Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Gênero profinito de grupos de variedades planas e solúveis

Genildo de Jesus Nery

Brasília

2021

Genildo de Jesus Nery

Gênero profinito de grupos de variedades planas e solúveis

Tese apresentada ao Programa de Pós-Graduação em Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de DOUTOR EM MATEMÁTICA.

Orientador:
Prof. Dr. Pavel Zalesski

Brasília

2021

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

NN456n1
89g

Nery, Genildo de Jesus
Gênero profinito de grupos de variedades planas e solúveis / Genildo de Jesus Nery; orientador Pavel Zalesski. -- Brasília, 2021.
113 p.

Tese (Doutorado - Doutorado em Matemática) -- Universidade de Brasília, 2021.

1. Gênero Profinito. 2. Grupos de Bieberbach. 3. Grupos Residualmente Finitos. I. Zalesski, Pavel, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Gênero profinito de grupos de variedades planos e solúveis.

por

Genildo de Jesus Nery *

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

DOUTOR EM MATEMÁTICA

Brasília, 18 de junho de 2021.

Comissão Examinadora:

Pavel Zalesski

Prof. Dr. Pavel Zalesski - MAT/UnB (Orientador)

Prof. Dr. Theo Allan Darn Zapata – MAT/UnB (Membro)

Prof. Dr. Ilir Snopche – UFRJ (Membro)

Prof. Dr. John William MacQuarrie- – UFMJ (Membro)

* O autor foi bolsista do CNPq durante a elaboração desta dissertação.

"Tudo tem o seu tempo determinado, e há tempo para todo o propósito debaixo do céu. Há tempo de nascer, e tempo de morrer; tempo de plantar, e tempo de arrancar o que se plantou."
Eclesiastes 3:1–2

Agradecimentos

Inicialmente a Deus, pelo dom da inteligência e pelo discernimento de perseverar no caminho da fé, ouvindo as suas palavras que me alimentou nos momentos alegres e difíceis.

Aos meus pais, Maria Gracelina de Jesus e Israel dos Santos Nery, pela formação moral e ética e por todo o incentivo durante minha vida acadêmica.

A minha esposa, Érica Nery, por me proporcionar o presente de poder compartilhar a sua vida comigo. Durante esse período, você foi minha família, minha amiga e minha melhor conselheira; nos momentos mais difíceis, você me fazia acreditar que esse sonho seria possível. A você, sou grato por cada palavra de incentivo e por toda a compreensão.

Ao meu orientador, professor Pavel Zalesski, por ter me aceitado como seu orientando e por ter me proposto essa linha de pesquisa. Meus sinceros agradecimentos, pelas correções e pelo suporte durante todo o período do doutorado, em especial no último ano, que apesar de estarmos impossibilitados de nos encontrarmos fisicamente, devido a pandemia do coronavírus, esteve sempre disponível virtualmente para sanar minhas dúvidas. Obrigado pela formação e por todo conhecimento proporcionado; com o senhor aprendi a Matemática que não se encontra em livros.

Aos professores do Programa de Pós-Graduação em Matemática da UnB, em especial, aos professores: Aline Pinto, Cristina Acciarri, Daniele Sobrinho, Emerson Melo, Hemar Godinho, Martino Garonzi e Sheila Chagas. Que foram meus professores durante o curso; agradeço por todo o conhecimento proporcionado.

Aos amigos que tive a oportunidade de conhecer, em especial: Elaine Silva, John Freddy, Luiz Gustavo, Marcelo Ribeiro, Nathália Gonçalves e Tulio Santos. Agradeço pela amizade.

Não poderia esquecer da minha sogra, Edna Santana, obrigado pelo apoio e incentivo. Suas visitas em Brasília, me fazia sentir mais perto de casa.

Por fim, agradeço a CAPES e ao CNPq pelo apoio financeiro.

Resumo

Nesta tese, investigamos até que ponto uma variedade plana compacta de dimensão n com grupo de holonomia cíclico de ordem livre de quadrados e um torus bundle, podem ser distinguidos pelos quocientes finitos dos seus respectivos grupos fundamentais. Em particular, exibimos fórmulas e cotas, inferiores e superiores, para a cardinalidade do gênero profinito dos grupos fundamentais de tais variedades.

Palavras-chave: Gênero profinito; Grupos de Bieberbach; Grupos Residualmente Finitos.

Abstract

In this thesis we study the extent to which an n-dimensional compact flat manifold with cyclic holonomy group of square-free order, and a torus bundle, may be distinguished by the finite quotients of its fundamental group. In particular, we display formulas and lower and upper bounds for the cardinality of the profinite genus of the fundamental groups of such manifolds.

Key-Words: Profinite Genus; Bieberbach Groups; Residually Finite Groups.

Notação

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$	conjuntos dos números inteiros, números racionais, números reais
(a, b)	máximo divisor comum de a, b
$a \mid b$, $a \nmid b$	a divide b, a não divide b
$\lvert S \rvert$	cardinalidade do conjunto S
$G \backslash X$	conjunto das órbitas da ação do grupo G no conjunto X
$\lvert G : H \rvert$	índice do subgrupo H no grupo G
$H \leq G$	H é subgrupo de G
$H \cong G$	H é isomorfo a G
$\langle S \rangle$	subgrupo gerado pelo subconjunto S
$\mathrm{Aut}(G), \mathrm{Inn}(G)$	grupo de automorfismos de G, grupo de automorfismos internos de G
$\mathrm{Out}(G)$	$\mathrm{Aut}(G)/\mathrm{Inn}(G)$
$\mathrm{Hom}_R(M, N)$	conjunto dos R-homomorfismos de M para N
$\mathcal{N}_G(H)$	normalizador do subgrupo H no grupo G
$C_G(H)$	centralizador do subgrupo H no grupo G
$A \times B, \prod A_i$	produto direto
$A \oplus B, \bigoplus A_i$	soma direta
$N \rtimes H, N \rtimes_\rho H$	produto semidireto
$\mathrm{GL}(n, \mathbb{Z})$	grupo de todas as matrizes invertíveis $n \times n$ sobre $\mathbb{Z}$
$\mathrm{tr}(A), \det(A)$	traço da matriz A, determinante da matriz A
ζ_m	raiz m-ésima primitiva da unidade
$\Phi_m(.)$	m-ésimo polinômio ciclotômico
$\mathrm{Gal}(F/K), \mathrm{Gal}(\zeta_m)$	grupo de Galois de F sobre K, grupo de Galois de $\mathbb{Q}(\zeta_m)$ sobre $\mathbb{Q}$
RG	anel de grupo de um grupo G sobre um anel R com elemento identidade
$\widehat{G}$	completamento profinito do grupo G

Sumário

Introdução

Nos últimos anos, tem havido um grande interesse em estudar se grupos residualmente finitos ou classes de grupos residualmente finitos, conectados com geometria ou topologia, podem ser distinguidos uns dos outros por seus conjuntos de grupos quocientes finitos.

Em Teoria de Grupos, os primeiros estudos nesta direção são da década de 70, quando Baumslag [Bau74], Stebe [Ste72] e outros encontraram exemplos de grupos finitamente gerados residualmente finitos não isomorfos com o mesmo conjunto de grupos quocientes finitos. A questão geral abordada nesse estudo pode ser formulada como

Questão 1. *Até que ponto um grupo finitamente gerado residualmente finito* Γ *pode ser determinado pelo seu completamento profinito?*

Tal estudo levou a noção de *gênero* $\mathfrak{g}(\Gamma)$, que é o conjunto de classes de isomorfismos de grupos finitamente gerados residualmente finitos com o mesmo conjunto de quocientes finitos que o grupo fixado Γ. Equivalentemente, $\mathfrak{g}(\Gamma)$ denota o conjunto de classes de isomorfismos de grupos finitamente gerados residualmente finitos com o completamento profinito isomorfo ao completamento profinito $\widehat{\Gamma}$ de Γ. Na verdade, o termo gênero foi emprestado da Teoria de Representações Integrais, em que o *gênero* de um $\mathbb{Z}G$-reticulado M, para um grupo finito G, é definido como o conjunto de classes de $\mathbb{Z}G$-reticulados N tais que os $\widehat{\mathbb{Z}}G$-módulos $\widehat{M}$ e $\widehat{N}$ são isomorfos (ver [CR81]).

A maioria dessas pesquisas tem-se concentrado em estabelecer se a cardinalidade $|\mathfrak{g}(\Gamma)|$ do gênero é finito ou igual 1 (ver [GPS79] ou [GS79] por exemplo).

O fluxo recente de pesquisas focou em identificar propriedades importantes de variedades que podem ser identificadas pelo completamento profinito dos seus grupos fundamentais (ver [WZ10, WZ17, Wil19]), ou resultados sobre "rigidez", quando o completamento profinito distingue o grupo fundamental de certas variedades de outros grupos fundamentais dentro desta família de variedades (ver [BCR16, Wil17]) ou resultados sobre "rigidez absoluta", quando o grupo fundamental de certas variedades tem gênero 1 (ver

[BMRS20-a, BMRS20-b]). Para ver mais trabalhos recentes e resultados, os leitores podem consultar [Rei18]. Vale salientar que existem alguns poucos trabalhos onde o número exato (ou estimativa) para a cardinalidade do gênero aparecem (ver dificuldade de tais cálculos em [GZ11, BZ13]).

Um dos objetos de estudo desta tese são as variedades planas compactas X de dimensão n. É bem conhecido que essas variedades são descritas pelos famosos teoremas de Bieberbach (ver [Cha86]), por isso, o grupo fundamental Γ de X é chamado de grupo de Bieberbach. Tais grupos são livres de torção com um subgrupo abeliano maximal normal M de índice finito; o quociente $G = \Gamma/M$, chamado o grupo de holonomia de Γ, é um grupo finito agindo fielmente em M. Note que Γ_d, a imagem inversa completa de um subgrupo H de G de ordem d, sobre a aplicação quociente $\Gamma \to \Gamma/M$, é um grupo de Bieberbach de dimensão n com subgrupo abeliano maximal normal M_d e grupo de holonomia H.

Foi provado recentemente por Piwek, Popović e Wilkes [PPW21] que cada grupo de Bieberbach de dimensão ≤ 4 é determinado pelo seu completamento profinito. Uma vez que não existe uma classificação completa para os grupos de Bieberbach em todas as dimensões, torna-se mais difícil investigar a Questão 1 no caso geral. Assim, faz sentido considerar esse problema para algumas famílias de tais grupos. Por exemplo, no presente trabalho respondemos a Questão 1 para a família dos grupos de Bieberbach de dimensão n com o grupo de holonomia cíclico de ordem livre de quadrados. Mais precisamente, exibimos uma fórmula para a cardinalidade do gênero de um grupo de Bieberbach de dimensão n com o grupo de holonomia cíclico de ordem livre de quadrados.

Vamos estudar primeiro o caso em que o grupo de holonomia tem ordem prima. Denote por $\mathbb{Q}(\zeta_m)$ o corpo ciclotômico gerado pela m-ésima raiz primitiva da unidade ζ_m com anel de inteiros $\mathbb{Z}[\zeta_m]$, por $H(\mathbb{Z}[\zeta_m])$ seu grupo de classes de ideais e por $\mathrm{Gal}(\zeta_m) = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ seu grupo de Galois. O último age naturalmente em $H(\mathbb{Z}[\zeta_m])$.

Teorema A. *Seja Γ um grupo de Bieberbach de dimensão n com grupo de holonomia C_p de ordem prima p.*

(i) Se todos os somandos indecomponíveis do $\mathbb{Z}C_p$-módulo M têm $\mathbb{Z}$-posto $p-1$ exceto um somando trivial de $\mathbb{Z}$-posto 1, então $|\mathfrak{g}(\Gamma)| = |C_2 \backslash H(\mathbb{Z}[\zeta_p])|$, onde C_2 é um grupo de ordem 2 agindo em $H(\mathbb{Z}[\zeta_p])$ por inversão.

(ii) Caso contrário, $|\mathfrak{g}(\Gamma)| = |\mathrm{Gal}(\zeta_p) \backslash H(\mathbb{Z}[\zeta_p])|$. [1]

Definição. *Um $\mathbb{Z}C_p$-módulo M que satisfaz as hipóteses (i) do Teorema A será chamado de **excepcional**.*

[1] O caso (ii) do Teorema A também foi enunciado com um esboço de prova em [GZ11]

Como uma consequência do Teorema A, obtemos o seguinte.

Corolário B. *Seja Γ um grupo de Bieberbach de dimensão n com grupo de holonomia C_p de ordem prima p. Então, $|\mathfrak{g}(\Gamma)| = 1$ se, e somente se, $p \leq 19$.*

Em outras palavras, o Corolário B afirma que todas as variedades planas compactas X de dimensão n com o grupo de holonomia C_p de ordem prima p, são determinadas, dentre todas as variedades planas compactas de dimensão n, pelo completamento profinito dos seus grupos fundamentais se, e somente se, $p \leq 19$. Além disso, usando o teorema de restrição cristalográfica (ver [Hil85]), obtemos o seguinte corolário.

Corolário C. *Seja X uma variedade plana compacta de dimensão n com grupo de holonomia de ordem prima. Se $n \leq 21$, então X é determinada, dentre todas as variedades planas compactas de dimensão n, pelo completamento profinito do seu grupo fundamental.*

Para provar o Teorema A, é suficiente considerar as classes de isomorfismos de grupos de Bieberbach em $\mathfrak{g}(\Gamma)$, porque cada $\Delta \in \mathfrak{g}(\Gamma)$ é um grupo de Bieberbach (ver Proposição 2.1.4). Um resultado importante que usamos para provar o Teorema A é a classificação de Charlap para grupos de Bieberbach com o grupo de holonomia de ordem prima (ver Subseção 1.5.2). Além disso, um fato crucial é a seguinte correspondência que estabelecemos, mostrando que o gênero $\mathfrak{g}(\Gamma)$, em nosso caso, coincide com o gênero do $\mathbb{Z}C_p$-reticulado M (no sentido da Teoria de Representações) no caso (ii) do Teorema A.

Teorema D. *Sejam M um grupo abeliano livre de posto n e C_p um grupo de ordem prima p. Sejam Γ_1 e Γ_2 grupos de Bieberbach de dimensão n que são extensões de M por C_p. Se M_1 e M_2 são $\mathbb{Z}C_p$-módulos induzidos pela ação de Γ_1 e Γ_2 em M, respectivamente, então*

(i) $\Gamma_1 \cong \Gamma_2$ se, e somente se, ou M_1 e M_2 são $\mathbb{Z}C_p$-módulos não excepcionais isomorfos ou M_1 e M_2 são $\mathbb{Z}C_p$-módulos excepcionais e são isomorfos a menos de um automorfismo de C_p por inversão.

(ii) $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$ se, e somente se, $\widehat{M_1} \cong \widehat{M_2}$ como $\widehat{\mathbb{Z}}C_p$-módulos.

Para generalizar o Teorema A para grupos de Bieberbach com grupo de holonomia cíclico $G = C_{p_1} \times \cdots \times C_{p_k}$ de ordem $p_1 p_2 \cdots p_k$, onde p_i $(i = 1, \cdots, k)$ são números primos distintos, precisamos de um pouco mais de terminologia e notação.

Tomemos um $\mathbb{Z}H$-reticulado fiel M de posto n para um grupo finito H (equivalentemente, um homomorfismo injetivo $\rho : H \to \mathrm{GL}(n, \mathbb{Z})$). Seguindo [Hil86], definimos a classe cristalográfica (H, M) como o conjunto de todas as extensões livres de torção Γ de H por M. Dizemos que duas classes cristalográficas (H, M) e (H', M') são aritmeticamente equivalentes se as imersões de H e H' são subgrupos conjugados de $\mathrm{GL}(n, \mathbb{Z})$ (para

mais detalhes ver Subseção 1.5.4). As classes de equivalências resultantes são chamadas de classes cristalográficas aritméticas. Similar à definição de $\mathfrak{g}(\Gamma)$, denotamos por $\mathcal{C}(M)$ o conjunto de classes de isomorfismos de $\mathbb{Z}H$-reticulados N, que correspondem às classes cristalográficas aritméticas (H, N), tais que os $\widehat{\mathbb{Z}}H$-módulos $\widehat{N}$ e $\widehat{M}$ são isomorfos.

Seja Γ um grupo de Bieberbach de dimensão n com subgrupo abeliano maximal normal M e grupo de holonomia cíclico $G = C_{p_1} \times \cdots \times C_{p_k}$, onde C_{p_i} é um grupo cíclico de ordem prima p_i e $\delta := p_1 p_2 \cdots p_k$ é livre de quadrados. Note que para calcular a cardinalidade do gênero $\mathfrak{g}(\Gamma)$, neste caso, temos que calcular o número de classes de isomorfismos de grupos de Bieberbach na classe cristalográfica (G, M) e a cardinalidade de $\mathcal{C}(M)$, que corresponde ao número de classes cristalográficas a menos de equivalência. Para este propósito, vamos dividir o estudo em dois casos: excepcional e não excepcional, de acordo com a seguinte definição.

Definição. *Diremos que o grupo de Bieberbach Γ é **excepcional**, se existe um primo p dividindo δ tal que o subgrupo de Bieberbach Γ_p de Γ tem $\mathbb{Z}C_p$-módulo correspondente M_p excepcional. Denotaremos por D o conjunto de tais números primos.*

Usando que

$$\mathrm{Gal}(\zeta_\delta) \cong \mathrm{Gal}(\zeta_{p_1}) \times \cdots \times \mathrm{Gal}(\zeta_{p_k}), \tag{1}$$

(ver [DF04, §14.5, Cor. 27]) definimos o grupo $\mathcal{H}_D$ como

$$\mathrm{Gal}(\zeta_{p_1}) \times \cdots \times \mathrm{Gal}(\zeta_{p_{i-1}}) \times C_2 \times \mathrm{Gal}(\zeta_{p_{i+1}}) \times \cdots \times \mathrm{Gal}(\zeta_{p_k})$$

se $p_i \in D$.

Com esta notação, obtemos a seguinte fórmula para $|\mathcal{C}(M)|$.

Teorema E. *Seja Γ um grupo de Bieberbach de dimensão n com subgrupo abeliano maximal normal M e grupo de holonomia cíclico G de ordem livre de quadrados δ. Se Γ é excepcional, então*

$$|\mathcal{C}(M)| = \left| \mathcal{H}_D \backslash \prod_{d|\delta} H(\mathbb{Z}[\zeta_d]) \right|.$$

Caso contrário,

$$|\mathcal{C}(M)| = \left| \mathrm{Gal}(\zeta_\delta) \backslash \prod_{d|\delta} H(\mathbb{Z}[\zeta_d]) \right|.$$

Seja M um $\mathbb{Z}C_p$-reticulado (para um grupo cíclico $C_p = \langle x \rangle$ de ordem prima p). Então, M pode ser escrito na forma $M = M_1 \oplus M_2$, onde M_1 é o maior somando direto de M em que C_p age trivialmente. Para um elemento $n \in \mathcal{N}_{\mathrm{Aut}(M)}(C_p)$, denotemos por $\tilde{n}$ um

automorfismo de C_p induzido pela conjugação de n em C_p, em outras palavras, $\tilde{n}$ é a imagem natural de n em $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ sobre a identificação $\mathrm{Aut}(C_p) \cong \mathbb{F}_p^*$.

Agora, no que segue a "barra" denota a redução módulo p. O normalizador $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ age de forma natural no conjunto dos elementos fixados M^{C_p} sobre a ação de C_p em M. Isto induz a ação de $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ em $\bar{M}^{C_p}$ e, consequentemente, $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ age em $\bar{M}^{C_p}/\Delta \cdot \bar{M} \cong \bar{M}_1$, onde $\Delta = 1 + x + \cdots + x^{p-1}$ (ver [Cha86, p. 168] para mais detalhes).

Definimos uma nova ação "$\bullet$" do normalizador $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ em $\bar{M}_1$ por

$$n \bullet m := n \cdot \widetilde{n} m, \quad (m \in \bar{M}_1) \tag{2}$$

onde "$\cdot$" denota a ação de $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ em $\bar{M}_1$ descrita no parágrafo anterior. Uma vez que, para cada primo p dividindo $|G|$, o normalizador $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ é um subgrupo de $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$, o normalizador $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ também age em M_1/pM_1 e, consequentemente, $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ age em $(M_1/pM_1)^{G/C_p} = (M_1/pM_1)^G$.

Denotamos $\bar{M}_1^* = \bar{M}_1 \setminus \{0\}$ e afirmamos o seguinte:

Teorema F. *Seja Γ um grupo de Bieberbach de dimensão n com subgrupo abeliano maximal normal M e grupo de holonomia cíclico G de ordem livre de quadrados δ. Então,*

$$|\mathfrak{g}(\Gamma)| = \sum_{M \in T} \left(\prod_{p|\delta} |\mathcal{N}_{\mathrm{Aut}(M)}(G) \backslash (\bar{M}_{1,p}^*)^G| \right),$$

onde T é um conjunto de representantes das classes de isomorfismos dos $\mathbb{Z}G$-reticulados em $\mathcal{C}(M)$ e $M_{1,p}$ é o maior somando direto de M em que C_p age trivialmente.

Corolário G. *Tem-se*

$$|\mathfrak{g}(\Gamma)| \leq |H(\mathbb{Z}[\zeta_\delta])|^a max_{p|\delta}\{|(\bar{M}_{1,p}^*)^G|^b\},$$

onde $max_{p|\delta}\{|(\bar{M}_{1,p}^*)^G|^b\}$ representa a maior cardinalidade dos conjuntos $(\bar{M}_{1,p}^*)^G$ elevado a b-ésima potência para todo $p \mid \delta$, a é o número de divisores de δ e b é o número de divisores primos de δ.

Corolário H. *Se Γ é um grupo de Bieberbach excepcional, então*

$$|\mathfrak{g}(\Gamma)| = \sum_{M \in T} \left(\prod_{p \in D} |\mathcal{N}_{\mathrm{Aut}(M)}(G) \backslash \mathbb{F}_p^*| \prod_{\substack{q|\delta \\ q \notin D}} |\mathcal{N}_{\mathrm{Aut}(M)}(G) \backslash (\bar{M}_{1,q}^*)^G| \right).$$

Além disso, podemos deduzir o Teorema A como um Corolário do Teorema F, uma vez que o normalizador $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ age transitivamente em $\bar{M}_1^*$ (ver Lema 1.5.33).

Em particular, temos o seguinte resultado.

Teorema I. *Seja Γ um grupo de Bieberbach de dimensão n com grupo de holonomia cíclico de ordem igual a $6, 10$ ou 14. Então, $|\mathfrak{g}(\Gamma)| = 1$.*

Finalizamos esta tese investigando a Questão 1 para variedades tridimensionais orientáveis compactas. Para sermos mais precisos em nossa explanação, reformulamos a Questão 1 para este caso particular.

Questão 2. *Seja X uma variedade tridimensional orientável compacta. Até que ponto o grupo fundamental $\pi_1(X)$ de X é determinado pelo seu completamento profinito?*

Thurston, em 1982, conjecturou que existem apenas oito modelos de geometrias tridimensionais, que são: $\mathbf{E}^3$, $\mathbf{H}^3$, $\mathbf{S}^3$, $\mathbf{S}^2 \times \mathbb{R}$, $\mathbf{H}^2 \times \mathbb{R}$, $\widetilde{\mathbf{SL}_2}(\mathbb{R})$, **Nil** e **Sol**; isto foi provado por Perelman em 2003 (ver [Sco83] para mais detalhes). Na última década deste século, Wilton e Zalesskii [WZ17, WZ19] provaram que a geometria de uma variedade tridimensional orientável compacta é determinada pelo completamento profinito do seu grupo fundamental. Devido a este resultado, para investigar a Questão 2 é suficiente considerar a variedade X modelada em uma das oito geometrias.

Em [Wil17, Wil18], Wilkes apresenta uma resposta completa para a Questão 2 para a família de variedades tridimensionais modeladas nas geometrias $\mathbf{S}^3$, $\mathbf{E}^3$, $\mathbf{S}^2 \times \mathbb{R}$, $\widetilde{\mathbf{SL}_2}(\mathbb{R})$ e **Nil**. Mais precisamente, ele provou que qualquer variedade tridimensional orientável compacta modelada em uma destas geometrias é determinada pelo completamento profinito do seu grupo fundamental. Em geral, não sabemos se variedades tridimensionais modeladas na geometria $\mathbf{H}^3$ são profinitamente rígidas, entretanto, Liu [Liu20] mostrou que o gênero do grupo fundamental de uma variedade tridimensional hiperbólica orientável de volume finito tem cardinalidade finita. Além disso, existe um estudo de Bridson, McReynolds, Reid e Spitler [BMRS20-a] que exibe exemplos de variedades tridimensionais hiperbólicas que são absolutamente rígidas. Em contraste, existem exemplos de variedades tridimensionais modeladas nas geometrias $\mathbf{H}^2 \times \mathbb{R}$ (construído por Hempel [Hem14]) e **Sol** (construído por Funar [Fun13]) que não são profinitamente rígidas. Chamaremos as variedades tridimensionais modeladas na geometria **Sol** de **Sol**-variedades (**Nil** de **Nil**-variedades, e assim por diante).

Apesar de sabermos que as **Sol**-variedades não são profinitamente rígidas, até o momento, não existe uma resposta completa para a Questão 2 para essa família de variedades. Em relação a isto, Wilton e Zalesskii [WZ19] destacam que um tratamento definitivo da

Questão 2 para **Sol**-variedades seria um acréscimo valioso à literatura. Neste sentido, fizemos um estudo da Questão 2 para uma família de **Sol**-variedades.

Se X é uma **Sol**-variedade, então $\pi_1(X) \cong \mathbb{Z}^2 \rtimes_A \mathbb{Z}$, onde A é uma matriz em $\mathrm{GL}(2,\mathbb{Z})$ tal que nenhum de seus autovalores tem valor absoluto igual a 1 (ou seja, A é uma matriz hiperbólica) (ver [Sco83] ou [JKM08, Lem. 2.6]). Rigorosamente, **Sol**-variedades são torus bundles (ou seja, suspensões de um homeomorfismo linear do toro), em particular, temos a seguinte caracterização. Seja X um torus bundle e denotemos por $\mathrm{tr}(A)$ o traço de A.

(i) Se $|\mathrm{tr}(A)| > 2$, então A é hiperbólica e X é uma **Sol**-variedade.

(ii) Se A tem ordem finita, então X é uma $\mathbf{E}^3$-variedade.

(iii) Se $|\mathrm{tr}(A)| \leq 2$, então ou A tem ordem finita, de modo que X é uma $\mathbf{E}^3$-variedade, ou A tem ordem infinita e X é uma **Nil**-variedade, ou A é hiperbólica e X é uma **Sol**-variedade.

(Cf. [Sco83, Thm. 5.5]). À luz dos resultados de Wilton e Zalesskii [WZ17, WZ19], refinamos a nossa definição de gênero para a seguinte: $\tilde{\mathfrak{g}}(\pi_1(X))$ denota o conjunto de classes de isomorfismos de grupos fundamentais de variedades tridimensionais orientáveis compactas, com o completamento profinito isomorfo a $\widehat{\pi_1(X)}$.

Em nosso estudo da Questão 2, iniciamos com o caso em que $\mathbb{Z}^2 \rtimes_A \mathbb{Z}$ é nilpotente.

Teorema J. *Seja $A \in \mathrm{GL}(2,\mathbb{Z})$ e considere o produto semidireto $G_A = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$. Se todos os autovalores de A são iguais a 1, então $|\tilde{\mathfrak{g}}(G_A)| = 1$.*

Para o caso em que $\mathbb{Z}^2 \rtimes_A \mathbb{Z}$ não é nilpotente, estabelecemos cotas inferiores e superiores para a cardinalidade de $\tilde{\mathfrak{g}}(\pi_1(X))$, em função do número de classes de ideais da ordem $\mathbb{Z}[\lambda]$, onde λ é um autovalor da matriz A. Para isso, usamos um famoso Teorema de Latimer e MacDuffee [New72, Thm. III. 13] que diz que, existe uma correspondência biunívoca entre as classes de conjugação de matriz n-por-n sobre $\mathbb{Z}$, com mesmo polinômio característico f, e as classes de ideais da ordem $\mathbb{Z}[\lambda]$, onde λ é uma raiz de f. Precisamente, obtemos o seguinte:

Teorema K. *Seja $A \in \mathrm{GL}(2,\mathbb{Z})$ e considere o produto semidireto $G_A = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$. Seja λ um autovalor de A. Então,*

(i) se A tem todos os seus autovalores distintos, $\mathrm{tr}(A) \neq 0$ e a classe de conjugação de

A corresponde para uma classe de ideais invertíveis da ordem $\mathbb{Z}[\lambda]$*, então*

$$\begin{cases} h(\mathbb{Z}[\lambda]) \leq |\tilde{\mathfrak{g}}(G_A)| \leq \tilde{h}(\lambda), & \text{se } \det(A) = -1 \\ h(\mathbb{Z}[\lambda])/2 \leq |\tilde{\mathfrak{g}}(G_A)| \leq \tilde{h}(\lambda), & \text{se } \det(A) = 1 \end{cases}$$

onde $h(\mathbb{Z}[\lambda])$ *é a ordem do grupo de classes de ideais e* $\tilde{h}(\lambda)$ *é o número de classes de ideais de* $\mathbb{Z}[\lambda]$*.*

(ii) *se* $\mathrm{tr}(A) = 0$ *ou* A *tem todos os seus autovalores iguais a* -1*, então*

$$|\tilde{\mathfrak{g}}(G_A)| = h(\mathbb{Z}[\lambda]) = 1.$$

Corolário L. *Seja* $A \in \mathrm{GL}(2,\mathbb{Z})$ *com* $\det(A) = -1$ *e considere o produto semidireto* $G_A = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$*. Se* $\mathrm{tr}(A)^2 - 4\det(A)$ *é livre de quadrados, então* $|\tilde{\mathfrak{g}}(G_A)| = h(\mathbb{Z}[\lambda])$ *onde* λ *é um autovalor de* A*.*

Corolário M. *Seja* A *uma matriz em* $\mathrm{GL}(2,\mathbb{Z})$*, como no Teorema K ou Teorema J, com autovalor* λ*. Se* $\tilde{h}(\lambda) = 1$*, então o torus bundle* X_A *é determinado, dentre as variedades tridimensionais, pelo completamento profinito do seu grupo fundamental.*

Observe que o Corolário M nos diz que existe uma família de torus bundles modelados com a geometria **Sol** que são determinados pelo completamento profinito dos seus grupos fundamentais. Combinando o Corolário M com a seguinte conjectura de Gauss – que ainda está em aberto – vemos que tal família pode ser infinita.

Conjectura (Gauss, 1801)**.** *Existem infinitos corpos quadráticos reais com número de classes um.*

A seguir, descrevemos a organização desta tese. No Capítulo 1, que denominamos de Preliminares, apresentamos um resumo das principais teorias que usamos para provar os nossos resultados.

No Capítulo 2, a Seção 2.1 contém algumas propriedades sobre o completamento profinito de um grupo de Bieberbach. Na Seção 2.2, iniciamos a nossa investigação da Questão 1 para a família dos grupos de Bieberbach com o grupo de holonomia de ordem prima. Nesta seção, provamos os Teoremas A e D e os Corolários B e C. Na Seção 2.3, generalizamos os resultados da Seção 2.2 para a família de grupos de Bieberbach com o grupo de holonomia cíclico de ordem livre de quadrados. Esta seção contém as provas dos Teoremas E, F e I e dos Corolários G e H.

No Capítulo 3, investigamos a Questão 2 para as **Sol**-variedades. Para esse fim, provamos os Teoremas J e K e os Corolários L e M.

Por fim, no Capítulo 4, apresentamos as nossas considerações finais.

Capítulo

1

Preliminares

Neste capítulo apresentamos os principais conceitos e resultados que serão úteis para o bom desenvolvimento do nosso trabalho. Vale salientar que, assumimos como conhecido algumas definições básicas e alguns resultados clássicos das Teorias de Grupos, Módulos, Topologia Geral e da Teoria dos Números.

Na Seção 1.1, definimos completamento profinito de um grupo abstrato e apresentamos algumas propriedades do completamento profinito de um grupo finitamente gerado residualmente finito. Para isso, usamos o livro de Ribes-Zalesskii [RZ00] como principal referência.

Na Seção 1.2, reunimos os principais resultados da Teoria dos Números que serão usados aqui e definimos o Grupo de Galois. As principais referências usadas na construção dessa seção formam os livros de Neukirch [Neu99] e Dummit-Foote [DF04].

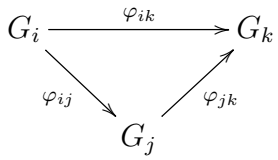
Seção 1.3 contém as descrições das extensões de módulos e de grupos. O livro do Rotman [Rot09] foi a principal referência usada aqui.

Na Seção 1.4, apresentamos as classificações de $\mathbb{Z}G$-reticulados sobre grupos G cíclicos de ordem prima (feita por Diederichsen e Reiner [CR62]) e cíclicos de ordem livre de quadrados (feita por Oppenheim [Opp62]).

Por fim, a Seção 1.5 contém a definição de grupos de Bieberbach e os métodos de classificação de Charlap [Cha65, Cha86], Auslander-Vasquez [Vas70] e a descrição via classes cristalográficas [Hil86].

1.1 Grupos profinitos

Um **conjunto dirigido** é um conjunto não vazio parcialmente ordenado $I = (I, \preceq)$ tal que para cada $i, j \in I$ existe $k \in I$ de modo que $i, j \preceq k$. Um **sistema inverso** de grupos (anéis) topológicos sobre um conjunto dirigido I, consiste em uma coleção $\{G_i : i \in I\}$ de grupos (anéis) topológicos e uma coleção de homomorfismos de grupos (anéis) contínuos $\varphi_{ij} : G_i \to G_j$, definidos sempre que $i \succeq j$, tal que os diagramas da forma



comutam sempre que $i, j, k \in I$ e $i \succeq j \succeq k$. Denotamos o sistema inverso por $\{G_i, \varphi_{ij}, I\}$. O **limite inverso** do sistema inverso $\{G_i, \varphi_{ij}, I\}$ é o conjunto

$$\varprojlim_{i \in I} G_i = \left\{ (x_i) \in \prod_{i \in I} G_i : \varphi_{ij}(x_i) = x_j, \text{ sempre que } i \succeq j \right\}.$$

Proposição 1.1.1 ([RZ00], Prop. 1.1.3)**.** *Se $\{G_i, \varphi_{ij}, I\}$ é um sistema inverso de grupos (anéis) topológicos compactos, Hausdorff e totalmente desconexos, então*

$$\varprojlim_{i \in I} G_i$$

é também um grupo (anel) topológico compacto, Hausdorff e totalmente desconexo.

Definição 1.1.2. *Um grupo Γ é um **grupo profinito** se é um limite inverso $\varprojlim \Gamma_i$ de grupos finitos, onde cada Γ_i está munido com a topologia discreta.*

Exemplo 1.1.3. *1. Qualquer grupo finito é naturalmente um grupo profinito.*

2. ***(Completamentos)** Seja Γ um grupo e considere o conjunto $\mathcal{N}$ de todos os subgrupos normais de índice finito de Γ. Note que, $\mathcal{N}$ é não vazio, pois $\Gamma \in \mathcal{N}$. Além disso, é imediato verificar que $\mathcal{N}$ é um conjunto dirigido com a ordem:*

$$M \preceq N \text{ se, e somente se, } N \subseteq M \text{ para } N, M \in \mathcal{N}.$$

Se $M, N \in \mathcal{N}$ e $N \succeq M$, seja $\varphi_{NM} : \Gamma/N \to \Gamma/M$ o epimorfismo natural. Então,

$\{\Gamma/N, \varphi_{NM}, \mathcal{N}\}$ *é um sistema inverso e o grupo*

$$\widehat{\Gamma} := \varprojlim_{N\in\mathcal{N}} \Gamma/N \tag{1.1}$$

é profinito. O grupo $\widehat{\Gamma}$ *é chamado o* ***completamento profinito*** *de* Γ*. Agora, se* p *é um número primo e* $\mathcal{N}$ *é o conjunto formado por todos os subgrupos normais de índice finito igual a uma potência de* p*, diremos que o grupo profinito em* (1.1) *é o* ***completamento pro-****p de* Γ*.*

3. *Como um caso especial de (2), considere o anel de inteiros* $\mathbb{Z}$*. Neste caso,*

$$\widehat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$$

é o completamento profinito de $\mathbb{Z}$ *e*

$$\mathbf{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

o completamento pro-p *de* $\mathbb{Z}$*.*

Note que, existe uma aplicação natural $\iota : \Gamma \to \widehat{\Gamma}$ definida por $g \mapsto (gN)$ e que, ι é injetiva se, e somente se, a interseção de todos os subgrupos normais de índice finito de Γ é trivial; neste caso, Γ é dito ser **residualmente finito**.

