Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Matemática

Solução do Problema da Conjugação para algumas extensões de grupos

Autor: *Wagner Carvalho Sgobbi*

Orientador: *Daniel Vendrúscolo*

São Carlos, 7 de agosto de 2017.

Solução do Problema da Conjugação para algumas extensões de grupos

Autor: *Wagner Carvalho Sgobbi*

Orientador: *Daniel Vendrúscolo*

Instituição: Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Matemática

Dissertação apresentada ao PPGM da UFSCar como parte dos requisitos para obtenção do título de Mestre em Matemática.

São Carlos, 7 de agosto de 2017.

Nome do Autor (aluno)	Nome do Orientador (orientador)

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Matemática

Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Wagner Carvalho Sgobbi, realizada em 23/02/2017:

Prof. Dr. Daniel Vendrúscolo
UFSCar

Prof. Dr. Humberto Luiz Talpo
UFSCar

Prof. Dr. Dessislava Hristova Kochloukova
UNICAMP

Ó profundidade das riquezas, tanto da sabedoria, como da ciência de Deus! Quão insondáveis são os seus juízos, e quão inescrutáveis os seus caminhos! Por que quem compreendeu a mente do Senhor? Ou quem foi seu conselheiro? Ou quem lhe deu primeiro a ele, para que lhe seja recompensado? Porque dele e por ele, e para ele, são todas as coisas; glória, pois, a ele eternamente. Amém. (Romanos 11:33-36)

Agradecimentos

Agradeço a Deus pela permissão de viver, pela graça e salvação imerecidas por meio de Jesus, pelo sustento material e espiritual diário e por ter, literalmente, me conduzido à matemática de uma forma soberana e imprevisível.

Agradeço à minha esposa, Karina, pelo amor, companheirismo, paciência e apoio diariamente demonstrados e pela alegria que sinto ao abrir os olhos pela manhã. Agradeço ao meu pai, Wagner, pelos princípios bíblicos e morais ensinados e pelos exemplos de fé, perseverança, domínio próprio e longanimidade. Agradeço novamente a meu Deus pela mãe que tive, da qual recebi doses imensuráveis de amor e ternura que nunca se esgotarão, e da qual a saudade só é menor do que a certeza de nosso reencontro na glória eterna, diante do Pai. Agradeço a todos os meus familiares, também pelo apoio, orações e carinho sempre presentes.

Agradeço ao meu orientador, Prof. Dr. Daniel Vendrúscolo, pela disposição durante todas as orientações, desde o começo dos estudos de Iniciação Científica em 2013 até os dias de hoje, e pela tamanha confiança depositada em mim. Agradeço também ao Prof. Dr. Humberto Luiz Talpo e ao colega de sala Dalton pela prontidão em ajudar em vários problemas algébricos e aos meus colegas de trabalho e de sala Bárbara, Tiago, Karina, Renato, Flávia, Renan, Lucas, entre outros, pela disposição em ouvir, discutir e opinar sobre os conteúdos deste trabalho.

Agradeço à CAPES, pelo apoio financeiro durante todo o mestrado.

Resumo

Esta dissertação é um estudo introdutório e detalhado da Teoria Combinatória de Grupos e de um de seus três problemas clássicos: o Problema da Conjugação. Estuda-se sua solução para várias classes de extensões de grupos, obtida nos artigos [1] e [2]. Dentre os resultados, destacam-se sua solução para grupos livre-por-cíclicos e para extensões livres da forma $\mathbb{Z}^n \rtimes_A \mathbb{Z}$, ou $\mathbb{Z}^2 \rtimes_{A_1,...,A_m} F_m$, ou $F_2 \rtimes_{\varphi_1,...,\varphi_m} F_m$ (com $A \in GL_n(\mathbb{Z})$, $A_1, ..., A_m \in GL_2(\mathbb{Z})$ e $\varphi_1, ..., \varphi_m \in Aut(F_2)$), bem como da forma $\mathbb{Z}^n \rtimes_{A_1,...,A_m} F_m$ com $\langle A_1, ..., A_m \rangle \leq GL_n(\mathbb{Z})$ subgrupo de índice finito ou virtualmente solúvel, ou, finalmente, da forma $F_n \rtimes_{\varphi_1,...,\varphi_m} F_m$, com $\langle \varphi_1, ..., \varphi_m \rangle \leq Aut(F_n)$ de índice finito. Também, resolve-se o Problema da Conjugação Torcida para grupos livres finitamente gerados, grupos policíclicos e grupos fundamentais de superfícies fechadas, entre outros. No desenvolver do texto, procura-se argumentar de forma simples e detalhada, de modo a proporcionar ao leitor um primeiro contato com a Teoria Combinatória de Grupos e desenvolver nele um certo nível de familiaridade com os problemas de decisão da teoria e com o conceito de algoritmo, amplamente utilizado.

Abstract

This essay is a detailed introductory study of Combinatorial Group Theory and one of its three classical problems: the Conjugacy Problem. We studied its solution for several classes of group extensions, obtained in [1] and [2]. Among the results, we point out its solution for free-by-cyclic groups and for some free extensions of the form $\mathbb{Z}^n \rtimes_A \mathbb{Z}$, or $\mathbb{Z}^2 \rtimes_{A_1,...,A_m} F_m$, or $F_2 \rtimes_{\varphi_1,...,\varphi_m} F_m$ (with $A \in GL_n(\mathbb{Z})$, $A_1, ..., A_m \in GL_2(\mathbb{Z})$ and $\varphi_1, ..., \varphi_m \in Aut(F_2)$), as well as $\mathbb{Z}^n \rtimes_{A_1,...,A_m} F_m$ with $\langle A_1, ..., A_m \rangle \leq GL_n(\mathbb{Z})$ a finite index or virtually solvable subgroup, or, finally, for groups of the type $F_n \rtimes_{\varphi_1,...,\varphi_m} F_m$, with $\langle \varphi_1, ..., \varphi_m \rangle \leq Aut(F_n)$ a finite index subgroup. We also studied solutions of the Twisted Conjugacy Problem for finitely generated free, polycyclic and surface groups. In the course of the text, one tries to argue in a simple and detailed way, providing the reader a first contact with Combinatorial Group Theory and a certain level of familiarity with its decision problems and with the vastly used concept of algorithm.

Sumário

Lista de Figuras

Introdução

A Teoria Combinatória de Grupos é a subárea da Álgebra moderna responsável por investigar, entre outras coisas, o conceito de grupo livre e os grupos em geral através de seus geradores e suas relações, ou seja, as presentações dos grupos. Nossos objetivos com esta introdução são: descrever os conteúdos de cada capítulo e nos situarmos com um realmente breve comentário histórico sobre a área (baseado em [6]), desde seu surgimento até a aparição dos três problemas clássicos, sendo um deles o Problema da Conjugação, o principal foco do texto.

Sendo uma parte bem específica da Álgebra, a Teoria Combinatória de Grupos tem apenas um pouco mais de um século de idade. Sua primeira aparição realmente notável se dá no ano de 1882, com os estudos e publicações iniciais de Walther Franz Anton von Dyck, matemático alemão que desenvolve, ainda que usando uma linguagem bem longe da atual (o que é completamente natural de se esperar), as primeiras ideias sobre grupo livre e relações. Traduzindo para o português, sua primeira definição é a seguinte:

> "Sejam A_1,...,A_m m operações que podem ser apilcadas a um objeto J, que será sempre denotado por 1. Então esses A_i podem sempre ser considerados como os geradores de um grupo que será obtido aplicando todas as combinações possíveis das operações no objeto J. O *grupo mais geral* com m operações geradoras será obtido se assumirmos que os A_i não são periódicos e, além disso, não são conectados entre si por qualquer relação. Vamos considerar também as operações opostas dos A_i, que denotaremos por ${A_i}^{-1}$. Então obteremos as infinitas substituições que pertencem ao nosso grupo G se aplicarmos primeiramente as operações A_1, ${A_1}^{-1}$, A_2, ${A_2}^{-1}$, ... , ${A_m}^{-1}$ à identidade, depois aplicarmos ao resultado as mesmas operações, e assim por diante. Como assumimos que não há relações entre as operações geradoras, as substituições produzidas são todas distintas entre si e cada uma delas pode ser obtida por um único processo, completamente determinado pelas operações geradoras. Isso pode ser expresso pela fórmula
>
> $$A_1{}^{\mu_1} A_2{}^{\mu_2} ... A_1{}^{\nu_1} A_2{}^{\nu_2} ... \text{ .}"$$

Nota-se uma tendência a dar significado geométrico à álgebra sendo construída, quando

Dyck pensa em um objeto J e nas operações a serem aplicadas ao mesmo, como acontece, por exemplo, nos grupos (finitos) de permutações e nos diedrais D_n, onde J é o polígono regular de n faces e A_1 e A_2 são, respectivamente, a rotação de ângulo $\frac{2\pi}{n}$ e uma reflexão coerente em relação a uma reta qualquer fixada do plano contendo a origem. Usando sua terminologia geométrica, Dyck desenvolve um belo trabalho e acerta em cheio em seus objetivos. Os principais resultados de seu artigo são dois dos mais fundamentais da Teoria Combinatória de Grupos: na linguagem atual, são a existência do grupo livre finitamente gerado, com única representação algébrica reduzida de seus elementos (como visto na citação acima), e a propriedade de que todo grupo finitamente gerado é a imagem por um homomorfismo de um grupo livre finitamente gerado, resultado que justifica o fato de que todo grupo (finitamente gerado) possui uma presentação. O problema é que, apesar de totalmente convincentes, as demonstrações que Dyck dá destes resultados não possuem o rigor da matemática atual e não seriam consideradas válidas hoje em dia. O tratamento geométrico dos grupos, segundo ele mesmo, o levou até a cometer um erro em um de seus artigos. Ainda bem que vinte e dois anos depois (1904), o matemático de Seguier já consegue descrever, em seus trabalhos, os geradores e as relações de um grupo de uma forma mais rigorosa e parecida que a atual, em contraste com Dyck. Sua demonstração do fato de que todo grupo é a imagem homomorfa de um grupo livre é muito mais precisa, simplificada e moderna.

O conceito de grupo fundamental de um espaço topológico é primeiramente introduzido por Henri Poincaré em seu famoso artigo "Analysis Situs" (1895). Segundo os autores de [6], este artigo é difícil de ser lido, pois as notações variam muito sem aviso prévio e, além disso, não há sequer uma tentativa de separar o que é intuição do que é demonstração. Por isso, grande parte do trabalho do austríaco Heinrich Franz Friedrich Tietze, em 1908, é um esclarecimento do que Poincaré fez. Tietze define de outra maneira os grupos fundamentais de uma variedade e prova que possuem presentações finitas; prova também que duas variedades homeomorfas possuem grupos fundamentais isomorfos. Assim, entra em jogo, já no século XX, o principal pensamento da Topologia Algébrica: provar que duas variedades não são homeomorfas, então, se torna provar que duas presentações finitas não são isomorfas. Concentrado nisso, Tietze define algumas transformações elementares que se podem aplicar a uma presentação sem mudar o grupo que ela gera, e demonstra que duas presentações finitas definem grupos isomorfos se, e somente se, uma pode ser levada à outra por meio de um número finito dessas transformações (que chamamos atualmente de transformações de Tietze). Esta propriedade, junto com o fato de que os abelianizados de dois grupos isomorfos são também isomorfos, são os primeiros grandes resultados a aparecer na Teoria Combinatória de Grupos, depois dos feitos por Dyck e de Seguier.

É claro que apenas algumas propriedades em relação a grupos espalhadas por aí no início do século XX – por mais fundamentais que fossem - ainda não haviam sido suficientes para que a Teoria Combinatória de Grupos já estivesse sendo considerada como uma nova e já independente teoria matemática. Parece haver um consenso de que essa independência

se inicia com Max Dehn, quando ele continua e aprofunda a produção de Tietze com várias publicações, em 1910, 1911, 1912 e 1914. Com uma motivação geométrica, a segunda delas começa com a formulação dos seguintes clássicos problemas de decisão da teoria:

- **O Problema da Palavra (PP):** dado um elemento arbitrário de um grupo em termos de seus geradores, decidir quando este é o elemento neutro do grupo.
- **O Problema da Conjugação (PC):** dados dois elementos x e y de um mesmo grupo em termos de seus geradores, decidir quando são conjugados, ou seja, quando existe um terceiro elemento u no grupo tal que $y = u^{-1}xu$.
- **O Problema do Isomorfismo (PI):** dados dois grupos em termos de seus geradores e relações, decidir quando são isomorfos entre si.

A partir deste estágio, como já dissemos, a Teoria Combinatória de grupos desabrocha como uma área independente e começam a surgir inúmeros outros problemas envolvendo grupos livres e presentações, e também outros problemas de decisão. Neste trabalho, focamos o Problema da Conjugação. Mais especificamente, estudamos as soluções para o mesmo encontradas em algumas classes de grupos pelos autores O. Bogopolski, A. Martino, E. Ventura e O. Maslakova, como os grupos livre-por-cíclicos em 2006 no artigo [1] e várias extensões livres de outros tipos de grupos no artigo [2].

No capítulo 1 relembramos os conceitos básicos de Álgebra, grupo livre e presentações de grupo, que são o contexto onde desenvolvemos a teoria. Também, mostramos propriedades do produto semidireto e das sequências exatas e as relações entre eles, que são usadas durante todo o restante do texto.

O capítulo 2 é uma breve introdução à noção intuitiva de algoritmo que usaremos aqui e uma exposição (um pouco mais detalhada do que a já feita acima) dos três problemas de decisão clássicos apresentados por Dehn e do Problema da Conjugação Torcida (PCT), generalização do PC que precisaremos frequentemente no desenvolvimento dos teoremas. Também, resolvemos alguns destes problemas em casos triviais, como em grupos finitos e grupos livres, e apresentamos alguns algoritmos explicitamente, com a intenção de que o leitor adquira certo nível de familiaridade com os objetos e as técnicas utilizadas.

Começamos a dar um foco mais específico ao Problema da Conjugação já no capítulo 3. Baseando-nos em [1], estudamos a solução do mesmo para todos os grupos livre-por-cíclicos a partir de uma solução mais delicada do Problema da Conjugação Torcida para qualquer grupo livre finitamente gerado, de algumas propriedades intrínsecas à conjugação torcida e de dois importantes teoremas, de P. Brinkmann e O. Maslakova.

O quarto e principal capítulo é dedicado ao teorema central do artigo [2], onde investiga-se quais condições devem ser impostas sobre uma sequência exata $1 \to F \to G \to H \to 1$ para que consiga-se resolver o Problema da Conjugação em seu grupo central G. Além de dar uma detalhada demonstração deste teorema, tentamos fazer as

ligações necessárias do mesmo com o teorema do capítulo anterior, para deixar claro que é uma generalização (o que não fica claro se apenas lermos seus enunciados).

No capítulo 5, continuamos investigando o teorema central, agora com o objetivo de encontrar classes de grupos e de sequências exatas que se encaixem em suas hipóteses, de modo a torná-lo um resultado mais abrangente e aplicável. Entre os resultados obtidos, destacamos a solução de PCT para qualquer grupo virtualmente abeliano, virtualmente livre, virtualmente policíclico ou virtualmente grupo de superfície. Depois disto, usamos as extensões livres para reescrever o teorema central em termos de presentações de grupos, tornando-o extremamente prático.

Finalmente, o sexto e último capítulo aproveita-se da praticidade e aplicabilidade obtida no capítulo 5 e de vários outros resultados e técnicas diferentes para resolver o Problema da Conjugação para extensões livres da forma $\mathbb{Z}^n \rtimes_A \mathbb{Z}$, ou $F_n \rtimes_\varphi \mathbb{Z}$, ou $\mathbb{Z}^2 \rtimes_{A_1,...,A_m} F_m$, ou $F_2 \rtimes_{\varphi_1,...,\varphi_m} F_m$ (com $A \in GL_n(\mathbb{Z})$, $A_1, ..., A_m \in GL_2(\mathbb{Z})$, $\varphi \in Aut(F_n)$ e $\varphi_1, ..., \varphi_m \in Aut(F_2)$), bem como da forma $\mathbb{Z}^n \rtimes_{A_1,...,A_m} F_m$ com $\langle A_1, ..., A_m \rangle \leq GL_n(\mathbb{Z})$ subgrupo de índice finito ou virtualmente solúvel, ou, finalmente, da forma $F_n \rtimes_{\varphi_1,...,\varphi_m} F_m$, com $\langle \varphi_1, ..., \varphi_m \rangle \leq Aut(F_n)$ de índice finito.

Capítulo 1

Conceitos preliminares

1.1 Álgebra básica

Apesar de acreditarmos que o leitor já está há muito tempo familiarizado com os conceitos desta seção, vamos defini-los para fixar as notações e apenas citar, sem demonstrações, as suas principais propriedades. Com isso, pretendemos clarear as leituras posteriores. No entanto, para não criarmos um texto demasiadamente longo e cansativo, é claro que precisamos assumir que o leitor já possua também o conhecimento das propriedades básicas da Lógica Clássica, da Teoria de Conjuntos e da Álgebra elementar.

Definição 1.1. Um *grupo* é um conjunto não vazio G munido de uma operação binária $G \times G \to G$, que denotaremos por $(a, b) \mapsto ab$, onde valem as seguintes propriedades:

(i) Associativa: $a(bc) = (ab)c,\ \forall a, b, c \in G$;

(ii) Elemento neutro: existe um elemento em G, que denotaremos por 1, tal que $1a = a1 = a$, para todo $a \in G$.

(iii) Inverso: Para todo $a \in G$ existe um elemento em G, que denotaremos por a^{-1}, tal que $a^{-1}a = aa^{-1} = 1$.

Um grupo é dito *abeliano* quando sua operação binária possui a propriedade

(iv) Comutativa: $ab = ba,\ \forall a, b \in G$.

Dizemos que um subconjunto H de G é um *subgrupo* de G quando, restringindo a operação de G a H, o mesmo se torna um grupo. Nesse caso, denotamos $H \leq G$ ou $G \geq H$.

Definição 1.2. Dado um subconjunto não vazio S de um grupo G, o *subgrupo gerado* por S em G é o menor subgrupo de G que contém S, ou a interseção de todos os subgrupos de G que contém S. O denotaremos por $\langle S \rangle$ e diremos que S *gera* $\langle S \rangle$. Quando $S = \{a_1, ..., a_n\}$, também denotaremos por $\langle a_1, ..., a_n \rangle$. Em particular, quando $S = \{a\}$ diremos que o subgrupo $\langle a \rangle$ é *cíclico*.

Escrevendo $S^{-1} = \{s^{-1} \mid s \in S\}$, um elemento arbitrário (não neutro) do subgrupo $\langle S \rangle$ acima é da forma $a_1 ... a_n$ com $a_i \in S \cup S^{-1}$ e $n \geq 1$, ou ainda, da forma ${a_1}^{k_1} ... {a_n}^{k_n}$, com $a_i \in S$ e $k_i \in \mathbb{Z}$, expressões que chamaremos também de *palavras* em S. Estamos nos apossando da notação multiplicativa para grupos, bem como a operação iterada natural a^n para $n \in \mathbb{Z}$.

Neste trabalho seguiremos a notação mais computacional, usada nos artigos [1] e [2], onde denotaremos a imagem de um elemento a por uma função φ como sendo $a\varphi$ ou $(a)\varphi$ ao invés de $\varphi(a)$, como estamos acostumados. Usaremos também $a\varphi\psi$ em vez de $\psi(\varphi(a))$ e $a\varphi^k$ em vez de $\varphi^k(a)$. Desta forma, vem a seguinte

Definição 1.3. Um *homomorfismo* entre dois grupos G e H é uma função $\varphi : G \to H$ tal que $(ab)\varphi = a\varphi b\varphi$, para quaisquer $a, b \in G$. Usaremos a notação $G \xrightarrow{\varphi} H$ ou $G \to H$, quando o homomorfismo estiver subentendido. O *núcleo* de φ é o subgrupo de G definido por $\ker(\varphi) = \{a \in G \mid a\varphi = 1\}$. A *imagem* de φ é o subgrupo de H definido por $\mathrm{im}(\varphi) = \{a\varphi \mid a \in G\}$, que também denotaremos por $G\varphi$ ou $\varphi(G)$. Quando φ é bijetor, dizemos que é um *isomorfismo entre G e H* e que G e H são *isomorfos*; neste caso, escrevemos $G \simeq H$ ou $G \overset{\varphi}{\simeq} H$. Um *automorfismo* é um isomorfismo $G \to G$.

Um homomorfismo é injetor se, e somente se, seu núcleo consiste somente do elemento neutro. Quando dois grupos G e H são isomorfos, eles compartilham igualmente de todas as propriedades algébricas que estamos interessados. Será comum, portanto, nos referirmos a G ou a H alternadamente ou até tratá-los como sendo o mesmo grupo, conforme for mais conveniente.

As classes laterais serão usadas com a notação usual:

Definição 1.4. Dado um subgrupo H de um grupo G e $a \in G$, a *classe lateral (à esquerda)* de a em relação a H é o conjunto $aH = \{ah \mid h \in H\}$, e a *classe lateral (à direita)* de a em relação a H é o conjunto $Ha = \{ha \mid h \in H\}$. Da mesma forma, se N é outro subgrupo de G, definimos $HN = \{hn \mid h \in H,\ n \in N\} \subset G$.

Por serem classes de equivalência das relações "$a \sim b \Leftrightarrow a^{-1}b \in H$" e "$a \sim b \Leftrightarrow ab^{-1} \in H$", respectivamente, o conjunto das classes laterais (à esquerda ou à direita) particionam o conjunto G.

Definição 1.5. Seja $H \leq G$. O *índice de H em G* é a cardinalidade do conjunto das classes laterais de H em G, que denotaremos por $|G : H|$. Se esta cardinalidade for finita, dizemos que H tem índice finito em G.

Para que possamos adicionar uma estrutura de grupo à coleção de classes laterais, precisamos do seguinte:

Definição 1.6. Diremos que um subgrupo N de um grupo G é *normal (em G)* quando, para todo $a \in G$ e todo $n \in N$, vale $a^{-1}na \in N$. Nesse caso, denotamos $N \lhd G$ ou $G \rhd N$.

Definição 1.7. Seja G grupo e $N \lhd G$. O *quociente de G por N* é o conjunto $G/N = \{gN \mid g \in G\}$ munido da operação $(gN)(hN) = (gh)N$. Eventualmente o denotaremos por $\frac{G}{N}$. Dizemos também que obtemos G/N *quocientando* G por N.

O elemento neutro de G/N é o elemento $1N = N$. A projeção $\pi : G \to G/N$ definida por $g\pi = gN$ é um homomorfismo sobrejetor, cujo núcleo é exatamente o subgrupo N. Reciprocamente, todo núcleo de qualquer homomorfismo é um subgrupo normal. Quando $N = \{1\}$, temos um isomorfismo natural $G/\{1\} \simeq G$.

Outras formas equivalentes de definir e/ou verificar que um subgrupo é normal são:

Proposição 1.8. *Seja $N \leq G$. Os seguintes items são equivalentes:*

(i) $N \lhd G$;

(ii) $aN = Na$ *para todo* $a \in G$;

(iii) $a^{-1}Na \subset N$ *para todo* $a \in G$;

(iv) $a^{-1}Na = N$ *para todo* $a \in G$.

(v) N *é o núcleo de algum homomorfismo* φ *de* G *a algum grupo* H.

Análogo ao conceito de subgrupo gerado é o de fecho normal:

Definição 1.9. Dado um subconjunto R de um grupo G, o *fecho normal* de R em G é o menor subgrupo normal de G que contém R, ou a interseção de todos os subgrupos normais de G que contém R. O denotaremos por $\ll R \gg$.

É fácil demonstrar que o fecho normal $\ll R \gg$ também é o subgrupo gerado pelo conjunto de todos os conjugados de R em G, ou seja,

$$\ll R \gg = \left\langle \{g^{-1}rg \mid g \in G, r \in R\} \right\rangle .$$

Outro tipo de subgrupo que podemos criar, agora a partir de um elemento $g \in G$, é o seu centralizador:

Definição 1.10. Dado um elemento g em um grupo G, o *centralizador* de g em G é dado por $C_G(g) = \{h \in G \mid hg = gh\}$. É elementar verificar que é um subgrupo de G contendo o subgrupo $\langle g \rangle$ e que $\langle g \rangle \lhd C_G(g)$.

Para finalizar a seção, relembremos dois teoremas fundamentais, que podem ser encontrados em [9], p.44: o primeiro vamos sempre nos referir por TFI.

Teorema 1.11 (Teorema Fundamental do Isomorfismo (TFI))**.** *Se $\varphi : G \to H$ é um homomorfismo de grupos e $N = \ker(\varphi)$, então a aplicação $\overline{\varphi} : G/\ker(\varphi) \to \mathrm{im}(\varphi)$ definida por $(gN)\overline{\varphi} = g\varphi$ é um isomorfismo. Em particular, se φ é sobrejetor, temos $G/\ker(\varphi) \overset{\overline{\varphi}}{\simeq} H$.*

É claro que, se o homomorfismo φ acima é injetor, temos $G \overset{\varphi}{\simeq} \mathrm{im}(\varphi)$.

Teorema 1.12 (Segundo Teorema Fundamental do Isomorfismo)**.** *Seja G grupo e K, N subgrupos de G com $N \lhd G$. Então*

$$\frac{K}{N \cap K} \simeq \frac{NK}{N}.$$

1.2 Grupo livre e presentações

Esta seção apresenta os grupos livres e as presentações de grupos, objetos centrais do estudo da Teoria Combinatória de Grupos. Também apresentamos as propriedades básicas que serão necessárias para o desenvolvimento do restante do trabalho.

Grupo livre

Definição 1.13. Seja F um grupo e $X \subset F$ um subconjunto não vazio qualquer, com a inclusão $i : X \to F$. Dizemos que F é *livre em X* quando, para qualquer grupo G e qualquer função $\varphi : X \to G$, existe um único homomorfismo $\tilde{\varphi} : F \to G$ tal que $i\tilde{\varphi} = \varphi$. Diremos que $\tilde{\varphi}$ é uma *extensão* de φ para F e que o diagrama da figura 1.1 *comuta*.

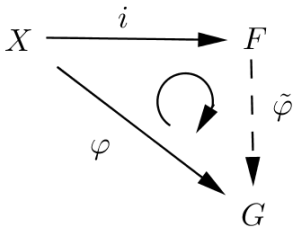
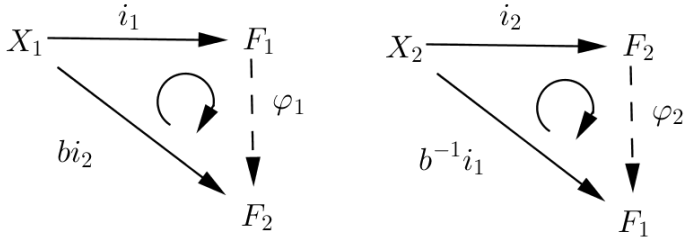


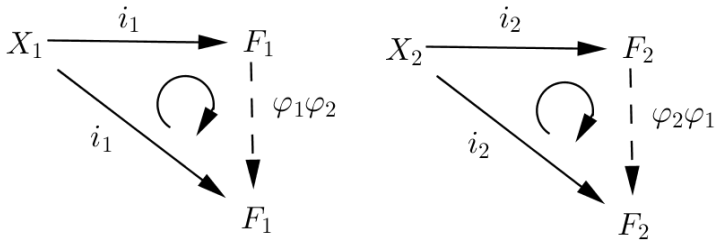
Figura 1.1: F é livre em X

Proposição 1.14. *Seja F_1 livre em X_1 e F_2 livre em X_2. Então $F_1 \simeq F_2$ se, e somente se,* $\mathrm{card}(X_1) = \mathrm{card}(X_2)$.

