boxed{F(\tau) = \sum_{n=-\infty}^{\infty} b_n e^{2\pi i(n+\kappa)\tau/\lambda}.}$$

Além disso, $A^{-1}\tau = (S^t)^{-1}(\tau) = \tau - t$, de modo que $\tau = A^{-1}\tau + t$. Substituindo este valor na expressão anterior, vem que

$$\begin{aligned} F(\tau) &= \sum_{n=-\infty}^{\infty} b_n e^{2\pi i(n+\kappa)(A^{-1}\tau+t)/\lambda} \\ &= \sum_{n=-\infty}^{\infty} \underbrace{b_n e^{2\pi i(n+\kappa)t/\lambda}}_{a_n(j)} e^{2\pi i(n+\kappa)(A^{-1}\tau)/\lambda}, \end{aligned}$$

para $\mathfrak{Im}(A^{-1}\tau) = \mathfrak{Im}(\tau) > y_j$, conforme a expressão (3.7) para o caso $q = \infty$. Finalmente, se $F(\tau)$ é regular em $\mathscr{H}$, então $h(w)$ é regular para $0 < |w| < 1$, de modo que podemos tomar $\rho = 1$ na demonstração anterior, donde $y_j = 0$.

Suponhamos agora $q \neq \infty$. Da mesma forma, consideremos $M = AS^\lambda A^{-1} \in \Gamma$. Observe que

$$M(q) = AS^\lambda A^{-1}(q) = A(S^\lambda(A^{-1}(q))) = A(S^\lambda(\infty)) = A(\infty) = q.$$

Logo, pelo Lema 2 e pela Observação 1 que o sucede, $M = \begin{pmatrix} * & * \\ \gamma & \delta \end{pmatrix}$ é uma transformação linear fracionária parabólica tal que $M(q) = q$. Definindo-se $\varphi(\tau) = (\tau - q)^r F(\tau)$, por (3.1) e pelo Lema 4, temos

$$\begin{aligned} \varphi(M\tau) &= (M\tau - q)^r F(M\tau) \\ &= (M\tau - q)^r (\gamma\tau + \delta)^r \upsilon(M) F(\tau) \\ &= (\tau - q)^r e^{2\pi i\kappa} F(\tau) \\ &= e^{2\pi i\kappa}\varphi(\tau), \end{aligned}$$

ou

$$\varphi(AS^\lambda A^{-1}\tau) = e^{2\pi i\kappa}\varphi(\tau),$$

expressão válida para todo $\tau \in \mathscr{H}$. Portanto, tomando-se $A\tau \in \mathscr{H}$ no lugar de τ, temos

$$\varphi(AS^\lambda\tau) = e^{2\pi i\kappa}\varphi(A\tau).$$

Agora, definindo $g(\tau) = e^{-2\pi i\kappa\tau/\lambda}\varphi(A\tau)$, temos que

$$\begin{aligned} g(\tau+\lambda) &= g(S^\lambda\tau) \\ &= e^{-2\pi i\kappa(\tau+\lambda)/\lambda}\varphi(AS^\lambda\tau) \\ &= e^{-2\pi i\kappa\tau/\lambda}e^{-2\pi i\kappa}e^{2\pi i\kappa}\varphi(A\tau) \\ &= e^{-2\pi i\kappa\tau/\lambda}\varphi(A\tau) = g(\tau). \end{aligned}$$

De agora em diante, a demonstração prossegue de maneira análoga ao caso $q = \infty$. Definimos $w = e^{2\pi i\tau/\lambda}$ e $h(w) = h(e^{2\pi i\tau/\lambda}) = g(\tau)$ (como $g(\tau+\lambda) = g(\tau)$, temos novamente que $h(w)$ está bem definida). Em termos da função original $F(\tau)$, temos

$$g(\tau) = e^{-2\pi i\kappa\tau/\lambda}\varphi(A\tau) = e^{-2\pi i\kappa\tau/\lambda}(A\tau - q)^r F(A\tau),$$

donde o fato de $F(\tau)$ ser meromorfa para $\tau \in \mathscr{H}$ implica que o mesmo vale para $g(\tau)$, donde $h(w)$ é meromorfa para $0 < |w| < 1$. Além disso, essa mesma relação mostra que $g(\tau)$ possui um número finito de pólos em $A^{-1}\left(\overline{\mathscr{R}}\right) \cap \mathscr{H} = \overline{A^{-1}(\mathscr{R})} \cap \mathscr{H}$, uma vez que $F(\tau)$ possui um número finito de pólos em $\overline{\mathscr{R}} \cap \mathscr{H}$.

Agora, observemos que a relação (3.1), válida para $F(\tau)$ em relação a Γ, é herdada por $g(\tau)$ em relação a $A^{-1}\Gamma A$. De fato, tomando-se $A^{-1}VA \in A^{-1}\Gamma A$, $V = \begin{pmatrix} * & * \\ c & d \end{pmatrix}$, e utilizando-se a relação entre $g(\tau)$ e $F(\tau)$, temos

$$\begin{aligned} g(A^{-1}VA\tau) &= e^{-2\pi i\kappa(A^{-1}VA\tau)/\lambda}(A(A^{-1}VA\tau) - q)^r F(A(A^{-1}VA\tau)) \\ &= e^{-2\pi i\kappa(A^{-1}VA\tau)/\lambda}(VA\tau - q)^r F(VA\tau) \\ &= e^{-2\pi i\kappa(A^{-1}VA\tau)/\lambda}(VA\tau - q)^r \upsilon(V)(cA\tau + d)^r F(A\tau) \\ &= e^{-2\pi i\kappa(A^{-1}VA\tau)/\lambda}(VA\tau - q)^r \upsilon(V)(cA\tau + d)^r \frac{g(\tau)e^{2\pi i\kappa\tau/\lambda}}{(A\tau - q)^r} \\ &= \alpha(\tau)g(\tau), \end{aligned} \tag{3.8}$$

onde

$$\alpha(\tau) = \frac{e^{2\pi i\kappa\tau/\lambda}e^{-2\pi i\kappa(A^{-1}VA\tau)/\lambda}\upsilon(V)(cA\tau + d)^r(VA\tau - q)^r}{(A\tau - q)^r}.$$

Agora, pelo Corolário 16 do Capítulo 2, temos que $A^{-1}(\mathscr{R})$ é uma região fundamental padronizada segundo $A^{-1}\Gamma A$. Como $g(\tau)$ possui um número finito de pólos em $\overline{A^{-1}(\mathscr{R})} \cap \mathscr{H}$, segue, pela relação (3.8) aplicada ao mesmo raciocínio do início desta demonstração, que $g(\tau)$ possui um número finito de pólos em $\overline{\mathscr{R}'} \cap \mathscr{H}$, para toda região fundamental

padronizada $\mathscr{R}'$ segundo $A^{-1}\Gamma A$. Como λ é o menor inteiro positivo tal que $S^\lambda \in A^{-1}\Gamma A$, podemos tomar os representantes distintos I, S, S^2, ..., $S^{\lambda-1}$ de $\Gamma(1)$ módulo $A^{-1}\Gamma A$. Logo, $g(\tau)$ possui um número finito de pólos na faixa $-1/2 \leq \mathfrak{Re}(\tau) \leq \lambda - 1/2$, $\mathfrak{Im}(\tau) \geq 1$, de modo que $h(w)$ é regular quando $0 < |w| < \rho$, para algum $\rho \leq 1$. Então $h(w)$ se expressa em série de Laurent em torno da origem, nesse disco, como

$$h(w) = \sum_{n=-\infty}^{\infty} b_n w^n.$$

Agora, vamos obter a expressão correspondente em termos de τ, primeiramente observando que

$$F(\tau) = (\tau - q)^{-r}\varphi(\tau) = (\tau - q)^{-r} e^{-2\pi i\kappa}\varphi(M\tau). \tag{3.9}$$

Além disso, sabemos que

$$\varphi(A\tau) = e^{2\pi i\kappa\tau/\lambda} g(\tau)$$

vale para todo $\tau \in \mathscr{H}$. Logo, tomando $A^{-1}M\tau \in \mathscr{H}$, temos

$$\varphi(M\tau) = e^{2\pi i\kappa(A^{-1}M\tau)/\lambda} g(A^{-1}M\tau)$$

e, como $M = AS^\lambda A^{-1}$, vem que

$$\begin{aligned}
\varphi(M\tau) &= e^{2\pi i\kappa(S^\lambda A^{-1}\tau)/\lambda} g(S^\lambda A^{-1}\tau) \\
&= e^{2\pi i\kappa(A^{-1}\tau+\lambda)/\lambda} g(A^{-1}\tau + \lambda) \\
&= e^{2\pi i\kappa(A^{-1}\tau)/\lambda} e^{2\pi i\kappa} g(A^{-1}\tau) \\
&= e^{2\pi i\kappa(A^{-1}\tau)/\lambda} e^{2\pi i\kappa} h(e^{2\pi i(A^{-1}\tau)/\lambda}) \\
&= e^{2\pi i\kappa(A^{-1}\tau)/\lambda} e^{2\pi i\kappa} \sum_{n=-\infty}^{\infty} b_n e^{2\pi i n(A^{-1}\tau)/\lambda},
\end{aligned} \tag{3.10}$$

sendo a última passagem válida apenas para $0 < \left|e^{2\pi i(A^{-1}\tau)/\lambda}\right| < \rho$. Como vimos no caso $q = \infty$, $\left|e^{2\pi i(A^{-1}\tau)/\lambda}\right| = e^{-2\pi\mathfrak{Im}(A^{-1}\tau)/\lambda}$. Logo, essa passagem é válida apenas quando $e^{-2\pi\mathfrak{Im}(A^{-1}\tau)/\lambda} < \rho$, ou seja, quando $\mathfrak{Im}(A^{-1}\tau) > (\lambda/2\pi)\ln(1/\rho) = y_j \geq 0$. Ocorre então que, para $\mathfrak{Im}(A^{-1}\tau) \geq y_j$, podemos substituir (3.10) em (3.9) a fim de obter

$$F(\tau) = (\tau - q)^{-r} \sum_{n=-\infty}^{\infty} \underbrace{b_n}_{a_n(j)} e^{2\pi i(n+\kappa)(A^{-1}\tau)/\lambda},$$

que é precisamente a expansão dada por (3.7) para o caso $q \neq \infty$. Finalmente, se $F(\tau)$ é regular em $\mathscr{H}$, então $h(w)$ é regular para $0 < |w| < 1$, donde podemos tomar $\rho = 1$ e, portanto, $y_j = 0$. □

Observações:

1. Existe uma espécie de recíproca do Teorema 5: "Se $F(\tau)$ é meromorfa em $\mathscr{H}$ e possui uma expansão da forma (3.7) em cada ponto parabólico q_j, válida para $\mathfrak{Im}(A_j^{-1}\tau) > y_j \geq 0$, então $F(\tau)$ possui um número finito de pólos em $\overline{\mathscr{R}} \cap \mathscr{H}$". É interessante notar que, para provar esta recíproca, não se utiliza o fato de $F(\tau)$ satisfazer (3.1) em Γ. Em suma, a partir da existência desta recíproca, podemos dizer que, se $F(\tau)$ é meromorfa em $\mathscr{H}$ e satisfaz (3.1) com relação a Γ, então são equivalentes o fato de existir a expansão de Fourier de $F(\tau)$ em cada ponto parabólico q_j de Γ em $\mathscr{R}$ e o fato de $F(\tau)$ possuir um número finito de pólos em $\overline{\mathscr{R}} \cap \mathscr{H}$.

2. Se $q_k = q_j$, $k \neq j$, então $F(\tau)$ possui duas expansões da forma (3.7) em q_j e em q_k, a saber,

$$F(\tau) = \sigma_j(\tau) \sum_{n=-\infty}^{\infty} a_n(j) e^{2\pi i(n+\kappa_j)(A_j^{-1}\tau)/\lambda_j} = \sigma_k(\tau) \sum_{n=-\infty}^{\infty} a_n(k) e^{2\pi i(n+\kappa_k)(A_k^{-1}\tau)/\lambda_k}.$$

Como $q_k = q_j$, segue de observações anteriores que $\kappa_k = \kappa_j$ e $\lambda_k = \lambda_j$. Segue também, trivialmente, que $\sigma_k(\tau) = \sigma_j(\tau)$. Além disso, por raciocínio que utilizamos freqüentemente, $A_k^{-1} = S^t A_j^{-1}$, para algum inteiro t (se necessário, reveja as observações após o Lema 1). Portanto, a expansão de $F(\tau)$ em q_k corresponde a

$$\begin{aligned} F(\tau) &= \sigma_j(\tau) \sum_{n=-\infty}^{\infty} a_n(k) e^{2\pi i(n+\kappa_j)(S^t A_j^{-1}\tau)/\lambda_j} \\ &= \sigma_j(\tau) \sum_{n=-\infty}^{\infty} a_n(k) e^{2\pi i(n+\kappa_j)(A_j^{-1}\tau+t)/\lambda_j} \\ &= \sigma_j(\tau) \sum_{n=-\infty}^{\infty} e^{2\pi i(n+\kappa_j)t/\lambda_j} a_n(k) e^{2\pi i(n+\kappa_j)(A_j^{-1}\tau)/\lambda_j}. \end{aligned}$$

Comparando agora esta expressão com a da expansão de $F(\tau)$ em q_j, pela unicidade da representação de uma função em série de Laurent em torno de um dado ponto, temos a relação

$$a_n(j) = e^{2\pi i(n+\kappa_j)t/\lambda_j} a_n(k).$$

Atentemo-nos agora a outra questão de invariância. Suponha que $\mathscr{R}$ e $\mathscr{R}'$ sejam regiões fundamentais padronizadas segundo Γ, como na Proposição 3. Por essa proposição, já sabemos que a largura do ponto parabólico $q'_j = A'_j(\infty)$ de Γ em $\mathscr{R}'$ é igual à largura do ponto parabólico $q_j = A_j(\infty)$ de Γ em $\mathscr{R}$. Definindo κ'_j como fizemos para κ_j, i. e., para $1 \leq j \leq \mu$, κ'_j é o único número real que satisfaz

$$\upsilon(A'_j S^{\lambda_j} A_j'^{-1}) = e^{2\pi i \kappa'_j}, \qquad 0 \leq \kappa'_j < 1,$$

podemos nos perguntar se existe alguma relação entre κ_j e κ'_j.

Além disso, supondo que $F(\tau)$, não identicamente nula, é meromorfa em $\mathscr{H}$, satisfaz (3.1) para todo $M \in \Gamma$, e possui um número finito de pólos em $\overline{\mathscr{R}} \cap \mathscr{H}$, como observamos no início da demonstração do Teorema 5, segue que $F(\tau)$ também possui um número finito de pólos em $\overline{\mathscr{R}'} \cap \mathscr{H}$. Assim, por esse mesmo teorema, $F(\tau)$ apresenta-se como em (3.7) em q_j e, em q'_j, para $\mathfrak{Im}(A_j'^{-1}\tau) > y'_j \geq 0$, apresenta-se como

$$F(\tau) = \sigma'_j(\tau) \sum_{n=-\infty}^{\infty} a'_n(j) e^{2\pi i (n+\kappa'_j)(A_j'^{-1}\tau)/\lambda_j}, \tag{3.11}$$

onde

$$\sigma'_j(\tau) = \begin{cases} 1, & \text{se } q'_j = \infty \\ (\tau - q'_j)^{-r}, & \text{se } q'_j < \infty \end{cases}$$

Em (3.11), já utilizamos que $\lambda'_j = \lambda_j$. Surge, então, a seguinte questão: como os termos das expansões (3.7) e (3.11) se relacionam? Em boa medida, o seguinte teorema nos responde essa questão:

Teorema 6. *Para $1 \leq j \leq \mu$, temos, em (3.11), $\kappa'_j = \kappa_j$ e $a'_n(j) = \beta(j) a_n(j)$ para todo n, sendo $\beta(j)$ uma constante complexa não nula independente de n.*

Demonstração. Vamos fixar j, e simplificar a notação escrevendo A, A', λ, q, q', κ, κ', $\sigma(\tau)$ e $\sigma'(\tau)$ em lugar dos correspondentes indexados por j. Além disso, suponhamos $y = \max\{y_j, y'_j\}$.

Como estamos utilizando, para $\mathscr{R}$ e $\mathscr{R}'$, a mesma indexação da Proposição 3, existe $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ tal que $A' = MA$, de modo que $q' = A'(\infty) = MA(\infty) = Mq$. Além disso, se $V = AS^{\lambda}A^{-1}$, então $V \in \Gamma$ (comentário após a Definição 4) e $V(q) = A(S^{\lambda}(A^{-1}(q))) = A(S^{\lambda}(\infty)) = A(\infty) = q$. Provaremos, então, que vale o seguinte resultado, análogo ao que foi provado no Lema 4:

$$(c\tau + d)^{-r} \sigma'(M\tau) = K\sigma(\tau), \tag{3.12}$$

sendo $K \neq 0$ um número complexo independente de τ. Para provar essa relação, temos quatro casos a considerar:

1. $q = q' = \infty$;
   Neste caso, como $Mq = q'$, temos $\frac{a}{c} = \infty$, donde $c = 0$ e, por conseguinte, $a = d = \pm 1$. Além disso, por definição, $\sigma(\tau)$ e $\sigma'(M\tau)$ são iguais a 1, de modo que

$$(c\tau + d)^{-r}\sigma'(M\tau) = \underbrace{(\pm 1)^{-r}}_{K} \cdot 1 = K\sigma(\tau).$$

2. $q, q' < \infty$;
   Neste caso,

$$\begin{aligned}
(c\tau + d)^{-r}\sigma'(M\tau) &= (c\tau + d)^{-r}(M\tau - q')^{-r} \\
&= (c\tau + d)^{-r}(M\tau - Mq)^{-r} \\
&= (c\tau + d)^{-r}\left(\frac{a\tau + b}{c\tau + d} - \frac{aq + b}{cq + d}\right)^{-r} \\
&= (c\tau + d)^{-r}\left(\frac{(a\tau + b)(cq + d) - (c\tau + d)(aq + b)}{(c\tau + d)(cq + d)}\right)^{-r} \\
&= (c\tau + d)^{-r}\left(\frac{(ad - bc)(\tau - q)}{(c\tau + d)(cq + d)}\right)^{-r} \\
&= (c\tau + d)^{-r}\left(\frac{\tau - q}{(c\tau + d)(cq + d)}\right)^{-r} \\
&= (c\tau + d)^{-r}\frac{(\tau - q)^{-r}}{(c\tau + d)^{-r}(cq + d)^{-r}}e^{-2\pi inr},
\end{aligned}$$

   para algum inteiro n. Desse modo,

$$(c\tau + d)^{-r}\sigma'(M\tau) = \underbrace{\frac{(cq + d)^r}{e^{2\pi inr}}}_{K}(\tau - q)^{-r} = K\sigma(\tau),$$

   onde $K \neq 0$ é um número complexo independente de τ.

3. $q' < \infty$ e $q = \infty$;

Agora,

$$\begin{aligned}
(c\tau+d)^{-r}\sigma'(M\tau) &= (c\tau+d)^{-r}(M\tau-q')^{-r} \\
&= (c\tau+d)^{-r}(M\tau-Mq)^{-r} \\
&= (c\tau+d)^{-r}\left(\frac{a\tau+b}{c\tau+d}-\frac{a}{c}\right)^{-r} \\
&= (c\tau+d)^{-r}\left(\frac{c(a\tau+b)-a(c\tau+d)}{c(c\tau+d)}\right)^{-r} \\
&= (c\tau+d)^{-r}\left(\frac{-(ad-bc)}{c(c\tau+d)}\right)^{-r} \\
&= (c\tau+d)^{-r}\left(\frac{-1}{c(c\tau+d)}\right)^{-r} \\
&= (c\tau+d)^{-r}\frac{(-1)^{-r}}{c^{-r}(c\tau+d)^{-r}}e^{-2\pi inr} \\
&= e^{\pi ir(1-2n)}c^r = K = K\cdot 1 = K\sigma(\tau),
\end{aligned}$$

onde $K\neq 0$ é um número complexo independente de τ e n é um inteiro.

4. $q'=\infty$ e $q\neq\infty$;
   Neste caso, $Mq=q'$ implica que $\frac{aq+b}{cq+d}=\infty$, donde $cq+d=0$, ou $q=-d/c$. Além disso, $\sigma'(M\tau)=1$, donde

$$\begin{aligned}
(c\tau+d)^{-r}\sigma'(M\tau) &= (c\tau+d)^{-r} \\
&= \left(c\left(\tau+\frac{d}{c}\right)\right)^{-r} \\
&= \underbrace{c^{-r}}_{K}(\tau-q)^{-r} = K\sigma(\tau),
\end{aligned}$$

   onde $K\neq 0$, novamente, é um número complexo independente de τ. Utilizamos acima que $(c(\tau-q))^{-r}=c^{-r}(\tau-q)^{-r}$, fato que pode ser provado de modo análogo ao que fizemos para a identidade (3.5) do Lema 4.

Deste modo, já podemos utilizar a relação (3.12). Considere agora a expansão de $F(\tau)$ em q', válida para $\mathfrak{Im}(A'^{-1}\tau)>y\geq 0$,

$$F(\tau)=\sigma'(\tau)\sum_{n=-\infty}^{\infty}a'_n(j)e^{2\pi i(n+\kappa')(A'^{-1}\tau)/\lambda}=\sigma'(\tau)\sum_{n=-\infty}^{\infty}a'_n(j)e^{2\pi i(n+\kappa')(A^{-1}M^{-1}\tau)/\lambda}.$$

Agora, para $\mathfrak{Im}(A^{-1}\tau) > y \geq 0$, podemos aplicar a expansão acima em $M\tau$, uma vez que, neste caso, $\mathfrak{Im}(A'^{-1}M\tau) = \mathfrak{Im}(A^{-1}M^{-1}M\tau) = \mathfrak{Im}(A^{-1}\tau) > y \geq 0$, donde

$$F(M\tau) = \sigma'(M\tau) \sum_{n=-\infty}^{\infty} a'_n(j) e^{2\pi i(n+\kappa')(A^{-1}\tau)/\lambda},$$

de modo que, utilizando (3.1), temos que

$$\upsilon(M)(c\tau + d)^r F(\tau) = \sigma'(M\tau) \sum_{n=-\infty}^{\infty} a'_n(j) e^{2\pi i(n+\kappa')(A^{-1}\tau)/\lambda},$$

ou

$$F(\tau) = \overline{\upsilon(M)}(c\tau + d)^{-r} \sigma'(M\tau) \sum_{n=-\infty}^{\infty} a'_n(j) e^{2\pi i(n+\kappa')(A^{-1}\tau)/\lambda},$$

onde $\overline{\upsilon(M)}$ é o número complexo conjugado de $\upsilon(M)$. Aplicando, agora, (3.12) a essa última igualdade, temos:

$$F(\tau) = \overline{\upsilon(M)} K\sigma(\tau) \sum_{n=-\infty}^{\infty} a'_n(j) e^{2\pi i(n+\kappa')(A^{-1}\tau)/\lambda}. \tag{3.13}$$

Note agora que $\mathfrak{Im}(A^{-1}V\tau) = \mathfrak{Im}(A^{-1}AS^{\lambda}A^{-1}\tau) = \mathfrak{Im}(A^{-1}\tau + \lambda) = \mathfrak{Im}(A^{-1}\tau) > y \geq 0$, de forma que podemos aplicar a expressão anterior em $V\tau$:

$$\begin{aligned}
F(V\tau) &= \overline{\upsilon(M)} K\sigma(V\tau) \sum_{n=-\infty}^{\infty} a'_n(j) e^{2\pi i(n+\kappa')(A^{-1}V\tau)/\lambda} \\
&= \overline{\upsilon(M)} K\sigma(V\tau) \sum_{n=-\infty}^{\infty} a'_n(j) e^{2\pi i(n+\kappa')(A^{-1}\tau+\lambda)/\lambda} \\
&= \overline{\upsilon(M)} K\sigma(V\tau) \sum_{n=-\infty}^{\infty} a'_n(j) e^{2\pi i(n+\kappa')(A^{-1}\tau)/\lambda} e^{2\pi i(n+\kappa')} \\
&= \overline{\upsilon(M)} K\sigma(V\tau) e^{2\pi i\kappa'} \sum_{n=-\infty}^{\infty} a'_n(j) e^{2\pi i(n+\kappa')(A^{-1}\tau)/\lambda} \\
&= \sigma(V\tau) e^{2\pi i\kappa'} \frac{F(\tau)}{\sigma(\tau)} = e^{2\pi i\kappa'} \frac{\sigma(V\tau)}{\sigma(\tau)} F(\tau).
\end{aligned} \tag{3.14}$$

Além disso, a expansão de $F(\tau)$ em q, como a exibida em (3.7), válida para $\mathfrak{Im}(A^{-1}\tau) >$

$y \geq 0$, pode também ser aplicada em $V\tau$, levando-nos a

$$\begin{aligned} F(V\tau) &= \sigma(V\tau) \sum_{n=-\infty}^{\infty} a_n(j) e^{2\pi i(n+\kappa)(A^{-1}V\tau)/\lambda} \\ &= \sigma(V\tau) e^{2\pi i\kappa} \sum_{n=-\infty}^{\infty} a_n(j) e^{2\pi i(n+\kappa)(A^{-1}\tau)/\lambda} \\ &= \sigma(V\tau) e^{2\pi i\kappa} \frac{F(\tau)}{\sigma(\tau)} = e^{2\pi i\kappa} \frac{\sigma(V\tau)}{\sigma(\tau)} F(\tau), \end{aligned} \tag{3.15}$$

efetuando cálculos similares aos que fizemos para chegar a (3.14). Dado que F não é identicamente nula, igualando-se (3.14) a (3.15), segue que $\kappa' = \kappa$. Finalmente, utilizando-se tal resultado em (3.13), temos que

$$F(\tau) = \sigma(\tau) \sum_{n=-\infty}^{\infty} \overline{\upsilon(M)} K a'_n(j) e^{2\pi i(n+\kappa)(A^{-1}\tau)/\lambda}.$$

Comparando-se com (3.7), a unicidade da representação de uma função em série de Laurent implica que $a_n(j) = \overline{\upsilon(M)} K a'_n(j)$, ou

$$a'_n(j) = \underbrace{\upsilon(M) K^{-1}}_{\beta(j)} a_n(j),$$

sendo $\beta(j)$ como no enunciado. □

Observação: Na demonstração do último teorema, $Vq = q$, de modo que, pelo Lema 4, se $q \neq \infty$, então

$$\frac{\sigma(V\tau)}{\sigma(\tau)} = \frac{(V\tau - q)^{-r}}{(\tau - q)^{-r}} = (\gamma\tau + \delta)^r,$$

para $V = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. Por outro lado, se $q = \infty$, então $Vq = q = \infty$. Neste caso, $\alpha/\gamma = \infty$, ou $\gamma = 0$, donde $\alpha = \delta = \pm 1$. Além disso, o Lema 2 implica que $\alpha + \delta = 2$, donde $\alpha = \delta = 1$. Logo, $(\gamma\tau + \delta)^r = 1$ e $\sigma(V\tau)/\sigma(\tau) = 1/1 = 1$. Em todo o caso, para $q \leq \infty$,

$$\frac{\sigma(V\tau)}{\sigma(\tau)} = (\gamma\tau + \delta)^r,$$

donde, utilizando também a relação (3.15),

$$F(V\tau) = e^{2\pi i\kappa} \frac{\sigma(V\tau)}{\sigma(\tau)} F(\tau) = e^{2\pi i\kappa} (\gamma\tau + \delta)^r F(\tau) = \upsilon(V)(\gamma\tau + \delta)^r F(\tau),$$

o que é consistente com relação a (3.1).