Proposição 1.1.4 ([Neu99], Prop. 2.4)**.** *Seja* p *um número primo. Então,*

1. $\mathbf{Z}_p$ *é um domínio de ideais principais com um único ideal maximal não nulo, a saber,* $p\mathbf{Z}_p$*.*

2. *A aplicação natural*

$$\iota : \mathbf{Z}_p \to \varprojlim_{n\in\mathbb{N}} \mathbf{Z}_p/p^n\mathbf{Z}_p$$

é um isomorfismo.

Em outras palavras, $\mathbf{Z}_p$ *é um domínio local noetheriano completo.*

Para produto semidireto, vale o seguinte:

Proposição 1.1.5 ([GZ11], Prop. 2.6)**.** *Sejam* N, H *grupos finitamente gerados residualmente finitos e* $\rho : H \to \mathrm{Aut}(N)$ *um homomorfismo. Então,* ρ *induz um homomorfismo* $\widehat{\rho} : \widehat{H} \to \mathrm{Aut}(\widehat{N})$ *e as imersões* $N \to \widehat{N}$ *e* $H \to \widehat{H}$ *induzem um isomorfismo*

$$\widehat{N \rtimes_\rho H} \cong \widehat{N} \rtimes_{\widehat{\rho}} \widehat{H}$$

de grupos profinitos.

Definição 1.1.6. *A **topologia profinita** sobre um grupo Γ é a topologia em Γ em que uma base para os conjuntos abertos é o conjunto de todas as classes laterais de subgrupos normais de índice finito em Γ.*

Sejam Γ um grupo topológico e H um subgrupo de Γ. Então, escreveremos $H \leq_\circ \Gamma$ e $H \leq_f \Gamma$ para indicar que H é um subgrupo aberto de Γ e H é um subgrupo de índice finito de Γ, respectivamente.

A seguinte proposição estabelece uma importante conexão entre os espaços discretos e profinitos.

Proposição 1.1.7 ([RZ00], Prop. 3.2.2 e Cor. 1.1.8)**.** *Seja Γ um grupo finitamente gerado residualmente finito. Identifique Γ com sua imagem em $\widehat{\Gamma}$ e denote por $\bar{X}$ o fecho em $\widehat{\Gamma}$ de um subconjunto X de Γ. Então, existe uma bijeção*

$$\{H \leq_f \Gamma\} \to \{U \leq_\circ \widehat{\Gamma}\}$$

$$H \mapsto \bar{H}$$

$$U \cap \Gamma \hookleftarrow U$$

Além disso, se $H, K \leq_f \Gamma$ com $H \leq K$, então

(a) $H \lhd K$ se, e somente se, $\bar{H} \lhd \bar{K}$.

(b) $|K : H| = |\bar{K} : \bar{H}|$.

(c) Se $H \lhd K$, então $K/H \cong \bar{K}/\bar{H}$.

(d) $\bar{H} \cong \widehat{H}$.

Demonstração. conteúdo... □

Vamos denotar por $\mathfrak{F}(\Gamma)$ o conjunto dos quocientes finitos de um grupo Γ. A próxima proposição é basicamente provada em [DFPR82, p. 227], entretanto, usamos [NS07, Thm. 1.1] para substituir "isomorfismo topológico" por "isomorfismo".

Proposição 1.1.8. *Sejam Γ_1 e Γ_2 grupos finitamente gerados. Então, $\widehat{\Gamma}_1$ e $\widehat{\Gamma}_2$ são grupos isomorfos se, e somente se, $\mathfrak{F}(\Gamma_1) = \mathfrak{F}(\Gamma_2)$.*

Isto nos permite enunciar a seguinte versão do Teorema de Grunewald e Scharlau.

Proposição 1.1.9 ([GS79], Prop. E)**.** *Sejam Γ_1 e Γ_2 grupos finitamente gerados, livres de torção, nilpotentes de classe 2, tais que o número de Hirsch* [1] *de Γ_1 é menor do que ou igual a 5 e $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$. Então, $\Gamma_1 \cong \Gamma_2$.*

Para qualquer grupo Γ escrevemos $tor(\Gamma)$ para o conjunto dos elementos de torção de Γ.

Proposição 1.1.10 ([RZ00], Thm. 4.7.10)**.** *Seja Γ um grupo finitamente gerado tendo um subgrupo normal abeliano com quociente nilpotente. Então, $\overline{tor(\Gamma)} = tor(\widehat{\Gamma})$.*

1.2 Grupos de Galois e classes de ideais

1.2.1 Extensões algébricas de Corpos

Um **corpo de números algébricos** é uma extensão de corpos K de $\mathbb{Q}$ com **grau** $(K : \mathbb{Q})$ finito, isto é, a dimensão de K como espaço vetorial sobre $\mathbb{Q}$ é finita. Os elementos de K são chamados **números algébricos**. Um número algébrico é chamado **inteiro algébrico** se é uma raiz de um polinômio mônico $f(x) \in \mathbb{Z}[x]$. O conjunto $\mathcal{O}_K$ de todos os inteiros algébricos forma um anel contendo $\mathbb{Z}$ (Cf. [Neu99, §2]).

Definição 1.2.1. *Uma extensão algébrica K/F é uma **extensão de Galois** se satisfaz as seguintes condições:*

*(i) K/F é uma **extensão normal**: qualquer polinômio irredutível de $F[x]$ com uma raiz em K pode ser decomposto em polinômios de grau 1 em $K[x]$.*

*(ii) K/F é uma **extensão separável**: qualquer polinômio irredutível de $F[x]$ não tem raízes múltiplas no seu corpo de decomposição* [2] *sobre F.*

Seja K/F uma extensão. Um **F-automorfismo** de K é um isomorfismo de anéis $f : K \to K$ tal que $f(u) = u$ para todo $u \in F$. Não é difícil provar que o conjunto $\mathrm{Aut}(K/F)$ de todos os F-automorfismos de K é um subgrupo de $\mathrm{Aut}(K)$.

Definição 1.2.2. *O grupo $\mathrm{Aut}(K/F)$ de todos os F-automorfismos de K de uma extensão de Galois K/F é chamado o **grupo de Galois** de K sobre F. Neste caso, escreveremos $\mathrm{Gal}(K/F)$ em vez de $\mathrm{Aut}(K/F)$.*

[1] Isto é, o número de quocientes cíclicos infinito em uma série com quocientes cíclicos ou finitos.

[2] O corpo de decomposição de um polinômio $f(x) \in F[x]$ é a menor extensão de corpos K/F em que $f(x)$ se decompõem em fatores lineares.

Proposição 1.2.3 ([DF04], §14.1, Prop. 5)**.** *Seja E o corpo de decomposição sobre F do polinômio $f(x) \in F[x]$. Então,*

$$|\mathrm{Aut}(E/F)| \leq (E : F),$$

com igualdade se $f(x)$ é separável sobre F, isto é, se f não tem raízes múltiplas em E.

A seguir, veremos dois exemplos de extensões de corpos que serão objetos de estudo desta tese.

Extensões quadráticas

Um **corpo quadrático** é uma extensão K de $\mathbb{Q}$ tal que $(K : \mathbb{Q}) = 2$.

Proposição 1.2.4 ([AW04], Thm. 5.4.1)**.** *Seja K um corpo quadrático. Então, existe um único inteiro livre de quadrados m tal que $K = \mathbb{Q}(\sqrt{m})$.*

O anel de inteiros algébricos de um corpo quadrático é calculado a seguir.

Proposição 1.2.5 ([AW04], Thm. 5.4.2)**.** *Seja K um corpo quadrático. Seja m o único inteiro livre de quadrados tal que $K = \mathbb{Q}(\sqrt{m})$. Então, o anel de inteiros algébricos de K é dado por*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m}, & \text{se } m \not\equiv 1 \pmod 4, \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right), & \text{se } m \equiv 1 \pmod 4. \end{cases}$$

Lema 1.2.6. *Seja A uma matriz em $\mathrm{GL}(2,\mathbb{Z})$. Se $\mathrm{tr}(A) \neq 0$ e A tem autovalores distintos λ_1 e λ_2, então $\mathbb{Q}(\lambda_1, \lambda_2)$ é um corpo quadrático.*

Demonstração. Seja $A \in \mathrm{GL}(2,\mathbb{Z})$. É fácil ver que o polinômio característico de A tem a forma $p(x) = x^2 - \mathrm{tr}(A)x + \det(A)$ e que

$$\lambda_{\pm} = \frac{\mathrm{tr}(A) \pm \sqrt{\mathrm{tr}(A)^2 - 4\det(A)}}{2}$$

são os autovalores de A. Note que, A tem autovalores iguais se, e somente se,

$$\begin{aligned} & \frac{\mathrm{tr}(A) + \sqrt{\mathrm{tr}(A)^2 - 4\det(A)}}{2} = \frac{\mathrm{tr}(A) - \sqrt{\mathrm{tr}(A)^2 - 4\det(A)}}{2} \\ \Leftrightarrow \quad & \sqrt{\mathrm{tr}(A)^2 - 4\det(A)} = -\sqrt{\mathrm{tr}(A)^2 - 4\det(A)} \\ \Leftrightarrow \quad & \mathrm{tr}(A)^2 - 4\det(A) = 0 \\ \Leftrightarrow \quad & \mathrm{tr}(A) = \pm 2 \ \text{ e } \ \det(A) = 1. \end{aligned}$$

Logo, como estamos supondo que $\mathrm{tr}(A) \neq 0$ e que os autovalores de A são distintos, temos que os possíveis valores para o traço e determinante da matriz A são:

(i) $\mathrm{tr}(A) = \pm 1$ e $\det(A) = \pm 1$ ou

(ii) $\mathrm{tr}(A) = \pm 2$ e $\det(A) = -1$ ou

(iii) $|\mathrm{tr}(A)| > 2$ e $\det(A) = \pm 1$.

Os casos (i) e (ii) são elementares. Se A satisfaz (iii), então os autovalores de A são irracionais. De fato, suponha que exista um inteiro k tal que $\mathrm{tr}(A)^2 - 4\det(A) = k^2$. Isto nos dá que $\mathrm{tr}(A)^2 - k^2 = \pm 4$, que implica $k = \mathrm{tr}(A) \pm 1$ e assim $\pm 2\mathrm{tr}(A) - 1 = \pm 4$, que é uma contradição, porque $|\mathrm{tr}(A)| > 2$. Logo, $\mathrm{tr}(A)^2 - 4\det(A) = rm$ onde $r, m \in \mathbb{Z}$ de modo que m é livre de quadrados. Portanto, $K = \mathbb{Q}(\lambda_+, \lambda_-) = \mathbb{Q}(\sqrt{m})$ é um corpo quadrático. □

Definição 1.2.7. *Seja $K/\mathbb{Q}$ um corpo de números algébricos de grau n. Uma* ***ordem*** *de K é um subanel $\mathcal{O}$ do anel de inteiros $\mathcal{O}_K$ de K que contém uma base integral de comprimento n. O anel $\mathcal{O}_K$ é chamado a* ***ordem maximal*** *de K.*

Exemplo 1.2.8. *Seja $A \in \mathrm{GL}(2, \mathbb{Z})$ com autovalores distintos tal que $\mathrm{tr}(A) \neq 0$. Então, $K = \mathbb{Q}(\lambda)$ é um corpo quadrático, onde λ é um autovalor de A. Uma vez que λ é raiz do polinômio $p(x) = x^2 - \mathrm{tr}(A)x + \det(A) \in \mathbb{Z}[x]$, temos que $\mathbb{Z}[\lambda]$ está contido no anel de inteiros $\mathcal{O}_K$ de K. Logo, $\mathbb{Z}[\lambda]$ é uma ordem de K que nem sempre é igual a $\mathcal{O}_K$ (ver Proposição 1.2.5).*

Definição 1.2.9. *Um domínio de integridade que é Noetheriano, integralmente fechado e que cada ideal primo não nulo é maximal é chamado um* ***domínio de Dedekind*** *.*

Proposição 1.2.10 ([DF04], §16.3, Prop. 14 e Cor. 19)**.** *O anel de inteiros $\mathcal{O}_K$ de um corpo de números algébricos K é um domínio de Dedekind. Em particular, se I é um ideal não nulo de $\mathcal{O}_K$, então cada ideal no quociente $\mathcal{O}_K/I$ é um ideal principal.*

Seja $K = \mathbb{Q}(\sqrt{m})$, onde m é um inteiro livre de quadrados. Definimos

$$r := \begin{cases} 1, & \text{se} \quad m \not\equiv 1 \pmod 4 \\ 2, & \text{se} \quad m \equiv 1 \pmod 4 \end{cases}$$

e $\omega_0 := (r - 1 + \sqrt{m})/r$.

Lema 1.2.11 ([JW09], Thm. 4.17)**.** *Se $\mathcal{O}$ é uma ordem de um corpo quadrático K, então $\mathcal{O}$ é um $\mathbb{Z}$-módulo com base $\{1, \omega\}$ onde $\omega := f\omega_0$ para algum $f \in \mathbb{Z}$.*

Assim, $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo com base $\{1, \omega_0\}$ e qualquer ordem $\mathcal{O}$ de K tem índice finito em $\mathcal{O}_K$.

Definição 1.2.12. *O índice $f = |\mathcal{O}_K : \mathcal{O}|$ é chamado o* ***condutor*** *de $\mathcal{O}$.*

Se $\alpha = a + b\sqrt{m}$, definimos o seu **conjugado** $\bar{\alpha}$ como $a - b\sqrt{m}$ e sua **norma** $N(\alpha)$ como $\alpha\bar{\alpha}$.

Proposição 1.2.13 ([JW09], Thm. 4.24)**.** *Seja $\mathcal{O}$ uma ordem de um corpo quadrático K. Então, I é um ideal de $\mathcal{O}$ se, e somente se, I é um $\mathbb{Z}$-módulo com base $\{a, b + c\omega\}$ onde $a, b, c \in \mathbb{Z},\ a > 0,\ c > 0,\ 0 \leq b < a,\ c \mid a,\ c \mid b$ e $ac \mid N(b + c\omega)$.*

Definição 1.2.14. *A* ***norma*** *$N(I)$ de um $\mathcal{O}$-ideal I é o índice $|\mathcal{O} : I|$.*

Lema 1.2.15 ([JW09], Prop. 4.23)**.** *Se I é um $\mathcal{O}$-ideal com $\mathbb{Z}$-base $\{a, b + c\omega\}$, onde $a, b, c \in \mathbb{Z}$ são como em Proposição 1.2.13, então $N(I) = ac$.*

Definição 1.2.16. *Seja K um corpo de números algébricos de grau n. Seja $\omega_1, \cdots, \omega_n$ elementos de K. Sejam $\sigma_i : K \to \mathbb{C}$ $(i = 1, \cdots, n)$ os n monomorfismos distintos. Para $j = 1, \cdots, n$ sejam*

$$\omega_i^{(1)} = \sigma_1(\omega_i) = \omega_i, \omega_i^{(2)} = \sigma_2(\omega_i), \cdots, \omega_i^{(n)} = \sigma_n(\omega_i).$$

Então, o ***discriminante*** *de $\{\omega_1, \cdots, \omega_n\}$ é*

$$\begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \vdots & \vdots & \cdots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2.$$

Proposição 1.2.17 ([AW04], Thm. 7.1.8)**.** *Seja K um corpo de números algébricos de grau n. Seja $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$. Se o discriminante de $\{1, \theta, \cdots, \theta^{n-1}\}$ é livre de quadrados, então $\{1, \theta, \cdots, \theta^{n-1}\}$ é uma $\mathbb{Z}$-base para $\mathcal{O}_K$.*

Lema 1.2.18. *Seja $A \in \mathrm{GL}(2, \mathbb{Z})$ com autovalores distintos. Se $\mathrm{tr}(A)^2 - 4\mathrm{det}(A)$ é livre de quadrados, então $\mathbb{Z}[\lambda] = \mathcal{O}_K$, onde λ é um autovalor de A.*

Demonstração. Note que $\{1, \lambda\}$ é uma $\mathbb{Z}$-base para $\mathbb{Z}[\lambda]$ e que o discriminante de $\{1, \lambda\}$ é

$$\begin{vmatrix} 1 & \frac{\mathrm{tr}(A)+\sqrt{D}}{2} \\ 1 & \frac{\mathrm{tr}(A)-\sqrt{D}}{2} \end{vmatrix}^2 = D,$$

onde $D = \mathrm{tr}(A)^2 - 4\det(A)$. Como D é livre de quadrados, segue pela Proposição 1.2.17 que $\{1, \lambda\}$ é uma $\mathbb{Z}$-base para o anel de inteiros $\mathcal{O}_K$. Portanto, $\mathbb{Z}[\lambda] = \mathcal{O}_K$. □

Extensões ciclotômicas

Seja n um número natural. O **n-ésimo corpo ciclotômico** é uma extensão $\mathbb{Q}(\zeta_n)$ de $\mathbb{Q}$, onde ζ_n é uma raiz n-ésima primitiva da unidade.

Definição 1.2.19. *Seja m um número natural. A **função totiente de Euler** $\varphi(m)$ é definida como o número de naturais menor ou igual a m que são relativamente primos para m.*

Definição 1.2.20. *O **n-ésimo polinômio ciclotômico** é o polinômio $\Phi_n(x)$ cujas raízes são n-ésimas raízes primitivas da unidade:*

$$\Phi_n(x) = \prod_{\substack{1 \le a < n \\ (a,n)=1}} (x - \zeta_n^a).$$

(que tem grau $\varphi(n)$).

O anel de inteiros de $\mathbb{Q}(\zeta_n)$ é determinado explicitamente como segue.

Proposição 1.2.21 ([Neu99], Prop. 10.2)**.** *Uma $\mathbb{Z}$-base do anel $\mathcal{O}_K$ de inteiros de $K = \mathbb{Q}(\zeta_n)$ é dada por $1, \zeta_n, \cdots, \zeta_n^{d-1}$, com $d = \varphi(n)$, em outras palavras,*

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\zeta_n + \cdots + \mathbb{Z}\zeta_n^{d-1} = \mathbb{Z}[\zeta_n].$$

A extensão $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ é uma extensão de Galois e seu grupo de Galois é descrito a seguir.

Proposição 1.2.22 ([DF04], §14.5, Thm. 26)**.** *O grupo $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ é isomorfo ao grupo multiplicativo $(\mathbb{Z}/n\mathbb{Z})^\times$ das unidades do anel $\mathbb{Z}/n\mathbb{Z}$. O isomorfismo é dado explicitamente pela aplicação*

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

$$a \pmod n \mapsto \sigma_a$$

onde σ_a é um automorfismo definido por $\sigma_a(\zeta_n) = \zeta_n^a$.

Assim, o grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ é abeliano e, em particular, admite a seguinte decomposição em soma direta.

Proposição 1.2.23 ([DF04], §14.5, Cor. 27)**.** *Seja $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ a decomposição de um inteiro positivo n em potências de primos distintos. Então,*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{a_1}})/\mathbb{Q}) \oplus \cdots \oplus \mathrm{Gal}(\mathbb{Q}(\zeta_{p_k^{a_k}})/\mathbb{Q}).$$

1.2.2 O Grupo de classes de ideais

Assim como para números diferentes de zero, podemos obter inversos para alguns ideais não nulos de uma ordem $\mathcal{O}$, introduzindo a noção de ideal fracionário no corpo de frações K.

Definição 1.2.24. *Um **ideal fracionário** de $\mathcal{O}$ é um $\mathcal{O}$-submódulo $I \neq 0$ de K tal que $dI \subseteq \mathcal{O}$ para algum $d \in \mathcal{O}$ não nulo.*

Assim, cada ideal (usual) de $\mathcal{O}$ é também um ideal fracionário (pegue $d = 1$). Caso seja necessária a distinção, os ideais usuais de $\mathcal{O}$ serão chamados de **ideais integrais**.

Para qualquer $a \in K \setminus \{0\}$, o $\mathcal{O}$-módulo $a\mathcal{O} = (a) = \{ax : x \in \mathcal{O}\}$ é chamado o **ideal principal fracionário** gerado por a.

Definição 1.2.25. *Dizemos que dois $\mathcal{O}$-ideais fracionários I e J são **equivalentes** ($I \sim J$), se existe $\alpha \in K \setminus \{0\}$ tal que $I = \alpha J$.*

É imediato ver que essa equivalência é reflexiva, simétrica e transitiva. Assim, podemos particionar o conjunto de ideais fracionários em **classes de ideais** com respeito a essa relação de equivalência.

Proposição 1.2.26 ([CR62], Thm. 20.6)**.** *O número de classes de $\mathcal{O}$-ideais fracionários é finito.*

Definição 1.2.27. *Um $\mathcal{O}$-ideal fracionário I é **invertível** se existe um outro $\mathcal{O}$-ideal fracionário J tal que $IJ = \alpha\mathcal{O}$ onde $\alpha \in \mathcal{O}$.*

Vale a multiplicatividade da norma de ideais invertíveis.

Proposição 1.2.28 ([JW09], Thm. 4.36)**.** *Se I e J são $\mathcal{O}$-ideais invertíveis, então IJ é invertível e $N(IJ) = N(I)N(J)$.*

Lema 1.2.29. *Seja $\mathcal{O}$ uma ordem de um corpo quadrático K. Se I é um $\mathcal{O}$-ideal invertível, então $|I/mI| = |\mathcal{O}/m\mathcal{O}|$ para cada inteiro positivo m.*

Demonstração. Para cada $m \in \mathbb{N}$, temos que $mI \subseteq I \subseteq \mathcal{O}$. Então,

$$\left|\frac{\mathcal{O}}{mI}\right| = \left|\frac{\mathcal{O}}{I}\right| \left|\frac{I}{mI}\right|.$$

Logo,

$$\left|\frac{I}{mI}\right| = \frac{|\mathcal{O}/mI|}{|\mathcal{O}/I|}. \tag{1.2}$$

Como $mI = m\mathcal{O}I$, segue pela Proposição 1.2.28 que

$$\left|\frac{\mathcal{O}}{mI}\right| = N(mI) = N(m\mathcal{O})N(I) = \left|\frac{\mathcal{O}}{m\mathcal{O}}\right| \left|\frac{\mathcal{O}}{I}\right|. \tag{1.3}$$

Substituindo equação (1.3) em equação (1.2), obtemos

$$\left|\frac{I}{mI}\right| = \left|\frac{\mathcal{O}}{m\mathcal{O}}\right|.$$

□

Proposição 1.2.30 ([Neu99], §12)**.** *Seja $\mathcal{O}$ uma ordem de um corpo de números algébricos K de grau n. Então, o conjunto dos $\mathcal{O}$-ideais fracionários invertíveis forma um grupo abeliano, o* ***grupo de ideais*** *$I(\mathcal{O})$. O elemento identidade é $(1) = \mathcal{O}$ e o inverso de I é*

$$I^{-1} = \{x \in K : xI \subseteq \mathcal{O}\}.$$

Além disso, o conjunto $P(\mathcal{O})$ dos $\mathcal{O}$-ideais principais fracionários não nulos é um subgrupo de $I(\mathcal{O})$.

Definição 1.2.31. *O grupo quociente $I(\mathcal{O})/P(\mathcal{O})$ é chamado de* ***grupo de classes de ideais*** *(ou* ***grupo de Picard****) de K e é denotado por $H(\mathcal{O})$. Escreveremos $[I]$ para indicar a classe de um ideal $I \in I(\mathcal{O})$, isto é, $[I] = IP(\mathcal{O})$.*

Observação 1.2.32. *Seja $\mathcal{O}$ uma ordem de um corpo de números algébricos K de grau n. Então, I e J são dois $\mathcal{O}$-ideais fracionários na mesma classe de ideais de $H(\mathcal{O})$ se, e somente se,*

$$\begin{aligned} IP(\mathcal{O}) = JP(\mathcal{O}) &\Leftrightarrow I^{-1}J \in P(\mathcal{O}) \\ &\Leftrightarrow I^{-1}J = (\alpha) \text{ para algum } \alpha \in K \setminus \{0\} \\ &\Leftrightarrow J = I(\alpha) \\ &\Leftrightarrow J = I\alpha \\ &\Leftrightarrow J \sim I. \end{aligned}$$

Assim, a próxima proposição é uma consequência imediata de Proposição 1.2.26.

Proposição 1.2.33. *O grupo de classes de ideais $H(\mathcal{O})$ é finito. Sua ordem será denotada por $h(\mathcal{O})$.*

Note que, $h(\mathcal{O}_K) = 1$ se, e somente se, $\mathcal{O}_K$ for um domínio de ideais principais.

Os corpos ciclotômicos com classe de número um foram classificados por Montgomery, assim como, por Uchida em 1971.

Proposição 1.2.34 ([Rib01], p. 652)**.** *Seja ζ_p uma p-ésima raiz primitiva da unidade para um primo p. Então, $h(\mathbb{Z}[\zeta_p]) = 1$ se, e somente se, $p \leq 19$.*

Definição 1.2.35. *Seja $\mathcal{O}$ uma ordem de um corpo quadrático K. Dizemos que um $\mathcal{O}$-ideal não nulo I é* ***relativamente primo para o condutor*** *f se $I + f\mathcal{O} = \mathcal{O}$.*

Lema 1.2.36 ([Cox89], Lem. 7.18 e Prop. 7.4)**.** *Seja $\mathcal{O}$ uma ordem de um corpo quadrático K com condutor f.*

1. *Um $\mathcal{O}$-ideal I é relativamente primo para f se, e somente se, a norma $N(I)$ é relativamente primo para f, isto é, $(N(I), f) = 1$.*

2. *Cada $\mathcal{O}$-ideal I relativamente primo para f é invertível.*

Recorde-se que $\mathcal{O}_K$ denota o anel de inteiros de um corpo de números algébricos K.

Lema 1.2.37. *Seja $\mathcal{O}$ uma ordem de um corpo quadrático K com condutor f. Para um $\mathcal{O}$-ideal J relativamente primo para f, o homomorfismo natural de anéis $\mathcal{O}/J \to \mathcal{O}_K/J\mathcal{O}_K$ é um isomorfismo.*

Demonstração. Como J é um $\mathcal{O}$-ideal relativamente primo para f, temos por definição que, $J + f\mathcal{O} = \mathcal{O}$. Assim,

$$J\mathcal{O}_K + f\mathcal{O}_K = (J + f\mathcal{O})\mathcal{O}_K = \mathcal{O}\mathcal{O}_K = \mathcal{O}_K.$$

Agora, afirmamos $J\mathcal{O}_K \cap \mathcal{O} = J$. De fato, note que

$$\begin{aligned} J &\subseteq J\mathcal{O}_K \cap \mathcal{O} \\ &\subseteq (J\mathcal{O}_K \cap \mathcal{O})\mathcal{O} \\ &\subseteq (J\mathcal{O}_K \cap \mathcal{O})(J + f\mathcal{O}) \\ &\subseteq J + f(J\mathcal{O}_K \cap \mathcal{O}) \\ &\subseteq J + J \cdot f\mathcal{O}_K \\ &\subseteq J + J \text{ pois } f\mathcal{O}_K \subseteq \mathcal{O} \\ &\subseteq J. \end{aligned}$$

Logo, $J\mathcal{O}_K \cap \mathcal{O} = J$. Por fim, considere o homomorfismo natural

$$\varphi : \mathcal{O} \to \frac{\mathcal{O}_K}{J\mathcal{O}_K}.$$

Uma vez que $J\mathcal{O}_K + f\mathcal{O}_K = \mathcal{O}_K$, temos que φ é sobrejetor. Agora, de $J\mathcal{O}_K \cap \mathcal{O} = J$ implica que $\ker(\varphi) = J$. Portanto, a afirmação segue por um dos teoremas de isomorfismo de anéis. □

Proposição 1.2.38 ([JW09], Thm. 4.37)**.** *Seja $\mathcal{O}$ uma ordem de um corpo quadrático K. Se I é um $\mathcal{O}$-ideal invertível e m é qualquer inteiro não nulo, então sempre existe algum $\mathcal{O}$-ideal J tal que $J \sim I$ e $(N(J), m) = 1$.*

Lema 1.2.39. *Seja $\mathcal{O}$ uma ordem de um corpo quadrático K com condutor f. Então, cada classe de ideais em $H(\mathcal{O})$ contém um ideal relativamente primo para f.*

Demonstração. Seja $[I] \in H(\mathcal{O})$. Podemos supor que I é um ideal integral de $\mathcal{O}$. Como I é invertível, segue pela Proposição 1.2.38 que existe um $\mathcal{O}$-ideal J tal que $J \sim I$ e $(N(J), f) = 1$. Pelo Lema 1.2.36, temos que J é um ideal invertível relativamente primo para f que pertence a classe de I. □

Seja I um $\mathcal{O}$-ideal e seja $m \in \mathbb{N}$. Observe que I/mI é um $\mathcal{O}/m\mathcal{O}$-módulo com a ação de $\mathcal{O}/m\mathcal{O}$ em I/mI dada por

$$(\theta + m\mathcal{O}) \cdot (\alpha + mI) := \theta\alpha + mI. \tag{1.4}$$

A fórmula em (1.4) define uma ação de $\mathcal{O}/m\mathcal{O}$ em I/mI, porque I é um $\mathcal{O}$-módulo.

Lema 1.2.40. *Seja $\mathcal{O}$ uma ordem de um corpo quadrático K com condutor f. Se I é um $\mathcal{O}$-ideal relativamente primo para f, então*

$$\frac{I}{p^i I} \cong \frac{\mathcal{O}}{p^i \mathcal{O}}$$

como $\mathcal{O}/p^i\mathcal{O}$-módulos, para cada primo p e $i \in \mathbb{N}$.

Demonstração. Vamos dividir a prova em dois casos.

Caso 1: Se p não divide f.

Pela Proposição 1.2.13, $\{a, b + c\omega\}$ é uma $\mathbb{Z}$-base para I, onde $a, b, c \in \mathbb{Z}$. O Lema 1.2.15 nos diz que $N(I) = ac$. Assim, $\{p^i a, p^i(b + c\omega)\}$ é uma $\mathbb{Z}$-base para $p^i I$ e $N(p^i I) = p^{2i}ac$. Como I é relativamente primo para f, temos que $1 = (N(I), f) = (ac, f)$ pelo Lema

1.2.36. Consequentemente, $(p^{2i}ac, f) = 1$, pois estamos supondo que $p \nmid f$. Logo, os ideais p^iI são invertíveis e relativamente primos para f pelo Lema 1.2.36. Agora, pelo Lema 1.2.37, temos que

$$\frac{\mathcal{O}}{p^iI} \cong \frac{\mathcal{O}_K}{p^iI\mathcal{O}_K}$$

como anéis. Como os ideais de $\mathcal{O}_K/p^iI\mathcal{O}_K$ são todos principais pela Proposição 1.2.10, assim são os ideais de $\mathcal{O}/p^iI$. Consequentemente, I/p^iI é um ideal principal de $\mathcal{O}/p^iI$. Uma vez que,

$$\left|\frac{I}{p^iI}\right| = \left|\frac{\mathcal{O}}{p^i\mathcal{O}}\right|$$

pelo Lema 1.2.29, e I/p^iI e $\mathcal{O}/p^i\mathcal{O}$ são $\mathcal{O}/p^i\mathcal{O}$-módulos 1-gerados, segue que

$$\frac{I}{p^iI} \cong \frac{\mathcal{O}}{p^i\mathcal{O}}$$

como $\mathcal{O}/p^i\mathcal{O}$-módulos, para cada primo p e $i \in \mathbb{N}$.

Caso 2: Se p divide f.

Uma vez que $(N(I), f) = 1 = (ac, f)$ e $p \mid f$ implica que $p \nmid ac$, que implica que $p \nmid a$ e $p \nmid c$.

Considere a aplicação $\varphi : I \to \mathcal{O}/p^i\mathcal{O}$ definida por

$$\alpha \mapsto \alpha a + p^i\mathcal{O}.$$

É imediato verificar que φ é um homomorfismo de grupos.

- φ é sobrejetor.

  Para provar a afirmação é suficiente provar que $aI + p^i\mathcal{O} = \mathcal{O}$. Como $(a, p) = 1$, temos que $(a^2, p^i) = 1$. Note que, $\{p^i, p^i\omega\}$ e $\{a^2, a(b + c\omega)\}$ são $\mathbb{Z}$-bases para $p^i\mathcal{O}$ e aI, respectivamente. Como a equação diofantina $xa^2 + yp^i = 1$ tem solução inteira, pois $(a^2, p^i) = 1$, então $1 \in aI + p^i\mathcal{O}$. Logo, $\mathcal{O} \subseteq aI + p^i\mathcal{O}$ e, portanto, $aI + p^i\mathcal{O} = \mathcal{O}$.

- $\ker(\varphi) = p^iI$.

  Temos que $\{a, b + c\omega\}$ é uma $\mathbb{Z}$-base para I. Se $a = 1$ temos que o resultado é óbvio pois, $I = \mathcal{O}$. Então, podemos supor $a \neq 1$. Como $p \nmid a$, temos que $p^i \notin I$.

  Seja $\beta \in \ker(\varphi)$. Então, $\beta a \in p^i\mathcal{O}$. Assim, existe $\alpha \in \mathcal{O}$ tal que $\beta a = p^i\alpha$. Afirmamos que $\beta \in p^iI$. Com efeito, temos que

$$\beta = ua + v(b + c\omega) \quad \text{e} \quad \alpha = r + s\omega$$

onde $u, v, r, s \in \mathbb{Z}$. Então,

$$\begin{aligned} r + s\omega &= \alpha \\ &= \frac{a}{p^i}\beta \\ &= \frac{a}{p^i}(ua + v(b + c\omega)) \\ &= \frac{a}{p^i}(ua + vb + vc\omega) \\ &= \frac{a}{p^i}(ua + vb) + \frac{a}{p^i}vc\omega \end{aligned}$$

Então,

$$r = \frac{a}{p^i}(ua + vb) \quad \text{e} \quad s = \frac{acv}{p^i}.$$

Como $p \nmid ac$ e $s \in \mathbb{Z}$, temos que $p^i \mid v$. Além disso, como $p \nmid a^2$, implica que $p^i \mid u$, pois $r \in \mathbb{Z}$. Logo, $u = p^i u'$ e $v = p^i v'$, onde $u', v' \in \mathbb{Z}$. Portanto,

$$\beta = ua + v(b + c\omega) = p^i(u'a + v'(b + c\omega)) \in p^i I,$$

e, assim, $\ker(\varphi) \subseteq p^i I$. Como $p^i I$ está claramente contido em $\ker(\varphi)$, temos que $\ker(\varphi) = p^i I$.

Portanto, segue dos pontos anteriores que a aplicação $\tilde{\varphi} : I/p^i I \to \mathcal{O}/p^i\mathcal{O}$ definida por $\tilde{\varphi}(\alpha + p^i I) = \alpha a + p^i\mathcal{O}$ é um isomorfismo de grupos abelianos. Como

$$\begin{aligned} \tilde{\varphi}((\theta + p^i\mathcal{O}) \cdot (\alpha + p^i I)) &= \tilde{\varphi}(\theta\alpha + p^i I) \\ &= \theta\alpha a + p^i\mathcal{O} \\ &= (\theta + p^i\mathcal{O})(\alpha a + p^i\mathcal{O}) \\ &= (\theta + p^i\mathcal{O})\tilde{\varphi}(\alpha + p^i I), \end{aligned}$$

temos que $\tilde{\varphi}$ é um isomorfismo de $\mathcal{O}/p^i\mathcal{O}$-módulos. □

Grupos de Galois agindo em grupos de classes de ideais

Seja n um número natural. O grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ age naturalmente em $\mathbb{Q}(\zeta_n)$ (resp. $\mathbb{Z}[\zeta_n]$) via automorfismos. Em particular, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ age no conjunto de ideais de $\mathbb{Z}[\zeta_n]$.

Lema 1.2.41. *Sejam I e J ideais de $\mathbb{Z}[\zeta_n]$. Se I e J estão na mesma classe de ideais, então $\sigma(I)$ e $\sigma(J)$ estão na mesma classe de ideais para qualquer $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.*

Demonstração. Os ideais I e J de $\mathbb{Z}[\zeta_n]$ estão na mesma classe de ideais se, e somente se, $J = I(a)$, onde (a) denota o ideal gerado por algum elemento $a \in \mathbb{Q}(\zeta_n) \setminus \{0\}$. Observe que,

$$\sigma(J) = \sigma(I(a)) = \sigma(I)(\sigma(a)).$$

Como $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, temos que $\sigma(a)$ é não nulo em $\mathbb{Q}(\zeta_n)$. Portanto, $\sigma(I)$ e $\sigma(J)$ estão na mesma classe de ideais. □

Segue do Lema 1.2.41 que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ age em $H(\mathbb{Z}(\zeta_n))$ via automorfismos.