Demonstração. Suponha primeiramente $\mathrm{card}(X_1) = \mathrm{card}(X_2)$ e seja $b : X_1 \to X_2$ uma bijeção. Construimos as seguintes extensões φ_1 e φ_2:



Pela comutatividade dos diagramas acima, veja que os seguintes diagramas também comutam:



De fato, $(x)i_1\varphi_1\varphi_2 = (x)bi_2\varphi_2 = (x)bb^{-1}i_1 = (x)i_1$ e $(y)i_2\varphi_2\varphi_1 = (y)b^{-1}i_1\varphi_1 = (y)b^{-1}bi_2 = (y)i_2$, para todo $x \in X_1$ e $y \in X_2$. Mas é óbvio que Id_{F_1} e Id_{F_2} também fazem os diagramas respectivos acima comutarem. Assim, pela unicidade, $\varphi_1\varphi_2 = Id_{F_1}$ e $\varphi_2\varphi_1 = Id_{F_2}$, ou seja, ${\varphi_1}^{-1} = \varphi_2$ e φ_1 é isomorfismo entre F_1 e F_2.

Para a recíproca, seja F livre em X qualquer. Construiremos um quociente F/N cuja cardinalidade é $2^{\text{card}(X)}$ se X é finito e $\text{card}(X)$, se X é infinito. Assim, se $F_1 \simeq F_2$, é fácil ver que $F_1/N_1 \simeq F_2/N_2$; logo, obtemos $\text{card}(X_1) = \text{card}(X_2)$, tanto no caso infinito com no finito. Vamos à construção: seja $N = \langle w^2 \mid w \in F\rangle$. Afirmo que $N \lhd F$. De fato, dado $x \in F$ e uma palavra qualquer ${w_1}^2...{w_n}^2$ de N, temos

$$\begin{aligned} x^{-1}{w_1}^2...{w_n}^2x &= x^{-1}w_1(xx^{-1})w_1(xx^{-1})w_2(xx^{-1})w_2(xx^{-1})...(xx^{-1})w_n(xx^{-1})w_nx \\ &= (x^{-1}w_1x)(x^{-1}w_1x)...(x^{-1}w_nx)(x^{-1}w_nx) \\ &= (x^{-1}w_1x)^2...(x^{-1}w_nx)^2 \in N. \end{aligned}$$

Agora, como $(wN)(wN) = w^2N = N$ para $w \in F$, segue que F/N é um grupo abeliano, pois $(uN)(wN) = ((uN)(wN))^{-1} = (wN)^{-1}(uN)^{-1} = (wN)(uN)$. Seus elementos são todos da forma $x_1...x_nN$, onde cada $x_i \in X$ aparece apenas uma vez na palavra $x_1...x_n$. Isto porque, se aparecesse mais uma vez, obteríamos uma parcela ${x_i}^2N = N$, e x_i desapareceria. Seja $P_f(X)$ o conjunto dos subconjuntos finitos de X. O argumento acima garante que a função $\lambda : P_f(X) \to F/N$ que associa a $\{x_1, ..., x_n\}$ o elemento $x_1...x_nN$ é sobrejetora. Ela é também injetora. De fato, sejam $\{x_1, ..., x_n\} \neq \{y_1, ..., y_m\}$. Suponha, sem perda de generalidade, que $x_1 \notin \{y_1, ..., y_m\}$ e considere o elemento $(x_1...x_nN)(y_1...y_mN)^{-1} = x_1...x_n{y_m}^{-1}...{y_1}^{-1}N$. Este elemento não pode ser igual a N, pois x_1 não pode ser cancelado, já que não aparece novamente em nenhum dos x_i, nem em nenhum dos y_i. Logo $x_1...x_nN \neq y_1...y_mN$. Isso nos garante que $\text{card}(F/N) = \text{card}(P_f(X))$. Pela teoria de conjuntos, $\text{card}(P_f(X))$ é igual a $\text{card}(X)$, se X é infinito e $2^{\text{card}(X)}$, se X é finito. □

Veremos agora como construir, dado um conjunto X não vazio, um grupo F que contenha X e que seja livre em X, no sentido acima. Este objeto será o *grupo livre com base* X. Daremos apenas uma ideia da construção. Os detalhes podem ser encontrados em [11].

Dado um conjunto $X \neq \emptyset$, considere um conjunto Y disjunto de X e uma bijeção $X \to Y$. Ao elemento de Y correspondente a $x \in X$ pela bijeção damos o nome de x^{-1}, e denotamos $X^{-1} = \{x^{-1} \mid x \in X\}$. Primeiro consideramos o conjunto W_X das expressões da forma "1" ou "$a_1a_2...a_n$", com $a_i \in X \cup X^{-1}$ e $n \geq 1$, que chamaremos de *palavras em* X, e colocamos a operação $(a_1...a_n)(b_1...b_m) = a_1...a_nb_1...b_m$. A esse conjunto com esta operação damos o nome de *semigrupo livre de base* X. Criamos agora uma relação de equivalência em W_X, fazendo uma palavra ser equivalente a qualquer outra que se obtenha adicionando ou cancelando expressões da forma aa^{-1} ou $a^{-1}a$ em seu início, meio ou fim (por exemplo, $abb^{-1}c \sim ac$), e dizemos que uma palavra na qual todas as letras se cancelam é equivalente à palavra "1". Dizemos que uma palavra em X é *reduzida* se não possui mais nenhum termo da forma aa^{-1} ou $a^{-1}a$ a ser cancelado (por exemplo, aca^{-1}). É extremamente técnico, agora, provar que cada classe de equivalência em W_X é representada por exatamente uma palavra reduzida e que cada uma delas possui uma palavra reduzida inversa, no sentido de que o produto dê 1. Definimos o *grupo livre de base* X como sendo então o conjunto das palavras reduzidas em X, com a mesma operação acima, com a diferença que tomamos como resultado de $(a_1...a_n)(b_1...b_m)$ a palavra reduzida que representa a classe de $a_1...a_nb_1...b_m$. Denotaremos este grupo por F ou F_X, ou ainda, F_n, se $\text{card}(X) = n$. Neste último caso, diremos que o grupo livre é *finitamente gerado.*

Podemos entender os elementos $a \in X \cup X^{-1}$ como também elementos de F, pensando em a como uma palavra em F, que chamaremos de *letra* de F. Dessa forma, temos $X \subset F$ e a inclusão $i : X \to F$.

Proposição 1.15. *O grupo livre F de base X é livre em X, no sentido da definição 1.13.*

Demonstração. Seja G um grupo e $\varphi : X \to G$ uma função qualquer. Para criar um homomorfismo $\tilde{\varphi} : F \to G$, escreva cada elemento de F na forma ${a_1}^{k_1}...{a_n}^{k_n}$, com $a_i \in X$ e $k_i = \pm 1$. Defina $({a_1}^{k_1}...{a_n}^{k_n})\tilde{\varphi} = (a_1\varphi)^{k_1}...(a_n\varphi)^{k_n}$. Para ver que é um homomorfismo, sejam ${a_1}^{k_1}...{a_n}^{k_n}$ e ${b_1}^{l_1}...{b_m}^{l_m}$ elementos de F de modo que o produto $({a_1}^{k_1}...{a_n}^{k_n})({b_1}^{l_1}...{b_m}^{l_m})$ seja igual a ${a_1}^{k_1}...{a_{n-s}}^{k_{n-s}}{b_{1+s}}^{l_{1+s}}...{b_m}^{l_m}$, depois do cancelamento de $2s$ termos no meio. Temos então as igualdades

$$a_{n-s+1} = b_s,\ a_{n-s+2} = b_{s-1},\ ...,\ a_n = b_1, \tag{1.1}$$

bem como

$$k_{n-s+1} = -l_s,\ k_{n-s+2} = -l_{s-1},\ ...,\ k_n = -l_1. \tag{1.2}$$

Assim,

$$\begin{aligned}((a_1^{k_1}...a_n^{k_n})(b_1^{l_1}...b_m^{l_m}))\tilde{\varphi} &= (a_1^{k_1}...a_{n-s}^{k_{n-s}}b_{1+s}^{l_{1+s}}...b_m^{l_m})\tilde{\varphi} \\ &= (a_1\varphi)^{k_1}...(a_{n-s}\varphi)^{k_{n-s}}(b_{1+s}\varphi)^{l_{1+s}}...(b_m\varphi)^{l_m}\end{aligned}$$

e também

$$\begin{aligned}(a_1{}^{k_1}...a_n{}^{k_n})\tilde{\varphi}(b_1{}^{l_1}...b_m{}^{l_m})\tilde{\varphi} &= (a_1\varphi)^{k_1}...(a_n\varphi)^{k_n}(b_1\varphi)^{l_1}...(b_m\varphi)^{l_m} \\ &= (a_1\varphi)^{k_1}...(a_{n-s}\varphi)^{k_{n-s}}(b_{1+s}\varphi)^{l_{1+s}}...(b_m\varphi)^{l_m},\end{aligned}$$

pois os $2s$ termos do meio se cancelam, graças às equações 1.1 e 1.2.

Veja também que $a(i\tilde{\varphi}) = a\tilde{\varphi} = a\varphi$ para todo $a \in X$. Para a unicidade, suponha que exista outro homomorfismo $\psi : F \to G$ tal que $i\psi = \varphi$, ou seja, $\psi|_X = \varphi|_X$. Logo, para todo elemento, $(a_1{}^{k_1}...a_n{}^{k_n})\psi = (a_1\psi)^{k_1}...(a_n\psi)^{k_n} = (a_1\varphi)^{k_1}...(a_n\varphi)^{k_n} = (a_1{}^{k_1}...a_n{}^{k_n})\tilde{\varphi}$. □

Dado um conjunto X, pela proposição 1.14 só existe um grupo F, a menos de isomorfismo, que seja livre em X. Assim, pela proposição acima, podemos dizer que o grupo livre com base X é o único satisfazendo a definição 1.13.

Observação 1.16. Duas palavras reduzidas $u = x_1...x_n$ e $v = y_1...y_m$, $x_i, y_i \in X \cup X^{-1}$ de um grupo livre coincidem se, e somente se, $m = n$ e $x_i = y_i$. Um lado é trivial. Reciprocamente, suponha $u = v$, e $n \geq m$, sem perda de generalidade. Então $x_1...x_n{y_m}^{-1}...{y_1}^{-1} = 1$ e daí todas as letras devem se cancelar, pois senão sobraria uma palavra reduzida diferente de 1. Como os x_i's já não se cancelam entre si, bem como os y_i's, devemos ter $x_n = y_m$, $x_{n-1} = y_{m-1}$,...,$x_{n-m+1} = y_1$. Como já não há mais cancelamentos a serem feitos, devemos ter $n - m + 1 = 1$, ou seja, $n = m$ e daí $x_i = y_i$. Uma consequência disto é que o único grupo livre abeliano é o de apenas um gerador, ou seja, $X = \{a\}$. Pois, se a e b são elementos distintos de X, então $ab \neq ba$ pelo argumento acima.

Mais à frente, precisaremos dos seguintes dois fatos:

Proposição 1.17. *Todo semigrupo livre com base enumerável é enumerável.*

Demonstração. Seja X enumerável e W_X o semigrupo livre com base X. Como conjunto, temos $W_X = \cup_{k=1}^{\infty} S_k$, onde S_k é o conjunto das palavras com exatamente k letras. Basta vermos, então, que cada S_k é enumerável, e o resultado seguirá da Teoria de Conjuntos. Ora, para formarmos um elemento de S_k, temos k escolhas a fazer; cada escolha corresponde a tomar uma letra de $X \cup X^{-1}$. Então $\text{card}\,(S_k) = \text{card}\,((X \cup X^{-1})^k)$, e $(X \cup X^{-1})^k$ é enumerável, pela Teoria de Conjuntos e pelo fato de ser X enumerável. □

Corolário 1.18. *Todo grupo livre com base enumerável é enumerável.*

Demonstração. Como conjunto, $F_X \subset W_X$. Logo, F_X também deve ser enumerável. □

Vale a pena também citar o utilíssimo

Teorema 1.19 (Teorema de Nielsen-Schreier)**.** *Todo subgrupo de um grupo livre é livre.*

Presentações

As presentações são uma forma simplificada de estudarmos os grupos nos desvencilhando de notações demasiadas e nos concentrando apenas em suas propriedades fundamentais. Para justificar que cada grupo possui pelo menos uma presentação, precisamos da seguinte

Proposição 1.20. *Todo grupo G é isomorfo ao quociente de um grupo livre.*

Demonstração. Graças ao TFI, basta criar um homomorfismo sobrejetor de um grupo livre em G. Seja S um subconjunto que gera G (sempre existe, pois, no pior dos casos, tome $S = G$). Tome o grupo livre F_S e a inclusão $j : S \to G$. Pela proposição 1.15, existe um homomorfismo $\varphi : F_S \to G$, que é da forma $({s_1}^{k_1}...{s_n}^{k_n})\varphi = (s_1 j)^{k_1}...(s_n j)^{k_n} = {s_1}^{k_1}...{s_n}^{k_n}$. Dado que S gera G, é óbvio então que φ é sobrejetor. □

Definição 1.21. Dado um conjunto X e $R \subset F_X$, dizemos que um grupo G tem uma *presentação* $\langle X \mid R\rangle$ (ou que $\langle X \mid R\rangle$ é uma presentação para G) quando G é isomorfo ao quociente $F_X / \ll R \gg$. O grupo quociente também será denotado por $\langle X \mid R\rangle$, e escreveremos $G = \langle X \mid R\rangle$. Os elementos de X são chamados de *geradores* e os de R de *relações* da presentação. Quando X for finito, diremos que a presentação é *finitamente gerada* e quando $X = \{x_1, ..., x_n\}$ e $R = \{r_1, ..., r_m\}$ forem finitos, diremos que G é *finitamente presentado*, que a presentação é *finita* e a denotaremos por $\langle x_1, ..., x_n \mid r_1, ..., r_m\rangle$. Quando uma igualdade $w = z$ entre duas palavras em X aparecer entre as relações, queremos dizer que $wz^{-1} \in R$. Se duas presentações $\langle X \mid R\rangle$ e $\langle X' \mid R'\rangle$ definem um mesmo grupo, escrevemos $\langle X \mid R\rangle = \langle X' \mid R'\rangle$.

Corolário 1.22. *Todo grupo possui uma presentação*

Demonstração. Basta usar a construção da proposição 1.20. Dado G, escolha um subconjunto gerador qualquer S e crie então o isomorfismo $\overline{\varphi} : F_S/\ker(\varphi) \to G$. Agora, tome um subconjunto R de $\ker(\varphi)$ tal que $\ll R \gg = \ker(\varphi)$ (que sempre existe, pois, no pior dos casos, podemos tomar $R = \ker(\varphi)$). Logo, $G = \langle S \mid R\rangle$. □

Observação 1.23. Um grupo pode ter várias presentações distintas. Note que, na construção acima, tivemos a liberdade de escolher o conjunto gerador S e as relações R. Cada tal escolha de S e R nos dá uma presentação distinta (no aspecto lexicográfico) para G. Por exemplo, $\langle z \mid z\rangle$ e $\langle a, b, c \mid a^3, b^3, c^4, acac^{-1}, aba^{-1}bc^{-1}b^{-1}\rangle$ são presentações do grupo trivial. Se $G = F_X$ é o grupo livre com base X, podemos escolher $S = X$ e $R = \{1\}$ na demonstração acima, de modo que $F_X = \langle X \mid 1 = 1\rangle$ é uma presentação. Como $1 = 1$ é redundante, escrevemos $F_X = \langle X \mid \emptyset\rangle$ ou $F_X = \langle X\rangle$, ou seja, os grupos livres são aqueles que possuem uma presentação sem relações.

Decidir se duas presentações distintas definem o mesmo grupo é exatamente o problema do isomorfismo (citado na Introdução), uma pergunta em geral muito complexa a se responder. Mas há um resultado positivo que vale a pena mencionar: apesar de ser

definida como um quociente, uma presentação $\langle X \mid R\rangle$ é até que simples de se manipular. Na prática, consiste do grupo de palavras em X onde a operação é dada intuitivamente, concatenando as palavras e cancelando tudo o que for possível, inclusive as palavras de R. Levando isso em conta, podemos tomar um elemento $r \in\ll R \gg$ e teremos que a nova presentação $\langle X \mid R \cup \{r\}\rangle$ define o mesmo grupo que $\langle X \mid R\rangle$, pois as letras são as mesmas e a palavra r que é 1 no novo grupo, também já era no antigo. Também podemos adicionar um novo gerador desconhecido z, tomar uma palavra w nas letras de X e acrescentar a igualdade $z = w$ nas relações, e obteremos

$$\langle X \mid R\rangle = \left\langle X \cup \{z\} \mid R \cup \{zw^{-1}\}\right\rangle,$$

pois estamos impondo que a única letra nova no novo grupo seja igual a uma palavra já existente no antigo. Estas manipulações (e suas inversas naturais) são as transformações de Tietze. Como já citamos, Tietze demonstra em 1908 o seguinte

Teorema 1.24. *Duas presentações finitas $\langle X \mid R\rangle$ e $\langle X' \mid R'\rangle$ definem um mesmo grupo se, e somente se, $\langle X \mid R\rangle$ pode ser transformada em $\langle X' \mid R'\rangle$ por um número finito de transformações de Tietze.*

1.3 Produto semidireto e sequência exata

O produto semidireto de dois grupos e as sequências exatas são dois conceitos fundamentais para o trabalho em questão e estão intimamente relacionados. Nesta seção, vamos defini-los, compará-los e encontrar uma condição para impor sobre uma sequência exata para que eles se tornem equivalentes.

Definição 1.25. Sejam G e H dois grupos e $\sigma : H \to Aut(G)$ um homomorfismo, onde $Aut(G)$ é o *grupo dos automorfismos* de G com a operação de composição natural. O *produto semidireto* (externo) de G por H, que denotaremos por $G \rtimes H$, é o conjunto $G \times H$ munido da operação

$$(g_1, h_1)(g_2, h_2) = (g_1(g_2)(h_1)\sigma, h_1h_2),$$

onde $(g_2)(h_1)\sigma$ é a imagem de g_2 através do automorfismo $(h_1)\sigma$ de G.

É mecânica a verificação de que temos realmente um grupo e uma operação. Vale destacar que o inverso de (g, h) é $((g^{-1})(h^{-1})\sigma, h^{-1})$. Como vamos definir o produto semidireto interno depois, colocamos a palavra "externo" entre parêntesis para distinguir, mas nem sempre a usaremos. A primeira observação a ser feita é a de que o produto semidireto é uma generalização do já conhecido *produto direto* $G \times H$ de dois grupos (operação $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$, coordenada a coordenada). Basta tomar σ como o homomorfismo que associa a todo elemento h o automorfismo $Id : G \to G$.

Sendo um caso mais particular, com uma operação mais natural, o produto direto deveria então, intuitivamente, possuir propriedades mais fortes em relação a seus subgrupos. Isso é o que acontecerá a seguir. Relembremos uma de suas caracterizações:

Proposição 1.26. *Se um grupo G possui dois subgrupos normais H e K tais que $G = HK$ e $H \cap K = \{1\}$, então $G \simeq H \times K$ (a saber, pelo isomorfismo $(h,k) \mapsto hk$). Reciprocamente, um produto direto $G \times H$ possui dois subgrupos normais (a saber, $G \times \{1\}$ e $\{1\} \times H$), isomorfos a G e a H, respectivamente, tais que $G \times H = (G \times \{1\})(\{1\} \times H)$ e cuja interseção é $\{1\}$.*

Colocamos esta propriedade acima para comparação, pois o produto semidireto satisfaz uma outra da mesma natureza, com hipóteses mais fracas:

Definição 1.27. Seja G grupo e $N, H \leq G$. Dizemos G é o *produto semidireto interno* de N por H quando $N \lhd G$, $G = NH$ e $N \cap H = \{1\}$.

Proposição 1.28. *Se G é o produto semidireto interno de N por H, então $G \simeq N \rtimes H$, onde a operação do produto semidireto externo é a dada pela conjugação $(n)(h)\sigma = hnh^{-1}$. Reciprocamente, um produto semidireto $G \rtimes H$ é o produto semidireto interno de dois de seus subgrupos (a saber, de $G \rtimes \{1\}$ por $\{1\} \rtimes H$).*

Demonstração. A recíproca é uma verificação mecânica. Seja agora G um grupo e $N \lhd G$, $H \leq G$ tais que $G = NH$ e $N \cap H = \{1\}$. Seja $N \rtimes H$ o produto semidireto com a operação dada pela conjugação acima. Cada elemento g de G pode ser escrito como $g = nh$, $n \in N$, $h \in H$. Esta forma é única. De fato, se $nh = n'h'$, temos que ${n'}^{-1}n = h'h^{-1}$ e daí ambos os lados pertencem a $N \cap H = \{1\}$, logo $n = n'$ e $h = h'$. Esta decomposição única garante que a função $\varphi : N \rtimes H \to G$ com $(n,h) \mapsto nh$ é bijetora. Para ver que é um isomorfismo, basta ver que

$$((n_1,h_1)(n_2,h_2))\varphi = (n_1(h_1n_2h_1^{-1}), h_1h_2)\varphi = n_1h_1n_2h_1^{-1}h_1h_2 = n_1h_1n_2h_2 = (n_1,h_1)\varphi(n_2,h_2)\varphi.$$

□

A proposição 1.28 nos diz, em suma, que todo produto semidireto interno é um produto semidireto e vice-versa. Em virtude disto, vamos confundir os dois conceitos e eventualmente escrever $G = N \rtimes H$ ou $G \simeq N \rtimes H$, mesmo para o caso interno.

Proposição 1.29. *Se $G = N \rtimes H$, então $G/N \simeq H$.*

Demonstração. Basta criar um homomorfismo sobrejetor $G \xrightarrow{\gamma} H$ com núcleo N e usar o TFI. Dado $g \in G$, decompomos $g = nh$ como na proposição 1.28 e definimos $g\gamma = h$. A unicidade da decomposição nos dá a boa definição de γ. A sobrejetividade é óbvia, pois $h \mapsto h$. Vejamos que γ é homomorfismo. Sejam $g, g' \in G$ e decomponha $g = nh$ e $g' = n'h'$. Como $N \lhd G$, temos $hn' \in hN = Nh$, logo $hn' = \tilde{n}h$ para algum $\tilde{n} \in N$. Daí $gg' = nhn'h' = (n\tilde{n})(hh')$ é a decomposição de gg', portanto $(gg')\gamma = hh' = g\gamma g'\gamma$, pela definição de γ. □

Definição 1.30. Entenderemos por *sequência exata* um objeto da forma

$$1 \xrightarrow{\varphi} F \xrightarrow{\alpha} G \xrightarrow{\beta} H \xrightarrow{\psi} 1,$$

onde 1 representa o grupo trivial $\{1\}$, F, G e H são grupos quaisquer, as setas são homomorfismos de grupos e valem as seguintes igualdades: $\text{im}(\varphi) = \ker(\alpha)$, $\text{im}(\alpha) = \ker(\beta)$ e $\text{im}(\beta) = \ker(\psi)$.

As igualdades $\text{im}(\varphi) = \ker(\alpha)$ e $\text{im}(\beta) = \ker(\psi)$ equivalem, respectivamente, a α ser injetor e β ser sobrejetor. Portanto, a partir de agora, vamos omitir as letras φ e ψ e apenas usar estes dois últimos fatos. A equação $\text{im}(\alpha) = \ker(\beta)$ também será chamada de *exatidão* da sequência em G, e G poderá ser chamado de o *grupo central*.

Sempre que N é um subgrupo normal de qualquer grupo G, pode-se criar a sequência exata $1 \to N \xrightarrow{i} G \xrightarrow{\pi} G/N \to 1$, onde i é a inclusão e π é a projeção ao quociente da página 3. Reciprocamente, se temos uma sequência exata qualquer $1 \to F \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$, conseguimos um subgrupo normal $\text{im}(\alpha) = \ker(\beta) \lhd G$. O conceito de sequência exata parece, então, ter a mesma força do que o de subgrupo normal. Como o produto semidireto exige mais do que uma normalidade, é natural pensar que ele é mais forte do que uma sequência exata:

Proposição 1.31. *Se $G = N \rtimes H$, então existe uma sequência exata*

$$1 \to N \to N \rtimes H \to H \to 1.$$

Demonstração. Da proposição 1.28, temos $H \leq G$, $N \lhd G$ e um isomorfismo $\varphi : N \rtimes H \to G$ dado por $(n, h) \mapsto nh$. Da proposição 1.29 temos um isomorfismo $G/N \xrightarrow{\psi} H$ com $nhN \mapsto h$. Considere os homomorfismos $i : N \to G$ e $\pi : G \to G/N$ como acima. Podemos criar com tudo isto a sequência

$$1 \longrightarrow N \xrightarrow{i\varphi^{-1}} N \rtimes H \xrightarrow{\varphi\pi\psi} H \longrightarrow 1.$$

Vejamos que ela é exata. Primeiramente, como φ e i são injetores, $i\varphi^{-1}$ é injetor, e como ψ, π e φ são sobrejetores, $\varphi\pi\psi$ é sobrejetor. Para a exatidão em $N \rtimes H$, veja que $n(i\varphi^{-1}) = n\varphi^{-1} = (n, 1)$ e $(n, h)(\varphi\pi\psi) = (nh)\pi\psi = (nhN)\psi = h$, logo $(n, h)\varphi\pi\psi = 1 \Leftrightarrow (n, h) = (n, 1) \in \text{im}(i\varphi^{-1})$, ou seja, $\ker(\varphi\pi\psi) = \text{im}(i\varphi^{-1})$, como desejado. □

Como já dissemos, a proposição acima nos diz que o conceito de produto semidireto é igual ou mais forte do que o de sequência exata. O exemplo a seguir mostra que é, na verdade, estritamente mais forte:

Exemplo 1.32. Considere a sequência $1 \to \mathbb{Z} \xrightarrow{\alpha} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_2 \to 1$, onde α é a multiplicação por dois e π a projeção ao quociente. É fácil ver que é uma sequência exata. Porém, não podemos ter um isomorfismo $\mathbb{Z} \simeq \mathbb{Z} \rtimes \mathbb{Z}_2$, pois temos $(0, 1) + (0, 1) = (0, 0)$ em $\mathbb{Z} \rtimes \mathbb{Z}_2$ e $\mathbb{Z}$ não possui um elemento não nulo com esta propriedade.

Portanto, nem toda sequência exata gera um isomorfismo entre o grupo central e o produto semidireto dos outros dois. O que veremos agora é uma condição sob a qual isto necessariamente acontece.

Definição 1.33. Dizemos que uma sequência exata $1 \to F \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$ *cinde* quando existe homomorfismo $\gamma : H \to G$ tal que $\gamma\beta = Id_H$.

Exemplo 1.34. Toda sequência exata $1 \to F \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$ com H sendo um grupo livre cinde. De fato, seja X a base de H. Dado $x \in X$, como β é sobrejetor, defina $x\varphi$ como sendo um elemento fixado da imagem inversa $\beta^{-1}(x)$ e estenda esta função para o homomorfismo $\tilde{\varphi} : H \to G$. Como $\tilde{\varphi}\beta$ é a identidade na base X (por construção), é claro que o será também em H todo.

Proposição 1.35. *Se uma sequência exata* $1 \to F \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$ *cinde, então* $G \simeq F \rtimes H$.