3.4 Definição de forma e função modular

Suponhamos que $F(\tau)$ seja uma função em $\mathscr{H}$ que satisfaça as condições do Teorema 5, de modo que ela se expresse como em (3.7) em cada ponto parabólico de Γ em uma dada região fundamental padronizada $\mathscr{R}$. Temos a seguinte definição:

Definição 5. *Se somente finitos termos não nulos com $n < 0$ aparecem na expansão (3.7) em q_j, dizemos que $F(\tau)$ é* meromorfa *em q_j. Neste caso, se o primeiro coeficiente $a_n(j)$ não nulo ocorre para $n = -n_0 < 0$, dizemos que $F(\tau)$ possui um pólo de ordem $n_0 - \kappa_j$ em q_j. Se o primeiro coeficiente $a_n(j)$ não nulo ocorre para $n = n_0 \geq 0$, dizemos que $F(\tau)$ é* regular *em q_j, com zero de ordem $n_0 + \kappa_j$ nesse ponto.*

Observações:

1. A terminologia da definição é justificada, em parte, pelo Lema 1: segundo ele, se $\tau \to q_j$ a partir de pontos de $\mathscr{R}$, $A^{-1}\tau \to \infty$ dentro de uma faixa determinada. Assim, se $n + \kappa < 0$ e $\tau \to q_j$, então $\left|e^{2\pi i(n+\kappa)(A_j^{-1}\tau)/\lambda_j}\right| \to \infty$ e, se $n + \kappa > 0$ e $\tau \to q_j$, então $e^{2\pi i(n+\kappa)(A_j^{-1}\tau)/\lambda_j} \to 0$.

2. As definições acima dependem apenas do ponto parabólico q_j. De fato, se $q_j = A_j(\infty) = A_k(\infty) = q_k$, $j \neq k$, então, pela Observação 2 após o Teorema 5, $a_n(j) = e^{2\pi i(n+\kappa_j)t/\lambda_j} a_n(k)$, para todo inteiro n. Como $e^{2\pi i(n+\kappa_j)t/\lambda_j} \neq 0$ para todo n, temos que $a_n(j) = 0$ se, e somente se, $a_n(k) = 0$. Portanto, $F(\tau)$ é meromorfa em q_j se, e somente se, $F(\tau)$ é meromorfa em q_k, sendo a ordem do pólo ou do zero a mesma para q_j e q_k.

3. Suponha que $\mathscr{R}$ e $\mathscr{R}'$ sejam duas regiões fundamentais padronizadas segundo Γ, como as da Proposição 3. Então, pelo Teorema 6, $a'_n(j) = \beta(j)a_n(j)$, sendo $\beta(j) \neq 0$, donde segue que $F(\tau)$ é meromorfa em q_j se, e somente se, $F(\tau)$ é meromorfa em q'_j, sendo também idênticas as ordens de $F(\tau)$ nesses dois pontos (como pólos ou como zeros).

Agora, finalmente, podemos definir o que é uma forma modular:

Definição 6. *Seja $r \in \mathbb{R}$ e v um sistema multiplicador de grau $-r$ para o subgrupo Γ de $\Gamma(1)$. Uma função $F(\tau)$, definida e meromorfa em $\mathscr{H}$, é dita* forma modular de grau $-r$, com sistema multiplicador v, com respeito a Γ, *se*

1. *$F(\tau)$ satisfaz (3.1) para todo $M \in \Gamma$;*

2. *Existe uma região fundamental padronizada $\mathscr{R}$ tal que $F(\tau)$ possui um número finito de pólos em $\overline{\mathscr{R}} \cap \mathscr{H}$ (segundo a Observação 1 que sucede o Teorema 5, isto equivale a $F(\tau)$ possuir uma expansão da forma (3.7) em cada ponto parabólico de Γ em $\mathscr{R}$);*

3. *$F(\tau)$ é meromorfa em cada ponto parabólico de Γ em $\mathscr{R}$.*

Embora as condições 2. e 3. se refiram a uma região fundamental padronizada específica, se tais condições valem para uma certa região fundamental padronizada, então elas valem para qualquer região fundamental padronizada. Isto é conseqüência da Observação 3 precedente a esta definição e da demonstração do Teorema 5. Este mesmo comentário é válido para as três definições que seguem:

Definição 7. *Se $F(\tau)$ é uma forma modular com respeito a Γ, dizemos que ela é uma* forma modular inteira *se*

1. *$F(\tau)$ é regular em $\mathscr{H}$;*

2. *$F(\tau)$ é regular em cada ponto parabólico de Γ em alguma região fundamental padronizada $\mathscr{R}$.*

Definição 8. *Se $F(\tau)$ é uma forma modular com respeito a Γ tal que $F(\tau)$ é regular em $\mathscr{H}$ e possui um zero de ordem positiva em cada ponto parabólico de Γ em alguma região fundamental padronizada $\mathscr{R}$, isto é, se $F(\tau)$ é uma forma modular inteira tal que cada ponto parabólico é um zero de ordem positiva, dizemos que $F(\tau)$ é uma* forma cúspide.

Definição 9. *Se $F(\tau)$ é uma forma modular com respeito a Γ tal que $r = 0$ e $\upsilon(M) = 1$, para todo $M \in \Gamma$, então $F(\tau)$ é dita* função modular com respeito a Γ. *Neste caso, a condição 1. da definição de forma modular se reduz a $F(M\tau) = F(\tau)$, para cada $M \in \Gamma$.*

3.5 Vários teoremas importantes

Os teoremas que provaremos nesta seção têm relação com a obtenção de limitantes para os valores assumidos por uma forma modular $F(\tau)$ (ou um caso particular de forma modular, segundo as definições da seção anterior) e, em particular, para os coeficientes $a_n(j)$ que aparecem na expansão de $F(\tau)$ em seu ponto parabólico q_j. Embora este texto

não chegue a tratar de aplicações das formas modulares à teoria dos números, optamos por apresentar esses resultados a fim de realizar um estudo sobre como, na prática, trabalha-se com formas modulares e suas expansões. Além disso, o leitor atento observará que o Teorema 8 e o corolário que o sucede, por exemplo, possuem enunciados semelhantes ao do famoso Teorema de Liouville (vide referência [4]), de modo que o conteúdo ora exibido não deve ser visto como exclusividade da teoria de formas modulares, mas sim espécies de "versões modulares" dos já conhecidos teoremas de variáveis complexas. Começamos pelo seguinte lema, que será utilizado na demonstração do Teorema 8:

Lema 7. *Se $f(\tau)$ é uma função modular com respeito a Γ tal que $f(\tau)$ é regular em $\mathscr{H}$ e em todos os pontos parabólicos de alguma região fundamental padronizada $\mathscr{R}$, ou seja, se $f(\tau)$ é uma função modular inteira, então $f(\tau) \to a_0(j)$ à medida que $\tau \to q_j$ a partir de pontos de $\mathscr{R}$, para cada ponto parabólico q_j de Γ em $\mathscr{R}$. Aqui, $a_0(j)$ é o coeficiente que ocorre na expansão (3.7) de $f(\tau)$ em q_j. Além disso, $f(\tau)$ é limitada em $\mathscr{H}$.*

Demonstração. Como $\upsilon(M) = 1$ para todo $M \in \Gamma$, a Definição 4 implica que $\kappa_j = 0$ para $1 \leq j \leq \mu$ e, como $r = 0$, temos que $\sigma_j(\tau) = 1$ para $q_j \leq \infty$. Utilizando-se também o fato de que $f(\tau)$ é regular em q_j, a expansão de Fourier de $f(\tau)$ em q_j se torna

$$f(\tau) = \sum_{n=0}^{\infty} a_n(j) e^{2\pi i n (A_j^{-1}\tau)/\lambda_j}, \tag{3.16}$$

válida em todo o semiplano $\mathscr{H}$, uma vez que $f(\tau)$ é regular nesse domínio. A expansão (3.16) nos mostra que $f(\tau)$ pode ser vista como uma série de potências na variável $z = e^{2\pi i (A_j^{-1}\tau)/\lambda_j}$, de tal modo que se tem

$$f(\tau) = \sum_{n=0}^{\infty} a_n(j) z^n = a_0(j) + a_1(j) z + a_2(j) z^2 + \cdots,$$

convergente para $|z| < 1$. Portanto, à medida que $\tau \to q_j$ de dentro de $\mathscr{R}$, o Lema 1 implica que $A_j^{-1}\tau \to \infty$ de dentro de uma faixa da forma $\mathfrak{Im}(w) > 0$, $a_i < \mathfrak{Re}(w) < b_i$. Sendo $A_j^{-1}\tau = x + iy$, isso implica que $y \to \infty$ e $a_i < x < b_i$, de modo que

$$z = e^{2\pi i (A_j^{-1}\tau)/\lambda_j} = e^{2\pi i (x+iy)/\lambda_j} = \frac{e^{2\pi i x/\lambda_j}}{e^{2\pi y/\lambda_j}} \to 0.$$

Ora, neste caso, $f(\tau) \to a_0(j)$, ficando provada uma das asserções do enunciado.

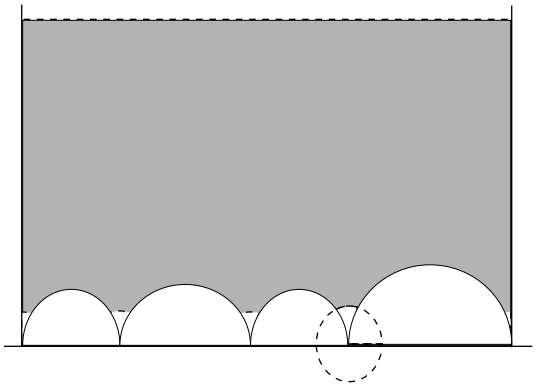
Pelo que foi provado, dado $\varepsilon > 0$, existe $\delta > 0$ tal que $|\tau - q_j| < \delta$ implica

$$|f(\tau)| = |f(\tau) - a_0(j) + a_0(j)| \leq |f(\tau) - a_0(j)| + |a_0(j)| < \varepsilon + |a_0(j)|,$$

utilizando também a desigualdade triangular. Como a convergência para q_j ocorre a partir de pontos de $\mathscr{R}$, a desigualdade acima implica que $f(\tau)$ é limitada na intersecção de $\mathscr{R}$ com alguma vizinhança D_j de cada ponto parabólico q_j. Se $q_j < \infty$, então D_j é um disco aberto centrado em q_j e, se $q_j = \infty$, D_j é um semiplano da forma $\mathfrak{Im}(\tau) > y_0$, com $y_0 > 0$. Definamos, então,

$$\mathscr{R}^* = \mathscr{R} \setminus \bigcup_{i=1}^{\mu} D_j. \tag{3.17}$$

Observemos agora que $\overline{\mathscr{R}^*}$ é um subconjunto compacto de $\mathscr{H}$, pois é fechado e limitado. Cabe aqui uma justificativa mais detalhada acerca desta segunda propriedade de $\overline{\mathscr{R}^*}$. Em primeiro lugar, sabemos que $\mathscr{R} = \bigcup_{i=1}^{\mu} A_i\{\mathscr{R}(\Gamma(1))\}$. Além disso, $\Gamma(1)$ é gerado por S e T (Corolário 4 do Capítulo 2), os A's são combinações finitas desses elementos, e $\mathscr{R}(\Gamma(1))$ possui a forma que também foi estabelecida no Capítulo 2. Quando T age num elemento de $\mathscr{R}(\Gamma(1))$, ela apenas leva este elemento ao interior do semicírculo unitário superior e, quando S age num elemento dessa região, ocorre apenas uma translação horizontal do mesmo. Deste modo, $\mathscr{R}$ é limitada, à esquerda e à direita, por duas faixas verticais, podendo, todavia, ser ilimitada em direção a ∞. Caso isto ocorra, ∞ é ponto parabólico de Γ em $\mathscr{R}$, de modo que $\mathscr{R}^*$ exclui de $\mathscr{R}$ a vizinhança relativa a esse ponto, tornando limitada a região $\overline{\mathscr{R}^*}$. A figura abaixo pode facilitar a compreensão. Nela, a parte hachurada se refere à $\mathscr{R}^*$, obtida de $\mathscr{R}$ por meio da retirada dos semicírculos tracejados (vizinhanças de pontos parabólicos finitos) e, eventualmente, da retirada da vizinhança superior, do ponto ∞:



Como $f(\tau)$ é regular em $\mathscr{H}$, vem que $f(\tau)$ é contínua em nesse conjunto e, portanto, $f\left(\overline{\mathscr{R}^*}\right)$ é compacto em $\mathscr{H}$, donde $f(\tau)$ é também limitada em $\overline{\mathscr{R}^*}$. Logo, $f(\tau)$ é limitada

em

$$\left(\bigcup_{j=1}^{\mu} \mathscr{R} \cap D_j\right) \cup \mathscr{R}^* = \mathscr{R}.$$

Além disso, também pelo fato de $f(\tau)$ ser contínua, $f\left(\overline{\mathscr{R}} \cap \mathscr{H}\right) \subset \overline{f\left(\mathscr{R}\right)} \cap \mathscr{H}$ e, como $\overline{f\left(\mathscr{R}\right)} \cap \mathscr{H}$ é compacto em $\mathscr{H}$, vem que $f\left(\overline{\mathscr{R}} \cap \mathscr{H}\right)$ é limitado. Logo, $f(\tau)$ é limitada em $\overline{\mathscr{R}} \cap \mathscr{H}$. Finalmente, como $\mathscr{R}$ é região fundamental segundo Γ, dado $\tau \in \mathscr{H}$, tome $M \in \Gamma$ tal que $M\tau \in \overline{\mathscr{R}} \cap \mathscr{H}$. Logo, como $f(M\tau) = f(\tau)$ para todo $M \in \Gamma$, segue que $f(\tau)$ é limitada em $\mathscr{H}$. □

Teorema 8. *Toda função modular inteira é constante.*

Demonstração. Consideremos, para esta demonstração, a função $f(\tau)$ e a mesma notação do Lema 7. Definindo-se $F(\tau) = \prod_{j=1}^{\mu}\{f(\tau) - a_0(j)\}$, temos que $F(\tau)$ é função modular com respeito a Γ, de modo que, aplicando-se o Lema 7 a $f(\tau)$, vem que $F(\tau)$ é também limitada em $\mathscr{H}$. Seja C o supremo de $|F(\tau)|$ em $\mathscr{H}$. Afirmamos que $C = 0$ e, para prová-lo, suponhamos, por absurdo, que $C > 0$. Neste caso, o Lema 7 implica que, dado $\varepsilon_j > 0$, existe $\delta_j > 0$ tal que $|\tau - q_j| < \delta_j$ implica $|f(\tau) - a_0(j)| < \varepsilon_j$, para $1 \leq j \leq \mu$ e $\tau \in \mathscr{R}$. Tomando, então, para cada j, $\varepsilon_j = \sqrt[\mu]{C/2}$, existem os números reais $\delta_j > 0$ tais que $|\tau - q_j| < \delta_j$ implica que

$$|F(\tau)| = \left|\prod_{j=1}^{\mu}\{f(\tau) - a_0(j)\}\right| = \prod_{j=1}^{\mu}|f(\tau) - a_0(j)| < \left(\sqrt[\mu]{C/2}\right)^{\mu} = C/2,$$

considerando sempre a topologia da esfera de Riemann. A existência dos números reais δ_j corresponde à existência das vizinhanças D_j da demonstração do Lema 7, de modo que podemos assegurar a existência de um conjunto $\mathscr{R}^*$ como em (3.17) tal que, em $\mathscr{R} \setminus \mathscr{R}^*$, $|F(\tau)| < C/2$. Como C é o supremo de $F(\tau)$ em $\mathscr{H}$, segue que o módulo máximo de $F(\tau)$ em $\overline{\mathscr{R}} \cap \mathscr{H}$, e portanto em $\mathscr{H}$, dado que $\mathscr{R}$ é região fundamental segundo Γ, ocorre em $\mathscr{R}^* \subset \mathscr{H}$. Cabe aqui uma justificativa mais detalhada desse fato. Primeiramente, observe que $\overline{\mathscr{R}} \cap \mathscr{H} = (\mathscr{R} \cup \partial\mathscr{R}) \cap \mathscr{H}$, onde $\partial\mathscr{R}$ se refere à fronteira do conjunto $\mathscr{R}$. Se o máximo de $|F(\tau)|$ em $\mathscr{H}$ ocorrer em $\partial\mathscr{R} \cap \mathscr{H}$, então deve existir τ' nesse conjunto tal que $|F(\tau')| = C$. Ora, isto é uma contradição com o fato de $F(\tau)$ ser contínua em $\mathscr{H}$ e possuir módulo menor do que $C/2$ nas proximidades de τ'. Portanto, o módulo máximo de $F(\tau)$ em $\mathscr{H}$ ocorre, de fato, em $\mathscr{R}^* \subset \mathscr{H}$ e, como $F(\tau)$ é regular em $\mathscr{H}$, isto contradiz o Princípio do Módulo Máximo (Capítulo 1), segundo o qual o valor máximo de $|F(\tau)|$ não ocorre em $\mathscr{H}$.

Portanto $C = 0$, donde $F(\tau)$ é identicamente nula em $\mathscr{H}$, de modo que, pela continuidade de $f(\tau)$ em $\mathscr{H}$, para um j fixo, $f(\tau) = a_0(j)$, para todo $\tau \in \mathscr{H}$, ou seja, $f(\tau)$ é constante. □

A fortiori, temos o seguinte

Corolário 9. *Toda função modular limitada em $\mathscr{H}$ é constante.*

Demonstração. Seja $f(\tau)$ uma função modular com respeito a Γ. Como $f(\tau)$ é, por definição, meromorfa em $\mathscr{H}$ e, pelo enunciado, limitada nesse conjunto, segue que $f(\tau)$ é regular em $\mathscr{H}$. Além disso, a expansão da forma (3.7) de $f(\tau)$ em cada ponto parabólico q_j é

$$f(\tau) = \sum_{n=-n_0(j)}^{\infty} a_n(j) e^{2\pi i n(A_j^{-1}\tau)/\lambda_j},$$

válida em $\mathscr{H}$, pois $f(\tau)$ é meromorfa em q_j. Além disso, como $f(\tau)$ é função modular, utilizamos que $\sigma_j(\tau) = 1$ e que $\kappa_j = 0$, como na demonstração do Lema 7. Também por aquela demonstração, sabemos que a expansão acima pode ser vista como uma série de potências na variável $z = e^{2\pi i(A_j^{-1}\tau)/\lambda_j}$, convergente para $|z| < 1$. Logo, caso, na expansão acima, apareça, para $n < 0$, um termo $a_n(j)$ não nulo, fazendo $\tau \to q_j$ de dentro de $\mathscr{R}$, teríamos $z \to 0$ e, portanto, $f(\tau)$ não seria limitada em $\mathscr{H}$. Desse modo, a expansão de $f(\tau)$ em cada ponto parabólico q_j possui a forma (3.16), donde $f(\tau)$ é regular também nos pontos parabólicos de Γ em $\mathscr{R}$, de tal maneira que o Teorema 8 nos garante o corolário. □

O lema que vem a seguir será utilizado na demonstração do Teorema 12. Ambos os resultados são devidos a Hecke (*apud* [11], consulte *Werke* (Göttingen: Vandenhoech and Ruprecht, 1959), pp. 461-486, esp. p. 484).

Lema 10. *Se $F(\tau)$ é uma forma cúspide de grau $-r$ com respeito a Γ, então $|F(\tau)| \leq C[\mathfrak{Im}(\tau)]^{-r/2}$, para todo $\tau \in \mathscr{H}$, onde C é uma constante positiva independente de τ.*

Demonstração. Sendo $\tau = x + iy \in \mathscr{H}$ $(y > 0)$, devemos mostrar que $|F(\tau)| \leq Cy^{-r/2}$. Considere $\varphi(\tau) = \varphi(x+iy) = |y^{r/2}F(x+iy)|$ e tome $M = \begin{pmatrix} * & * \\ \gamma & \delta \end{pmatrix} \in \Gamma$. Sabemos, pela relação (2.2) do Capítulo 2, que

$$\mathfrak{Im}(M\tau) = \frac{\mathfrak{Im}(\tau)}{|\gamma\tau + \delta|^2} = \frac{y}{|\gamma\tau + \delta|^2},$$

donde

$$\begin{aligned}\varphi(M\tau) &= \left|[\mathfrak{Im}(M\tau)]^{r/2}F(M\tau)\right| \\ &= \left|\frac{y^{r/2}}{|\gamma\tau+\delta|^r}\upsilon(M)(\gamma\tau+\delta)^r F(\tau)\right| \\ &= \left|y^{r/2}F(\tau)\right| = \varphi(\tau),\end{aligned}$$

utilizando-se também (3.1) para $F(\tau)$ e o fato de que $|\upsilon(M)| = 1$. Deste modo, $\varphi(\tau)$ é invariante com respeito a Γ. Provaremos, a seguir, que $\varphi(\tau) \to 0$ à medida que $\tau \to q_j$ de dentro de $\mathscr{R}$, para $1 \leq j \leq \mu$, similarmente à maneira que procedemos no Lema 7. Como $F(\tau)$ é uma forma cúspide, a expansão de Fourier de $F(\tau)$ em cada ponto parabólico q_j tem a forma

$$F(\tau) = \sigma_j(\tau)\sum_{n+\kappa_j>0} a_n(j)e^{2\pi i(n+\kappa_j)(A_j^{-1}\tau)/\lambda_j},$$

para todo $\tau \in \mathscr{H}$. Considere $A_j^{-1}\tau = x' + iy'$, sendo $A_j = \begin{pmatrix} a & * \\ c & * \end{pmatrix}$ e, portanto, $A_j^{-1} = \begin{pmatrix} * & * \\ -c & a \end{pmatrix}$. Neste caso, $q_j = A_j(\infty) = a/c < \infty$ se, e somente se, $c \neq 0$, de modo que, se $c \neq 0$,

$$\begin{aligned}y^{r/2} &= [\mathfrak{Im}(\tau)]^{r/2} \\ &= \left[\mathfrak{Im}(A_j^{-1}\tau)|-c\tau+a|^2\right]^{r/2} \\ &= (y')^{r/2}|-c\tau+a|^r \\ &= (y')^{r/2}\left|-c\left(\tau-\frac{a}{c}\right)\right|^r \\ &= (y')^{r/2}|c|^r|\tau-q_j|^r = (y')^{r/2}|\sigma_j(\tau)|^{-1}|c|^r\end{aligned}$$

e, se $c = 0$, então $a = \pm 1$, donde

$$y^{r/2} = \left[\mathfrak{Im}(A_j^{-1}\tau)|-c\tau+a|^2\right]^{r/2} = (y')^{r/2} = (y')^{r/2}\underbrace{|\sigma_j(\tau)|^{-1}}_{1}\cdot 1.$$

Em resumo,

$$y^{r/2} = (y')^{r/2}|\sigma_j(\tau)|^{-1}\beta(c),$$

onde

$$\beta(c) = \begin{cases} |c|^r, & \text{se } c \neq 0 \\ 1, & \text{se } c = 0 \end{cases}$$