Observação 1.2.42. *(i) Seja $\delta = p_1 p_2 \cdots p_k$ a decomposição de um inteiro positivo em fatores primos distintos e suponha que $d \in \mathbb{N}$ divide δ. Então, existe $u \in \mathbb{N}$ tal que $\delta = du$. Assim, se ζ_δ é uma δ-ésima raiz primitiva da unidade, então ζ_δ^u é uma d-ésima raiz primitiva da unidade. Consequentemente, o corpo $\mathbb{Q}(\zeta_d)$ é um subcorpo de $\mathbb{Q}(\zeta_\delta)$. Logo, para qualquer $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_\delta)/\mathbb{Q})$, temos que a restrição de σ para $\mathbb{Q}(\zeta_d)$ é um elemento de $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ para cada $d \mid \delta$.*

(ii) De (i) segue que $\mathrm{Gal}(\zeta_\delta)$ age via automorfismos no produto direto $\prod_{d|\delta} H(\mathbb{Z}(\zeta_d))$.

(iii) Se D é um subconjunto de $\{p_1, p_2, \cdots, p_k\}$, usando a Proposição 1.2.23 definimos o grupo

$$\mathcal{H}_D = \mathrm{Gal}(\zeta_{p_1}) \times \cdots \times \mathrm{Gal}(\zeta_{p_{i-1}}) \times C_2 \times \mathrm{Gal}(\zeta_{p_{i+1}}) \times \cdots \times \mathrm{Gal}(\zeta_{p_k}),$$

para cada $p_i \in D$. Como o grupo de classes de ideais $H(\mathbb{Z}[\zeta_2])$ é trivial, temos uma ação trivial de C_2 sobre $H(\mathbb{Z}[\zeta_2])$. Logo, $\mathcal{H}_D$ também age sobre $\prod_{d|\delta} H(\mathbb{Z}(\zeta_d))$.

Lema 1.2.43. *Seja n um número natural. O grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ age transitivamente em $H(\mathbb{Z}(\zeta_n))$ se, e somente se, $h(\mathbb{Z}(\zeta_n)) = 1$.*

Demonstração. A suficiência é imediata. Provaremos a necessidade. Se $H(\mathbb{Z}(\zeta_n))$ não é trivial, então existe um ideal I de $\mathbb{Z}[\zeta_n]$ que não é principal. Note que,

$$\sigma(I(a)) = \sigma(I)(\sigma(a)), \quad a \in \mathbb{Q}(\zeta_n) \setminus \{0\}$$

não é um ideal principal para todo $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Assim, o elemento identidade de $H(\mathbb{Z}(\zeta_n))$ não pertence a órbita de $[I]$. Portanto, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ não age transitivamente em $H(\mathbb{Z}(\zeta_n))$ se $h(\mathbb{Z}(\zeta_n)) \neq 1$. □

1.3 Ext e cohomologia de grupos

Nesta tese, a menos de menção contrária, R será um anel com elemento identidade e todos os R-módulos são R-módulos à esquerda.

Vamos iniciar generalizando a noção de grupos abelianos livres para módulos.

Definição 1.3.1. *Um R-módulo F é **livre** se possui uma base, isto é, um subconjunto $\{x_i\}$ (possivelmente vazio $\{\ \}$) onde i varia sobre algum conjunto de índice, tal que cada $x \in F$ pode ser escrito como uma soma finita $\sum r_i x_i$ onde os coeficientes $r_i \in R$ são unicamente determinados.*

Assim, F é um R-módulo livre se, e somente se, $F = \oplus_i R_i$ onde $R_i \cong R$. Além disso, módulos arbitrários podem ser descritos em termos de módulos livres.

Proposição 1.3.2 ([Rot09], Thm. 2.35)**.** *Cada R-módulo M é um quociente de um R-módulo livre.*

Seja N um R-módulo. Pela Proposição 1.3.2, podemos construir os seguintes epimorfismos: $d_0 : F_0 \to N$ onde F_0 é um R-módulo livre; $d_1 : F_1 \to \ker(d_0)$ onde F_1 é um R-módulo livre, etc. Isso nos dá uma sequência exata longa infinita de módulos livres

$$\cdots \to F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} N \to 0, \tag{1.5}$$

chamada **resolução livre** de N. Podemos obter uma noção mais geral para essa construção.

Definição 1.3.3. *Um R-módulo é **projetivo** se é um somando direto de uma R-módulo livre.*

Então, cada R-módulo livre é projetivo. A recíproca não é verdadeira, conforme mostra o seguinte exemplo.

Exemplo 1.3.4. *O anel $R = \mathbb{Z}/6\mathbb{Z}$ é a soma direta dos ideais $\mathbb{Z}/2\mathbb{Z}$ e $\mathbb{Z}/3\mathbb{Z}$. Agora, $\mathbb{Z}/6\mathbb{Z}$ é um módulo livre sobre si mesmo. Então, $\mathbb{Z}/2\mathbb{Z}$ e $\mathbb{Z}/3\mathbb{Z}$ são R-módulos projetivos. Entretanto, nem $\mathbb{Z}/2\mathbb{Z}$ e nem $\mathbb{Z}/3\mathbb{Z}$ são R-módulos livres, pois cada R-módulo livre não nulo tem pelo menos 6 elementos.*

Assim, podemos generalizar a noção de resolução livre para resolução projetiva, isto é, podemos construir uma sequência exata longa infinita

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} N \to 0, \tag{1.6}$$

para qualquer R-módulo N, onde cada P_i é um R-módulo projetivo. A sequência (1.6) é chamada **resolução projetiva** de N.

Agora, seja $f \in \mathrm{Hom}_R(M,N)$, onde M e N são R-módulos. Para cada R-módulo L, o homomorfismo f induz um homomorfismo aditivo

$$f^* : \mathrm{Hom}_R(N,L) \to \mathrm{Hom}_R(M,L),$$

definido por

$$f^*(\phi) = \phi \circ f, \phi \in \mathrm{Hom}_R(N,L). \tag{1.7}$$

Para cada R-módulo M, usamos a resolução projetiva (1.6) e a definição (1.7) para construir a sequência de grupos aditivos

$$0 \to \mathrm{Hom}_R(P_0,M) \overset{d_1^*}{\to} \mathrm{Hom}_R(P_1,M) \overset{d_2^*}{\to} \mathrm{Hom}_R(P_2,M) \to \cdots .$$

Note que,

$$d_{i+1}^* \circ d_i^* = (d_i \circ d_{i+i})^* = 0, i \geq 1.$$

Assim, $\mathrm{im}(d_i^*) \subseteq \ker(d_{i+1}^*),\ i \geq 1$, e podemos definir a seguinte família de grupos aditivos

$$\mathrm{Ext}_R^n(N,M) := \frac{\ker(d_{n+1}^*)}{\mathrm{im}(d_n^*)}, n \geq 1.$$

Proposição 1.3.5 ([Rot09], Cor. 6.57)**.** *Os grupos* $\mathrm{Ext}_R^n(N,M)$ *não depende da escolha da resolução projetiva de* N.

Em particular, temos o seguinte caso especial.

Definição 1.3.6. *Se* G *é um grupo e* M *é um* $\mathbb{Z}G$*-módulo, então o* n***-ésimo grupo de cohomologia*** *de* G *com coeficientes em* M *é*

$$H^n(G,M) := \mathrm{Ext}_{\mathbb{Z}G}^n(\mathbb{Z},M)$$

onde $\mathbb{Z}$ *é visto como um* $\mathbb{Z}G$*-módulo trivial, isto é,* $g \cdot z = z$ *para cada* $g \in G$ *e* $z \in \mathbb{Z}$.

Aqui, particularmente, estamos interessados nos grupos

1. $\mathrm{Ext}_R^1(N,M)$, onde M e N são R-módulos.
2. $H^2(G,M)$, onde G é um grupo e M é um $\mathbb{Z}G$-módulo.

O interesse por esses grupos se justifica pelo fato de que o primeiro descreve, a menos de isomorfismo, as extensões de módulos e o segundo as extensões de grupos. Como

veremos, a teoria de extensões será fundamental para a prova de muitos resultados desta tese.

1.3.1 Ext^1 e extensões

Sejam A e C módulos sobre um anel fixado R. Uma **extensão** de A por C é uma sequência exata curta

$$E : 0 \to A \xrightarrow{i} B \xrightarrow{\pi} C \to 0$$

de R-módulos e homomorfismos de R-módulos. Às vezes, o próprio módulo B será referido como uma extensão. Duas extensões

$$E : 0 \to A \to B \to C \to 0$$

e

$$E' : 0 \to A \to B' \to C \to 0$$

de A por C são **equivalentes** se existe um diagrama comutativo

$$\begin{array}{ccccccccc} E: & 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & & \downarrow{\scriptstyle 1_A} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_C} & & \\ E': & 0 & \longrightarrow & A & \longrightarrow & B' & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

A aplicação φ é necessariamente um R-isomorfismo. Vamos denotar a classe de equivalência da extensão E por $[E]$ e definimos

$$\mathrm{Ext}(C, A) = \{[E] : E \text{ é uma extensão de } A \text{ por } C\}.$$

A extensão E acima **cinde** se existe uma aplicação $s : C \to B$ tal que $\pi \circ s = 1_C$. Equivalentemente, E é uma extensão cinde se é equivalente para extensão

$$0 \to A \to A \oplus B \to B \to 0,$$

com as aplicações naturais. No que segue, vamos definir uma operação em $\mathrm{Ext}(C, A)$, conhecida como a **soma de Baer**, que torna $\mathrm{Ext}(C, A)$ um grupo abeliano.

Sejam

$$E_1 : 0 \to A \xrightarrow{i_1} B_1 \xrightarrow{\pi_1} C \to 0 \quad \text{e} \quad E_2 : 0 \to A \xrightarrow{i_2} B_2 \xrightarrow{\pi_2} C \to 0$$

duas extensões de A por C. A soma direta de E_1 e E_2 é a extensão

$$E_1 \oplus E_2 : 0 \to A \oplus A \overset{i_1 \oplus i_2}{\to} B_1 \oplus B_2 \overset{\pi_1 \oplus \pi_2}{\to} C \oplus C \to 0.$$

Definimos a **aplicação diagonal** $\triangle_C$: $C \to C \oplus C$ por $\triangle_C$: $c \mapsto (c, c)$ e definimos a **aplicação codiagonal** $\nabla_A : A \oplus A \to A$ por $\nabla_A : (a_1, a_2) \mapsto a_1 + a_2$.

Agora, definimos a soma das extensões E_1 e E_2, que denotamos por $E_1 + E_2$, como segue:

1. Considere o pullback B' da aplicação diagonal $\triangle_C$ e $\pi_1 \oplus \pi_2$, para construir o seguinte diagrama comutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A \oplus A & \xrightarrow{i} & B' & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1} & & \downarrow & & \downarrow{\scriptstyle \triangle_C} & & \\ 0 & \longrightarrow & A \oplus A & \xrightarrow{i_1 \oplus i_2} & B_1 \oplus B_2 & \xrightarrow{\pi_1 \oplus \pi_2} & C \oplus C & \longrightarrow & 0. \end{array}$$

2. Considere o pushout B'' da aplicação codiagonal ∇_A e i, para construir o seguinte diagrama comutativo:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A \oplus A & \xrightarrow{i} & B' & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \nabla_A} & & \downarrow & & \downarrow{\scriptstyle 1} & & \\ 0 & \longrightarrow & A & \longrightarrow & B'' & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

3. Por fim, a soma das extensões E_1 e E_2 é a extensão

$$E_1 + E_2 : 0 \to A \to B'' \to C \to 0.$$

Definição 1.3.7. *A operação*

$$+_B : \mathrm{Ext}(C, A) \times \mathrm{Ext}(C, A) \to \mathrm{Ext}(C, A)$$
$$([E_1], [E_2]) \mapsto [E_1 + E_2]$$

é chamada a ***soma de Baer****.*

O próximo teorema é devido a Baer.

Teorema 1.3.8 ([Rot09], Thm. 7.35)**.** *Para cada R-módulos A e C o conjunto* $\mathrm{Ext}(C, A)$ *é um grupo abeliano munido com a soma de Baer cuja a classe das extensões cindem é o elemento neutro da soma. Além disso,* $\mathrm{Ext}(C, A)$ *é isomorfo a* $\mathrm{Ext}^1_R(C, A)$.

1.3.2 Cohomologia de grupos

Sejam G um grupo e M um $\mathbb{Z}G$-módulo. Vamos iniciar apresentando uma descrição mais explícita para os n-ésimos grupos de cohomologia $H^n(G, M)$. Para isso, usaremos uma resolução livre específica.

Definição 1.3.9. *A **resolução de barras** (ou **normalizada**) é*

$$\mathbf{B} : \cdots \to B_2 \xrightarrow{d_2} B_1 \xrightarrow{d_1} B_0 \xrightarrow{d_0} \mathbb{Z} \to 0,$$

onde B_n é um $\mathbb{Z}G$-módulo livre com base formada por todas as n-tuplas $\{(x_1, \cdots, x_n) : x_i \in G \text{ e } x_i \neq 1\}$ e, para $n = 0$, B_0 é um $\mathbb{Z}G$-módulo livre em um único gerador, que denotamos pelo símbolo $(\ )$, assim B_0 é isomorfo a $\mathbb{Z}G$. Os $\mathbb{Z}G$-homomorfismos $d_n : B_n \to B_{n-1}$ são definidos por

$$\begin{aligned}
&d_0(\ ) = 1,\\
&d_1(x) = x(\ ) - (\ ),\\
&d_2(x, y) = x(y) - (xy) + (x),\\
&d_3(x, y, z) = x(y, z) - (xy, z) + (x, yz) - (x, y),\\
&\qquad\vdots\\
&d_n(x_1, \cdots, x_n) = x_1(x_2, \cdots, x_n) + \sum_{i=1}^{n-1}(-1)^i(x_1, \cdots, x_{i-1}, x_ix_{i+1}, \cdots, x_n)\\
&\qquad\qquad +(-1)^n(x_1, \cdots, x_{n-1}).
\end{aligned}$$

Observação 1.3.10.

1. *Para que d_n seja bem definido, assumimos que $(x_1, \cdots, x_n) = 0$ sempre que algum $x_i = 1$.*

2. *A resolução $\mathbf{B}$ é chamada resolução de barras, porque a notação original para $(x_1, \cdots, x_n)$ era $(x_1|x_2|\cdots|x_n)$.*

Proposição 1.3.11 ([Rot09], Thm. 9.37)**.** *A resolução de barras $\mathbf{B}$ é uma resolução livre de $\mathbb{Z}$.*

Assim, para qualquer $\mathbb{Z}G$-módulo M, podemos usar a resolução $\mathbf{B}$ para calcular $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, M)$. Para esse fim, considere a sequência de grupos aditivos

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(B_0, M) \xrightarrow{d_1^*} \mathrm{Hom}_{\mathbb{Z}G}(B_1, M) \xrightarrow{d_2^*} \mathrm{Hom}_{\mathbb{Z}G}(B_2, M) \to \cdots .$$

Então, $\mathrm{im}(d_n^*) \subseteq \ker(d_{n+1}^*)$ para $n \geq 1$, e

$$H^n(G, M) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, M) = \frac{\ker(d_{n+1}^*)}{\mathrm{im}(d_n^*)},\ n \geq 1$$

e

$$H^0(G, M) = \ker(d_1^*) \cong \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M).$$

Uma vez que, cada $f \in \mathrm{Hom}_{\mathbb{Z}G}(B_n, M)$ é completamente determinado pelas imagens $\{f(x_1, \cdots, x_n) : x_i \in G\}$, podemos identificar $\mathrm{Hom}_{\mathbb{Z}G}(B_n, M)$ com o conjunto de todas as funções de $G \times \cdots \times G$ para M, onde G ocorre em n fatores. Assim, dado uma função $f : G^n \to M$, temos

$$d_{n+1}^* f = f \circ d_{n+1} \in \mathrm{Hom}_{\mathbb{Z}G}(B_n, M),\ n \geq 0$$

por definição de d_{n+1}^* (ver (1.7)). Explicitamente, obtemos

$$\begin{aligned}
(d_1^* f)(x) &= f \circ d_1(x) = xf(\ ) - f(\ ),\\
(d_2^* f)(x, y) &= f \circ d_2(x, y) = xf(y) - f(xy) + f(x),\\
(d_3^* f)(x, y, z) &= xf(y, z) - f(xy, z) + f(x, yz) - f(x, y),\\
&\vdots\\
(d_{n+1}^* f)(x_1, \cdots, x_{n+1}) &= x_1 f(x_2, \cdots, x_{n+1}) + \sum_{i=1}^{n} (-1)^i f(x_1, \cdots, x_{i-1}, x_i x_{i+1}, \cdots, x_{n+1})\\
&\quad + (-1)^{n+1} f(x_1, \cdots, x_n).
\end{aligned}$$

Em particular, $\ker(d_3^*)$ consiste de todas as funções $f : G \times G \to M$ tais que

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0,$$

para cada $x, y, z \in G$. Tais funções f são chamadas de **2-cociclo**. Agora, os 2-cociclos em $\mathrm{im}(d_2^*)$ são chamados **2-cobordos**. Note que, cada função $h : G \to M$ determina um 2-cociclo $f = d_2^* h$, dado por

$$f(x, y) = xh(y) - h(xy) + h(x),$$

para cada $x, y \in G$. Então, por definição,

$$H^2(G, M) = \frac{\{\text{2-cociclos}\}}{\{\text{2-cobordos}\}}.$$

Como exemplo, vamos calcular a cohomologia de um grupo cíclico finito.

Definição 1.3.12. *Se G é um grupo e A é um $\mathbb{Z}G$-módulo, então o submódulo dos* ***elementos G-fixados*** *é definido por*

$$A^G = \{a \in A : x \cdot a = a \text{ para todo } x \in G\}.$$

Exemplo 1.3.13 (Para os detalhes, ver [Rot09], p. 521 e p. 522)**.** *Suponha que G é um grupo cíclico finito de ordem k gerado por x e defina elementos D e N de $\mathbb{Z}G$ por $D = x - 1$ e $N = 1 + x + x^2 + \cdots + x^{k-1}$. Então, $DN = ND = x^k - 1 = 0$ e, assim, obtemos uma resolução $\mathbb{Z}G$-livre*

$$\cdots \to \mathbb{Z}G \xrightarrow{D} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{D} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

onde as aplicações alternadas são multiplicações por D e por N e a aplicação $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ é definida por $\sum r_x x \mapsto \sum r_x$ (ε é conhecida como a ***aplicação de aumento****). Assim, para qualquer $\mathbb{Z}G$-módulo A, podemos construir a sequência*

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \xrightarrow{D^*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \xrightarrow{N^*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \xrightarrow{D^*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \xrightarrow{N^*} \cdots .$$

Desse modo, temos que

$$\ker(N^*) = {}_NA, \quad \mathrm{im}(N^*) = NA, \quad \ker(D^*) = A^G, \quad \mathrm{im}(D^*) = DA,$$

onde ${}_NA = \{a \in A : Na = 0\}$. Agora, por definição de $H^n(G, A)$, temos que

$$H^0(G, A) = A^G, \quad H^{2n-1}(G, A) = \frac{{}_NA}{DA}, \quad H^{2n}(G, A) = \frac{A^G}{NA}.$$

Em particular,

Proposição 1.3.14 ([Cha86], Chap. IV, Thm. 5.1)**.** *Seja M um $\mathbb{Z}C_p$-módulo finitamente gerado livre de torção como um grupo abeliano para um grupo cíclico C_p de ordem prima p. Então,*

$$H^2(C_p, M) \cong \bar{M}_1, \ (\bar{M}_1 \text{ é a redução de } M_1 \text{ módulo } p)$$

onde $M = M_1 \oplus M_2$ de modo que M_1 é o maior somando direto de M em que C_p age trivialmente.

Finalizamos essa subseção com uma série de propriedades sobre os grupos $H^n(G, M)$ que serão úteis mais tarde.

Proposição 1.3.15 ([Wei94], Cor. 6.5.10)**.** *Se G é um grupo finito e M é um $\mathbb{Z}G$-módulo finitamente gerado, então $H^n(G,M)$ é um grupo abeliano finito para todo $n>0$.*

Observação 1.3.16. *Consequentemente, se G é um grupo finito e M é um $\mathbb{Z}G$-módulo finitamente gerado, então existe uma decomposição p-primária*

$$H^n(G,M)=\bigoplus_p H^n(G,M)_p,$$

onde p varia sobre os divisores primos de $|G|$ e

$$H^n(G,M)_p=\{\alpha\in H^n(G,M):\alpha^{p^k}=1 \text{ para algum } k\geq 1\}.$$

Proposição 1.3.17 ([Bro82], p. 84, Thm. 10.3)**.** *Sejam G um grupo finito e P um p-subgrupo de Sylow normal de G. Então,*

$$H^n(G,M)_p\cong H^n(P,M)^{G/P}$$

para todo $n>0$.

Interpretação do grupo $H^2(G,M)$

Agora podemos apresentar uma interpretação do grupo $H^2(G,M)$ em termos de **extensões de grupos**, isto é, em termos das sequências exatas de grupos

$$\mathcal{E}: 1\to M\xrightarrow{i} E\xrightarrow{\pi} G\to 1. \tag{1.8}$$

Para o que segue, vamos assumir que $\mathcal{E}$ é uma extensão de um grupo abeliano M por um grupo G.

Definição 1.3.18. *Seja $\mathcal{E}$ uma extensão como em (1.8). Um **levantamento** é uma função $l:G\to E$ com $\pi\circ l=\mathrm{id}_G$ e $l(1)=1$. Em particular, a extensão $\mathcal{E}$ **cinde** se existe um homomorfismo $\lambda:G\to E$ tal que $\pi\circ\lambda=\mathrm{id}_G$. Neste caso, o grupo E é chamado um **produto semidireto** de M por G.*

Assim, assumindo que $i:M\to E$ é a inclusão, podemos definir uma aplicação $\theta_g: M\to M$ por $\theta_g: m\mapsto l(g)ml(g)^{-1}$, onde $g\in G$. O próximo lema nos diz que θ_g não depende da escolha do levantamento $l(g)$ de g.

Lema 1.3.19. *Sejam $l,l':G\to E$ levantamentos de G. Então, $l(g)ml(g)^{-1}=l(g)'m(l(g)')^{-1}$ para todos $m\in M$ e $g\in G$.*

Demonstração. Seja $m \in M$. Como $\pi(l(g)) = \pi(l(g)')$, temos que

$$l(g)^{-1}l(g)' \in \ker(\pi) = M.$$

Então, $l(g)^{-1}l(g)'m = ml(g)^{-1}l(g)'$, uma vez que M é abeliano. Agora, multiplicando ambos os lados desta equação, à esquerda por $l(g)$ e à direita por $(l(g)')^{-1}$, obtemos o resultado desejado. □

Então, a função $\theta : G \to \mathrm{Aut}(M)$, definida por $\theta : g \mapsto \theta_g$, é bem definida. É imediato verificar que θ é um homomorfismo. Consequentemente, θ induz uma ação de G em M. Assim, obtemos o seguinte

Proposição 1.3.20. *Seja M um grupo abeliano. Então, a extensão $\mathcal{E}$ de M por G induz uma estrutura de $\mathbb{Z}G$-módulo em M.*

Demonstração. Pelos comentários acima, $\mathbb{Z}G$ age em M pela seguinte fórmula:

$$(\sum_{g\in G} r_g g) \cdot m := \sum_{g\in G} r_g(g \cdot m),$$

onde $g \cdot m := \theta_g(m)$, para $m \in M$. Com essa definição, é imediato concluir que M é um $\mathbb{Z}G$-módulo. □

Dado um $\mathbb{Z}G$-módulo M, gostaríamos de determinar quantas extensões de M por G existem nas quais a ação induzida de G sobre M concorda com a estrutura do $\mathbb{Z}G$-módulo dado, isto é, em que $g \cdot m = l(g)ml(g)^{-1}$ onde $g \in G$, $m \in M$ e $l : G \to M$ é um levantamento de G.

A noção de equivalência de extensões de módulos, que apresentamos na Subseção 1.3.1, surgiu primeiro no contexto de extensões de grupos.

Definição 1.3.21. *Dizemos que duas extensões $1 \to M \to E_i \to G \to 1$ são **equivalentes** se existe um isomorfismo $\varphi : E_1 \cong E_2$ tal que o diagrama*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M & \longrightarrow & E_1 & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_M} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 1 & \longrightarrow & M & \longrightarrow & E_2 & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

comuta.

Teorema 1.3.22 ([Wei94], Thm. 6.6.3)**.** *Sejam G um grupo, M um $\mathbb{Z}G$-módulo, e denote por $e(G, M)$ o conjunto de todas as classes de equivalência de extensões de M por*

G. Então, existe uma bijeção entre $H^2(G,M)$ e $e(G,M)$ que associa 0 com a classe de extensões cinde.

O homomorfismo de restrição de $H^2(G,M)$

Definição 1.3.23. *Sejam G e H grupos. Um homomorfismo de grupos $\varphi : G \to H$ induz um homomorfismo de anéis $\mathbb{Z}G \to \mathbb{Z}H$, também representado por φ, dado por*

$$\varphi : \sum_{g\in G} r_g g \mapsto \sum_{g\in G} r_g \varphi(g).$$

Então, se M é um $\mathbb{Z}H$-módulo, podemos ver M como um $\mathbb{Z}G$-módulo com a ação $g \cdot m := \varphi(g) \cdot m$ para $g \in G$ e $m \in M$. Denotamos o $\mathbb{Z}H$-módulo M visto como $\mathbb{Z}G$-módulo por $(M)^{\varphi}$.

Usando isso, podemos construir um homomorfismo $\varphi_* : H^2(H,M) \to H^2(G,(M)^{\varphi})$.

Proposição 1.3.24 ([Cha86], p. 78)**.** *Sejam $\varphi : G \to H$ um homomorfismo de grupos e $f : M \to N$ um homomorfismo de $\mathbb{Z}H$-módulos. Então, as seguintes definições*

$$[\varphi_{\#}(c)](g_1,g_2) = c(\varphi(g_1),\varphi(g_2))$$

e

$$[f_{\#}(c)](h_1,h_2) = f(c(h_1,h_2)),$$

onde $c : H \times H \to M$ é um 2-cociclo, $g_1, g_2 \in G$ e $h_1, h_2 \in H$, induzem homomorfismos

$$\varphi_* : H^2(H,M) \to H^2(G,(M)^{\varphi}) \quad e \quad f_* : H^2(H,M) \to H^2(H,N),$$

respectivamente.

Definição 1.3.25. *Se $\iota : H \to G$ é a inclusão (ou um monomorfismo), chamamos $res^G_H = \iota_* : H^2(G,M) \to H^2(H,(M)^{\iota})$ de **homomorfismo de restrição**. Neste caso, comumente, identificamos $(M)^{\iota}$ com M.*

Definição 1.3.26. *Seja M um $\mathbb{Z}G$-módulo finitamente gerado e livre como um $\mathbb{Z}$-módulo. Um elemento $\alpha \in H^2(G,M)$ é dito ser **especial** se para qualquer subgrupo cíclico C_p de ordem prima p de G, tem-se que $res^G_{C_p}(\alpha) \neq 0$.*

1.4 A classificação de $\mathbb{Z}G$-reticulados

Definição 1.4.1. *Seja G um grupo finito. Um $\mathbb{Z}G$-**reticulado** é um $\mathbb{Z}G$-módulo que é finitamente gerado e livre como um $\mathbb{Z}$-módulo.*

Definição 1.4.2. *Um módulo M sobre um anel R é **indecomponível** se M não pode ser expresso como uma soma direta de dois submódulos não triviais.*

Em geral, o conjunto de classes de isomorfismo de $\mathbb{Z}G$-reticulados indecomponíveis é infinito. Em 1963, Jones [Jon63] descreveu sobre quais hipóteses esse conjunto é finito.

Teorema 1.4.3 (Jones, [Jon63])**.** *Seja G um grupo finito. O número de $\mathbb{Z}G$-reticulados indecomponíveis é finito se, e somente se, para cada primo p dividindo $|G|$, os p-subgrupos de Sylow de G são cíclicos de ordem p ou p^2.*

É uma consequência imediata do Teorema 1.4.3 que existe um número finito de $\mathbb{Z}C$-reticulados indecomponíveis, quando C é um grupo cíclico de ordem $p_1p_2\cdots p_k$, em que $p_1, \cdots, p_k$ são números primos distintos. Assim, é possível classificar esses reticulados, como veremos a seguir. À luz do Teorema 1.4.3, vemos que é muito difícil obter uma classificação para $\mathbb{Z}G$-reticulados em geral. Até o momento, além da classe de grupos cíclicos mencionada acima, existem poucas classes de grupos finitos G para a qual uma classificação dos $\mathbb{Z}G$-reticulados é conhecida. Por exemplo, para os grupos cíclicos de ordem p^2, onde p é um número primo – classificado por Troy [Tro61] em 1961; grupos diedrais de ordem $2p$, onde p é um primo ímpar – classificado por Lee [Lee64] em 1964; grupos não abelianos de ordem pq, onde p e q são primos distintos – classificado por Pu [Pu65] em 1965. Para mais exemplos e informações, recomendamos a leitura de [CR81, §34].

1.4.1 Reticulados sobre grupos cíclicos de ordem prima

Ao longo desta tese, C_p denota um grupo cíclico de ordem prima p gerado por um elemento x. O principal resultado desta subseção é o teorema de classificação dos $\mathbb{Z}C_p$-reticulados. Esta classificação é devido a Diederichsen (1938), que foi estendida por Reiner (1957).

Sejam ζ_p uma raiz p-ésima primitiva da unidade, $\mathbb{Q}(\zeta_p)$ o corpo ciclotômico gerado por ζ_p com anel de inteiros $\mathbb{Z}[\zeta_p]$. Suponha agora que A é qualquer ideal não nulo de $\mathbb{Z}[\zeta_p]$. Então, A tem $\mathbb{Z}$-posto $p-1$, $\mathbb{Z}[\zeta_p]A \subseteq A$ e, além disso, podemos transformar A em um $\mathbb{Z}C_p$-módulo, pela definição

$$x \cdot a := \zeta_p a,$$

para todo $a \in A$. Por causa desta definição, dois ideais de $\mathbb{Z}[\zeta_p]$ são isomorfos como $\mathbb{Z}C_p$-módulos se, e somente se, são isomorfos como $\mathbb{Z}[\zeta_p]$-módulos. Por outro lado, temos o seguinte

Lema 1.4.4 ([CR62], Lem. 22.2)**.** *Seja K um corpo de números algébricos com anel de inteiros $\mathcal{O}_K$. Então, dois ideais fracionários A e B de $\mathcal{O}_K$ são isomorfos como $\mathcal{O}_K$-módulos se, e somente se, A e B estão na mesma classe de ideais.*

Seja A um ideal de $\mathbb{Z}[\zeta_p]$ e seja a_0 algum elemento fixado de A tal que $a_0 \notin (\zeta_p - 1)A$. Considere a soma direta $A \oplus \mathbb{Z}y$ de um $\mathbb{Z}$-módulo A e o $\mathbb{Z}$-módulo livre $\mathbb{Z}y$. Podemos definir uma ação de C_p em $A \oplus \mathbb{Z}y$ por

$$x \cdot a = \zeta_p a, \quad x \cdot y = a_0 + y, \tag{1.9}$$

onde $a \in A$. As fórmulas em (1.9) definem uma ação de C_p em $A \oplus \mathbb{Z}y$. De fato, para isso, provaremos a etapa mais difícil, que é verificar que x^p age como a identidade em $A \oplus \mathbb{Z}y$. Como $x^p \cdot a = \zeta_p^p a = a$, é suficiente mostrar que $x^p \cdot y = y$. Denotemos por $\Phi_p(\cdot)$ o p-ésimo polinômio ciclotômico. Note que,

$$\begin{aligned} x \cdot y &= a_0 + y, \\ x^2 \cdot y &= x \cdot (a_0 + y) = \zeta_p a_0 + x \cdot y = (\zeta_p + 1)a_0 + y, \\ &\vdots \\ x^p \cdot y &= \Phi_p(\zeta_p)a_0 + y = y. \end{aligned}$$

Então, $A \oplus \mathbb{Z}y$ munido com ação definida em (1.9) é um $\mathbb{Z}C_p$-módulo. Aqui, vamos denotar esse módulo por (A, a_0). A classe de isomorfismo de (A, a_0) não depende da escolha de a_0, (Cf. [CR62, §74]).

O próximo teorema nos diz que qualquer $\mathbb{Z}C_p$-reticulado é uma soma direta de módulos do tipo $A, (A, a_0)$ e $\mathbb{Z}$-módulos em que C_p age trivialmente.

Teorema 1.4.5 (Diederichsen–Reiner, [CR62], Thm. 74.3)**.** *Cada $\mathbb{Z}C_p$-reticulado M é isomorfo a uma soma direta*

$$M = \bigoplus_{i=1}^{c} (A_i, a_i) \oplus \bigoplus_{j=c+1}^{c+b} A_j \oplus \mathbb{Z}^a \tag{1.10}$$

onde os $\{A_v\}$ são ideais em $\mathbb{Z}[\zeta_p]$, os $\{a_v\}$ são escolhidos de modo que $a_i \in A_i \setminus (\zeta_p - 1)A_i$ e $\mathbb{Z}^a$ é um $\mathbb{Z}C_p$-módulo trivial de posto a. A classe de isomorfismo de M é determinada pelos inteiros a, b, c e a classe de ideais do produto $A_1 \cdots A_{c+b}$ em $\mathbb{Q}(\zeta_p)$.

Consequentemente, se $B_1, \cdots, B_{h_p}$ são os representantes das h_p classes de ideais distintas de $\mathbb{Q}(\zeta_p)$, temos a seguinte lista completa de $\mathbb{Z}C_p$-reticulados indecomponíveis não isomorfos:

$$(B_1, b_1), \cdots, (B_{h_p}, b_{h_p}), B_1, \cdots, B_{h_p}, \mathbb{Z}$$

onde $b_i \in B_i \smallsetminus (\zeta_p - 1)B_i$, $1 \leq i \leq h_p$.

Observação 1.4.6.

1. *Sejam A e B ideais de $\mathbb{Z}[\zeta_p]$. Então, o $\mathbb{Z}C_p$-módulo $M = A \oplus B$ é isomorfo a $\mathbb{Z}[\zeta_p] \oplus AB$ (Cf. [CR62, p. 514]). Isso mostra que as componentes indecomponíveis de um $\mathbb{Z}C_p$-módulo não são unicamente determinadas.*

2. *Se p é um número primo que não divide n ($n \in \mathbb{Z}$), então*

$$(\mathbb{Z}[\zeta_p], n \cdot 1) \cong (\mathbb{Z}[\zeta_p], 1) \cong \mathbb{Z}C_p$$

é um $\mathbb{Z}C_p$-módulo livre cíclico (Cf. [CR62, p. 512 e p. 514]).

Definição 1.4.7. *Dizemos que um $\mathbb{Z}C_p$-reticulado M é **excepcional** se na decomposição* (1.10) *temos os invariantes $a = 1$ e $c = 0$, isto é, se $M = \bigoplus_{j=1}^{b} A_j \oplus \mathbb{Z}$.*

O teorema a seguir especifica condições suficientes para que um reticulado seja expresso unicamente como uma soma direta finita de submódulos indecomponíveis.

Teorema 1.4.8 (Krull-Schmidt-Azumaya, [CR81], Thm. 6.12)**.** *Sejam R um anel local noetheriano, comutativo e completo e Ω uma R-álgebra finitamente gerada como um R-módulo. Então, um Ω-módulo finitamente gerado M é a soma direta finita de submódulos indecomponíveis. Além disso, se*

$$M = \bigoplus_{i=1}^{r} M_i = \bigoplus_{j=1}^{s} N_j$$

são duas tais somas, então $r = s$ e $M_1 \cong N_{j_1}, \cdots, M_r \cong N_{j_r}$, onde $\{j_1, \cdots, j_r\}$ é alguma permutação de $\{1, \cdots, r\}$.

Observação 1.4.9. *Pela Proposição 1.1.4, temos que $\mathbf{Z}_p$ é um anel local noetheriano, comutativo e completo. Uma vez que $\mathbf{Z}_pC_p$ é uma $\mathbf{Z}_p$-álgebra de grupo gerada por C_p com $\mathbf{Z}_p$-módulo, segue que o Teorema 1.4.8 vale para os $\mathbf{Z}_pC_p$-módulos finitamente gerados.*

Existem apenas três $\mathbf{Z}_pC_p$-módulos indecomponíveis não isomorfos.