Demonstração. Considere o homomorfismo $\gamma : H \to G$ tal que $\gamma\beta = Id_H$. Na verdade, provaremos que G é o produto semidireto interno de $\mathrm{im}(\alpha) \simeq F$ e $\mathrm{im}(\gamma) \simeq H$ (estes dois isomorfismos valem porque α e γ são injetores). Temos $\mathrm{im}(\alpha) = \ker(\beta) \lhd G$. Basta então provar que $\mathrm{im}(\alpha) \cap \mathrm{im}(\gamma) = \{1\}$ e $G = \mathrm{im}(\alpha)\,\mathrm{im}(\gamma)$. Para a primeira igualdade, seja $g \in \mathrm{im}(\alpha) \cap \mathrm{im}(\gamma)$. Então, como $\mathrm{im}(\alpha) = \ker(\beta)$, temos $g\beta = 1$. Por outro lado, $g = h\gamma$ para algum $h \in H$. Daí $1 = g\beta = h\gamma\beta = h(\gamma\beta) = h$, e portanto $g = 1\gamma = 1$. Para a segunda igualdade, tome $g \in G$ qualquer e escreva

$$g = g(g\beta\gamma)^{-1}(g\beta\gamma).$$

Agora note que a parte da direita $g\beta\gamma = (g\beta)\gamma$ está em $\mathrm{im}(\gamma)$ e a parte restante da esquerda $g(g\beta\gamma)^{-1}$ está em $\mathrm{im}(\alpha) = \ker(\beta)$, pois

$$(g(g\beta\gamma)^{-1})\beta = (g\beta)((g\beta)^{-1}\gamma\beta) = (g\beta)(g\beta)^{-1} = 1.$$

□

Em resumo, o produto semidireto é uma forma de se decompor um grupo. É um conceito mais fraco do que o de produto direto, mais forte do que o de sequências exatas e equivalente ao de sequências exatas que cindem. Em virtude da proposição 1.35 acima e do fato de que a sequência exata criada na proposição 1.31 cinde, obtemos o

Corolário 1.36. *Um grupo G é o produto semidireto de F por H se, e somente se, G é o grupo central de uma sequência exata* $1 \to F \to G \to H \to 1$ *que cinde.*

Definição 1.37. Sejam N, G e H grupos quaisquer. Dizemos que G é *N-por-H* (ou que G é uma *extensão de N por H*) quando possui um subgrupo normal (isomorfo a) N com $G/N \simeq H$. Quando N ou H são livres, ou cíclicos, ou abelianos, etc., dizemos que G é

livre-por-cíclico, livre-por-livre, abeliano-por-livre, etc. Por exemplo, se N é abeliano e H é livre, dizemos que G é abeliano-por-livre.

Proposição 1.38. *G é N-por-H se, e somente se, existe sequência exata $1 \to N \to G \to H \to 1$.*

Demonstração. Se G é N-por-H, tome os isomorfismos $N \xrightarrow{\alpha} N\alpha$, $G/N\alpha \xrightarrow{\beta} H$, a inclusão $N\alpha \xrightarrow{i} G$ e a projeção $G \xrightarrow{\pi} G/N\alpha$ e é fácil ver que a sequência $1 \to N \xrightarrow{\alpha i} G \xrightarrow{\pi\beta} H \to 1$ é exata. Se $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$ é exata, então $N\alpha$ é um subgrupo normal de G (pois é o núcleo de β), isomorfo a N (pois α é injetor) e temos $G/N\alpha \simeq H$, pois β é um homomorfismo sobrejetor de núcleo $N\alpha$. □

Corolário 1.39. *Um grupo G é N-por-livre se, e somente se, G é o produto semidireto de N por um grupo livre.*

Demonstração. Seja F o grupo livre. Se G é N-por-F, a Proposição 1.38, o exemplo 1.34 e, finalmente, a Proposição 1.35 garantem que $G \simeq N \rtimes F$. A recíproca é imediata da Proposição 1.31. □

Usaremos várias vezes, mais adiante, a seguinte construção:

Definição 1.40. Seja $F = \langle X \mid R\rangle$ um grupo com uma presentação qualquer e $\varphi_1, ..., \varphi_m \in Aut(F)$. Chamamos de *extensão livre de F por $\varphi_1, ..., \varphi_m$* e denotamos por $F \rtimes_{\varphi_1,...,\varphi_m} F_m$ o grupo que tem a seguinte presentação:

$$F \rtimes_{\varphi_1,...,\varphi_m} F_m = \left\langle X, t_1, ..., t_m \mid R, {t_i}^{-1} x t_i = x\varphi_i \ (x \in X, i = 1, ..., m)\right\rangle. \tag{1.3}$$

Observação 1.41. Vamos dar sentido à notação $F \rtimes_{\varphi_1,...,\varphi_m} F_m$ e ao nome do grupo acima. Afirmo que um grupo tem a presentação 1.3 se, e somente se, é um produto semidireto de F por F_m. De fato, suponha que G é dado pela presentação 1.3. Seja $\langle X\rangle \subset F \rtimes_{\varphi_1,...,\varphi_m} F_m$ o subgrupo gerado pelas letras de X e $\langle t_1, ..., t_m\rangle \subset F \rtimes_{\varphi_1,...,\varphi_m} F_m$ o subgrupo gerado por $t_1, ..., t_m$ (ambos os subgrupos estão claramente submetidos às relações do grupo maior). Como as relações ${t_i}^{-1} x t_i = x\varphi_i$ envolvem os t_i, elas não têm nenhum papel em $\langle X\rangle$, logo $\langle X\rangle$ é o grupo das palavras em X submetidas apenas às relações de R, ou seja, $\langle X\rangle \simeq F$. Analogamente, como as relações ${t_i}^{-1} x t_i = x\varphi_i$ também envolvem os $x \in X$, elas não afetam $\langle t_1, ..., t_m\rangle$, de modo que $\langle t_1, ..., t_m\rangle \simeq F_m$. É claro que a interseção destes dois subgrupos é $\{1\}$ e que eles geram o grupo todo. Por último, veja que F é um subgrupo normal, pois, conjugando um elemento de F por uma letra de X obviamente nos mantemos em F, e conjugando por uma letra t_i obtemos

$${t_i}^{-1} x_1 ... x_n t_i = (t_i^{-1} x_1 t_i) ... (t_i^{-1} x_n t_i) = x_1\varphi_i ... x_n\varphi_i = (x_1 ... x_n)\varphi_i \in F,$$

graças às relações ${t_i}^{-1} x t_i = x\varphi_i$, novamente. Logo, o grupo $F \rtimes_{\varphi_1,...,\varphi_m} F_m$ é realmente o produto semidireto de F por F_m (portanto, a notação faz sentido), e o homomorfismo

$\sigma : F_m \to Aut(F)$ da definição 1.25 é dado, graças à proposição 1.28, por

$$\begin{aligned}(x_1...x_n)(t_{i_i}...t_{i_k})\sigma &= (t_{i_1}...t_{i_k})^{-1}(x_1...x_n)(t_{i_1}...t_{i_k}) \\ &= {t_{i_k}}^{-1}...{t_{i_1}}^{-1}x_1...x_n t_{i_1}...t_{i_k} \\ &= (x_1...x_n)\varphi_{i_1}...\varphi_{i_k}.\end{aligned}$$

Provamos que, se um grupo tem a presentação 1.3, então é o produto semidireto de F por F_m pelos φ_i dados. Por outro lado, suponha que G seja um produto semidireto qualquer de F por F_m e vamos justificar porque G tem uma presentação como 1.3. Como $G = F_m F$, os geradores de F (o conjunto X) junto com os de F_m $(t_1, ..., t_m)$ geram G. Como em G há uma cópia de F e outra de F_m, em G devem valer as relações de F (o conjunto R), as de F_m (o conjunto vazio) e também as relações entre F e F_m. Estas relações são as seguintes: como $F \lhd G$, temos ${t_i}^{-1}xt_i \in F$ para todo $x \in X$ e $i = 1, ..., m$. Logo, denotemos ${t_i}^{-1}xt_i = x\varphi_i$ e estenda as funções φ_i para homomorfismos φ_i de F em F, que se tornam automorfismos de conjugação em F. As relações entre F e F_m são exatamente dadas pelas equações ${t_i}^{-1}xt_i = x\varphi_i$, de modo que G tem exatamente a presentação 1.3.

Usando a afirmação provada acima, como F_m é livre e temos um produto semidireto, o Corolário 1.39 garante que um grupo $F \rtimes_{\varphi_1,...,\varphi_m} F_m$ como acima é F-por-livre, ou uma extensão de F pelo grupo livre F_m, o que dá sentido ao nome "extensão livre" dado e também garante que um grupo G terá uma presentação deste tipo se, e somente se, for o termo central de uma sequência exata da forma $1 \to F \to G \to F_m \to 1$.

Capítulo 2

Algoritmos e problemas de decisão

As demonstrações dos resultados positivos da Teoria Combinatória de Grupos, neste trabalho, se baseiam em duas estratégias: a construção de algoritmos que possam resolver os problemas de decisão, e as justificativas teóricas do porquê dos mesmos funcionarem. É imprescindível, portanto, entendermos bem o que são problemas de decisão e algoritmos. Neste capítulo, vamos iniciar esta discussão e apresentar alguns exemplos explícitos, para um melhor entendimento do texto posterior.

2.1 Definições e conceitos

Entenderemos aqui um *algoritmo* da maneira intuitiva: um conjunto finito de instruções passo-a-passo que associa a cada entrada um dado final, totalmente determinado pela entrada. A finitude dos algoritmos talvez seja a propriedade mais importante neste trabalho. Estamos excluindo os casos indesejáveis onde o processo nunca pára e não nos dá uma resposta efetiva, o que seria obviamente péssimo, tanto no meio de uma demonstração quanto na hora de uma computação explícita. O fato de o resultado final ser totalmente determinado pela entrada tem a ver com o algoritmo ser *determinístico*: basicamente, quer dizer que não depende de variáveis exteriores e não possui nenhum tipo de aleatoriedade. Isto implica que todas as vezes que entrarmos com o mesmo conjunto inicial de dados, obteremos o mesmo dado final. Vale ressaltar também que não estamos interessados em otimizar algoritmos, mas apenas em demonstrar que eles são finitos, por mais obsoletos que sejam.

Entenderemos por um *problema de decisão* uma questão a ser respondida (com um sim ou um não) para um certo conjunto de entradas, através de um algoritmo. Se existe tal algoritmo, dizemos que o problema é decidível ou *solúvel* para o conjunto de entradas. Caso contrário, dizemos que o problema é indecidível ou *insolúvel*.

Note que não podemos dizer que um problema do tipo acima é insolúvel simplesmente por não termos achado um algoritmo que o resolva, mas sim por termos efetivamente demonstrado que não é possível construir tal algoritmo. Neste sentido, é natural de se

esperar que seja muito mais fácil, em geral, tentar construir um algoritmo que resolva positivamente um problema do que demonstrar uma tal não existência. Isto justifica o seguinte acontecimento na Teoria Combinatória de Grupos: segundo [3], nos anos de 1935-1936, quando a noção ainda intuitiva de algoritmo foi precisamente descrita por Alan Turing e também por Alonzo Church (possibilitando provas reais de insolubilidade que vieram somente alguns anos depois), vários algoritmos já haviam sido criados para provar resultados positivos de solubilidade, como, por exemplo, o Problema da Palavra e da Conjugação para presentações de grupos fundamentais de superfícies fechadas com genus 2 ou mais (feito por Dehn), e o Problema da palavra para qualquer presentação com apenas uma relação (generalização do anterior, feita por W. Magnus em 1932). Atualmente, tanto a Álgebra algorítmica quanto a Lógica de decidabilidade são amplamente usadas e tanto resultados positivos quanto negativos são estudados.

Antes de continuarmos, vamos reenunciar mais precisamente os três problemas clássicos:

- **O Problema da Palavra (PP):** dado um grupo $G = \langle X \mid R\rangle$ e $w \in G$ uma palavra em termos da presentação de G, decidir quando $w = 1$ em G (ou seja, quando w se escreve como produto das relações R e seus conjugados).
- **O Problema da Conjugação (PC):** dados dois elementos x e y de um mesmo grupo $G = \langle X \mid R\rangle$ em termos desta presentação, decidir quando são *conjugados* em G (denotaremos $x \sim y$), ou seja, quando existe $u \in G$ tal que $x = u^{-1}yu$.
- **O Problema do Isomorfismo (PI):** dados dois grupos $G = \langle X \mid R\rangle$ e $H = \langle X' \mid R'\rangle$, decidir quando são isomorfos.

Se PC(G) é solúvel, também o é PP(G), pois, dado $w \in G$, $w = 1$ se, e somente se, $w \sim 1$, o que é decidível por hipótese. O PI é diferente dos demais, pois diz respeito a uma propriedade global, e não de elementos de um grupo. Vale a pena observar também que PP(G) equivale a decidir quando duas palavras u e v em termos da presentação de G são iguais em G. Isto acontece porque $u = v \leftrightarrow uv^{-1} = 1$ em G. Logo, se temos PP, podemos decidir quando $uv^{-1} = 1$, ou seja, quando $u = v$. Reciprocamente, se podemos decidir quando duas palavras são iguais em G, podemos decidir quando uma palavra w é igual à palavra 1, que é PP.

Definição 2.1. Dado um automorfismo φ de um grupo G, dizemos que dois elementos x e y de G são *φ-conjugados* em G quando existe $u \in G$ tal que $x = (u\varphi)^{-1}yu$. Neste caso, escrevemos $x \sim_\varphi y$.

Proposição 2.2. *A relação $\sim_\varphi$ é de equivalência, que chamaremos de* conjugação torcida.

Demonstração. Para provar que $x \sim_\varphi x$, basta tomar $u = 1$, já que $1\varphi = 1$. Para a simetria, observe que $x = (u\varphi)^{-1}yu$ implica $y = (u^{-1}\varphi)^{-1}xu^{-1}$. Para a transitividade, veja

que $x = (u\varphi)^{-1}yu$ e $y = (v\varphi)^{-1}zv$ implica que $x = (u\varphi)^{-1}((v\varphi)^{-1}zv)u = ((vu)\varphi)^{-1}z(vu)$. □

Agora podemos apresentar o

- **O Problema da Conjugação Torcida (PCT):** dados um automorfismo φ e dois elementos x e y de um mesmo grupo $G = \langle X \mid R\rangle$ em termos desta presentação, decidir quando são *φ-conjugados* em G (denotaremos $x \sim_\varphi y$), ou seja, quando existe $u \in G$ tal que $x = (u\varphi)^{-1}yu$.

É claro que PCT(G) é uma grande generalização de PC(G), onde tomamos sempre $\varphi = Id_G$. Portanto, PCT(G) solúvel implica PC(G) solúvel.

Note que todos os quatro problemas que apresentamos estão enunciados não somente a partir de grupos, mas de presentações dadas a eles. Poderíamos nos perguntar então se existem, por exemplo, grupos com algumas presentações com PC solúvel e outras com PC não solúvel. A resposta é negativa, no caso de sabermos passar algoritmicamente de uma presentação para outra:

Proposição 2.3. *Seja G um grupo com duas presentações $\langle X \mid R\rangle$ e $\langle X' \mid R'\rangle$. Suponha que podemos escrever algoritmicamente cada elemento de g em termos de $\langle X \mid R\rangle$ e de $\langle X' \mid R'\rangle$, e vice-versa. Então PP, PC ou PCT é solúvel em $\langle X \mid R\rangle$ se, e somente se, o for em $\langle X' \mid R'\rangle$.*

Demonstração. Considere os isomorfismos $\langle X \mid R\rangle \xrightarrow{\alpha} G$ e $\langle X' \mid R'\rangle \xrightarrow{\beta} G$. Suponha que PP, PC ou PCT é solúvel em $\langle X \mid R\rangle$ e sejam $u', v' \in \langle X' \mid R'\rangle$ duas palavras (e $\varphi \in Aut(G)$ no caso PCT). Por hipótese, computamos explicitamente $u'\beta, v'\beta \in G$. Novamente por hipótese, computamos $u = u'\beta\alpha^{-1}, v = v'\beta\alpha^{-1} \in \langle X \mid R\rangle$. Ora, u e v são palavras tais que $u\alpha = u'\beta$ e $v\alpha = v'\beta$. Por isto, temos as óbvias equivalências:

$$\begin{aligned} u'\beta = v'\beta &\Leftrightarrow u\alpha = v\alpha, \\ \text{existe } g \in G \text{ tal que } g^{-1}(u'\beta)g = v'\beta &\Leftrightarrow \text{existe } g \in G \text{ tal que } g^{-1}(u\alpha)g = v\alpha, \\ \text{existe } g \in G \text{ tal que } (g\varphi)^{-1}(u'\beta)g = v'\beta &\Leftrightarrow \text{existe } g \in G \text{ tal que } (g\varphi)^{-1}(u\alpha)g = v\alpha. \end{aligned}$$

Agora, decidir sobre as afirmações à esquerda é exatamente resolver PP, PC ou PCT para $\langle X' \mid R'\rangle$, e decidir sobre as da direita é possível por hipótese. Logo, $\langle X' \mid R'\rangle$ tem PP, PC ou PCT solúvel. □

Observação 2.4. Após nos depararmos com tais problemas de decisão, é natural nos perguntarmos em quais grupos conseguimos resolvê-los. Há alguns casos triviais, que listamos abaixo:

- **PP, PC e PCT em grupos finitos:** todo grupo finito $G = \{g_1, ..., g_n\}$ (com $g_1 = 1$) possui uma presentação dada pela sua tabela de multiplicação $g_ig_j = g_{ij}$,

que é a presentação $G = \langle g_1, g_2, ..., g_n \mid g_i g_j {g_{ij}}^{-1},\ (1 \leq i, j \leq n)\rangle$. Dada uma palavra $w = {g_{i_1}}^{e_1} ... {g_{i_r}}^{e_r}$, com $e_k = \pm 1$, para vermos se $w = 1$ em G basta operarmos as letras de w duas a duas através da tabela de multiplicação de G obtendo no final que $w = g_{k(w)} := g_w$ (em G) para algum $1 \leq k(w) \leq n$ e daí $w = 1$ exatamente quando $k(w) = 1$, o que sabemos obviamente responder, logo PP(G) é solúvel. PCT(G) (e, portanto, PC(G)) é semelhante: dado um automorfismo φ e duas palavras u e v como acima, fazemos para ambas o que fizemos para w acima obtendo $u = g_u$ e $v = g_v$. Então para decidir se u e v são conjugadas em G basta fazer os n testes de verificar quando $({g_i}^{-1})\varphi g_u g_i {g_v}^{-1} = 1$ em G, novamente através da tabela de multiplicação.

- **PP em grupos livres:** seja w uma palavra reduzida em $F = F_X$. Como o grupo livre possui uma presentação sem relações, é claro que decidir se $w = 1$ em F é ver se w já é a palavra trivial 1, ou seja, qualquer palavra reduzida que contenha qualquer uma das letras de X já não pode ser 1.

- **PI em grupos livres finitamente gerados:** já sabemos que dois grupos livres F_X e F_Y são isomorfos se, e somente se, $|X| = |Y|$. Então PI para grupos livres se resume em decidir quando dois conjuntos têm a mesma cardinalidade, o que é óbvio para dois conjuntos finitos dados.

Poderíamos, ingenuamente, tentar usar PP(F) para um grupo livre de base enumerável F para resolver PC(F): tome uma enumeração $F = \{w_1, w_2, ...\}$ (Proposição 1.18). Dadas duas palavras u e v, podemos verificar (em ordem crescente) para todo w_i se ele conjuga u e v, usando PP(F) na palavra ${w_i}^{-1} u w_i v^{-1}$. Se u e v são realmente conjugados, em algum momento encontramos o w_i correto e o algoritmo pára. O problema é que se u e v não são conjugados, o algoritmo segue indefinidamente e nunca descobre este desagradável fato. Este método não é, portanto, efetivo, e este problema é um caso particular do argumento mais geral:

Observação 2.5. Seja $X = \{x_1, x_2, ...\}$ um conjunto enumerável e suponha que exista uma pergunta "P" que pode ser algoritmicamente respondida (com sim ou não) para todo $x_i \in X$, o que podemos abreviar por "$P(x_i)$ é solúvel". Isto não implica que o problema "$\tilde{P}(X)$: existe $x_i \in X$ tal que $P(x_i)$ é válido" é solúvel. De fato, podemos testar individualmente para cada x_i. Se existir algum x_i tal que $P(x_i)$ é válido, em algum instante nós encontraremos com o algoritmo, pois testando para todo x_i atingimos todo elemento de X em algum momento, já que X é enumerável. Porém, caso um tal x_i não exista por algum motivo, nossos testes cegos e individuais seguirão indefinidamente nos dando sempre respostas negativas (portanto não poderemos nunca afirmar que tal x_i existe) e também não podemos afirmar que x_i não existe, pois sempre haverão infinitos testes que ainda não foram feitos.

Porém, o Problema da Conjugação é, sim, solúvel em qualquer grupo livre. A justificativa passa por palavras ciclicamente reduzidas:

Definição 2.6. Seja $F = F_X$ um grupo livre e $1 \neq w = x_1...x_n \in F$, $x_i \in X \cup X^{-1}$ uma palavra reduzida qualquer. Dizemos que w é *ciclicamente reduzida* quando $x_n x_1 \neq 1$ em F.

Proposição 2.7. *Toda palavra reduzida* $1 \neq w = x_1...x_n$ *em um grupo livre* F_X *pode ser escrita unicamente da forma*

$$w = a^{-1}\tilde{w}a,$$

onde $a \in F$ *e* $1 \neq \tilde{w} \in F$ *é ciclicamente reduzida.*

Demonstração. Comparando x_1 com x_n, x_2 com x_{n-1} e assim sucessivamente, consegue-se o menor inteiro positivo s tal que $x_{1+s}x_{n-s} \neq 1$. Este inteiro existe pois, se w possui um número ímpar $n = 2k + 1$ de letras, no pior dos casos todas as letras x_{1+i} e x_{n-i} se cancelam simetricamente e resta a letra do meio x_{k+1}, de modo que $s = k$, e se w possui um número par $n = 2k$ de letras, no pior dos casos todas as letras x_{1+i} e x_{n-i} se cancelam até que restem as letras do meio $x_k x_{k+1}$ que não se cancelam pois, se também se cancelassem teríamos $w = 1$. Depois de encontrarmos tal s, por construção temos

$$w = x_1...x_s x_{1+s}...x_{n-s}x_{n-s+1}...x_n = (x_{n-s+1}...x_n)^{-1}x_{1+s}...x_{n-s}(x_{n-s+1}...x_n) = a^{-1}\tilde{w}a,$$

onde $a = x_{n-s+1}...x_n$ e $\tilde{w} = x_{1+s}...x_{n-s} \neq 1$ é ciclicamente reduzida. Esta decomposição é a única que satisfaz estas propriedades, pois, para índices maiores do que o s tomado, não conseguiríamos as palavras a e a^{-1} de forma que $w = a^{-1}\tilde{w}a$, e para índices menores não teríamos $\tilde{w}$ ciclicamente reduzido. □

Proposição 2.8. *O Problema da Conjugação é solúvel em grupos livres.*

Demonstração. Seja F um grupo livre de base X e $u, v \in F$. Decomponha $u = a^{-1}\tilde{u}a$ e $v = b^{-1}\tilde{v}b$, como na proposição 2.7. É fácil ver que u e v são conjugados em F se, e somente se $\tilde{u}$ e $\tilde{v}$ o forem, logo podemos supor u e v ciclicamente reduzidas. Afirmo que u e v são conjugados por um elemento c se, e somente se, u é uma permutação yc de dois blocos de letras de $v = cy$, e isto torna o problema solúvel, pois decidir se são conjugados se torna fazer um número finito de testes, já que só existe um número finito de tais permutações.

Provemos agora a afirmação. De fato, se $u = yc$ e $v = cy$, é claro que $c^{-1}vc = c^{-1}cyc = yc = u$. Por outro lado, se $c^{-1}vc = u$, a palavra à esquerda deve ser ciclicamente reduzida (pois u o é), logo c^{-1} deve se cancelar inteiramente com as primeiras letras de v ou c deve se cancelar inteiramente com as últimas (pois, caso contrário, $c^{-1}vc$ seria uma palavra começando com a primeira letra de c^{-1} e terminando com sua inversa, absurdo com o fato de ser ciclicamente reduzido). Analisemos os dois casos. No caso em que c^{-1} cancela,

devemos ter $v = cy$ para alguma palavra y e daí $u = c^{-1}vc = c^{-1}cyc = yc$. No caso em que c se cancela, devemos ter $v = yc^{-1}$, logo $u = c^{-1}vc = c^{-1}yc^{-1}c = c^{-1}y$. Em ambos os casos, u é uma permutação de dois pedaços de v. □

2.2 Alguns algoritmos explícitos

Neste trabalho, não estamos interessados em construir programas computacionais que resolvam os problemas algebricamente; tampouco queremos nos debruçar sobre demasiados cálculos. Mas acreditamos que seja importante reservar um momento para entender melhor o conceito de algoritmo, dado no início deste capítulo, em seu aspecto prático, para nos atentarmos que eles são realmente computáveis, mesmo alguns sendo obsoletos do ponto de vista computacional. Nesta seção, vamos resolver algoritmicamente alguns problemas.

No Problema da Palavra

Suponha termos uma palavra reduzida w em $G = \langle X \mid R \rangle$ que sabemos ser igual a 1, por algum resultado teórico. Então, teoricamente, w se escreve como produto dos elementos de R e seus conjugados. A pergunta é: conseguimos então, explicitamente, escrever w como um tal produto? A resposta é positiva para um grupo finitamente presentado.

Proposição 2.9. *Se $G = \langle x_1, ..., x_n \mid r_1, ..., r_k \rangle$ é finitamente presentado e $w = 1$ em G, existe um algoritmo que computa $r_{i_1}, ..., r_{i_k} \in R$ e $w_1, ..., w_k \in F_X$ tal que $w = ({w_1}^{-1} r_{i_1} w_1)...({w_k}^{-1} r_{i_k} w_k)$.*

Demonstração. Seja W_X o semigrupo livre com base $X = \{x_1, ..., x_n\}$. Cada elemento de $\ll R \gg$ é a redução em F_X de um produto finito de elementos de R e seus conjugados em F_X da forma $({w_1}^{-1} r_{i_1} w_1)...({w_k}^{-1} r_{i_k} w_k)$, $w_i \in F_X$. Se consideramos, então, o subconjunto $\overline{\ll R \gg} \subset W_X$ de todos os produtos finitos (não necessariamente reduzidos) dos elementos de R e seus conjugados (em W_X) e os reduzimos um a um, estamos realizando em particular todos os elementos de $\ll R \gg$. Como W_X é enumerável (Proposição 1.17) e $\overline{\ll R \gg} \subset W_X$, $\overline{\ll R \gg}$ é enumerável. Seja $\{w_1, w_2, w_3, ...\}$ uma enumeração do mesmo. Agora, começando por w_1, depois w_2 e assim sucessivamente, reduzimos w_i (que é obviamente um processo algorítmico) e checamos se $w_i = w$. O algoritmo termina pois $w \in \ll R \gg$ e, como já dissemos, $\ll R \gg$ é inteiramente atingido pelas reduções. Desta forma, obtemos que w é algum produto w_i dos elementos de R e seus conjugados, como queríamos. □

Observação 2.10. Note que, se $w \neq 1$ em G, nunca obteríamos uma igualdade e o algoritmo nunca pararia, pois w não pertenceria a $\ll R \gg$.

Teoricamente estaríamos satisfeitos com a demonstração acima, mas vamos criar um algoritmo para solucionar o problema explicitamente. A única coisa que falta fazer é dar

um algoritmo para enumerarmos $\overline{\ll R \gg}$:

Passo 1: enumerar W_X. Temos $W_X = \cup_{k=1}^{\infty} S_k$ (vide Proposição 1.17). Como cada S_k é finito (possui nk elementos), basta então ordenar W_X colocando primeiramente os elementos de S_1, os de S_2, e assim sucessivamente. Falta então ordenarmos cada S_k. Estabelecemos, então, a ordem "alfabética" das letras da forma $\{x_1, {x_1}^{-1}, ..., x_n, {x_n}^{-1}\}$ e, a partir dela, estabelecemos a ordem lexicográfica natural em S_k, que nos dá uma enumeração para este, pois é um conjunto finito.