Assim, para $\tau \in \mathscr{H}$,

$$\begin{aligned}
\varphi(\tau) &= |y^{r/2}F(\tau)| \\
&= y^{r/2}|F(\tau)| \\
&= (y')^{r/2}|\sigma_j(\tau)|^{-1}\beta(c)\left|\sigma_j(\tau)\sum_{n+\kappa_j>0} a_n(j)e^{2\pi i(n+\kappa_j)(A_j^{-1}\tau)/\lambda_j}\right| \\
&= (y')^{r/2}\beta(c)\left|\sum_{n+\kappa_j>0} a_n(j)e^{2\pi i(n-n_0+n_0+\kappa_j)(A_j^{-1}\tau)/\lambda_j}\right| \\
&= (y')^{r/2}\beta(c)\left|\sum_{n+\kappa_j>0} a_n(j)e^{2\pi i(n-n_0)(A_j^{-1}\tau)/\lambda_j}e^{2\pi i(n_0+\kappa_j)(A_j^{-1}\tau)/\lambda_j}\right| \\
&= (y')^{r/2}\beta(c)\left|e^{2\pi i(n_0+\kappa_j)(A_j^{-1}\tau)/\lambda_j}\sum_{n+\kappa_j>0} a_n(j)e^{2\pi i(n-n_0)(A_j^{-1}\tau)/\lambda_j}\right| \\
&= (y')^{r/2}\beta(c)\left|e^{2\pi i(n_0+\kappa_j)x'/\lambda_j}e^{2\pi i(n_0+\kappa_j)iy'/\lambda_j}\sum_{n+\kappa_j>0} a_n(j)e^{2\pi i(n-n_0)(A_j^{-1}\tau)/\lambda_j}\right| \\
&= (y')^{r/2}\beta(c)e^{-2\pi(n_0+\kappa_j)y'/\lambda_j}\left|\sum_{n+\kappa_j>0} a_n(j)e^{2\pi i(n-n_0)(A_j^{-1}\tau)/\lambda_j}\right| \\
&= (y')^{r/2}\beta(c)e^{-2\pi(n_0+\kappa_j)y'/\lambda_j}\left|\sum_{n\geq n_0} a_n(j)e^{2\pi i(n-n_0)(A_j^{-1}\tau)/\lambda_j}\right|,
\end{aligned}$$

supondo-se, na última passagem, que n_0 é o inteiro não negativo tal que $n_0+\kappa_j>0$ é a ordem do zero de $F(\tau)$ em q_j. O somatório da última igualdade pode ser visto como uma série de potências na variável $z=e^{2\pi i(A_j^{-1}\tau)/\lambda_j}$, convergente para $|z|<1$. Conforme $\tau\to q_j$ a partir de pontos de $\mathscr{R}$, o Lema 1 nos diz que $y'=\mathfrak{Im}\left(A_j^{-1}\tau\right)\to\infty$ de dentro de uma faixa vertical contida em $\mathscr{H}$, donde $z\to 0$ e, portanto, a série acima tende ao valor fixo $a_{n_0}(j)$. Portanto, como $e^{-2\pi(n_0+\kappa_j)y'/\lambda_j}\to 0$, vem que $\varphi(\tau)\to 0$ à medida que $\tau\to q_j$ de dentro de $\mathscr{R}$. Aqui, utilizamos também que, se $r<0$, então $(y')^{r/2}\to 0$ e, se $r>0$, então $(y')^{r/2}$ possui crescimento ilimitado, porém inibido pelo decréscimo de $e^{-2\pi(n_0+\kappa_j)y'/\lambda_j}$. Assim, utilizando-se o mesmo raciocínio da demonstração do Teorema 8, como isso ocorre para cada ponto parabólico q_j, segue que $\varphi(\tau)$ assume seu máximo num conjunto $\mathscr{R}^*$ da forma exibida em (3.17). Como $\overline{\mathscr{R}^*}$ é um subconjunto compacto de $\mathscr{H}$ e $\varphi(\tau)$ é contínua nesse conjunto, temos que $\varphi\left(\overline{\mathscr{R}^*}\right)$ é compacto em $[0,\infty)$. Nesse caso,

$\varphi(\tau)$ é limitada em $\overline{\mathscr{R}^*}$, e portanto em $\mathscr{R}^*$, ou seja, $\varphi(\tau) \leq C$, $C > 0$, para todo $\tau \in \mathscr{H}$, por argumento similar ao da demonstração do Lema 7. Logo,

$$|F(\tau)| = \frac{\varphi(\tau)}{y^{r/2}} \leq Cy^{-r/2},$$

para todo $\tau \in \mathscr{H}$. □

Através de um raciocínio semelhante ao da demonstração anterior, podemos mostrar também o seguinte resultado mais fraco, porém mais geral, acerca de formas modulares:

Proposição 11. *Suponha que $F(\tau)$ seja uma forma modular com respeito a Γ e que q seja um dos pontos parabólicos de Γ em $\mathscr{R}$. Então, se $F(\tau)$ possui um zero de ordem positiva em q, segue que $F(\tau) \to 0$ à medida que $\tau \to q$ de dentro de $\mathscr{R}$.*

Demonstração. Diferentemente do lema anterior, neste caso, é-nos garantido que $F(\tau)$ possui um zero de ordem positiva apenas no ponto parabólico q. Neste ponto, a expansão da forma (3.7) de $F(\tau)$ é

$$F(\tau) = \sigma(\tau) \sum_{n+\kappa>0} a_n e^{2\pi i(n+\kappa)(A^{-1}\tau)/\lambda}, \qquad \tau \in \mathscr{H},$$

desconsiderando-se os índices. Efetuando-se cálculos parecidos com os que fizemos para $\varphi(\tau)$ no lema anterior, temos

$$|F(\tau)| = |\sigma(\tau)| e^{-2\pi(n_0+\kappa)\mathfrak{Im}(A^{-1}\tau)/\lambda} \left| \sum_{n \geq n_0} a_n e^{2\pi i(n-n_0)(A^{-1}\tau)/\lambda} \right|,$$

sendo n_0 o inteiro tal que $n_0 + \kappa > 0$ é a ordem do zero de $F(\tau)$ em q. Se $\tau \to q$ de dentro de $\mathscr{R}$, a série acima converge para a_{n_0} e $e^{-2\pi(n_0+\kappa)\mathfrak{Im}(A^{-1}\tau)/\lambda} \to \infty$. Ademais, se $q = \infty$, então $\sigma(\tau) = 1$ e, se $q \neq \infty$, $\sigma(\tau) \to \infty$, porém $e^{-2\pi(n_0+\kappa)\mathfrak{Im}(A^{-1}\tau)/\lambda}$ predomina em relação a $\sigma(\tau)$, donde $|F(\tau)| \to 0$, ou $F(\tau) \to 0$. □

Teorema 12. *Suponha que $F(\tau)$ seja uma forma cúspide de grau $-r$ com respeito a Γ. Seja $\mathscr{R}$ uma região fundamental padronizada segundo Γ, normalizada de modo que $A_1 = I$, e portanto $q_1 = \infty$. Seja $\kappa = \kappa_1$, $\lambda = \lambda_1$ e $a_n = a_n(1)$, de modo que a expansão de Fourier de $F(\tau)$ em q_1 assume a forma*

$$F(\tau) = \sum_{n+\kappa>0} a_n e^{2\pi i(n+\kappa)\tau/\lambda}, \qquad \tau \in \mathscr{H}. \tag{3.18}$$

Então $|a_n| \leq C' n^{r/2}$, para todo $n \geq 1$, onde C' é uma constante positiva que não depende de n.

Demonstração. Seja $z = x + iy \in \mathscr{H}$, de modo que, para $n \geq 1$ fixo, porém arbitrário,

$$\begin{aligned}\int_z^{z+\lambda} F(\zeta)e^{-2\pi i(n+\kappa)\zeta/\lambda}\mathrm{d}\zeta &= \int_z^{z+\lambda}\left(\sum_{m+\kappa>0} a_m e^{2\pi i(m+\kappa)\zeta/\lambda}\right)e^{-2\pi i(n+\kappa)\zeta/\lambda}\mathrm{d}\zeta \\ &= \int_z^{z+\lambda}\left(\sum_{m+\kappa>0} a_m e^{2\pi i(m-n)\zeta/\lambda}\right)\mathrm{d}\zeta \\ &= \sum_{m+\kappa>0}\left(\int_z^{z+\lambda} a_m e^{2\pi i(m-n)\zeta/\lambda}\mathrm{d}\zeta\right),\end{aligned}$$

sendo a permutação dos símbolos de integral e somatório justificada pelo fato da série acima ser simplesmente uma série de potências na variável $e^{2\pi i\zeta/\lambda}$. Agora, para $m \neq n$, podemos calcular cada integral do somatório acima ao longo do caminho horizontal que une z a $z+\lambda$. Denotando $\zeta = \phi(t) + i\psi(t)$, temos $\phi(t) = t$ e $\psi(t) = y$, para $x \leq t \leq x+\lambda$, e $\mathrm{d}\zeta = \mathrm{d}\phi(t) + i\mathrm{d}\psi(t) = \mathrm{d}t + i\cdot 0 = \mathrm{d}t$. Logo, nesse caso,

$$\begin{aligned}&\int_z^{z+\lambda} a_m e^{2\pi i(m-n)\zeta/\lambda}\mathrm{d}\zeta = \\ &= a_m\int_x^{x+\lambda} e^{2\pi i(m-n)(t+iy)/\lambda}\mathrm{d}t \\ &= a_m e^{-2\pi(m-n)y/\lambda}\int_x^{x+\lambda} e^{2\pi i(m-n)t/\lambda}\mathrm{d}t \\ &= a_m e^{-2\pi(m-n)y/\lambda}\left[\int_x^{x+\lambda}\cos\left(\frac{2\pi(m-n)t}{\lambda}\right)\mathrm{d}t + i\int_x^{x+\lambda}\operatorname{sen}\left(\frac{2\pi(m-n)t}{\lambda}\right)\mathrm{d}t\right] \\ &= a_m e^{-2\pi(m-n)y/\lambda}\frac{\lambda}{2\pi(m-n)}\underbrace{\left[\operatorname{sen}\left(\frac{2\pi(m-n)t}{\lambda}\right) - i\cos\left(\frac{2\pi(m-n)t}{\lambda}\right)\right]_x^{x+\lambda}}_{0} = 0.\end{aligned}$$

Por outro lado, para $m = n$, considerando novamente $\zeta = t+iy$, $x \leq t \leq x+\lambda$, e $\mathrm{d}\zeta = \mathrm{d}t$, vem

$$\int_z^{z+\lambda} a_m e^{2\pi i(m-n)\zeta/\lambda}\mathrm{d}\zeta = a_n\int_x^{x+\lambda}\mathrm{d}\zeta = \lambda a_n,$$

donde

$$\int_z^{z+\lambda} F(\zeta)e^{-2\pi i(n+\kappa)\zeta/\lambda}\mathrm{d}\zeta = \lambda a_n,$$

ou

$$\boxed{a_n = \tfrac{1}{\lambda}\textstyle\int_z^{z+\lambda} F(\zeta)e^{-2\pi i(n+\kappa)\zeta/\lambda}\mathrm{d}\zeta,}$$

para todo $n \geq 1$, sendo $z \in \mathscr{H}$ arbitrário. Utilizando-se o Lema 10 e algumas propriedades de integrais, vem

$$\begin{aligned}
|a_n| &= \frac{1}{\lambda}\left|\int_z^{z+\lambda} F(\zeta)e^{-2\pi i(n+\kappa)\zeta/\lambda}\mathrm{d}\zeta\right| \\
&\leq \frac{1}{\lambda}\int_z^{z+\lambda}\left|F(\zeta)e^{-2\pi i(n+\kappa)\zeta/\lambda}\right|\mathrm{d}\zeta \\
&= \frac{1}{\lambda}\int_x^{x+\lambda}|F(\zeta)|\left|e^{-2\pi i(n+\kappa)(t+iy)/\lambda}\right|\mathrm{d}t \\
&= \frac{e^{2\pi(n+\kappa)y/\lambda}}{\lambda}\int_x^{x+\lambda}|F(\zeta)|\mathrm{d}t \\
&\leq \frac{e^{2\pi(n+\kappa)y/\lambda}}{\lambda}\int_x^{x+\lambda}Cy^{-r/2}\mathrm{d}t \\
&= Cy^{-r/2}e^{2\pi(n+\kappa)y/\lambda},
\end{aligned}$$

uma vez que y é constante no caminho horizontal que une z a $z+\lambda$. Como a desigualdade acima vale para todo $z \in \mathscr{H}$, podemos tomar $y = \mathfrak{Im}(z) = 1/n$, donde, para $n \geq 1$,

$$|a_n| \leq C\left(\frac{1}{n}\right)^{-r/2} e^{2\pi(n+\kappa)/n\lambda} \leq Cn^{r/2}e^{2\pi(2n)/n\lambda} = \underbrace{Ce^{4\pi/\lambda}}_{C'}n^{r/2},$$

onde C' é uma constante positiva independente de n. □

Corolário 13. *Toda forma cúspide de grau positivo é identicamente nula.*

Demonstração. Suponhamos $F(\tau)$ como no Teorema 12, com $r < 0$. No decorrer da demonstração desse teorema, vimos que $|a_n| \leq Cy^{-r/2}e^{2\pi(n+\kappa)y/\lambda}$, para todo $n \geq 1$, sendo y um número real positivo arbitrário. Fazendo $y \to 0^+$, temos que $y^{-r/2} \to 0$ e $e^{2\pi(n+\kappa)y/\lambda} \to 1$. Logo, como $\lim_{y\to 0^+}|a_n| = |a_n|$ $(= 0)$, temos que $|a_n| = 0$, ou $a_n = 0$, para todo n. Portanto, lembrando-se da expressão de $F(\tau)$, dada por (3.18), vem que $F(\tau)$ é identicamente nula. □

Mais forte do que o último corolário, temos o seguinte teorema, bastante conhecido dentro da teoria que estudamos.

Teorema 14. *Se $F(\tau)$ é uma forma modular inteira de grau positivo com respeito a Γ, então $F(\tau)$ é identicamente nula.*

Demonstração. Afirmamos, primeiramente, que sempre existe uma região fundamental padronizada $\mathscr{R}'$ segundo Γ tal que ∞ não é um ponto parabólico de Γ em $\mathscr{R}'$. Para constatá-lo, observe que sempre existe um inteiro positivo n tal que $W^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \in \Gamma$, sendo $W = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \Gamma(1)$. De fato, caso contrário, W, W^2, W^3, ..., constituiriam uma família infinita de elementos distintos módulo Γ, contradizendo o fato de Γ ser de índice finito em $\Gamma(1)$.

Suponhamos, então, que $\mathscr{R} = \bigcup_{j=1}^{\mu} A_j\{\mathscr{R}(\Gamma(1))\}$ seja uma região fundamental padronizada arbitrária segundo Γ. Efetuando-se a substituição

$$\begin{cases} B_j = A_j, & \text{se } A_j(\infty) \neq \infty \\ B_j = W^n A_j, & \text{se } A_j(\infty) = \infty \end{cases},$$

para $1 \leq j \leq \mu$, como $W^n \in \Gamma$, podemos considerar uma nova decomposição $\Gamma(1) = \bigcup_{j=1}^{\mu} \Gamma B_j$ e, portanto, uma nova região fundamental padronizada

$$\mathscr{R}' = \bigcup_{j=1}^{\mu} B_j\{\mathscr{R}(\Gamma(1))\},$$

cujos pontos parabólicos são todos distintos de ∞. De fato, sendo $q_j = B_j(\infty)$, $1 \leq j \leq \mu$, os pontos parabólicos de Γ nessa nova região fundamental padronizada, se $B_j = A_j$, então $q_j = A_j(\infty) \neq \infty$ e, se $B_j = W^n A_j$, então $q_j = W^n A_j(\infty) = W^n(\infty) = 1/n \neq \infty$.

Portanto, a expansão de Fourier de $F(\tau)$ em cada ponto parabólico q_j de Γ em $\mathscr{R}'$ é

$$F(\tau) = (\tau - q_j)^{-r} \sum_{n+\kappa_j \geq 0} a_n(j) e^{2\pi i (n+\kappa_j)(B_j^{-1}\tau)/\lambda_j}, \qquad \tau \in \mathscr{H}.$$

Na expressão acima, $r < 0$ e o somatório envolve apenas $n + \kappa_j \geq 0$ porque $F(\tau)$ é uma forma modular inteira de grau positivo. Além disso, o fato de q_j ser distinto de ∞ implica que $\sigma_j(\tau) = (\tau - q_j)^{-r}$. Como na prova do Lema 10, a função $\varphi(\tau) = \varphi(x+iy) = \left| y^{r/2} F(x+iy) \right|$ tem a propriedade de que $\varphi(V\tau) = \varphi(\tau)$, para todo $V \in \Gamma$. Pelo Lema 1, se $\tau \to q_j$ de dentro de $\mathscr{R}'$, $B_j^{-1}\tau \to \infty$ de dentro de uma faixa vertical da forma $a_j < x < b_j$, $y > 0$, para $z = x + iy$. Denotando $B_j^{-1}\tau = x' + iy'$, com $B_j = \begin{pmatrix} * & * \\ c & * \end{pmatrix}$, repetindo os cálculos da prova do Lema 10, temos

$$y^{r/2} = (y')^{r/2} |\tau - q_j|^r |c|^r,$$

donde

$$\varphi(\tau) = \left|y'^{r/2}F(\tau)\right| = |c|^r (y')^{r/2} \left| \sum_{n+\kappa_j \geq 0} a_n(j) e^{2\pi i (n+\kappa_j)(B_j^{-1}\tau)/\lambda_j} \right|,$$

Assim, se $\tau \to q_j$ a partir de pontos de $\mathscr{R}'$, $y' = \mathfrak{Im}(B_j^{-1}\tau) \to \infty$, donde $(y')^{r/2} \to 0$, uma vez que $r < 0$. Logo, $\varphi(\tau) \to 0$. Como na demonstração do Lema 10, como isso ocorre para cada ponto parabólico de Γ em $\mathscr{R}'$, segue que existe $C > 0$ tal que $\varphi(\tau) \leq C$, para todo $\tau \in \mathscr{H}$, e, portanto, $|F(\tau)| \leq C y^{-r/2}$, $\tau \in \mathscr{H}$.

O último resultado a que chegamos independe da região fundamental padronizada considerada. Assim, consideremos uma região fundamental padronizada $\mathscr{R}$ normalizada como a do enunciado do Teorema 12, e tomemos a expansão de Fourier de $F(\tau)$ em ∞

$$F(\tau) = \sum_{n+\kappa \geq 0} a_n e^{2\pi i (n+\kappa)\tau/\lambda}, \qquad \tau \in \mathscr{H}.$$

Como na demonstração daquele teorema, podemos concluir que $|a_n| \leq C y^{-r/2} e^{2\pi(n+\kappa)y/\lambda}$, para $n \geq 0$ e $y > 0$ arbitrário. Daqui em diante, a prova segue exatamente como a do corolário anterior: fazendo $y \to 0^+$, concluimos que $a_n = 0$ para $n \geq 0$ e, portanto, que $F(\tau)$ é identicamente nula. □

Observação: A maior dificuldade dessa demonstração foi chegar-se ao fato de que, para $\tau \in \mathscr{H}$, $|F(\tau)| \leq C y^{-r/2}$. A partir desse ponto, seguiram-se apenas resultados anteriores. Poderíamos, nessa demonstração, ter utilizado o mesmo procedimento da demonstração do Lema 10 (um dos motivos pelos quais não fizemos isso foi a oportunidade de exibir a construção da região fundamental padronizada $\mathscr{R}'$ do teorema, cujos pontos parabólicos são todos finitos). Neste caso, concluiríamos, a certa altura, que

$$\varphi(\tau) = (y')^{r/2} \beta(c) e^{-2\pi(n_0+\kappa_j)y'/\lambda_j} \left| \sum_{n \geq n_0} a_n(j) e^{2\pi i (n-n_0)(A_j^{-1}\tau)/\lambda_j} \right|,$$

para $\tau \in \mathscr{H}$. Utilizando-se o mesmo raciocínio lá empregado, somos tentados a afirmar que, à medida que $\tau \to q_j$ de dentro de $\mathscr{R}$, $\varphi(\tau) \to 0$ e, repetindo toda a argumentação da prova do teorema, $F(\tau)$ é identicamente nula, mesmo sendo de grau negativo ($r > 0$). Entretanto, o fato de r ser negativo é condição *sine qua non* mesmo para esta demonstração. De fato, como $F(\tau)$ não é forma cúspide, não temos a garantia de que $n_0 + \kappa_j > 0$. Sabemos apenas que $n_0 + \kappa_j \geq 0$, donde $e^{-2\pi(n_0+\kappa_j)y'/\lambda_j}$ pode ser igual a 1, não convergindo para 0.

O seguinte teorema finaliza este capítulo, e será de utilidade em situações futuras:

Teorema 15. *Sejam Γ_1 e Γ_2 subgrupos de índice finito em $\Gamma(1)$ tais que $\Gamma_2 \leqslant \Gamma_1 \leqslant \Gamma(1)$. Suponhamos, ainda, que $\Gamma_1 = \bigcup_{i=1}^{\mu} \Gamma_2 A_i$ seja uma decomposição de Γ_1 em μ classes laterais distintas de Γ_2. Seja $g(\tau)$ uma função invariante com relação a Γ_2, no sentido de que $g(V\tau) = g(\tau)$, para todo $V \in \Gamma_2$. Então, se $F(x_1, x_2, \ldots, x_\mu)$ é simétrica com respeito a seus μ parâmetros, a função $f(\tau) = F(g(A_1\tau), g(A_2\tau), \ldots, g(A_\mu\tau))$ é invariante com relação a Γ_1.*

Demonstração. Se $M \in \Gamma_1$, então, para cada i, $A_iM \in \Gamma_1$. Como $\Gamma_1 = \bigcup_{i=1}^{\mu} \Gamma_2 A_i$, vem que $A_iM = M_iA_i'$, onde $M_i \in \Gamma_2$ e $A_i' \in \{A_1, A_2, \ldots, A_\mu\} = C$. Afirmamos que, conforme se atribuem as μ possibilidades para A_i, as μ possibilidades de A_i' correspondentes percorrem todo o conjunto C. De fato, supondo-se que $A_iM = M_iA_i'$ e $A_jM = M_jA_j'$, com $A_i' = A_j'$, temos

$$A_iA_j^{-1} = (A_iM)(A_jM)^{-1} = (M_iA_i')(M_jA_j')^{-1} = M_iM_j^{-1} \in \Gamma_2,$$

donde $i = j$ e, portanto, $A_i = A_j$. Portanto, temos que

$$\begin{aligned} f(M\tau) &= F(g(A_1M\tau), g(A_2M\tau), \ldots, g(A_\mu M\tau)) \\ &= F(g(M_1A_1'\tau), g(M_2A_2'\tau), \ldots, g(M_\mu A_\mu'\tau)) \\ &= F(g(A_1'\tau), g(A_2'\tau), \ldots, g(A_\mu'\tau)) \\ &= F(g(A_1\tau), g(A_2\tau), \ldots, g(A_\mu\tau)) = f(\tau), \end{aligned}$$

utilizando-se que $g(\tau)$ é Γ_2-invariante, que os elementos A' percorrem o conjunto C e que F é simétrica. Como isso é válido para todo $M \in \Gamma_1$, segue que $f(\tau)$ é Γ_1-invariante. □

Observação: Se $g(\tau)$ é uma função modular com respeito a Γ_2, então $r = 0$ e $\upsilon \equiv 1$ em Γ_2 e, portanto, $g(V\tau) = g(\tau)$ para cada $V \in \Gamma_2$. Logo, se $F(x_1, x_2, \ldots, x_\mu)$ é um polinômio simétrico, então, pelo teorema anterior, $f(M\tau) = f(\tau)$, para cada $M \in \Gamma_1$. Além disso, como $f(\tau) = F(g(A_1\tau), g(A_2\tau), \ldots, g(A_\mu\tau))$, dado que F é um polinômio simétrico, as propriedades necessárias para que $f(\tau)$ seja considerada forma modular são satisfeitas, donde se conclui que $f(\tau)$ é uma função modular com respeito a Γ_1.

Capítulo 4

As formas modulares $\eta(\tau)$ e $\vartheta(\tau)$

4.1 A função $\eta(\tau)$

Para $\tau \in \mathscr{H}$, definimos

$$\eta(\tau) = e^{\pi i \tau/12} \prod_{m=1}^{\infty} \left(1 - e^{2\pi i m \tau}\right).$$

Um dos grandes objetivos deste capítulo é mostrar que $\eta(\tau)$ que, como veremos, possui relação com teoria dos números, é uma forma modular de grau $-1/2$ com respeito a $\Gamma(1)$. Para alcançá-lo, precisamos provar que $\eta(\tau)$ satisfaz as condições da Definição 6 do Capítulo 3, o que não é tarefa das mais triviais. Afirmamos primeiro que $\eta(\tau) \neq 0$, para todo $\tau = x + iy \in \mathscr{H}$. De fato, como $e^{\pi i \tau/12} \neq 0$, vem que que $\eta(\tau) = 0$ se, e somente se, existe um inteiro positivo m tal que $1 - e^{2\pi i m \tau} = 0$. Ora, nesse caso, $e^{2\pi i m x} = e^{2\pi m y}$, ou $\cos(2\pi m x) + i\text{sen}(2\pi m x) = e^{2\pi m y}$, donde

$$\begin{cases} \cos(2\pi m x) = e^{2\pi m y} \\ \text{sen}(2\pi m x) = 0 \end{cases}$$

e, portanto, $2\pi m x = 0$ ou $2\pi m x = -\pi$. A primeira possibilidade implica que $x = 0$ e $e^{2\pi m y} = \cos 0 = 1$, ou $y = 0$. A segunda implica que $x = -1/(2m)$ e $e^{2\pi m y} = \cos(-\pi) = -1$. Ambas são contradições, ora com o fato de y ser positivo, ora com o fato de que $e^{2\pi m y}$ é sempre maior do que 0, para qualquer y real.