Proposição 1.4.10 ([HR62], Thm. 2.6)**.** *Os únicos $\mathbf{Z}_pC_p$-módulos indecomponíveis (a menos de isomorfismo) são $\mathbf{Z}_p, \mathbf{Z}_p[\zeta_p]$ e $\mathbf{Z}_pC_p$.*

Seja M um $\mathbb{Z}C_p$-reticulado. A componente pro-p de $\widehat{M}$ é o $\mathbf{Z}_pC_p$-módulo

$$M_p = M \otimes_{\mathbb{Z}} \mathbf{Z}_p,$$

que é o completamento pro-p de M (Cf. [CR81, §4]).

Proposição 1.4.11 ([HR62], Cor. 1.5)**.** *O $\mathbb{Z}C_p$-módulo M é indecomponível se, e somente se, o correspondente $\mathbf{Z}_pC_p$-módulo M_p for indecomponível.*

Observação 1.4.12. *1. O completamento pro-p de cada ideal não nulo A de $\mathbb{Z}[\zeta_p]$ é isomorfo a $\mathbf{Z}_p[\zeta_p]$ como $\mathbf{Z}_pC_p$-módulos, pois $\mathbf{Z}_p[\zeta_p]$ é um domínio local de ideais principais (Cf. [CR62, §19]).*

2. O completamento pro-p de (A, a_0) é isomorfo a $\mathbf{Z}_pC_p$ como $\mathbf{Z}_pC_p$-módulos, onde A é um ideal não nulo de $\mathbb{Z}[\zeta_p]$. De fato, isto segue das Proposições 1.4.10 e 1.4.11.

Proposição 1.4.13 ([CR81], Prop. 31.2 (ii))**.** *Sejam G um grupo finito e M, N $\mathbb{Z}G$-reticulados. Considere os completamentos pro-q $M_q = M \otimes_{\mathbb{Z}} \mathbf{Z}_q$ e $N_q = N \otimes_{\mathbb{Z}} \mathbf{Z}_q$ de M e N, respectivamente, para todo primo q. Então, $M_q \cong N_q$ como $\mathbf{Z}_qG$-módulos para todos os primos q se, e somente se, $M_p \cong N_p$ como $\mathbf{Z}_pG$-módulos para todos os primos p dividindo $|G|$.*

1.4.2 Reticulados sobre grupos cíclicos de ordem livre de quadrados

Esta subseção é baseada na tese de doutorado de Oppenheim (1962) [Opp62]. Neste trabalho, ele apresenta uma classificação para os $\mathbb{Z}G$-reticulados sobre grupos cíclicos G de ordem livre de quadrados.

Definição 1.4.14. *Um inteiro positivo m é dito ser **livre de quadrados** se não for divisível pelo quadrado de qualquer primo. Em outras palavras, se a fatoração de m em fatores primos é da forma $p_1p_2\cdots p_k$ onde $p_1, \cdots, p_k$ são números primos dois a dois distintos.*

No que segue, exceto menção em contrário, δ sempre denotará um número inteiro positivo livre de quadrados, C_δ um grupo cíclico de ordem δ gerado por x, D_0 é o conjunto de todos os $n \in \mathbb{N}$ que divide δ tal que existe somente um número par de primos distintos

em sua decomposição. Similarmente, D_1 é o conjunto de todos os $n \in \mathbb{N}$ que divide δ tal que existe somente um número ímpar de primos distintos em sua decomposição.

Em $\mathbb{Z}[X]$, definimos

$$s_0(X) := \prod_{d \in D_0} \Phi_d(X), s_1(X) := \prod_{d \in D_1} \Phi_d(X)$$

e $s_i := s_i(x)$, $i = 0, 1$.

Observação 1.4.15. *Temos que $s_0 s_1 = 0$ em $\mathbb{Z}C_\delta$. De fato,*

$$0 = x^\delta - 1 = \prod_{d|\delta} \Phi_d(x) = s_0 s_1$$

em $\mathbb{Z}C_\delta$.

Lema 1.4.16 ([Opp62], Lem. 3.4)**.** *Seja M um $\mathbb{Z}C_\delta$-reticulado. Então,*

$$M_0 = \{m \in M : s_0 m = 0\}$$

e $M_1 := M/M_0$ são $\mathbb{Z}C_\delta$-reticulados.

Em outras palavras, Lema 1.4.16 nos diz que qualquer $\mathbb{Z}C_\delta$-reticulado M define uma extensão

$$E : 0 \to M_0 \to M \to M_1 \to 0$$

de $\mathbb{Z}C_\delta$-reticulados. Pela discussão da Subseção 1.3.1, vemos que as extensões E de M_0 por M_1 são descritas (a menos de isomorfismo) pelo grupo $\mathrm{Ext}^1_{\mathbb{Z}C_\delta}(M_1, M_0)$. Assim, para classificar os $\mathbb{Z}C_\delta$-reticulados, devemos descrever não apenas a estrutura de M_0 e M_1, mas também a do grupo $\mathrm{Ext}^1_{\mathbb{Z}C_\delta}(M_1, M_0)$.

Proposição 1.4.17 ([Opp62], p. 17)**.** *Sejam M_0 e M_1 $\mathbb{Z}C_\delta$-reticulados como no Lema 1.4.16. Então,*

$$M_i \cong \bigoplus_{d \in D_i} \mathcal{M}_d$$

onde $\mathcal{M}_d := t_d M_i$, com $t_d := s_i/\Phi_d(x)$, $i = 0, 1$.

Seja M um $\mathbb{Z}C_\delta$-reticulado. Note que, $s_0 M_0 = 0$. Além disso, para cada $m \in M$, temos que $s_0 s_1 m = 0$, pois $s_0 s_1 = 0$ pela Observação 1.4.15. Assim, $s_1 M \subseteq M_0$ e, consequentemente, $s_1 M_1 = 0$. Logo,

$$\Phi_d(x)\mathcal{M}_d = \Phi_d(x)\frac{s_i}{\Phi_d(x)} M_i = s_i M_i = 0, \quad (i = 0, 1)$$

para cada $d \mid \delta$. Então, $\mathcal{M}_d$ é um $\mathbb{Z}C_\delta/\Phi_d(x)\mathbb{Z}C_\delta$-módulo.

Seja ζ_d uma raiz d-ésima primitiva da unidade. Temos um isomorfismo

$$\frac{\mathbb{Z}C_\delta}{\Phi_d(x)\mathbb{Z}C_\delta} \cong \mathbb{Z}[\zeta_d]$$

dado por $x \mapsto \zeta_d$. Assim, podemos transformar $\mathcal{M}_d$ em um $\mathbb{Z}[\zeta_d]$-módulo definindo $\zeta_d \cdot m := xm, m \in \mathcal{M}_d$. Como $\mathbb{Z}[\zeta_d]$ é um domínio de Dedekind, temos que

$$\mathcal{M}_d \cong I_{1,d} \oplus I_{2,d} \oplus \cdots \oplus I_{r(d),d}$$

onde os $\{I_{j,d}\}$ são ideais em $\mathbb{Z}[\zeta_d]$ (ver [CR81, Thm. 4.13]). Além disso, os invariantes de isomorfismo de $\mathcal{M}_d$ são seu posto $r(d)$ e a classe de ideais do produto $I_{1,d}I_{2,d}\cdots I_{r(d),d}$.

Proposição 1.4.18 ([Opp62], Thm. 4.1 e Cor. 4.8)**.** *Sejam M_0 e M_1 $\mathbb{Z}C_\delta$-reticulados como no Lema 1.4.16. Então,*

$$\mathrm{Ext}^1_{\mathbb{Z}C_\delta}(M_1, M_0) \cong \bigoplus_{(s,t)\in D_1\times D_0} \Lambda(s,t)$$

onde $\Lambda(s,t)$ é o $\mathbb{Z}[\zeta_s]/\Phi_t(\zeta_s)\mathbb{Z}[\zeta_s]$-módulo de matrizes $r(s)\times r(t)$ com entradas em $\mathbb{Z}[\zeta_s]/(\Phi_t(\zeta_s)\mathbb{Z}[\zeta_s])$.

Para simplificar a notação, vamos denotar $\mathbb{Z}[\zeta_s]/(\Phi_t(\zeta_s)\mathbb{Z}[\zeta_s])$ simplesmente por $L(s,t)$. Suponha agora que M é uma extensão de M_0 por M_1 correspondendo para um elemento $\lambda \in \mathrm{Ext}^1_{\mathbb{Z}C_\delta}(M_1, M_0)$. Pela Proposição 1.4.18 podemos escrever

$$\lambda = (\lambda(s_1,t_1), \cdots, \lambda(s_l,t_l)),$$

onde $(s_i,t_i) \in D_1 \times D_0$ e $\lambda(s_i,t_i)$ é uma matriz $r(s_i) \times r(t_i)$ com entradas em $L(s_i,t_i)$, $i = 1, \cdots, l$.

Lema 1.4.19 ([Opp62], Lem. 4.4)**.** *Sejam $s \mid \delta, t \mid \delta$ e $t > s$. Então, $L(s,t)$ é um anel trivial, a menos que exista um primo p tal que $t = ps$. Se $t = ps$, então $L(s,t) = \mathbb{F}_{p,1} \oplus \cdots \oplus \mathbb{F}_{p,v}$, onde $\mathbb{F}_{p,i}$ é um corpo de característica p, $i = 1, \cdots, v$.*

Assim, as entradas $a_{ij} \in L(s,t)$ da matriz $\lambda(s,t)$ podem ser escritas como

$$a_{ij} = (\alpha^1_{ij}, \cdots, \alpha^v_{ij}),$$

onde $\alpha^k_{ij} \in \mathbb{F}_{p,k}$. Então, para $\lambda(s,t)$ corresponde a v-tupla de matrizes $((\alpha^1_{ij}), \cdots, (\alpha^v_{ij}))$. Definimos $\rho_k(\lambda(s,t)) := \mathrm{posto}(\alpha^k_{ij})$.

Precisamos de um pouco mais de notação para enunciar o teorema de classificação dos $\mathbb{Z}C_\delta$-reticulados. Definimos

$$D^* := \{(s,t) : s \mid \delta, t \mid \delta \text{ e } t/s = p, \text{ onde } p \text{ é primo}\}$$

e $D_1^* := \{(s,t) : (s,t) \in D^*, s \in D_1\}$.

Teorema 1.4.20 ([Opp62], Thm. 4.13)**.** *Seja M um $\mathbb{Z}C_\delta$-reticulado. Um conjunto completo de invariantes de isomorfismo consiste de:*

(i) O $\mathbb{Z}C_\delta$-posto de $\mathcal{M}_d$, $r(d)$, para cada $\mathcal{M}_d$ e $d \mid \delta$.

(ii) A classe de ideais do produto $I_{1,d}I_{2,d}\cdots I_{r(d),d}$ associado com $\mathcal{M}_d$, para cada $d \mid \delta$.

(iii) $\{\rho_k(\lambda(s,t)) : (\lambda(s,t)) \in \mathrm{Ext}^1_{\mathbb{Z}G}(M_1, M_0), (s,t) \in D_1^*, k = 1, \cdots, v\}$.

No que segue, $r(d,M)$ e $\lambda(s,t,M)$ denotam $r(d)$ e $\lambda(s,t)$ no $\mathbb{Z}C_\delta$-reticulado M, respectivamente. Além disso, para encurtar a notação, $[I_{\mathcal{M}_d}]$ denota a classe de ideais do produto $I_{1,d}I_{2,d}\cdots I_{r(d),d}$ associado com $\mathcal{M}_d$, para cada $d \mid \delta$.

Por [Opp62, Thm. 7.3] e [CR81, Prop. 31.15] temos a seguinte versão profinita do Teorema 1.4.20.

Teorema 1.4.21. *Sejam M e N $\mathbb{Z}C_\delta$-reticulados. Então, $\widehat{M} \cong \widehat{N}$ como $\widehat{\mathbb{Z}}C_\delta$-módulos se, e somente se,*

(i) $r(d,M) = r(d,N)$ para cada $d \mid \delta$.

(ii) $\rho_k(\lambda(s,t,M)) = \rho_k(\lambda(s,t,N))$ para cada $k = 1, \cdots, v$ e $(s,t) \in D_1^*$.

O cancelamento na soma direta de $\mathbb{Z}C_\delta$-reticulados vale nas seguintes condições.

Proposição 1.4.22 ([Wie84], Prop. 5.1)**.** *Sejam M, N e L $\mathbb{Z}C_\delta$-reticulados. Então,*

$$M \oplus L \cong N \oplus L \text{ implica } M \cong N$$

se, e somente se, $\delta = 6, 10, 14$ ou δ é primo.

O próximo resultado nos diz que cancelamento na soma direta vale para $\widehat{\mathbb{Z}}C_\delta$-módulos.

Proposição 1.4.23. *Sejam M_1, M_2, N_1 e N_2 $\mathbb{Z}C_\delta$-reticulados. Então,*

$$\widehat{M_1} \oplus \widehat{M_2} \cong \widehat{N_1} \oplus \widehat{N_2}$$

se, e somente se,

$$r(d, M_1) + r(d, M_2) = r(d, N_1) + r(d, N_2)$$

e

$$\rho_k(\lambda(s, t, M_1)) + \rho_k(\lambda(s, t, M_2)) = \rho_k(\lambda(s, t, N_1)) + \rho_k(\lambda(s, t, N_2))$$

para cada $d \mid \delta$ *e* $k = 1, \cdots, v$.

Demonstração. Isto segue de [Opp62, Thm. 7.4] e [CR81, Prop. 31.15]. □

1.4.3 Os invariantes de isomorfismo semilinear

Definição 1.4.24. *Seja* G *um grupo finito e sejam* M *e* N $\mathbb{Z}G$*-módulos. Um* ***homomorfismo semilinear*** *de* M *para* N *é um par* (f, φ) *onde* $f : M \to N$ *é um homomorfismo de grupos abelianos e* $\varphi : G \to G$ *é um automorfismo tal que*

$$f(g \cdot m) = \varphi(g) \cdot f(m)$$

para cada $g \in G$ *e* $m \in M$.

Lembre-se que, $[A]$ denota a classe de ideais de um ideal fracionário A de um corpo de números algébricos (ver Definição 1.2.31). Se A é um ideal de $\mathbb{Z}[\zeta_p]$, vamos denotar por $M(a, b, c; [A])$ o único $\mathbb{Z}C_p$-reticulado (a menos de isomorfismo) com invariantes $a, b, c \in \mathbb{Z}$ e $[A]$, isto é,

$$M(a, b, c; [A]) = \bigoplus_{i=1}^{c} (A_i, a_i) \oplus \bigoplus_{j=c+1}^{c+b} A_j \oplus \mathbb{Z}^a$$

onde $A = A_1 \cdots A_{c+b}$ (ver Teorema 1.4.5).

Proposição 1.4.25 ([Cha86], Chap. IV, Thm. 6.2)**.** *Sejam* $M = M(a, b, c; [A])$ *e* $M' = M(a', b', c'; [A'])$ $\mathbb{Z}C_p$*-reticulados. Então,* M *é isomorfo semilinearmente para* M' *se, e somente se,* $a = a', b = b', c = c'$ *e* $\sigma \cdot [A] = [A']$ *para algum* $\sigma \in \mathrm{Gal}(\zeta_p)$.

Mais geral, para grupos cíclicos C_δ de ordem δ livre de quadrados, temos a proposição a seguir.

Proposição 1.4.26. *Sejam* M *e* N $\mathbb{Z}C_\delta$*-reticulados. Então,* M *é isomorfo semilinearmente para* N *se, e somente se,*

(i) $r(d, M) = r(d, N)$ *para cada* $d \mid \delta$.

(ii) $\rho_k(\lambda(s, t, M)) = \rho_k(\lambda(s, t, N))$ *para cada* $k = 1, \cdots, v$ *e* $(s, t) \in D_1^*$.

(iii) $\sigma \cdot [I_{\mathcal{M}_d}] = [J_{\mathcal{N}_d}]$ *para cada* $d \mid \delta$ *e para algum* $\sigma \in \mathrm{Gal}(\zeta_\delta)$.

Demonstração. Sejam M e N $\mathbb{Z}C_\delta$-reticulados. Note que, M é isomorfo semilinearmente para N se, e somente se, $M \cong (N)^\varphi$ (ver Definição 1.3.23) como $\mathbb{Z}C_\delta$-módulos, para algum $\varphi \in \mathrm{Aut}(C_\delta)$. Uma vez que C_δ é um grupo cíclico de ordem δ livre de quadrados, segue pelo Teorema 1.4.20 que $M \cong (N)^\varphi$ como $\mathbb{Z}C_\delta$-módulos se, e somente se,

(i) $r(d, M) = r(d, N)$ para cada $d \mid \delta$.

(ii) $\rho_k(\lambda(s, t, M)) = \rho_k(\lambda(s, t, N))$ para cada $k = 1, \cdots, v$ e $(s, t) \in D_1^*$.

(iii) $I_{\mathcal{M}_d} \cong (J_{\mathcal{N}_d})^\varphi$ como $\mathbb{Z}[\zeta_d]$-módulos para cada $d \mid \delta$ e para algum $\varphi \in \mathrm{Aut}(C_\delta)$ (ver Lema 1.4.4).

Para cada d dividindo δ, vamos denotar por C_d o subgrupo de C_δ de ordem d. Lembre-se que, $\mathrm{Gal}(\zeta_\delta) \cong (\mathbb{Z}/\delta\mathbb{Z})^\times \cong \mathrm{Aut}(C_\delta)$. Assim, para finalizar a prova é suficiente mostrar que $(J_{\mathcal{N}_d})^\varphi \cong \varphi^{-1} \cdot J_{\mathcal{N}_d}$ como $\mathbb{Z}C_\delta$-módulos. Suponha que $\varphi(c) = c^l$ onde $c \in C_d$ e l é um inteiro positivo tal que $(l, \delta) = 1$. Considere a aplicação

$$\begin{aligned} \eta : (J_{\mathcal{N}_d})^\varphi &\to \varphi^{-1} \cdot J_{\mathcal{N}_d} \\ u &\mapsto \varphi^{-1}(u). \end{aligned}$$

É claro que η é um isomorfismo de grupos, assim resta mostrar que η é um $\mathbb{Z}C_d$-homomorfismo. Note que,

$$\begin{aligned} \eta(c \star u) &= \eta(\varphi(c) \cdot u) \\ &= \varphi^{-1}(c^l \cdot u) \\ &= \varphi^{-1}(\zeta_d^l u) \\ &= \varphi^{-1}(\zeta_d^l)\varphi^{-1}(u) \\ &= \zeta_d \varphi^{-1}(u) \\ &= c \cdot \eta(u) \end{aligned}$$

onde $c \in C_d$ e "$\star$" denota a C_d-ação em $(J_{\mathcal{N}_d})^\varphi$. Isto conclui a prova da Proposição 1.4.26. □

1.5 Grupos de Bieberbach

Seja $\mathbb{R}^n$ o espaço Euclidiano de dimensão n. Uma **isometria** de $\mathbb{R}^n$ é uma função $f : \mathbb{R}^n \to \mathbb{R}^n$ que preserva distância em relação à métrica Euclidiana. Exemplos interes-

santes de isometrias são os operadores ortogonais em $\mathbb{R}^n$, isto é, transformações lineares invertíveis de $\mathbb{R}^n$ para $\mathbb{R}^n$ que preservam o produto interno. O conjunto de tais operadores forma um subgrupo $O(n)$ do grupo de todas as transformações lineares invertíveis de $\mathbb{R}^n$ para $\mathbb{R}^n$. Usando a identificação matricial, temos que $O(n)$ é um subgrupo do grupo linear geral real $\mathrm{GL}(n,\mathbb{R})$.

Vamos denotar o conjunto de todas isometrias de $\mathbb{R}^n$ por $\mathrm{Isom}(\mathbb{R}^n)$. Então,

Proposição 1.5.1 ([Cha86], Chap. I). *(i)* $\mathrm{Isom}(\mathbb{R}^n)$ *é um grupo com respeito à composição de funções.*

(ii) O grupo $\mathrm{Isom}(\mathbb{R}^n)$ *cinde como o produto semidireto* $\mathbb{R}^n \rtimes O(n)$.

Observe que $\mathrm{Isom}(\mathbb{R}^n) \subseteq \mathbb{R}^n \rtimes \mathrm{GL}(n,\mathbb{R})$. Seja $(a,A) \in \mathbb{R}^n \rtimes \mathrm{GL}(n,\mathbb{R})$. Temos uma matriz $(n+1)\times(n+1)$

$$\begin{pmatrix} 1 & 0 \\ a & A \end{pmatrix}$$

que obviamente define uma inclusão $\mathbb{R}^n \rtimes \mathrm{GL}(n,\mathbb{R}) \subseteq \mathrm{GL}(n+1,\mathbb{R})$. Assim, podemos considerar $\mathrm{Isom}(\mathbb{R}^n)$ como um espaço topológico com a topologia induzida do espaço Euclidiano $\mathbb{R}^{(n+1)^2}$. O grupo $\mathbb{R}^n \rtimes \mathrm{GL}(n,\mathbb{R})$ é conhecido como **grupo afim** e comumente é denotado por $\mathrm{Aff}(\mathbb{R}^n)$.

Seja Γ um subgrupo de $\mathrm{Isom}(\mathbb{R}^n)$. O espaço das órbitas da ação de Γ em $\mathbb{R}^n$, via isometria, é o conjunto das Γ-órbitas $\mathbb{R}^n/\Gamma = \{\Gamma x : x \in \mathbb{R}\}$ munido com a topologia quociente de $\mathbb{R}^n$.

Definição 1.5.2. *Dizemos que um subgrupo* Γ *de* $\mathrm{Isom}(\mathbb{R}^n)$ *é um* ***grupo cristalográfico*** *de dimensão* n *se* Γ *é discreto e* $\mathbb{R}^n/\Gamma$ *é compacto. Se, além disso,* Γ *for livre de torção, dizemos que* Γ *é um* ***grupo de Bieberbach*** *de dimensão* n.

Se Γ é um grupo de Bieberbach de dimensão n, então o espaço $\mathbb{R}^n/\Gamma$ é uma variedade plana compacta com grupo fundamental Γ. Na verdade, todas as variedades planas compactas são obtidas desta forma (ver [Cha86, Chap. II, Cor. 5.1]). Assim, grupos de Bieberbach são exatamente os grupos fundamentais das variedades planas compactas.

Exemplo 1.5.3. *1. Sejam* $e_1,\cdots,e_n$ *a base canônica de* $\mathbb{R}^n$. *Seja* Γ *o subgrupo discreto de* $\mathrm{Isom}(\mathbb{R}^n)$ *gerado por* $(e_1,I),\cdots,(e_n,I)$. *Então* $\Gamma \cong \mathbb{Z}^n$ *é um grupo de Bieberbach de dimensão* n *e o espaço das órbitas* $\mathbb{R}^n/\Gamma$ *é o toro* n*-dimensional.*

2. Seja $\Gamma \leq \mathrm{Isom}(\mathbb{R}^n)$ *gerado por*

$$\left(\begin{pmatrix} 0 \\ 1/2 \end{pmatrix}, B\right), \quad \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, I\right)$$

onde

$$B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Então Γ *é um grupo de Bieberbach de dimensão* 2 *cuja o espaço das órbitas* $\mathbb{R}^2/\Gamma$ *é a garrafa de Klein.*

3. *O subgrupo discreto* Γ *de* $\mathrm{Isom}(\mathbb{R})$ *gerado por* $(1, 1)$ *e* $(0, -1)$ *é um grupo cristalográfico de dimensão* 1 *que não é livre de torção, em outras palavras,* Γ *não é um grupo de Bieberbach. Note que* $\Gamma \cong \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ *é isomorfo ao grupo diedral infinito* $\mathcal{D}_\infty$.

Grupos cristalográficos são bem conhecidos por causa dos trabalhos de Bieberbach, que apresentam uma bonita descrição para esses grupos. A seguir, vamos enunciar três famosos teoremas, comumente conhecidos como Teoremas de Bieberbach, que foram provados em 1910 e 1912 por Bieberbach e Fröbenius.

Teorema 1.5.4 (Primeiro Teorema de Bieberbach, 1910)**.** *Seja* Γ *um grupo cristalográfico de dimensão* n*. Então,* $M = \Gamma \cap (\mathbb{R}^n \times \{I\})$ *é um reticulado de* $\mathbb{R}^n$ *e* Γ/M *é um grupo finito.*

Em particular, o Teorema 1.5.4 nos diz que qualquer grupo cristalográfico define uma sequência exata

$$1 \to M \to \Gamma \to G \to 1, \tag{1.11}$$

onde $M \cong \mathbb{Z}^n$ é abeliano maximal em Γ e G é um grupo finito. Os grupos M e G são conhecidos como o **subgrupo de translações** e o **grupo de holonomia** de Γ, respectivamente. Reciprocamente,

Proposição 1.5.5 ([Szc12], Thm. 2.2)**.** *Um grupo* Γ *é isomorfo a um grupo cristalográfico de dimensão* n *se, e somente se,* Γ *tem um subgrupo normal abeliano livre* $\mathbb{Z}^n$ *de índice finito que é um subgrupo abeliano maximal de* Γ.

Proposição 1.5.6 ([Cha86], Chap. I, Prop. 4.1)**.** *O subgrupo de translações de um grupo cristalográfico* Γ *é o único subgrupo abeliano maximal normal de índice finito de* Γ.

Usando a sequência exata (1.11), vimos na Subseção 1.3.2 que podemos definir uma representação $\rho : G \to \mathrm{Aut}(M) \cong \mathrm{GL}(n, \mathbb{Z})$ do grupo de holonomia G por

$$\rho(g)(m) = l(g)ml(g)^{-1}, \quad (g \in G \text{ e } m \in M)$$

onde $l : G \to \Gamma$ é um levantamento. Como M é abeliano maximal em Γ, temos que ρ é uma representação fiel, isto é, ρ é injetiva. Consequentemente, ρ induz uma estrutura de $\mathbb{Z}G$-módulo fiel em M (ver Proposição 1.3.20).

Teorema 1.5.7 (Segundo Teorema de Bieberbach, 1912)**.** *Sejam Γ e Γ' grupos cristalográficos de dimensão n. Se $f : \Gamma \to \Gamma'$ é um isomorfismo, então existe um elemento $\alpha \in \mathrm{Aff}(\mathbb{R}^n)$ tal que $f(\gamma) = \alpha^{-1}\gamma\alpha$ para cada $\gamma \in \Gamma$.*

Como consequência deste teorema, podemos deduzir que duas variedades planas compactas com grupos fundamentais isomorfos são difeomorfas. Em outras palavras, variedades planas compactas são completamente determinadas pelo seu grupo fundamental, a menos de difeomorfismo.

Teorema 1.5.8 (Terceiro Teorema de Bieberbach (ou Teorema de Fröbenius), 1912)**.** *A menos de conjugação em $\mathrm{Aff}(\mathbb{R}^n)$, existe apenas um número finito de grupos cristalográficos de dimensão n.*

Consequentemente, a menos de difeomorfismo, há apenas um número finito de variedades planas compactas de dimensão n. A seguinte tabela foi extraída de [Cha86, p. 41].

NÚMERO DE GRUPOS CRISTALOGRÁFICOS		
Dimensão	# Grupos Cristalográficos	# Grupos de Bierberbach
1	1	1
2	17	2
3	219	10
4	4783	74

1.5.1 Um esquema geral para a classificação de grupos de Bieberbach

Se Γ é um grupo de Bieberbach, então Γ define uma sequência exata

$$1 \to M \to \Gamma \to G \to 1, \tag{1.12}$$

onde M é abeliano livre e abeliano maximal em Γ e G é um grupo finito. Vimos que a sequência (1.12) induz uma estrutura de $\mathbb{Z}G$-módulo em M. Além disso, pela Proposição 1.3.22 as extensões (1.12) são descritas pelos elementos de $H^2(G, M)$. Logo, é natural usar a linguagem das teorias de representações e cohomologia de grupos finitos para classificar os grupos cristalográficos. Para esse fim, Charlap [Cha65] propõe o seguinte algoritmo para classificar os grupos de Bieberbach com grupo de holonomia G.

(1) Encontrar todos os $\mathbb{Z}G$-reticulados fiéis M.

(2) Encontrar todas as extensões de M por G, isto é, calcular $H^2(G, M)$.

(3) Determinar quais dessas extensões são livres de torção.

(4) Ver quais dessas extensões são isomorfas.

A etapa (1) é a mais difícil, pois não existe, em geral, uma classificação para os $\mathbb{Z}G$-reticulados para todas as classes de grupos finitos G. Na Seção 1.4, listamos algumas classes de grupos finitos G para a qual uma classificação dos $\mathbb{Z}G$-reticulados é conhecida.

A etapa (3) reduz-se à determinação das classes especiais de $H^2(G, M)$ (ver Definição 1.3.26), em virtude do seguinte resultado.

Proposição 1.5.9 ([Cha86], Chap. III, Thm. 2.1)**.** *Seja M um $\mathbb{Z}G$-módulo. A extensão de M por G, correspondente a $\alpha \in H^2(G, M)$, é livre de torção se, e somente se, α é especial.*

Já a etapa (4), pode ser examinada por meio do seguinte resultado, que estabelece uma condição necessária e suficiente para duas extensões serem isomorfas.

Proposição 1.5.10 ([Cha86], Chap. III, Thm. 2.2)**.** *Sejam M e N $\mathbb{Z}G$-módulos fiéis e sejam $\alpha \in H^2(G, M)$ e $\beta \in H^2(G, N)$. Suponha que Γ (resp. Π) é uma extensão correspondente para α (resp. β). Então, Γ é isomorfo a Π se, e somente se, existe um isomorfismo semilinear $(f, \varphi) : M \to N$ tal que $f_*(\alpha) = \varphi_*(\beta)$.*

Analisando esse algoritmo, vemos que os grupos de holonomia são peças importantes para a classificação dos grupos de Bieberbach, tanto que, não seria redundante acrescentar a esse algoritmo uma etapa zero, como:

(0) Encontrar todos os grupos finitos que podem ser realizados como um grupo de holonomia de um grupo de Bieberbach.

A etapa (0) foi respondida, em parte, por Auslander e Kuranishi [AK57] em 1957, que deram a seguinte resposta surpreendente para esse problema.

Teorema 1.5.11 ([Cha86], Chap. III, Thm. 5.2)**.** *Seja G qualquer grupo finito. Então G é grupo de holonomia de algum grupo de Bieberbach.*

Note que, o Teorema 1.5.11 não dá informação em relação a dimensão em que o grupo finito G pode aparecer como grupo de holonomia. Assim, temos uma resposta parcial para a etapa (0). Em particular, Hiller (1985) [Hil85] estabeleceu uma cota inferior para a dimensão de um grupo cristalográfico em função da ordem dos elementos do grupo de holonomia. Antes de apresentar esse resultado, vamos relembrar alguns conceitos.

A versão aditiva da função totiente de Euler $\varphi(\cdot)$ é a seguinte.

Definição 1.5.12. *Uma função $\Phi(\cdot)$ que satisfaz as condições*

(i) se p é primo, então $\Phi(p^k) = \varphi(p^k) = p^k - p^{k-1} = p^k(1-1/p)$, para todo $k \in \mathbb{N}$.

(ii) se r e s são relativamente primos, então

$$\Phi(rs) = \Phi(r) + \Phi(s),$$

a menos que $s = 2$ e r é um número ímpar, caso em que $\Phi(2r) = \Phi(r)$.

é chamada a ***versão aditiva da função de Euler****.*

Agora, considere a seguinte função

$$g(m) := \text{menor } n \text{ tal que } \mathrm{GL}(n,\mathbb{Z}) \text{ contém uma matriz de ordem } m.$$

O próximo resultado é conhecido como o teorema da restrição cristalográfica.

Teorema 1.5.13 ([Hil85], Prop. 1.3 e Thm. 1.5)**.** *(i) $g(m)$ é a menor dimensão de um grupo cristalográfico cujo grupo de holonomia contém um elemento de ordem m.*

(ii) $g(m) = \Phi(m)$.

Para um número natural n fixado, $\mathrm{Ord}(n)$ denota o conjunto de todos os números naturais que ocorre como ordem de um elemento no grupo de holonomia de grupos cristalográficos de dimensão n.

Pelo Teorema 1.5.13,

$$\mathrm{Ord}(n) = \{m : \Phi(m) \leq n\}.$$

O próximo resultado é uma consequência imediata do Teorema 1.5.13.

Corolário 1.5.14. *Seja Γ um grupo cristalográfico com grupo de holonomia de ordem p. Então, o posto do subgrupo abeliano maximal normal de Γ é pelo menos $p-1$.*

Agora, o Teorema 1.5.11 com o Teorema 1.5.13 dá uma resposta mais completa para a etapa (0).

1.5.2 A classificação de Charlap

Em 1965, Charlap [Cha65], combinando as quatro etapas do algoritmo da subseção anterior com a linguagem de categorias, obteve uma bonita classificação para os grupos de Bieberbach com o grupo de holonomia cíclico C_p de ordem prima p. Ele define $\mathcal{E}(C_p)$ como a categoria cujos objetos são todos os pares (M, α), onde M é um $\mathbb{Z}C_p$-módulo e α é um elemento especial de $H^2(C_p, M)$, isto é, um elemento não nulo. Os morfismos dessa categoria são todas as aplicações $(M, \alpha) \to (N, \beta)$ dadas pelos pares (f, φ) onde

(i) (f, φ) é um homomorfismo semilinear de M para N.

(ii) $f_*(\alpha) = \varphi_*(\beta) \in H^2(C_p, (N)^\varphi)$.

Recorde-se de que, $(N)^\varphi$ é o $\mathbb{Z}C_p$-módulo com grupo N e ação "$\star$" dada por $x \star n := \varphi(x)n$. Por brevidade, escreveremos H-grupo de Bieberbach para significar um grupo de Bieberbach de dimensão n com grupo de holonomia H.

Usando a classificação de Reiner para representações integrais dos grupos cíclicos de ordem prima, Charlap provou que a classe de isomorfismo de um C_p-grupo de Bieberbach é completamente determinada pela estrutura do $\mathbb{Z}C_p$-módulo associado.

Proposição 1.5.15 ([Cha86], Chap. IV, Thm. 6.1)**.** *Seja M um $\mathbb{Z}C_p$-módulo e sejam α e α' classes não nulas em $H^2(C_p, M)$. Então, existe um C_p-automorfismo $f : M \to M$ com $f_*(\alpha) = \alpha'$ se, e somente se, M é um $\mathbb{Z}C_p$-módulo não excepcional ou $\alpha' = \pm\alpha$ se M é um $\mathbb{Z}C_p$-módulo excepcional.*

Definição 1.5.16. *Um C_p-grupo de Bieberbach Γ é **excepcional** se seu subgrupo abeliano maximal normal M é um $\mathbb{Z}C_p$-módulo excepcional.*

No caso não excepcional, Charlap obteve o seguinte conjunto de invariantes para a classe de isomorfismo de um C_p-grupo de Bieberbach.

Teorema 1.5.17 ([Cha86], Chap. IV, Thm. 6.3)**.** *Existe uma correspondência biunívoca entre as classes de isomorfismo de C_p-grupos de Bieberbach não excepcionais e as 4-tuplas $(a, b, c; \theta)$ onde $a, b, c \in \mathbb{Z}$ com $a > 0, b \geq 0, c \geq 0, (a, c) \neq (1, 0), (b, c) \neq (0, 0)$ e $\theta \in \mathrm{Gal}(\zeta_p)\backslash H(\mathbb{Z}[\zeta_p])$.*

Em outras palavras, Teorema 1.5.17 nos diz que dois C_p-grupos de Bieberbach não excepcionais são isomorfos se, e somente se, seus subgrupos de translações são isomorfos como $\mathbb{Z}C_p$-módulos (ver Proposição 1.4.25).

Agora, para o caso em que o C_p-grupo de Bieberbach é excepcional, ele obteve o seguinte conjunto de invariantes de isomorfismo.