Passo 2: enumerar os elementos de R *e seus conjugados.* Seja $W_X = \{w_1, w_2, ...\}$ a enumeração de W_X acima. Seja $\tilde{R}$ o conjunto dos elementos de R e seus conjugados em W_X. Todos os elementos de $\tilde{R}$ podem ser listados abaixo:

$$r_1, {w_1}^{-1} r_1 w_1, {w_2}^{-1} r_1 w_2, ..., {w_n}^{-1} r_1 w_n, ...$$

$$r_2, {w_1}^{-1} r_2 w_1, {w_2}^{-1} r_2 w_2, ..., {w_n}^{-1} r_2 w_n, ...$$

$$...$$

$$r_k, {w_1}^{-1} r_k w_1, {w_2}^{-1} r_k w_2, ..., {w_n}^{-1} r_k w_n, ...$$

A partir da lista acima, criamos a enumeração considerando as colunas verticais da esquerda para a direita e, dentro de cada coluna, contando de cima para baixo.

Passo 3: enumerando $\overline{\ll R \gg}$. Vamos usar o processo de diagonalização da Teoria de Conjuntos: se $A = \{a_1, a_2, ...\}$ e $B = \{b_1, b_2, ...\}$ são conjuntos enumeráveis, procedemos na ordem da figura 2.1 para construir uma enumeração de $A \times B$ da forma

$$A \times B = \{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_1, b_3), (a_2, b_2), (a_3, b_1), ..., (a_1, b_n), (a_2, b_{n-1}), ..., (a_n, b_1), ...\}$$

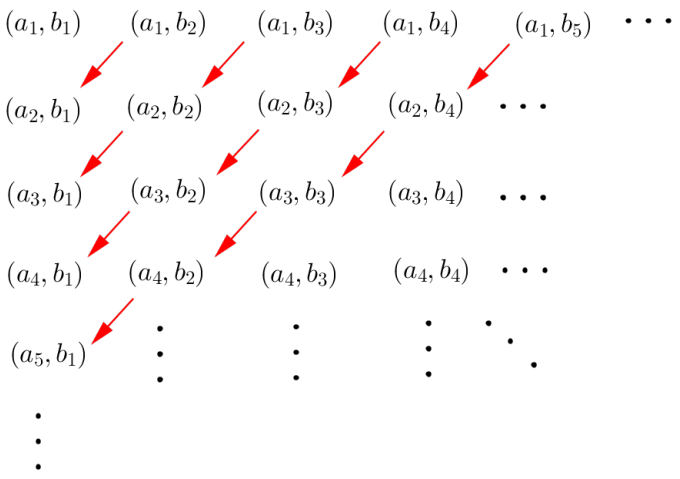


Figura 2.1: Uma enumeração para $A \times B$

Cada elemento de $\overline{\ll R \gg}$ é uma concatenação de k elementos de $\tilde{R}$. Seja então

$\{s_1, s_2, ...\}$ a enumeração de $\tilde{R}$ obtida no passo 2. Podemos pensar no conjunto das concatenações $s_i s_j$ em W_X como o produto cartesiano $\tilde{R} \times \tilde{R}$ e usar o processo de diagonalização acima para enumerá-lo. Da mesma forma, o conjunto das concatenações triplas $s_i s_j s_k$ pode ser visto recursivamente, como $(\tilde{R} \times \tilde{R}) \times \tilde{R}$. Assim, recursivamente, obtemos uma enumeração C_{k+1} das concatenações $(k+1)$-uplas a partir da enumeração anterior $C_k = \{c_k^1, c_k^2, ...\}$. Por fim, podemos alinhar todas as enumerações C_k em uma tabela infinita da forma

$$c_1^1, c_1^2, c_1^3, ..., c_1^n, ...$$

$$c_2^1, c_2^2, c_2^3, ..., c_2^n, ...$$

$$...$$

$$c_k^1, c_k^2, c_k^3, ..., c_k^n, ...$$

$$...$$

semelhante à tabela infinita da figura 2.1 e usar novamente o processo de diagonalização para criar a enumeração desejada em $\overline{\ll R \gg} = \cup_{k=1}^{\infty} C_k$.

Em resumo, o algoritmo criado acima faz o seguinte: toma uma enumeração de $\overline{\ll R \gg}$ de modo que, dada uma palavra reduzida w, realiza consecutivos testes para cada um dos elementos $\tilde{w}$ de $\overline{\ll R \gg}$, de acordo com a enumeração. Cada teste consiste em reduzir $\tilde{w}$ e comparar com w. Quando $w = 1$ em G, a igualdade eventualmente ocorre. Em caso contrário, uma igualdade jamais ocorre e o algoritmo não termina.

No Problema da Conjugação

Suponha, agora, que tenhamos duas palavras reduzidas u e v em F_X que sabemos serem conjugadas em G. Então existe $w \in G$ tal que $w^{-1}uw = v$. A pergunta é: existe algum algoritmo para calcular explicitamente w? Novamente, para a presentação finita G, a resposta é positiva.

Tomamos a enumeração de $W_X = \{w_1, w_2, ...\}$ da seção anterior. Como u e v são conjugados, sabemos (teoricamente) que existe n tal que, ao reduzirmos w_n, vale ${w_n}^{-1}uw_nv^{-1} = 1$ em G. Logo, se para cada n realizarmos os testes do algoritmo da seção anterior para a palavra ${w_n}^{-1}uw_nv^{-1}$ reduzida, algum dos algoritmos deve parar em algum momento, nos indicando qual é a palavra explícita w_n que conjuga u e v. O problema é: se escolhemos o n errado e nos concentramos apenas neste algoritmo fixado, não vamos obter resposta alguma. A solução é realizar os testes de uma forma diagonal. Denotemos por $T_i w_j$ o i-ésimo teste a ser realizado para a palavra ${w_j}^{-1}uw_jv^{-1}$, reduzida. Procedemos diagonalmente com T_1w_1, T_1w_2, T_2w_1, T_1w_3, T_2w_2 e assim sucessivamente, como na figura 2.2. Assim, realizamos todos os testes para todos os w_n e em algum momento paramos com a resposta desejada.

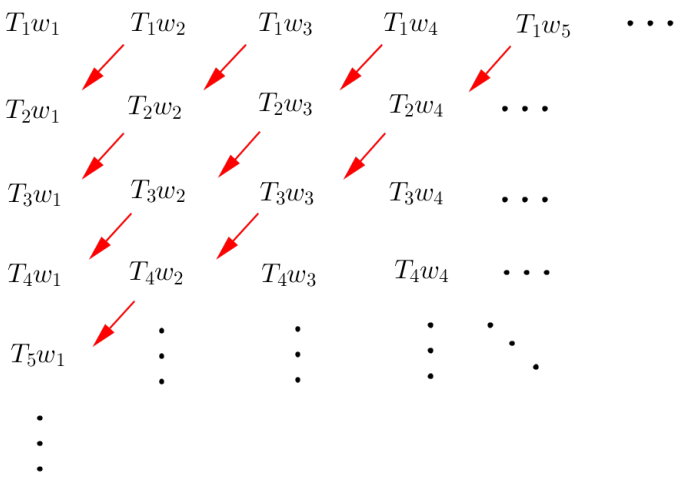


Figura 2.2: Realizando testes na diagonal

No Problema da Conjugação Torcida

Semelhantemente ao caso anterior, suponha que exista um automorfismo φ em G tais que u e v sejam φ-conjugados em G. Da mesma forma, tomando a mesma enumeração de W_X, existe n tal que $(w_n\varphi)^{-1}uw_nv^{-1} = 1$ em G. Supondo que conhecemos explicitamente φ em termos de sua ação sobre os geradores X, denotamos T_iw_j o i-ésimo teste a ser realizado (novamente com o algoritmo da proposição 2.9) para a palavra explícita $(w_j\varphi)^{-1}uw_jv^{-1}$ reduzida, e realizamos todos os testes da forma diagonal (Figura 2.2). Por hipótese, algum n-ésimo algoritmo pára com algum teste T_iw_n, nos indicando que w_n reduzida é a palavra que φ-conjuga u e v.

No Problema da Membresia

O Problema da Membresia é mais um problema de decisão na Teoria Combinatória de Grupos:

Definição 2.11 (O Problema da Membresia (PM(F,G)))**.** Seja $G = \langle X \mid R\rangle$ presentado e $F \leq G$. Dizemos que o par (F, G) tem o *Problema da Membresia* solúvel quando, dada uma palavra $w \in G$, é decidível quando $w \in F$.

Podemos propor o seguinte problema, análogo às subseções anteriores: suponha que exista $w \in G$ que sabemos pertencer a F, por algum motivo teórico. É possível, então, escrever w explicitamente como produto de elementos de F? Novamente, obtemos resposta positiva se as presentações são finitas. Suponha que $G = \langle x_1, ..., x_n \mid r_1, ..., r_k\rangle$ e que F é finitamente gerado por palavras $\tilde{f}_1, ..., \tilde{f}_s$ escritas em termos de $x_1, ..., x_n$. Seja $w \in G$ tal que $w \in F$. Então sabemos que w é a redução de um produto finito qualquer entre as $\tilde{f}_i$ e suas inversas. Considere uma enumeração $\{f_1, f_2, ...\}$ do conjunto $\overline{F}$ de tais produtos finitos (através da mesma técnica acima, usando recursivamente enumerações do produto cartesiano, etc.). Como na seção anterior, existe n tal que $w^{-1}f_n = 1$ em G. Seja T_{ij}

o i-ésimo teste (do algoritmo da Proposição 2.9) a ser realizado para a palavra $w^{-1}f_j$. Podemos realizar estes testes na diagonal, similarmente às seções anteriores; a certeza de que $w^{-1}f_n = 1$ para algum n garante novamente que algum dos algoritmos terminará em um tempo finito nos dando $w = f_j$ explicitamente.

Encontrando a raiz de uma palavra

Para esta seção, seja F um grupo livre qualquer. Vamos definir o que é a raiz de uma palavra reduzida em F e dar um algoritmo extremamente simples para calculá-la, justificando, é claro, o porquê dele funcionar. Vamos usar fortemente o conceito de palavras ciclicamente reduzidas definidas em 2.6 e a Proposição 2.7.

Definição 2.12. O *comprimento* de uma palavra (não necessariamente reduzida) w é o número de letras da palavra reduzida de w, que denotaremos por $|w|$. Note que, se $w = x_1...x_n$ já está reduzida, então $|w| = n$. Definimos também o comprimento da palavra nula, $|1| = 0$.

Proposição 2.13. *Se $1 \neq w = x_1...x_n$ é ciclicamente reduzida e é uma k-potência de $s \in F$ (ou seja, $s^k = w$ com $k \geq 1$), então $s \neq 1$ é ciclicamente reduzida e $s = x_1...x_{(n/k)}$.*

Demonstração. Seja $w = s^k$ e decomponha $w = a^{-1}\tilde{w}a$, $s = b^{-1}\tilde{s}b$, como na proposição 2.7. Da unicidade, devemos ter $a = 1$. Temos $w = s^k = (b^{-1}\tilde{s}b)^k = b^{-1}\tilde{s}^k b$, logo novamente da unicidade temos $b = 1$, ou seja, s é ciclicamente reduzido. Agora observe que quando elevamos uma palavra $s = y_1...y_r$ ciclicamente reduzida a uma potência k, como y_r e y_1 não se cancelam, o resultado final em forma reduzida é a própria concatenação $(y_1...y_r)(y_1...y_r)...(y_1...y_r)$ (k vezes). Daí $s^k = w$ implica $(y_1...y_r)(y_1...y_r)...(y_1...y_r) = x_1...x_n$, e daí $kr = n$ e $y_1 = x_1$, ... , $y_r = x_r = x_{(n/k)}$. □

Dentro da demonstração acima está o fato de que, se s é ciclicamente reduzida, então $|s^k| = k|s|$. Ela nos deixa evidente também o seguinte algoritmo:

Corolário 2.14. *Dado w ciclicamente reduzida, existe um algoritmo que calcula o maior inteiro positivo k e a palavra s tal que $s^k = w$.*

Demonstração. $|w|$ é o maior inteiro para o qual precisamos testar pois para qualquer s tal que $s^k = w$, temos $k \leq k|s| = |s^k| = |w|$. Para cada $1 \leq k \leq |w|$, então, primeiro verificamos se $|w|$ é múltiplo de k. Em caso negativo, não adianta procurarmos tal s por causa de $k|s| = |w|$. Em caso positivo, pela proposição acima basta olharmos para as $|w|/k$ primeiras letras de w (nosso candidato a s) e vermos se w é a concatenação delas, k vezes. Como o algoritmo é finito, obviamente podemos escolher o maior k e sua palavra correspondente s tal que $s^k = w$. □

Vamos definir a raiz primitiva de uma palavra reduzida de F.

Definição 2.15. Se $1 \neq w \in F$, a *raiz* de w é uma palavra $s \in F$ tal que $s^m = w$ $(m \geq 1)$ e m é o maior inteiro positivo tal que $r^m = w$ para algum $r \in F$.

Proposição 2.16. *Seja $w \neq 1 \neq s$ palavras reduzidas em F e considere suas decomposições $w = a^{-1}\tilde{w}a$ e $s = b^{-1}\tilde{s}b$, conforme a proposição 2.7. Seja $k \geq 1$. Então*

$$s^k = w \;\leftrightarrow\; \begin{cases} \tilde{s}^k = \tilde{w} \\ a = b \end{cases}$$

Demonstração. Se valem as duas igualdades da direita, então $s^k = b^{-1}\tilde{s}^k b = a^{-1}\tilde{w}a = w$. Por outro lado, se $s^k = w$, temos $b^{-1}\tilde{s}^k b = w = a^{-1}\tilde{w}a$, logo da unicidade devemos ter as duas igualdades da direita. □

Corolário 2.17. *A raiz de $w \neq 1$ existe e é única.*

Demonstração. Para a existência, considere o conjunto $A = \{k \geq 1 \mid \exists\ s \in F : s^k = w\}$. É não vazio, pois $1 \in A$. É limitado, pois para qualquer $k \in A$, decompomos $s = b^{-1}\tilde{s}b$ e temos $|s^k| = 2|b| + k|\tilde{s}|$, de modo que

$$k \leq k|\tilde{s}| + 2|b| = |s^k| = |w|.$$

Logo, pelo Axioma da Boa Ordem, existe um maior elemento m (e sua correspondente raiz s de w). Para a unicidade, suponha que existam r, s duas raizes de w. Devemos ter $s^m = w = r^m$ (o expoente m é o mesmo para r e s, pois é maximal). Decompondo novamente $s = b^{-1}\tilde{s}b$ e $r = c^{-1}\tilde{r}c$, temos $b^{-1}\tilde{s}^m b = w = c^{-1}\tilde{r}^m c$, logo $b = c$ e $\tilde{s}^m = \tilde{r}^m$ da unicidade. Como estas duas últimas palavras estão já na forma reduzida, suas $|\tilde{s}| = |\tilde{r}|$ primeiras letras coincidem duas a duas, ou seja, $\tilde{s} = \tilde{r}$. Daí é claro que $r = s$. □

Agora estamos prontos para dar um algoritmo explícito que calcule a raiz de qualquer palavra reduzida.

Proposição 2.18. *Se $w \neq 1$ em F, existe um algoritmo para calcular a raiz de w.*

Demonstração. Basta decompormos $w = a^{-1}\tilde{w}a$ e usarmos o algoritmo da Proposição 2.14 para acharmos $\tilde{s}$ com $\tilde{s}^m = \tilde{w}$ e m maximal (em relação a $\tilde{w}$). Afirmo que $a^{-1}\tilde{s}a$ é a raiz de w. De fato, é claro que $(a^{-1}\tilde{s}a)^m = a^{-1}\tilde{s}^m a = a^{-1}\tilde{w}a = w$. Provemos que m é também maximal em relação à definição de raiz. Suponha, por absurdo, que exista $r \in F$ e $M > m$ tal que $r^M = w$. Decompondo $r = c^{-1}\tilde{r}c$, teríamos $c^{-1}\tilde{r}^M c = w = a^{-1}\tilde{w}a$, logo $\tilde{r}^M = \tilde{w}$, contrariando a maximalidade de m em relação a $\tilde{w}$. □

Capítulo 3

O Problema da Conjugação em grupos livre-por-cíclicos

O Problema da Conjugação foi resolvido para qualquer grupo livre no capítulo anterior. Já o Problema da Conjugação Torcida é mais complexo. Neste capítulo, porém, estudaremos a solução encontrada em [1] para PCT em grupos livres finitamente gerados e, como consequência, uma solução para PC em qualquer grupo livre-por-cíclico. Cada um destes resultados depende fundamentalmente de um dos dois teoremas que citamos abaixo, que podem ser encontrados, respectivamente, em [13] e [5]:

Teorema 3.1 (Maslakova)**.** *Seja F um grupo livre finitamente gerado, $\varphi \in Aut(F)$ e defina $Fix(\varphi) = \{w \in F \mid w\varphi = w\} \leq F$ o* subgrupo dos pontos fixos *de φ. Então existe um algoritmo para computar um conjunto finito $\{w_1, ..., w_k\}$ que gera $Fix(\varphi)$.*

Teorema 3.2 (Brinkmann)**.** *Seja F um grupo livre finitamente gerado, $u, v \in F$ e $\varphi \in Aut(F)$. Então é decidível quando existe $k \in \mathbb{Z}$ tal que u e $v\varphi^k$ são conjugados em F.*

Eis o primeiro resultado de [1]:

Teorema 3.3. *O Problema da Conjugação Torcida é solúvel em grupos livres finitamente gerados.*

Demonstração. Seja $F = F_X$ grupo livre finitamente gerado, com $X = \{x_1, ..., x_n\}$. Seja $\varphi \in Aut(F)$ e sejam $u, v \in F$. Precisamos saber decidir se $u \sim_\varphi v$, ou seja, se u e v são φ-conjugados em F. Para isto, considere $z \notin X$ uma nova letra qualquer e tome $F' = F_{X\cup\{z\}}$ o grupo livre gerado por $\{x_1, ..., x_n, z\}$, com a letra z a mais. É claro que $F \leq F'$. Considere a função $\varphi' : X \cup \{z\} \to F'$ dada por $x_i\varphi' = x_i\varphi$ e $z\varphi' = uzu^{-1}$ e use a propriedade universal (Definição 1.13) para estender φ' ao homomorfismo $\varphi' : F' \to F'$, que é um automorfismo e obviamente coincide com φ em F, por construção. Para cada $y \in F'$, denotemos por γ_y os automorfismos de conjugação padrão em F' da forma $x\gamma_y = y^{-1}xy$ para todo $x \in F'$. É claro que a composição $\varphi'\gamma_v$ é um automorfismo de F'.

Afirmação 1: $u \sim_\varphi v$ se, e somente se, existe $g \in F$ tal que $g^{-1}zg \in Fix(\varphi'\gamma_v)$. De fato, se $u \sim_\varphi v$, temos $v = (g\varphi)^{-1}ug$ para $g \in F$ (portanto também temos $v^{-1} = g^{-1}u^{-1}g\varphi$). Daí

$$\begin{aligned}(g^{-1}zg)\varphi'\gamma_v &= (g^{-1}\varphi' z\varphi' g\varphi')\gamma_v \\ &= v^{-1}((g\varphi)^{-1}uzu^{-1}g\varphi)v \\ &= (g^{-1}u^{-1}g\varphi)((g\varphi)^{-1}uzu^{-1}g\varphi)((g\varphi)^{-1}ug) \\ &= g^{-1}zg,\end{aligned}$$

ou seja, $g^{-1}zg \in Fix(\varphi'\gamma_v)$. Por outro lado, se $g^{-1}zg \in Fix(\varphi'\gamma_v)$ para algum $g \in F$, temos

$$g^{-1}zg = (g^{-1}zg)\varphi'\gamma_v = v^{-1}((g\varphi)^{-1}uzu^{-1}g\varphi)v,$$

logo

$$z = gv^{-1}(g\varphi)^{-1}uzu^{-1}(g\varphi)vg^{-1} = (gv^{-1}(g\varphi)^{-1}u)z(gv^{-1}(g\varphi)^{-1}u)^{-1}$$

e daí

$$z^{-1}(gv^{-1}(g\varphi)^{-1}u)z(gv^{-1}(g\varphi)^{-1}u)^{-1} = 1.$$

Como a expressão inteira acima é igual a 1 no grupo livre F', todas as letras devem se cancelar de alguma maneira. Em particular, z e z^{-1} devem se cancelar. Agora note que as palavras entre parênteses acima estão ambas em F. Então a única maneira de z e z^{-1} se cancelarem é se a expressão entre eles se cancelar inteiramente. Então $gv^{-1}(g\varphi)^{-1}u = 1$ e esta expressão é equivalente a $(g\varphi)^{-1}ug = v$, ou seja, $u \sim_\varphi v$, e isto completa a demonstração da Afirmação 1 (Note que o elemento $g \in F$ procurado que conjuga u e v é o mesmo g tal que $g^{-1}zg \in Fix(\varphi'\gamma_v)$).

Afirmação 2: Existe $g \in F$ tal que $g^{-1}zg \in Fix(\varphi'\gamma_v)$ se, e somente se, existe uma palavra reduzida qualquer em $Fix(\varphi'\gamma_v)$ envolvendo a letra z. De fato, uma das implicações é óbvia. Suponha agora que exista uma palavra reduzida qualquer w em $Fix(\varphi'\gamma_v)$ contendo a letra z e vamos escrevê-la da forma reduzida $w = gz^{k_0}f_1z^{k_1}...f_rz^{k_r}$, com $g, f_i \in F,\ f_i \neq 1,\ k_0, ..., k_{r-1} \in \mathbb{Z} - \{0\},\ k_r \in \mathbb{Z}$. Dessa forma, temos:

$$\begin{aligned}gz^{k_0}f_1z^{k_1}...f_rz^{k_r} &= (gz^{k_0}f_1z^{k_1}...f_rz^{k_r})\varphi'\gamma_v \\ &= v^{-1}(g\varphi)uz^{k_0}u^{-1}(f_1\varphi)uz^{k_1}u^{-1}...(f_r\varphi)uz^{k_r}u^{-1}v\end{aligned}$$

e daí

$$z^{-k_r} {f_r}^{-1} ... z^{-k_1} {f_1}^{-1} z^{-k_0} [g^{-1}v^{-1}(g\varphi)u] z^{k_0} u^{-1}(f_1\varphi) u z^{k_1} u^{-1} ... (f_r\varphi) u z^{k_r} u^{-1} v = 1. \quad (3.1)$$

Isto quer dizer que todas as letras da palavra acima devem se cancelar de alguma forma, pois estamos em um grupo livre. Note agora que as expressões z^{k_i} à direita dos colchetes ($i = 0, ..., r$) não se cancelam entre si, pois os termos $u(f_i\varphi)u^{-1}$ entre elas estão em F e não se cancelam inteiramente. De fato, se $u(f_i\varphi)u^{-1} = 1$ teríamos $f_i\varphi = 1$ e daí $f_i = 1$ (pois φ é isomorfismo), um absurdo.

Afirmo que z^{-k_0} se cancela com z^{k_0}. De fato, z^{-k_0} não pode se cancelar com os z^{-k_i} à sua esquerda, pois a palavra w (e, portanto, também w^{-1}) já foi escrita na forma reduzida. z^{-k_0} também não pode cancelar com z^{k_1}, pois para que isto aconteça deveriamos ter $[g^{-1}v^{-1}(g\varphi)u]z^{k_0}u^{-1}(f_1\varphi)u = 1$ e daí z^{k_0} deveria se cancelar com alguma das palavras em F nesta expressão, o que jamais acontece. Por último, z^{-k_0} não pode se cancelar com nenhum dos z^{k_2},...,z^{k_r}, pois, pelo mesmo argumento que acabamos de usar, para que se cancele com algum destes z^{k_i}, a palavra z^{k_0} já deve ter se cancelado com algum dos z^{k_1},...,$z^{k_{i-1}}$, o que já provamos que não acontece no parágrafo anterior.

Da afirmação acima obtemos que toda a expressão entre colchetes em 3.1 deve se cancelar, ou seja, $g^{-1}v^{-1}(g\varphi)u = 1$ e daí $g = v^{-1}(g\varphi)u$. Isto nos dá, finalmente, que

$$(gzg^{-1})\varphi'\gamma_v = v^{-1}(g\varphi)uzu^{-1}(g\varphi)^{-1}v = gzg^{-1},$$

ou seja, $gzg^{-1} \in Fix(\varphi'\gamma_v)$. Daí, o inverso da palavra g é o elemento do enunciado da Afirmação 2 que procurávamos.

Pelas afirmações 1 e 2, decidir se $u \sim_\varphi v$ é simplesmente decidir se existe a letra z em alguma palavra de $Fix(\varphi'\gamma_v)$, o que é equivalente a decidir o mesmo para os geradores de $Fix(\varphi'\gamma_v)$. Pelo Teorema 3.1, conseguimos calcular explicitamente estes geradores, digamos, $\{w_1, ..., w_k\}$. Logo, basta olhar para cada um dos w_i e ver se algum deles contém z, o que é absolutamente decidível. □

Observação 3.4. Além de responder quando é que u e v são φ-conjugados, o teorema acima nos dá uma maneira de calcular explicitamente um elemento g que os conjuga. Pelas observações feitas nos finais das afirmações 1 e 2, se algum dos w_i contém a letra z, basta escrever w_i da forma $gz^{k_0}f_1z^{k_1}...f_rz^{k_r}$ conforme a Afirmação 2 e g^{-1} será exatamente um elemento que conjuga u e v.

Agora estamos aptos para resolver PC para grupos livre-por-cíclicos. Na verdade, quando dizemos que um grupo é livre-por-cíclico, estamos abreviando o termo, mas trataremos de um grupo (livre finitamente gerado)-por-cíclico. De acordo com a Definição 1.37, podemos reescrever:

Definição 3.5. Um grupo G é dito *livre-por-cíclico* quando possui um subgrupo livre finitamente gerado F, normal em G, e cujo quociente G/F é um grupo cíclico.

Para resolver o Problema da Conjugação em um grupo como tal, vamos encontrar uma presentação para o mesmo e, a partir dela, obteremos o resultado de uma forma relativamente simples.

Observação 3.6. Vamos obter uma decomposição única de todo elemento de G em termos de F e G/F. O fato fundamental é que, como G/F é cíclico, temos que $G/F = \langle tF \rangle$ é gerado por alguma classe lateral, com $t \in G$. Há dois casos: se G/F é cíclico infinito, temos infinitas classes laterais t^kF com $k \in \mathbb{Z}$, e se G/F é cíclico finito (digamos, $\mathbb{Z}_n$) temos apenas as classes $F, tF, ..., t^{n-1}F$ para n fixado. Dado um elemento $g \in G$, $gF \in G/F = \langle tF \rangle$, logo $gF = t^kF$ para um único k ($k \in \mathbb{Z}$ no caso infinito e $0 \leq k \leq n-1$ no caso finito). Então $g \in gF = t^kF$ e daí $g = t^kf$, para um único k e para algum $f \in F$. Na verdade, obtemos unicidade tanto de k como de f nesta decomposição, pois se $t^kf = g = t^lf'$ temos $g \in t^kF \cap t^lF$, de onde concluímos que $k = l$, e daí $t^kf = t^kf'$ implica obviamente $f = f'$. Em ambos os casos (finito ou infinito) também temos que $g = t^kf$ pertence a F se, e somente se, $k = 0$ (ou se k for um múltiplo de n, se não estivermos nos dando o trabalho de considerar o representante certo $0 \leq k \leq n-1$, no caso finito).