A seguir, apresentamos uma definição bastante conhecida, cujo objeto será a ponte entre a função $\eta(\tau)$ e a teoria dos números:

Definição 1. *Definimos $p(n)$ como a função que associa a cada número inteiro positivo n o número de partições de n em partes inteiras também positivas. Aqui, as partes não*

são necessariamente distintas, e sua ordem na partição não é relevante. Além disso, convencionamos que $p(0) = 1$.

Exemplo: Temos que $p(6) = 11$, pois 6 pode ser particionado como 6, $5+1$, $4+2$, $4+1+1$, $3+3$, $3+2+1$, $3+1+1+1$, $2+2+2$, $2+2+1+1$, $2+1+1+1+1$ e $1+1+1+1+1+1$.

Euler foi o primeiro a observar a seguinte identidade:

$$\prod_{n=1}^{\infty}(1-x^n)^{-1} = \sum_{m=0}^{\infty} p(m)x^m. \tag{4.1}$$

Essa identidade admite uma demonstração combinatória muito simples. O coeficiente de x^m em seu membro direito corresponde a $p(m)$. Por outro lado, em seu membro esquerdo, para n variando de 1 a m, $(1-x^n)^{-1}$ controla o número de partes iguais a n numa dada partição de m. Por exemplo,

$$(1-x^3)^{-1} = \frac{1}{1-x^3} = 1 + x^3 + x^6 + x^9 + \cdots = 1 + x^3 + x^{3+3} + x^{3+3+3} + \cdots .$$

Fica claro, portanto, que o coeficiente de x^m no membro esquerdo de (4.1) se refere também ao número de partições de m, estabelecendo-se a identidade.

Na argumentação anterior, utilizamos o fato de que $(1-x^n)^{-1} = 1 + x^n + x^{2n} + \cdots$, sem nos preocuparmos com questões de convergência. Com efeito, essas identidades possuem validade estritamente assegurada apenas para $|x| < 1$. Entretanto, no contexto de funções geradoras (em Combinatória, costumamos denominar o membro esquerdo de (4.1) a *função geradora* para o número de partições de m), interessam-nos apenas os coeficientes dessas funções, uma vez que não atribuimos valor à variável x. Vistas desta forma, tais séries são chamadas *séries formais*. Caso haja interesse por parte do leitor nesse aspecto, sugerimos, *apud* [23], a leitura do artigo [20]. Desta maneira, o que exibimos acima é uma demonstração formal de que (4.1) é verdadeira.

No caso que aqui nos interessa, todavia, vamos atribuir valor à variável x, de modo que precisamos demonstrar analiticamente a identidade em questão.

Proposição 1. *Se* $|x| < 1$, *então ambos os membros de (4.1) convergem e são iguais.*

Demonstração. Se $|x| < 1$, então $\sum_{n=1}^{\infty} x^n$ converge absolutamente, donde o mesmo ocorre para $\prod_{n=1}^{\infty}(1-x^n)$ (consulte o Capítulo 1). Logo, este produto também converge. Ademais, como $1 - x^n \neq 0$ para cada inteiro positivo n, vem que $\prod_{n=1}^{\infty}(1-x^n)$ converge para

uma função analítica sem zeros em $|x| < 1$. Logo, $\prod_{n=1}^{\infty}(1-x^n)^{-1} = \left(\prod_{n=1}^{\infty}(1-x^n)\right)^{-1}$ também possui tal propriedade.

Agora, provaremos que $\sum_{m=0}^{\infty} p(m)x^m$ também converge quando $|x| < 1$. Primeiramente, todavia, consideremos $0 \leq x < 1$. Sendo N um inteiro positivo, temos

$$\prod_{n=1}^{N}(1-x^n)^{-1} = \prod_{n=1}^{N}\left(\sum_{j=0}^{\infty} x^{nj}\right).$$

Pelo mesmo argumento que apresentamos antes desta proposição, o coeficiente de x^m $(0 \leq m \leq N)$ em $\prod_{n=1}^{N}\left(\sum_{j=0}^{\infty} x^{nj}\right)$ é igual a $p(m)$ (neste caso, a maior parte que pode ocorrer numa partição de m é, de fato, N), e podemos escrever

$$\prod_{n=1}^{N}(1-x^n)^{-1} = \sum_{m=0}^{N} p(m)x^m + \sum_{m=N+1}^{\infty} a_m x^m, \tag{4.2}$$

onde $0 \leq a_m \leq p(m)$. Em suma, (4.2) é verdadeira porque seu membro esquerdo é justamente a função geradora para o número de partições em partes que valem, no máximo, N. Portanto, segue, para $0 \leq x < 1$, que

$$\sum_{m=0}^{N} p(m)x^m \leq \prod_{n=1}^{N}(1-x^n)^{-1} \leq \prod_{n=1}^{\infty}(1-x^n)^{-1},$$

sendo a última desigualdade justificada pelo fato de que, para cada n,

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

Como $p(m)x^m \geq 0$, para cada m, temos que $\sum_{m=0}^{N} p(m)x^m$ é uma função monótona crescente de N, limitada por $\prod_{n=1}^{\infty}(1-x^n)^{-1}$, que sabemos convergir. Logo, $\sum_{m=0}^{N} p(m)x^m$ é convergente, com $\sum_{m=0}^{\infty} p(m)x^m \leq \prod_{n=1}^{\infty}(1-x^n)^{-1}$. Por outro lado, também utilizando a relação (4.2), temos

$$\prod_{n=1}^{N}(1-x^n)^{-1} \leq \sum_{m=0}^{N} p(m)x^m + \sum_{m=N+1}^{\infty} p(m)x^m = \sum_{m=0}^{\infty} p(m)x^m,$$

para cada inteiro positivo N, donde, tomando $N \to \infty$, temos que $\prod_{n=1}^{\infty}(1-x^n)^{-1} \leq \sum_{m=0}^{\infty} p(m)x^m$. Logo, para $0 \leq x < 1$, $\prod_{n=1}^{\infty}(1-x^n)^{-1} = \sum_{m=0}^{\infty} p(m)x^m$, e a proposição é válida.

Agora, suponhamos apenas que $|x| < 1$. Já sabemos que, nesse caso, o membro esquerdo de (4.1) converge. Além disso, $\sum_{m=0}^{\infty} |p(m)x^m| = \sum_{m=0}^{\infty} p(m)|x|^m$, pelo raciocínio

anterior, como $0 \leq |x| < 1$, converge para $\prod_{n=1}^{\infty}(1-|x|^n)^{-1}$. Dado que convergência absoluta implica convergência, segue que $\sum_{m=0}^{\infty} p(m)x^m$ converge para uma função analítica quando $|x|<1$. Pelo raciocínio anterior, podemos aplicar o Teorema 1 do Capítulo 1, considerando-se $D = D_1 = D_2 = \{x \in \mathbb{C} \mid |x| < 1\}$, $f(x) = \prod_{n=1}^{\infty}(1-x^n)^{-1}$, $g(x) = \sum_{m=0}^{\infty} p(m)x^m$ e, por exemplo, $x_k = 1/(k+1)$, donde $f(x_k) = g(x_k)$ (isso é garantido pelo que provamos para $0 \leq x < 1$), para cada inteiro positivo k, e $x_k \to 0 \in D$. Como conclusão do teorema, temos que $f(x) = g(x)$ em D, completando a prova. □

A relação entre $\eta(\tau)$ e $p(m)$ está contida no seguinte corolário:

Corolário 2. *Para $\tau \in \mathscr{H}$,*

$$[\eta(\tau)]^{-1} = \sum_{m=0}^{\infty} p(m)e^{2\pi i(m-1/24)\tau} = \sum_{m=-1}^{\infty} p(m+1)e^{2\pi i(m+23/24)\tau}.$$

Demonstração. Se $\tau = x + iy \in \mathscr{H}$, então $|e^{2\pi i\tau}| = e^{-2\pi y} < 1$, pois $y > 0$. Logo, pela Proposição 1 e pela definição de $\eta(\tau)$, vem que

$$\begin{aligned}
[\eta(\tau)]^{-1} &= \left[e^{\pi i\tau/12}\prod_{m=1}^{\infty}\left(1-\left(e^{2\pi i\tau}\right)^m\right)\right]^{-1} \\
&= e^{-\pi i\tau/12}\prod_{m=1}^{\infty}\left(1-\left(e^{2\pi i\tau}\right)^m\right)^{-1} \\
&= e^{-\pi i\tau/12}\sum_{m=0}^{\infty} p(m)\left(e^{2\pi i\tau}\right)^m \\
&= \sum_{m=0}^{\infty} p(m)e^{2\pi i(m-1/24)\tau} = \sum_{m=-1}^{\infty} p(m+1)e^{2\pi i(m+23/24)\tau},
\end{aligned}$$

como queríamos demonstrar. □

Finalizamos esta seção observando que $\eta(\tau)$, pela Proposição 1 e pela demonstração do corolário precedente, é regular em $\mathscr{H}$.

4.2 Várias identidades famosas

Nesta seção, apresentaremos algumas famosas identidades, dentre as quais a de Jacobi (produto triplo) e a de Euler. A primeira delas possui várias demonstrações, dentre as quais selecionamos uma devida a Andrews (*apud* [11], consulte a referência [2]). Para demonstrá-la, contudo, precisaremos do

Lema 3 (Euler). *1. Para $|x| < 1$ e qualquer número complexo z,*

$$\prod_{n=0}^{\infty}(1+x^n z) = \sum_{m=0}^{\infty} \frac{x^{m(m-1)/2} z^m}{(1-x)(1-x^2)\cdots(1-x^m)}.$$

2. Para $|x| < 1$ e $|z| < 1$,

$$\prod_{n=0}^{\infty}(1+x^n z)^{-1} = \sum_{m=0}^{\infty} \frac{(-1)^m z^m}{(1-x)(1-x^2)\cdots(1-x^m)}.$$

Demonstração. 1. Definamos $f(x,z) = \prod_{n=0}^{\infty}(1+x^n z)$. Notemos que $\sum_{n=0}^{\infty}|x^n z| = |z|\sum_{n=0}^{\infty}|x|^n$, para z complexo e $|x| < 1$, converge. Logo, $\prod_{n=0}^{\infty}(1+x^n z)$ converge absolutamente e, portanto, converge. Deste modo, podemos considerar, para x fixo e z arbitrário, $f(x,z) = \sum_{m=0}^{\infty} a_m(x) z^m$, onde $a_m(x)$, para cada m, é um polinômio na variável x ($|x| < 1$). Segue da definição de $f(x,z)$ que

$$\begin{aligned} f(x,z) &= \prod_{n=0}^{\infty}(1+x^n z) \\ &= (1+z)\prod_{n=1}^{\infty}(1+x^n z) \\ &= (1+z)\prod_{n=0}^{\infty}(1+x^n(zx)) = (1+z)f(x,zx), \end{aligned}$$

donde

$$\begin{aligned} \sum_{m=0}^{\infty} a_m(x) z^m &= (1+z)\sum_{m=0}^{\infty} a_m(x)(zx)^m \\ &= \sum_{m=0}^{\infty} a_m(x) x^m z^m + \sum_{m=0}^{\infty} a_m(x) x^m z^{m+1} \\ &= \sum_{m=0}^{\infty} a_m(x) x^m z^m + \sum_{m=1}^{\infty} a_{m-1}(x) x^{m-1} z^m. \end{aligned}$$

Portanto, para $m \geq 1$, igualando-se os coeficientes de z^m de ambos os membros da igualdade acima, vem que $a_m(x) = a_m(x)x^m + a_{m-1}(x)x^{m-1}$, ou

$$a_m(x) = \frac{a_{m-1}(x)x^{m-1}}{1-x^m}. \tag{4.3}$$

Além disso, pela expressão inicial de $f(x,z)$, é claro que $a_0(x)=1$, donde, iterando-se repetidamente a relação (4.3), vem que

$$\begin{aligned} a_m(x) &= \frac{x^{m-1}}{1-x^m}\cdot a_{m-1}(x) \\ &= \frac{x^{m-1}}{1-x^m}\cdot\frac{x^{m-2}}{1-x^{m-1}}\cdot a_{m-2}(x) \\ &= \cdots \\ &= \frac{x^{m-1}}{1-x^m}\cdot\frac{x^{m-2}}{1-x^{m-1}}\cdots\frac{x^0}{1-x}\cdot a_0(x) \\ &= \frac{x^{m(m-1)/2}}{(1-x)(1-x^2)\cdots(1-x^m)}, \end{aligned}$$

donde segue o resultado desejado. Rigorosamente, é claro, a expressão obtida para $a_m(x)$ deve ser provada por indução sobre m, mas o método iterativo que aplicamos pode ser considerado uma simplificação do raciocínio indutivo, que seria menos ilustrativo.

2. Neste caso, consideremos $g(x,z)=\prod_{n=0}^{\infty}(1+x^nz)^{-1}$. Analogamente ao item anterior, $\prod_{n=0}^{\infty}(1+x^nz)$ converge, se $|x|,|z|<1$, para uma função analítica sem zeros, uma vez que, para cada n, $1+x^nz\neq 0$ (nisto se justifica a importância da restrição $|z|<1$). Logo, o mesmo ocorre com $g(x,z)$. Desta maneira, também aqui podemos considerar, para x fixo e z arbitrário, $g(x,z)=\sum_{m=0}^{\infty}b_m(x)z^m$, sendo $b_m(x)$ um polinômio na variável x, com $b_0(x)=1$. Como procedemos no item precedente, podemos concluir que $g(x,zx)=(1+z)g(x,z)$ e, portanto, que $\sum_{m=0}^{\infty}b_m(x)x^mz^m=\sum_{m=0}^{\infty}b_m(x)z^m+\sum_{m=1}^{\infty}b_{m-1}(x)z^m$, donde

$$b_m(x)=\frac{-b_{m-1}(x)}{(1-x^m)}, \tag{4.4}$$

para $m\geq 1$. Logo, iterando-se repetidamente (4.4), segue que

$$\begin{aligned} b_m(x)=\frac{-1}{1-x^m}\cdot b_{m-1}(x) & \\ &= \frac{-1}{1-x^m}\cdot\frac{-1}{1-x^{m-1}}\cdot b_{m-2}(x) \\ &= \cdots \\ &= \frac{-1}{1-x^m}\cdot\frac{-1}{1-x^{m-1}}\cdots\frac{-1}{1-x}\cdot b_0(x) \\ &= \frac{(-1)^m}{(1-x)(1-x^2)\cdots(1-x^m)}, \end{aligned}$$

concluindo a prova da identidade.

□

Agora, sim, estamos em condições de enunciar e demonstrar o

Teorema 4 (Produto Triplo de Jacobi). *Suponha que x e z sejam números complexos tais que $|x| < 1$ e $z \neq 0$. Então*

$$\prod_{n=0}^{\infty} \left(1 - x^{2n+2}\right)\left(1 + x^{2n+1}z\right)\left(1 + x^{2n+1}z^{-1}\right) = \sum_{m=-\infty}^{\infty} x^{m^2}z^m.$$

Demonstração. Como $|x| < 1$ e $z \neq 0$, a identidade 1. do Lema 3, para x^2 e xz nos lugares de x e z, respectivamente, implica que

$$\begin{aligned}
\prod_{n=0}^{\infty}\left(1 + x^{2n+1}z\right) &= \prod_{n=0}^{\infty}\left(1 + \left(x^2\right)^n (xz)\right) \\
&= \sum_{m=0}^{\infty} \frac{x^{m(m-1)}(xz)^m}{(1-x^2)(1-x^4)\cdots(1-x^{2m})} \\
&= \sum_{m=0}^{\infty} \frac{x^{m^2}z^m}{(1-x^2)(1-x^4)\cdots(1-x^{2m})} \\
&= \sum_{m=0}^{\infty} x^{m^2}z^m \left\{\frac{\prod_{j=0}^{\infty}(1-x^{2j+2+2m})}{\prod_{j=0}^{\infty}(1-x^{2j+2})}\right\} \\
&= \prod_{j=0}^{\infty}\left(1-x^{2j+2}\right)^{-1} \sum_{m=0}^{\infty} x^{m^2}z^m \prod_{j=0}^{\infty}\left(1-x^{2j+2+2m}\right). \qquad (4.5)
\end{aligned}$$

Note agora que, se $m < 0$, então, tomando-se $j = -m-1 \geq 0$, segue que $2j+2+2m = 0$, donde $1 - x^{2j+2+2m} = 0$. Deste modo, para $m < 0$, $\prod_{j=0}^{\infty}(1-x^{2j+2+2m}) = 0$, de maneira que podemos reescrever a expressão (4.5) como

$$\prod_{j=0}^{\infty}\left(1-x^{2j+2}\right)^{-1} \sum_{m=-\infty}^{\infty} x^{m^2}z^m \prod_{j=0}^{\infty}\left(1-x^{2j+2+2m}\right).$$

Aplicando-se novamente a identidade 1. do Lema 3, para x^2 e $-x^{2+2m}$ nos lugares de x e

z, respectivamente, temos também

$$\begin{aligned}\prod_{j=0}^{\infty}\left(1-x^{2j+2+2m}\right) &= \prod_{j=0}^{\infty}\left(1+\left(x^2\right)^j\left(-x^{2+2m}\right)\right)\\ &= \sum_{k=0}^{\infty}\frac{x^{k(k-1)}\left(-x^{2+2m}\right)^k}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}\\ &= \sum_{k=0}^{\infty}\frac{(-1)^k x^{k^2+k+2mk}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})} \qquad (4.6)\end{aligned}$$

Substituindo-se, pois, (4.6) em (4.5), vem que

$$\begin{aligned}\prod_{n=0}^{\infty}\left(1+x^{2n+1}z\right) &= \prod_{j=0}^{\infty}\left(1-x^{2j+2}\right)^{-1}\sum_{m=-\infty}^{\infty}x^{m^2}z^m\sum_{k=0}^{\infty}\frac{(-1)^k x^{k^2+k+2mk}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}\\ &= \prod_{j=0}^{\infty}\left(1-x^{2j+2}\right)^{-1}\sum_{m=-\infty}^{\infty}\sum_{k=0}^{\infty}\frac{(-1)^k z^m x^{k^2+m^2+k+2mk}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}. \qquad (4.7)\end{aligned}$$

Pelo raciocínio empregado até aqui e pelo Lema 3, a identidade expressa em (4.7) é válida para $|x|<1$ e z arbitrário. Portanto, nesse caso, o somatório duplo de seu membro direito é convergente. Todavia, para que possamos trocar a ordem de tais somatórios, mantendo-se os mesmos intervalos dos índices, devemos encontrar a condição necessária para que a série por eles definida convirja absolutamente. Agora, notemos que, se $|x|<|z|<1$, então

$$\begin{aligned}\left|\frac{(-1)^k z^m x^{k^2+m^2+k+2mk}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}\right| &= \frac{|z|^m|x|^{k^2+m^2+k+2mk}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}\\ &< |z|^{m+k^2+m^2+k+2mk}<1,\end{aligned}$$

de tal maneira que, nesse caso, o somatório duplo acima é absolutamente convergente. Assim, para $|x|<|z|<1$, podemos trocar a ordem de seus membros:

$$\begin{aligned}&\sum_{m=-\infty}^{\infty}\sum_{k=0}^{\infty}\frac{(-1)^k z^m x^{k^2+m^2+k+2mk}}{(1-x^2)(1-x^4)\cdots(1-x^{2k})} =\\ &\quad=\sum_{k=0}^{\infty}\frac{(-1)^k x^k}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}\sum_{m=-\infty}^{\infty}x^{(m+k)^2}z^m\\ &\quad=\sum_{k=0}^{\infty}\frac{(-1)^k\left(xz^{-1}\right)^k}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}\sum_{m=-\infty}^{\infty}x^{(m+k)^2}z^{m+k}\\ &\quad=\sum_{k=0}^{\infty}\frac{(-1)^k(xz^{-1})^k}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}\sum_{m=-\infty}^{\infty}x^{m^2}z^m.\end{aligned}$$

Aplicando-se este resultado a (4.7), vem

$$\begin{aligned}\prod_{n=0}^{\infty}\left(1+x^{2n+1}z\right) &= \prod_{j=0}^{\infty}\left(1-x^{2j+2}\right)^{-1}\sum_{k=0}^{\infty}\frac{(-1)^k(xz^{-1})^k}{(1-x^2)(1-x^4)\cdots(1-x^{2k})}\sum_{m=-\infty}^{\infty}x^{m^2}z^m \\ &= \sum_{m=-\infty}^{\infty}x^{m^2}z^m\prod_{j=0}^{\infty}\left(1-x^{2j+2}\right)^{-1}\sum_{k=0}^{\infty}\frac{(-1)^k\left(xz^{-1}\right)^k}{(1-x^2)(1-x^4)\cdots(1-x^{2k})} \\ &= \sum_{m=-\infty}^{\infty}x^{m^2}z^m\prod_{j=0}^{\infty}\left(1-x^{2j+2}\right)^{-1}\prod_{n=0}^{\infty}\left(1+\left(x^2\right)^n\left(xz^{-1}\right)\right)^{-1} \\ &= \sum_{m=-\infty}^{\infty}x^{m^2}z^m\prod_{j=0}^{\infty}\left(1-x^{2j+2}\right)^{-1}\prod_{n=0}^{\infty}\left(1+x^{2n+1}z^{-1}\right)^{-1}, \qquad (4.8)\end{aligned}$$

utilizando-se, na penúltima passagem, a identidade 2. do Lema 3, para x^2 e xz^{-1} nos lugares de x e z, respectivamente (note que, como $|x|<|z|$, segue que $|xz^{-1}|<1$). Assim, resulta de (4.8) que

$$\prod_{n=0}^{\infty}\left(1-x^{2n+2}\right)\left(1+x^{2n+1}z\right)\left(1+x^{2n+1}z^{-1}\right)=\sum_{m=-\infty}^{\infty}x^{m^2}z^m.$$

Ambos os membros da identidade acima são funções analíticas para $|x|<1$ e $z\neq 0$. Ademais, sabemos que a identidade vale na região $|x|<|z|<1$, donde podemos encontrar uma seqüência infinita de pontos nela convergentes, e tais que vale a igualdade de ambos os membros acima. Logo, pelo Teorema 1 do Capítulo 1, segue que a identidade vale para $|x|<1$ e $z\neq 0$, como queríamos demonstrar. □

A seguir, apresentamos dois corolários do Teorema 4, um devido a Euler, outro a Jacobi. O primeiro possui uma demonstração bastante simples, enquanto o segundo apresenta alguns detalhes relativamente elaborados.

Corolário 5 (Identidade de Euler). *Para $|x|<1$, tem-se que*

$$\prod_{n=1}^{\infty}(1-x^n)=\sum_{m=-\infty}^{\infty}(-1)^m x^{m(3m+1)/2}.$$

Demonstração. Basta que se substitua, no Teorema 4, x por $x^{3/2}$ e z por $-x^{1/2}$, desde que $|x^{3/2}|<1$ e $-x^{1/2}\neq 0$, ou seja, $0<|x|<1$,

$$\prod_{n=0}^{\infty}\left(1-\left(x^{3/2}\right)^{2n+2}\right)\left(1+\left(x^{3/2}\right)^{2n+1}\left(-x^{1/2}\right)\right)\left(1+\left(x^{3/2}\right)^{2n+1}\left(-x^{1/2}\right)^{-1}\right)=$$

$$\sum_{m=-\infty}^{\infty}\left(x^{3/2}\right)^{m^2}\left(-x^{1/2}\right)^m,$$

donde

$$\prod_{n=0}^{\infty}\left(1-x^{3n+3}\right)\left(1-x^{3n+2}\right)\left(1-x^{3n+1}\right)=\sum_{m=-\infty}^{\infty}(-1)^m x^{m(3m+1)/2},$$

ou

$$\prod_{n=1}^{\infty}(1-x^n)=\sum_{m=-\infty}^{\infty}(-1)^m x^{m(3m+1)/2},$$

para $0<|x|<1$. Além disso, para $x=0$, seu membro esquerdo resulta 1, enquanto seu membro direito pode ser expresso por

$$\sum_{m=-\infty}^{\infty}(-1)^m x^{m(3m+1)/2}=\cdots+x^{-5}-x+1-x^2+x^7-\cdots,$$

donde $x=0$ também implica que o seu membro direito é igual a 1. Logo, a identidade é válida para $|x|<1$, como queríamos demonstrar. □

Corolário 6 (Identidade de Jacobi). *Para $|x|<1$, temos que*

$$\prod_{n=1}^{\infty}(1-x^n)^3=\sum_{m=0}^{\infty}(2m+1)x^{m(m+1)/2}.$$

Demonstração. Lembrando-se do método empregado na demonstração do corolário anterior, poderíamos substituir, no Teorema 4, x por $x^{1/2}$ e z por $-x^{1/2}$, para $0<|x|<1$, donde

$$\prod_{n=0}^{\infty}\left(1-\left(x^{1/2}\right)^{2n+2}\right)\left(1+\left(x^{1/2}\right)^{2n+1}\left(-x^{1/2}\right)\right)\left(1+\left(x^{1/2}\right)^{2n+1}\left(-x^{1/2}\right)^{-1}\right)=$$
$$\sum_{m=-\infty}^{\infty}\left(x^{1/2}\right)^{m^2}\left(-x^{1/2}\right)^{m}.$$

Mas isso conduziria a

$$\prod_{n=0}^{\infty}\left(1-x^{n+1}\right)\left(1-x^{n+1}\right)\left(1-x^{n}\right)=\sum_{m=-\infty}^{\infty}(-1)^m x^{m(m+1)/2}.$$

Ocorre que, para $n=0$, $1-x^n=0$, donde o primeiro membro da igualdade acima se reduziria a zero. Por outro lado, no membro direito, cada inteiro m contribui, para a soma, com $(-1)^m x^{m(m+1)/2}$, enquanto que $-m-1$ contribui com $(-1)^{-m-1}x^{(-m-1)(-m-1+1)/2}=-(-1)^m x^{m(m+1)/2}$, de modo que os termos do somatório anulam-se entre si. Deste modo, a aplicação direta do Teorema 4, neste caso, reduz ambos os membros daquela identidade a zero.