Teorema 1.5.18 ([Cha86], Chap. IV, Thm. 6.4 ou [Cha65], Thm. 3.7)**.** *Existe uma correspondência biunívoca entre as classes de isomorfismo de grupos de Bieberbach excepcionais cujo o grupo de holonomia tem ordem prima p e os pares (b, θ) onde $b \in \mathbb{Z}, b > 0$ e $\theta \in C_2\backslash H(\mathbb{Z}[\zeta_p])$.*

Observação 1.5.19. *No caso excepcional, o Teorema 1.5.18 nos diz que a classe de isomorfismo de um C_p-grupo de Bieberbach é determinada pela estrutura do $\mathbb{Z}C_p$-módulo associado até um automorfismo por inversão de C_p. Mais especificamente, se pensarmos os C_p-grupos de Bieberbach excepcionais Γ e Γ' como uma tripla (b, A, α) e (b', A', α'), respectivamente, com $b, b' \in \mathbb{Z}$, A e A' são classes de ideais em $H(\mathbb{Z}[\zeta_p])$ e $\alpha \in H^2(C_p, M(1, b, 0; A))$, $\alpha' \in H^2(C_p, M(1, b', 0; A'))$. Então, pela Proposição 1.4.25 temos que os correspondentes subgrupos de translações são isomorfos como módulos se, e somente se, $b = b'$ e $A = A'$. Agora, pelo Teorema 1.5.18, $\Gamma \cong \Gamma'$ se, e somente se, existe $\varphi \in \mathrm{Gal}(\zeta_p)$ com $\varphi \cdot A = A'$ e $\varphi_*(\alpha') = \pm\alpha$.*

1.5.3 O método de classificação de Auslander-Vasquez

O principal resultado desta seção, conhecido como *o método de classificação de Auslander – Vasquez*, foi em sua essência conjecturado por Auslander e provado por Vasquez em 1970, com algumas ideias dadas por Auslander.

Teorema 1.5.20 ([Vas70], Thm. 3.6)**.** *Seja G um grupo finito. Então, existe um inteiro positivo $n(G)$ com a seguinte propriedade: se Γ é um grupo de Bieberbach com o grupo de holonomia isomorfo a G, então o subgrupo de translações $M \leq \Gamma$ contém um subgrupo normal M' tal que Γ/M' é um grupo de Bieberbach de dimensão $\leq n(G)$.*

Esse teorema sugere o seguinte método de classificação para grupos de Bieberbach com um dado grupo de holonomia G:

Método de classificação de Auslander-Vasquez: *qualquer grupo de Bieberbach Γ com grupo de holonomia G e dimensão $n \geq n(G)$ pode ser definido por uma sequência exata*

$$1 \to \mathbb{Z}^{(n-n(G))} \to \Gamma \to \Gamma_G \to 1,$$

onde Γ_G é um grupo de Bieberbach de dimensão $n(G)$.

O número $n(G)$ é chamado de **invariante de Vasquez** de um grupo finito G. Usando [Szc97, Thm. 3] podemos caracterizar $n(G)$ de forma puramente algébrica.

Definição 1.5.21. *Seja M um $\mathbb{Z}G$-reticulado. Dizemos que um $\mathbb{Z}G$-reticulado L tem a propriedade $\mathcal{S}$, quando para cada elemento especial $\alpha \in H^2(G, M)$ existe um $\mathbb{Z}G$-homomorfismo $f : M \to L$ tal que $f_*(\alpha) \in H^2(G, L)$ é especial.*

Proposição 1.5.22. *O invariante de Vasquez de um grupo finito G é igual a*

$$n(G) = min\{\mathbb{Z}\text{-posto}(N) \ : \ N \text{ é um } \mathbb{Z}G\text{-reticulado com a propriedade } \mathcal{S}\}.$$

O Teorema 1.5.20 sugere a seguinte questão.

Questão. *Calcule o invariante de Vasquez $n(G)$ para um grupo finito G.*

Essa questão está em aberto, com exceção se G é um p-grupo finito, que foi calculado por Cliff and Weiss em 1989 [CW89] e se G é um grupo cíclico finito com ordem livre de quadrados, que foi calculado por Szczepasńki em 1997, que obteve o seguinte resultado.

Teorema 1.5.23 ([Szc97], Thm. 2)**.** *$n(G) = 1$ se, e somente se, G é um grupo cíclico com ordem livre de quadrados.*

A combinação dos Teoremas 1.5.20 e 1.5.23, nos dá a seguinte caracterização para os grupos de Bieberbach com grupo de holonomia cíclico de ordem livre de quadrados.

Proposição 1.5.24. *Seja Γ um grupo de Bieberbach de dimensão n com o grupo de holonomia cíclico G de ordem livre de quadrados δ e subgrupo de translações M. Então, $M = M_{n-1} \oplus \mathbb{Z}$ admite uma $\mathbb{Z}G$-decomposição, onde $\mathbb{Z}$ é um módulo trivial gerado pela δ-ésima potência de algum elemento c de Γ e $\Gamma = M_{n-1} \rtimes C$ com $C = \langle c \rangle$.*

Demonstração. Uma vez que G é um grupo cíclico de ordem livre de quadrados, temos que $n(G) = 1$ pelo Teorema 1.5.23. Assim, pelo método de classificação de Auslander-Vasquez, Γ é definido pela sequência exata

$$1 \to M_{n-1} \to \Gamma \xrightarrow{\pi} \mathbb{Z} \to 1 \tag{1.13}$$

onde $M_{n-1} \cong \mathbb{Z}^{n-1}$. Note que esta extensão cinde, pois para qualquer $\gamma \in \Gamma$ tal que $\pi(\gamma) = 1 \in \mathbb{Z}$ a aplicação $s : \mathbb{Z} \to \Gamma$ definida por $s(m) = \gamma^m$ é um homomorfismo com $\pi \circ s = \mathrm{id}_{\mathbb{Z}}$. Portanto, $\Gamma = M_{n-1} \rtimes C$ onde C é um grupo cíclico infinito gerado por algum elemento c de Γ que age em M_{n-1} como G. Além disso, M admite a $\mathbb{Z}G$-decomposição $M_{n-1} \oplus \mathbb{Z}$ onde $\mathbb{Z}$ é um módulo trivial gerado pela δ-ésima potência de c. □

1.5.4 A classificação via classes cristalográficas

Vimos na Subseção 1.5.1 que os parâmetros naturais para classificar grupos cristalográficos são: o grupo de holonomia G e o $\mathbb{Z}G$-reticulado M.

Definição 1.5.25. *Fixe um $\mathbb{Z}G$-reticulado fiel M para um grupo finito G. Definimos a* ***classe cristalográfica*** *(G, M) como sendo o conjunto de todas as extensões Γ de M por G. Além disso, diremos que duas classes cristalográficas (G, M) e (G', M') são* ***aritmeticamente equivalentes*** *se existem isomorfismos $\phi : M \to M'$ e $\varphi : G \to G'$ tais que*

$$\phi(g \cdot m) = \varphi(g) \cdot \phi(m)$$

para cada $m \in M$ e $g \in G$. Equivalentemente, as classes cristalográficas (G, M) e (G', M') são aritmeticamente equivalentes se G e G' são subgrupos conjugados de $\mathrm{GL}(n, \mathbb{Z})$. As classes de equivalência resultantes são as ***classes cristalográficas aritméticas****.*

Observação 1.5.26 (Uma caracterização para as classes cristalográficas)**.** *Sejam $M = \mathbb{Z}^n$ um grupo abeliano livre e G um grupo finito. Seja $\rho : G \to \mathrm{GL}(n, \mathbb{Z})$ uma representação fiel e considere o produto semidireto*

$$G_\rho = M \rtimes_\rho G.$$

Note que, a representação $\rho : G \to \mathrm{GL}(n, \mathbb{Z})$ e grupo finito G definem uma classe cristalográfica (G, M). Logo, os grupos G_ρ podem ser associados para as classes cristalográficas (G, M). Reciprocamente, dada uma classe cristalográfica (G, M), temos por definição uma representação fiel $\rho : G \to \mathrm{GL}(n, \mathbb{Z})$, consequentemente, podemos definir um produto semidireto $G_\rho = M \rtimes_\rho G$. Assim, as classes cristalográficas (G, M) podem ser associadas

para os grupos G_ρ. Isso mostra que existe uma correspondência biunívoca entre o conjunto formado por todos os grupos G_ρ e o conjunto formado por todas as classes cristalográficas (G, M). Além disso, por [GZ11, Prop. 2.17] temos que duas classes cristalográficas são aritmeticamente equivalentes se os correspondentes produtos semidiretos são grupos isomorfos.

Lema 1.5.27. *Grupos cristalográficos isomorfos determinam a mesma classe cristalográfica aritmética.*

Demonstração. Sejam Γ_1 e Γ_2 grupos cristalográficos de dimensão n com grupos de holonomia H_1, H_2 e subgrupos de translações M_1, M_2, respectivamente. Suponha que $F : \Gamma_1 \to \Gamma_2$ é um isomorfismo. Pela Proposição 1.5.6, $F(M_1) = M_2$. Como M_1 e M_2 são grupos abelianos livres de mesmo posto, segue que a restrição de F para M_1, que denotaremos por f, é um isomorfismo de M_1 para M_2. Consequentemente, F induz um isomorfismo $\varphi : H_1 \to H_2$ de modo que o diagrama

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M_1 & \longrightarrow & \Gamma_1 & \xrightarrow{\pi_1} & H_1 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & M_2 & \longrightarrow & \Gamma_2 & \xrightarrow{\pi_2} & H_2 & \longrightarrow & 1. \end{array}$$

é comutativo. Suponha que $\pi_1(\gamma_1) = h_1 \in H_1$. Por definição de φ, temos que $\pi_2(F(\gamma_1)) = \varphi(h_1)$. Logo,

$$f(h_1 \cdot m) = F(\gamma_1^{-1} m \gamma_1) = F(\gamma_1)^{-1} F(m) F(\gamma_1) = \varphi(h_1) \cdot f(m), \tag{1.14}$$

onde $m \in M$. Note que, a equação (1.14) nos diz que $f H_1 f^{-1} = H_2$ em $\mathrm{GL}(n, \mathbb{Z})$. Portanto, Γ_1 e Γ_2 determinam a mesma classe cristalográfica aritmética. □

Lema 1.5.28. *Sejam (H, M) e (H', M') classes cristalográficas aritmeticamente equivalentes. Então, para cada grupo cristalográfico Γ em (H, M) existe um grupo isomorfo Γ' em (H', M').*

Demonstração. Seja Γ um grupo cristalográfico na classe cristalográfica (H, M). Seja $\xi : H \times H \to M$ um 2-cociclo correspondente para a extensão

$$1 \to M \to \Gamma \to H \to 1,$$

e considere Γ como sendo $M \times H$ com a multiplicação

$$(m_1, h_1)(m_2, h_2) = (m_1 + h_1 m_2 + \xi(h_1, h_2), h_1 h_2),$$

onde $m_1, m_2 \in M$ e $h_1, h_2 \in H$. Uma vez que (H, M) e (H', M') são aritmeticamente equivalentes, existem isomorfismos $\varphi : H \to H'$ e $f : M \to M'$ tais que

$$f(h \cdot m) = \varphi(h) \cdot f(m),$$

para todos $h \in H$ e $m \in M$. Agora, defina a função $F : M \times H \to M' \times H'$ por

$$F(m, h) = (f(m), \varphi(h)),$$

para $m \in M$ e $h \in H$. Vamos mostrar que F é um isomorfismo. Como f e φ são bijeções, temos que F também é. Assim, resta mostrar que F é um homomorfismo. Note que,

$$\begin{aligned}
F[(m_1, h_1)(m_2, h_2)] &= F(m_1 + h_1 m_2 + \xi(h_1, h_2), h_1 h_2) \\
&= (f(m_1) + \varphi(h_1) f(m_2) + f(\xi(h_1, h_2)), \varphi(h_1)\varphi(h_2)) \\
&= (f(m_1) + \varphi(h_1) f(m_2) + f(\xi(f^{-1} f h_1 f^{-1} f, f^{-1} f h_2 f^{-1} f)), \varphi(h_1)\varphi(h_2)) \\
&= (f(m_1) + \varphi(h_1) f(m_2) + f(\xi(f^{-1}\varphi(h_1) f, f^{-1}\varphi(h_2) f)), \varphi(h_1)\varphi(h_2)) \\
&= (f(m_1) + \varphi(h_1) f(m_2) + \xi'(\varphi(h_1), \varphi(h_2)), \varphi(h_1)\varphi(h_2)) \\
&= (f(m_1), \varphi(h_1))(f(m_2), \varphi(h_2)) \\
&= F(m_1, h_1) F(m_2, h_2),
\end{aligned}$$

onde $\xi'(\varphi(h_1), \varphi(h_2)) = f(\xi(f^{-1}\varphi(h_1) f, f^{-1}\varphi(h_2) f))$ é um 2-cociclo de $H' \times H'$ para M'. Portanto, F é um homomorfismo e, consequentemente, um isomorfismo. Assim, $\Gamma' := F(\Gamma)$ é um grupo cristalográfico na classe cristalográfica (H', M') isomorfo a Γ. □

Observação 1.5.29. *Segue dos Lemas 1.5.27 e 1.5.28 que para encontrar todos os grupos cristalográficos (a menos de isomorfismo) de uma classe cristalográfica aritmética é suficiente encontrar todos os possíveis grupos cristalográficos de um representante de tal classe.*

Seja Γ um grupo cristalográfico de dimensão n definindo a sequência exata

$$1 \to M \to \Gamma \to G \to 1. \tag{1.15}$$

Então, Γ define uma classe cristalográfica (G, M). Para caracterizar todas as classes de isomorfismos de grupos cristalográficos em (G, M), precisamos definir uma ação de $\mathcal{N}_{\mathrm{Aut}(M)}(G)$, o normalizador de G em $\mathrm{Aut}(M)$, em $H^2(G, M)$. Seja $\phi \in \mathcal{N}_{\mathrm{Aut}(M)}(G)$ e defina $\phi' \in \mathrm{Aut}(G)$ por

$$\phi'(g) = \phi^{-1} g \phi,$$

para cada $g \in G$. Seja $c : G \times G \to M$ um 2-cociclo correspondendo para extensão (1.15). Então, $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ age em $H^2(G, M)$ pela fórmula

$$[\phi \circledast c](g, h) = \phi[c(\phi'(g), \phi'(h))], \tag{1.16}$$

para $g, h \in G$ (Cf. [Cha86, p. 168]). A seguir, veremos um caso particular desta ação.

Seja M um $\mathbb{Z}C_p$-reticulado para um grupo cíclico $C_p = \langle x \rangle$ de ordem prima p. Pelo Teorema 1.4.5, $M = M_1 \oplus M_2$ onde M_1 é o maior somando direto de M em que C_p age trivialmente. Consequentemente, $H^2(C_p, M) \cong \bar{M}_1$ pela Proposição 1.3.14. Então, temos a ação "$\bullet$" de $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ em $H^2(C_p, M)$, definida em (2) na introdução desta tese. Recordemos essa definição.

Para um elemento $n \in \mathcal{N}_{\mathrm{Aut}(M)}(C_p)$, denotemos por $\tilde{n}$ sua imagem natural em $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ sobre a identificação $\mathrm{Aut}(C_p) \cong \mathbb{F}_p^*$. O normalizador $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ age de forma natural no conjunto dos elementos fixados M^{C_p} sobre a ação de C_p em M. Isto induz a ação de $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ em $\bar{M}^{C_p}$ e, consequentemente, $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ age em $\bar{M}^{C_p}/\Delta \cdot \bar{M} \cong \bar{M}_1$, onde $\Delta = 1 + x + \cdots + x^{p-1}$.

Definimos uma nova ação "$\bullet$" do normalizador $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ em $\bar{M}_1$ por

$$n \bullet m := n \cdot \tilde{n} m, \quad (m \in \bar{M}_1) \tag{1.17}$$

onde "$\cdot$" denota a ação de $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ em $\bar{M}_1$ descrita no parágrafo anterior.

Observação 1.5.30. *Afirmamos que as ações "$\circledast$" e "$\bullet$", de $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ em $H^2(C_p, M)$, são iguais neste caso. De fato, seja $\phi \in \mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ e defina $\tilde{\phi} \in \mathrm{Aut}(C_p)$ por $\tilde{\phi}(x) = \phi^{-1} x \phi$. Note que, se $c : C_p \times C_p \to M$ é um 2-cociclo, então*

$$[\tilde{\phi}_{\#}(c)](x, y) = c(\tilde{\phi}(x), \tilde{\phi}(y)) \tag{1.18}$$

e

$$[\phi_{\#}(c)](x, y) = \phi(c(x, y)), \tag{1.19}$$

para $x, y \in C_p$, definem homomorfismos

$$\tilde{\phi_*} : H^2(C_p, M) \to H^2(C_p, M) \quad e \quad \phi_* : H^2(C_p, M) \to H^2(C_p, M),$$

respectivamente, pela Proposição 1.3.24. Desse modo, a ação "$\circledast$" definida em (1.16) *pode ser reescrita como*

$$\phi \circledast \alpha = \phi_*(\tilde{\phi}_*(\alpha)), \tag{1.20}$$

onde $\alpha \in H^2(C_p, M)$. *Por outro lado, como* $H^2(C_p, M) \cong \bar{M}_1$, *a ação "*$\bullet$*" definida em* (2) *pode ser reescrita como*

$$\phi \bullet m = \phi \cdot \tilde{\phi} m = \phi_*(\tilde{\phi}_*(m)), \tag{1.21}$$

onde $m \in \bar{M}_1$. *Portanto, de* (1.20) *e* (1.21) *vemos que a ação "*$\circledast$*", definida em* (1.16), *é igual à ação "*$\bullet$*", definida em* (2), *neste caso.*

Teorema 1.5.31 ([Hil86], Thm. 5.2)**.** *Existe uma correspondência biunívoca entre as classes de isomorfismo de grupos cristalográficos na classe cristalográfica* (G, M) *e as órbitas da ação de* $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ *em* $H^2(G, M)$.

Em particular, se $X(G, M)$ é o subconjunto de $H^2(G, M)$ formado por todos os elementos especias, temos:

Corolário 1.5.32. *Existe uma correspondência biunívoca entre as classes de isomorfismo de grupos de Bieberbach na classe cristalográfica* (G, M) *e as órbitas da ação de* $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ *em* $X(G, M)$.

Lema 1.5.33. *Seja* C_p *um grupo cíclico de ordem prima* p. *Então,* $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ *age transitivamente em* $H^2(C_p, M)^* := H^2(C_p, M) \smallsetminus \{0\}$.

Demonstração. Vamos dividir a prova em dois casos.

Caso 1: O $\mathbb{Z}C_p$-módulo M não é excepcional.

Sejam $\alpha, \alpha' \in H^2(C_p, M)^*$. Como M é um $\mathbb{Z}C_p$-módulo não excepcional, temos pela Proposição 1.5.15 que existe um elemento ϕ no centralizador $C_{\mathrm{Aut}(M)}(C_p)$ (de C_p em $\mathrm{Aut}(M)$) tal que

$$\phi \circledast \alpha = \phi_*(\mathrm{id}_*(\alpha)) = \phi_*(\alpha) = \alpha'.$$

Isso mostra que $C_{\mathrm{Aut}(M)}(C_p)$ age transitivamente em $H^2(C_p, M)^*$ e, consequentemente, $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ age transitivamente em $H^2(C_p, M)^*$.

Caso 2: O $\mathbb{Z}C_p$-módulo M é excepcional.

Uma vez que M é um $\mathbb{Z}C_p$-módulo excepcional, temos que $M = \bigoplus_{i=1}^{r} A_i \oplus \mathbb{Z}$ onde cada A_i é um ideal de $\mathbb{Z}[\zeta_p]$. Seja $\varphi \in \mathrm{Gal}(\zeta_p)$ e considere a aplicação $\phi : M \to M$ definida por

$$a_1 \oplus \cdots \oplus a_r \oplus u \mapsto \varphi(a_1) \oplus \cdots \oplus \varphi(a_r) \oplus u,$$

para $a_i \in A_i$ e $u \in \mathbb{Z}$. Claramente, ϕ é um automorfismo do grupo abeliano M. Lembre-se que: $\mathrm{Gal}(\zeta_p) \cong \mathrm{Aut}(C_p)$; cada $\varphi \in \mathrm{Aut}(C_p)$ é da forma $\varphi(x) = x^k$ onde x é um gerador

de C_p e k é algum inteiro entre 0 e p. Note que,

$$\varphi(x \cdot a_i) = \varphi(\zeta_p a_i) = \varphi(\zeta_p)\varphi(a_i) = \varphi(x) \cdot \varphi(a_i),$$

para $i = 1, \cdots, r$. Como $\mathbb{Z}$ é um $\mathbb{Z}C_p$-módulo trivial, então $\phi(x \cdot m) = \varphi(x) \cdot \phi(m)$ para cada $m \in M$. Consequentemente, $\phi \in \mathcal{N}_{\mathrm{Aut}(M)}(C_p)$. Uma vez que $H^2(C_p, M) \cong \mathbb{Z}/p\mathbb{Z}$ (ver Proposição 1.3.14), temos que

$$\phi \circledast \alpha = \mathrm{id}_*(\tilde{\phi}_*(\alpha)) = \tilde{\phi}_*(\alpha) = k\alpha,$$

onde $\tilde{\phi}$ é um automorfismo de C_p induzido pela conjugação de ϕ em C_p e α é qualquer elemento não nulo de $\mathbb{Z}/p\mathbb{Z}$. Pela generalidade da construção, podemos assumir que k é qualquer inteiro entre 0 e p. Isso implica que, para quaisquer dois elementos não nulos α e α' em $\mathbb{Z}/p\mathbb{Z}$, existe k entre 0 e p, tal que $k\alpha = \alpha'$. Isso prova que, $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$ age transitivamente em $H^2(C_p, M)^*$. □

Combinando os Teoremas 1.5.17 e 1.5.18 com Corolário 1.5.32 e Lema 1.5.33, obtemos o seguinte:

Corolário 1.5.34. *Seja M um $\mathbb{Z}C_p$-reticulado fiel. Existe uma correspondência biunívoca entre o conjunto das classes cristalográficas aritméticas (C_p, M) e o conjunto das classes de isomorfismos de grupos de Bieberbach Γ com grupo de holonomia C_p e subgrupo de translações M.*

Finalizamos essa seção, com uma fórmula para calcular o número de órbitas da ação de $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ em $X(G, M)$, quando G é um grupo cíclico de ordem livre de quadrados.

Lema 1.5.35. *Seja M um $\mathbb{Z}G$-reticulado para um grupo cíclico G de ordem δ livre de quadrados. Então,*

$$|\mathcal{N}_{\mathrm{Aut}(M)}(G)\backslash X(G, M)| = \prod_{p|\delta} |\mathcal{N}_{\mathrm{Aut}(M)}(G)\backslash(\bar{M}^*_{1,p})^G|, \tag{1.22}$$

onde $M_{1,p}$ é o maior somando direto de M em que C_p age trivialmente.

Demonstração. Uma vez que $G = C_{p_1} \times \cdots \times C_{p_k}$ é um grupo cíclico de ordem $\delta = p_1 p_2 \cdots p_k$ livre de quadrados, segue pela Observação 1.3.16 e Proposição 1.3.17 que

$$X(G, M) = \prod_{p|\delta} (\bar{M}^*_{1,p})^{G/C_p} = \prod_{p|\delta} (\bar{M}^*_{1,p})^G.$$

Como $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ é um subgrupo de $\mathcal{N}_{\mathrm{Aut}(M)}(C_p)$, para cada primo p dividindo δ, temos que $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ age em cada $(\bar{M}^*_{1,p})^G$ para todo $p \mid \delta$ e, consequentemente, temos a fórmula (1.22) para a cardinalidade do conjunto das órbitas da ação de $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ em $X(G, M)$. □

Capítulo

2

Gênero Profinito de Grupos de Bieberbach

Neste Capítulo, respondemos a Questão 1 para a família dos grupos de Bieberbach Γ de dimensão n com grupo de holonomia cíclico de ordem livre de quadrados. Mais precisamente, exibimos fórmulas para a cardinalidade do gênero $\mathfrak{g}(\Gamma)$. Iniciamos, Seção 2.1, apresentando propriedades gerais sobre a estrutura do completamento profinito de um grupo de Bieberbach com grupo de holonomia qualquer. Em seguida, na Seção 2.2, realizamos o estudo da Questão 1 para grupos de Bieberbach com grupo de holonomia de ordem prima e, posteriormente, estudamos o caso com ordem livre de quadrados.

2.1 O completamento profinito de grupos de Bieberbach

Lema 2.1.1. *Seja Γ um grupo de Bieberbach de dimensão n com subgrupo de translações M. Então, $\widehat{M}$ é o único subgrupo normal aberto, abeliano maximal, livre de torção de $\widehat{\Gamma}$.*

Demonstração. Pela Proposição 1.1.7, existe uma correspondência biunívoca entre o conjunto de todos os subgrupos normais de índice finito de Γ e o conjunto de todos os subgrupos normais abertos de $\widehat{\Gamma}$. Portanto, o lema segue das Proposições 1.5.6 e 1.1.10. □

Se Γ é um grupo de Bieberbach definido pela sequência exata

$$1 \to M \to \Gamma \to G \to 1,$$

onde M é o subgrupo de translações e G é um grupo finito, então pelo Lema 2.1.1 obtemos

a seguinte sequência exata

$$1 \to \widehat{M} \to \widehat{\Gamma} \to G \to 1$$

para os completamentos profinitos correspondentes.

Proposição 2.1.2. *O completamento profinito de um grupo de Bieberbach é um grupo profinito livre de torção.*

Demonstração. Seja Γ um grupo de Bieberbach definido pela sequência exata

$$1 \to M \to \Gamma \xrightarrow{\pi} G \to 1,$$

onde M é o subgrupo de translações e G o grupo de holonomia. Pela discussão acima, temos

$$1 \to \widehat{M} \to \widehat{\Gamma} \xrightarrow{\widehat{\pi}} G \to 1.$$

Suponha que $\widehat{\Gamma}$ tem um elemento de ordem finita. Consequentemente, $\widehat{\Gamma}$ tem um elemento de ordem prima. Como $\widehat{M}$ é livre de torção pelo Lema 2.1.1, existe um elemento $g \in G$ de ordem prima p tal que $\widehat{\pi}^{-1}(\langle g \rangle)$ não é livre de torção. Note que, $\widehat{\pi}^{-1}(\langle g \rangle)$ é um subgrupo aberto de $\widehat{\Gamma}$ contendo $\widehat{M}$ de modo que $\widehat{\pi}^{-1}(\langle g \rangle)/\widehat{M} \cong \langle g \rangle$. Agora, pela Proposição 1.1.7, existe um subgrupo Γ_p de Γ contendo M tal que $\Gamma_p/M \cong \langle g \rangle$ e $\widehat{\Gamma}_p \cong \widehat{\pi}^{-1}(\langle g \rangle)$. Então, $\widehat{\Gamma}_p$ não é livre de torção, uma contradição em vista da Proposição 1.1.10. Portanto, Γ é um grupo profinito livre de torção. □

Lema 2.1.3. *Sejam Γ_1 e Γ_2 grupos de Bieberbach de dimensão n com subgrupos de translações M_1 e M_2 e grupos de holonomia G_1 e G_2, respectivamente. Se $\psi : \widehat{\Gamma}_1 \to \widehat{\Gamma}_2$ é um isomorfismo, então existem isomorfismos $\phi : \widehat{M}_1 \to \widehat{M}_2$ e $\varphi : G_1 \to G_2$ tais que o seguinte diagrama comuta:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \widehat{M}_1 & \longrightarrow & \widehat{\Gamma}_1 & \longrightarrow & G_1 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & \widehat{M}_2 & \longrightarrow & \widehat{\Gamma}_2 & \longrightarrow & G_2 & \longrightarrow & 1. \end{array} \tag{2.1}$$

Demonstração. Pelo Lema 2.1.1, $\psi(\widehat{M}_1) = \widehat{M}_2$. Definimos ϕ como sendo a restrição de ψ para $\widehat{M}_1$. Então, $\phi : \widehat{M}_1 \to \widehat{M}_2$ é um isomorfismo. Logo, ψ induz um isomorfismo $\varphi : G_1 \to G_2$ de modo que o diagrama (2.1) comuta. □

A próxima proposição nos diz que, para calcular a cardinalidade $|\mathfrak{g}(\Gamma)|$ do gênero de um grupo de Bieberbach Γ, é suficiente considerar as classes de isomorfismos dos grupos de Bieberbach em $\mathfrak{g}(\Gamma)$.

Proposição 2.1.4. *Seja Γ um grupo de Bieberbach de dimensão n com grupo de holonomia G. Se $\Delta \in \mathfrak{g}(\Gamma)$, então Δ é um grupo de Bieberbach de dimensão n com grupo de holonomia G.*

Demonstração. Seja Γ um grupo de Bieberbach de dimensão n com subgrupo de translações M e grupo de holonomia G. Uma vez que $\Delta \leq \widehat{\Delta}$ e $\widehat{\Delta} \cong \widehat{\Gamma}$, segue pela Proposição 2.1.2 que Δ é livre de torção. Então, resta mostrar que Δ tem um subgrupo abeliano maximal normal N tal que $N \cong \mathbb{Z}^n$. Pelo Lema 2.1.1, $\widehat{M}$ é o único subgrupo normal aberto abeliano maximal de $\widehat{\Gamma}$. Como $\widehat{\Delta} \cong \widehat{\Gamma}$, segue pela Proposição 1.1.7 que existe um subgrupo abeliano maximal normal N de Δ tal que $\widehat{N} \cong \widehat{M}$ e $\Delta/N \cong G$. Então, N é um grupo abeliano, finitamente gerado, livre de torção, isto é, $N \cong \mathbb{Z}^m$. Afirmamos que $m = n$. De fato, por exemplo, se $n > m$, podemos construir um quociente finito $(\mathbb{Z}/k\mathbb{Z})^n$ de M que não pode ser um quociente de N, para algum inteiro positivo k. Então, $\widehat{N}$ não é isomorfo a $\widehat{M}$, uma contradição em vista da Proposição 1.1.8. Portanto, Δ é um grupo de Bieberbach de dimensão n com grupo de holonomia G. □

2.2 Grupos de Bieberbach com grupo de holonomia de ordem prima

Note que, $\widehat{M}$ pode ser considerado simplesmente como um G-módulo por [RZ00, Prop. 5.3.6].

Lema 2.2.1. *Sejam*

$$M = \bigoplus_{i=1}^{c}(A_i, a_i) \oplus \bigoplus_{j=1}^{b} A_j \oplus \mathbb{Z}^a, \quad M' = \bigoplus_{i=1}^{c'}(B_i, b_i) \oplus \bigoplus_{j=1}^{b'} B_j \oplus \mathbb{Z}^{a'}$$

$\mathbb{Z}C_p$-reticulados. Então, $\widehat{M} \cong \widehat{M'}$ como $\widehat{\mathbb{Z}}C_p$-módulos se, e somente se, $a = a', b = b'$ e $c = c'$.

Demonstração. Iniciamos observando que,

$$\widehat{M} = \bigoplus_{i=1}^{c}\widehat{(A_i, a_i)} \oplus \bigoplus_{j=1}^{b}\widehat{A}_j \oplus \widehat{\mathbb{Z}}^a \quad \text{e} \quad \widehat{M'} = \bigoplus_{i=1}^{c'}\widehat{(B_i, b_i)} \oplus \bigoplus_{j=1}^{b'}\widehat{B}_j \oplus \widehat{\mathbb{Z}}^{a'}.$$

Se $\widehat{M} \cong \widehat{M'}$ como $\widehat{\mathbb{Z}}C_p$-módulos, então as componentes pro-p de $\widehat{M}$ e $\widehat{M'}$ são isomorfos como $\mathbf{Z}_pC_p$-módulos. Portanto, a necessidade segue de Observação 1.4.12 e Proposições 1.4.8 e 1.4.10.

Por outro lado, pela Observação 1.4.12 a afirmação vale para a componente pro-p de $\widehat{M}$ e $\widehat{M'}$. Consequentemente, pela Proposição 1.4.13, $M_q \cong M'_q$ para todo primo q, e portanto, $\widehat{M} \cong \widehat{M'}$ como $\widehat{\mathbb{Z}}C_p$-módulos. □

Proposição 2.2.2. *Sejam Γ_1 e Γ_2 grupos de Bieberbach de dimensão n com grupo de holonomia C_p e subgrupos de translações M_1 e M_2, respectivamente. Então, $\Gamma_1 \cong \Gamma_2$ se, e somente se, $M_1 \cong (M_2)^\varphi$ como $\mathbb{Z}C_p$-módulos, onde $\varphi \in \mathrm{Aut}(C_p)$.*

Demonstração. Suponha que $\psi : \Gamma_1 \to \Gamma_2$ é um isomorfismo. Pelo Lema 1.5.27, temos que existem isomorfismos $\phi : M_1 \to M_2$ e $\varphi : C_p \to C_p$ de modo que

$$\phi(x \cdot m) = \varphi(x) \cdot \phi(m),$$

para cada $m \in M_1$ e $x \in C_p$. Logo, $M_1 \cong (M_2)^\varphi$ como $\mathbb{Z}C_p$-módulos.

Reciprocamente, suponha que existe $\varphi \in \mathrm{Aut}(C_p)$ tal que $M_1 \cong (M_2)^\varphi$ como $\mathbb{Z}C_p$-módulos. Então, M_1 é isomorfo semilinearmente para M_2. Portanto, pela Proposição 1.4.25 juntamente aos Teoremas 1.5.17 e 1.5.18, temos que $\Gamma_1 \cong \Gamma_2$. □

O próximo lema será útil para o caso em que o grupo de Bieberbach Γ têm grupo holonomia cíclico G de ordem δ prima e, também, se δ for livre de quadrados. Se o subgrupo de translações de Γ é M, então pela Proposição 1.5.24 temos que $M = M_{n-1} \oplus \mathbb{Z}$, de modo que, $\Gamma = M_{n-1} \rtimes C$ onde C contém $\mathbb{Z}$ como subgrupo de índice δ. Com essa notação temos o seguinte.

Lema 2.2.3. *Sejam $\Gamma_1 = M_{n-1} \rtimes C_1$ e $\Gamma_2 = N_{n-1} \rtimes C_2$ grupos de Bieberbach de dimensão n com grupo de holonomia cíclico G de ordem livre de quadrados δ e subgrupos de translações $M_{n-1} \oplus \mathbb{Z}$ e $N_{n-1} \oplus \mathbb{Z}'$, respectivamente. Se existe $\varphi \in \mathrm{Aut}(G)$ tal que*

(i) $M_{n-1} \cong (N_{n-1})^\varphi$ como $\mathbb{Z}G$-módulos, então $\Gamma_1 \cong \Gamma_2$.

(ii) $\widehat{M}_{n-1} \cong (\widehat{N}_{n-1})^\varphi$ como $\widehat{\mathbb{Z}}G$-módulos, então $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$.

Demonstração. Suponha que $G = \langle g \rangle$ e seja $\varphi \in \mathrm{Aut}(G)$. Pela Proposição 1.5.24, existem representações fiéis $j_1 : G \to \mathrm{Aut}(M_{n-1})$ e $j_2 : G \to \mathrm{Aut}(N_{n-1})$, assim, podemos ver G como subgrupo de $\mathrm{Aut}(M_{n-1})$ e $\mathrm{Aut}(N_{n-1})$. Sejam $\Gamma_1 = M_{n-1} \rtimes_{\rho_1} C_1$ e $\Gamma_2 = N_{n-1} \rtimes_{\rho_2} C_2$ onde $\rho_1 : C_1 \to \mathrm{Aut}(M_{n-1})$ e $\rho_2 : C_2 \to \mathrm{Aut}(N_{n-1})$ são homomorfismos tais que

- $\rho_1(c_1) = g$ onde $C_1 = \langle c_1 \rangle$ e $\mathbb{Z} = \langle c_1^\delta \rangle$,
- $\rho_2(c_2) = \varphi(g)$ onde $C_2 = \langle c_2 \rangle$ e $\mathbb{Z}' = \langle c_2^\delta \rangle$.

Considere as projeções naturais $\pi_1 : C_1 \to C_1/\mathbb{Z} = G$ e $\pi_2 : C_2 \to C_2/\mathbb{Z}' = G$ e o isomorfismo $\Theta : C_1 \to C_2$ definido por $\Theta(c_1) = c_2$. Note que, Θ induz um automorfismo $\varphi : G \to G$ de modo que o seguinte diagrama comuta

$$\begin{array}{ccc} C_1 & \xrightarrow{\Theta} & C_2 \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ G & \xrightarrow{\varphi} & G. \end{array}$$

Por hipótese, existe um isomorfismo $f : M_{n-1} \to N_{n-1}$ tal que

$$f(g \cdot m) = \varphi(g) \cdot f(m),$$

para todo $m \in M_{n-1}$. Assim,

$$f(\rho_1(c_1) \cdot m) = \rho_2(\Theta(c_1)) \cdot f(m),$$

para cada $m \in M_{n-1}$. Isto implica que $f\rho_1(c_1)f^{-1} = \rho_2(\Theta(c_1))$. Como $M_{n-1} \cong \mathbb{Z}^{n-1} \cong N_{n-1}$ e $C_1 \cong \mathbb{Z} \cong C_2$ podemos assumir que $f \in \mathrm{Aut}(\mathbb{Z}^{n-1})$ e $\Theta \in \mathrm{Aut}(\mathbb{Z})$. Agora, pela [GZ11, Prop. 2.5], temos que a aplicação

$$F : \Gamma_1 \to \Gamma_2$$
$$(m, c) \mapsto (f(m), \Theta(c))$$

é um isomorfismo. Isto conclui a prova do item (i).