Agora vamos obter uma presentação para G. No caso G/F infinito (digamos, $\mathbb{Z}$), existe uma sequência exata $1 \to F \to G \to \mathbb{Z} \to 1$ e daí o final da Observação 1.41 nos garante que uma presentação para G é da forma

$$G = \left\langle x_1, ..., x_n, t \mid t^{-1}x_it = x_i\varphi,\ i = 1, ..., n \right\rangle, \tag{3.2}$$

onde φ é um automorfismo de conjugação de G. No caso G/F cíclico finito ($\mathbb{Z}_n$), a estrutura de F não se altera. Já em G/F, a única mudança é que $t^nF = F$ e portanto $t^n \in F$, digamos, $t^n = f_0$. Daí uma presentação para G é semelhante à de 3.2 acima, dada por

$$G = \left\langle x_1, ..., x_n, t \mid t^n = f_0,\ t^{-1}x_it = x_i\varphi,\ i = 1, ..., n \right\rangle. \tag{3.3}$$

Observação 3.7. Note que, neste último caso (finito), G não é o produto semidireto de F por $G/F \simeq \langle t \rangle$, pois o elemento t^n é diferente de 1 em $\langle t \rangle$ e está na interseção $F \cap \langle t \rangle$.

Precisamos do seguinte lema técnico:

Lema 3.8. *Seja G grupo, $\varphi \in Aut(G)$, $u \in G$ e $k, r \in \mathbb{Z}$. Então*

$$u\varphi^k \sim_{\varphi^r} u\varphi^{k \pm qr},$$

para todo $q \in \mathbb{Z}$.

Demonstração. Vamos fazer primeiramente o caso "+". Temos que $((u\varphi^k)\varphi^r)^{-1}(u\varphi^{k+r})u\varphi^k = u\varphi^k$, e isto quer dizer exatamente que $u\varphi^k \sim_{\varphi^r} u\varphi^{k+r}$. Para o caso "-", note que $((v\varphi^{-r})\varphi^r)^{-1}(v\varphi^{-r}\varphi^r)v\varphi^{-r} = v\varphi^{-r}$, ou seja, $v = v\varphi^{-r}\varphi^r \sim_{\varphi^r} v\varphi^{-r}$, para todo $v \in G$. Daí, para $v = u\varphi^k$ obtemos $u\varphi^k \sim_{\varphi^r} u\varphi^k\varphi^{-r} = u\varphi^{k-r}$, como queríamos.

O resultado para $q \in \mathbb{Z}$ qualquer agora segue facilmente por indução, tanto no caso "+" como no caso "-". □

Teorema 3.9. *O Problema da Conjugação é solúvel em grupos livre-por-cíclicos.*

Demonstração. Seja G um grupo livre por cíclico como na definição 3.5, que sabemos ter a presentação

$$G = \langle x_1, ..., x_n, t \mid t^n = f_0,\ t^{-1}x_i t = x_i\varphi,\ i = 1, ..., n\rangle$$

para algum automorfismo φ de G, com ou sem a relação $t^n = f_0$. Usando a decomposição única da Observação 3.6, sejam $t^r u$ e $t^s v$ dois elementos quaisquer de G, e decidamos se eles são conjugados. Conjugando $t^r u$ por um elemento qualquer $t^k g$ de G e usando que $t^{-1}xt = x\varphi$ para qualquer $x \in F$, temos

$$\begin{aligned}(t^k g)^{-1}(t^r u)(t^k g) &= g^{-1}t^{-k}t^r u t^k g \\ &= (t^r t^{-r})g^{-1}t^r t^{-k}u t^k g \\ &= t^r(t^{-r}g^{-1}t^r)t^{-k}u t^k g \\ &= t^r(g\varphi^r)^{-1}(u\varphi^k)g \in t^r F.\end{aligned}$$

Logo, temos $(t^k g)^{-1}(t^r u)(t^k g) = t^s v$ se, e somente se, $t^r(g\varphi^r)^{-1}(u\varphi^k)g = t^s v$; novamente pela unicidade de decomposição, isto acontece se, e somente se, $r = s$ e $(g\varphi^r)^{-1}(u\varphi^k)g = v$. Em outras palavras,

$$t^r u \sim t^s v \Leftrightarrow \begin{cases} r = s; \\ \text{existe } k \in \mathbb{Z} \text{ tal que } v \sim_{\varphi^r} u\varphi^k \text{ em } F. \end{cases}$$

A primeira equação $r = s$ é obviamente decidível. Precisamos decidir quando a segunda é válida. Se $r = 0$, então $\varphi^r = Id$ e precisamos saber se existe $k \in \mathbb{Z}$ tal que $v \sim u\varphi^k$ em F, o que é decidível pelo Teorema 3.2. Se $r \neq 0$, o Teorema 3.3 nos garante que podemos decidir se $v \sim_{\varphi^r} u\varphi^k$ para cada k fixado. Porém, caso tal k não exista, poderíamos ficar procurando indefinidamente sem obter uma resposta efetiva, como vimos na Observação 2.5. Precisamos reduzir nossa pergunta a um número finito de testes. Pelo Lema 3.8, temos $u\varphi^k \sim_{\varphi^r} u\varphi^{k\pm qr}$ para qualquer $q \in \mathbb{Z}$. Para todo $k \in \mathbb{Z}$, pelo algoritmo de Euclides temos $k = qr + k'$ com $0 \leq k' \leq |r| - 1$ e daí $u\varphi^k \sim_{\varphi^r} u\varphi^{k-qr} = u\varphi^{k'}$, logo, como $\sim_{\varphi^r}$ é uma relação transitiva, decidir se $v \sim_{\varphi^r} u\varphi^k$ para $k \in \mathbb{Z}$ é decidir se $v \sim_{\varphi^r} u\varphi^{k'}$ para algum dos finitos valores $0 \leq k' \leq |r| - 1$, e cada um destes $|r|$ testes é decidível pelo Teorema 3.3. □

Observação 3.10. O algoritmo acima, além de responder se os elementos $t^r u$ e $t^s v$ de G são conjugados ou não, calcula explicitamente o conjugador em caso afirmativo. De fato:

observamos na demonstração que ele será da forma $t^k g$, onde $k \in \mathbb{Z}$ e $g \in F$ são tais que $(g\varphi^r)^{-1}(u\varphi^k)g = v$. No caso $r = 0$, k e g são explicitamente encontrados pelo Teorema de Brinkmann. No caso $r \neq 0$, k é o inteiro para o qual o algoritmo do Teorema 3.3 respondeu positivamente e $g \in F$ é exatamente o elemento que φ^r-conjuga $u\varphi^k$ e v, que é explicitamente calculável, pela Observação 3.4.

Capítulo 4

O Problema da Conjugação e Decidabilidade por Órbitas

A partir da solução do Problema da Conjugação para grupos livre-por-cíclicos (encontrada no Teorema 3.9 do capítulo anterior), a ideia principal dos autores foi generalizar tal resultado para qualquer grupo livre-por-livre (rigorosamente, (livre finitamente gerado)-por-livre). Neste processo de generalização, um complexo problema de decisão veio à tona: a Decidabilidade por Órbitas. Aconteceu que, mesmo com tal impecilho, quatro anos depois de publicado o artigo [1], os autores publicaram em [2] um resultado extremamente mais geral do que o Teorema 3.9 (inclusive mais geral do que a própria ideia inicial para grupos livre-por-livres), cuja Decidabilidade por Órbitas se reduz ao Teorema de Brinkmann no caso livre-por-cíclico. O objetivo deste capítulo é demonstrar este resultado (Teorema 4.3) e mostrar suas conexões com o Teorema 3.9, justificando o porquê de ser uma generalização do mesmo. Sendo assim, recomendamos fortemente que o leitor tenha lido o capítulo anterior antes de prosseguir.

4.1 Uma conta que dá errado

A estratégia mais óbvia para tentar generalizar o Teorema 3.9 para qualquer grupo livre-por-livre seria adaptar sua demonstração. Porém, como veremos agora, encontramos problemas ao seguir a mesma ideia da prova. Vamos recapitular o que foi feito. Os grupos livre-por-cíclicos têm a presentação

$$G = \langle x_1, ..., x_n, t \mid t^{-1}x_i t = x_i\varphi,\ i = 1, ..., n \rangle,$$

onde a relação $t^n = f_0 \in F$ pode aparecer no caso cíclico finito. No caso cíclico infinito, temos exatamente a presentação descrita acima e caímos num caso particular de grupo livre-por-livre. A demonstração do Teorema 3.9 se baseia no seguinte cálculo, que já usamos:

$$\begin{aligned}(t^k g)^{-1}(t^r u)(t^k g) &= g^{-1}t^{-k}t^r u t^k g \\ &= (t^r t^{-r})g^{-1}t^r t^{-k} u t^k g \\ &= t^r (t^{-r} g^{-1} t^r) t^{-k} u t^k g \\ &= t^r (g\varphi^r)^{-1}(u\varphi^k) g.\end{aligned}$$

Em essência, usamos fortemente a comutatividade entre t^{-k} e t^r no cálculo acima, a unicidade da decomposição de elementos na forma $t^s v$ e um lema técnico para garantir que

$$t^r u \sim t^s v \Leftrightarrow \begin{cases} r = s; \\ \text{existe } 0 \leq k \leq |r| - 1 \text{ tal que } v \sim_{\varphi^r} u\varphi^k \text{ em } F \end{cases}$$

e concluir o resultado para $r \neq 0$, e usamos o Teorema de Brinkmann para $r = 0$. Se quiséssemos generalizar, poderíamos trabalhar, por exemplo, com as extensões livres

$$F \rtimes_{\varphi_1,...,\varphi_m} F_m = \left\langle X, t_1, ..., t_m \mid R, {t_i}^{-1} x t_i = x\varphi_i \ (x \in X, i = 1, ..., m) \right\rangle$$

vistas em 1.3, com F livre finitamente gerado. Neste caso, continuamos com um produto semidireto; logo, ainda temos a unicidade de decomposição: todo elemento se escreve unicamente da forma $t_{k_1}^{e_1} ... t_{k_r}^{e_r} x$, com $1 \leq k_i \leq m, k_i \neq k_{i+1}, e_i \neq 0$ e $x \in F$. O problema é que, conjugando por um elemento qualquer $t_{l_1}^{h_1} ... t_{l_s}^{h_s} y$ obtemos

$$(t_{l_1}^{h_1} ... t_{l_s}^{h_s} y)^{-1} t_{k_1}^{e_1} ... t_{k_r}^{e_r} x (t_{l_1}^{h_1} ... t_{l_s}^{h_s} y) = y^{-1} (t_{l_1}^{h_1} ... t_{l_s}^{h_s})^{-1} (t_{k_1}^{e_1} ... t_{k_r}^{e_r}) x (t_{l_1}^{h_1} ... t_{l_s}^{h_s}) y \qquad (4.1)$$

e não conseguimos fazer com que comutem as palavras $(t_{l_1}^{h_1} ... t_{l_s}^{h_s})^{-1}$ e $(t_{k_1}^{e_1} ... t_{k_r}^{e_r})$, como fizemos acima com t^{-k} e t^r. Seria preciso, então, buscar outra estratégia que permitisse o desvio destas e de outras dificuldades, como a falta de comutatividade que acabamos de ver.

4.2 O teorema central

Nesta seção, vamos enunciar e demonstrar o Teorema 4.3, generalização do Teorema 3.9 e principal resultado deste trabalho. Seu anunciado, contudo, não nos dá indício nenhum de que é uma generalização, muito menos uma ideia de como chegamos ao seu delicado contexto a partir do simples contexto dos grupos livre-por-cíclicos. Tentaremos fazer todas estas comparações e ligações durante o texto.

Na prática, a ideia do Teorema 4.3 é resolver o Problema da Conjugação para a maior quantidade possível de grupos N-por-H, as chamadas extensões de grupos, como vimos em 1.37. Segundo a Proposição 1.38, o contexto mais geral no qual podemos pensar em tratar tais grupos é o das sequências exatas. Porém, não poderíamos considerar

uma sequência exata qualquer, pois ainda estamos na Teoria Combinatória de Grupos, teoria cujos problemas de decisão envolvem processos algorítmicos. O contexto a ser trabalhado é, então, o das sequências exatas onde conseguimos computar algoritmicamente (e explicitamente) imagens e pré-imagens:

Definição 4.1. Dizemos que uma sequência exata

$$1 \to F \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$$

é *algorítmica* quando:

i) os grupos F, G e H e os homomorfismos α e β estão dados de forma que conseguimos operar explicitamente os elementos e computar explicitamente suas imagens por α e β;

ii) dado $h \in H$, podemos computar explicitamente pelo menos um elemento $g \in G$ tal que $g\beta = h$;

iii) dado $g \in G$ tal que $g\beta = 1$, podemos computar explicitamente o único elemento $f \in F$ tal que $f\alpha = g$.

De longe, o melhor exemplo de sequência exata algorítmica se dá quando os grupos F, G e H são dados por presentações e os homomorfismos α e β são dados explicitamente pelas suas imagens nos geradores de F e G, respectivamente. Desta forma, é claro que podemos operar explicitamente dentro dos grupos e que podemos calcular imagens. Além disso, considerando que as presentações envolvidas são finitas, podemos usar o algoritmo do Problema da Membresia que demos na página 23 para os pares $(Im(\beta), H)$ e $(Im(\alpha), G)$ para calcular as pré-imagens dos elementos desejados.

É fácil vermos que qualquer grupo G livre-por-cíclico se encaixa neste contexto. No caso cíclico infinito, temos a sequência exata algorítmica

$$1 \to F \xrightarrow{i} G \xrightarrow{\beta} \mathbb{Z} \to 1,$$

onde i é a inclusão $f \mapsto f$ e $(t^k f)\beta = k$. Mais geralmente, as extensões livres

$$F \rtimes_{\varphi_1,...,\varphi_m} F_m = \left\langle X, t_1, ..., t_m \mid R, {t_i}^{-1} x t_i = x\varphi_i \ (x \in X, i = 1, ..., m) \right\rangle$$

são o termo central da sequência exata algorítmica

$$1 \to F \xrightarrow{i} F \rtimes_{\varphi_1,...,\varphi_m} F_m \xrightarrow{\beta} F_m \to 1$$

onde i é a inclusão e $(t_{k_1}...t_{k_r}x)\beta = t_{k_1}...t_{k_r}$.

Dada uma sequência exata algorítmica $1 \to F \to G \to H \to 1$, o Teorema 4.3 propõe a seguinte pergunta: quais hipóteses são necessárias sobre F e H para que resolvamos o

Problema da Conjugação no grupo central G? Ao tentar respondê-la, mais problemas de decisão vêm à tona:

- **O Problema da Conjugação restrito a um subgrupo F:** seja $G = \langle X \mid R \rangle$ presentado e $F \leq G$. dados $x, y \in F$ em termos desta presentação, decidir quando são conjugados em G, ou seja, quando existe $u \in G$ tal que $x = u^{-1}yu$.
- **O Problema da Conjugação Torcida de um Automorfismo (PCT(φ)):** Seja $G = \langle X \mid R \rangle$ grupo e $\varphi \in Aut(G)$ fixados. Dados $x, y \in G$, decidir quando são φ-*conjugados* em G, ou seja, quando existe $u \in G$ tal que $x = (u\varphi)^{-1}yu$ (note que a solução de PCT(φ) para todo $\varphi \in Aut(G)$ é equivalente à solução de PCT).
- **Decidabilidade por Órbitas (DO):** seja F um grupo e $A \leq Aut(F)$. Dados $u, v \in F$, decidir se existe $\varphi \in A$ tal que $u\varphi$ e v são conjugados em F.

Quando o problema de Decidabilidade por Órbitas acima é solúvel no grupo A, dizemos que A é *decidível por órbitas*. Neste trabalho, trataremos da decidabilidade por órbitas de um subgrupo específico: o *subgrupo de ação*, que está descrito abaixo. Dada a sequência exata

$$1 \to F \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1,$$

podemos identificar F com $\alpha(F)$ e dizer que F é normal em G. Desta forma, os automorfismos de conjugação $\gamma_g \in Aut(G)$ dados por $x\gamma_g = g^{-1}xg$, quando restritos a F, se tornam automorfismos de F, pois $g^{-1}yg \in F$ se $y \in F$. Denotaremos estes automorfismos por φ_g, para cada $g \in G$.

Definição 4.2. Dada a sequência exata acima, chamamos de *subgrupo de ação* o subgrupo $A_G = \{\varphi_g \mid g \in G\} \leq Aut(F)$.

Agora temos todo o ferramental para enunciar o

Teorema 4.3. *Seja*

$$1 \to F \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$$

uma sequência exata algorítmica tal que

i) F tem PCT solúvel;

ii) H tem PC solúvel;

iii) para qualquer $1 \neq h \in H$, o grupo $C_H(h)/\langle h \rangle$ é finito e existe um algoritmo que computa representantes $z_1, ..., z_t \in C_H(h)$ (que dependem de h) tais que

$$C_H(h) = \langle h \rangle z_1 \sqcup ... \sqcup \langle h \rangle z_t.$$

Então, as seguintes condições são equivalentes:

a) G tem PC solúvel;

b) G tem PC restrito a F solúvel;

c) A_G é decidível por órbitas.

Observação 4.4. Vamos investigar novamente as semelhanças com o Teorema 3.9 e concluir daí a naturalidade das suposições *i)* a *iii)*. Primeiramente, a solução do PCT para o subgrupo normal F suposta em *i)* é exatamente o que acontece no caso livre-por-cíclicos (Teorema 3.3), onde F é livre finitamente gerado. Com relação ao item *ii)*, é claro que qualquer grupo cíclico (de fato, qualquer grupo abeliano finitamente gerado) possui PC solúvel (o que mostraremos mais à frente), mas podemos notar uma semelhança ainda mais forte com o Teorema 3.9: vimos que uma condição necessária para que os dois elementos $t^r u$ e $t^s v$ sejam conjugados é que $r = s$, ou seja, $(t^r u)\beta = (t^s v)\beta$. Logo, a primeira coisa que fazemos é calcular suas imagens por β: se não forem iguais, os elementos já não são conjugados. O leitor notará que este é exatamente o primeiro argumento na demonstração do item "*b)* $\Rightarrow$ *a)*" abaixo. Por último, a condição sobre os centralizadores que supomos em *iii)* - que provaremos ser verdadeira em qualquer grupo cíclico no Corolário 4.7 - é exatamente o que acaba com o problema da falta de comutatividade em H que comentamos no final da primeira seção deste capítulo, para $H = F_m$.

Demonstração.

- *a)* $\Rightarrow$ *b)* é claro que se podemos responder quando dois elementos de G são conjugados em G, podemos responder em particular esta pergunta para dois elementos de F.

- *b)* $\Leftrightarrow$ *c)* dados $u, v \in F$, temos a seguinte equivalência:

$$\exists\ \varphi_g \in A_G \text{ tal que } u = v\varphi_g \quad \Leftrightarrow \quad \exists\ \varphi_g \in A_G \text{ e } f \in F \text{ tal que } u = f^{-1}v\varphi_g f.$$

De fato, basta tomar $f = 1$ para a ida e usar o fato que $f^{-1}v\varphi_g f = v\varphi_{gf}$ para a volta. Assim, temos:

$$\begin{aligned} \exists\ g \in G \text{ tal que } u = g^{-1}vg \quad &\Leftrightarrow \quad \exists\ \varphi_g \in A_G \text{ tal que } u = v\varphi_g \\ &\Leftrightarrow \quad \exists\ \varphi_g \in A_G \text{ e } f \in F \text{ tal que } u = f^{-1}v\varphi_g f \\ &\Leftrightarrow \quad \exists\ \varphi_g \in A_G \text{ tal que } u \sim v\varphi_g \text{ em } F, \end{aligned}$$

e isto nos diz exatamente que o Problema da Conjugação de G restrito a F é equivalente à decidabilidade de órbitas de A_G.

- *b)* $\Rightarrow$ *a)* Suponha que o Problema da Conjugação em G, restrito a F, é solúvel, e vamos provar que é solúvel em todo G. Sejam $g, g' \in G$ e respondamos se são conjugados ou não. Calculamos $g\beta$ e $g'\beta$ e usamos PC de H para decidir se estes são conjugados ou não em H. Se não o forem, isto quer dizer que g e g' não são conjugados em G (o que resolve o problema), pois se o fossem teríamos $u^{-1}gu = g'$ e daí $(u\beta)^{-1}g\beta(u\beta) = g'\beta$. Nos resta então tratar o caso em que $g\beta$ e $g'\beta$ são conjugados, digamos, por v. Calcule u uma pré-imagem de v em G, e temos que

$$(u^{-1}gu)\beta = (u\beta)^{-1}g\beta(u\beta) = v^{-1}g\beta v = g'\beta.$$

Como a conjugação é relação de equivalência e $g \sim u^{-1}gu$, basta sabermos responder se $u^{-1}gu$ e g' são conjugados, e agora temos a vantagem que estes dois elementos são levados por β num mesmo elemento de H, pela equação acima. Por isto, para simplificar a notação vamos chamar $u^{-1}gu$ de g, supor que $g\beta = g'\beta$ e decidir se g e g' são conjugados. Se $g\beta = g'\beta = 1$, então g e g' estão em F, e isto nos permite aplicar PC de G restrito a F para responder se são conjugados. Nos resta então apenas o caso $g\beta = g'\beta \neq 1$. Neste caso, temos $(g^{-1}g')\beta = 1$ e daí $g^{-1}g' = f \in F$, ou $g' = gf$. Como $g\beta \neq 1$, use *iii)* para computar $z_1, ..., z_t$ tais que

$$C_H(g\beta) = \langle g\beta \rangle\, z_1 \sqcup ... \sqcup \langle g\beta \rangle\, z_t.$$

Compute algoritmicamente pré-imagens $y_i \in G$ dos z_i respectivos. Para todo i, $g\beta$ e $y_i\beta$ comutam, pois $y_i\beta = z_i \in C_H(g\beta)$. Daí, $(g^{-1}{y_i}^{-1}gy_i)\beta = 1$ e conseguimos computar $p_i \in F$ tal que $g^{-1}{y_i}^{-1}gy_i = p_i$, ou ${y_i}^{-1}gy_i = gp_i$. Afirmamos que

$$g \sim g' \Leftrightarrow \text{existem } 1 \leq i \leq t \text{ e } x \in F \text{ tais que } gf = x^{-1}gp_ix.$$

De fato, se existe $1 \leq i \leq t$ e $x \in F$ tais que $gf = x^{-1}gp_ix$, temos

$$g' = gf = x^{-1}gp_ix = x^{-1}{y_i}^{-1}gy_ix = (y_ix)^{-1}g(y_ix),$$

ou seja, $g \sim g'$. Por outro lado, se $g \sim g'$, tome $v \in G$ tal que $v^{-1}gv = g'$. Aplicando β à igualdade $gv = vg'$ obtemos

$$(g\beta)(v\beta) = (gv)\beta = (vg')\beta = (v\beta)(g'\beta) = (v\beta)(g\beta),$$

logo $v\beta$ está no centralizador de $g\beta$ e encontramos i tal que $v\beta \in \langle g\beta \rangle\, z_i$. Daí $v\beta = (g\beta)^r z_i = (g\beta)^r y_i\beta = (g^r y_i)\beta$. Agrupando, obtemos $(v^{-1}g^r y_i)\beta = 1$ e então existe $x^{-1} \in F$ tal que $v^{-1}g^r y_i = x^{-1}$, ou $v = g^r y_i x$. Finalmente, concluímos que

$$gf = g' = v^{-1}gv = x^{-1}{y_i}^{-1}g^{-r}gg^r y_i x = x^{-1}{y_i}^{-1}gy_ix = x^{-1}gp_ix,$$

o que conclui a demonstração da afirmação. Agora note que

$$gf = x^{-1}gp_ix \Leftrightarrow f = g^{-1}x^{-1}gp_ix \Leftrightarrow f = (x\varphi_g)^{-1}p_ix,$$

logo, pela afirmação,

$$\begin{aligned} g \sim g' &\Leftrightarrow \text{existem } 1 \leq i \leq t \text{ e } x \in F \text{ tais que } f = (x\varphi_g)^{-1}p_ix \\ &\Leftrightarrow \text{existem } 1 \leq i \leq t \text{ tal que } f \sim_{\varphi_g} p_i \text{ em } F. \end{aligned}$$

Então, decidir se g e g' são conjugados em G se resume em fazer t testes de conjugação torcida em F, o que é algoritmicamente possível por i).

□

Observação 4.5. Na demonstração $b) \Rightarrow a)$ acima, usamos PCT somente para os automorfismos $\varphi_g \in A_G$, não para qualquer automorfismo de F, e não precisamos de PCT em nenhum outro momento. Desta forma, podemos enfraquecer a hipótese i), se necessário.

Observação 4.6. Mesmo com todos os comentários da seção e também os da Observação 4.4, ainda falta justificarmos por que a Decidabilidade por Órbitas apareceu no teorema acima e qual sua relação com o Teorema 3.9. Note que ela foi usada para decidir se $g \sim g'$ apenas no caso $g, g' \in F$. Assim também o Teorema de Brinkmann (3.2) foi usado para decidir se $t^ru \sim t^sv$ apenas no caso $r = s = 0$, ou seja, se $u \sim v$ com $u, v \in F$. É natural esperarmos então que a decidabilidade de órbitas aqui tem a mesma função que o Teorema de Brinkmann teve no capítulo anterior. De fato, seja G livre-por-cíclico e tome sua sequência exata $1 \to F \to G \to H \to 1$. O subgrupo de ação, neste caso, é dado pelas conjugações φ_{t^kf} em F, para $k \in \mathbb{Z}$ e $f \in F$. Dados $u, v \in F$, temos as seguintes equivalências:

$$\begin{aligned} \exists\ \varphi_{t^kf} \in A_G \text{ tal que } u\varphi_{t^kf} \sim v \text{ em } F &\Leftrightarrow \exists\ k \in \mathbb{Z},\ f, x \in F \text{ tal que } x^{-1}(f^{-1}t^{-k})u(t^kf)x = v \\ &\Leftrightarrow \exists\ k \in \mathbb{Z},\ g \in F \text{ tal que } g^{-1}u{\varphi_t}^kg = v \\ &\Leftrightarrow \exists\ k \in \mathbb{Z} \text{ tal que } u{\varphi_t}^k \sim v \text{ em } F, \end{aligned}$$

onde basta tomar $g = fx$ da segunda para a terceira afirmação, e tomar $x = 1$ e $f = g$ da terceira para a segunda. Sendo F livre finitamente gerado e φ_t um automorfismo de F, o Teorema de Brinkmann garante que podemos decidir quando a última das afirmações é válida. Logo, A_G é decidível por órbitas, graças ao Teorema de Brinkmann, como suspeitávamos.

Como consequência da observação acima, obtemos a solução do Problema da Conjugação para grupos livre-por-cíclicos (que já vimos), o que mostra definitivamente que o Teorema 4.3 é uma generalização do 3.9:

Corolário 4.7. *O Problema da Conjugação é solúvel em grupos livre-por-cíclicos*

Demonstração. Basta verificarmos que a sequência exata $1 \to F \to G \to H \to 1$ do grupo livre-por-cíclico G satisfaz as hipóteses $i) - iii)$ do Teorema 4.3, pois A_G é decidível por órbitas, pela observação acima. Já provamos que F satisfaz PCT em 3.3. Já vimos também que PC é solúvel em grupos livres (Proposição 2.8) e em grupos finitos (Observação 2.4), logo é solúvel em qualquer grupo cíclico. Resta vermos que qualquer grupo cíclico H satisfaz $iii)$. No caso $H = \mathbb{Z}$, dado $0 \neq k \in \mathbb{Z}$ (por exemplo, $k > 0$) temos $C_{\mathbb{Z}}(k)/\langle k \rangle = \mathbb{Z}/k\mathbb{Z} \simeq \mathbb{Z}_k$ e conseguimos computar os representantes, que são $0, ..., k-1$. No caso $H = \mathbb{Z}_n$, dado $\overline{0} \neq \overline{k} \in \mathbb{Z}_n$, também temos $C_{\mathbb{Z}_n}(\overline{k}) = \mathbb{Z}_n$ e $\mathbb{Z}_n/\left\langle \overline{k} \right\rangle$ também é um grupo cíclico (por exemplo, é o grupo trivial se $mdc(k,n) = 1$ e é isomorfo a $\mathbb{Z}_\lambda$ se $n = \lambda k$), cujos representantes também encontramos explicitamente (por exemplo, $\mathbb{Z}_6/\left\langle \overline{3} \right\rangle = \overline{0}\left\langle \overline{3} \right\rangle \sqcup\ \overline{1}\left\langle \overline{3} \right\rangle \sqcup\ \overline{2}\left\langle \overline{3} \right\rangle$), o que conclui a demonstração. □

Capítulo 5

Aumentando a aplicabilidade e a praticidade do teorema central

Neste capítulo, vamos investigar as condições $i) - iii)$ do Teorema 4.3 e encontrar classes de grupos que as satisfazem, de modo a tornar mais prática a aplicação do mesmo. Com a mesma intenção, vamos, então, reescrevê-lo em termos das presentações das extensões livres apresentadas na seção 1.3. Mantenhamos sempre em mente a sequência exata algorítmica

$$1 \to F \to G \to H \to 1$$

e o fato de que a condição $i)$ é imposta sobre F e as condições $ii)$ e $iii)$ sobre H. Esta seção é baseada na seção 4 de [2].