A idéia desta demonstração, então, é empregar um método mais sutil. No Teorema 4, substituindo-se x por $x^{1/2}$ e z por $x^{1/2}(-1+\varepsilon)$, com $0<\varepsilon<1$, tomaremos, ao final, $\varepsilon \to 0^+$, de modo que o efeito produzido será parecido com o de se realizar a substituição proposta inicialmente. Neste caso, contanto que $|x|<1$, teremos

$$\prod_{n=0}^{\infty}\left(1-\left(x^{1/2}\right)^{2n+2}\right)\left(1+\left(x^{1/2}\right)^{2n+1}\left(x^{1/2}(-1+\varepsilon)\right)\right)\left(1+\left(x^{1/2}\right)^{2n+1}\left(x^{1/2}(-1+\varepsilon)\right)^{-1}\right) = \sum_{m=-\infty}^{\infty}\left(x^{1/2}\right)^{m^2}\left(x^{1/2}(-1+\varepsilon)\right)^{m}.$$

Agora, o membro esquerdo da igualdade acima se reduz a

$$\begin{aligned}
&\prod_{n=0}^{\infty}\left(1-x^{n+1}\right)\left(1+x^{n+1}(-1+\varepsilon)\right)\left(1+x^{n}(-1+\varepsilon)^{-1}\right) = \\
&\quad = \prod_{n=1}^{\infty}\left(1-x^{n}\right)\left(1+x^{n}(-1+\varepsilon)\right)\left(1+x^{n-1}(-1+\varepsilon)^{-1}\right) \\
&\quad = \left(1+(-1+\varepsilon)^{-1}\right)\prod_{n=1}^{\infty}\left(1-x^{n}\right)\left(1+x^{n}(-1+\varepsilon)\right)\left(1+x^{n}(-1+\varepsilon)^{-1}\right) \\
&\quad = \frac{\varepsilon}{-1+\varepsilon}\prod_{n=1}^{\infty}\left(1-x^{n}\right)\left(1+x^{n}(-1+\varepsilon)\right)\left(1+x^{n}(-1+\varepsilon)^{-1}\right),
\end{aligned}$$

de tal maneira que

$$\underbrace{\frac{1}{-1+\varepsilon}\prod_{n=1}^{\infty}\left(1-x^{n}\right)\left(1+x^{n}(-1+\varepsilon)\right)\left(1+x^{n}(-1+\varepsilon)^{-1}\right)}_{f(\varepsilon)} = \underbrace{\frac{1}{\varepsilon}\sum_{m=-\infty}^{\infty}x^{m(m+1)/2}(-1+\varepsilon)^{m}}_{g(\varepsilon)},$$

para x fixo tal que $|x|<1$. Observemos, então, que $f(\varepsilon)$ é contínua para $\varepsilon \neq 1$. Em particular, $f(\varepsilon)$ é contínua em $\varepsilon = 0$, donde

$$\lim_{\epsilon\to 0^+} g(\varepsilon) = \lim_{\epsilon\to 0^+} f(\varepsilon) = f(0) = -\prod_{n=1}^{\infty}(1-x^n)^3.$$

Agora, analisemos $\lim_{\varepsilon\to 0^+} g(\varepsilon)$ independentemente de $f(\varepsilon)$. Primeiramente, consideremos

$$(-1+\varepsilon)^m = (-1)^m(1-\varepsilon)^m = (-1)^m(1-m\varepsilon-\rho), \tag{4.9}$$

onde $\rho = 1-(1-\varepsilon)^m - m\varepsilon$. Agora, consideremos $\varphi(x) = (1-x)^m$, para $0 \le x \le \varepsilon$. Pelo Teorema de Taylor, expresso na relação (1.2) do Capítulo 1, temos que

$$(1-\varepsilon)^m = \varphi(\varepsilon) = \varphi(0) + \frac{\varphi'(0)\varepsilon}{1!} + \frac{\varepsilon^2}{2!}\varphi''(\theta\varepsilon) = 1 - m\varepsilon + \frac{m(m-1)}{2}(\underbrace{1-\theta\varepsilon}_{\alpha})^{m-2}\varepsilon^2,$$

sendo $0 \leq \theta \leq 1$ e, portanto, $1 - \varepsilon \leq \alpha \leq 1$. Assim, para cada inteiro m, tem-se que

$$|\rho| = \frac{|m(m-1)|}{2}\alpha^{m-2}\varepsilon^2 < \frac{1}{2}\left(|m|+1\right)^2\varepsilon^2.$$

Portanto, utilizando-se (4.9), vem que

$$\begin{aligned} g(\varepsilon) &= \frac{1}{\varepsilon}\sum_{m=-\infty}^{\infty} x^{m(m+1)/2}(-1)^m(1-m\varepsilon-\rho) \\ &= \frac{1}{\varepsilon}\sum_{m=-\infty}^{\infty}(-1)^m x^{m(m+1)/2} + \sum_{m=-\infty}^{\infty}(-1)^{m+1}mx^{m(m+1)/2} + R, \end{aligned}$$

onde $R = \frac{1}{\varepsilon}\sum_{m=-\infty}^{\infty}(-1)^{m+1}\rho x^{m(m+1)/2}$. Logo,

$$\begin{aligned} |R| &= \left|\frac{1}{\varepsilon}\sum_{m=-\infty}^{\infty}(-1)^{m+1}\rho x^{m(m+1)/2}\right| \\ &\leq \frac{1}{\varepsilon}\sum_{m=-\infty}^{\infty}|\rho||x|^{m(m+1)/2} \\ &< \frac{\varepsilon}{2}\sum_{m=-\infty}^{\infty}(|m|+1)^2|x|^{m(m+1)/2} = K\varepsilon, \end{aligned}$$

sendo K independente de ε e, portanto, $\lim_{\varepsilon\to 0^+} R = 0$. Além disso, já argumentamos, no início desta demonstração, que $\sum_{m=-\infty}^{\infty}(-1)^m x^{m(m+1)/2} = 0$, donde

$$\lim_{\varepsilon\to 0^+} g(\varepsilon) = \sum_{m=-\infty}^{\infty}(-1)^{m+1}mx^{m(m+1)/2}.$$

Finalmente, cada $m \geq 0$ contribui com $(-1)^{m+1}mx^{m(m+1)/2}$ no somatório acima, enquanto a contribuição de $-m-1$ é igual a

$$(-1)^{-m-1+1}(-m-1)x^{(-m-1)(-m-1+1)/2} = (-1)^{m+1}(m+1)x^{m(m+1)/2},$$

de tal maneira que o coeficiente de $x^{m(m+1)/2}$ é $(-1)^{m+1}(2m+1)$, e podemos escrever

$$\lim_{\varepsilon\to 0^+} g(\varepsilon) = -\sum_{m=0}^{\infty}(-1)^m(2m+1)x^{m(m+1)/2},$$

o que termina a prova. □

4.3 Fórmulas de transformação para $\eta(\tau)$

Nesta seção, provaremos que $\eta(\tau)$ é uma forma cúspide de grau $-1/2$ com respeito a $\Gamma(1)$. Essa prova, como dissemos no início deste capítulo, não é simples, e ainda temos um resultado que provar antes de exibirmo-la.

Teorema 7. *Para $\tau \in \mathscr{H}$, temos*

$$\eta\left(-\frac{1}{\tau}\right) = (-i)^{1/2}\tau^{1/2}\eta(\tau),$$

onde as raízes são calculadas de acordo com a convenção expressa na relação (3.2) do Capítulo 3, qual seja, $-\pi \leq \arg(z) < \pi$, para $z \in \mathbb{C}$.

Demonstração. Por definição,

$$\eta(\tau) = e^{\pi i\tau/12}\prod_{m=1}^{\infty}\left(1 - e^{2\pi im\tau}\right), \qquad \tau \in \mathscr{H}.$$

Se $\tau = x + iy \in \mathscr{H}$, então $|e^{2\pi i\tau}| = e^{-2\pi y} < e^0 = 1$, donde podemos aplicar o Corolário 5 para $x = e^{2\pi i\tau}$, obtendo

$$\eta(\tau) = e^{\pi i\tau/12}\sum_{n=-\infty}^{\infty}(-1)^n\left(e^{2\pi i\tau}\right)^{n(3n+1)/2} = e^{\pi i\tau/12}\sum_{n=-\infty}^{\infty}(-1)^n e^{\pi i\tau n(3n+1)}.$$

Agora, observe que $e^{\pi i\tau n(3n+1)} = e^{3\pi i\tau n^2}e^{\pi i\tau n}$ e, como n percorre todos os valores inteiros (positivos e negativos), segue que, no somatório acima, podemos considerar $3n-1$ no lugar de $3n+1$, ou seja,

$$\eta(\tau) = e^{\pi i\tau/12}\sum_{n=-\infty}^{\infty}(-1)^n e^{\pi i\tau n(3n-1)},$$

de modo que, a cada n no somatório original, corresponde $-n$ neste último somatório, e

vice-versa. Desenvolvendo-se tal expressão, temos

$$\begin{aligned}
\eta(\tau) &= e^{\pi i\tau/12}\sum_{n=-\infty}^{\infty}\left(e^{\pi i}\right)^n e^{3\pi i\tau n^2-\pi i\tau n} \\
&= e^{\pi i\tau/12}\sum_{n=-\infty}^{\infty} e^{3\pi i\tau n^2-\pi i\tau n(1-1/\tau)} \\
&= e^{\pi i\tau/12}\sum_{n=-\infty}^{\infty} e^{3\pi i\tau[n^2-(n/3)(1-1/\tau)]} \\
&= e^{\pi i\tau/12}\sum_{n=-\infty}^{\infty} e^{3\pi i\tau[n^2-(n/3)(1-1/\tau)+(1/6)^2(1-1/\tau)^2-(1/6)^2(1-1/\tau)^2]} \\
&= e^{\pi i\tau/12}\sum_{n=-\infty}^{\infty} e^{3\pi i\tau[n-(1/6)(1-1/\tau)]^2} e^{-(\pi i\tau/12)(1-1/\tau)^2} \\
&= e^{\pi i\tau/12}e^{-(\pi i\tau/12)(1-1/\tau)^2}\sum_{n=-\infty}^{\infty} e^{3\pi i\tau[n-(1/6)(1-1/\tau)]^2} \\
&= e^{(\pi i\tau/12)(2/\tau-1/\tau^2)}\sum_{n=-\infty}^{\infty} e^{3\pi i\tau[n-(1/6)(1-1/\tau)]^2} \\
&= e^{-\pi i/12\tau}e^{\pi i/6}\sum_{n=-\infty}^{\infty} e^{3\pi i\tau[n-(1/6)(1-1/\tau)]^2}.
\end{aligned}$$

Agora, vamos aplicar o Teorema 9 do Capítulo 1, para $t=-3i\tau$ e $z=-(1/6)(1-1/\tau)$ (note que $\mathfrak{Re}(t)=3y>0$), donde

$$\begin{aligned}
\eta(\tau) &= e^{-\pi i/12\tau}e^{\pi i/6}\frac{1}{\sqrt{-3i\tau}}\sum_{n=-\infty}^{\infty} e^{-\pi n^2/(-3i\tau)+2\pi in[-(1/6)(1-1/\tau)]} \\
&= e^{-\pi i/12\tau}e^{\pi i/6}\frac{1}{\sqrt{-3i\tau}}\sum_{n=-\infty}^{\infty} e^{-\pi in^2/3\tau-\pi in(1-1/\tau)/3} \qquad (4.10)
\end{aligned}$$

Denotando-se

$$g_k(\tau)=\sum_{\mu=-\infty}^{\infty} e^{-\pi i(3\mu+k)^2/3\tau-\pi i(3\mu+k)(1-1/\tau)/3},$$

para $k=0,1,2$, segue, em (4.10), que

$$\sum_{n=-\infty}^{\infty} e^{-\pi in^2/3\tau-\pi in(1-1/\tau)/3}=g_0(\tau)+g_1(\tau)+g_2(\tau).$$

Assim, temos

$$\begin{aligned} g_0(\tau) &= \sum_{\mu=-\infty}^{\infty} e^{-\pi i(3\mu)^2/3\tau - \pi i(3\mu)(1-1/\tau)/3} \\ &= \sum_{\mu=-\infty}^{\infty} e^{-\pi i(3\mu^2)/\tau - \pi i\mu + \pi i\mu/\tau} \\ &= \sum_{\mu=-\infty}^{\infty} \left(e^{-\pi i}\right)^{\mu} e^{(-\pi i/\tau)(3\mu^2-\mu)} \\ &= \sum_{\mu=-\infty}^{\infty} (-1)^{\mu} e^{-(\pi i/\tau)(3\mu^2-\mu)}; \end{aligned}$$

$$\begin{aligned} g_1(\tau) &= \sum_{\mu=-\infty}^{\infty} e^{-\pi i(3\mu+1)^2/3\tau - \pi i(3\mu+1)(1-1/\tau)/3} \\ &= \sum_{\mu=-\infty}^{\infty} e^{-3\pi i\mu^2/\tau - 2\pi i\mu/\tau - \pi i/3\tau - \pi i\mu + \pi i\mu/\tau - \pi i/3 + \pi i/3\tau} \\ &= e^{-\pi i/3} \sum_{\mu=-\infty}^{\infty} \left(e^{-\pi i}\right)^{\mu} \left(e^{-2\pi i\mu}\right)^{1/\tau} e^{(-\pi i/\tau)(3\mu^2+\mu)} \\ &= e^{-\pi i/3} \sum_{\mu=-\infty}^{\infty} (-1)^{\mu} e^{-(\pi i/\tau)(3\mu^2-\mu)} = e^{-\pi i/3} g_0(\tau); \end{aligned}$$

$$\begin{aligned} g_2(\tau) &= \sum_{\mu=-\infty}^{\infty} e^{-\pi i(3\mu+2)^2/3\tau - \pi i(3\mu+2)(1-1/\tau)/3} \\ &= \sum_{\mu=-\infty}^{\infty} e^{-3\pi i\mu^2/\tau - 4\pi i\mu/\tau - 4\pi i/3\tau - \pi i\mu + \pi i\mu/\tau - 2\pi i/3 + 2\pi i/3\tau} \\ &= e^{-2\pi i/3} \sum_{\mu=-\infty}^{\infty} \left(e^{-\pi i}\right)^{\mu} \left(e^{-2\pi i}\right)^{1/3\tau} e^{-3\pi i\mu^2/\tau - 3\pi i\mu/\tau} \\ &= e^{-2\pi i/3} \sum_{\mu=-\infty}^{\infty} (-1)^{\mu} e^{-(3\pi i/\tau)\mu(\mu+1)}. \end{aligned}$$

Nesta última expressão, se $\mu \geq 0$, então há uma contribuição, para o somatório, de $(-1)^{\mu} e^{-(3\pi i/\tau)\mu(\mu+1)}$. Por outro lado, $-\mu - 1 < 0$ contribui com

$$(-1)^{-\mu-1} e^{-(3\pi i/\tau)(-\mu-1)(-\mu-1+1)} = -(-1)^{\mu} e^{-(3\pi i/\tau)\mu(\mu+1)},$$

donde o somatório em questão se anula. Logo, $g_2(\tau) = 0$ e, portanto, subtitindo-se os valores encontrados em (4.10), vem que

$$\begin{aligned}
\eta(\tau) &= e^{-\pi i/12\tau} e^{\pi i/6} \frac{1}{\sqrt{-3i\tau}} \left(g_0(\tau) + e^{-\pi i/3} g_0(\tau)\right) \\
&= e^{-\pi i/12\tau} \frac{g_0(\tau)}{\sqrt{3}\sqrt{-i\tau}} (\underbrace{e^{\pi i/6} + e^{-\pi i/6}}_{\sqrt{3}}) \\
&= e^{-\pi i/12\tau} \frac{1}{\sqrt{-i\tau}} \sum_{\mu=-\infty}^{\infty} (-1)^{\mu} e^{-(\pi i/\tau)(3\mu^2-\mu)} \\
&= \frac{1}{\sqrt{-i\tau}} e^{\pi i(-1/\tau)/12} \sum_{\mu=-\infty}^{\infty} (-1)^{\mu} \left(e^{2\pi i(-1/\tau)}\right)^{\mu(3\mu+1)/2},
\end{aligned}$$

utilizando-se, na última passagem, argumento similar ao do início da demonstração. Agora, como $\left|e^{2\pi i(-1/\tau)}\right| = e^{-2\pi y/(x^2+y^2)} < e^0 = 1$, podemos aplicar, novamente, o Corolário 5 para $x = e^{2\pi i(-1/\tau)}$, obtendo

$$\eta(\tau) = \frac{1}{\sqrt{-i\tau}} e^{\pi i(-1/\tau)/12} \prod_{n=1}^{\infty} \left(1 - \left(e^{2\pi i(-1/\tau)}\right)^n\right) = \frac{1}{\sqrt{-i\tau}} \eta(-1/\tau),$$

donde segue que

$$\eta\left(-\frac{1}{\tau}\right) = \sqrt{-i\tau}\,\eta(\tau).$$

Resta-nos provar que $(-i\tau)^{1/2} = (-i)^{1/2}\tau^{1/2}$. É claro que, em módulo, esta igualdade é válida. Ademais, $\arg(-i) = -\pi/2$ e, como $\tau \in \mathscr{H}$, $0 < \arg(\tau) < \pi$ e $-\pi/2 < \arg(-i\tau) < \pi/2$. Logo, observando que

$$\arg(-i\tau) = \arg(-i) + \arg(\tau) + 2n\pi,$$

para n inteiro, segue que

$$2|n|\pi = |\arg(-i\tau) - \arg(-i) - \arg(\tau)| < 2\pi,$$

donde $n = 0$ e, portanto,

$$(1/2)\arg(-i\tau) = (1/2)\arg(-i) + (1/2)\arg(\tau),$$

ou

$$\arg(-i\tau)^{1/2} = \arg(-i)^{1/2}\tau^{1/2},$$

concluindo a prova. □

Finalmente, o principal teorema:

Teorema 8. *$\eta(\tau)$ é uma forma modular de grau $-1/2$ em $\Gamma(1)$. Particularmente, $\eta(\tau)$ é uma forma cúspide de grau $-1/2$ em $\Gamma(1)$. Além disso, denotando-se υ_η o sistema multiplicador dessa forma, temos que $\upsilon_\eta(S) = e^{\pi i/12}$ e $\upsilon_\eta(T) = (-i)^{1/2} = e^{-\pi i/4}$.*

Demonstração. Já sabemos que $\eta(\tau)$ é regular em $\mathscr{H}$ (e portanto meromorfa em $\mathscr{H}$). Considerando-se $\mathscr{R} = \mathscr{R}(\Gamma(1))$ na Definição 6 do Capítulo 3, temos que provar:

1.

$$\eta(M\tau) = \upsilon_\eta(M)(c\tau + d)^{1/2}\eta(\tau), \tag{4.11}$$

para todo $M = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma(1)$, *onde* $|\upsilon_\eta(M)| = 1$;

No Teorema 7, provamos que $\eta(T\tau) = \eta(-1/\tau) = (-i)^{1/2}\tau^{1/2}\eta(\tau)$, donde (4.11) é válida para $M = T$, com $\upsilon_\eta(T) = (-i)^{1/2} = e^{-\pi i/4}$. Ademais

$$\begin{aligned} \eta(S\tau) &= \eta(\tau+1) \\ &= e^{\pi i(\tau+1)/12}\prod_{m=1}^{\infty}\left(1 - e^{2\pi i m(\tau+1)}\right) \\ &= e^{\pi i/12}e^{\pi i\tau/12}\prod_{m=1}^{\infty}\left(1 - e^{2\pi i m\tau}\right) = e^{\pi i/12}\eta(\tau), \end{aligned}$$

donde (4.11) também é válida para $M = S$, sendo $\upsilon_\eta(S) = e^{\pi i/12}$.

Agora, notemos que cada elemento $M \in \Gamma(1)$, visto como matriz, pode ser escrito na forma

$$M = T^{\varepsilon_1}S^{\alpha_1}TS^{\alpha_2}T\cdots TS^{\alpha_{n-1}}TS^{\alpha_n}T^{\varepsilon_2},$$

onde $\varepsilon_1 = 0, 1, 2, 3$, $\varepsilon_2 = 0, 1$ e α_i é inteiro. Isto é verdade, essencialmente, pelo Corolário 4 do Capítulo 2, que afirma que $\Gamma(1)$ é gerado por S e T. Ademais, sabemos que $T^2 = -I$ e $T^3 = -T$ (como matrizes), de modo que permitimos ε_1 variar de 0 a 3 a fim de incluir os casos $M = -I$ e $M = -T$. Definamos, pois, o *comprimento* de M pela soma $\varepsilon_1+\varepsilon_2+|\alpha_1|+\cdots+|\alpha_n|+n-1$, ou seja, pela soma dos módulos dos expoentes que aparecem nas matrizes S e T da decomposição de M. Agora, observe que $T^2 = (ST)^3 = -I$, embora os comprimentos de T^2 e de $(ST)^3$ sejam, respectivamente, 2 e 6. Assim, dada uma matriz $M \in \Gamma(1)$, sua decomposição

em termos S e T e seu comprimento não são únicos. Esse fato, todavia, não será empecilho à nossa demonstração, que se dará por indução sobre o comprimento de M.

Se o comprimento de M for igual a 0, então $M = I$, donde $\eta(I\tau) = \eta(\tau)$, donde (4.11) é satisfeita, com $\upsilon_\eta(I) = 1$.

Suponha agora que (4.11) seja satisfeita para cada $M \in \Gamma(1)$ tal que seu comprimento seja $k-1$, $k \geq 1$. Suponhamos, então, que $M' \in \Gamma(1)$ é expresso como uma palavra de comprimento k. Nesse caso, temos $M' = MS$, $M' = MT$ ou $M' = MS^{-1}$, sendo o comprimento de $M = \begin{pmatrix} * & * \\ c & d \end{pmatrix}$ igual a $k-1$. No primeiro caso, temos

$$\begin{aligned} \eta(M'\tau) &= \eta(M(S\tau)) \\ &= \upsilon_\eta(M)(cS\tau + d)^{1/2}\eta(S\tau) \\ &= \upsilon_\eta(M)(c\tau + c + d)^{1/2}\upsilon_\eta(S)\eta(\tau) \\ &= \upsilon_\eta(M)e^{\pi i/12}(c\tau + c + d)^{1/2}\eta(\tau). \end{aligned}$$

Como $M' = MS = \begin{pmatrix} * & * \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} * & * \\ c & c+d \end{pmatrix}$, vem que M' satisfaz a relação (4.11), com $\upsilon_\eta(M') = \upsilon_\eta(M)e^{\pi i/12}$. É importante observar que, apesar de M' possuir várias representações, o valor $\upsilon_\eta(M')$ é independente de tais representações, pelo fato de que $\upsilon_\eta(M') = \eta(M'\tau)(c\tau+c+d)^{-1/2}/\eta(\tau)$, sendo o membro direito desta igualdade univocamente determinado. De fato, o caráter funcional de um sistema multiplicador não pode ser contrariado, comentário este que também é relevante para as duas outras possibilidades de M'.

Suponhamos, agora, $M' = MT = \begin{pmatrix} * & * \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} * & * \\ d & -c \end{pmatrix}$. Nesse caso,

$$\begin{aligned} \eta(M'\tau) &= \eta(M(T\tau)) \\ &= \upsilon_\eta(M)(cT\tau + d)^{1/2}\eta(T\tau) \\ &= \upsilon_\eta(M)(-c/\tau + d)^{1/2}\upsilon_\eta(T)\tau^{1/2}\eta(\tau) \\ &= \upsilon_\eta(M)\frac{(d\tau - c)^{1/2}}{\tau^{1/2}}e^{2\pi in(1/2)}e^{-\pi i/4}\tau^{1/2}\eta(\tau) \\ &= \upsilon_\eta(M)e^{\pi in}e^{-\pi i/4}(d\tau - c)^{1/2}\eta(\tau), \end{aligned}$$

sendo n um inteiro dependente apenas de c e d (acerca disso, e também para entender a penúltima passagem acima, reveja comentário situado à página 38, acerca de potências de quocientes de números complexos). Portanto, (4.11) também vale para $M' = MT$, com $\upsilon_\eta(M') = \upsilon_\eta(M)e^{\pi i n}e^{-\pi i/4}$.