A prova do item (ii) é análoga a prova do item (i). □

Teorema D. *Sejam M um grupo abeliano livre de posto n e C_p um grupo de ordem prima p. Sejam Γ_1 e Γ_2 grupos de Bieberbach de dimensão n que são extensões de M por C_p. Se M_1 e M_2 são $\mathbb{Z}C_p$-módulos induzidos pela ação de Γ_1 e Γ_2 em M, respectivamente, então*

(i) $\Gamma_1 \cong \Gamma_2$ se, e somente se, ou M_1 e M_2 são $\mathbb{Z}C_p$-módulos não excepcionais isomorfos ou M_1 e M_2 são $\mathbb{Z}C_p$-módulos excepcionais e são isomorfos a menos de um automorfismo de C_p por inversão.

(ii) $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$ se, e somente se, $\widehat{M_1} \cong \widehat{M_2}$ como $\widehat{\mathbb{Z}}C_p$-módulos.

Demonstração. (i) Segue da Proposição 2.2.2 e da Observação 1.5.19.

(ii) ($\Rightarrow$) Pelo Lema 2.1.3, vemos que existem isomorfismos $\phi : \widehat{M_1} \to \widehat{M_2}$ e $\varphi : C_p \to C_p$

tal que o seguinte diagrama é comutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \widehat{M}_1 & \longrightarrow & \widehat{\Gamma}_1 & \xrightarrow{\widehat{\pi}_1} & C_p & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & \widehat{M}_2 & \longrightarrow & \widehat{\Gamma}_2 & \xrightarrow{\widehat{\pi}_2} & C_p & \longrightarrow & 1. \end{array} \tag{2.2}$$

Seja $\gamma_1 \in \widehat{\Gamma}_1$ tal que $\widehat{\pi}(\gamma_1) = x \in C_p$. Pela comutatividade do diagrama (2.2), temos que

$$\widehat{\pi}_2(\psi(\gamma_1)) = \varphi(\widehat{\pi}_1(\gamma_1)) = \varphi(x).$$

Assim,

$$\phi(x \cdot m) = \psi(\gamma_1 m \gamma_1^{-1}) = \psi(\gamma_1)\psi(m)\psi(\gamma_1)^{-1} = \varphi(x) \cdot \phi(m),$$

para cada $m \in \widehat{M}_1$. Portanto, $\widehat{M}_1 \cong (\widehat{M}_2)^{\varphi}$ como $\widehat{\mathbb{Z}}C_p$-módulos.

($\Leftarrow$) Pela Proposição 1.5.24, $M_1 = M_{n-1} \oplus \mathbb{Z}$ e $M_2 = M'_{n-1} \oplus \mathbb{Z}'$ tais que $\Gamma_1 = M_{n-1} \rtimes_x C_1$ e $\Gamma_2 = M'_{n-1} \rtimes_x C_2$, onde C_1 e C_2 contém $\mathbb{Z}$ e $\mathbb{Z}'$ como subgrupo de índice p e agem em M_{n-1} e M'_{n-1} como $C_p = \langle x \rangle$, respectivamente. Agora, $\widehat{M}_1 = \widehat{M}_{n-1} \oplus \widehat{\mathbb{Z}}, \widehat{M}_2 = \widehat{M'}_{n-1} \oplus \widehat{\mathbb{Z}}'$, $\widehat{\Gamma}_1 = \widehat{M}_{n-1} \rtimes_x \widehat{C}_1$ e $\widehat{\Gamma}_2 = \widehat{M'}_{n-1} \rtimes_x \widehat{C}_2$ onde $\widehat{C}_1$ e $\widehat{C}_2$ também agem em $\widehat{M}_{n-1}$ e $\widehat{M'}_{n-1}$ como C_p. Segue pelo Lema 2.2.1 e Teorema 1.4.8 que $\widehat{M}_{n-1} \cong \widehat{M'}_{n-1}$ como $\widehat{\mathbb{Z}}C_p$-módulos (isso porque as componentes pro-p de $\widehat{M}_{n-1}$ e $\widehat{M'}_{n-1}$ são $\mathbf{Z}_pC_p$-módulos isomorfos para todo primo p). Portanto, $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$ pelo Lema 2.2.3.

□

A versão profinita dos Teoremas 1.5.17 e 1.5.18 é a seguinte.

Corolário 2.2.4. *Seja Γ um grupo de Bieberbach de dimensão n com grupo de holonomia de ordem prima. Então, existe uma correspondência biunívoca entre as classes de isomorfismo de $\widehat{\Gamma}$ e a tripla (a, b, c) da decomposição (1.10) com $a > 0$.*

Demonstração. Isto segue imediatamente do Teorema D e do Lema 2.2.1. □

Agora podemos provar o principal resultado desta subseção.

Teorema A. *Seja Γ um grupo de Bieberbach de dimensão n com subgrupo de translações M e grupo de holonomia C_p de ordem prima p.*

(i) Se M é um $\mathbb{Z}C_p$-reticulado excepcional, então $|\mathfrak{g}(\Gamma)| = |C_2 \backslash H(\mathbb{Z}[\zeta_p])|$, onde C_2 é um grupo de ordem 2 agindo em $H(\mathbb{Z}[\zeta_p])$ por inversão.

(ii) Caso contrário, $|\mathfrak{g}(\Gamma)| = |\mathrm{Gal}(\zeta_p)\backslash H(\mathbb{Z}[\zeta_p])|$. [1]

Demonstração. Pela Proposição 2.1.4, para calcular a cardinalidade do gênero $\mathfrak{g}(\Gamma)$, de um grupo de Bieberbach Γ, é suficiente considerar as classes de isomorfismos dos grupos de Bieberbach em $\mathfrak{g}(\Gamma)$.

Sejam Γ_1 e Γ_2 grupos de Bieberbach com grupos de holonomia de ordem prima e subgrupos de translações M_1 e M_2, respectivamente. Pelo Lema 2.1.3, podemos assumir que Γ_1 e Γ_2 tem o mesmo grupo de holonomia C_p de ordem prima p. Como M_1 e M_2 são $\mathbb{Z}C_p$-reticulados, pelo Teorema 1.4.5,

$$M_1 \cong \bigoplus_{i=1}^{c}(A_i, a_i) \oplus \bigoplus_{j=1}^{b} A_j \oplus \mathbb{Z}^a$$

e

$$M_2 \cong \bigoplus_{i=1}^{c'}(B_i, b_i) \oplus \bigoplus_{j=1}^{b'} B_j \oplus \mathbb{Z}^{a'}$$

onde A_i e B_i são ideais de $\mathbb{Z}[\zeta_p]$. Uma vez que $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$, temos que $\widehat{M_1} \cong \widehat{M_2}$ como $\widehat{\mathbb{Z}}C_p$-módulos pelo Teorema D. Consequentemente, $a = a', b = b'$ e $c = c'$ pelo Lema 2.2.1. Portanto, o resultado segue pelos Teoremas 1.5.17 e 1.5.18 e Teorema D. □

Corolário 2.2.5. *Seja Γ um grupo de Bieberbach de dimensão n com grupo de holonomia de ordem prima. Se $H(\mathbb{Z}[\zeta_p])$ não é trivial, então $|\mathfrak{g}(\Gamma)| > 1$.*

Demonstração. Isto é uma consequência do Teorema A e Lema 1.2.43. □

Observação 2.2.6. *Segue que a cardinalidade $|\mathfrak{g}(\Gamma)|$ do gênero de um grupo de Bieberbach Γ com subgrupo de translações M e grupo de holonomia C_p é igual à cardinalidade do gênero do $\mathbb{Z}C_p$-módulo M se Γ não é excepcional e metade se Γ é excepcional.*

Corolário B. *Seja Γ um grupo de Bieberbach de dimensão n com grupo de holonomia C_p de ordem prima p. Então, $|\mathfrak{g}(\Gamma)| = 1$ se, e somente se, $p \leq 19$.*

Demonstração. Isto segue do Teorema A e da Proposição 1.2.34 e Lema 1.2.43. □

Corolário C. *Seja X uma variedade compacta plana de dimensão n com grupo de holonomia de ordem prima. Se $n \leq 21$, então X é determinada dentre todas as variedades compactas planas de dimensão n pelo completamento profinito do seu grupo fundamental.*

Demonstração. Pelo Corolário 1.5.14, deduzimos que para todo $n \leq 21$, nenhum número primo $p \geq 23$ pode ocorrer como ordem de um elemento no grupo de holonomia de grupos de Bieberbach de dimensão n. Portanto, o resultado segue pelo Corolário B. □

[1] O caso (ii) do Teorema A também foi enunciado com um esboço de prova em [GZ11]

Observação 2.2.7. *Se $\Gamma = M \rtimes C_p$, com M abeliano livre de posto n e C_p um grupo de ordem prima p agindo em M de forma não trivial, então Γ não é um grupo de Bieberbach. Entretanto, usando que Γ e $M_1 \rtimes C_p$ são isomorfos se, e somente se, $M \cong M_1$ como $\mathbb{Z}C_p$-módulos (até um automorfismo de C_p) e que o mesmo vale para o completamento profinito (ver [GZ11, §2.2]), podemos deduzir que o gênero de Γ tem a mesma cardinalidade como no Teorema A (ii) (ver Proposição 2.2.2). Além disso, considerando C_p como um subgrupo de $\mathrm{Aut}(M) = \mathrm{GL}(n, \mathbb{Z})$, deduzimos de [GZ11, Prop. 2.17] que a cardinalidade do gênero é exatamente o número de classes de conjugação de subgrupos de ordem p de $\mathrm{GL}(n, \mathbb{Z})$ na classe de conjugação de C_p em $\mathrm{GL}(n, \widehat{\mathbb{Z}})$.*

2.3 Grupos de Bieberbach com o grupo de holonomia cíclico de ordem livre de quadrados

Neste seção vamos provar uma generalização do Teorema A. Para isso, exceto menção em contrário, G sempre será um grupo cíclico de ordem δ livre de quadrados.

Lema 2.3.1. *Sejam Γ_1 e Γ_2 grupos de Bieberbach com grupo de holonomia cíclico G de ordem livre de quadrados δ e subgrupos de translações M e N, respectivamente. Então, Γ_1 e Γ_2 estão na mesma classe cristalográfica aritmética se, e somente se,*

(i) $r(d, M) = r(d, N)$ *para cada* $d \mid \delta$.

(ii) $\rho_k(\lambda(s, t, M)) = \rho_k(\lambda(s, t, N))$ *para cada* $k = 1, \cdots, v$ *e* $(s, t) \in D_1^*$.

(iii) $\sigma \cdot [I_{\mathcal{M}_d}] = [J_{\mathcal{N}_d}]$ *para cada* $d \mid \delta$ *e para algum* $\sigma \in \mathrm{Gal}(\zeta_\delta)$.

Demonstração. Isto é uma consequência da Proposição 1.4.26. □

Em particular, quando $\delta = 6, 10, 14$ ou δ é primo, temos o seguinte.

Proposição 2.3.2. *Sejam Γ_1 e Γ_2 grupos de Bieberbach de dimensão n com grupo de holonomia cíclico G de ordem $\delta = 6, 10, 14$ ou δ é primo. Sejam M e N os subgrupos de translações de Γ_1 e Γ_2, respectivamente. Então, $\Gamma_1 \cong \Gamma_2$ se, e somente se,*

(i) $r(d, M) = r(d, N)$ *para cada* $d \mid \delta$.

(ii) $\rho_k(\lambda(s, t, M)) = \rho_k(\lambda(s, t, N))$ *para cada* $k = 1, \cdots, v$ *e* $(s, t) \in D_1^*$.

(iii) $\sigma \cdot [I_{\mathcal{M}_d}] = [J_{\mathcal{N}_d}]$ *para cada* $d \mid \delta$ *e para algum* $\sigma \in \mathrm{Gal}(\zeta_\delta)$.

Demonstração. ($\Rightarrow$) Se $\Gamma_1 \cong \Gamma_2$, então M é isomorfo semilinearmente para N pelo Lema 1.5.27. Portanto, segue pela Proposição 1.4.26 que as condições (i)–(iii) são satisfeitas.

($\Leftarrow$) Suponha que os $\mathbb{Z}G$-reticulados M e N satisfazem as condições (i)–(iii). Pela Proposição 1.5.24, $M = M_{n-1} \oplus \mathbb{Z}$ e $N = N_{n-1} \oplus \mathbb{Z}'$ tais que $\Gamma_1 = M_{n-1} \rtimes C_1$ e $\Gamma_2 = N_{n-1} \rtimes C_2$ onde C_1 e C_2 contém $\mathbb{Z}$ e $\mathbb{Z}'$ como subgrupos de índice δ e agem em M_{n-1} e N_{n-1} como G. Uma vez que as condições (i)–(iii) são satisfeitas para $M_{n-1} \oplus \mathbb{Z}$ e $N_{n-1} \oplus \mathbb{Z}'$, segue pela Proposição 1.4.26 que $M_{n-1} \oplus \mathbb{Z}$ é isomorfo semilinearmente para $N_{n-1} \oplus \mathbb{Z}'$. Consequentemente, $M_{n-1} \cong (N_{n-1})^{\varphi}$ para algum $\varphi \in \mathrm{Aut}(G)$ pela Proposição 1.4.22 e, portanto, $\Gamma_1 \cong \Gamma_2$ pelo Lema 2.2.3. □

Um conjunto completo de invariantes de isomorfismo para o completamento profinito de um grupo de Bieberbach, com o grupo de holonomia cíclico de ordem livre de quadrados, é dado a seguir.

Proposição 2.3.3. *Sejam Γ_1 e Γ_2 grupos de Bieberbach de dimensão n com grupo de holonomia G e subgrupos de translações M e N, respectivamente. Então, $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$ se, e somente se,*

(i) $r(d, M) = r(d, N)$ para cada $d \mid \delta$.

(ii) $\rho_k(\lambda(s, t, M)) = \rho_k(\lambda(s, t, N))$ para cada $k = 1, \cdots, v$ e $(s, t) \in D_1^*$.

Demonstração. ($\Rightarrow$) Suponha que $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$. Pelo Lema 2.1.3, existem isomorfismos $\phi : \widehat{M} \to \widehat{N}$ e $\varphi : G \to G$ tais que o seguinte diagrama é comutativo

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \widehat{M} & \longrightarrow & \widehat{\Gamma}_1 & \xrightarrow{\widehat{\pi}_1} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & \widehat{N} & \longrightarrow & \widehat{\Gamma}_2 & \xrightarrow{\widehat{\pi}_2} & G & \longrightarrow & 1. \end{array} \tag{2.3}$$

Mostraremos que $\widehat{M} \cong (\widehat{N})^{\varphi}$ como $\widehat{\mathbb{Z}}G$-módulos por argumentos análogos ao da prova do item (ii) do Teorema D. Seja $\gamma_1 \in \widehat{\Gamma}_1$ tal que $\widehat{\pi}_1(\gamma_1) = g \in G$. Pela comutatividade do diagrama (2.3), temos que

$$\widehat{\pi}_2(\psi(\gamma_1)) = \varphi(\widehat{\pi}_1(\gamma_1)) = \varphi(g).$$

Assim,

$$\phi(g \cdot m) = \phi(\gamma_1 m \gamma_1^{-1}) = \psi(\gamma_1)\psi(m)\psi(\gamma_1)^{-1} = \varphi(g) \cdot \phi(m),$$

onde $m \in \widehat{M}$. Portanto, $\widehat{M} \cong (\widehat{N})^{\varphi}$ como $\widehat{\mathbb{Z}}G$-módulos. Logo, as afirmações (i) e (ii) seguem imediatamente do Teorema 1.4.21.

($\Leftarrow$) Assuma que M e N são subgrupos normais abelianos maximais de Γ_1 e Γ_2, respectivamente, satisfazendo as condições (i) e (ii). Pela Proposição 1.5.24, $M = M_{n-1} \oplus \mathbb{Z}$ e $N = N_{n-1} \oplus \mathbb{Z}'$ tais que $\Gamma_1 = M_{n-1} \rtimes C_1$ e $\Gamma_2 = N_{n-1} \rtimes C_2$ onde C_1 e C_2 contém $\mathbb{Z}$ e $\mathbb{Z}'$ como subgrupos de índice δ e agem em M_{n-1} e N_{n-1} como G. Consequentemente, $\widehat{M} = \widehat{M}_{n-1} \oplus \widehat{\mathbb{Z}}, \widehat{N} = \widehat{N}_{n-1} \oplus \widehat{\mathbb{Z}}'$ e $\widehat{\Gamma}_1 = \widehat{M}_{n-1} \rtimes \widehat{C}_1, \widehat{\Gamma}_2 = \widehat{N}_{n-1} \rtimes \widehat{C}_2$, onde $\widehat{C}_1$ e $\widehat{C}_2$ agem em $\widehat{M}_{n-1}$ e $\widehat{N}_{n-1}$ como G. Temos que,

$$\widehat{M}_{n-1} \oplus \widehat{\mathbb{Z}} \cong \widehat{N}_{n-1} \oplus \widehat{\mathbb{Z}}'$$

como $\widehat{\mathbb{Z}}G$-módulos pelo Teorema 1.4.21 e, consequentemente,

$$r(d, M_{n-1}) + r(d, \mathbb{Z}) = r(d, N_{n-1}) + r(d, \mathbb{Z}')$$

e

$$\rho_k(\lambda(s,t,M_{n-1})) + \rho_k(\lambda(s,t,\mathbb{Z})) = \rho_k(\lambda(s,t,N_{n-1})) + \rho_k(\lambda(s,t,\mathbb{Z}')),$$

para cada $d \mid \delta$ e $k = 1, 2, \cdots, v$ pela Proposição 1.4.23. Uma vez que $\mathbb{Z} \cong \mathbb{Z}'$ como $\mathbb{Z}G$-módulos, pelo Teorema 1.4.20, temos que

$$r(d, \mathbb{Z}) = r(d, \mathbb{Z}') \quad \text{e} \quad \rho_k(\lambda(s,t,\mathbb{Z})) = \rho_k(\lambda(s,t,\mathbb{Z}')),$$

para cada $d \mid \delta$ e $k = 1, 2, \cdots, v$. Assim,

$$r(d, M_{n-1}) = r(d, N_{n-1}) \quad \text{e} \quad \rho_k(\lambda(s,t,M_{n-1})) = \rho_k(\lambda(s,t,N_{n-1})),$$

para cada $k = 1, 2, \cdots, v$ e $d \mid \delta$, de modo que, pelo Teorema 1.4.21, $\widehat{M}_{n-1} \cong \widehat{N}_{n-1}$ como $\widehat{\mathbb{Z}}G$-módulos. Portanto, $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$ pelo Lema 2.2.3. □

Passemos agora a provar os resultados principais desta seção. À luz do Corolário 1.5.32, para calcular a cardinalidade do gênero $\mathfrak{g}(\Gamma)$ de um grupo de Bieberbach Γ, de dimensão n, com subgrupo de translações M e grupo de holonomia cíclico G de ordem livre de quadrados δ, temos que seguir as etapas:

1. Calcular o número de grupos de Bieberbach (a menos de isomorfismo) na classe cristalográfica (G, M).

2. Calcular o número de classes cristalográficas (a menos de equivalência) determinadas pelos grupos de Bieberbach em $\mathfrak{g}(\Gamma)$.

Por definição, cada classe cristalográfica (G, M) corresponde para um $\mathbb{Z}G$-reticulado M. Lembre-se que, $\mathcal{C}(M)$ denota o conjunto de classes de isomorfismos de $\mathbb{Z}G$-reticulados

N, que corresponde para uma classe cristalográfica (G, N), de modo que $\widehat{N} \cong \widehat{M}$ como $\widehat{\mathbb{Z}}G$-módulos. Então, para etapa 2, temos que calcular a cardinalidade do conjunto $\mathcal{C}(M)$.

Teorema E. *Seja Γ um grupo de Bieberbach de dimensão n com subgrupo abeliano maximal normal M e grupo de holonomia cíclico G de ordem livre de quadrados δ. Se Γ é excepcional, então*

$$|\mathcal{C}(M)| = \left| \mathcal{H}_D \backslash \prod_{d|\delta} H(\mathbb{Z}[\zeta_d]) \right|.$$

Caso contrário,

$$|\mathcal{C}(M)| = \left| \mathrm{Gal}(\zeta_\delta) \backslash \prod_{d|\delta} H(\mathbb{Z}[\zeta_d]) \right|.$$

Demonstração. Sejam Γ_1 e Γ_2 grupos de Bieberbach de dimensão n com o grupo de holonomia cíclico de ordem livre de quadrados e subgrupos de translações M e N, respectivamente. Suponha que $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$. Pelo Lema 2.1.3, podemos assumir que Γ_1 e Γ_2 têm o mesmo grupo de holonomia cíclico G de ordem livre de quadrados δ.

Para cada $d \mid \delta$, C_d denota o subgrupo de G de ordem d e $\Gamma_{i,d}$ denota o subgrupo de Bieberbach de dimensão n de Γ_i com grupo de holonomia C_d, para $i = 1, 2$.

Segue pela Proposição 2.3.3 e Teorema 1.4.21 que

$$\begin{aligned} \widehat{\Gamma}_1 \cong \widehat{\Gamma}_2 &\Leftrightarrow \widehat{M} \cong \widehat{N} \text{ como } \widehat{\mathbb{Z}}G\text{-módulos} \\ &\Leftrightarrow \text{para cada } d \mid \delta, \widehat{M} \cong \widehat{N} \text{ como } \widehat{\mathbb{Z}}C_d\text{-módulos} \\ &\Leftrightarrow \text{para cada } d \mid \delta, \widehat{\Gamma}_{1,d} \cong \widehat{\Gamma}_{2,d}. \end{aligned} \tag{2.4}$$

Agora, suponha que existem números primos p e q dividindo δ tais que os grupos de Bieberbach $\Gamma_{1,p}$ e $\Gamma_{2,q}$ são excepcionais. Uma vez que $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$, segue de (2.4) que $\widehat{\Gamma}_{1,d} \cong \widehat{\Gamma}_{2,d}$ para cada $d \mid \delta$. Em particular, $\widehat{\Gamma}_{1,p} \cong \widehat{\Gamma}_{2,p}$ e $\widehat{\Gamma}_{1,q} \cong \widehat{\Gamma}_{2,q}$. Isto implica que, se $p \neq q$, então os grupos de Bieberbach $\Gamma_{i,p}$ e $\Gamma_{i,q}$ são excepcionais, para $i = 1, 2$. Assim, como $\delta = p_1 p_2 \cdots p_k$ onde p_l $(l = 1, \cdots, k)$ são números primos distintos, podemos assumir que existe um inteiro positivo r com $1 \leq r \leq k$ tal que $D = \{q_1, \cdots, q_r\}$ é um subconjunto de $\{p_1, \cdots, p_k\}$ com r elementos distintos, de modo que, os grupos de Bieberbach $\Gamma_{i,q}$ são excepcionais, para cada $q \in D$ e $i = 1, 2$.

Usando a Proposição 1.2.23, definimos o grupo

$$\mathcal{H}_D = \mathrm{Gal}(\zeta_{p_1}) \times \cdots \times \mathrm{Gal}(\zeta_{p_{i-1}}) \times C_2 \times \mathrm{Gal}(\zeta_{p_{i+1}}) \times \cdots \times \mathrm{Gal}(\zeta_{p_k}),$$

para cada $p_i \in D$. Pela Observação 1.2.42 vemos que $\mathcal{H}_D$ age sobre $\prod_{p|\delta} H(\mathbb{Z}[\zeta_d])$. Nesta

prova usaremos, sem menção, a seguinte identificação $\mathrm{Gal}(\zeta_\delta) \cong (\mathbb{Z}/\delta\mathbb{Z})^\times \cong \mathrm{Aut}(G)$.

Agora, se $[(G,M)]$ representa a classe cristalográfica aritmética de Γ_1, então, pelo Lema 2.3.1 e Proposição 1.4.26, temos que

$$\begin{aligned}\Gamma_1, \Gamma_2 \in [(G,M)] &\Leftrightarrow M \cong (N)^\varphi \text{ como } \mathbb{Z}G\text{-módulos para algum } \varphi \in \mathcal{H}_D \\ &\Leftrightarrow \text{para cada } d \mid \delta, M \cong (N)^\varphi \text{ como } \mathbb{Z}C_d\text{-módulos para algum } \varphi \in \mathcal{H}_D \\ &\Leftrightarrow \text{para cada } d \mid \delta, \Gamma_{1,d}, \Gamma_{2,d} \in [(C_d, M)].\end{aligned}$$

Como os grupos de Bieberbach $\Gamma_{i,q}$ $(q \in D, i = 1,2)$ são excepcionais, combinando Proposição 2.3.3, Teoremas 1.5.17 e 1.5.18, Lema 2.3.1 e Corolário 1.5.34, obtemos que

$$|\mathcal{C}(M)| = \left| \mathcal{H}_D \backslash \prod_{d|\delta} H(\mathbb{Z}[\zeta_d]) \right|.$$

Caso contrário, se para cada primo p dividindo δ os grupos de Bieberbach $\Gamma_{i,p}$ $(i = 1,2)$ não são excepcionais, então pela Proposição 2.3.3 e Teorema 1.5.17, Lema 2.3.1 e Corolário 1.5.34, obtemos que

$$|\mathcal{C}(M)| = \left| \mathrm{Gal}(\zeta_\delta) \backslash \prod_{d|\delta} H(\mathbb{Z}[\zeta_d]) \right|,$$

e, portanto, o Teorema E está provado. □

Agora estamos em condições de calcular a cardinalidade de $\mathfrak{g}(\Gamma)$.

Teorema F. *Seja Γ um grupo de Bieberbach de dimensão n com subgrupo de translações M e grupo de holonomia cíclico G de ordem livre de quadrados δ. Então,*

$$|\mathfrak{g}(\Gamma)| = \sum_{M \in T} \left(\prod_{p|\delta} |\mathcal{N}_{\mathrm{Aut}(M)}(G) \backslash (\bar{M}^*_{1,p})^G| \right),$$

onde T é um conjunto completo de representantes das classes de isomorfismos dos $\mathbb{Z}G$-reticulados em $\mathcal{C}(M)$ e $M_{1,p}$ é o maior somando direto de M em que C_p age trivialmente.

Demonstração. Pela Proposição 2.1.4, para calcular a cardinalidade do gênero $\mathfrak{g}(\Gamma)$ de um grupo de Bieberbach Γ, é suficiente considerar as classes de isomorfismos dos grupos de Bieberbach em $\mathfrak{g}(\Gamma)$. Suponha que Γ tem subgrupo de translações M e grupo de holonomia cíclico G de ordem livre de quadrados δ. Segue pela Observação 1.5.29, que para encontrar todas as classes de isomorfismos de grupos de Bieberbach nas classes cristalográficas aritméticas, é suficiente considerar um conjunto T de representantes das

classes de isomorfismos de $\mathbb{Z}G$-reticulados em $\mathcal{C}(M)$. Vimos que Teorema E estabelece uma fórmula para calcular a cardinalidade de T. Agora, aplicando primeiro Corolário 1.5.32 e, então, Lema 1.5.35, temos que

$$\begin{aligned} |\mathfrak{g}(\Gamma)| &= \sum_{M\in T} |\mathcal{N}_{\mathrm{Aut}(M)}(G)\backslash X(G,M)| \\ &= \sum_{M\in T}\left(\prod_{p|\delta} |\mathcal{N}_{\mathrm{Aut}(M)}(G)\backslash(\bar{M}^*_{1,p})^G|\right), \end{aligned}$$

onde $M_{1,p}$ é o maior somando direto de M em que C_p age trivialmente. □

Em vista do Lema 1.5.33, vemos que o Teorema A segue como uma consequência do Teorema F. A seguir, apresentamos outras consequências do Teorema F.

Corolário G.

$$|\mathfrak{g}(\Gamma)| \leq |H(\mathbb{Z}[\zeta_\delta])|^a max_{p|\delta}\{|(\bar{M}^*_{1,p})^G|^b\}$$

onde a é o número de divisores de δ e b é o número de divisores primos de δ.

Demonstração. Para simplificar a notação, escreveremos $max\{|(\bar{M}^*_{1,p})^G|\}$ para denotar $max\{|(\bar{M}^*_{1,p})^G| \ : \ p \mid \delta\}$. Pelo Teorema F,

$$\begin{aligned} |\mathfrak{g}(\Gamma)| &= \sum_{M\in T}\left(\prod_{p|\delta} \left|\mathcal{N}_{\mathrm{Aut}(M)}(G)\backslash((\bar{M}_{1,p})^*)^G\right|\right) \\ &\leq \sum_{M\in T}\left(\prod_{p|\delta} max\{|(\bar{M}^*_{1,p})^G|\}\right) \\ &= \sum_{M\in T}\left(max\{|(\bar{M}^*_{1,p})^G|\}\right)^b \\ &= |\mathcal{C}(M)|max\{|(\bar{M}^*_{1,p})^G|\}^b \\ &\leq (H(\mathbb{Z}[\zeta_\delta]))^a \, max\{|(\bar{M}^*_{1,p})^G|\}^b, \quad \text{(Pelo Teorema E)} \end{aligned}$$

□

Corolário H. *Se Γ é um grupo de Bieberbach excepcional, então*

$$|\mathfrak{g}(\Gamma)| = \sum_{M\in T}\left(\prod_{p\in D} |\mathcal{N}_{\mathrm{Aut}(M)}(G)\backslash\mathbb{F}_p^*| \prod_{\substack{q|\delta \\ q\notin D}} |\mathcal{N}_{\mathrm{Aut}(M)}(G)\backslash(\bar{M}^*_{1,q})^G|\right)$$

Demonstração. Isto segue pelo Teorema F e pela Proposição 1.5.24. □

Em particular, temos o seguinte caso especial.

Teorema I. *Seja* Γ *um grupo de Bieberbach de dimensão* n *com grupo de holonomia cíclico de ordem igual a* $6, 10$ *ou* 14. *Então,* $|\mathfrak{g}(\Gamma)| = 1$.

Demonstração. Em vista da Proposição 2.1.4, para calcular a cardinalidade do gênero $\mathfrak{g}(\Gamma)$ de uma grupo de Bieberbach Γ é suficiente considerar as classes de isomorfismos de grupos de Bieberbach em $\mathfrak{g}(\Gamma)$.

Sejam Γ_1 e Γ_2 grupos de Bieberbach de dimensão n com subgrupos de translações M_1 e M_1 e grupo de holonomia cíclico de ordem igual a $6, 10$ ou 14. Suponha que $\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2$. Pelo Lema 2.1.3 podemos assumir que Γ_1 e Γ_2 tem o mesmo grupo de holonomia G de ordem $\delta = 6, 10$ ou 14. Pela Proposição 2.3.3 e Teorema 1.4.21 vemos que

$$\widehat{\Gamma}_1 \cong \widehat{\Gamma}_2 \Leftrightarrow \widehat{M_1} \cong \widehat{M_2} \text{ como } \widehat{\mathbb{Z}}G\text{-módulos.}$$

Uma vez que o grupo de classe $H(\mathbb{Z}[\zeta_d])$ é trivial para todo divisor d de δ (Cf. [AW04, Table 10]), segue pelas Proposições 2.3.3 e 2.3.2 que $|\mathfrak{g}(\Gamma_1)| = 1$, como queríamos. □

2.4 Exemplos

Suponha que G é um grupo cíclico de ordem livre de quadrados $\delta > 1$. Seja $\langle a, b | R\rangle$ uma apresentação de G, isto é, $G \cong F_2/\tilde{R}$ onde F_2 é o grupo livre em $\{a, b\}$ e $\tilde{R}$ é o fecho normal de R em F_2. Isto define uma sequência exata

$$1 \to \tilde{R} \to F_2 \to G \to 1. \tag{2.5}$$

Consequentemente, se $[\tilde{R}, \tilde{R}]$ denota o subgrupo comutador de $\tilde{R}$, então (2.5) induz a sequência

$$1 \to M \to \Gamma \to G \to 1,$$

onde $M = \tilde{R}/[\tilde{R}, \tilde{R}]$ e $\Gamma = F_2/[\tilde{R}, \tilde{R}]$. Pela [Joh97, Chap. 6, Prop. 2], M é um grupo abeliano livre cuja o posto é dado pela fórmula de Schreier $(\text{posto}(F_2) - 1)\delta + 1 = \delta + 1$.

Fato 2.4.1. *M é um subgrupo abeliano maximal de Γ.*

Demonstração. Suponha que essa afirmação é falsa. Então, podemos encontrar $x \in F_2$ tal que a imagem de x em G não é trivial, de modo que, $[x, r] \in [\tilde{R}, \tilde{R}]$ para todo $r \in \tilde{R}$. Note

que, $F = \langle x, \tilde{R} \rangle$ é um grupo livre de posto finito definindo a seguinte sequência exata

$$1 \to \tilde{R} \to F \to C \to 1,$$

onde $C \neq \{1\}$ é o grupo cíclico gerado pela imagem de x em G. Então,

$$M = \frac{\tilde{R}}{[\tilde{R}, \tilde{R}]} \text{ está no centro de } \frac{F}{[\tilde{R}, \tilde{R}]}$$

e, consequentemente, $F/[\tilde{R}, \tilde{R}]$ é abeliano e $[F, F] = [\tilde{R}, \tilde{R}]$. Como M tem índice finito em $F/[\tilde{R}, \tilde{R}]$, temos que $\text{posto}(\tilde{R}) = \text{posto}(F)$ (Cf. [Joh97, Chap. 6, Prop. 2]). Assim,

$$\text{posto}(\tilde{R}) = (\text{posto}(F) - 1)|C| + 1 \quad \Rightarrow \quad |C| = \frac{\text{posto}(F) - 1}{\text{posto}(F) - 1} = 1,$$

uma contradição, pois supomos $C \neq \{1\}$. Portanto, M é um subgrupo abeliano maximal de Γ. □

Fato 2.4.2. Γ *é livre de torção.*

Demonstração. Como $F_2/\tilde{R} \cong G$, temos que $[F_2, F_2] \leq \tilde{R}$. Então, $[\tilde{R}, \tilde{R}] \leq [F_2, F_2] \leq \tilde{R}$ e, consequentemente, $[F_2, F_2]/[\tilde{R}, \tilde{R}]$ é um subgrupo do grupo abeliano finitamente gerado livre de torção $M = \tilde{R}/[\tilde{R}, \tilde{R}]$. Logo, $[F_2, F_2]/[\tilde{R}, \tilde{R}]$ é livre de torção. Agora, uma vez que

$$\frac{F_2/[\tilde{R}, \tilde{R}]}{[F_2, F_2]/[\tilde{R}, \tilde{R}]} \cong \frac{F_2}{[F_2, F_2]} \cong \mathbb{Z} \times \mathbb{Z}$$

é livre de torção, segue que $\Gamma = F_2/[\tilde{R}, \tilde{R}]$ é livre de torção. □

Portanto, segue pela Proposição 1.5.5 que Γ é um grupo de Bieberbach de dimensão $\delta + 1$ com grupo de holonomia G. Agora, por [Ten97, Cor. 1] vemos que $M = \mathbb{Z}G \oplus \mathbb{Z}$ onde $\mathbb{Z}$ é um $\mathbb{Z}G$-módulo trivial. Assim, pelo Teorema F,

$$|\mathfrak{g}(\Gamma)| = \sum_{M \in T} \left(\prod_{p|\delta} |\mathcal{N}_{\text{Aut}(M)}(G) \backslash \mathbb{F}_p^*| \right),$$

uma vez que $\mathbb{Z}$ é o maior somando direto de M em que C_p age trivialmente para cada primo $p \mid \delta$. Como $\mathbb{Z}G$ é um $\mathbb{Z}G$-módulo permutacional (isto é, a $\mathbb{Z}$-base de $\mathbb{Z}G$ é fixada sobre a ação de G), temos que $G \leq \text{Sym}(G) \leq \text{GL}(\delta + 1, \mathbb{Z}) \cong \text{Aut}(M)$, onde $\text{Sym}(G)$ é o grupo de todas as permutações dos elementos de G. Consequentemente, $\mathcal{N}_{\text{Aut}(M)}(G)$ contém o normalizador de G em $\text{Sym}(G)$ e, portanto, contém $\text{Aut}(G)$ pelo

[Hal59, Thm. 6.3.2]. Então, $\mathcal{N}_{\mathrm{Aut}(M)}(G)$ age transitivamente em $\mathbb{F}_p^*$ para todo primo $p \mid \delta$, pois $\mathrm{Aut}(C_p) \leq \mathrm{Aut}(G)$ para todo primo $p \mid \delta$ (ver Lema 1.5.33). Logo,

$$|\mathfrak{g}(\Gamma)| = \left| \mathrm{Gal}(\zeta_\delta) \backslash \prod_{d|\delta} H(\mathbb{Z}[\zeta_d]) \right|,$$

pelo Teorema E.