5.1 Resolvendo i) para mais grupos F

Observação 5.1. Já sabemos que PCT é solúvel em qualquer grupo livre finitamente gerado (Teorema 3.3). O mesmo acontece para qualquer grupo G abeliano finitamente gerado. De fato, pela classificação dos grupos abelianos finitamete gerados (Teorema 2.6 em [9]), podemos escrever

$$G \simeq \mathbb{Z}^n \oplus \mathbb{Z}_{m_1} \oplus ... \oplus \mathbb{Z}_{m_k}$$

para certos inteiros positivos $n, m_1, ..., m_k$ (que podem, obviamente, nem aparecer na decomposição). Dados $u, v \in G$ e $\varphi \in Aut(G)$ e escrevendo em notação abeliana, o Problema da Conjugação Torcida se resume em encontrarmos $x \in G$ tal que

$$-x\varphi + u + x = v \Leftrightarrow \ x(Id - \varphi) = v - u,$$

ou seja, $u \sim_\varphi v \Leftrightarrow v - u \in Im(Id - \varphi)$. Agora, u e v estão dados explicitamente. Também conhecemos explicitamente o homomorfismo $Id - \varphi$ (pois conhecemos φ), logo conhecemos a forma do subgrupo $Im(Id - \varphi)$, e decidir se $v - u$ pertence a este subgrupo se torna resolver um sistema de equações diofantinas sobre $\mathbb{Z}$ e/ou sobre $\mathbb{Z}_{m_1}, ..., \mathbb{Z}_{m_k}$, o

que é sempre possível.

O que faremos agora é provar uma proposição que se assemelha a uma recíproca do Teorema 4.3, no caso $H = \mathbb{Z}$, ou seja, no caso $G = F \rtimes_\varphi \mathbb{Z}$ para algum automorfismo $\varphi = \varphi_t$ de F. Já vimos em 4.7 que as hipóteses *ii)* e *iii)* são satisfeitas por H, e sabemos que podemos exigir PCT apenas para os automorfismos $\varphi^k, k \in \mathbb{Z}$ (Observação 4.5). Também, pelas equivalências que vimos na Observação 4.6, a Decidabilidade por Órbitas de A_G é equivalente à de $\langle\varphi\rangle$. Assim, o Teorema 4.3 nos diz que a solução de PCT para qualquer φ^k e a Decidabilidade por Órbitas em $\langle\varphi\rangle$ implica a solução de PC em $F \rtimes_\varphi \mathbb{Z}$. Em resumo:

$$\text{PCT para qualquer } \varphi^k, k \in \mathbb{Z} \ + \ \text{DO para } \langle\varphi\rangle \ \Rightarrow \ \text{PC para } F \rtimes_\varphi \mathbb{Z}.$$

A proposição a seguir demonstra o seguinte fato:

$$\text{PC para } F \rtimes_\varphi \mathbb{Z} \ \Rightarrow \ \text{PCT para } \varphi + \text{DO para } \langle\varphi\rangle\,.$$

Proposição 5.2. *Seja $F = \langle X \mid R\rangle$ grupo finitamente presentado e $\varphi \in Aut(F)$ dado de forma algorítmica. Se PC é solúvel em $F \rtimes_\varphi \mathbb{Z}$ então PCT(φ) é solúvel em F e $\langle\varphi\rangle$ é decidível por órbitas.*

Demonstração. Sendo PC solúvel em $F \rtimes_\varphi \mathbb{Z}$, também o é restrito ao subgrupo F. Mas vimos na demonstração do Teorema 4.3 que isto é equivalente à Decidabilidade por Órbitas de A_G, que por sua vez é equivalente à de $\langle\varphi\rangle$, como vimos logo antes desta proposição. Logo, $\langle\varphi\rangle$ é decidível por órbitas. Vamos resolver agora PCT(φ) em F. Sejam $u, v \in F$ e recordemos que temos a presentação

$$F \rtimes_\varphi \mathbb{Z} = \left\langle X, t \mid R,\ t^{-1}xt = x\varphi,\ x \in X \right\rangle.$$

Por um lado, dado $x \in F$, temos $(x\varphi)^{-1}ux = v \Leftrightarrow x^{-1}(tu)x = tv$ (basta multiplicar por t na ida e por t^{-1} na volta, e usar a relação $t^{-1}xt = x\varphi$). Logo, $u \sim_\varphi v$ se, e somente se, tu e tv são conjugados em $F \rtimes_\varphi \mathbb{Z}$ por algum elemento de F. Guardemos esta informação. Por outro lado, a hipótese garante que podemos decidir quando tu e tv são conjugados em $F \rtimes_\varphi \mathbb{Z}$ por um elemento arbitrário da forma $t^k x$. Mas

$$(t^k x)^{-1}(tu)(t^k x) = x^{-1}t^{-k}tut^k x = x^{-1}t(u\varphi^k)x,$$

logo tu e tv são conjugados em $F \rtimes_\varphi \mathbb{Z}$ se, e somente se, $x^{-1}t(u\varphi^k)x = tv$, ou seja, se, e somente se, para algum inteiro k, $t(u\varphi^k)$ e tv são conjugados em $F \rtimes_\varphi \mathbb{Z}$ por um elemento de F, o que é equivalente a dizer, pela informação guardada, que $u\varphi^k \sim_\varphi v$ para algum inteiro k. Isto é, então, o que podemos decidir. Mas $u\varphi^k \sim_\varphi u$, pelo Lema 3.8, logo decidir se $u\varphi^k \sim_\varphi v$ é equivalente a decidir se $u \sim_\varphi v$, que era o que queríamos. □

Corolário 5.3. *Seja $F = \langle X \mid R \rangle$ finitamente presentado. Então todas as extensões cíclicas $F \rtimes_\varphi \mathbb{Z}$ têm PC solúvel se, e somente se, F tem PCT solúvel e todos os subgrupos cíclicos de $Aut(F)$ são decidíveis por órbitas.*

Demonstração. Para a ida, note que a proposição acima demonstrou que

$$\text{PC para } F \rtimes_\varphi \mathbb{Z} \;\Rightarrow\; \text{PCT para } \varphi + \text{DO para } \langle\varphi\rangle\,,$$

para um automorfismo fixado φ. Logo, vale

$$\text{PC para qualquer } F \rtimes_\varphi \mathbb{Z} \;\Rightarrow\; \text{PCT para qualquer } \varphi + \text{DO para qualquer } \langle\varphi\rangle\,,$$

que é exatamente o que queremos. Para a volta, basta lembrar de novo que, para qualquer $\varphi \in Aut(F)$, DO de $\langle\varphi\rangle$ é equivalente à DO do subgrupo de ação $A_{F\rtimes_\varphi\mathbb{Z}}$ da sequência exata $1 \to F \to F \rtimes_\varphi \mathbb{Z} \to \mathbb{Z} \to 1$. Logo, se vale PCT para F e DO para qualquer $\langle\varphi\rangle$, basta aplicar o Teorema 4.3 a esta sequência e obtemos PC para qualquer $F \rtimes_\varphi \mathbb{Z}$. □

Graças ao corolário acima, podemos resolver o Problema da Conjugação Torcida para duas classes de grupos: os grupos fundamentais de superfícies fechadas (vamos assumir que o leitor conheça os conceitos básicos de variedades e de grupo fundamental) e os grupos policíclicos.

Corolário 5.4. *Seja F o grupo fundamental de uma superfície S fechada (conexa, compacta e sem bordo), que dizemos ser um* grupo de superfície. *Então PCT é solúvel em F e todos os subgrupos cíclicos de $Aut(F)$ são decidíveis por órbitas.*

Demonstração. Dado um automorfismo φ de F, é um fato conhecido da Topologia que o grupo $F \rtimes_\varphi \mathbb{Z}$ é o grupo fundamental de alguma variedade fibrada sobre S^1 (uma variedade de dimensão 3 que obtemos tomando o cartesiano $S \times [0,1]$ e fazendo as identificações $(x,0) \sim (x\tilde{\varphi},1)$, para algum homeomorfismo $\tilde{\varphi} : S \to S$, que depende de φ). Pelos artigos [14] e [15], $F \rtimes_\varphi \mathbb{Z}$ tem então PC solúvel. Logo, a tese é consequência imediata do Corolário 5.3. □

Definição 5.5. Um grupo G é dito *policíclico* quando existe uma sequência finita de subgrupos

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_n = 1,$$

sendo cada H_{i+1} normal em H_i e cada quociente H_i/H_{i+1} cíclico. No caso em que todos os quocientes são cíclicos infinitos, dizemos que G é *poli-$\mathbb{Z}$*

Corolário 5.6. *Seja F um grupo policíclico. Então PCT é solúvel em F e todos os subgrupos cíclicos de $Aut(F)$ são decidíveis por órbitas.*

Demonstração. Seja $F = H_0 \rhd H_1 \rhd \ldots \rhd H_n = 1$ a sequência dada pela definição 5.5. Dado um automorfismo φ de F, temos que $F \rtimes_\varphi \mathbb{Z}$ é também policíclico graças à sequência

$F \rtimes_\varphi \mathbb{Z} \rhd F \rhd H_1 \rhd ... \rhd H_n = 1$, pois F é normal em $F \rtimes_\varphi \mathbb{Z}$ e o quociente $(F \rtimes_\varphi \mathbb{Z})/F$ é isomorfo a $\mathbb{Z}$, cíclico. Agora, o Problema da Conjugação já foi resolvido para grupos policíclicos em [16], logo PC é solúvel em $F \rtimes_\varphi \mathbb{Z}$. O resultado segue então do Corolário 5.3. □

Antes de continuar, vamos provar que as propriedades "policíclico" e "grupo de superfície" passam para subgrupos.

Proposição 5.7. *Seja G policíclico e $K \leq G$. Então K é policíclico. Se G é poli-$\mathbb{Z}$, então K também é poli-$\mathbb{Z}$.*

Demonstração. Seja

$$G = H_0 \rhd H_1 \rhd ... \rhd H_n = 1,$$

a cadeia de subgrupos da definição 5.5. Fazendo a interseção de cada termo com K, obtemos a seguinte cadeia de subgrupos:

$$K = (H_0 \cap K) \rhd (H_1 \cap K) \rhd ... \rhd (H_n \cap K) = 1.$$

Para ver que cada $H_{i+1} \cap K$ é normal em $H_i \cap K$, seja $n \in H_{i+1} \cap K$ e $g \in H_i \cap K$. Temos que $g^{-1}ng$ pertence obviamente a K, e por ser H_{i+1} normal em H_i, $g^{-1}ng$ também pertence a H_{i+1}, pertencendo portanto a $H_{i+1} \cap K$, como queríamos. Para ver que cada quociente $(H_i \cap K)/(H_{i+1} \cap K)$ é cíclico, veja que $H_i \cap K$ e H_{i+1} são dois subgrupos de H_i, o segundo deles sendo normal em H_i. Logo, usando o Teorema 1.12,

$$\frac{H_i \cap K}{H_{i+1} \cap K} = \frac{H_i \cap K}{H_{i+1} \cap (H_i \cap K)} \simeq \frac{H_{i+1}(H_i \cap K)}{H_{i+1}} \leq \frac{H_i}{H_{i+1}},$$

e este último é um grupo cíclico por hipótese. Como todo subgrupo de grupo cíclico é cíclico, concluímos o resultado. A demonstração do caso poli-$\mathbb{Z}$ é exatamente a mesma, usando que todo subgrupo de $\mathbb{Z}$ é trivial ou isomorfo a $\mathbb{Z}$, e no caso em que for trivial, retirando um dos fatores repetidos da sequência de subgrupos acima. □

Assumindo conhecimentos básicos sobre topologia, recobrimentos e variedades, podemos fazer algo análogo para grupos de superfície:

Proposição 5.8. *Seja F um grupo de superfície, isto é, o grupo fundamental de uma superfície S fechada (conexa, compacta e sem bordo), e seja $K \leq F$ um subgrupo de índice finito. Então K é um grupo de superfície.*

Demonstração. Dado que S é conexo, localmente conexo por caminhos e semilocalmente simplesmente conexo, sabemos que, dado o subgrupo K, existe um espaço topológico conexo $\tilde{S}$ cujo grupo fundamental é isomorfo a K e uma aplicação de recobrimento $p : \tilde{S} \to S$ (veja [8]). Como tal aplicação é um homeomorfismo local, $\tilde{S}$ também é uma superfície sem bordo. Sabemos também da teoria de recobrimentos que o número de folhas de p

é igual ao índice de K em F, que é finito por hipótese. Logo, sendo p um recobrimento de finitas folhas e S compacto, temos que $\tilde{S}$ é compacto, logo é uma superfície fechada e $K = \pi_1(\tilde{S})$ é grupo de superfície, como queríamos. □

Compilando os resultados até aqui, já resolvemos PCT para grupos livres finitamente gerados, abelianos finitamente gerados e para grupos de superfície e policíclicos. Agora, nossa intenção é estender este ambiente de solubilidade do PCT para grupos que tenham um subgrupo de índice finito com estas propriedades.

Definição 5.9. Seja P uma certa classe de grupos. Dizemos que um grupo G é *virtualmente-P* quando G possui um subgrupo de índice finito H que pertence à classe P. Quando P é a classe dos grupos de superfície, ou abelianos, ou livres, ou policíclicos, dizemos que G é, respectivamente, *virtualmente de superfície*, ou *virtualmente abeliano*, ou *virtualmente livre*, ou *virtualmente policíclico*.

O primeiro resultado na direção da extensão que faremos já é por si só uma ótima notícia, pois nos permite estender PCT de um subgrupo *característico* (isto é, invariante por automorfismos) de índice finito para o grupo inteiro. Para isto, precisamos assumir o teorema seguinte, encontrado em [10]:

Teorema 5.10 (Algoritmo de Todd-Coxeter)**.** *Seja $F = \langle X \mid R\rangle$ finitamente presentado e $K = \langle w_1, ..., w_r\rangle \leq F$ subgrupo finitamente gerado de índice finito. Então existe um algoritmo que computa representantes $1 = y_0, y_1, ..., y_s \in F$ tais que*

$$F = K \sqcup y_1K \sqcup ... \sqcup y_sK$$

e que permite decidir a qual destas classes laterais pertence w_jy_i, para qualquer i, j. Ainda mais, é possível escrever algoritmicamente qualquer $g \in F$ da forma y_pk para algum $0 \leq p \leq s$ e algum $k \in K$, escrito em termos dos w_j. Em particular, o Problema da Membresia PM(K,F) é solúvel.

Proposição 5.11. *Seja $F = \langle X \mid R\rangle$ finitamente presentado e $K = \langle w_1, ..., w_r\rangle \leq F$ um subgrupo finitamente gerado de índice finito. Então*

1) *Se K é característico em F e PCT é solúvel em K, então PCT é solúvel em todo F;*

2) *Se K é normal em F e PCT é solúvel em K, então PC é solúvel em todo F.*

Demonstração. 1) Use o Algoritmo de Todd-Coxeter acima e compute $1 = y_0, y_1, ..., y_s \in F$ tais que $F = K \sqcup y_1K \sqcup ... \sqcup y_sK$, antes de tudo. Agora, sejam $u, v \in F$ e $\varphi \in Aut(F)$, e use o algoritmo acima novamente para escrever $u = y_iz$ e $v = y_jz'$ para $0 \leq i, j \leq s$ e $z, z' \in K$. Agora, φ-conjugando y_iz por um elemento qualquer y_lk^{-1} obtemos

$$((y_lk^{-1})\varphi)^{-1}(y_iz)(y_lk^{-1}) = (ky_l^{-1})\varphi(y_iz)(y_lk^{-1}) = (k\varphi)(y_l\varphi)^{-1}y_izy_lk^{-1}.$$

Igualando com $y_j z'$ temos

$$(k\varphi)(y_l\varphi)^{-1}y_i z y_l k^{-1} = y_j z' \Leftrightarrow (y_l\varphi)^{-1}y_i z y_l = (k\varphi)^{-1}y_j z' k = y_j[{y_j}^{-1}(k\varphi)^{-1}y_j z' k].$$

Logo,

$$\begin{aligned} u \sim_\varphi v &\Leftrightarrow \text{existe } 0 \leq l \leq s \text{ e } k \in K \text{ tais que } ((y_l k^{-1})\varphi)^{-1}(y_i z)(y_l k^{-1}) = y_j z' \\ &\Leftrightarrow \text{existe } 0 \leq l \leq s \text{ e } k \in K \text{ tais que } (y_l\varphi)^{-1}y_i z y_l = y_j[{y_j}^{-1}(k\varphi)^{-1}y_j z' k]. \end{aligned}$$

Como K é característico, todo o termo entre colchetes acima está em K, logo toda a palavra à direita da igualdade está em $y_j K$. Uma condição necessária, então, para $u = y_i z$ e $v = y_j z'$ serem φ-conjugados é que $(y_l\varphi)^{-1}y_i z y_l$ pertença a $y_j K$ para algum $0 \leq l \leq s$, e isto podemos verificar: para cada tal l, compute explicitamente a palavra $(y_l\varphi)^{-1}y_i z y_l$ e a escreva (usando o algoritmo de Todd-Coxeter) da forma $y_r k'$, para ver se $r = j$. Se isto não acontecer para nenhum dos l então u e v não são φ-conjugados. Caso aconteça para alguns índices l, então encontramos para cada um deles um $k_l \in K$ tal que $(y_l\varphi)^{-1}y_i z y_l = y_j k_l$, e estes índices l são então os únicos candidatos possíveis para que algum elemento $y_l k^{-1}$ φ-conjugue u e v. Para dizer se $u \sim_\varphi v$, então, resta decidir se para algum destes índices existe $k \in K$ tal que $k_l = {y_j}^{-1}(k\varphi)^{-1}y_j z' k = (k\varphi\gamma_{y_j})^{-1}z' k$, o que é exatamente decidir se k_l e z' são $\varphi\gamma_{y_j}$-conjugados em K (o que faz sentido porque φ e γ_{y_j} se restringem a automorfismos de K), e cada um destes finitos testes é decidível por hipótese.

2) A demonstração e o algoritmo deste item são exatamente os mesmos do item anterior, substituindo φ por Id_F e usando que K é normal para garantir novamente que o termo entre colchetes que apareceu no item acima está em K.

□

Agora, precisamos de um lema que encontre, dentro de um certo subgrupo de um grupo F, um subgrupo característico de índice finito, para podermos usar a proposição anterior 5.11 no teorema seguinte. A demonstração deste lema (Lema 4.6 em [2]) passa por técnicas geométricas envolvendo grafos e técnicas de pullback, que fogem completamente do objetivo deste trabalho.

Lema 5.12. *Seja $F = \langle X \mid R\rangle$ finitamente presentado e $K = \langle w_1, ..., w_r\rangle \leq F$ um subgrupo finitamente gerado de índice finito. Então existe um subgrupo característico finitamente gerado $K_0 \leq F$ de índice finito, contido em K, e cujos geradores são explicitamente computáveis.*

Lema 5.13. *Dada uma presentação finita $P = \langle Y \mid S\rangle = \langle y_1, ..., y_n \mid s_1, ..., s_k\rangle$, existe um número enumerável de presentações que podemos obter explicitamente a partir de P aplicando um número finito de transformações de Tietze.*

Demonstração. Reveja os quatro tipos de transformações de Tietze que definimos logo depois da observação 1.23. Existe um número enumerável de transformações de Tietze que podemos aplicar a P: podemos escolher qualquer palavra no fecho normal de S (que é enumerável) e adicioná-la ao conjunto de relações; inversamente, podemos retirar uma relação que esteja no fecho normal das outras (nesse caso temos apenas k escolhas no máximo, e pode ser que nenhuma delas seja possível). Também, podemos adicionar um novo gerador qualquer t e escolher uma palavra w nas letras de X para adicionar $t^{-1}w$ às relações (novamente, enumeráveis escolhas); inversamente, podemos excluir um gerador que já esteja escrito em função dos outros em alguma das relações (no máximo n escolhas, talvez nenhuma sendo possível). Enumere todas estas transformações e as denote por $T_1, T_2, ...$, e denotemos por T_iP a presentação obtida aplicando T_i em P, e recursivamente denotemos por T_jT_iP, $T_kT_jT_iP$, etc, as iteradas naturais.

Agora, toda presentação obtida a partir de P através de um número finito de transformações de Tietze é da forma $T_{k_n}...T_{k_1}P$ para algum n. Seja B a coleção de todas estas presentações, e seja A o conjunto (enumerável) de todos os vetores de finitas coordenadas com entradas inteiras positivas. Então é claro que a função

$$f : A \to B, \quad f(k_1, ..., k_n) = T_{k_n}...T_{k_1}P$$

é sobrejetora, de onde concluímos o resultado. □

Agora, obtemos o resultado de extensão esperado:

Teorema 5.14. *Seja $F = \langle X \mid R \rangle$ finitamente presentado. Se F é*

1) virtualmente abeliano, ou

2) virtualmente livre, ou

3) virtualmente grupo de superfície, ou

4) virtualmente policíclico,

então PCT é solúvel em F.

Demonstração. A estratégia de demonstração para cada um dos quatro casos é a mesma; por isto, vamos fazer todas de uma vez, destacando as diferenças quando necessário. Sabemos que F possui um subgrupo K de índice finito que é abeliano, ou livre, ou grupo de superfície, ou policíclico (neste último caso, pela Proposição 2 do Capítulo 1 de [17] sabemos que todo grupo policíclico é virtualmente poli-$\mathbb{Z}$; logo, tomando novamente um subgrupo poli-$\mathbb{Z}$ de índice finito de K e o chamando de K, podemos supor que K é poli-$\mathbb{Z}$). É uma consequência do Teorema de Reidemeister-Schreier (que é a Proposição 4.1 em [11]) que qualquer subgrupo de índice finito de um grupo finitamente gerado é também

finitamente gerado ([12], p.90). Logo, como F é finitamente gerado (por ser finitamente presentado), K também o é.

A estratégia será construir um algoritmo que calcule explicitamente uma presentação finita *canônica* $\langle Y \mid S\rangle$ para K (mais adiante definiremos "presentação canônica"). Uma vez obtida tal presentação, conhecemos explicitamente um conjunto de geradores $\{w_1, ..., w_r\}$ para K, o que nos permite usar o Lema 5.12 para computar geradores $x_1, ..., x_c$ para o subgrupo $K_0 \leq K$ que é característico e de índice finito em F. Logo, se PCT for solúvel em K_0, pela Proposição 5.11 será solúvel em todo F, que é o que queremos. Para garantir que PCT é solúvel em K_0, note que K é abeliano, ou livre, ou grupo de superfície, ou poli-$\mathbb{Z}$, e que todas estas propriedades se passam de K para K_0 (a primeira trivialmente, a segunda pelo Teorema de Nielsen-Schreier (1.19), a terceira por 5.8 (e usando que K_0 tem índice finito em K, pois $|F : K_0| = |F : K||K : K_0|$ e os dois primeiros índices são finitos) e a quarta por 5.7). Logo, K_0 é abeliano finitamente gerado, ou livre finitamente gerado, ou grupo de superfície, ou policíclico, e PCT já foi resolvido para estes casos (respectivamente, em 5.1, 3.3, 5.4 e 5.6).

Vamos definir o que é uma presentação canônica para K. Diremos, nos três primeiros casos, que uma presentação finita $\langle Y \mid S\rangle$ para K é *canônica* quando o conjunto de relações, respectivamente, contém todos os comutadores, ou é vazio, ou é apenas uma palavra (do tipo encontrado nos grupos fundamentais de superfícies fechadas). No caso poli-$\mathbb{Z}$, tomando a sequência $K = H_0 \rhd H_1 \rhd ... \rhd H_n = 1$, sabemos que K é a extensão de H_1 por $\mathbb{Z}$, que por sua vez é a extensão de H_2 por $\mathbb{Z}$, e assim por diante. Logo, denotando por $EC(\langle z_1, ..., z_n \mid T\rangle) = \langle z_1, ..., z_n, t \mid T, t^{-1}z_it = z_i\varphi,\ 1 \leq i \leq n\rangle$ a extensão cíclica em $\mathbb{Z}$ por algum automorfismo φ de uma presentação $\langle z_1, ..., z_n \mid T\rangle$, sabemos que K possui uma presentação

$$K = EC(EC(...EC(\langle x \mid \emptyset\rangle)...)),$$

que chamaremos de canônica. Note que precisamos obter uma presentação canônica para K (e não uma qualquer), pois os algoritmos que demos para resolver PCT não foram construídos com base apenas no fato teórico de que os grupos são abelianos, livres, etc., mas com base em uma presentação explícita que reflita estas propriedades (veja, por exemplo, no Teorema 3.3, onde tomamos a presentação explícita $F = \langle x_1, ..., x_n \mid \emptyset\rangle$ e construímos todo o algoritmo a partir dela). Note também que, por hipótese, K possui uma presentação canônica, mas precisamos encontrar uma explicitamente.

Agora vamos construir o algoritmo: dentro da demonstração do Lema 5.12, garante-se que podemos montar uma lista enumerável $K_1, K_2, K_3, ...$ de todos os subgrupos de índice finito de F (portanto, K é um deles) e computar algoritmicamente cada um deles, como conjunto. Para todo i, é possível, então, computar K_i e usar o Teorema de Reidemeister-Schreier para computar uma presentação $P_i = \langle Y_i \mid S_i\rangle$ para K_i. Pelo Lema 5.13, existe um número enumerável de presentações que podemos obter a partir de P_i aplicando um número finito de transformações de Tietze, que vamos denotar por $\{T_1P_i, T_2P_i, T_3P_i, ...\}$,

todas algoritmicamente calculáveis. O algoritmo é fazer as seguintes computações: primeiramente P_1, depois T_1P_1, P_2, e assim sucessivamente, conforme a Figura 5.1. Pelo Teorema 1.24, a presentação canônica procurada para K que sabemos existir é alguma das T_jP_i, logo o algoritmo pára no momento em que reconhecemos a canonicidade de T_jP_i.

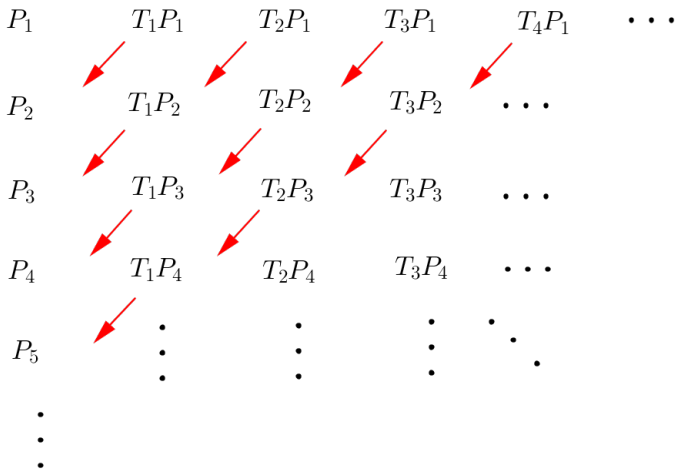


Figura 5.1: Calculando as presentações na diagonal

□

5.2 Resolvendo ii) e iii) para mais grupos H

Com relação às condições *ii*) e *iii*) do Teorema 4.3, é suficiente para o restante do trabalho provar que qualquer grupo livre as satisfazem. Logo depois, exibiremos alguns grupos hiperbólicos que também podem ser usados na posição de H.