Finalmente, se $M' = MS^{-1} = \begin{pmatrix} * & * \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} * & * \\ c & d-c \end{pmatrix}$, então

$$\begin{aligned}
\eta(M'\tau) &= \eta(M(S^{-1}\tau)) \\
&= \upsilon_\eta(M)(cS^{-1}\tau + d)^{1/2}\eta(S^{-1}\tau) \\
&= \upsilon_\eta(M)(c\tau + d - c)^{1/2}e^{\pi i(\tau-1)/12}\prod_{m=1}^{\infty}\left(1 - e^{2\pi i m(\tau-1)}\right) \\
&= \upsilon_\eta(M)e^{-\pi i/12}(c\tau + d - c)^{1/2}\eta(\tau),
\end{aligned}$$

realizando cálculos similares aos do início da demonstração. Deste modo, também $M' = MS^{-1}$ satisfaz (4.11) e, por indução, o resultado segue para cada $M \in \Gamma(1)$.

2. *$\eta(\tau)$ possui uma expansão de Fourier em cada ponto parabólico de $\Gamma(1)$ em $\mathscr{R}$;*
O único ponto parabólico de $\Gamma(1)$ em $\mathscr{R}$ é ∞. Aplicando-se o Corolário 5 à definição de $\eta(\tau)$, para $x = e^{2\pi i\tau}$, temos que

$$\begin{aligned}
\eta(\tau) &= e^{\pi i\tau/12}\prod_{m=1}^{\infty}\left(1 - \left(e^{2\pi i\tau}\right)^m\right) \\
&= e^{\pi i\tau/12}\sum_{n=-\infty}^{\infty}(-1)^n\left(e^{2\pi i\tau}\right)^{n(3n+1)/2} \\
&= \sum_{n=-\infty}^{\infty}(-1)^n e^{2\pi i[n(3n+1)/2+1/24]\tau}. \qquad (4.12)
\end{aligned}$$

Como o ponto parabólico é $q = \infty$, temos, relativos a tal ponto, $\sigma(\tau) = 1$, $A = I$, $\lambda = 1$ e $\kappa = 1/24$, de modo que a expansão acima coincide, a menos de uma mudança de índices no somatório, com a de $\eta(\tau)$ em $q = \infty$, de acordo com a relação (3.7) do Capítulo 3.

3. *$\eta(\tau)$ é meromorfa em cada ponto parabólico de $\Gamma(1)$ em $\mathscr{R}$.*
Já vimos, no item anterior, que a expansão de Fourier de $\eta(\tau)$ no único ponto parabólico de $\Gamma(1)$ em $\mathscr{R}$ é dada por (4.12). Note então, que, para cada inteiro n, $n(3n+1)/2 + 1/24 > 0$, donde $\eta(\tau)$ é meromorfa em cada ponto parabólico de $\Gamma(1)$ em $\mathscr{R}$.

Pelo três itens acima, temos que $\eta(\tau)$ é uma forma modular de grau $-1/2$ com relação a $\Gamma(1)$. Mais do que isso, nossas observações anteriores nos permitem afirmar que $\eta(\tau)$ é uma forma cúspide. □

4.4 A função $\vartheta(\tau)$

Apresentaremos, nesta seção, outra forma modular muito importante para a teoria dos números, a saber, $\vartheta(\tau)$. Para nossa sorte, o fato de já sabermos que $\eta(\tau)$ é uma forma cúspide (seção anterior) poderá ser aproveitado na demonstração de que $\vartheta(\tau)$ também é forma modular, principalmente em virtude do Teorema 10, que estabelecerá uma relação entre ambas as formas modulares.

Para $\tau \in \mathscr{H}$, definimos a função em questão por:

$$\vartheta(\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau} = 1 + 2\sum_{n=1}^{\infty} e^{\pi i n^2 \tau}.$$

Se $\tau = x + iy \in \mathscr{H}$, então $\left|e^{\pi i n^2 \tau}\right| = e^{-\pi n^2 y} < e^0 = 1$, donde o último dos somatórios que aparecem na definição de $\vartheta(\tau)$ é convergente para uma função analítica em $\mathscr{H}$. Logo, $\vartheta(\tau)$ é regular em $\mathscr{H}$.

A importância de $\vartheta(\tau)$, para a teoria dos números, reside no fato de que, se s for um inteiro não negativo,

$$[\vartheta(\tau)]^s = \underbrace{\left(\sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}\right)\left(\sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}\right)\cdots\left(\sum_{n=-\infty}^{\infty} e^{\pi i n^2 \tau}\right)}_{s \text{ vezes}}.$$

Na expansão acima, é evidente que o coeficiente de $e^{\pi i m \tau}$ corresponde ao número de maneiras de se representar o inteiro não negativo m como soma de exatamente s quadrados, sendo estes não necessariamente distintos e importando sua ordem em cada soma. Assim, denotando-se tal valor por $r_s(m)$, temos

$$[\vartheta(\tau)]^s = 1 + \sum_{m=1}^{\infty} r_s(m) e^{\pi i m \tau}. \tag{4.13}$$

Como exemplo, temos $r_3(9) = 30$, pois $9 = (\pm 3)^2 + 0^2 + 0^2 = 0^2 + (\pm 3)^2 + 0^2 = 0^2 + 0^2 + (\pm 3)^2 = (\pm 1)^2 + (\pm 2)^2 + (\pm 2)^2 = (\pm 2)^2 + (\pm 1)^2 + (\pm 2)^2 = (\pm 2)^2 + (\pm 2)^2 + (\pm 1)^2$. Com

esta definição de $r_s(m)$, (4.13) segue imediatamente do fato, já comentado acima, de $\vartheta(\tau)$ convergir absolutamente.

A prova de que $\eta(\tau) \neq 0$ em $\mathscr{H}$ foi relativamente simples, não tendo havido nenhum teorema especial para ela. Em contrapartida, pelo fato da definição de $\vartheta(\tau)$ expressá-la num somatório infinito, essa nova função exigirá um resultado não trivial, a saber, o

Teorema 9. *Para $\tau \in \mathscr{H}$, tem-se que*

$$\vartheta(\tau) = \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n\tau}\right)\left(1 + e^{(2n-1)\pi i\tau}\right)^2. \tag{4.14}$$

Além disso, é conseqüência de (4.14) que $\vartheta(\tau) \neq 0$ para cada $\tau \in \mathscr{H}$.

Demonstração. Observe que, se $\tau \in \mathscr{H}$, $|e^{\pi i\tau}| < 1$. Portanto, podemos aplicar o Teorema 4 na definição de $\vartheta(\tau)$, para $x = e^{\pi i\tau}$ e $z = 1 \neq 0$, obtendo

$$\begin{aligned}
\vartheta(\tau) &= \sum_{n=-\infty}^{\infty} \left(e^{\pi i\tau}\right)^{n^2} \\
&= \prod_{n=0}^{\infty} \left(1 - \left(e^{\pi i\tau}\right)^{2n+2}\right)\left(1 + \left(e^{\pi i\tau}\right)^{2n+1}\right)\left(1 + \left(e^{\pi i\tau}\right)^{2n+1}\right) \\
&= \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n\tau}\right)\left(1 + e^{(2n-1)\pi i\tau}\right)^2,
\end{aligned}$$

que é o resultado desejado.

Agora, sabemos que $|e^{\pi i m\tau}| < 1$, donde $1 - e^{\pi i m\tau} \neq 0$, para cada $\tau \in \mathscr{H}$ e cada inteiro positivo m, de modo que (4.14) nos garante que $\vartheta(\tau) \neq 0$, para cada $\tau \in \mathscr{H}$. □

O teorema seguinte estabelece a desejada relação entre $\eta(\tau)$ e $\vartheta(\tau)$:

Teorema 10. *Se $\tau \in \mathscr{H}$, então*

$$\vartheta(\tau) = \frac{\left[\eta\left(\frac{\tau+1}{2}\right)\right]^2}{\eta(\tau+1)}.$$

Demonstração. Se $\tau \in \mathscr{H}$, então é claro que $(\tau+1)/2$ e $\tau+1$ também pertencem a $\mathscr{H}$. Logo, por definição,

$$\begin{aligned}
\left[\eta\left(\frac{\tau+1}{2}\right)\right]^2 &= \left\{e^{\pi i[(\tau+1)/2]/12} \prod_{m=1}^{\infty} \left(1 - e^{2\pi i m[(\tau+1)/2]}\right)\right\}^2 \\
&= e^{\pi i(\tau+1)/12} \prod_{m=1}^{\infty} \left(1 - e^{\pi i m(\tau+1)}\right)^2,
\end{aligned}$$

e

$$\eta(\tau+1) = e^{\pi i(\tau+1)/12} \prod_{m=1}^{\infty} \left(1 - e^{2\pi i m(\tau+1)}\right),$$

de tal maneira que

$$\begin{aligned}
\frac{\left[\eta\left(\frac{\tau+1}{2}\right)\right]^2}{\eta(\tau+1)} &= \frac{\prod_{m=1}^{\infty}\left(1-e^{\pi i m(\tau+1)}\right)^2}{\prod_{m=1}^{\infty}\left(1-e^{2\pi i m(\tau+1)}\right)} \\
&= \frac{\prod_{m=1}^{\infty}\left(1-e^{2\pi i m(\tau+1)}\right)^2\left(1-e^{(2m-1)\pi i(\tau+1)}\right)^2}{\prod_{m=1}^{\infty}\left(1-e^{2\pi i m(\tau+1)}\right)} \\
&= \prod_{m=1}^{\infty}\left(1-e^{2\pi i m\tau}\right)\left(1+e^{(2m-1)\pi i\tau}\right)^2 = \vartheta(\tau),
\end{aligned}$$

pelo Teorema 9. □

Deste modo, a partir de propriedades conhecidas para $\eta(\tau)$, podemos deduzir propriedades análogas para $\vartheta(\tau)$, dentre as quais a tese do seguinte teorema:

Teorema 11. *A função $\vartheta(\tau)$ é uma forma modular inteira de grau $-1/2$ com respeito a $\Gamma_\vartheta = \langle S^2, T\rangle \leqslant \Gamma(1)$ (este subgrupo de $\Gamma(1)$ já nos foi apresentado no Capítulo 2). Ademais, se denotarmos o sistema multiplicador dessa forma por υ_ϑ, temos que $\upsilon_\vartheta(S^2) = 1$ e $\upsilon_\vartheta(T) = (i)^{-1/2} = e^{-\pi i/4}$.*

Demonstração. Já discutimos anteriormente o fato de que $\vartheta(\tau)$ é regular em $\mathscr{H}$. De acordo com a definição de forma modular (Capítulo 3), basta que provemos a asserção do enunciado para uma particular região fundamental padronizada segundo Γ_ϑ. No Corolário 15 do Capítulo 2, vimos que

$$\mathscr{R} = \mathscr{R}(\Gamma(1)) \cup S^{-1}\{\mathscr{R}(\Gamma(1))\} \cup S^{-1}T\{\mathscr{R}(\Gamma(1))\}$$

é uma região fundamental padronizada segundo Γ_ϑ. Assim, de acordo com a definição de forma modular, temos de satisfazer as condições enumeradas de 1. a 3. que seguem:

1.

$$\vartheta(M\tau) = \upsilon_\vartheta(M)(c\tau+d)^{1/2}\vartheta(\tau), \tag{4.15}$$

para todo $M = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma_\vartheta$, *onde* $|\upsilon_\vartheta(M)| = 1$;

Seja $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_\vartheta$. Então

$$\begin{aligned} \frac{M\tau+1}{2} &= \frac{\frac{a\tau+b}{c\tau+d}+1}{2} \\ &= \frac{(a+c)\tau+b+d}{2c\tau+2d} \\ &= \frac{2(a+c)\left(\frac{\tau+1}{2}\right)+b+d-(a+c)}{4c\left(\frac{\tau+1}{2}\right)+2d-2c} \\ &= \frac{(a+c)\left(\frac{\tau+1}{2}\right)+\left(\frac{b-c}{2}+\frac{d-a}{2}\right)}{(2c)\left(\frac{\tau+1}{2}\right)+(d-c)} = M_1\left(\frac{\tau+1}{2}\right), \end{aligned}$$

onde

$$M_1 = \begin{pmatrix} a+c & \frac{b-c}{2}+\frac{d-a}{2} \\ 2c & d-c \end{pmatrix} \in \Gamma(1),$$

uma vez que

$$\begin{aligned} (a+c)(d-c)-\left(\frac{b-c}{2}+\frac{d-a}{2}\right)(2c) &= ad-ac+cd-c^2-(b-c+d-a)c \\ &= ad-ac+cd-c^2-bc+c^2-cd+ac \\ &= ad-bc=1. \end{aligned}$$

Cabe aqui uma explicação acerca do fato de $\frac{b-c}{2}+\frac{d-a}{2}$ também ser inteiro. Como $M \in \Gamma_\vartheta$, o Corolário 5 do Capítulo 2 nos garante que $a \equiv d \pmod 2$ e $b \equiv c \pmod 2$, de tal maneira que $d-a$ e $b-c$ são pares, garantindo-se que $\frac{b-c}{2}$ e $\frac{d-a}{2}$ sejam inteiros. Da mesma forma,

$$M\tau+1 = \frac{a\tau+b}{c\tau+d}+1 = \frac{(a+c)\tau+(b+d)}{c\tau+d} = M_2\tau,$$

onde

$$M_2 = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} \in \Gamma(1),$$

dado que

$$(a+c)d-(b+d)c = ad+cd-bc-cd = ad-bc = 1.$$

Agora, se $\tau \in \mathscr{H}$, então $M\tau \in \mathscr{H}$, pela relação (2.2) do Capítulo 2. Portanto, o Teorema 10 implica que

$$\vartheta(M\tau) = \frac{\left[\eta\left(\frac{M\tau+1}{2}\right)\right]^2}{\eta(M\tau+1)} = \frac{\left[\eta\left(M_1\left(\frac{\tau+1}{2}\right)\right)\right]^2}{\eta(M_2\tau)}. \tag{4.16}$$

Por outro lado, o Teorema 8 nos comunica

$$\begin{aligned}\eta\left(M_1\left(\frac{\tau+1}{2}\right)\right) &= \upsilon_\eta(M_1)\left((2c)\left(\frac{\tau+1}{2}\right)+(d-c)\right)^{1/2}\eta\left(\frac{\tau+1}{2}\right)\\ &= \upsilon_\eta(M_1)(c\tau+d)^{1/2}\eta\left(\frac{\tau+1}{2}\right)\end{aligned}$$

e

$$\begin{aligned}\eta(M_2\tau) &= \upsilon_\eta(M_2)(c\tau+d)^{1/2}\eta(\tau)\\ &= \upsilon_\eta(M_2)(c\tau+d)^{1/2}[\upsilon_\eta(S)]^{-1}\eta(S\tau)\\ &= \upsilon_\eta(M_2)e^{-\pi i/12}(c\tau+d)^{1/2}\eta(\tau+1).\end{aligned}$$

Substituindo-se em (4.16) as expressões encontradas, temos

$$\begin{aligned}\vartheta(M\tau) &= \frac{\left[\upsilon_\eta(M_1)(c\tau+d)^{1/2}\eta\left(\frac{\tau+1}{2}\right)\right]^2}{\upsilon_\eta(M_2)e^{-\pi i/12}(c\tau+d)^{1/2}\eta(\tau+1)}\\ &= [\upsilon_\eta(M_1)]^2[\upsilon_\eta(M_2)]^{-1}e^{\pi i/12}(c\tau+d)^{1/2}\frac{\left[\eta\left(\frac{\tau+1}{2}\right)\right]^2}{\eta(\tau+1)}\\ &= \upsilon_\vartheta(M)(c\tau+d)^{1/2}\vartheta(\tau),\end{aligned}$$

utilizando-se novamente o Teorema 10, e considerando-se

$$\upsilon_\vartheta(M) = [\upsilon_\eta(M_1)]^2[\upsilon_\eta(M_2)]^{-1}e^{\pi i/12}, \tag{4.17}$$

tal que $|\upsilon_\vartheta(M)| = 1$. Isto termina a prova deste item, mas antes de passar ao próximo, encontremos as expressões para $\upsilon_\vartheta(S^2)$ e $\upsilon_\vartheta(T)$.

Pela definição de $\vartheta(\tau)$, temos

$$\vartheta(S^2\tau) = \vartheta(\tau+2) = 1+2\sum_{n=1}^{\infty}e^{\pi i n^2(\tau+2)} = 1+2\sum_{n=1}^{\infty}e^{\pi i n^2\tau} = \vartheta(\tau).$$

Como $S^2 = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$, e já sabemos que vale (4.15), segue que $\upsilon_\vartheta(S^2) = 1$ (lembrando também que $\vartheta(\tau)\neq 0$, para cada $\tau\in\mathscr{H}$). Ademais,

$$\vartheta(T\tau) = \upsilon_\vartheta(T)\tau^{1/2}\vartheta(\tau),$$

donde, tomando-se $\tau = i\in\mathscr{H}$, vem

$$\vartheta(i) = \upsilon_\vartheta(T)(i)^{1/2}\vartheta(i),$$

ou seja, $\upsilon_\vartheta(T) = (i)^{-1/2} = e^{-\pi i/4}$ ($\vartheta(i)\neq 0$, pelo Teorema 9).

2. *$\vartheta(\tau)$ possui uma expansão de Fourier em cada ponto parabólico de Γ_ϑ em $\mathscr{R}$;*
   Os pontos parabólicos de Γ_ϑ em $\mathscr{R}$, como vimos no Capítulo 3, são apenas dois: -1 ($S^{-1}T(\infty) = -1$) e ∞ ($I(\infty) = S^{-1}(\infty) = \infty$). Tratemos separadamente dos dois casos:

   (a) $q = -1$;
   Vimos, no exemplo seguinte à Definição 3 do Capítulo 3, que $\lambda = 1$. Ademais, temos $A = S^{-1}T = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, $\sigma(\tau) = (\tau+1)^{1/2}$, e

$$v_\vartheta((S^{-1}T)S^2(S^{-1}T)^{-1}) = v_\vartheta \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} = e^{\pi i/4} = e^{2\pi i(1/8)},$$

   utilizando-se a fórmula explícita para v_ϑ, que se encontra demonstrada no próximo capítulo. Neste ponto, revela-se de fundamental importância o fato de que aquela demonstração não leva em conta o fato de $\vartheta(\tau)$ ser forma modular. Como veremos, a obtenção de uma fórmula explícita para v_ϑ utiliza somente o item anterior e, particularmente, a relação de consistência exprimida em (3.3), no Capítulo 3. Deste modo, vem que $\kappa = 1/8$. Por outro lado, pelo Teorema 10, como $A\tau \in \mathscr{H}$, vem

$$\vartheta(A\tau) = \vartheta\left(\frac{-\tau-1}{\tau}\right) = \vartheta(-1-1/\tau) = \frac{\left[\eta\left(\frac{-1/\tau}{2}\right)\right]^2}{\eta(-1/\tau)} = \frac{[\eta(-1/2\tau)]^2}{\eta(-1/\tau)}.$$

   Agora, aplicando-se o Teorema 7, temos

$$\eta\left(-\frac{1}{2\tau}\right) = (-i)^{1/2}(2\tau)^{1/2}\eta(2\tau),$$

   e

$$\eta\left(-\frac{1}{\tau}\right) = (-i)^{1/2}\tau^{1/2}\eta(\tau),$$

donde

$$\begin{aligned}
\vartheta(A\tau) &= \frac{\left[(-i)^{1/2}(2\tau)^{1/2}\eta(2\tau)\right]^2}{(-i)^{1/2}\tau^{1/2}\eta(\tau)} \\
&= 2(-i)^{1/2}\tau^{1/2}\frac{[\eta(2\tau)]^2}{\eta(\tau)} \\
&= 2(-i)^{1/2}\tau^{1/2}\frac{\left[e^{\pi i\tau/6}\prod_{m=1}^{\infty}(1-e^{4\pi im\tau})\right]^2}{e^{\pi i\tau/12}\prod_{m=1}^{\infty}(1-e^{2\pi im\tau})} \\
&= 2(-i)^{1/2}\tau^{1/2}e^{\pi i\tau/4}\prod_{m=1}^{\infty}\left(1-e^{4\pi im\tau}\right)^2\prod_{m=1}^{\infty}\left(1-e^{2\pi im\tau}\right)^{-1} \\
&= 2(-i)^{1/2}\tau^{1/2}e^{\pi i\tau/4}\sum_{m'=0}^{\infty}a_{m'}e^{4\pi im'\tau}\sum_{n'=0}^{\infty}p(n')e^{2\pi in'\tau} \\
&= 2(-i)^{1/2}\tau^{1/2}e^{\pi i\tau/4}\sum_{n=0}^{\infty}b_n e^{2\pi in\tau} \\
&= \tau^{1/2}\sum_{n=0}^{\infty}2(-i)^{1/2}b_n e^{2\pi i[n+(1/8)]\tau},
\end{aligned}$$

para cada $\tau \in \mathscr{H}$, utilizando-se também a Proposição 1, para $x = e^{2\pi i\tau}$. Finalmente, tomando-se, na expressão anterior, $A^{-1}\tau = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\tau = -1/(\tau+1)$ em lugar de τ, temos

$$\begin{aligned}
\vartheta(\tau) &= \left(\frac{-1}{\tau+1}\right)^{1/2}\sum_{n=0}^{\infty}2(-i)^{1/2}b_n e^{2\pi i[n+(1/8)]A^{-1}\tau} \\
&= \frac{(-1)^{1/2}}{(\tau+1)^{1/2}}e^{2\pi ik(1/2)}\sum_{n=0}^{\infty}2(-i)^{1/2}b_n e^{2\pi i[n+(1/8)]A^{-1}\tau} \\
&= (\tau+1)^{-1/2}\sum_{n=0}^{\infty}\underbrace{e^{\pi ik}e^{-\pi i/2}2(-i)^{1/2}b_n}_{a_n}e^{2\pi i[n+(1/8)]A^{-1}\tau},
\end{aligned}$$

sendo k algum inteiro. Deste modo, a expressão acima coincide com a expansão de $\vartheta(\tau)$ em $q=-1$, de acordo com a relação (3.7) do Capítulo 3.

(b) $q = \infty$.

Neste caso, $\lambda = 2$, $\sigma(\tau) = 1$, $A = I$ (ou S^{-1}) e $\kappa = 0$ e, por definição,

$$\vartheta(\tau) = 1 + 2\sum_{n=1}^{\infty}e^{\pi in^2\tau},$$

que é, como podemos ver, a expansão de Fourier de $\vartheta(\tau)$ em $q=\infty$.

Logo, também este item está provado.

3. *$\vartheta(\tau)$ é meromorfa em cada ponto parabólico de Γ_ϑ em $\mathscr{R}$.*
   No item anterior, encontramos as expansões de Fourier de $\vartheta(\tau)$ nos pontos parabólicos de Γ_ϑ em $\mathscr{R}$. Nelas, vimos que os índices dos somatórios percorrem apenas valores não negativos, de modo que segue o resultado.

Em particular pelo comentário do último item acima, segue que $\vartheta(\tau)$ é regular em cada ponto parabólico de Γ_ϑ em $\mathscr{R}$. Portanto $\vartheta(\tau)$ é uma forma modular inteira de grau $-1/2$ com respeito a Γ_ϑ. Observe que $\vartheta(\tau)$ não é cúspide, uma vez que não há um zero de ordem positiva no ponto parabólico ∞. □

Capítulo 5

Os sistemas multiplicadores υ_η e υ_ϑ

Este capítulo se dedica à obtenção de fórmulas exatas para $\upsilon_\eta(M_1)$ e $\upsilon_\vartheta(M_2)$, sendo $M_1 \in \Gamma(1)$ e $M_2 \in \Gamma_\vartheta$, ou seja, fórmulas explícitas para tais funções, em termos dos coeficientes das matrizes em que se aplicam. Embora conceitualmente elementares, as demonstrações que faremos acerca dessas fórmulas apresentam bastante complexidade computacional, justificando-se a dedicação de um capítulo inteiro a elas. As fórmulas explícitas para os sistemas multiplicadores em questão são importantes para as aplicações da teoria de formas modulares à teoria dos números. Em particular, ainda que não seja objeto deste texto, são importantes à obtenção de resultados concernentes a $p(n)$ e $r_s(n)$ a partir de $\eta(\tau)$ e $\vartheta(\tau)$. A primeira fórmula exata para υ_η foi obtida por Rademacher, em termos de somas de Dedekind. A que apresentaremos aqui, todavia, é uma versão mais recente, devida a Petersson (*apud* [11], consulte *Abhandl. Deut. Akad. Wiss. Berlin, 2* (1954), 59 pp.).

Ambas as fórmulas são obviamente idênticas, diferindo apenas na forma em que se apresentam. A fórmula em termos de somas de Dedekind seria mais construtiva, dando-nos informações relativas às idéias que a ela conduziram, e, calculando-se as somas de Dedekind em termos do símbolo de Jacobi, obteríamos a versão que será aqui apresentada. Entretanto, para desenvolver a demonstração de Rademacher, seria necessário o desenvolvimento prévio de mais teoria, estendendo muito a demonstração. Deste modo, optamos, por brevidade, pela apresentação direta da fórmula devida a Petersson, procedendo sua prova por indução sobre o tamanho das matrizes em questão (idéia análoga à que foi aplicada no Teorema 8 do Capítulo 4). Uma vez obtida a fórmula para υ_η, a de υ_ϑ será conseqüência imediata da fórmula (4.17) do Capítulo 4. A título de curiosidade,

o leitor poderá notar, nas demonstrações que faremos, que não serão utilizadas todas as propriedades que tornam $\eta(\tau)$ e $\vartheta(\tau)$ formas modulares. De fato, como já dissemos na demonstração do Teorema 11 do capítulo anterior, só utilizaremos a relação (3.1) do Capítulo 3.