Em particular, se $\delta = 6, 10, 14, 15, 21$ ou δ é primo ≤ 19, por exemplo, então $|\mathfrak{g}(\Gamma)| = 1$, porque para cada $d \mid \delta$ o grupo de classe $H(\mathbb{Z}[\zeta_d])$ é trivial (ver [AW04, Table 10]).

Agora, se $\delta = 46, 55, 105$ ou δ é primo > 19, por exemplo, então $|\mathfrak{g}(\Gamma)| > 1$, porque $23 \mid 46$ e $h(\mathbb{Z}[\zeta_{23}]) \geq 3$; $h(\mathbb{Z}[\zeta_{55}]) \geq 10$; $h(\mathbb{Z}[\zeta_{105}]) \geq 13$; e $h(\mathbb{Z}[\zeta_p]) > 1$ para todo primo $p > 19$ (ver [Was82, Thm. 11.1 e p. 353]).

Observação 2.4.3. *Em geral, calcular o normalizador de um grupo finito em* $\mathrm{GL}(n, \mathbb{Z})$ *não é fácil. Sugerimos ao leitor interessado ver [BNZ73], que apresenta um método para calcular tais normalizadores.*

Capítulo

3

Gênero Profinito do Grupo $\mathbb{Z}^2 \rtimes \mathbb{Z}$

Neste capítulo, exibimos cotas inferiores e superiores para a cardinalidade do gênero $\tilde{\mathfrak{g}}(\mathbb{Z}^2 \rtimes_A \mathbb{Z})$. Além disso, estabelecemos condições para que o gênero tenha cardinalidade igual a 1. Vale salientar que, se $B \in \mathrm{GL}(2,\mathbb{Z})$ é uma matriz de ordem finita, então $\mathbb{Z}^2 \rtimes_B \mathbb{Z}$ é um grupo de Bieberbach de dimensão 3. Logo, se os grupos de holonomia de $\mathbb{Z}^2 \rtimes_B \mathbb{Z}$ são cíclicos de ordem livres de quadrados, já sabemos quando a cardinalidade do gênero de $\mathbb{Z}^2 \rtimes_B \mathbb{Z}$ é igual a 1, pelo o que foi provado no Capítulo 2.

3.1 Condições para isomorfismo de produtos semidireto

Sejam H e N grupos e $\rho : H \to \mathrm{Aut}(N)$ um homomorfismo de grupos. Escrevemos $N \rtimes_\rho H$ para o correspondente produto semidireto, isto é, $N \rtimes_\rho H = N \times H$ munido com a multiplicação

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \rho_{h_1}(n_2), h_1 h_2)$$

para $n_1, n_2 \in N$ e $h_1, h_2 \in H$. As duas proposições a seguir estabelecem condições e caracterizações para o isomorfismo de produtos semidiretos. Denotamos por $\mathrm{Out}(H)$ o grupo de automorfismos externos de H, isto é, $\mathrm{Aut}(H)$ módulo os automorfismos internos de H.

Proposição 3.1.1 ([GZ11], Cor. 2.2)**.** *Sejam H, N grupos e $\varphi_1, \varphi_2 : H \to \mathrm{Aut}(N)$ homomorfismos. Sejam $G_1 = N \rtimes_{\varphi_1} H$ e $G_2 = N \rtimes_{\varphi_2} H$ os correspondentes produtos semidiretos e seja $f : G_1 \to G_2$ um isomorfismo tal que $f(N) = N$. Então, $\tilde{\varphi}_1(h)^{\tilde{f}^{-1}} = \tilde{\varphi}_2(f(h))$ para todo $h \in H$, onde $\tilde{f}$ é a imagem da restrição $f_{|_N}$ em $\mathrm{Out}(N)$ e $\tilde{\varphi}_i$ é a composição de φ_i com o homomorfismo natural $\mathrm{Aut}(N) \to \mathrm{Out}(N)$ para $i = 1, 2$. Em particular, $\tilde{\varphi}_1(H)$ e $\tilde{\varphi}_2(H)$ são conjugados em $\mathrm{Out}(N)$.*

Proposição 3.1.2 ([GZ11], Prop. 2.5)**.** *Sejam H, N grupos e $\rho_1, \rho_2 : H \to \mathrm{Aut}(N)$ homomorfismos. Sejam $G_1 = N \rtimes_{\rho_1} H$ e $G_2 = N \rtimes_{\rho_2} H$ os correspondentes produtos semidiretos. As seguintes afirmações valem.*

(i) Suponha que exista $\Theta \in \mathrm{Aut}(H)$ e $\bar{f} \in \mathrm{Aut}(N)$ tais que

$$\rho_1(h)^{\bar{f}^{-1}} = \rho_2(\Theta(h)) \tag{3.1}$$

para todo $h \in H$. Então, a aplicação $f : G_1 \to G_2$ definida por $f(n,h) = (\bar{f}(n), \Theta(h))$ é um isomorfismo que satisfaz $f(N) = N$ e $f(H) = H$.

(ii) Suponha agora que N é abeliano e que $f : G_1 \to G_2$ é um isomorfismo tal que $f(N) = N$. Defina $\bar{f} := f_{|_N}$ e $\Theta : H \to H$ pela indução de f para $G_1/N = H$. Então, o par $(\bar{f}, \Theta)$ satisfaz (3.1) e, consequentemente, também define um isomorfismo de G_1 para G_2.

Valem versões similares das Proposições 3.1.1 e 3.1.2 para grupos profinitos e homomorfismos contínuos. Vemos que as mesmas provas apresentadas em [GZ11] valem para essas reformulações.

Proposição 3.1.3. *Sejam H, N grupos profinitos e $\varphi_1, \varphi_2 : H \to \mathrm{Aut}(N)$ homomorfismos contínuos. Sejam $G_1 = N \rtimes_{\varphi_1} H$ e $G_2 = N \rtimes_{\varphi_2} H$ os correspondentes produtos semidiretos e seja $f : G_1 \to G_2$ um isomorfismo topológico tal que $f(N) = N$. Então, $\tilde{\varphi}_1(h)^{\tilde{f}^{-1}} = \tilde{\varphi}_2(f(h))$ para todo $h \in H$, onde $\tilde{f}$ é a imagem da restrição $f_{|_N}$ em $\mathrm{Out}(N)$ e $\tilde{\varphi}_i$ é a composição de φ_i com o homomorfismo natural $\mathrm{Aut}(N) \to \mathrm{Out}(N)$ para $i = 1, 2$. Em particular, $\tilde{\varphi}_1(H)$ e $\tilde{\varphi}_2(H)$ são conjugados em $\mathrm{Out}(N)$.*

Proposição 3.1.4. *Sejam H, N grupos profinitos e $\rho_1, \rho_2 : H \to \mathrm{Aut}(N)$ homomorfismos contínuos. Sejam $G_1 = N \rtimes_{\rho_1} H$ e $G_2 = N \rtimes_{\rho_2} H$ os correspondentes produtos semidiretos. As seguintes afirmações valem.*

(i) Suponha que exista $\Theta \in \mathrm{Aut}(H)$ e $\bar{f} \in \mathrm{Aut}(N)$ tais que

$$\rho_1(h)^{\bar{f}^{-1}} = \rho_2(\Theta(h)) \tag{3.2}$$

para todo $h \in H$. Então, a aplicação $f : G_1 \to G_2$ definida por $f(n,h) = (\bar{f}(n), \Theta(h))$ é um isomorfismo topológico que satisfaz $f(N) = N$ e $f(H) = H$.

(ii) Suponha agora que N é um subgrupo fechado abeliano e que $f : G_1 \to G_2$ é um isomorfismo topológico tal que $f(N) = N$. Defina $\bar{f} := f_{|_N}$ e $\Theta : H \to H$ pela indução de f para $G_1/N = H$. Então, o par $(\bar{f}, \Theta)$ satisfaz (3.2) e, consequentemente, também define um isomorfismo topológico de G_1 para G_2.

Agora vamos estudar os isomorfismos de produtos semidiretos de $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ por $\mathbb{Z}$. Note que o homomorfismo $\rho : \mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}(2, \mathbb{Z})$ é determinado por $\rho(1) = A \in \mathrm{GL}(2, \mathbb{Z})$. Assim, para $A \in \mathrm{GL}(2, \mathbb{Z})$ vamos denotar por G_A o produto semidireto $N \rtimes_A C$, onde $N \cong \mathbb{Z}^2$ e $C \cong \mathbb{Z}$ de modo que o gerador $1 \in C$ age em N via A.

Lema 3.1.5. *Seja $A \in \mathrm{GL}(2, \mathbb{Z})$ tal que nenhum dos seus autovalores é igual a 1. Seja $G_A = N \rtimes_A C$. Então,*

(i) $(\mathrm{id} - A)(N)$ *é um subgrupo de índice finito de N.*

(ii) O subgrupo derivado de G_A é igual a $(\mathrm{id} - A)(N)$.

Demonstração. Vamos escrever G_A como os pares $(x, i) \in N \times C$ com a multiplicação

$$(x, i)(y, j) = (x + A^i y, i + j).$$

(i) Considere a aplicação

$$f : N \to N$$

$$x \mapsto x - Ax.$$

É imediato verificar que f é um homomorfismo. Logo, $f(N) = (\mathrm{id} - A)(N)$ é um subgrupo de N.

Suponha agora que 1 não é autovalor de A. Neste caso, f é injetiva, pois se $x \in \ker(f)$ temos que

$$0 = f(x) = x - Ax \quad \Rightarrow Ax = x \quad \Rightarrow x = 0.$$

Assim, $(\mathrm{id} - A)(N) \cong n\mathbb{Z} \times m\mathbb{Z}$ para alguns inteiros não nulos n e m. Portanto, $(\mathrm{id} - A)(N)$ tem índice finito em N.

(ii) Note que, o quociente

$$\frac{G_A}{(\mathrm{id} - A)(N)} = \frac{N}{(\mathrm{id} - A)(N)} \rtimes_A C$$

é um grupo abeliano, pois A age trivialmente em $N/(\mathrm{id} - A)(N)$. Assim,

$$[G_A, G_A] \leq (\mathrm{id} - A)(N).$$

Por outro lado, temos que

$$\begin{aligned}(x - Ax, 0) &= (x, i)(Ax, i)^{-1} \\ &= (x, i)\left((0,1)(x,i)(0,1)^{-1}\right)^{-1} \\ &= (x, i)(0,1)(x,i)^{-1}(0,1)^{-1},\end{aligned}$$

para quaisquer $x \in N$ e $i \in C$. Então, $(\mathrm{id} - A)(N) \subseteq [G_A, G_A]$ e, portanto, $[G_A, G_A] = (\mathrm{id} - A)(N)$, como queríamos.

□

Sejam A e B matrizes em $\mathrm{GL}(2, \mathbb{Z})$. Considere os produtos semidiretos $G_A = N_1 \rtimes_A C$ e $G_B = N_2 \rtimes_B C$, onde $N_1 \cong \mathbb{Z} \times \mathbb{Z} \cong N_2$ e $C \cong \mathbb{Z}$.

Lema 3.1.6.

(i) Sejam A e B matrizes em $\mathrm{GL}(2, \mathbb{Z})$ tais que nenhum dos seus autovalores é igual a 1. Se $f : G_A \to G_B$ é um isomorfismo, então $f(N_1) = N_2$.

(ii) Sejam A e B matrizes em $\mathrm{GL}(2, \widehat{\mathbb{Z}})$ tais que nenhum dos seus autovalores é igual a 1. Se $f : \widehat{G}_A \to \widehat{G}_B$ é um isomorfismo, então $f(\widehat{N}_1) = \widehat{N}_2$.

Demonstração. (i) Pelo Lema 3.1.5, temos que o subgrupo derivado $[G_B, G_B]$ tem índice finito em N_2. Considere

$$L = \{\alpha \in G_B : \exists\ n \in \mathbb{Z}, n \neq 0, \text{ tal que } \alpha^n \in [G_B, G_B]\}.$$

Afirmamos que $L = N_2$. Com efeito, como o índice de $[G_B, G_B]$ em N_2 é finito segue que $N_2 \subseteq L$. Por outro lado, se $\alpha = (x, i) \in L$ $(x \in N_2, i \in C)$, então existe $n \in \mathbb{Z},\ n \neq 0$, tal que $\alpha^n \in [G_B, G_B] \leq N_2$. Note que,

$$\alpha^n = (x, i)^n = (x + A^i x + \cdots + A^{(n-1)i} x, ni).$$

Uma vez que $\alpha^n \in N_2$ e $n \neq 0$, temos que $i = 0$. Logo, $L \subseteq N_2$ e, portanto, $L = N_2$.

Seja $x \in N_1$, então existe $n \in \mathbb{Z},\ n \neq 0$, tal que $x^n \in [G_A, G_A]$. Consequentemente, $f(x)^n \in [G_B, G_B]$ e assim $f(x) \in N_2$. Portanto, $f(N_1) \subseteq N_2$. Por um argumento similar, $N_2 \subseteq f(N_1)$.

(ii) Isto segue do item (i) com Proposição 1.1.5.

□

3.2 Conjugação em $\mathrm{GL}(2,\mathbb{Z})$ e $\mathrm{GL}(2,\widehat{\mathbb{Z}})$

Nesta seção, continuamos escrevendo $G_A = N_1 \rtimes_A C$ e $G_B = N_2 \rtimes_B C$, onde $N_1 \cong \mathbb{Z}^2 \cong N_2$ e $C \cong \mathbb{Z}$.

Lema 3.2.1. *Seja $A \in \mathrm{GL}(2,\mathbb{Z})$. Então, $G_A \cong G_{A^{-1}}$.*

Demonstração. Lembre-se que G_A denota o grupo dos pares (u,r) com $r \in N_1, r \in C$ e com a multiplicação

$$(u,r)(v,s) = (u + A^r v, r + s).$$

Considere a aplicação

$$f : G_A \to G_{A^{-1}}$$

$$(u,r) \mapsto (u,-r).$$

É imediato verificar que f é uma bijeção. Mais que isso, f é um isomorfismo, pois

$$\begin{aligned} f((u,r)(v,s)) &= f(u + A^r v, r + s) \\ &= (u + A^r v, -r - s) \\ &= (u + (A^{-1})^{-r} v, -r - s) \\ &= (u,-r)(v,-s) \\ &= f(u,r)f(v,s). \end{aligned}$$

□

O próximo lema nos dá uma condição necessária e suficiente para os grupos G_A e G_B serem isomorfos.

Lema 3.2.2. *Sejam A e B matrizes em $\mathrm{GL}(2,\mathbb{Z})$ de tal forma que nenhum dos seus autovalores é igual a 1. Então, G_A e G_B são isomorfos se, e somente se, A é conjugada a B ou B^{-1} em $\mathrm{GL}(2,\mathbb{Z})$.*

Demonstração. ($\Rightarrow$) Segue do Lema 3.1.6 (i) que se $f : G_A \to G_B$ é um isomorfismo, então a restrição de f para N_1 define um isomorfismo $P : N_1 \to N_2$. Então, $P \in \mathrm{GL}(2,\mathbb{Z})$. Vamos escrever $f(0,1) = (v,t)$, onde $v \in N_1$ e $t \in C$. Note que

$$(0,1)(x,0)(0,-1) = (Ax,0).$$

Assim,

$$\begin{aligned}(PAx, 0) &= f((0,1)(x,0)(0,-1)) \\ &= f(0,1)f(x,0)f(0,-1) \\ &= (v,t)(Px,0)(v,t)^{-1} \\ &= (v + B^tPx, t)(B^{-t}(-v), -t) \\ &= (B^tPx, 0).\end{aligned}$$

Logo, $B^tP = PA$. Vamos mostrar agora que $t = \pm 1$. Para isso note que,

$$\begin{aligned}f(-P^{-1}v, 1) &= f((P^{-1}(-v), 0)(0,1)) \\ &= (PP^{-1}(-v), 0)f(0,1) \\ &= (-v, 0)(v,t) \\ &= (0,t).\end{aligned}$$

Como $(0,1)^t = (0,t)$, implica que existe $\beta \in G_A$ tal que $\beta^t = (-P^{-1}v, 1)$. Então, t divide 1 e, consequentemente, $t = \pm 1$. Portanto, $PAP^{-1} = B$ ou $PAP^{-1} = B^{-1}$.

($\Leftarrow$) Segue pela Proposição 3.1.2 que se $B = PAP^{-1}$ com $P \in \mathrm{GL}(2,\mathbb{Z})$, então $G_A \cong G_B$. Agora, suponha que $B^{-1} = PAP^{-1}$, onde $P \in \mathrm{GL}(2,\mathbb{Z})$. Novamente, pela Proposição 3.1.2 temos que $G_A \cong G_{B^{-1}}$. Pelo Lema 3.2.1 temos que $G_{B^{-1}} \cong G_B$. Portanto, $G_A \cong G_B$. □

Vale uma versão profinita do Lema 3.2.2.

Lema 3.2.3. *Sejam A e B matrizes em $\mathrm{GL}(2,\mathbb{Z})$ tais que nenhum dos seus autovalores é igual a 1. Então, $\widehat{G}_A$ e $\widehat{G}_B$ são isomorfos se, e somente se, A é conjugada a B ou B^{-1} em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$.*

Demonstração. ($\Rightarrow$) Pelo Lema 3.1.6 (ii) temos que se $f : \widehat{G}_A \to \widehat{G}_B$ é um isomorfismo, então a restrição de f para $\widehat{N}_1$ define um isomorfismo $P : \widehat{N}_1 \to \widehat{N}_2$. Então, $P \in \mathrm{GL}(2,\widehat{\mathbb{Z}})$. Suponha que $f(0,1) = (v,t)$, onde $v \in \widehat{N}_1$ e $t \in \widehat{C}$. Note que,

$$(0,1)(x,0)(0,-1) = (Ax, 0).$$

Agora, como na prova do Lema 3.2.2, concluímos que $B^t = PAP^{-1}$ onde t é uma unidade de $\widehat{C}$. Uma vez que $\det(B) \in \mathbb{Z}$ e

$$\det(B^t) = (\det(B))^t \in \mathbb{Z}$$

concluímos que $t = \pm 1$.

($\Leftarrow$) Suponha que exista $P \in \mathrm{GL}(2,\widehat{\mathbb{Z}})$ tal que $B = PAP^{-1}$. Segue pela Proposição 3.1.4 que $\widehat{N}_1 \rtimes_A \widehat{C} \cong \widehat{N}_2 \rtimes_B \widehat{C}$. Agora se $B^{-1} = PAP^{-1}$ temos que $\widehat{N}_1 \rtimes_A \widehat{C} \cong \widehat{N}_2 \rtimes_{B^{-1}} \widehat{C}$ também pela Proposição 3.1.4. Como $N_1 \rtimes_{B^{-1}} C \cong N_2 \rtimes_B C$ pelo Lema 3.2.1, temos que $\widehat{N}_1 \rtimes_{B^{-1}} \widehat{C} \cong \widehat{N}_2 \rtimes_B \widehat{C}$. Assim, $\widehat{N}_1 \rtimes_A \widehat{C} \cong \widehat{N}_2 \rtimes_B \widehat{C}$. Agora usando a Proposição 1.1.5 temos que $\widehat{G}_A \cong \widehat{G}_B$ em ambos os casos. □

Lema 3.2.4. *Sejam C e D matrizes em $\mathrm{GL}(2,\mathbb{Z})$. Se C e D são conjugadas em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$, então*

(i) $\det(C) = \det(D)$.

(ii) $\mathrm{tr}(C) = \mathrm{tr}(D)$.

(iii) C e D têm o mesmo polinômio característico.

Demonstração. Se C e D são matrizes conjugadas em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$, então para cada inteiro positivo m, temos que:

- $\det(C)$ é congruente a $\det(D)$ módulo m.
- $\mathrm{tr}(C)$ é congruente a $\mathrm{tr}(D)$ módulo m.

Logo, $\det(C) = \det(D)$ e $\mathrm{tr}(C) = \mathrm{tr}(D)$.

Uma vez que os polinômios característicos de C e D são $p_C(x) = x^2 - \mathrm{tr}(C)x + \det(C)$ e $p_D(x) = x^2 - \mathrm{tr}(D)x + \det(D)$, respectivamente, (iii) segue de (i) e (ii). □

Proposição 3.2.5. *Sejam $A, B \in \mathrm{GL}(2,\mathbb{Z})$ e considere os produtos semidiretos $G_A = N_1 \rtimes_A C$ e $G_B = N_2 \rtimes_B C$ com $N_1 \cong \mathbb{Z}^2 \cong N_2$ e $C \cong \mathbb{Z}$. Se $G_B \in \tilde{\mathfrak{g}}(G_A)$, então as matrizes A e B têm os mesmos autovalores.*

Demonstração. Sejam $A, B \in \mathrm{GL}(2,\mathbb{Z})$. Note que os polinômios característicos de A e B são

$$f_A(x) = x^2 - \mathrm{tr}(A)x + \det(A) \quad \text{e} \quad f_B(x) = x^2 - \mathrm{tr}(B)x + \det(B).$$

Vamos dividir a prova em três casos.

Caso 1: Se $|\mathrm{tr}(A)| < 2$.

Neste caso, temos que A é uma matriz de ordem finita e, consequentemente, G_A é um grupo de Bieberbach de dimensão 3 (Cf. [Sco83, p. 481]). Como $G_B \in \tilde{\mathfrak{g}}(G_A)$, segue pela Proposição 2.1.4 e Lema 2.1.3 que G_B é também um grupo de Bieberbach de dimensão 3 de modo que as matrizes A e B são conjugadas em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$. Assim, pelo Lema 3.2.4 temos que A e B têm os mesmos autovalores.

Caso 2: Se $|\mathrm{tr}(A)| = 2$ e $\det(A) = 1$.

Neste caso, temos que A tem todos os seus autovalores iguais a 1 ou -1. Se todos os autovalores de A são iguais a 1 temos que G_A é nilpotente (ver (Cf. [Sco83, p. 481]) ou Lema 3.3.2). Assim, $\widehat{G}_A$ também é um grupo nilpotente por [Seg83, Thm. 2, p. 231]. Consequentemente, $\widehat{G}_B$ também é um grupo nilpotente e, portanto, todos os autovalores de B são iguais a 1 (caso contrário, se B tem um dos seus autovalores diferentes de 1, então o centro de $\widehat{G}_B$ é trivial, assim, $\widehat{G}_B$ não é nilpotente).

Agora, se todos os autovalores de A são iguais a -1, temos que G_A é um grupo de Bieberbach de dimensão 3 (Cf. [Sco83, p. 481]). Assim, o resultado segue por argumentos análogos aos do Caso 1.

Caso 3: Se $|\mathrm{tr}(A)| > 2$, ou se $|\mathrm{tr}(A)| = 2$ e $\det(A) = -1$.

Neste caso, temos que os autovalores de A são números reais diferentes de ± 1. Consequentemente, A tem ordem infinita e G_A é um grupo solúvel que não é nilpotente (Cf. [Sco83, p. 481]). Logo, se $G_B \in \tilde{\mathfrak{g}}(G_A)$ temos que B tem todos os seus autovalores distintos e diferentes de ± 1. Assim, A e B são matrizes conjugadas em $\mathrm{GL}(2, \widehat{\mathbb{Z}})$ pelo Lema 3.2.3. Portanto, pelo Lema 3.2.4, A e B têm os mesmo autovalores. □

O próximo lema nos diz que matrizes em $\mathrm{GL}(2, \mathbb{Z})$ com determinante igual a -1 não são conjugadas a sua inversa.

Lema 3.2.6. *Seja $A \in \mathrm{GL}(2, \mathbb{Z})$ tal que $\det(A) = -1$. Então, $\mathrm{tr}(A^{-1}) = -\mathrm{tr}(A)$.*

Demonstração. Seja $A \in \mathrm{GL}(2, \mathbb{Z})$. Já sabemos que o polinômio característico de A é

$$p_A(x) = x^2 - \mathrm{tr}(A)x + \det(A)$$

e que seus autovalores são

$$\lambda_{\pm} = \frac{\mathrm{tr}(A) \pm \sqrt{(\mathrm{tr}(A))^2 - 4\det(A)}}{2}.$$

Note que,

$$\begin{aligned} \frac{\det(A)}{\lambda_+} &= \frac{2\det(A)}{\mathrm{tr}(A) + \sqrt{(\mathrm{tr}(A))^2 - 4\det(A)}} \\ &= \frac{\mathrm{tr}(A) - \sqrt{(\mathrm{tr}(A))^2 - 4\det(A)}}{2} \\ &= \lambda_-. \end{aligned}$$

Assim, como o traço de A^{-1} é igual ao traço da matriz diagonal de A^{-1}, temos

$$\begin{aligned}
\mathrm{tr}(A^{-1}) &= \frac{1}{\lambda_+} + \frac{1}{\lambda_-} \\
&= \frac{1}{\lambda_+} + \frac{\lambda_+}{\det(A)} \\
&= \frac{2}{\mathrm{tr}(A) + \sqrt{(\mathrm{tr}(A))^2 - 4\det(A)}} + \frac{\mathrm{tr}(A) + \sqrt{(\mathrm{tr}(A))^2 - 4\det(A)}}{2\det(A)} \\
&= \frac{\mathrm{tr}(A) - \sqrt{(\mathrm{tr}(A))^2 - 4\det(A)}}{2\det(A)} + \frac{\mathrm{tr}(A) + \sqrt{(\mathrm{tr}(A))^2 - 4\det(A)}}{2\det(A)} \\
&= \frac{\mathrm{tr}(A)}{\det(A)}.
\end{aligned}$$

Portanto, se $\det(A) = -1$, então $\mathrm{tr}(A^{-1}) = -\mathrm{tr}(A)$. □

Corolário 3.2.7. *Seja A uma matriz em $\mathrm{GL}(2,\mathbb{Z})$ tal que $\det(A) = -1$ e nenhum dos seus autovalores é igual a 1. Então, a cardinalidade do gênero $\tilde{\mathfrak{g}}(G_A)$ de G_A é igual ao número de classes de conjugação de matrizes em $\mathrm{GL}(2,\mathbb{Z})$ que pertencem a classe de conjugação de A em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$.*

Demonstração. Suponha que exista $B \in \mathrm{GL}(2,\mathbb{Z})$ que não é conjugada a A em $\mathrm{GL}(2,\mathbb{Z})$ mas é conjugada a A em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$. Então, $\mathrm{tr}(A) = \mathrm{tr}(B)$ e $\det(A) = \det(B)$ pelo Lema 3.2.4. Como $\det(A) = -1$, temos que $\mathrm{tr}(B^{-1}) = -\mathrm{tr}(B)$. Consequentemente, B^{-1} não é conjugada a B e nem A em $\mathrm{GL}(2,\mathbb{Z})$. Portanto, a afirmação segue pelos Lemas 3.2.3 e 3.2.2. □

Assim, se os grupos G_A e G_B estão em $\tilde{\mathfrak{g}}(G_A)$, as matrizes A e B têm polinômios característicos iguais. Como isso, para estudar até que ponto as matrizes A e B são conjugadas em $\mathrm{GL}(2,\mathbb{Z})$, precisamos estudar o conjunto das classes de conjugação de matrizes em $\mathrm{GL}(2,\mathbb{Z})$ que têm o mesmo polinômio característico. Para este propósito, o próximo teorema nos diz que é suficiente estudar as classe de ideais de ordens de corpos quadráticos.

Teorema 3.2.8 (Latimer-MacDuffee, [New72], Thm. III. 13)**.** *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio mônico de grau n que é irredutível sobre $\mathbb{Q}$ e seja λ uma raiz de $f(x)$. Então, existe uma correspondência biunívoca entre as $\mathbb{Z}$-classes de conjugação de matrizes $n \times n$ sobre $\mathbb{Z}$, com polinômio característico f, e as classes de ideais da ordem $\mathbb{Z}[\lambda]$.*

Nesta tese estamos interessados no caso em que $n = 2$. Seja

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z})$$

com polinômio característico $f(x) = x^2 - \mathrm{tr}(A) + \det(A)$. Então,

$$\lambda = \frac{\mathrm{tr}(A) + \sqrt{\mathrm{tr}(A)^2 - 4\det(A)}}{2}$$

é um autovalor de A. Um autovetor correspondente para λ é $v = (b, \lambda - a)$. De fato, note que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} b \\ \lambda - a \end{pmatrix} = \begin{pmatrix} ab + b(\lambda - a) \\ bc + d(\lambda - a) \end{pmatrix} = \begin{pmatrix} b\lambda \\ d\lambda - \det(A) \end{pmatrix}. \tag{3.3}$$

Por outro lado,

$$\lambda \begin{pmatrix} b \\ \lambda - a \end{pmatrix} = \begin{pmatrix} b\lambda \\ \lambda^2 - a\lambda \end{pmatrix}. \tag{3.4}$$

Uma vez que,

$$f(\lambda) = \lambda^2 - (a + d)\lambda + \det(A) = 0 \quad \Rightarrow \quad \lambda^2 - a\lambda = d\lambda - \det(A),$$

segue que as equações em (3.3) e (3.4) são iguais. Logo, $Av = \lambda v$.

Agora considere o $\mathbb{Z}$-módulo

$$I_A = \langle b, \lambda - a \rangle = \{mb + n(\lambda - a) : m, n \in \mathbb{Z}\}. \tag{3.5}$$

Teorema 3.2.9 ([Hen97], Thm. 1)**.** *I_A é um ideal da ordem $\mathbb{Z}[\lambda]$.*

Temos a seguinte versão do Teorema 3.2.8 para $\mathrm{GL}(2, \mathbb{Z})$.

Proposição 3.2.10 ([Hen97], Thm. 2)**.** *Sejam A e B matrizes em $\mathrm{GL}(2, \mathbb{Z})$ com o mesmo polinômio característico $f(x)$. Então, A e B são matrizes conjugadas em $\mathrm{GL}(2, \mathbb{Z})$ se, e somente se, os ideais correspondentes I_A e I_B estão na mesma classe de ideais de $\mathbb{Z}[\lambda]$, onde λ é uma raiz de $f(x)$.*

Seja λ um autovalor da matriz $A \in \mathrm{GL}(2, \mathbb{Z})$. Para qualquer $\mathbb{Z}[\lambda]$-ideal fracionário I, a multiplicação por λ é uma aplicação $\mathbb{Z}$-linear, isto é, $m_{I,\lambda} : I \to I$ definida por $x \mapsto x\lambda$. Uma vez que I é um $\mathbb{Z}$-módulo, escolhendo uma $\mathbb{Z}$-base podemos representar

$m_{I,\lambda}$ por uma matriz 2×2 $[m_{I,\lambda}]$ com entradas inteiras. Note que, se λ é uma unidade de $\mathbb{Z}[\lambda]$, temos que $m_{I,\lambda}$ é uma bijeção (isso porque a aplicação $m_{I,\lambda^{-1}} : I \to I$ definida por $x \mapsto x\lambda^{-1}$ é uma inversa para $m_{I,\lambda}$). Assim, se λ é uma unidade de $\mathbb{Z}[\lambda]$, temos que $[m_{I,\lambda}] \in \mathrm{GL}(2,\mathbb{Z})$.

Lema 3.2.11. *Seja $A \in \mathrm{GL}(2,\mathbb{Z})$ com autovalores distintos e $\mathrm{tr}(A) \neq 0$. Sejam I e J ideais em classes distintas de $H(\mathbb{Z}[\lambda])$, onde λ é um autovalor de A. Então, as matrizes $[m_{I,\lambda}]$ e $[m_{J,\lambda}]$ não são conjugadas em $\mathrm{GL}(2,\mathbb{Z})$.*

Demonstração. Inicialmente, como λ é uma raiz do polinômio $p(x) = x^2 - \mathrm{tr}(A)x + \det(A)$, temos que λ é um inteiro algébrico do corpo quadrático $K = \mathbb{Q}(\lambda)$. Como $\det(A) = \pm 1$, implica que $N(\lambda) = \pm 1$ e, então, λ é uma unidade da ordem $\mathbb{Z}[\lambda]$.

Sejam $B_1 = \{v_1, w_1\}$ e $B_2 = \{v_2, w_2\}$ duas $\mathbb{Z}$-bases fixadas para os $\mathbb{Z}$-módulos I e J, respectivamente. Considere as representações matriciais $[m_{I,\lambda}]$ e $[m_{J,\lambda}]$ dos automorfismos $\mathbb{Z}$-lineares $m_{I,\lambda} : I \to I$ e $m_{J,\lambda} : J \to J$ definidos pelas multiplicações por λ com respeito as bases B_1 e B_2, respectivamente. Vamos denotar por $\{e_1, e_2\}$ a base canônica de $\mathbb{Z}^2$. Agora, considere os isomorfismos $\mathbb{Z}$-lineares $f : I \to \mathbb{Z}^2$ e $g : J \to \mathbb{Z}^2$ tais que $f(v_1) = e_1 = g(v_2)$ e $f(w_1) = e_2 = g(w_2)$. Segue por construção que os diagramas

$$\begin{array}{ccc} I & \xrightarrow{f} & \mathbb{Z}^2 \\ \downarrow{\scriptstyle m_{I,\lambda}} & & \downarrow{\scriptstyle [m_{I,\lambda}]} \\ I & \xrightarrow{f} & \mathbb{Z}^2 \end{array} \quad \text{e} \quad \begin{array}{ccc} J & \xrightarrow{g} & \mathbb{Z}^2 \\ \downarrow{\scriptstyle m_{J,\lambda}} & & \downarrow{\scriptstyle [m_{J,\lambda}]} \\ J & \xrightarrow{g} & \mathbb{Z}^2 \end{array}$$

são comutativos.

Suponha que as matrizes $[m_{I,\lambda}]$ e $[m_{J,\lambda}]$ são conjugadas em $\mathrm{GL}(2,\mathbb{Z})$, isto é, que existe uma matriz $P \in \mathrm{GL}(2,\mathbb{Z})$ tal que $P^{-1}[m_{I,\lambda}]P = [m_{J,\lambda}]$. Assim, obtemos o seguinte diagrama de isomorfismos $\mathbb{Z}$-lineares

$$\begin{array}{ccccccc} I & \xrightarrow{f} & \mathbb{Z}^2 & \xrightarrow{P} & \mathbb{Z}^2 & \xrightarrow{g^{-1}} & J \\ \downarrow{\scriptstyle m_{I,\lambda}} & & \downarrow{\scriptstyle [m_{I,\lambda}]} & & \downarrow{\scriptstyle [m_{J,\lambda}]} & & \downarrow{\scriptstyle m_{J,\lambda}} \\ I & \xrightarrow{f} & \mathbb{Z}^2 & \xrightarrow{P} & \mathbb{Z}^2 & \xrightarrow{g^{-1}} & J\,. \end{array}$$

Como cada quadrado do diagrama é comutativo, temos que todo o diagrama é comutativo. Afirmamos que a composição $g^{-1}Pf : I \to J$ é um isomorfismo de $\mathbb{Z}[\lambda]$-módulos. De fato, note que para cada $\alpha \in I$ temos

$$g^{-1}Pf(\alpha\lambda) = g^{-1}Pf(m_{I,\lambda}(\alpha)) = m_{J,\lambda}g^{-1}Pf(\alpha) = g^{-1}Pf(\alpha)\lambda.$$

Uma vez que a composição $g^{-1}Pf : I \to J$ é claramente um isomorfismo $\mathbb{Z}$-linear, segue que $g^{-1}Pf : I \to J$ é um isomorfismo de $\mathbb{Z}[\lambda]$-módulos. Considere agora a extensão $g^{-1}Pf : I \to J$ para um K-isomorfismo $\psi : KI \to KJ$. Então temos

$$\psi(m\xi) = \psi(m)\xi, \quad m \in KI,\ \xi \in K.$$

Em particular, se $m = 1$ e restringindo ξ para I, temos que

$$g^{-1}Pf(\xi) = \psi(\xi) = \psi(1)\xi, \quad \xi \in I.$$

Portanto, $g^{-1}Pf : I \to J$ é a multiplicação por $\psi(1)$ e, assim, $I = \psi(1)J$. Logo, I e J estão na mesma classe de ideais, uma contradição. Portanto, as matrizes $[m_{I,\lambda}]$ e $[m_{J,\lambda}]$ não são conjugadas em $\mathrm{GL}(2,\mathbb{Z})$. □

Seja $A \in \mathrm{GL}(2,\mathbb{Z})$ uma matriz fixada. Definimos

$$\approx_A\text{-class} := \{B \in \mathrm{GL}(2,\mathbb{Z}) : B \text{ é conjugada a } A \text{ em } \mathrm{GL}(2,\widehat{\mathbb{Z}})\}.$$

Recorde-se que $h(\mathbb{Z}[\lambda])$ denota a ordem do grupo de classes de ideais de $\mathbb{Z}[\lambda]$, onde λ é um autovalor de A.