Já sabemos que qualquer grupo livre satisfaz a condição *ii*) (Proposição 2.8). Vamos resolver agora a condição *iii*):

Proposição 5.15. *Seja F um grupo livre e $1 \neq w \in F$. Então o grupo $C_F(w)/\langle w\rangle$ é finito e existe um algoritmo que computa representantes $z_1, ..., z_t \in C_F(w)$ (que dependem de w) tais que*

$$C_F(w) = \langle w\rangle\, z_1 \sqcup ... \sqcup \langle w\rangle\, z_t.$$

Demonstração. Seja s a raiz de w, que podemos encontrar explicitamente pelo algoritmo da Proposição 2.18, e seja m o inteiro maximal da Definição 2.15, tal que $s^m = w$. Afirmo que $C_F(w) = \langle s\rangle$. É claro que $\langle s\rangle \subset C_F(w)$, pois toda potência de s comuta com $w = s^m$, outra potência de s. Vamos provar agora a igualdade. Pelo Teorema de Nielsen-Schreier, $C_F(w) \leq F$ é um grupo livre. Pela Proposição 2.18 em [11], a relação de comutatividade ($a \sim b \Leftrightarrow ab = ba$) em um grupo livre é de equivalência. Assim, se $x, y \in C_F(w)$, por definição x e y comutam com w, logo comutam entre si, de modo que

$C_F(w)$ é abeliano. Mas todo grupo livre e abeliano tem que ser cíclico (Observação 1.16). Escreva $C_F(w) = \langle h \rangle$ para algum $h \in F$ e, como $s \in \langle s \rangle \subset C_F(w)$, escreva $s = h^k$ para algum $k \in \mathbb{Z}$. Resta apenas provar que $k = 1$. Temos $k \neq 0$ (pois $s \neq 1$), e podemos supor $k > 0$, trocando h por h^{-1} se necessário (já que $\langle h \rangle = \langle h^{-1} \rangle$). Isto nos dá

$$w = s^m = (h^k)^m = h^{km},$$

com $km \geq 1$. Pela maximalidade de m, temos $km \leq m$ e portanto $k \leq 1$. Como $k > 0$, concluímos que $k = 1$, o que prova a afirmação.

Agora, temos o quociente

$$\frac{C_F(w)}{\langle w \rangle} = \frac{\langle s \rangle}{\langle s^m \rangle},$$

e acontece exatamente como no quociente $\mathbb{Z}/m\mathbb{Z}$:

$$C_F(w) = \langle w \rangle \sqcup \langle w \rangle\, s \sqcup ... \sqcup \langle w \rangle\, s^{m-1};$$

ou seja, os representantes das classes laterais são computáveis, como queríamos. □

Para finalizar a seção, vamos apenas citar e exibir o mesmo resultado acima para alguns grupos hiperbólicos. Esta é uma classe deveras recente de grupos, amplamente estudada nos últimos anos, desenvolvida primeiramente pelo matemático russo Mikhail Leonidovich Gromov, em 1987 (veja [7]). Não vamos aqui desenvolver o conceito preciso de grupo hiperbólico, pois tem motivação geométrica e utiliza grafos de Cayley, que fogem do nosso objetivo. A questão é que o Problema da Conjugação já foi resolvido para estes grupos (vide [4]). Agora, com argumentos geométricos, os autores em [2] criam os seguintes algoritmos:

Proposição 5.16. *Seja H um grupo hiperbólico finitamente presentado, e $h \in H$.*

1) *Existe um algoritmo que determina quando o centralizador $C_H(h)$ é finito ou não e computa todos os seus elementos, em caso positivo.*

2) *Se h tem ordem infinita em H (isto é, $h^n = 1 \Leftrightarrow n = 0$), então $\langle h \rangle$ tem índice finito em $C_H(h)$ e existe um algoritmo que computa $z_1, ..., z_t$ tais que*

$$C_H(h) = \langle h \rangle\, z_1 \sqcup \langle h \rangle\, z_2 \sqcup ... \sqcup \langle h \rangle\, z_t.$$

Com o algoritmo acima, fica fácil garantir que certos grupos hiperbólicos satisfazem a condição *iii*).

Proposição 5.17. *Seja H um grupo hiperbólico finitamente presentado tal que todo elemento $1 \neq h \in H$ de ordem finita ($h^n = 1$ para algum $n \geq 2$) possui centralizador finito.*

Então, para todo $1 \neq h \in H$, $\langle h \rangle$ *tem índice finito em* $C_H(h)$ *e existe um algoritmo que computa* $z_1, ..., z_t$ *tais que*

$$C_H(h) = \langle h \rangle z_1 \sqcup \langle h \rangle z_2 \sqcup ... \sqcup \langle h \rangle z_t.$$

Demonstração. Seja $1 \neq h \in H$. Use o algoritmo 1) em 5.16 para determinar se $C_H(h)$ é finito. Se não o for, pela hipótese temos que h tem ordem infinita em H e o algoritmo 2) da mesma proposição calcula os finitos representantes das classes laterais de $\langle h \rangle$ em $C_H(h)$, que é o que queremos. No caso de $C_H(h)$ ser finito, o algoritmo 1) computa explicitamente seus elementos, digamos, $C_H(h) = \{1 = a_0, a_1, ..., a_k\}$. Como PC é solúvel em H, em particular é solúvel o Problema da Palavra. Isto nos permite saber operar explicitamente no subgrupo $C_H(h)$: dados dois elementos a_i, a_j, tomamos a palavra $a_i a_j$ e usamos PP para compará-la com cada um dos $a_r, 0 \leq r \leq k$, até encontrarmos uma igualdade. Conhecendo $C_H(h)$ perfeitamente (seus elementos e sua operação), calculamos explicitamente cada classe lateral $\langle h \rangle a_r$ (em ordem crescente de r, por exemplo) até que cubramos todo $C_H(h)$ e obtenhamos uma lista de representantes laterais, como queríamos. □

5.3 Consequências

A partir dos resultados que provamos neste capítulo, obtemos algumas consequências quase que imediatas do Teorema 4.3 que o deixam com um aspecto muito mais prático. Primeiramente, agrupando o Teorema 5.14 e a Proposição 5.17, obtemos o

Corolário 5.18. *Seja*

$$1 \to F \to G \to H \to 1$$

uma sequência exata algorítmica com F *finitamente presentado e virtualmente abeliano, ou virtualmente livre, ou virtualmente grupo de superfície, ou virtualmente policíclico, e* H *hiperbólico finitamente presentado tal que todo elemento* $h \neq 1$ *de ordem finita (*$h^n = 1$ *para algum* $n \geq 2$*) possui centralizador finito. Então,* G *tem PC solúvel se, e somente se,* A_G *é decidível por órbitas.*

Demonstração. Pelo Teorema 5.14, F satisfaz i). Ainda, H satisfaz ii) (vide [4]) e iii), pela Proposição 5.17. Logo, basta aplicar o Teorema 4.3. □

Exatamente como acabamos de fazer, mas usando a Proposição 5.15 ao invés da 5.17, obtemos o seguinte

Corolário 5.19. *Seja*

$$1 \to F \to G \to H \to 1$$

uma sequência exata algorítmica com F *finitamente presentado e virtualmente abeliano, ou virtualmente livre, ou virtualmente grupo de superfície, ou virtualmente policíclico, e* H *livre. Então,* G *tem PC solúvel se, e somente se,* A_G *é decidível por órbitas.*

Demonstração. Imediata usando o Teorema 4.3, pois F satisfaz i) pelo Teorema 5.14 e H satisfaz ii) pela Proposição 2.8 e iii) pela Proposição 5.15. □

Para deixar ainda mais prático o Teorema 4.3, vamos reescrevê-lo em termos de presentações com base no resultado acima.

Teorema 5.20. *Seja $F = \langle X \mid R\rangle$ finitamente presentado e virtualmente abeliano, ou virtualmente livre, ou virtualmente grupo de superfície, ou virtualmente policíclico. Sejam $\varphi_1, ..., \varphi_m \in Aut(F)$. Então a extensão livre*

$$F \rtimes_{\varphi_1,...,\varphi_m} F_m = \left\langle X, t_1, ..., t_m \mid R, {t_i}^{-1} x t_i = x\varphi_i \ (x \in X, i = 1, ..., m)\right\rangle$$

tem o Problema da Conjugação solúvel se, e somente se, $\langle \varphi_1, ..., \varphi_m\rangle \leq Aut(F)$ é decidível por órbitas.

Demonstração. Basta ver que $G = F \rtimes_{\varphi_1,...,\varphi_m} F_m$ se encaixa perfeitamente nas hipóteses do corolário acima. Temos a sequência exata algorítmica

$$1 \to F \xrightarrow{i} F \rtimes_{\varphi_1,...,\varphi_m} F_m \xrightarrow{\beta} F_m \to 1$$

onde i é a inclusão e $(t_{k_1}...t_{k_r}x)\beta = t_{k_1}...t_{k_r}$. Logo, $F \rtimes_{\varphi_1,...,\varphi_m} F_m$ tem PC solúvel se, e somente se, A_G é decidível por órbitas. Agora, usamos a unicidade de decomposição de G na forma $t_{k_1}^{e_1}...t_{k_r}^{e_r} f$, com $1 \leq k_i \leq m, k_i \neq k_{i+1}, e_i \neq 0$ e $f \in F$. Então, dados $u, v \in F$,

$$\begin{aligned}
\exists\, \varphi_{(t_{k_1}^{e_1}...t_{k_r}^{e_r} f)} \in A_G \ : \ u\varphi_{(t_{k_1}^{e_1}...t_{k_r}^{e_r} f)} \sim v \ &\Leftrightarrow \ \exists\, x \in F \ : \ x^{-1} f^{-1} (t_{k_1}^{e_1}...t_{k_r}^{e_r})^{-1} u (t_{k_1}^{e_1}...t_{k_r}^{e_r}) f x = v \\
&\Leftrightarrow \ \exists\, g \in F \ : \ g^{-1} (t_{k_1}^{e_1}...t_{k_r}^{e_r})^{-1} u (t_{k_1}^{e_1}...t_{k_r}^{e_r}) g = v \\
&\Leftrightarrow \ \exists\, \varphi_{k_1}^{e_1}...\varphi_{k_r}^{e_r} \in \langle \varphi_1, ..., \varphi_m\rangle \ : \ u\varphi_{k_1}^{e_1}...\varphi_{k_r}^{e_r} \sim v,
\end{aligned}$$

tomando $g = fx$ da segunda para a terceira afirmação, e $f = g$ e $x = 1$ para sua recíproca, exatamente como fizemos na Observação 4.6. Logo, A_G é decidível por órbitas se, e somente se, $\langle \varphi_1, ..., \varphi_m\rangle$ o é, donde concluímos o resultado. □

Capítulo 6

Aplicações

Para finalizar o trabalho, apresentaremos neste capítulo uma série de aplicações (todas encontradas em [2]) com base nos resultados obtidos nos capítulos anteriores. Mais precisamente, vamos solucionar o Problema da Conjugação para algumas extensões livres de grupos através de soluções da Decidabilidade por Órbitas de alguns subgrupos de automorfismos específicos. Usaremos especificamente o Teorema 5.20 para a sequência exata algorítmica

$$1 \to F \xrightarrow{i} F \rtimes_{\varphi_1,...,\varphi_m} F_m \xrightarrow{\beta} F_m \to 1$$

onde i é a inclusão e $(t_{k_1}...t_{k_r}x)\beta = t_{k_1}...t_{k_r}$. Analisaremos cinco casos especiais para o subgrupo $A \leq Aut(F)$ e, dentro de cada caso, consideraremos dois subcasos: $F = \mathbb{Z}^n = \mathbb{Z} \oplus ... \oplus \mathbb{Z}$ (abeliano finitamente gerado e livre de torção) e $F = F_n$ (livre finitamente gerado). Note que, no primeiro subcaso, F é virtualmente abeliano e, no segundo, virtualmente livre, de modo que podemos aplicar tranquilamente o Teorema 5.20. Até o fim do trabalho, identificaremos naturalmente $Aut(\mathbb{Z}^n)$ com $GL_n(\mathbb{Z})$, o grupo das matrizes com entradas em $\mathbb{Z}$ n-dimensionais e invertíveis (equivalentemente, com determinante ± 1).

6.1 Aut(F)

O caso $\mathbb{Z}^n$

Segundo [2], é um fato da Álgebra Linear que, dados dois vetores $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n)$ de entradas inteiras, existe uma matriz $A \in GL_n(\mathbb{Z})$ com $(a_1, ..., a_n)A = (b_1, ..., b_n)$ se, e somente se, $mdc(a_1, ..., a_n) = mdc(b_1, ..., b_n)$, e que esta matriz é algoritmicamente computável em caso positivo (note que isto é exatamente a Decidabilidade por Órbitas do subgrupo $Aut(\mathbb{Z}^n) = GL_n(\mathbb{Z})$). De fato, uma das implicações obtemos

facilmente usando a regra de Cramer: suponha que exista uma matriz

$$A = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} \in GL_n(\mathbb{Z})$$

tal que $aA = b$ (onde aA é a notação computacional para $A(a)$). Então temos o seguinte sistema:

$$\begin{cases} b_1 = x_{11}a_1 + ... + x_{1n}a_n; \\ \quad \vdots \\ b_n = x_{n1}a_1 + ... + x_{nn}a_n. \end{cases}$$

Agora, como A é invertível, pela regra de Cramer temos $a_i = det(A_i)/det(A) = \pm det(A_i)$, onde

$$A_i = \begin{pmatrix} x_{11} & \cdots & x_{1(i-1)} & b_1 & x_{1(i+1)} & \cdots & x_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ x_{n1} & \cdots & x_{n(i-1)} & b_n & x_{n(i+1)} & \cdots & x_{nn} \end{pmatrix}.$$

Desenvolvendo o determinante de A_i a partir da i-ésima coluna obtemos

$$a_i = \lambda_{i1}b_1 + ... + \lambda_{in}b_n$$

para alguns coeficientes $\lambda_{ij} \in \mathbb{Z}$. Como cada a_i é combinação dos b_j e cada b_i é combinação dos a_j, é fácil ver que o conjunto dos divisores comuns dos a_i é o mesmo dos b_i. Em particular, $mdc(a_1, ..., a_n) = mdc(b_1, ..., b_n)$. Com relação à recíproca, suponha que $d = mdc(a_1, ..., a_n) = mdc(b_1, ..., b_n)$. Vamos exibir um algoritmo para encontrar a matriz invertível $A \in GL_n(\mathbb{Z})$ tal que $aA = b$ no caso $n = 2$. Queremos encontrar $x, y, z, w \in \mathbb{Z}$ tais que

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \quad \text{e} \quad det \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \pm 1,$$

ou, equivalentemente,

$$\begin{cases} xa_1 + ya_2 = b_1; \\ za_1 + wa_2 = b_2; \\ xw - yz = \pm 1. \end{cases} \tag{6.1}$$

Pela teoria dos números, podemos computar $s_1, s_2 \in \mathbb{Z}$ tais que $s_1a_1 + s_2a_2 = d$. Como d divide b_1 e b_2, podemos multiplicar esta igualdade pelos inteiros b_1/d e b_2/d obtendo, respectivamente,

$$\left(\frac{b_1}{d}s_1\right)a_1 + \left(\frac{b_1}{d}s_2\right)a_2 = b_1 \quad \text{e} \quad \left(\frac{b_2}{d}s_1\right)a_1 + \left(\frac{b_2}{d}s_2\right)a_2 = b_2.$$

logo, tomando os quatro inteiros entre parênteses acima como x, y, z e w, respectivamente, obtemos as duas primeiras equações de 6.1, porém não necessariamente a terceira. Para isto, vamos introduzir dois novos parâmetros $t, \tilde{t}$. Definindo

$$x = \frac{b_1}{d}s_1 + ta_2,\ y = \frac{b_1}{d}s_2 - ta_1,\ z = \frac{b_2}{d}s_1 + \tilde{t}a_2,\ w = \frac{b_2}{d}s_2 - \tilde{t}a_1,$$

continuamos tendo

$$xa_1 + ya_2 = \frac{b_1}{d}s_1a_1 + ta_2a_1 + \frac{b_1}{d}s_2a_2 - ta_1a_2 = \frac{b_1}{d}(s_1a_1 + s_2a_2) = b_1,$$

bem como $za_1 + wa_2 = b_2$, para quaisquer $t, \tilde{t} \in \mathbb{R}$. Resta acharmos $t, \tilde{t} \in \mathbb{R}$ tais que $det(A) = 1$ e tais que $ta_1, ta_2, \tilde{t}a_1, \tilde{t}a_2 \in \mathbb{Z}$ (para que A tenha entradas inteiras). Mas

$$\begin{aligned} det(A) &= xw - yz \\ &= \left(\frac{b_1}{d}s_1 + ta_2\right)\left(\frac{b_2}{d}s_2 - \tilde{t}a_1\right) - \left(\frac{b_1}{d}s_2 - ta_1\right)\left(\frac{b_2}{d}s_1 + \tilde{t}a_2\right) \\ &= \frac{b_1b_2}{d^2}s_1s_2 - \tilde{t}\frac{b_1}{d}s_1a_1 + t\frac{b_2}{d}a_2s_2 - t\tilde{t}a_2a_1 - \frac{b_1b_2}{d^2}s_1s_2 - \tilde{t}\frac{b_1}{d}s_2a_2 + t\frac{b_2}{d}a_1s_1 + t\tilde{t}a_1a_2 \\ &= t\frac{b_2}{d}(s_1a_1 + s_2a_2) - \tilde{t}\frac{b_1}{d}(s_1a_1 + s_2a_2) \\ &= tb_2 - \tilde{t}b_1. \end{aligned}$$

Compute $r_1, r_2 \in \mathbb{Z}$ tais que $r_1b_1 + r_2b_2 = d$, ou $\frac{r_1}{d}b_1 + \frac{r_2}{d}b_2 = 1$. Logo, tomando $t = r_2/d$ e $\tilde{t} = -r_1/d$, temos $det(A) = tb_2 - \tilde{t}b_1 = 1$, $ta_1 = \frac{r_2}{d}a_1 = r_2\frac{a_1}{d} \in \mathbb{Z}$ e semelhantemente $ta_2, \tilde{t}a_1, \tilde{t}a_2 \in \mathbb{Z}$, e todas as equações de 6.1 são satisfeitas pela matriz

$$A = \begin{pmatrix} \frac{b_1}{d}s_1 + \frac{r_2}{d}a_2 & \frac{b_1}{d}s_2 - \frac{r_2}{d}a_1 \\ \frac{b_2}{d}s_1 + \frac{-r_1}{d}a_2 & \frac{b_2}{d}s_2 - \frac{-r_1}{d}a_1 \end{pmatrix},$$

como queríamos. É fácil ver que podemos introduzir um novo parâmetro livre k definindo $t = \frac{r_2}{d} + kb_1$ e $\tilde{t} = \frac{-r_1}{d} + kb_2$ e a matriz

$$A_k = \begin{pmatrix} \frac{b_1}{d}s_1 + \left(\frac{r_2}{d} + kb_1\right)a_2 & \frac{b_1}{d}s_2 - \left(\frac{r_2}{d} + kb_1\right)a_1 \\ \frac{b_2}{d}s_1 + \left(\frac{-r_1}{d} + kb_2\right)a_2 & \frac{b_2}{d}s_2 - \left(\frac{-r_1}{d} + kb_2\right)a_1 \end{pmatrix}$$

continua satisfazendo tudo o que queremos, de modo que encontramos explicitamente infinitas matrizes $A_k \in GL_n(\mathbb{Z})$ tais que $aA_k = b$. No caso $(a_1, a_2) = (3, 6)$ e $(b_1, b_2) = (6, 9)$, por exemplo, temos $d = mdc(3, 6) = mdc(6, 9) = 3$ e o algoritmo acima nos dá a família

$$A_k = \begin{pmatrix} 4 + 36k & -1 - 18k \\ 5 + 54k & -1 - 27k \end{pmatrix}$$

de matrizes, como o leitor pode verificar.

Como já dissemos, os fatos acima garantem que $Aut(\mathbb{Z}^n)$ é decidível por órbitas. Logo,

temos o

Corolário 6.1. *Se $A_1, ..., A_m \in GL_n(\mathbb{Z})$ são tais que $\langle A_1, ..., A_m \rangle = GL_n(\mathbb{Z})$, então a extensão livre $\mathbb{Z}^n \rtimes_{A_1,...,A_m} F_m$ tem o Problema da Conjugação solúvel.*

O caso F_n

Em relação à Decidabilidade por Órbitas de $Aut(F_n)$, a Proposição I.4.19 em [11] cria um algoritmo que decide, dados dois elementos u, v de um grupo livre F qualquer, quando é que existe um automorfismo φ de F tal que $u\varphi = v$. Mas temos a equivalência

$$\exists\ \varphi \in Aut(F) : u\varphi = v \Leftrightarrow\ \exists\ \varphi \in Aut(F) : u\varphi \sim v,$$

onde basta conjugar $u\varphi$ por 1 da primeira para a segunda afirmação, e tomar $\varphi' = \varphi\gamma_x$, onde x conjuga $u\varphi$ e v, para a recíproca. Mas decidir se a segunda afirmação é verdadeira é exatamente a Decidabilidade por órbitas de $Aut(F)$, que era o que queríamos provar para o caso particular $F = F_n$. Logo, obtemos o seguinte corolário, análogo ao caso $\mathbb{Z}^n$:

Corolário 6.2. *Se $\varphi_1, ..., \varphi_m \in Aut(F_n)$ são tais que $\langle \varphi_1, ..., \varphi_m \rangle = Aut(F_n)$, então a extensão livre $F_n \rtimes_{\varphi_1,...,\varphi_m} F_m$ tem o Problema da Conjugação solúvel.*

6.2 Subgrupos cíclicos

O caso $\mathbb{Z}^n$

Seja $A \in GL_n(\mathbb{Z})$ e considere $u, v \in \mathbb{Z}^n$. Segundo os autores em [2], é possível decidir quando existe $k \in \mathbb{Z}$ tal que $uA^k = v$ usando técnicas de aproximação de autovalores e a forma canônica de Jordan de A, pensada como uma matriz complexa. Isto provaria exatamente a Decidabilidade de Órbitas de $\langle A \rangle$, e teríamos o seguinte corolário:

Corolário 6.3. *Qualquer extensão livre $\mathbb{Z}^n \rtimes_A \mathbb{Z}$ com $A \in GL_n(\mathbb{Z})$ tem o Problema da Conjugação solúvel.*

Porém, não precisamos nos concentrar em provar este fato pois ele já foi resolvido em um aspecto mais geral:

Proposição 6.4. *Toda extensão livre da forma $\mathbb{Z}^n \rtimes_A \mathbb{Z}$ é um grupo policíclico.*

Demonstração. Basta ver que, denotando por $\mathbb{Z}^k$ o subgrupo

$$\mathbb{Z}^k \oplus \{0\}^{n-k} = \mathbb{Z} \oplus ... \oplus \mathbb{Z} \oplus \{0\} \oplus ... \oplus \{0\} \leq \mathbb{Z}^n,$$

temos $\mathbb{Z}^n/\mathbb{Z}^k \simeq \mathbb{Z}^{n-k}$, logo podemos tomar a sequência de subgrupos

$$\mathbb{Z}^n \rtimes_A \mathbb{Z} \rhd \mathbb{Z}^n \rhd \mathbb{Z}^{n-1} \rhd ... \rhd \mathbb{Z} \rhd \{0\}$$

e teremos os quocientes cíclicos

$$\frac{\mathbb{Z}^n \rtimes_A \mathbb{Z}}{\mathbb{Z}^n} \simeq \mathbb{Z} \text{ e } \frac{\mathbb{Z}^{i+1}}{\mathbb{Z}^i} \simeq \mathbb{Z}.$$

□

Corolário 6.5. *Qualquer extensão livre $\mathbb{Z}^n \rtimes_A \mathbb{Z}$ com $A \in GL_n(\mathbb{Z})$ tem o Problema da Conjugação Torcida solúvel.*

Demonstração. Imediata, da proposição acima e do Teorema 5.6. □

O caso F_n

Este caso é simples: a Decidabilidade por Órbitas de subgrupos cíclicos $\langle\varphi\rangle \leq Aut(F_n)$ é garantida exatamente pelo Teorema de Brinkmann (3.2). Como já vimos anteriormente algumas vezes, podemos enunciar novamente o

Corolário 6.6. *Qualquer extensão livre $F_n \rtimes_\varphi \mathbb{Z}$ com $\varphi \in Aut(F_n)$ tem o Problema da Conjugação solúvel.*

6.3 Subgrupos de índice finito

Conseguimos resolver a Decidabilidade por Órbitas para qualquer subgrupo B de índice finito dado por alguns geradores, nos dois casos abaixo. Esta seção estende, portanto, a primeira seção deste capítulo. A ideia principal é reduzir o problema a um subgrupo normal $A \leq B$ de índice finito e usar o Problema da Membresia. Precisaremos de dois lemas:

Lema 6.7. *Seja F grupo, $Aut(F) = \langle X \mid R\rangle$ finitamente presentado e $A \leq B \leq Aut(F)$ dois subgrupos dados por conjuntos finitos de geradores tais que $|B : A|$ e $|Aut(F) : B|$ são finitos. Então, se A é decidível por órbitas, B também o é.*

Demonstração. Primeiramente, usamos o processo de Reidemeister-Schreier para computar uma presentação finita $B = \langle Y \mid S\rangle$ para B (podemos fazer isto, pois estamos sob as mesmas condições do Teorema 5.14, por exemplo, onde o processo foi usado não somente uma, mas um número arbitrário de vezes). Escreva os geradores de A em termos desta presentação. Agora, pelo algoritmo de Todd-Coxeter, podemos computar automorfismos representantes $\beta_1, ..., \beta_m \in B$ tais que $B = A \sqcup \beta_1 A \sqcup ... \sqcup \beta_m A$ (escreva $Id = \beta_0$). Para resolver a Decidabilidade por Órbitas de B, sejam $u, v \in F$. Usando a decomposição em classes laterais, temos a óbvia equivalência:

$$\exists\ \beta \in B : u\beta \sim v \Leftrightarrow \exists\ 0 \leq i \leq m \text{ e } \alpha \in A : u\beta_i\alpha \sim v.$$

Podemos decidir se é verdadeira esta última afirmação da seguinte forma: compute os elementos $u\beta_i$ para cada i e use a Decidabilidade por Órbitas de A para decidir se, para algum deles, existe $\alpha \in A$ tal que $(u\beta_i)\alpha \sim v$. Logo, B é decidível por órbitas. □

Lema 6.8. *Seja B subgrupo de índice finito de um grupo G, com $G = B \sqcup Ba_1 \sqcup ... \sqcup Ba_n$. Então o subgrupo*

$$A = \bigcap_{a \in G} (a^{-1}Ba)$$

é normal e de índice finito em B e vale

$$A = \bigcap_{a \in G} (a^{-1}Ba) = B \cap {a_1}^{-1}Ba_1 \cap ... \cap {a_n}^{-1}Ba_n. \tag{6.2}$$

Demonstração. Para provar a normalidade, seja $g \in G$, $n \in A$ e provemos que $g^{-1}ng \in A$. Seja então $a \in G$ e provemos que $g^{-1}ng \in a^{-1}Ba$. Como $n \in A$, tome $a' = ag^{-1}$ e temos que $n \in {a'}^{-1}Ba' = ga^{-1}Bag^{-1}$, logo $n = ga^{-1}bag^{-1}$ para algum $b \in B$ e daí $g^{-1}ng = a^{-1}ba \in a^{-1}Ba$, como desejado. Vamos provar 6.2. É claro que a interseção total dos subgrupos conjugados está contida na interseção finita. Por outro lado, seja $g \in B \cap {a_1}^{-1}Ba_1 \cap ... \cap {a_n}^{-1}Ba_n$ (escreva $a_0 = 1$). Seja $a \in G$ e provemos que $g \in a^{-1}Ba$. Usando a decomposição de G nas classes laterais, existe $0 \leq i \leq n$ e $b \in B$ tal que $a = ba_i$, de modo que $a^{-1}Ba = {a_i}^{-1}b^{-1}Bba_i = {a_i}^{-1}Ba_i$, logo por hipótese $g \in {a_i}^{-1}Ba_i = a^{-1}Ba$, como queríamos. Por último, vamos provar que A tem índice finito em B. É fácil ver que imagem por isomorfismo de subgrupo de índice finito é também de índice finito. Assim, sendo B de índice finito em G, também são os subgrupos ${a_1}^{-1}Ba_1, ..., {a_n}^{-1}Ba_n$. Pela Proposição 4.9 em [9] (p.40), temos $|G : H \cap K| \leq |G : H||G : K|$ para quaisquer subgrupos H, K de índice finito. Logo, por indução,

$$|G : H_1 \cap ... \cap H_n| \leq |G : H_1|...|G : H_n|$$

para quaisquer subgrupos H_i de índice finito. Usando isto em nosso caso e usando que vale $|H : H \cap K| \leq |G : K|$ para quaisquer subgrupos H, K de G (Proposição 4.8 de [9], p.39), obtemos

$$\begin{aligned} |B : A| = |B : B \cap (({p_1}^{-1}Bp_1) \cap ... \cap ({p_n}^{-1}Bp_n))| &\leq |G : ({p_1}^{-1}Bp_1) \cap ... \cap ({p_n}^{-1}Bp_n)| \\ &\leq |G : {p_1}^{-1}Bp_1|...|G : {p_n}^{-1}Bp_n| \\ &< \infty, \end{aligned}$$

o que conclui o resultado. □

O caso $\mathbb{Z}^n$

Proposição 6.9. *Seja $B = \langle B_1, ..., B_k \rangle$ um subgrupo de índice finito de $G = GL_n(\mathbb{Z})$. Então B é decidível por órbitas.*

Demonstração. Tome uma presentação finita para $GL_n(\mathbb{Z})$ (veja o Teorema N4 da seção 3.5 de [12]) e escreva os geradores $B_1, ..., B_k$ em termos da mesma. Pelo Algoritmo de Todd-Coxeter (5.10) podemos computar explicitamente representantes $P_1, ..., P_m \in G$ tais que $G = B \sqcup BP_1 \sqcup ... \sqcup BP_m$. Segundo [2], podemos usar o mesmo argumento da demonstração do Lema 5.12 para computar explicitamente um conjunto de geradores $A_1, ..., A_s$ para o subgrupo de B

$$A = \bigcap_{a \in G} (a^{-1}Ba) = B \cap {P_1}^{-1}BP_1 \cap ... \cap {P_m}^{-1}BP_m,$$

que já sabemos ser normal e de índice finito em B pelo Lema 6.8. Por ser de índice finito e termos os geradores, o Lema 6.7 garante que B será decidível por órbitas se A o for, o que provaremos abaixo.