Finalmente, se necessário, indicamos ao leitor a revisão das propriedades dos símbolos de Jacobi e Legendre, resumida no Capítulo 1, na parte que trata de teoria dos números.

5.1 Fórmula explícita para υ_η

Esta seção se resume a um teorema e sua demonstração (quanto à notação aqui empregada, consulte a Seção 1.4 do Capítulo 1):

Teorema 1. *O sistema multiplicador υ_η da forma modular $\eta(\tau)$ é dado pela seguinte fórmula:*

$$\upsilon_\eta(M) = \begin{cases} \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) - 3c]\right\}, & \text{se } c \text{ é ímpar,} \\ \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) + 3d - 3 - 3cd]\right\}, & \text{se } c \text{ é par,} \end{cases}$$

para cada $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$.

Demonstração. Na demonstração do Teorema 8 do Capítulo 4, definimos o comprimento de um elemento de $\Gamma(1)$, quando escrito como produto finito dos elementos geradores S e T, e provamos o desejado por indução sobre esse comprimento. Para esta demonstração, o procedimento adotado será análogo, de modo que provaremos a fórmula para $\upsilon_\eta(M)$ por indução sobre o comprimento de M. Para tanto, a única relação de que nos utilizaremos é a dada por (3.3), no Capítulo 3, a saber,

$$\upsilon_\eta(M_3)(c_3\tau + d_3)^{1/2} = \upsilon_\eta(M_1)\upsilon_\eta(M_2)(c_1 M_2\tau + d_1)^{1/2}(c_2\tau + d_2)^{1/2}, \tag{5.1}$$

para o caso particular $\upsilon = \upsilon_\eta$, onde $M_1 = \begin{pmatrix} * & * \\ c_1 & d_1 \end{pmatrix}$, $M_2 = \begin{pmatrix} * & * \\ c_2 & d_2 \end{pmatrix}$ e $M_3 = M_1M_2 = \begin{pmatrix} * & * \\ c_3 & d_3 \end{pmatrix}$.

O único elemento de $\Gamma(1)$ que possui comprimento zero é a matriz I, e sabemos que $\upsilon_\eta(I) = 1$. Por outro lado, a fórmula proposta nos diz que

$$\upsilon_\eta(I) = \left(\frac{0}{1}\right)_* \exp\left\{\frac{\pi i}{12}(3-3)\right\} = 1,$$

donde a mesma é válida para palavras de comprimento zero. Agora, suponhamos que a fórmula dada seja válida para toda palavra de $\Gamma(1)$ cujo comprimento é $n-1$, sendo $n \geq 1$, e suponhamos que $M' \in \Gamma(1)$ e pode ser expressa como palavra de comprimento n. Neste caso, como no Teorema 8, $M' = MS$, ou $M' = MT$, ou $M' = MS^{-1}$, onde $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ possui comprimento $n-1$. Resta-nos, pois, provar que a fórmula proposta vale para cada uma dessas três possibilidades de M':

1. $M' = MS = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$;

   (a) *c é ímpar;*

   Neste caso, a relação (5.1) resulta

   $$\upsilon_\eta(M')(c\tau + c + d)^{1/2} = \upsilon_\eta(M)\upsilon_\eta(S)(cS\tau + d)^{1/2} = \upsilon_\eta(M)\upsilon_\eta(S)(c\tau + c + d)^{1/2},$$

   ou

   $$\begin{aligned} \upsilon_\eta(M') &= \upsilon_\eta(M)\upsilon_\eta(S) \\ &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) - 3c]\right\} e^{\pi i/12} \\ &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) - 3c + 1]\right\}, \end{aligned}$$

   utilizando-se a hipótese de indução e o Teorema 8. Por outro lado, a fórmula proposta para $\upsilon_\eta(M')$ nos fornece

   $$\begin{aligned} \upsilon_\eta(M') &= \left(\frac{c+d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+c+d)c - (a+b)(c+d)(c^2-1) - 3c]\right\} \\ &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) - 3c + E]\right\}, \end{aligned}$$

   onde $E = c^2 - (ac + bc + ad)(c^2-1)$, e utilizando-se que

   $$\left(\frac{c+d}{c}\right)^* = \left(\frac{c+d}{|c|}\right) = \left(\frac{d}{|c|}\right) = \left(\frac{d}{c}\right)^*,$$

   pois $|c|$ é ímpar positivo tal que $c + d \equiv d \pmod{|c|}$ e $(d, |c|) = 1$ $(c \neq 0)$.

Agora, como $ad - bc = 1$, temos

$$\begin{aligned} E &= c^2 - (ac + bc + ad)(c^2 - 1) \\ &= c^2 - (ac + 2bc + 1)(c^2 - 1) \\ &= -c^2(ac + 2bc) + ac + 2bc + 1 \\ &= c(a + 2b)(1 - c^2) + 1 \\ &= (1 - c)c(1 + c)(a + 2b) + 1. \end{aligned}$$

Se $c = \pm 1$, então $E = 1$. Caso contrário, $1-c$, c e $1+c$ definem uma seqüência de três números consecutivos, dentre os quais um é múltiplo de 3. Ademais, entre $1-c$ e $1+c$, temos dois números pares tais que um é múltiplo de 4. Logo, $8 \mid (1 - c)(1 + c)$ e $3 \mid (1 - c)c(1 + c)$, donde $24 \mid (1 - c)c(1 + c)(a + 2b)$, ou $E \equiv 1 \pmod{24}$. Logo,

$$v_\eta(M') = \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a + d)c - bd(c^2 - 1) - 3c + 1]\right\},$$

coincidindo com a expressão anterior.

(b) *c é par.*

Neste caso, analogamente ao anterior, temos

$$\begin{aligned} v_\eta(M') &= v_\eta(M)v_\eta(S) \\ &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a + d)c - bd(c^2 - 1) + 3d - 3 - 3cd]\right\} e^{\pi i/12} \\ &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a + d)c - bd(c^2 - 1) + 3d - 2 - 3cd]\right\}, \qquad (5.2) \end{aligned}$$

utilizando-se a hipótese de indução, agora para c par. Por outro lado, a fórmula proposta para $v_\eta(M')$ nos fornece

$$\begin{aligned} v_\eta(M') &= \left(\frac{c}{c + d}\right)_* \exp\left\{\frac{\pi i}{12}[(a + c + d)c - (a + b)(c + d)(c^2 - 1)\right. \\ &\quad \left. + 3(c + d) - 3 - 3c(c + d)]\right\}. \qquad (5.3) \end{aligned}$$

Como c é par e $ad - bc = 1$, temos que d é ímpar, donde $c + d$ também é ímpar. Se $c = 0$, então $a = d = \pm 1$, e (5.2) se reduz a

$$v_\eta(M') = \left(\frac{0}{\pm 1}\right)_* \exp\left\{\frac{\pi i}{12}[bd + 3d - 2]\right\},$$

enquanto (5.3) resulta

$$\begin{aligned} v_\eta(M') &= \left(\frac{0}{\pm 1}\right)_* \exp\left\{\frac{\pi i}{12}[(a+b)d+3d-3]\right\} \\ &= \left(\frac{0}{\pm 1}\right)_* \exp\left\{\frac{\pi i}{12}[bd+3d-2]\right\}, \end{aligned}$$

de modo que a fórmula vale para $c=0$. Portanto, podemos assumir $c \neq 0$, escrevendo $c = 2^\alpha c_0$, onde c_0 é ímpar e $\alpha \geq 1$. Desse modo, utilizando-se as partes do Lema 12 do Capítulo 1 indicadas acima dos sinais de igualdade, temos

$$\begin{aligned} \left(\frac{c}{c+d}\right)_* &= \left(\frac{2^\alpha c_0}{|c+d|}\right)(-1)^{\frac{\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(c+d)-1}{2}} \\ &\overset{3.}{=} \left(\frac{2}{|c+d|}\right)^\alpha \left(\frac{c_0}{|c+d|}\right)(-1)^{\frac{\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(c+d)-1}{2}} \\ &\overset{7.}{=} \left(\frac{2}{|c+d|}\right)^\alpha \left(\frac{c+d}{|c_0|}\right)(-1)^{\frac{\mathrm{sign}(c_0)-1}{2}\frac{\mathrm{sign}(c+d)-1}{2}}(-1)^{\frac{c_0-1}{2}\frac{c+d-1}{2}} \\ &\quad \cdot (-1)^{\frac{\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(c+d)-1}{2}} \\ &= \left(\frac{2}{|c+d|}\right)^\alpha \left(\frac{c+d}{|c_0|}\right)\left((-1)^{\frac{\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(c+d)-1}{2}}\right)^2 (-1)^{\frac{c_0-1}{2}\frac{c+d-1}{2}} \\ &= \left(\frac{2}{|c+d|}\right)^\alpha \left(\frac{c+d}{|c_0|}\right)(-1)^{\frac{c_0-1}{2}\frac{c+d-1}{2}} \\ &\overset{1.}{=} \left(\frac{2}{|c+d|}\right)^\alpha \left(\frac{d}{|c_0|}\right)(-1)^{\frac{c_0-1}{2}\frac{c+d-1}{2}} \\ &\overset{7.}{=} \left(\frac{2}{|c+d|}\right)^\alpha \left(\frac{c_0}{|d|}\right)(-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(c_0)-1}{2}}(-1)^{\frac{d-1}{2}\frac{c_0-1}{2}}(-1)^{\frac{c_0-1}{2}\frac{c+d-1}{2}} \\ &= \left(\frac{2}{|c+d|}\right)^\alpha \left(\frac{c_0}{|d|}\right)(-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(c_0)-1}{2}}(-1)^{\frac{c_0-1}{2}\frac{c}{2}} \underbrace{(-1)^{\frac{c_0-1}{2}(d-1)}}_{1} \\ &\overset{5.}{=} \left((-1)^{\frac{|c+d|^2-1}{8}}\right)^\alpha \left(\frac{c_0}{|d|}\right)(-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(c_0)-1}{2}}(-1)^{\frac{c_0-1}{2}\frac{c}{2}} \\ &= \left((-1)^{\frac{d^2-1}{8}}(-1)^{\frac{c^2+2cd}{8}}\right)^\alpha \left(\frac{c_0}{|d|}\right)(-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(c_0)-1}{2}}(-1)^{\frac{c_0-1}{2}\frac{c}{2}} \\ &\overset{5.}{=} \left(\frac{2}{|d|}\right)^\alpha \left(\frac{c_0}{|d|}\right)(-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(c_0)-1}{2}}(-1)^{\frac{c_0-1}{2}\frac{c}{2}}(-1)^{\frac{c^2+2cd}{8}\alpha} \\ &\overset{3.}{=} \left(\frac{2^\alpha c_0}{|d|}\right)(-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(c_0)-1}{2}}(-1)^{\frac{c_0-1}{2}\frac{c}{2}}(-1)^{\frac{c^2+2cd}{8}\alpha} \\ &= \left(\frac{c}{d}\right)_*(-1)^{\frac{c_0-1}{2}\frac{c}{2}}(-1)^{\frac{c^2+2cd}{8}\alpha} = \left(\frac{c}{d}\right)_* e^{(\pi i/12)\left[\frac{3}{2}\alpha(c^2+2cd)+3c(c_0-1)\right]}. \end{aligned}$$

Cabe aqui uma justificativa acerca do fato indispensável de que $(c_0, |c+d|) = 1$. Se $(c_0, c+d) = m$, então $m \mid c_0$ e $m \mid c+d$, donde $m \mid c$ e $m \mid d$. Portanto,

$m \mid (c,d) = 1$, donde $m = 1$, seguindo o resultado. Agora, substituindo-se o resultado anterior em (5.3), temos

$$\begin{aligned} v_\eta(M') &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a+c+d)c-(a+b)(c+d)(c^2-1)+3(c+d)-3\right. \\ &\quad \left. -3c(c+d)+\frac{3}{2}\alpha(c^2+2cd)+3c(c_0-1)\right]\Bigg\} \\ &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a+d)c-bd(c^2-1)+3d-2-3cd+E]\right\}, \end{aligned}$$

onde

$$E = c^2-(ac+bc+ad)(c^2-1)+3c-1-3c^2+\frac{3}{2}\alpha(c^2+2cd)+3c(c_0-1).$$

Comparando-se a expressão a que chegamos com (5.2), resta-nos provar que $E \equiv 0 \pmod{24}$. Note que

$$\begin{aligned} E &= -2c^2-(ac+2bc+1)(c^2-1)+3c-1+\frac{3}{2}\alpha c^2+3\alpha cd+3c(c_0-1) \\ &= -3c^2-(ac+2bc)(c^2-1)+3c+\frac{3}{2}\alpha c^2+3\alpha cd+3c(c_0-1). \end{aligned}$$

Como c é par não nulo, todos os termos da expressão acima são múltiplos de 3, donde $3 \mid E$, restando-nos provar que $8 \mid E$. Se $\alpha \geq 3$, então $8 \mid c$, sendo imediato o fato de que $8 \mid E$. Se $\alpha = 2$, então

$$\begin{aligned} E &= -3c^2-(ac+2bc)(c^2-1)+3c+3c^2+6cd+3c(c_0-1) \\ &= -(ac+2bc)(c^2-1)+6cd+3cc_0 \\ &= c[3c_0+6d-(a+2b)(c^2-1)] \end{aligned}$$

Agora, como $ad-bc = 1$ e $c \neq 0$ é par, temos que a é ímpar, donde $(a+2b)(c^2-1)$ também é ímpar. Ademais, o fato de c_0 ser ímpar implica que $3c_0$ é também ímpar. Logo, $3c_0-(a+2b)(c^2-1)$ é par, e o termo entre colchetes da expressão anterior é par. Como $4 \mid c$, segue, enfim, que $8 \mid E$. Finalizando, se $\alpha = 1$, então

$$\begin{aligned} E &= -3c^2-(ac+2bc)(c^2-1)+3c+\frac{3}{2}c^2+3cd+3c\left(\frac{c}{2}-1\right) \\ &= -(ac+2bc)(c^2-1)+3cd \\ &= c[3d-(a+2b)(c^2-1)]. \end{aligned}$$

Agora, temos que

$$3d-(a+2b)(c^2-1)\equiv 3d-(a+2b)(-1)=3d+a+2b \pmod 4,$$

uma vez que $c\neq 0$ é par. Agora, se b é par, então $ad=1+bc\equiv 1 \pmod 4$, donde $a\equiv d\equiv \pm 1 \pmod 4$ e, se b é ímpar, então $ad\equiv -1 \pmod 4$, donde $a\equiv d\pm 2 \pmod 4$. Em todo o caso, segue que $4 \mid 3d+a+2b$, donde $8 \mid E$. Assim, a prova deste item e deste caso se completam.

2. $M'=MS^{-1}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a & b-a \\ c & d-c \end{pmatrix}$;

A prova deste caso será análoga à do anterior e, por isso, alguns detalhes serão omitidos.

(a) *c é ímpar;*

Neste caso, a relação (5.1) resulta

$$\begin{aligned} v_\eta(M')(c\tau+d-c)^{1/2} &= v_\eta(M)v_\eta(S^{-1})(cS^{-1}\tau+d)^{1/2} \\ &= v_\eta(M)v_\eta(S^{-1})(c\tau+d-c)^{1/2}, \end{aligned}$$

ou

$$\begin{aligned} v_\eta(M') &= v_\eta(M)v_\eta(S^{-1}) \\ &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c-bd(c^2-1)-3c]\right\} e^{-\pi i/12} \\ &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c-bd(c^2-1)-3c-1]\right\}. \end{aligned}$$

Por outro lado, a fórmula proposta para $v_\eta(M')$ nos fornece

$$\begin{aligned} v_\eta(M') &= \left(\frac{d-c}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d-c)c-(b-a)(d-c)(c^2-1)-3c]\right\} \\ &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c-bd(c^2-1)-3c-1+E]\right\}, \end{aligned}$$

onde $E=-c^2+(ad+bc-ac)(c^2-1)+1$. Agora, como $ad-bc=1$, temos

$$\begin{aligned} E &= -c^2+(2bc-ac+1)(c^2-1)+1 \\ &= c^2(2bc-ac)-2bc+ac-1+1 \\ &= c(2b-a)(c^2-1) \\ &= (c-1)c(c+1)(2b-a), \end{aligned}$$

donde $E \equiv 0 \pmod{24}$. Logo,

$$v_\eta(M') = \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) - 3c - 1]\right\},$$

coincidindo com a expressão anterior.

(b) *c é par.*

Neste caso, temos

$$\begin{aligned} v_\eta(M') &= v_\eta(M)v_\eta(S^{-1}) \\ &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) + 3d - 3 - 3cd]\right\} e^{-\pi i/12} \\ &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) + 3d - 4 - 3cd]\right\}. \end{aligned} \tag{5.4}$$

Por outro lado, a fórmula proposta para $v_\eta(M')$ nos fornece

$$\begin{aligned} v_\eta(M') &= \left(\frac{c}{d-c}\right)_* \exp\left\{\frac{\pi i}{12}[(a+d-c)c - (b-a)(d-c)(c^2-1)\right. \\ &\quad \left. + 3(d-c) - 3 - 3c(d-c)]\right\}. \end{aligned} \tag{5.5}$$

Como c é par e $ad - bc = 1$, temos que a, d e $c+d$ são ímpares. Se $c = 0$, então $a = d = \pm 1$, de modo que (5.4) e (5.5) se reduzem a

$$v_\eta(M') = \left(\frac{0}{\pm 1}\right)_* \exp\left\{\frac{\pi i}{12}[bd + 3d - 4]\right\},$$

donde a fórmula é verdadeira para $c = 0$. Portanto, podemos assumir $c \neq 0$, escrevendo $c = 2^\alpha c_0$, onde c_0 é ímpar e $\alpha \geq 1$. Agora, realizando-se cálculos similares aos do caso anterior, temos:

$$\begin{aligned} \left(\frac{c}{d-c}\right)_* &= \left(\frac{2}{|d-c|}\right)^\alpha \left(\frac{c_0}{|d-c|}\right) (-1)^{\frac{\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d-c)-1}{2}} \\ &= \left(\frac{2}{|d-c|}\right)^\alpha \left(\frac{d-c}{|c_0|}\right) (-1)^{\frac{\mathrm{sign}(c_0)-1}{2}\frac{\mathrm{sign}(d-c)-1}{2}} (-1)^{\frac{c_0-1}{2}\frac{d-c-1}{2}} \\ &\quad \cdot (-1)^{\frac{\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d-c)-1}{2}} \\ &= \left(\frac{2}{|d-c|}\right)^\alpha \left(\frac{d}{|c_0|}\right) (-1)^{\frac{c_0-1}{2}\frac{d-c-1}{2}} \\ &= \left(\frac{2}{|d-c|}\right)^\alpha \left(\frac{c_0}{|d|}\right) (-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(c_0)-1}{2}} (-1)^{\frac{d-1}{2}\frac{c_0-1}{2}} (-1)^{\frac{c_0-1}{2}\frac{d-c-1}{2}} \\ &= \left((-1)^{\frac{|d-c|^2-1}{8}}\right)^\alpha \left(\frac{c_0}{|d|}\right) (-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(c_0)-1}{2}} (-1)^{\frac{c_0-1}{2}\frac{(-c)}{2}} \\ &= \left(\frac{2}{|d|}\right)^\alpha \left(\frac{c_0}{|d|}\right) (-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(c_0)-1}{2}} (-1)^{\frac{c_0-1}{2}\frac{(-c)}{2}} (-1)^{\frac{c^2-2cd}{8}\alpha} \\ &= \left(\frac{c}{d}\right)_* (-1)^{\frac{c_0-1}{2}\frac{(-c)}{2}} (-1)^{\frac{c^2-2cd}{8}\alpha} = \left(\frac{c}{d}\right)_* e^{(\pi i/12)\left[\frac{3}{2}\alpha(c^2-2cd) - 3c(c_0-1)\right]}. \end{aligned}$$

Substituindo-se o resultado anterior em (5.5), temos

$$\begin{aligned} v_\eta(M') &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a+d-c)c-(b-a)(d-c)(c^2-1)+3(d-c) \right. \\ &\quad \left. -3-3c(d-c)+\frac{3}{2}\alpha(c^2-2cd)-3c(c_0-1)\right]\right\} \\ &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a+d)c-bd(c^2-1)+3d-4-3cd+E]\right\}, \end{aligned}$$

onde

$$E = -c^2+(ad+bc-ac)(c^2-1)-3c+1+3c^2+\frac{3}{2}\alpha(c^2-2cd)-3c(c_0-1).$$

Comparando-se a expressão a que chegamos com (5.4), resta-nos provar que $E \equiv 0 \pmod{24}$. Note que

$$\begin{aligned} E &= 2c^2+(2bc-ac+1)(c^2-1)-3c+1+\frac{3}{2}\alpha(c^2-2cd)-3c(c_0-1) \\ &= 3c^2+(2bc-ac)(c^2-1)-3c+\frac{3}{2}\alpha c^2-3\alpha cd-3c(c_0-1). \end{aligned}$$

Agora, dividindo-se nos casos $\alpha = 1$, $\alpha = 2$ e $\alpha \geq 3$, provamos também que $24 \mid E$, de maneira análoga ao caso anterior.

3. $M' = MT = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$.

Este caso é o que apresenta maior dificuldade, devendo ser subdividido em três itens. Antes, porém, teremos de obter um resultado auxiliar. Da relação (5.1), resulta que

$$\begin{aligned} v_\eta(M')(d\tau-c)^{1/2} &= v_\eta(M)v_\eta(T)(cT\tau+d)^{1/2}\tau^{1/2} \\ &= v_\eta(M)v_\eta(T)(-c/\tau+d)^{1/2}\tau^{1/2} \\ &= v_\eta(M)v_\eta(T)\left(\frac{d\tau-c}{\tau}\right)^{1/2}\tau^{1/2}. \end{aligned}$$

Provemos que

$$\frac{\left(\frac{d\tau-c}{\tau}\right)^{1/2}\tau^{1/2}}{(d\tau-c)^{1/2}} = \underbrace{(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}}}_{w}, \qquad \text{se } c \neq 0,\ d \neq 0. \tag{5.6}$$

É claro que ambos os membros de (5.6) possuem o mesmo valor absoluto, igual a 1. Portanto, falta-nos provar que seus argumentos também são iguais. Mas sabemos que

$$\arg(w) = \arg\left(\frac{d\tau-c}{\tau}\right)+\arg(\tau)-\arg(d\tau-c)+2n\pi,$$

para algum n inteiro, e também que, se $\tau = x + iy \in \mathscr{H}$,

$$d\tau - c = (dx - c) + i(dy),$$

e

$$\frac{d\tau - c}{\tau} = \left(d - \frac{cx}{x^2+y^2}\right) + i\left(\frac{cy}{x^2+y^2}\right).$$

Se provarmos que $n = 0$, ou seja, que

$$2|n|\pi = \left|\arg(w) - \arg\left(\frac{d\tau - c}{\tau}\right) - \arg(\tau) + \arg(d\tau - c)\right| < 2\pi,$$

para cada combinação de sinais de c e d, a prova de (5.6) termina. Isso é análogo ao que fizemos em demonstrações anteriores, considerando-se a convenção (3.2) do Capítulo 3. Assim, (5.6) já pode ser admitida, de tal maneira que

$$\begin{aligned} \upsilon_\eta(M') &= \upsilon_\eta(M)\upsilon_\eta(T)(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}} \\ &= \upsilon_\eta(M)e^{-\pi i/4}(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}}, \end{aligned} \tag{5.7}$$

desde que $c \neq 0$ e $d \neq 0$, utilizando-se também o Teorema 8 do Capítulo 4. Agora, estamos em condições de tratar dos três itens acima mencionados:

(a) *c e d são ímpares;*

Neste caso, em particular, c e d são não nulos, de forma que (5.7) se aplica e, utilizando-se a hipótese de indução para M, temos que

$$\upsilon_\eta(M') = \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) - 3c - 3]\right\}(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}},$$

enquanto a fórmula proposta nos dá

$$\upsilon_\eta(M') = \left(\frac{-c}{d}\right)^* \exp\left\{\frac{\pi i}{12}[(b-c)d - ac(d^2-1) - 3d]\right\}.$$

Agora, temos que

$$\begin{aligned} \left(\frac{-c}{d}\right)^* &= \left(\frac{-c}{|d|}\right) \\ &= \left(\frac{d}{|-c|}\right)(-1)^{\frac{\mathrm{sign}(-c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}}(-1)^{\frac{-c-1}{2}\frac{d-1}{2}} \\ &= \left(\frac{d}{c}\right)^*(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}}\left(e^{\pi i}\right)^{\frac{-c-1}{2}\frac{d-1}{2}} \\ &= \left(\frac{d}{c}\right)^*(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}}e^{(-\pi i/12)[3(c+1)(d-1)]}, \end{aligned}$$

de modo que a fórmula proposta se torna

$$\begin{aligned} v_\eta(M') &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(b-c)d - ac(d^2-1) - 3d - 3(c+1)(d-1)]\right\} \\ &\quad \cdot (-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}} \\ &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) - 3c - 3 + E]\right\} \\ &\quad \cdot (-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}}, \end{aligned}$$

sendo

$$\begin{aligned} E &= [(b-c)d - ac(d^2-1) - 3d - 3(c+1)(d-1)] \\ &\quad - [(a+d)c - bd(c^2-1) - 3c - 3] \\ &= bd - cd - acd^2 + ac - 3d - 3cd + 3c - 3d + 3 \\ &\quad - ac - cd + bdc^2 - bd + 3c + 3 \\ &= -5cd - cd(1+bc) - 6d + 6c + 6 + bdc^2 \\ &= -6cd - 6d + 6c + 6 \\ &= -6(c+1)(d-1) \equiv 0 \pmod{24}, \end{aligned}$$

uma vez que c e d são ímpares, utilizando-se, ainda, que $ad - bc = 1$. Daqui segue o que queríamos mostrar.