Proposição 3.2.12. *Seja A uma matriz em $\mathrm{GL}(2,\mathbb{Z})$ tais que seus autovalores são distintos e $\mathrm{tr}(A) \neq 0$. Seja λ um autovalor de A. Se a classe de conjugação de A corresponde para uma classe de ideais invertíveis $[I_A]$ de $\mathbb{Z}[\lambda]$, onde I_A é como em (3.5), então existe pelo menos $h(\mathbb{Z}[\lambda])$ matrizes em $\approx_A$-class que não são conjugadas duas a duas.*

Demonstração. Sejam $I_1, \cdots, I_k$ representantes das classes distintas de ideais do grupo $H(\mathbb{Z}[\lambda])$. Pelo Lema 1.2.39, podemos supor que cada I_i é relativamente primo para o condutor $f = |\mathcal{O}_K : \mathbb{Z}[\lambda]|$. Seja B_i uma $\mathbb{Z}$-base fixada para cada I_i e considere $A_i \in \mathrm{GL}(2,\mathbb{Z})$ a matriz de multiplicação por λ em relação a base B_i, $i = 1, \cdots, k$. Pelo Lema 3.2.11, as matrizes A_i e A_j não são conjugadas sempre que $i \neq j$.

Por outro lado, pelo Lema 1.2.40,

$$\frac{I_i}{p^l I_i} \cong \frac{\mathbb{Z}[\lambda]}{p^l\mathbb{Z}[\lambda]} \tag{3.6}$$

como $\mathbb{Z}[\lambda]/p^l\mathbb{Z}[\lambda]$-módulos, para todo primo p e $l \in \mathbb{N}$. Agora, considere as imagens canônicas $\bar{A}_i, \bar{A}_1$ em $\mathrm{GL}(2,\mathbb{Z}/p^l\mathbb{Z})$ das matrizes A_i, A_1. Por (3.6), vemos que $\bar{A}_i$ é conjugada a $\bar{A}_1$ em $\mathrm{GL}(2,\mathbb{Z}/p^l\mathbb{Z})$ para todo $l \in \mathbb{N}$ e todo $i = 1, \cdots, k$. Logo, as matrizes A_i e A_1 são conjugadas em $\mathrm{GL}(2,\mathbf{Z}_p)$ para todo primo p e $i = 1, \cdots, k$. Consequentemente, A_i é

conjugada a A_1 em

$$\mathrm{GL}(2, \widehat{\mathbb{Z}}) = \prod_p \mathrm{GL}(2, \mathbf{Z}_p),$$

para cada $i = 1, \cdots, k$.

Como a classe de conjugação da matriz A corresponde para uma classe de ideais invertível $[I_A]$ de $\mathbb{Z}[\lambda]$, segue pelo Teorema 3.2.8 que existe $j \in \{1, \cdots, k\}$ tal que A é conjugada a A_j em $\mathrm{GL}(2, \mathbb{Z})$. Portanto, existem pelo menos $h(\mathbb{Z}[\lambda])$ matrizes em $\approx_A$-class que não são conjugadas duas a duas. □

O próximo resultado será útil posteriormente.

Lema 3.2.13 ([CT91], Lem. 3.2)**.** *Sejam A e B matrizes em $\mathrm{GL}(2, \mathbb{Z})$. Se $\det(A) = \det(B)$ e $\mathrm{tr}(A) = \mathrm{tr}(B) \neq 0$, então A é conjugada a B em $\mathrm{GL}(2, \mathbb{Z})$ se, e somente se, A^2 é conjugada a B^2 em $\mathrm{GL}(2, \mathbb{Z})$.*

3.3 O gênero de $\mathbb{Z}^2 \rtimes \mathbb{Z}$ – Caso nilpotente

Nesta seção, vamos calcular a cardinalidade do gênero $\tilde{\mathfrak{g}}(G_A)$, quando $G_A = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$ é um grupo nilpotente.

Lema 3.3.1 ([DK18], Lem. 13.27)**.** *Se uma matriz A em $\mathrm{GL}(n, \mathbb{Z})$ tem todos os seus autovalores iguais a 1, então existe uma série ascendente finita de subgrupos*

$$\{1\} = \Lambda_0 \leq \Lambda_1 \leq \cdots \leq \Lambda_{n-1} \leq \Lambda_n = \mathbb{Z}^n$$

tal que $\Lambda_i \cong \mathbb{Z}^i$, $\Lambda_{i+1}/\Lambda_i \cong \mathbb{Z}$ para todo $i \geq 0$, $A(\Lambda_i) = \Lambda_i$ e A age em Λ_{i+1}/Λ_i como a identidade.

Lema 3.3.2. *Seja $A \neq I$ uma matriz em $\mathrm{GL}(2, \mathbb{Z})$. Então, o grupo G_A é nilpotente se, e somente se, todos os autovalores de A são iguais a 1. Além disso, a classe de nilpotência de G_A é igual a 2.*

Demonstração. ($\Rightarrow$) Note que, se a matriz A tem pelo menos um autovalor diferente de 1, então o centro do grupo G_A é trivial e, consequentemente, G_A não é nilpotente.

($\Leftarrow$) Seja $A \in \mathrm{GL}(2, \mathbb{Z})$ tendo todos os seus autovalores iguais a 1. Pelo Lema 3.3.1,

$$\{1\} \leq \mathbb{Z} \leq \mathbb{Z}^2$$

é uma série de $\mathbb{Z}^2$ tal que A age em $\mathbb{Z}^2/\mathbb{Z}$ e $\mathbb{Z}$ como a identidade. Assim, $\mathbb{Z}$ é um subgrupo central de G_A, isto é, $\mathbb{Z}$ está contido no centro $Z_1(G_A)$ de G_A. Note que, G_A é nilpotente

de classe 2 se, e somente se, temos a seguinte série central superior

$$\{1\} = Z_0(G_A) \leq Z_1(G_A) \leq Z_2(G_A) = G_A,$$

se, e somente se, o grupo $G_A/Z_1(G_A)$ é abeliano. O que é o caso, pois o grupo

$$\frac{\mathbb{Z}^2}{\mathbb{Z}} \rtimes_A \mathbb{Z} \cong \frac{G_A}{\mathbb{Z}}$$

é abeliano (porque A age trivialmente em $\mathbb{Z}^2/\mathbb{Z}$) e

$$\frac{G_A}{Z_1(G_A)} \cong \frac{G_A/\mathbb{Z}}{Z_1(G_A)/\mathbb{Z}}.$$

□

Agora podemos provar o principal resultado desta seção.

Teorema J. *Seja $A \in \mathrm{GL}(2,\mathbb{Z})$ e considere o produto semidireto $G_A = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$. Se todos os autovalores de A são iguais a 1, então $|\tilde{\mathfrak{g}}(G_A)| = 1$.*

Demonstração. Se $A = I$, então o grupo $G_A \cong \mathbb{Z}^3$ e o resultado segue [Rei18, Prop. 3.1]. Agora, suponha que $A \neq I$ e que tem todos os seus autovalores iguais a 1. Seja $B \in \mathrm{GL}(2,\mathbb{Z})$ tal que $\widehat{G}_A \cong \widehat{G}_B$. Segue pela Proposição 3.2.5 que B também tem todos os seus autovalores iguais a 1. Pelo Lema 3.3.2, G_A e G_B são grupos nilpotentes de classe 2. Além disso, note que G_A e G_B tem número de Hirsch 3 (isto é, o número de quocientes cíclicos infinitos em uma série com quocientes cíclicos ou finitos). Uma vez que G_A e G_B são finitamente gerados e livres de torção, segue pela Proposição 1.1.9 que $G_A \cong G_B$ e, portanto, $|\tilde{\mathfrak{g}}(G_A)| = 1$. □

3.4 O gênero de $\mathbb{Z}^2 \rtimes \mathbb{Z}$ – Caso não nilpotente

Seja $A \in \mathrm{GL}(2,\mathbb{Z})$. Nesta seção, vamos calcular a cardinalidade do gênero $\tilde{\mathfrak{g}}(G_A)$, quando $G_A = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$ é um grupo não nilpotente.

Teorema K. *Seja $A \in \mathrm{GL}(2,\mathbb{Z})$ e considere o produto semidireto $G_A = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$. Seja λ um autovalor de A. Então,*

(i) se A tem todos os seus autovalores distintos, $\mathrm{tr}(A) \neq 0$ e a classe de conjugação de A corresponde para uma classe de ideais invertíveis $[I_A]$ da ordem $\mathbb{Z}[\lambda]$, onde I_A é

como em (3.5)*, então*

$$\begin{cases} h(\mathbb{Z}[\lambda]) \leq |\tilde{\mathfrak{g}}(G_A)| \leq \tilde{h}(\lambda), & \text{se } \det(A) = -1 \\ h(\mathbb{Z}[\lambda])/2 \leq |\tilde{\mathfrak{g}}(G_A)| \leq \tilde{h}(\lambda), & \text{se } \det(A) = 1 \end{cases}$$

onde $h(\mathbb{Z}[\lambda])$ é a ordem do grupo de classes de ideais e $\tilde{h}(\lambda)$ é o número de classes de ideais de $\mathbb{Z}[\lambda]$.

(ii) se $\operatorname{tr}(A) = 0$ ou A tem todos os seus autovalores iguais a -1, então

$$|\tilde{\mathfrak{g}}(G_A)| = h(\mathbb{Z}[\lambda]) = 1.$$

Demonstração. Sejam A e B matrizes em $\mathrm{GL}(2,\mathbb{Z})$ e seja λ um autovalor de A. Considere os produtos semidiretos $G_A = N_1 \rtimes_A C$ e $G_B = N_2 \rtimes_B C$, onde $N_1 \cong \mathbb{Z}^2 \cong N_2$ e $C \cong \mathbb{Z}$. Suponha que

$$\widehat{G}_A \cong \widehat{G}_B.$$

(i) Vamos assumir que todos os autovalores de A são distintos, $\operatorname{tr}(A) \neq 0$ e que a classe de conjugação de A em $\mathrm{GL}(2,\mathbb{Z})$ corresponde para uma classe de ideais invertíveis $[I_A]$ de $\mathbb{Z}[\lambda]$. Então, nenhum dos autovalores de A são iguais a 1, e como $\widehat{G}_A \cong \widehat{G}_B$, segue pela Proposição 3.2.5 que os autovalores de B são distintos e diferentes de 1.

Pela Proposição 3.2.12 existem pelo menos $h(\mathbb{Z}[\lambda])$ matrizes em $\approx_A$-class que não são conjugadas duas a duas em $\mathrm{GL}(2,\mathbb{Z})$, mas são conjugadas entre si em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$. Agora temos dois casos a considerar para estabelecer a cota inferior.

Caso (a): Se $\det(A) = -1$.

Note que, se $A, B \in \approx_A$-class temos que $\det(A) = \det(B) = -1$ e $\operatorname{tr}(A) = \operatorname{tr}(B)$ pelo Lema 3.2.4. Então, $\operatorname{tr}(B^{-1}) = -\operatorname{tr}(B)$ pelo Lema 3.2.6 e, consequentemente, B^{-1} não é conjugada a nenhuma matriz de $\approx_A$-class. Portanto,

$$h(\mathbb{Z}[\lambda]) \leq |\tilde{\mathfrak{g}}(G_A)|$$

pelos Lemas 3.2.2 e 3.2.3.

Caso (b): Se $\det(A) = 1$.

Note que, se existe uma ou duas classes de conjugação de matrizes em $\approx_A$-class, então o resultado segue imediatamente pelo Lema 3.2.2. Agora, suponha que $\approx_A$-class possui mais que duas matrizes que não são conjugadas entre si e sejam

$A, B, C \in \mathrm{GL}(2,\mathbb{Z})$ três dessas matrizes. Observe que se A^{-1} é conjugada a B em $\mathrm{GL}(2,\mathbb{Z})$ e C^{-1} também é conjugada a B em $\mathrm{GL}(2,\mathbb{Z})$, então A^{-1} é conjugada a C^{-1} em $\mathrm{GL}(2,\mathbb{Z})$, que implica em A ser conjugada a C em $\mathrm{GL}(2,\mathbb{Z})$, que é uma contradição. Então, A^{-1} e C^{-1} não podem ser conjugadas a mais de uma matriz do subconjunto de $\approx_A$-class formado pelas matrizes que não são conjugadas entre si. Assim, pelos Lemas 3.2.2 e 3.2.3 temos

$$h(\mathbb{Z}[\lambda])/2 \leq |\tilde{\mathfrak{g}}(G_A)|.$$

Por outro lado, como as matrizes A e B são conjugadas em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$, temos que os polinômios característicos

$$p_A(x) = x^2 - \mathrm{tr}(A)x + \det(A) \;\text{ e }\; p_B(x) = x^2 - \mathrm{tr}(B)x + \det(B)$$

de A e B, respectivamente, são iguais (ver Lema 3.2.4). Agora, o Teorema 3.2.8 nos diz que existe uma correspondência biunívoca entre as classes de conjugação de matrizes em $\mathrm{GL}(2,\mathbb{Z})$, com polinômio característico $p_A(x)$, e as classes de ideais da ordem $\mathbb{Z}[\lambda]$. Logo, se $\tilde{h}(\lambda)$ denota o número de classes de ideais da ordem $\mathbb{Z}[\lambda]$, segue pelo Lema 3.2.2 que

$$|\tilde{\mathfrak{g}}(G_A)| \leq \tilde{h}(\lambda)$$

e, portanto, concluímos que

$$\begin{cases} h(\mathbb{Z}[\lambda]) \leq |\tilde{\mathfrak{g}}(G_A)| \leq \tilde{h}(\lambda), & \text{se } \det(A) = -1 \\ h(\mathbb{Z}[\lambda])/2 \leq |\tilde{\mathfrak{g}}(G_A)| \leq \tilde{h}(\lambda), & \text{se } \det(A) = 1. \end{cases}$$

(ii) Vamos dividir a prova deste item em dois casos.

Caso 1: Se A tem todos os seus autovalores iguais a -1.

É imediato verificar que $G_{A^2} = N_1 \rtimes_{A^2} \mathbb{Z}$ e $G_{B^2} = N_2 \rtimes_{B^2} \mathbb{Z}$ são subgrupos de G_A e G_B de índice finito, respectivamente (corresponde a substituir o segundo fator $\mathbb{Z}$ por $2\mathbb{Z}$). Assim, temos as seguintes sequências exatas

$$1 \to G_{A^2} \to G_A \to C_A \to 1 \;\text{ e }\; 1 \to G_{B^2} \to G_B \to C_B \to 1,$$

onde $C_A \cong \mathbb{Z}/2\mathbb{Z} \cong C_A$. Consequentemente, pelo [Seg83, p. 223, Cor. 1] temos as

seguintes sequências exatas para os completamentos profinitos correspondentes

$$1 \to \widehat{G}_{A^2} \to \widehat{G}_A \xrightarrow{\widehat{p}_A} C_A \to 1 \quad \text{e} \quad 1 \to \widehat{G}_{B^2} \to \widehat{G}_B \xrightarrow{\widehat{p}_B} C_B \to 1.$$

Agora, como nenhum dos autovalores das matrizes A e B são iguais a 1 pela Proposição 3.2.5, temos pelo Lema 3.1.6 que para qualquer isomorfismo $f : \widehat{G}_B \to \widehat{G}_A$, $f(\widehat{N}_2) = \widehat{N}_1$. Consequentemente, f induz um isomorfismo $\psi : C_B \to C_A$. Assim, obtemos o seguinte diagrama comutativo onde a restrição de f para $\widehat{G}_{B^2}$ é um isomorfismo de $\widehat{G}_{B^2}$ para $\widehat{G}_{A^2}$,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \widehat{G}_{B^2} & \longrightarrow & \widehat{G}_B & \xrightarrow{\widehat{p}_B} & C_B & \longrightarrow & 1 \\ & & \downarrow & & \downarrow f & & \downarrow \psi & & \\ 1 & \longrightarrow & \widehat{G}_{A^2} & \longrightarrow & \widehat{G}_A & \xrightarrow{\widehat{p}_A} & C_A & \longrightarrow & 1\,. \end{array}$$

Note que, como A^2 e B^2 têm todos os seus autovalores iguais a 1, temos que existe um isomorfismo $\phi : G_{B^2} \to G_{A^2}$ pelo Teorema J. Uma vez que $N_2 \rtimes_B 2\mathbb{Z} = G_{B^2}$ e $N_1 \rtimes_A 2\mathbb{Z} = G_{A^2}$ e nenhum dos autovalores das matrizes A e B são iguais a 1, segue pelo Lema 3.1.6 que $\phi(N_2) = N_1$. Além disso, as matrizes B^2 e A^2 são conjugadas em $\mathrm{GL}(2,\mathbb{Z})$ pela Proposição 3.1.1. Por outro lado, de A ser conjugada a B ou B^{-1} em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$, segue que $\mathrm{tr}(A) = \mathrm{tr}(B)$ ou $\mathrm{tr}(A) = \mathrm{tr}(B^{-1})$ e $\det(A) = \det(B)$ (ver Lema 3.2.4). Vamos assumir que A é conjugada a B em $\mathrm{GL}(2,\widehat{\mathbb{Z}})$. Uma vez que todos os autovalores de A e B são iguais a -1, temos que $\mathrm{tr}(A) = \mathrm{tr}(B) = -2$ e, consequentemente, as matrizes A e B são conjugadas em $\mathrm{GL}(2,\mathbb{Z})$ pelo Lema 3.2.13. Logo, $G_A \cong G_B$ pelo Lema 3.2.2 e, portanto, $|\mathfrak{g}(G_A)| = h(\mathbb{Z}) = 1$, uma vez que $\mathbb{Z}$ é um domínio de ideais principais.

Caso 2: Se $\mathrm{tr}(A) = 0$.

Primeiro suponha que $\det(A) = 1$. Neste caso, todos os autovalores de A são distintos e diferentes de 1. Como $\widehat{G}_A \cong \widehat{G}_B$, segue pela Proposição 3.2.5 com os Lemas 3.2.3 e 3.2.4 que $\mathrm{tr}(B) = \mathrm{tr}(A) = 0$ e $\det(B) = \det(A) = 1$. Agora, por [Hen97, Thm. 3] vemos que toda matriz com traço igual a zero e determinante igual a 1 é conjugada em $\mathrm{GL}(2,\mathbb{Z})$ para

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Logo, as matrizes A e B são conjugadas em $\mathrm{GL}(2,\mathbb{Z})$ e, consequentemente, $G_A \cong G_B$ pelo Lema 3.2.2. Portanto, $|\tilde{\mathfrak{g}}(G_A)| = 1$. Por outro lado, como o polinômio característico de A é $p(x) = x^2 + 1$, temos que $\sqrt{-1}$ e $-\sqrt{-1}$ são os autovalores de A. Pela Proposição 1.2.5 vemos que $\mathbb{Z}[\sqrt{-1}]$ é o anel de inteiros do corpo $\mathbb{Q}(\sqrt{-1})$. Portanto, $|\tilde{\mathfrak{g}}(G_A)| = h(\mathbb{Z}[\sqrt{-1}]) = 1$ por [AW04, p. 325].

Por fim, suponha que $\det(A) = -1$. Por [Hen97, Thm. 3] temos que A é conjugada em $\mathrm{GL}(2,\mathbb{Z})$ para

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Como $P^2 = I$, segue que G_A é um grupo de Bieberbach de dimensão 3 com grupo de holonomia $\mathbb{Z}/2\mathbb{Z}$ (ver [Szc12, Thm. 3.2]). Logo, pelo Corolário B temos que $|\tilde{\mathfrak{g}}(G_A)| = 1$. Neste caso, o polinômio característico de A é $p(x) = x^2 - 1$, assim, 1 e -1 são os autovalores de A. Portanto, como no caso 1, vemos que $|\tilde{\mathfrak{g}}(G_A)| = h(\mathbb{Z}) = 1$.

□

Finalizamos com as seguintes consequências.

Corolário L. *Seja $A \in \mathrm{GL}(2,\mathbb{Z})$ com $\det(A) = -1$ e considere o produto semidireto $G_A = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$. Se $\mathrm{tr}(A)^2 - 4\det(A)$ é livre de quadrados, então $|\tilde{\mathfrak{g}}(G_A)| = h(\mathbb{Z}[\lambda])$ onde λ é um autovalor de A.*

Demonstração. Pelo Lema 1.2.18, vemos que $h(\mathbb{Z}[\lambda]) = \tilde{h}(\lambda)$. Portanto, $|\tilde{\mathfrak{g}}(G_A)| = h(\mathbb{Z}[\lambda])$ pelo Teorema K. □

Corolário M. *Seja A uma matriz em $\mathrm{GL}(2,\mathbb{Z})$, como no Teorema K ou Teorema J, com autovalor λ. Se $\tilde{h}(\lambda) = 1$, então o torus bundle X_A é determinado, dentre as variedades tridimensionais, pelo completamento profinito do seu grupo fundamental.*

Demonstração. Isto é uma consequência imediata dos Teoremas J e K. □

3.5 Exemplos

Vamos agora exibir alguns exemplos de aplicações dos Teoremas J e K.

Exemplo 3.5.1. *Considere*

$$A = \begin{pmatrix} 2 & 1 \\ 5 & 2 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Z})$$

com polinômio característico $f_A(x) = x^2 - 4x - 1$. *Então, os autovalores de* A *são*

$$\lambda_{\pm} = \frac{4 \pm \sqrt{(-4)^2 - 4(-1)}}{2} = \frac{4 \pm 2\sqrt{5}}{2} = 2 \pm \sqrt{5}.$$

Como $5 \equiv 1 \pmod 4$, *segue pela Proposição 1.2.5 que a ordem* $\mathbb{Z}[\lambda_+] = \mathbb{Z}[\sqrt{5}]$ *não é maximal, em outras palavras,* $\mathbb{Z}[\sqrt{5}]$ *não é o anel de inteiros do corpo quadrático* $\mathbb{Q}(\sqrt{5})$. *Considere* $I = \langle 2, 1 + \sqrt{5} \rangle$. *Pela Proposição 1.2.13 vemos que* I *é um ideal de* $\mathbb{Z}[\sqrt{5}]$. *Por [Mol11, Ex. 1.32] vemos que* I *é um ideal não invertível de* $\mathbb{Z}[\sqrt{5}]$. *Isso implica que a ordem* $h(\mathbb{Z}[\sqrt{5}])$ *do grupo de classes de ideais de* $\mathbb{Z}[\sqrt{5}]$ *é estritamente menor do que o número de classes de ideais* $\tilde{h}(\lambda_+)$ *de* $\mathbb{Z}[\sqrt{5}]$. *Como o ideal correspondente para a matriz* A *é* $I_A = \langle 1, \lambda_+ - 2 \rangle = \mathbb{Z}[\sqrt{5}]$ *(ver* (3.5)*), que é invertível, e* $\det(A) = -1$, *segue pelo Teorema K que vale a seguinte desigualdade*

$$h(\mathbb{Z}[\sqrt{5}]) \leq |\tilde{\mathfrak{g}}(\mathbb{Z}^2 \rtimes_A \mathbb{Z})| \leq \tilde{h}(\lambda_+) \quad \textit{com} \quad h(\mathbb{Z}[\sqrt{5}]) < \tilde{h}(\lambda_+).$$

O próximo exemplo, nos diz que os torus bundles modelados com a geometria **Sol** não são determinados pelo completamento profinito dos seus grupos fundamentais.

Exemplo 3.5.2. *Considere*

$$B = \begin{pmatrix} 4 & 7 \\ 3 & 5 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}).$$

Note que o polinômio característico de B *é* $f_B(x) = x^2 - 9x - 1$ *e que*

$$\lambda_{\pm} = \frac{9 \pm \sqrt{(-9)^2 - 4(-1)}}{2} = \frac{9 \pm \sqrt{85}}{2}$$

são os autovalores. Como 85 *é livre de quadrados de* $\det(B) = -1$, *segue pelo Corolário L que*

$$|\tilde{\mathfrak{g}}(\mathbb{Z}^2 \rtimes_B \mathbb{Z})| = h(\mathbb{Z}[\lambda_+]).$$

Agora, por [AW04, Table 8] vemos que $h(\mathbb{Z}[\lambda_+]) = 2$. *Uma vez que* $|\mathrm{tr}(B)| > 2$, *segue que o torus bundle* X_B, *tal que* $\pi_1(X_B) \cong \mathbb{Z}^2 \rtimes_B \mathbb{Z}$, *está modelado com a geometria* **Sol** *(Cf. [Sco83, Thm. 5.5]).*

Em contrapartida, o Corolário M nos diz que existe uma família de torus bundles, modelados com a geometria **Sol**, que são determinados pelos completamentos profinitos dos seus grupos fundamentais.

Exemplo 3.5.3. *Considere as matrizes*

$$D = \begin{pmatrix} 2 & 7 \\ 1 & 3 \end{pmatrix}, \ E = \begin{pmatrix} 5 & 1 \\ 11 & 2 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}).$$

Como o traço destas matrizes são absolutamente maiores do que 2*, temos que os torus bundles* X_D *e* X_E*, tais que*

$$\pi_1(X_D) \cong \mathbb{Z}^2 \rtimes_D \mathbb{Z} \text{ e } \pi_1(X_E) \cong \mathbb{Z}^2 \rtimes_E \mathbb{Z},$$

são todos modelados com a geometria **Sol** *(Cf. [Sco83, Thm. 5.5]). Agora, note que os polinômios característicos de* D *e* E *são*

$$f_D(x) = x^2 - 5x - 1, \ f_E(x) = x^2 - 7x - 1,$$

respectivamente. Consequentemente, os autovalores de D *e* E *são*

$$\lambda_{\pm,D} = \frac{5 \pm \sqrt{29}}{2}, \ \lambda_{\pm,E} = \frac{7 \pm \sqrt{53}}{2},$$

respectivamente. Como 29 *e* 53 *são livres de quadrados e* $\det(D) = \det(E) = -1$*, segue pelo Corolário L com [AW04, Table 8] que*

$$|\tilde{\mathfrak{g}}(\mathbb{Z}^2 \rtimes_D \mathbb{Z})| = 1, |\tilde{\mathfrak{g}}(\mathbb{Z}^2 \rtimes_E \mathbb{Z})| = 1.$$

Portanto, os torus bundles X_D *e* X_E *são determinados, dentre as variedades tridimensionais, pelo completamento profinito dos seus grupos fundamentais.*

Capítulo

4

Considerações Finais

Encerramos esta tese com alguns cometários gerais, em relação aos nossos resultados, e apresentando algumas indicações para futuras pesquisas.

Em nosso estudo da Questão 1, para a família dos grupos de Bieberbach Γ com grupo de holonomia cíclico de ordem livre de quadrados, só foi possível exibir fórmulas para a cardinalidade do gênero $\mathfrak{g}(\Gamma)$, porque existe uma classificação para os $\mathbb{Z}G$-reticulados sobre grupos cíclicos G de ordem livre de quadrados. Uma vez que, em geral, o conjunto de classes de isomorfismos de $\mathbb{Z}G$-reticulados é infinito, torna-se muito difícil investigar a Questão 1 para a família dos grupos de Bieberbach completa. Entretanto, como mencionado na Seção 1.4, existem algumas classes de grupos G, para os quais, os $\mathbb{Z}G$-reticulados são bem classificados, por exemplo:

- os grupos cíclicos de ordem p^2, onde p é primo;
- grupos diedrais de ordem $2p$, onde p é um primo ímpar;
- grupos não abelianos de ordem pq, onde p e q são primos distintos.

Para a família de grupos de Bieberbach com o grupo de holonomia G, onde G pertence a uma das classes listadas nos pontos anteriores, acreditamos que é possível realizar um estudo da Questão 1 de forma semelhante ao nosso.

Referências Bibliográficas

[AW04] S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, New York, (2004).

[AK57] L. Auslander and M. Kuranishi, *On the Holonomy Group of Locally Euclidean Spaces*, Annals of Mathematics, **65** (1957), 411–415.

[Bau74] G. Baumslag, *Residually finite groups with the same finite images*, Compositio Mathematica, **29** (1974), 249–252.

[BZ13] V. R. Bessa and P. A. Zalesskii, *The genus for HNN-extensions*, Mathematische Nachrichten, **286** (2013), 817–831.

[BCR16] M. R. Bridson, M. D. E. Conder, and A. W. Reid, *Determining Fuchsian groups by their finite quotients*, Israel Journal of Mathematics, **214** (2016), 1–41.

[BMRS20-a] M. R. Bridson, D. B. McReynolds, A. W. Reid, and R. Spitler, *Absolute profinite rigidity and hyperbolic geometry*, Annals of Mathematics, **192** (2020), 679–719.

[BMRS20-b] M. R. Bridson, D. B. McReynolds, A. W. Reid, and R. Spitler, *On the profinite rigidity of triangle groups*, arXiv:2004.07137, 2020.

[BNZ73] H. Brown, J. Neubüser, and H. Zassenhaus, *On Integral Groups. III: Normalizers*, Mathematics of Computation, **27** (1973), 167–182.

[Bro82] K. S. Brown, *Cohomology of Groups*, Springer, New York (1982).

[CT91] J. T. Campbell and E. C. Trouy, *When are two elements of* $\mathrm{GL}(2,\mathbb{Z})$ *similar?*, Elsevier Science Publishing, **157** (1991): 175–184.

[Cha65] L. S. Charlap, *Compact Flat Riemannian Manifolds: I*, Annals of Mathematics, **81** (1965), 15–30.

[Cha86] L. S. Charlap, *Bieberbach groups and flat manifolds*, Springer-Verlag, New York (1986).

[CW89] G. Cliff and A. Weiss, *Torsion free space groups and permutation lattices for finite groups*, Contemporary Mathematics, **93** (1989), 123–132.

[Cox89] D. A. Cox, *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, New York (1989).

[CR62] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, John Wiley & Sons, New York (1962).

[CR81] C. W. Curtis and I. Reiner, *Methods of representation theory – with applications to finite groups and ordes*, John Wiley & Sons, New York (1981).

[DFPR82] J. D. Dixon, E. W. Formanek, J. C. Poland and L. Ribes, *Profinite completions and isomorphic finite quotients*, Journal of Pure and Applied Algebra, **23** (1982), 227–231.

[DK18] C. Druţu and M. Kapovich, *Geometric Group Theory*, Colloquium Publications, Vol. 63, American Mathematical Society, Providence (2018).

[DF04] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Third Edition, John Wiley & Sons, New York (2004).

[Fun13] L. Funar, *Torus bundles not distinguished by TQFT invariants*. Geometry and Topology, **17** (2013), 2289–2344.

[GPS79] F. J. Grunewald, P. F. Pickel, D. Segal, *Finiteness theorems for polycyclic groups*, Bulletin of the American Mathematical Society (N.S.), **1**, n. 3 (1979), 575–578.

[GS79] F. Grunewald and R. Scharlau, *A note on finitely generated torsion-free nilpotent groups of class 2*, Journal of Algebra. **58** (1979), 162–175.

[GZ11] F. Grunewald, P. Zalesskii, *Genus for groups*, Journal of Algebra, **326** (2011), 130–168.

[Hal59] M. Hall, *The theory of groups*, The Macmillan Company, New York (1959).

[HR62] A. Heller and I. Reiner, *Representations of Cyclic Groups in Ring of Integers, I*, Annals of Mathematics, **76** (1962), 73–92.

[Hem14] J. Hempel, *Some* 3*-manifold groups with the same finite quotients*, arXiv:1409.3509, 2014.

[Hen97] J. P. Henniger, *Factorization and similarity in* $\mathrm{GL}(2,\mathbb{Z})$, Linear Algebra and its Applications, **251** (1997), 223–237.

[Hil85] H. Hiller, *The Crystallographic Restriction in Higher Dimensions*, Acta Crystallographica Section A, **41** (1985), 541–544.

[Hil86] H. Hiller, *Crystallography and Cohomology of Groups*, The American Mathematical Monthly **93** (10) (1986), 765–779.

[JW09] M. J. Jacobson, Jr. and H. C. Williams, *Solving the Pell Equation*, CMS Books in Mathematics, Springer, New York (2009).

[JKM08] J. Jezierski, E. Keppelmann and W. Marzantowicz, *Homotopy minimal periods for maps of three-dimensional solvmanifolds*, Topology and its Applications, **155** (2008), 923–945.

[Joh97] D. J. Johnson, *Presentations of Groups*, Second Edition, Cambridge University Press, Cambridge (1997).

[Jon63] A. Jones, *Groups with a finite number of indecomposable integral representations*, Michigan Mathematical Journal, **10** (1963), 257–261.

[Lee64] M. P. Lee, *Integral representations of dihedral groups of order* $2p$, Transactions of the American Mathematical Society, **110** (1964), 213–231.

[Liu20] Y. Liu, *Finite-volume hyperbolic* 3*-manifolds are almost determined by their finite quotient groups*, arXiv:2011.09412, 2020.

[Mol11] R. A. Mollin, *Algebraic Number Theory*, Discrete mathematics and its applications, Second Edition, CRC Press, London (2011).

[Neu99] J. Neukirch, *Algebraic number theory*, Springer-Verlag, New York (1999).

[New72] M. Newman, *Integral matrices*, Academic Press, New York (1972).

[NS07] N. Nikolov and D. Segal, *On finitely generated profinite groups, I: strong completeness and uniform bounds*, Annals of mathematics, **165** (2007), 171–238.

[Opp62] J. H. Oppenheim, *Integral representations of cyclic groups of squarefree order*, Ph.D. thesis, University of Illinois, Urbana (1962).

[PPW21] P. Piwek, D. Popović, G. Wilkes, *Distinguishing crystallographic groups by their finite quotients*, Journal of Algebra, **565** (2021), 548–563.

[Pu65] L. C. Pu, *Integral representations of non-abelian groups of order pq,* Michigan Mathematical Journal, **12** (1965), 231–246.

[Rei18] A. W. Reid, *Profinite rigidity*, The Proceedings of the 2018 I.C.M. Rio de Janeiro, vol. 2, 1211–1234.

[Rib01] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, New York (2001).

[RZ00] L. Ribes and P. Zalesskii, *Profinite groups*, volume 40, Springer-Verlag, New York (2000).

[Rot09] J. J. Rotman, *An introduction to homological algebra*, Second Edition, Springer, New York (2009).

[Sco83] P. Scott, *The geometries of* 3*-manifolds*, Bulletin of the London Mathematical Society, **15** (1983), 401–487.

[Seg83] D. Segal, *Polycyclic groups*, Cambridge University Press, New York (1983).

[Ste72] P. F. Stebe, *Conjugacy separability of groups of integer matrices*, Proceedings of the American Mathematical Society, **32** (1972), 1–7.

[Szc97] A. Szczepasńki, *Decomposition of flat manifolds*, Mathematika, **44** (1997), 113–119.

[Szc12] A. Szczepasńki, *Geometry of Crystallographic Groups*, Algebra and Discrete Mathematics, Vol. 4, World Scientific Publishing, Singapore (2012).

[Ten97] R. F. Tennant, *Classifying Free Bieberbach Groups*, Trans. Ky. Acad. Sci., **58**(1) (1997), 29–32.

[Tro61] A. Troy, *Integral representations of cyclic groups of order* p^2, PhD thesis, Univ. of Illinois, Urbana (1961).

[Vas70] A. T. Vasquez, *Flat Riemannian Manifolds*, Journal of Differential Geometry, **4** (1970), 367–382.

[Was82] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York (1982).

[Wei94] C. A. Weibel, *An introduction to Homological Algebra*, Cambridge University Press, New York (1994).

[Wie84] R. Wiegand, *Cancellation over commutative rings of dimension one and two*, Journal of Algebra, **88** (1984), 438–459.

[Wil17] G. Wilkes, *Profinite rigidity for Seifert fibre spaces*, Geometriae Dedicata, **188** (2017), 141–163.

[Wil18] G. Wilkes, *Profinite rigidity of graph manifolds and JSJ decompositions of* 3*-manifolds*, Journal of Algebra, **502** (2018), 538–587.

[Wil19] G. Wilkes, Profinite rigidity of graph manifolds, II: knots and mapping classes, Israel Journal of Mathematics, **233** (2019), 351–378.

[WZ10] H. Wilton and P. Zalesskii, *Profinite properties of graph manifolds*, Geometriae Dedicata, **147** (2010), 29–45.

[WZ17] H. Wilton and P. Zalesskii, *Distinguishing geometries using finite quotients*, Geometry and Topology, **21** (2017), 345–384.

[WZ19] H. Wilton and P. Zalesskii, *Profinite detection of* 3*-manifold decompositions*, Compositio Mathematica, **155** (2019), 246–259.

Índice Remissivo