Dados $u, v \in \mathbb{Z}^n$, precisamos decidir se existe uma matriz $N \in A$ tal que $uN = v$ (note que, a princípio, Decidabilidade por Órbitas pede apenas $uN \sim v$, mas em grupos abelianos a conjugação é equivalente à igualdade). Pelos comentários no início da primeira seção, podemos decidir quando existe uma matriz $M \in GL_n(\mathbb{Z})$ (não necessariamente em A) tal que $uM = v$. Se tal M não existe, então é claro que não existirá nenhuma tal matriz em A, e terminamos. Vamos para o caso em que M existe (e compute M explicitamente). Nesse caso, se denotarmos $Stab(v) = \{N \in GL_n(\mathbb{Z}) \mid vN = v\} \leq GL_n(\mathbb{Z})$, teremos

$$\{N \in GL_n(\mathbb{Z}) \mid uN = v\} = M(Stab(v)).$$

De fato, se $uN = v$, podemos escrever $N = M(M^{-1}N) \in M(Stab(v))$, pois $vM^{-1}N = uN = v$. Por outro lado, toda matriz da forma MS com $S \in Stab(v)$ é tal que $uMS = vS = v$, o que conclui a igualdade dos conjuntos. Desta igualdade concluímos que o que precisamos decidir é se existe $N \in A \cap M(Stab(v))$, ou seja, se $A \cap M(Stab(v)) \neq \emptyset$. Mas

$$A \cap M(Stab(v)) \neq \emptyset \Leftrightarrow M \in A(Stab(v)).$$

De fato, se $N \in A \cap M(Stab(v))$, escreva $N = MS$ com $S \in Stab(v)$ e teremos $M = NS^{-1} \in A(Stab(v))$. Por outro lado, se $M \in A(Stab(v))$, escreva $M = NS$ com $N \in A$ e $S \in Stab(v)$, e daí $N = N(Id) \in N(Stab(v)) = MS^{-1}(Stab(v)) = M(Stab(v))$, logo $N \in A \cap M(Stab(v)) \neq \emptyset$, como desejado. O que temos de decidir então é se $M \in A(Stab(v))$. Agora, segundo [2] é possível computar um conjunto $\{K_1, ..., K_r\}$ de geradores de $Stab(v)$. Então, por ser A normal em G,

$$A(Stab(v)) = \langle A_1, ..., A_s \rangle \langle K_1, ..., K_r \rangle = \langle A_1, ..., A_s, K_1, ..., K_r \rangle$$

é um subgrupo finitamente gerado e é de índice finito em G, pois

$$|G : A(Stab(v)| \leq |G : A(Stab(v))||A(Stab(v)) : A| = |G : A| = |G : B||B : A| < \infty.$$

Logo, pelo Algoritmo de Todd-Coxeter, o Problema da Membresia PM($A(Stab(v))$,G) é solúvel, que é exatamente o que precisávamos para decidir se $M \in A(Stab(v))$. □

Com a decidabilidade acima, é natural o seguinte

Corolário 6.10. *Se $A_1, ..., A_m \in GL_n(\mathbb{Z})$ são tais que $\langle A_1, ..., A_m \rangle$ tem índice finito em $GL_n(\mathbb{Z})$, então a extensão livre $\mathbb{Z}^n \rtimes_{A_1,...,A_m} F_m$ tem o Problema da Conjugação solúvel.*

O caso F_n

Este caso é inteiramente análogo ao caso $\mathbb{Z}^n$, apenas com as modificações necessárias.

Proposição 6.11. *Seja $B = \langle \varphi_1, ..., \varphi_k \rangle$ um subgrupo de índice finito de $Aut(F_n)$. Então B é decidível por órbitas.*

Demonstração. Tome uma presentação finita para $G = Aut(F_n)$ (veja o Teorema N1 da seção 3.5 de [12]) e escreva os geradores $\varphi_1, ..., \varphi_k$ em termos da mesma. Pelo Algoritmo de Todd-Coxeter (5.10) podemos computar explicitamente representantes $\psi_1, ..., \psi_m \in G$ tais que $G = B \sqcup B\psi_1 \sqcup ... \sqcup B\psi_m$. Segundo [2], podemos usar o mesmo argumento da demonstração do Lema 5.12 e computar um conjunto de geradores $\alpha_1, ..., \alpha_s$ para o subgrupo de B

$$A = \bigcap_{a \in G} (a^{-1}Ba) = B \cap {\psi_1}^{-1}B\psi_1 \cap ... \cap {\psi_m}^{-1}B\psi_m,$$

que já sabemos ser normal e de índice finito em B pelo Lema 6.8. Por ser de índice finito e termos os geradores, o Lema 6.7 garante que B será decidível por órbitas se A o for. Vamos provar então que A é decidível por órbitas.

Dados $u, v \in F_n$, precisamos decidir se existe um automorfismo $\varphi \in A$ tal que $u\varphi \sim v$. Pelos comentários da primeira seção deste capítulo, podemos decidir quando existe $\psi \in Aut(F_n)$ (não necessariamente em A) tal que $u\psi = v$. Se tal ψ não existe, então não existirá nenhum tal automorfismo em A, e terminamos. Considere o caso em que ψ existe. Nesse caso, denotando $Stab(v) = \{\varphi \in Aut(F_n) \mid v\varphi = v\} \leq Aut(F_n)$ e $Inn(F_n) = \{\gamma_g \mid g \in F_n\} \leq Aut(F_n)$ o subgrupo dos automorfismos de conjugação em F_n, teremos

$$\{\varphi \in Aut(F_n) \mid u\varphi \sim v\} = \psi Stab(v) Inn(F_n).$$

De fato, se $u\varphi \sim v$, temos $x^{-1}u\varphi x = v$ para $x \in F_n$. Daí escrevemos $\varphi = \psi(\psi^{-1}\varphi\gamma_x)\gamma_{x^{-1}} \in \psi Stab(v) Inn(F_n)$, pois $v\psi^{-1}\varphi\gamma_x = u\varphi\gamma_x = x^{-1}u\varphi x = v$. Por outro lado, todo automorfismo da forma $\psi\beta\gamma_x$ para algum $\beta \in Stab(v)$ é tal que $u\psi\beta\gamma_x = v\beta\gamma_x = v\gamma_x = x^{-1}vx \sim v$,

o que conclui a igualdade dos conjuntos. Desta igualdade concluímos que o que precisamos decidir é se existe $\varphi \in A \cap \psi Stab(v)Inn(F_n)$, ou seja, se $A \cap \psi Stab(v)Inn(F_n) \neq \emptyset$. Mas

$$A \cap \psi Stab(v)Inn(F_n) \neq \emptyset \Leftrightarrow \psi \in A(Stab(v))Inn(F_n).$$

De fato, se $\varphi \in A \cap \psi Stab(v)Inn(F_n)$, temos $\varphi = \psi\beta\gamma_x$ para algum $\beta \in Stab(v)$ e $x \in F_n$. Daí, usando explicitamente a normalidade de $Inn(F_n)$ temos

$$\psi = \varphi\gamma_{x^{-1}}\beta^{-1} = \varphi\beta^{-1}(\beta\gamma_{x^{-1}}\beta^{-1}) = \varphi\beta^{-1}\gamma_{(x\beta)^{-1}} \in A(Stab(v))Inn(F_n).$$

Por outro lado, se $\psi \in A(Stab(v))Inn(F_n)$, escreva $\psi = \varphi\beta\gamma_x$ para $\varphi \in A, \beta \in Stab(v)$ e $x \in F_n$ e podemos usar o fato de que $Stab(v)Inn(F_n) = Inn(F_n)Stab(v)$ (pois $Inn(F_n) \lhd Aut(F_n)$) para concluir que

$$\begin{aligned} \psi Stab(v)Inn(F_n) &= \varphi\beta\gamma_x Stab(v)Inn(F_n) \\ &= \varphi\beta\gamma_x Inn(F_n)Stab(v) \\ &= \varphi\beta Inn(F_n)Stab(v) \\ &= \varphi\beta Stab(v)Inn(F_n) \\ &= \varphi Stab(v)Inn(F_n), \end{aligned}$$

e daí $\varphi = \varphi(Id)(Id) \in \varphi Stab(v)Inn(F_n) = \psi Stab(v)Inn(F_n)$, logo $\varphi \in A \cap \psi Stab(v)Inn(F_n) \neq \emptyset$, como desejado. O que temos de decidir então é se $\psi \in A(Stab(v))Inn(F_n)$. Agora, pela Proposição I.5.7 de [11], é possível computar um conjunto $\{\beta_1, ..., \beta_r\}$ de geradores de $Stab(v)$. Também, é claro que $Inn(F_n) = \langle \gamma_{x_1}, ..., \gamma_{x_n} \rangle$, onde os x_i são os geradores de F_n. Então, por serem A e $Inn(F_n)$ normais em $G = Aut(F_n)$,

$$A(Stab(v))Inn(F_n) = \langle \alpha_1, ..., \alpha_s, \beta_1, ..., \beta_r, \gamma_{x_1}, ..., \gamma_{x_n} \rangle$$

é um subgrupo finitamente gerado e é de índice finito em G, pois

$$|G : A(Stab(v))Inn(F_n)| \leq |G : A| = |G : B||B : A| < \infty.$$

Logo, pelo Algoritmo de Todd-Coxeter, o Problema da Membresia PM($A(Stab(v))Inn(F_n)$,G) é solúvel, que é exatamente o que precisávamos para decidir se $\psi \in A(Stab(v))Inn(F_n)$. □

Corolário 6.12. *Se $\varphi_1, ..., \varphi_m \in Aut(F_n)$ são tais que $\langle \varphi_1, ..., \varphi_m \rangle$ tem índice finito em $Aut(F_n)$, então a extensão livre $F_n \rtimes_{\varphi_1,...,\varphi_m} F_m$ tem o Problema da Conjugação solúvel.*

6.4 Subgrupos finitamente gerados

Podemos encontrar também uma solução para a Decidabilidade por Órbitas de subgrupos finitamente gerados de $Aut(\mathbb{Z}^2)$ e $Aut(F_2)$, usando uma estratégia parecida com a do caso anterior. Aqui, a vantagem de termos $n = 2$ nos dá a solução de um outro problema de decisão: o Problema da Interseção de Classes Laterais, e isto nos permite descartar a hipótese do subgrupo ter índice finito como acima.

- **O Problema da Interseção de Classes Laterais (PICL):** seja $G = \langle X \mid R \rangle$ presentado. Dados $\{a_1, ..., a_r\}$ e $\{b_1, ..., b_s\}$ dois conjuntos finitos em G e $x, y \in G$ (em termos desta presentação), decidir quando a interseção

$$x \langle a_1, ..., a_r \rangle \cap \ y \langle b_1, ..., b_s \rangle$$

é vazia ou não.

Usaremos o seguinte lema de [2], cuja demonstração está baseada em métodos geométricos e foge do objetivo deste trabalho:

Lema 6.13. *O Problema da Interseção de Classes Laterais é solúvel em $GL_2(\mathbb{Z})$.*

O caso $\mathbb{Z}^2$

Proposição 6.14. *Todo subgrupo finitamente gerado $A = \langle A_1, ..., A_s \rangle \leq GL_2(\mathbb{Z})$ é decidível por órbitas.*

Demonstração. Sejam $u, v \in \mathbb{Z}^2$ e decidamos se existe $N \in A$ tal que $uN = v$. Como fizemos na Proposição 6.9, podemos decidir se existe $M \in GL_2(\mathbb{Z})$ (não necessariamente em A) tal que $uM = v$. Se tal M não existe, é claro que N não existirá, e terminamos. Suponha então que tenhamos encontrado tal M. Então, com a mesma demonstração da Proposição 6.9, temos

$$\{N \in GL_2(\mathbb{Z}) \mid uN = v\} = M(Stab(v)),$$

logo o que precisamos decidir é se a interseção $A \cap M(Stab(v))$ é vazia ou não. Tomando explicitamente geradores $K_1, ..., K_r$ de $Stab(v)$ (como em 6.9), temos que decidir quando a interseção $A \cap M(Stab(v)) = \langle A_1, ..., A_s \rangle \cap M \langle K_1, ..., K_r \rangle$ é vazia ou não, o que é possível pelo Lema 6.13. □

Corolário 6.15. *O Problema da Conjugação é solúvel em qualquer extensão livre $\mathbb{Z}^2 \rtimes_{A_1,...,A_m} F_m$, com $A_1, ..., A_m \in GL_2(\mathbb{Z})$.*

O caso F_2

Proposição 6.16. *Todo subgrupo finitamente gerado $A = \langle \varphi_1, ..., \varphi_s \rangle \leq F_2$ é decidível por órbitas.*

Demonstração. Sejam $u, v \in F_2$ e decidamos se existe $\varphi \in A$ tal que $u\varphi \sim v$. Assim como comentamos na Proposição 6.11, podemos decidir se existe $\psi \in Aut(F_2)$ (não necessariamente em A) tal que $u\psi = v$. Se ψ não existe, é claro que φ não existirá, e terminamos. Suponha então que ψ exista. Então, com a mesma demonstração da Proposição 6.11, temos

$$\{\varphi \in Aut(F_2) \mid u\varphi \sim v\} = \psi Stab(v) Inn(F_2),$$

logo o que precisamos decidir é se a interseção $A \cap (\psi Stab(v) Inn(F))$ é vazia ou não. Agora, seja $\pi : Aut(F_2) \to GL_2(\mathbb{Z})$ o homomorfismo projeção, cujo núcleo é $\ker(\pi) = Inn(F_2)$. Afirmamos que

$$A \cap (\psi Stab(v) Inn(F)) \neq \emptyset \Leftrightarrow A\pi \cap (\psi\pi)(Stab(v))\pi \neq \emptyset.$$

De fato, se $z \in A \cap (\psi Stab(v) Inn(F))$, temos $z = \psi\beta\gamma_x$ para $\beta \in Stab(v)$. Logo, é óbvio que $z\pi \in A\pi$ e $z\pi = (\psi\pi)(\beta\pi)(\gamma_x\pi) = (\psi\pi)(\beta\pi) \in (\psi\pi)(Stab(v))\pi$ e daí a interseção $A\pi \cap (\psi\pi)(Stab(v))\pi$ é não vazia. Por outro lado, se $y \in A\pi \cap (\psi\pi)(Stab(v))\pi$, escreva $a\pi = y = (\psi\pi)(\beta\pi) = (\psi\beta)\pi$, para $a \in A$ e $\beta \in Stab(v)$. Disso temos $a\beta^{-1}\psi^{-1} \in \ker(\pi)$ e podemos escrever $a\beta^{-1}\psi^{-1} = \gamma_x$. Isolando a, obtemos

$$a = \gamma_x\psi\beta = \psi\beta(\psi\beta)^{-1}\gamma_x(\psi\beta) = \psi\beta\gamma_{x\psi\beta} \in \psi Stab(v) Inn(F_2),$$

e daí $a \in A \cap (\psi Stab(v) Inn(F_2)) \neq \emptyset$, como desejado. Temos de decidir então se $A\pi \cap (\psi\pi)(Stab(v))\pi \neq \emptyset$. Tomemos um conjunto gerador $\beta_1, ..., \beta_r$ de $Stab(v)$ (como em 6.11). Como homomorfismo leva conjunto de geradores em conjunto de geradores, temos que decidir se a interseção

$$A\pi \cap (\psi\pi)(Stab(v))\pi = \langle \varphi_1\pi, ..., \varphi_s\pi \rangle \cap (\psi\pi) \langle \beta_1\pi, ..., \beta_r\pi \rangle$$

é vazia, o que é decidível pelo Lema 6.13. □

Corolário 6.17. *O Problema da Conjugação é solúvel em qualquer extensão livre $F_2 \rtimes_{\varphi_1,...,\varphi_m} F_m$, com $\varphi_1, ..., \varphi_m \in Aut(F_2)$.*

6.5 Subgrupos virtualmente solúveis

O último tipo de subgrupo de $Aut(F)$ que analisaremos aqui é o dos virtualmente solúveis. A estratégia é filosoficamente parecida com a da seção de índice finito: reduzir a Decidabilidade por Órbitas a um subgrupo poli-$\mathbb{Z}$ e resolvê-la neste subgrupo escrevendo-

o como o subgrupo de ação de um grupo com PC solúvel no qual vale o Teorema 4.3. Nesta seção, apenas analisaremos o caso $\mathbb{Z}^n$, pois não se sabe se todo subgrupo $A = \langle \varphi_1, ..., \varphi_s \rangle \leq Aut(F_n)$ virtualmente solúvel é decidível por órbitas. Lembremos a definição de um grupo ser solúvel: dado um grupo G, podemos criar o grupo de comutadores

$$G' = \left\langle \{aba^{-1}b^{-1} \mid a, b \in G\} \right\rangle \lhd G.$$

Denotando $G^1 = G'$, $G^2 = (G')'$, $G^3 = ((G')')'$ e assim por diante, obtemos um sequência $G \rhd G^1 \rhd G^2 \rhd ... \rhd G^n \rhd ....$

Definição 6.18. Um grupo G é dito *solúvel* quando $G^n = \{1\}$ para algum $n \geq 1$.

O caso $\mathbb{Z}^n$

O principal resultado (além do Teorema 5.20) que usaremos aqui é o seguinte, que pode ser encontrado no capítulo 2 de [17]:

Proposição 6.19. *Todo subgrupo solúvel de $GL_n(\mathbb{Z})$ é policíclico.*

Proposição 6.20. *Todo subgrupo virtualmente solúvel $A = \langle A_1, ..., A_s \rangle \leq GL_n(\mathbb{Z})$ é decidível por órbitas.*

Demonstração. Por hipótese, existe um subgrupo $C \leq A$ que é solúvel e de índice finito em A. Pela proposição acima, C é policíclico. Como todo grupo policíclico é virtualmente poli-$\mathbb{Z}$ (Proposição 2 do Capítulo 1 de [17]), podemos tomar um subgrupo poli-$\mathbb{Z}$ de índice finito em C (portanto, também em A) e denotá-lo também por C, esquecendo o anterior.

Vamos usar as presentações canônicas de grupos poli-$\mathbb{Z}$

$$K = CE(CE(...CE(\langle x \mid \emptyset \rangle)...)),$$

que definimos no Teorema 5.14. Qualquer presentação de qualquer grupo poli-$\mathbb{Z}$ é obtida a partir de uma presentação como a acima, a partir de um número finito de transformações de Tietze. Logo, com argumentos de diagonalização similares aos do Lema 5.13 e do Teorema 5.14, podemos computar uma a uma (sem nunca terminar) todas as presentações de todos os grupos policíclicos, digamos, $\{P_1, P_2, ...\}$, com $P_i = \langle t_1, ..., t_{k_i} \mid R_1, ..., R_{l_i} \rangle$. Também podemos, com técnicas geométricas (vide [2]), computar uma lista de triplas $\{(C_1, D_1, M_1), (C_2, D_2, M_2), ...\}$, onde $\{C_1, C_2, ...\}$ é a lista de todos os subgrupos de índice finito de A, D_i é um conjunto finito de geradores para C_i e $M_i = \{M_i^1, ..., M_i^{r_i}\}$ é um conjunto de representantes laterais, ou seja,

$$A = M_i^1 C_i \sqcup ... \sqcup M_i^{r_i} C_i. \tag{6.3}$$

Para cada $i, j \geq 1$, podemos testar algoritmicamente se existe um epimorfismo

$$P_i = \langle t_1, ..., t_{k_i} \mid R_1, ..., R_{l_i} \rangle \to C_j,$$

testando se existe alguma função $\{t_1, ..., t_{k_i}\} \to D_j$ que se estende a um tal epimorfismo (basta verificar para cada função se todas as relações em P_i estão no núcleo do homomorfismo induzido do grupo livre $F_{\{t_1,...,t_{k_i}\}}$ em C_j). Vamos executar então o seguinte algoritmo: seja $T(P_i, C_j)$ o teste acima que fazemos para verificar se existe um epimorfismo $P_i \to C_j$, depois de termos calculado a presentação P_i e a tripla (C_j, D_j, M_j). Realizamos estes testes diagonalmente, como no Teorema 5.14. O algoritmo terminará em algum momento, pois o subgrupo C possui uma presentação exatamente igual a alguma das P_i's e temos $C = C_j$ para algum j, de modo que em algum momento obteremos um isomorfismo explícito $P_i \to C_j$, o objetivo final do algoritmo.

Agora, temos um epimorfismo $P_i \to C_j \leq Aut(\mathbb{Z}^n)$ que nos permite fazer o produto semidireto $G = \mathbb{Z}^n \rtimes P_i$. Como G é claramente policíclico, possui PC solúvel. Logo, pelo item $(a) \Rightarrow c)$) do Teorema 4.3, A_G é decidível por órbitas. Mas toda vez que temos uma sequência exata

$$1 \to F \to G = F \rtimes H \to H \to 1$$

com F abeliano, o subgrupo de ação A_G é dado apenas pelos automorfismos induzidos por H, pois conjugando $f \in F$ por um elemento qualquer $f'h \in G$ temos

$$f\varphi_{f'h} = (f'h)^{-1} f(f'h) = h^{-1}f'^{-1}ff'h = h^{-1}fh = f\varphi_h.$$

Logo, em nosso caso, a abelianidade de $\mathbb{Z}^n$ garante que A_G é o subgrupo formado apenas pelos automorfismos induzidos por P_i através do epimorfismo $P_i \to C_j$, ou seja, $A_G = C_j$. Finalmente, a Decidabilidade por Órbitas de C_j garante a de A, pois, dados $u, v \in \mathbb{Z}^n$, decidir se existe $N \in A$ tal que $uN = v$ é equivalente, graças à decomposição 6.3, a decidir se existe $1 \leq k \leq r_j$ e $Q \in C_j$ tal que $uM_j^k Q = v$, o que se resume a r_j testes de Decidabilidade por Órbitas de C_j. □

Corolário 6.21. *Se $A_1, ..., A_m \in GL_n(\mathbb{Z})$ são tais que $\langle A_1, ..., A_m \rangle$ é virtualmente solúvel, então a extensão livre $\mathbb{Z}^n \rtimes_{A_1,...,A_m} F_m$ tem o Problema da Conjugação solúvel.*

Referências Bibliográficas

[1] O. Bogopolski, A. Martino, O. Maslakova, E. Ventura. *The Conjugacy Problem is solvable in Free-by-cyclic groups*, Bulletin of the London Mathematical Society 38(5), 2006, 787-794.

[2] O. Bogopolski, A. Martino, E. Ventura. *Orbit Decidability and the Conjugacy Problem for some extensions of groups*, Transactions of the London Mathematical Society volume 362, number 4, 2010, 2003-2036.

[3] W.W. Boone, F.B. Cannonito, R.C.Lyndon. *Word Problems. Decision Problems and the Burnside Problem in Group Theory*, North-Holland Publishing Company, 1973.

[4] M.R. Bridson, A. Haefliger. *Metric spaces of non-positive curvature*, Grundlehren der Mathematischen Wissenschaften 319, Springer-Verlag, 1999.

[5] P. Brinkmann. *Dynamics of free group automorphisms*, Combinatorial and Geometric Group Theory, Trends in Mathematics, 19–53, 2010, Springer Basel AG.

[6] Bruce Chandler and Wilhelm Magnus. *The History of Combinatorial Group Theory: a Case Study in the History of Ideas*, Springer-Verlag, 1982.

[7] Gromov, M. *Hyperbolic groups*, Essays in group theory, 75–263, Math. Sci. Res. Inst. Publ., 8, Springer, New York, 1987.

[8] Hatcher, A. *Algebraic Topology*, Cambridge University Press, 2002.

[9] Hungerford, Thomas W. *Algebra*, Springer-Verlag, 1974.

[10] D.L.Johnson. *Presentations of groups*, London Math. Soc. Student texts 15, Cambridge University Press, 1990.

[11] R.C. Lyndon, P.E. Schupp. *Combinatorial Group Theory*, Springer-Verlag, 1977.

[12] Magnus, W., Karras, A., Solitar, D.. *Combinatorial Group Theory*, New York: Wiley 1966.

[13] O. S. Maslakova. *the fixed point group of a free group automorphism* Algebra Logic 42 (2003) 237-265.

[14] J.P.Preaux. *Conjugacy problem in groups of oriented geometrizable 3-manifolds*, Topology 45(1) (2006), 171-208

[15] J.P.Preaux. *Conjugacy problem in groups of non-oriented geometrizable 3-manifolds*, Disponível em http://arxiv.org/pdf/1202.4148.pdf

[16] V.N. Remeslennikov. *Conjugacy in polycyclic groups*, Algebra and Logic 8 (1969), 404-411.

[17] D.Segal. *Polyciclic groups*, Cambridge Tracts in Mathematics 82, Cambridge University Press, 1983.

Índice Remissivo