(b) *c é impar e d é par;*

Agora, $c \neq 0$. Se $d = 0$, então $ad - bc = 1$ implica $bc = -1$, donde $b = -c = \pm 1$. Portanto, a relação (5.1) implica

$$v_\eta(M') = v_\eta(M)v_\eta(T)\frac{\left(\frac{-c}{\tau}\right)^{1/2}\tau^{1/2}}{(-c)^{1/2}}.$$

Analogamente ao que fizemos para o caso geral, podemos concluir que, se $c = 1$, então

$$\frac{\left(\frac{-c}{\tau}\right)^{1/2}\tau^{1/2}}{(-c)^{1/2}} = -1$$

e, se $c = -1$, então

$$\frac{\left(\frac{-c}{\tau}\right)^{1/2}\tau^{1/2}}{(-c)^{1/2}} = 1,$$

ou, em suma,

$$\frac{\left(\frac{-c}{\tau}\right)^{1/2}\tau^{1/2}}{(-c)^{1/2}} = (-1)^{\frac{c+1}{2}} = -c.$$

Portanto, pela hipótese de indução,

$$\begin{aligned}\upsilon_\eta(M') &= \upsilon_\eta(M)e^{-\pi i/4}(-1)^{\frac{c+1}{2}} \\ &= \left(\frac{0}{c}\right)^* \exp\left\{\frac{\pi i}{12}(ac-3c)\right\} e^{-\pi i/4}\left(e^{\pi i}\right)^{\frac{c+1}{2}} \\ &= \exp\left\{\frac{\pi i}{12}(ac+3c+3)\right\},\end{aligned}$$

pois $c = \pm 1$. Por outro lado, a fórmula proposta para $\upsilon_\eta(M')$ resulta, pelo fato de $d = 0$ ser par,

$$\begin{aligned}\upsilon_\eta(M') &= \left(\frac{0}{-c}\right)_* \exp\left\{\frac{\pi i}{12}[(b-c)0-(-a)(-c)(0^2-1)+3(-c)-3-3(0)(-c)]\right\} \\ &= (-1)^{\frac{c+1}{2}} \exp\left\{\frac{\pi i}{12}[(ac-3c-3]\right\} \\ &= \exp\left\{\frac{\pi i}{12}[(ac+3c+3]\right\},\end{aligned}$$

utilizando-se também que $c = \pm 1$. Isso termina a demonstração para o caso $d = 0$.

Agora, se $d \neq 0$, podemos aplicar (5.7) e a hipótese de indução, obtendo

$$\upsilon_\eta(M') = \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c-bd(c^2-1)-3c-3]\right\}(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}},$$

enquanto a fórmula proposta resulta

$$\begin{aligned}\upsilon_\eta(M') &= \left(\frac{d}{-c}\right)_* \exp\left\{\frac{\pi i}{12}[(b-c)d-ac(d^2-1)-3c-3+3cd]\right\} \\ &= \left(\frac{d}{|-c|}\right)(-1)^{\frac{\mathrm{sign}(d)-1}{2}\frac{\mathrm{sign}(-c)-1}{2}} \exp\left\{\frac{\pi i}{12}[(b-c)d-ac(d^2-1)-3c \right. \\ &\quad \left. -3+3cd]\right\} \\ &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[(b-c)d-ac(d^2-1)-3c-3+3cd]\right\} \\ &\quad \cdot(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}}.\end{aligned}$$

Note, porém, que

$$\begin{aligned}&(b-c)d-ac(d^2-1)-3c-3+3cd = \\ &\quad = bd-cd-cd(1+bc)+ac-3c-3+3cd \\ &\quad = (a+d)c-bd(c^2-1)-3c-3,\end{aligned}$$

de modo que a fórmula proposta é, também neste caso, verdadeira.

(c) *c é par.*

Como $ad - bc = 1$, então d é ímpar e, em particular, $d \neq 0$. Se $c = 0$, então $d = \pm 1$, e (5.7) se torna

$$\upsilon_\eta(M') = \upsilon_\eta(M)\upsilon_\eta(T)\frac{d^{1/2}\tau^{1/2}}{(d\tau)^{1/2}}.$$

Como procedemos nos outros casos, podemos provar que $(d\tau)^{1/2} = d^{1/2}\tau^{1/2}$, de modo que

$$\begin{aligned}
\upsilon_\eta(M') &= \upsilon_\eta(M)\upsilon_\eta(T) \\
&= \left(\frac{0}{d}\right)_* \exp\left\{\frac{\pi i}{12}[bd + 3d - 3]\right\} e^{-\pi i/4} \\
&= (-1)^{\frac{d-1}{2}} \exp\left\{\frac{\pi i}{12}[bd + 3d - 6]\right\} \\
&= \left(e^{\pi i}\right)^{\frac{d-1}{2}} \exp\left\{\frac{\pi i}{12}[bd + 3d - 6]\right\} \\
&= \exp\left\{\frac{\pi i}{12}[bd + 9d - 12]\right\},
\end{aligned}$$

utilizando-se a hipótese de indução. Por outro lado, a fórmula proposta nos sugere que

$$\begin{aligned}
\upsilon_\eta(M') &= \left(\frac{0}{d}\right)^* \exp\left\{\frac{\pi i}{12}(bd - 3d)\right\} \\
&= \exp\left\{\frac{\pi i}{12}(bd - 3d)\right\} \\
&= \exp\left\{\frac{\pi i}{12}(bd + 9d - 12 + E)\right\},
\end{aligned}$$

onde

$$E = 12 - 12d \equiv 0 \pmod{24},$$

concluindo esta possibilidade.

Agora, podemos assumir $c \neq 0$, aplicando novamente o resultado (5.7) e a

hipótese de indução:

$$\begin{aligned}
\upsilon_\eta(M') &= \upsilon_\eta(M)\upsilon_\eta(T)(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}} \\
&= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) + 3d - 3 - 3cd]\right\} e^{-\pi i/4} \\
&\quad \cdot (-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}} \\
&= \left(\frac{c}{|d|}\right)(-1)^{\frac{\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}} \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) + 3d - 6\right. \\
&\quad \left. - 3cd]\right\}(-1)^{\frac{-\mathrm{sign}(c)-1}{2}\frac{\mathrm{sign}(d)-1}{2}} \\
&= \left(\frac{c}{|d|}\right)(-1)^{\frac{\mathrm{sign}(d)-1}{2}} \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) + 3d - 6 - 3cd]\right\} \\
&= \left(\frac{c}{d}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) + 3d - 6 - 3cd]\right\}(-1)^{\frac{\mathrm{sign}(d)-1}{2}}.
\end{aligned}$$

A fórmula proposta, por outro lado, nos dá

$$\begin{aligned}
\upsilon_\eta(M') &= \left(\frac{-c}{d}\right)^* \exp\left\{\frac{\pi i}{12}[(b-c)d - ac(d^2-1) - 3d]\right\} \\
&= \left(\frac{-1}{|d|}\right)\left(\frac{c}{|d|}\right) \exp\left\{\frac{\pi i}{12}[(b-c)d - ac(d^2-1) - 3d]\right\} \\
&= (-1)^{\frac{|d|-1}{2}}\left(\frac{c}{d}\right)^* \exp\left\{\frac{\pi i}{12}[(b-c)d - ac(d^2-1) - 3d]\right\} \\
&= (-1)^{\frac{|d|-1}{2}}\left(\frac{c}{d}\right)^* \exp\left\{\frac{\pi i}{12}[(a+d)c - bd(c^2-1) + 3d - 6 - 3cd]\right\} \\
&\quad \cdot e^{\pi i E/12},
\end{aligned}$$

onde

$$\begin{aligned}
E &= [(b-c)d - ac(d^2-1) - 3d] - [(a+d)c - bd(c^2-1) + 3d - 6 - 3cd] \\
&= bd - cd - acd^2 + ac - 3d - ac - cd + bdc^2 - bd - 3d + 6 + 3cd \\
&= cd - cd(ad-bc) - 6d + 6 = 6 - 6d
\end{aligned}$$

utilizando acima as partes 3. e 4. do Lema 12 do Capítulo 1. Para provarmos a veracidade da fórmula nesse caso, basta que mostremos que

$$(-1)^{\frac{|d|-1}{2}} e^{\pi i E/12} = (-1)^{\frac{\mathrm{sign}(d)-1}{2}}.$$

De fato, como $E = 6 - 6d$, temos

$$(-1)^{\frac{|d|-1}{2}} e^{\pi i E/12} = (-1)^{\frac{|d|-1}{2}}(-1)^{\frac{6-6d}{12}} = (-1)^{\frac{|d|-d}{2}} = (-1)^{\frac{\mathrm{sign}(d)-1}{2}},$$

pois d é ímpar. Isto termina a prova deste item, deste caso, e deste teorema.

□

5.2 Fórmula explícita para υ_ϑ

Como vimos no Capítulo 4, muitas das propriedades de $\vartheta(\tau)$ podem ser deduzidas a partir das propriedades de $\eta(\tau)$. A seção anterior trouxe a trabalhosa demonstração da fórmula explícita para $\eta(\tau)$. Assim, utilizando-nos desse resultado e de alguns outros do capítulo anterior, a prova de uma fórmula explícita para υ_ϑ será facilitada sobremaneira.

Teorema 2. *O sistema multiplicador υ_ϑ da forma modular $\vartheta(\tau)$ é dado pela seguinte fórmula:*

$$\upsilon_\vartheta(M) = \begin{cases} \left(\frac{d}{c}\right)^* e^{-\pi i c/4}, & \text{se } a \equiv d \equiv 0,\ b \equiv c \equiv 1 \pmod 2, \\ \left(\frac{c}{d}\right)_* e^{\pi i (d-1)/4}, & \text{se } a \equiv d \equiv 1,\ b \equiv c \equiv 0 \pmod 2, \end{cases}$$

para cada $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_\vartheta$.

Demonstração. Para esta demonstração, faremos uso do Teorema 11 do Capítulo 4. Naquele teorema, comentamos que, se $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_\vartheta$, então $a \equiv d$ e $b \equiv c$. Observando-se, ainda, que $ad - bc = 1$, segue que, no enunciado deste teorema, estão realmente indicadas todas as possibilidades para M. Além disso, também mostramos, naquele teorema, que, se considerarmos

$$M_1 = \begin{pmatrix} a+c & \frac{b-c}{2} + \frac{d-a}{2} \\ 2c & d-c \end{pmatrix} \quad \text{e} \quad M_2 = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix},$$

ambos elementos de $\Gamma(1)$, vale o seguinte

$$\upsilon_\vartheta(M) = [\upsilon_\eta(M_1)]^2 [\upsilon_\eta(M_2)]^{-1} e^{\pi i/12}.$$

Agora, já temos uma expressão para υ_ϑ, uma vez que já sabemos calcular υ_η. Todavia, para que cheguemos à fórmula na maneira expressa no enunciado, dividamos em dois casos:

1. $a \equiv d \equiv 0$, $b \equiv c \equiv 1 \pmod 2$;

Em M_1, $2c$ é par e, em M_2, c é ímpar. Logo, o Teorema 1 nos dá

$$\begin{aligned}
v_\eta(M_1) &= \left(\frac{2c}{d-c}\right)_* \exp\left\{\frac{\pi i}{12}\left[((a+c)+(d-c))(2c) - \left(\frac{b-c}{2}+\frac{d-a}{2}\right)(d-c)\right.\right. \\
&\quad \left.\left.\cdot((2c)^2-1) + 3(d-c) - 3 - 3(2c)(d-c)\right]\right\} \\
&= \left(\frac{2c}{d-c}\right)_* \exp\left\{\frac{\pi i}{24}\left[4ac + 4cd - 4bc^2d + 4c^3d - 4c^2d^2 + 4ac^2d + 4bc^3\right.\right. \\
&\quad \left. - 4c^4 + 4c^3d - 4ac^3 + bd - cd + d^2 - ad - bc + c^2 - cd + ac + 6d\right. \\
&\quad \left.\left. - 6c - 6 - 12cd + 12c^2\right]\right\} \\
&= \left(\frac{2c}{d-c}\right)_* \exp\left\{\frac{\pi i}{24}\left[5ac - 10cd - 4bc^2d + 8c^3d - 4c^2d^2 + 4ac^2d + 4bc^3\right.\right. \\
&\quad \left.\left. - 4c^4 - 4ac^3 + bd + d^2 - ad - bc + c^2 + 6d - 6c - 6 + 12c^2\right]\right\}
\end{aligned}$$

e

$$\begin{aligned}
v_\eta(M_2) &= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[((a+c)+d)c - (b+d)d(c^2-1) - 3c]\right\} \\
&= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[ac + c^2 + cd - bc^2d + bd - c^2d^2 + d^2 - 3c]\right\}.
\end{aligned}$$

Deste modo, temos

$$\begin{aligned}
v_\vartheta(M) &= [v_\eta(M_1)]^2[v_\eta(M_2)]^{-1}e^{\pi i/12} \\
&= \left[\left(\frac{2c}{d-c}\right)_* \exp\left\{\frac{\pi i}{24}\left[5ac - 10cd - 4bc^2d + 8c^3d - 4c^2d^2 + 4ac^2d + 4bc^3\right.\right.\right. \\
&\quad \left.\left.\left. - 4c^4 - 4ac^3 + bd + d^2 - ad - bc + c^2 + 6d - 6c - 6 + 12c^2\right]\right\}\right]^2 \\
&\quad \cdot \left[\left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}[ac + c^2 + cd - bc^2d + bd - c^2d^2 + d^2 - 3c]\right\}\right]^{-1} e^{\pi i/12} \\
&= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}\left[(5ac - 10cd - 4bc^2d + 8c^3d - 4c^2d^2 + 4ac^2d + 4bc^3\right.\right. \\
&\quad - 4c^4 - 4ac^3 + bd + d^2 - ad - bc + c^2 + 6d - 6c - 6 + 12c^2) \\
&\quad \left.\left. - (ac + c^2 + cd - bc^2d + bd - c^2d^2 + d^2 - 3c) + 1\right]\right\} \\
&= \left(\frac{d}{c}\right)^* \exp\left\{\frac{\pi i}{12}\left[4ac - 11cd - 3bc^2d + 8c^3d - 3c^2d^2 + 4ac^2d + 4bc^3\right.\right. \\
&\quad \left.\left. - 4c^4 - 4ac^3 - ad - bc + 6d - 3c - 5 + 12c^2\right]\right\}
\end{aligned}$$

Agora, como c é ímpar, temos que $c^2 - 1 = (c-1)(c+1)$ é um múltiplo de 4. Além disso, é claro que $3 \mid c(c^2-1) = (c-1)c(c+1)$ (três números consecutivos).

Portanto, lembrando também que a e d são pares e que $ad - bc = 1$, trabalhando com congruências módulo 24, temos

$$\begin{aligned}
& 4ac - 11cd - 3bc^2d + 8c^3d - 3c^2d^2 + 4ac^2d + 4bc^3 - 4c^4 - 4ac^3 - ad - bc + 6d \\
& - 3c - 5 + \underbrace{12c^2}_{\equiv 12} \\
\equiv\ & \underbrace{4ac(1-c^2)}_{\equiv 0} + \underbrace{8cd(c^2-1)}_{\equiv 0} - 3cd - 3bc^2d - 3c^2d^2 + 4c^2(1+bc) + 4bc^3 \\
& - 4c^4 - (1+bc) - bc + 6d - 3c + 7 \\
\equiv\ & -3cd - 3bc^2d - 3c^2d^2 + 8bc^3 + \underbrace{4c^2(1-c^2)}_{\equiv 0} - 2bc + 6d - 3c + 6 \\
\equiv\ & -3cd - 3bc^2d - 3c^2d^2 + \underbrace{8bc(c^2-1)}_{\equiv 0} + 6bc + 6d - 3c + 6 \\
\equiv\ & -9cd - 3bc^2d - 3c^2d^2 + \underbrace{6(bc+1)}_{6ad \equiv 0} + \underbrace{6d(c+1)}_{\equiv 0} - 3c \\
\equiv\ & \underbrace{-3cd(3+bc+cd)}_{\equiv 0} - 3c \\
\equiv\ & -3c \pmod{24}.
\end{aligned}$$

Quanto à última passagem acima, sabemos que $6 \mid (-3cd)$. É claro, ainda, que $3 + bc + cd$ é um número par. Todavia, apenas isso não nos assegura que $24 \mid [-3cd(3 + bc + cd)]$. Observe, porém, que, se $3 + bc + cd = 0$, então, nada há que se provar; se $3 + bc + cd = 2$, então $3 + (ad - 1) + cd = 2$, donde $d(a + c) = 0$, ou seja, $d = 0$, uma vez que $a + c$ é ímpar; se $3 + bc + cd = -2$, então $d(a + c) = -4$, donde $d = \pm 4$ e $a + c = \mp 1$; finalmente, se $3 + bc + cd$ é um par cujo módulo é maior do que 2, então o resultado também é imediato. Segue que $-3cd(3+bc+cd) \equiv 0 \pmod{24}$. Pelo resultado anterior, temos que

$$v_\vartheta(M) = \left(\frac{d}{c}\right)^* e^{(\pi i/12)(-3c)} = e^{-\pi ic/4},$$

como queríamos mostrar.

2. $a \equiv d \equiv 1$, $b \equiv c \equiv 0 \pmod 2$;
   Neste caso, em M_1, $2c$ é par e, em M_2, c também é par. Logo, o Teorema 1 nos dá

o mesmo valor do item anterior para $\upsilon_\eta(M_1)$ e, para $\upsilon_\eta(M_2)$, temos

$$\begin{aligned}\upsilon_\eta(M_2) &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[((a+c)+d)c-(b+d)d(c^2-1)+3d-3-3cd]\right\}\\ &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[ac+c^2-2cd-bc^2d+bd-c^2d^2+d^2+3d-3]\right\}\end{aligned}$$

Deste modo, temos

$$\begin{aligned}\upsilon_\vartheta(M) &= [\upsilon_\eta(M_1)]^2[\upsilon_\eta(M_2)]^{-1}e^{\pi i/12}\\ &= \left[\left(\frac{2c}{d-c}\right)_* \exp\left\{\frac{\pi i}{24}\left[5ac-10cd-4bc^2d+8c^3d-4c^2d^2+4ac^2d+4bc^3\right.\right.\right.\\ &\quad \left.\left.\left.-4c^4-4ac^3+bd+d^2-ad-bc+c^2+6d-6c-6+12c^2\right]\right\}\right]^2\\ &\quad \cdot\left[\left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}[ac+c^2-2cd-bc^2d+bd-c^2d^2+d^2+3d-3]\right\}\right]^{-1}\\ &\quad \cdot e^{\pi i/12}\\ &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}\left[(5ac-10cd-4bc^2d+8c^3d-4c^2d^2+4ac^2d+4bc^3\right.\right.\\ &\quad -4c^4-4ac^3+bd+d^2-ad-bc+c^2+6d-6c-6+12c^2)\\ &\quad \left.\left.-(ac+c^2-2cd-bc^2d+bd-c^2d^2+d^2+3d-3)+1\right]\right\}\\ &= \left(\frac{c}{d}\right)_* \exp\left\{\frac{\pi i}{12}\left[4ac-8cd-3bc^2d+8c^3d-3c^2d^2+4ac^2d+4bc^3-4c^4\right.\right.\\ &\quad \left.\left.-4ac^3-ad-bc+3d-6c-2+12c^2\right]\right\}\end{aligned}$$

Agora, trabalhando-se com a expressão que está entre colchetes, módulo 24, como

no item anterior, temos

$$\begin{aligned}
& 4ac - 8cd - \underbrace{3bc^2d}_{\equiv 0} + 8c^3d - 3c^2d^2 + 4ac^2d + 4bc^3 - 4c^4 - 4ac^3 - ad - bc + 3d \\
& - 6c - 2 + \underbrace{12c^2}_{\equiv 0} \\
\equiv\ & \underbrace{4ac(1-c^2)}_{\equiv 0} + \underbrace{8cd(c^2-1)}_{\equiv 0} - 3c^2d^2 + 4c^2(1+bc) + \underbrace{4bc(c^2-1)}_{\equiv 0} + 4bc - 4c^4 \\
& - (1+bc) - bc + 3d - 6c - 2 \\
\equiv\ & -3c^2d^2 + 4c^2 + 4bc^3 + 2bc - 4c^4 + 3d - 6c - 3 \\
\equiv\ & -3c^2d^2 + \underbrace{4c^2(1-c^2)}_{\equiv 0} + \underbrace{4bc(c^2-1)}_{\equiv 0} + \underbrace{6bc}_{\equiv 0} + 3d - 6c - 3 \\
\equiv\ & \underbrace{-3c(cd^2+2)}_{\equiv 0} + 3d - 3 \\
\equiv\ & 3(d-1)
\end{aligned}$$

Quanto à última passagem acima, podemos justificá-la de modo semelhante ao que fizemos no item anterior, dividindo nos casos $cd^2+2=0$, $cd^2+2=2$, $cd^2+2=-2$, e $|cd^2+2|>2$. Em todos, é verdade que $24 \mid [-3c(cd^2+2)]$, como afirmamos. Assim, temos que

$$v_\vartheta(M) = \left(\frac{c}{d}\right)_* e^{(\pi i/12)(3(d-1))} = e^{\pi i(d-1)/4},$$

como queríamos mostrar. Isto termina a prova deste teorema e, com ela, a dissertação.

□

Referências Bibliográficas

[1] ABLOWITZ, M. J., FOKAS, A. S. **Complex variables: introduction and applications**. New York: Cambridge University Press, 1997. 647 pp.

[2] ANDREWS, G. E. "A simple proof of Jacobi triple product identity". Proc. Amer. Math. Soc. 16, 1965, pp 333-334.

[3] BARTLE, R. G. **The elements of integration and Lebesgue measure**. New York: John Wiley & Sons, 1966. 179 pp.

[4] CHURCHILL, R. V. **Variáveis Complexas e suas aplicações**. São Paulo: McGraw-Hill do Brasil/Editora da USP, 1975. 276 pp.

[5] CONWAY, J. B. **Functions of one complex variable I**. New York: Springer-Verlag, 1978. 317 pp.

[6] DOMINGUES, H. H. **Espaços métricos e introdução à topologia**. São Paulo: Atual, 1982. 184 pp.

[7] GUNNING, R. C. **Lectures on modular forms**. New Jersey: Princeton University Press, 1962. 86 pp.

[8] HILLE, E. **Analytic function theory**. New York: Chelsea, 1973. 308 pp, v. I.

[9] HILLE, E. **Analytic function theory**. New York: Chelsea, 1987. 496 pp, v. II.

[10] KNOPP, K. **Theory and applications os infinite series**. New York: Dover, 1990. 563 pp.

[11] KNOPP, M. I. **Modular functions in analytic number theory**. New York: Chelsea, 1993. 154 pp.

[12] KOBLITZ, N. **Introduction to elliptic curves and modular forms**. New York: Springer-Verlag, 1984. 248 pp.

[13] KOCHLOUKOVA, D. H. *Notas de aula da disciplina MM446: Grupos e Representações*, UNICAMP, primeiro semestre de 2005.

[14] LANG, S. **Introduction to modular forms**. New Jersey: Springer-Verlag, 1976. 261 pp.

[15] LEVEQUE, W. J. **Topics in number theory**. London: Addison-Wesley, 1956. 270 pp, v. II.

[16] LIMA, E. L. **Curso de análise**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2002. 344 pp, v. I.

[17] MILNE, J. S. *Modular functions and modular forms*. Notas de aula de Math 678, Michigan University, outono de 1990.

[18] MIYAKE, T. **Modular forms**. New York: Springer-Verlag, 1989. 335 pp.

[19] MUJICA, J. *Notas de Topologia Geral*. Notas de aula de MM733, UNICAMP, primeiro semestre de 2004.

[20] NIVEN, I. M. "Formal power series". Amer. Math. Monthly 76, 1969, pp 871-889.

[21] OLIVEIRA, E. C., MAIORINO, J. E. **Introdução aos métodos da matemática aplicada**. Campinas: Editora da UNICAMP, 2003. 241 pp.

[22] SANTOS, J. P. O. **Introdução à teoria dos números**.

[23] SANTOS, J. P. O., MELLO, M. P., MURARI, I. T. C. **Introdução à análise combinatória**. Campinas: Editora da UNICAMP, 2002. 297 pp.

[24] SERRE, J. P. **A course in arithmetic**. New York: Springer-Verlag, 1973. 115 pp.

[25] SHOKRANIAN, S., SOARES, M., GODINHO, H. **Teoria dos números**. Brasília: Editora da UNB, 1999. 325 pp.

[26] SIDKI

[27] TITCHMARSH, E. C. **The theory of functions**. New York: Oxford University Press, 1952.

[28] WHITTAKER, E. T., WATSON, G. N. **A course of modern analysis**. New York: Cambridge University Press, 1988. 608 pp.

[29] **www.mathworld.wolfram.com**. Acessado no dia 10/01/2006.

Índice Remissivo