UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA

PSEUDOVARIEDADES DE GRUPOS E VARIEDADES DE LINGUAGENS ASSOCIADAS

Eliana Nunes de Castro

Mestrado em Matemática

2008

UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA

PSEUDOVARIEDADES DE GRUPOS E VARIEDADES DE LINGUAGENS ASSOCIADAS

Eliana Nunes de Castro
Dissertação orientada pela
Professora Doutora Gracinda M. S. Gomes

Mestrado em Matemática

2008

Agradecimentos

Em primeiro lugar gostaria de agradecer à minha orientadora, a Professora Doutora Gracinda M. S. Gomes, por me cativar para esta área da Matemática, pela sua direcção, compreensão e apoio, pessoal e científico, sem o qual este trabalho não teria sido possível.

Em segundo lugar, gostaria de agradecer aos Professores Mário Branco e Jorge Almeida e aos Doutores Xaro Escrivà e Csaba Schneider pela ajuda que me proporcionaram no esclarecimento de algumas questões.

Agradeço aos meus pais o seu inestimável apoio, fundamental nos momentos difíceis, e o terem-me proporcionado a oportunidade de prosseguir os meus estudos.

Aos meus amigos da FCUL, sempre presentes durante o meu percurso académico, agradeço terem-me apoiado de inúmeras formas, sem eles este percurso teria sido muito menos enriquecedor.

Por fim um agradecimento especial ao Filipe, pela atenção e pela dedicação que me concedeu durante a preparação deste trabalho.

Resumo

O principal objectivo deste trabalho consiste em dar uma descrição das linguagens reconhecidas pelos grupos super-resolúveis finitos. Essa descrição será feita de dois modos distintos: através de produtos modulares concatenados, mostrando que uma tal linguagem pertence à álgebra de Boole gerada por produtos modulares concatenados de linguagens comutativas elementares e, através de transdutores, provando que essas linguagens são combinações Booleanas de linguagens da forma $r\tau^{-1}$, em que p é um número primo, $r \in \mathbb{Z}_p$ e $\tau : A^* \to \mathbb{Z}_p$ é uma função realizada por algum transdutor na forma triangular estrita.

Com vista a esse estudo, faremos uma análise detalhada da pseudovariedade dos grupos super-resolúveis e também de outras pseudovariedades de grupos, em particular, das pseudovariedades dos p-grupos e dos grupos abelianos cujo expoente divide um dado natural n. Caracterizaremos também o produto de pseudovariedades e daremos especial atenção à pseudovariedade $\mathbf{G}_p * \mathbf{Ab}^{p-1}$.

Estudaremos as variedades de linguagens associadas às pseudovariedades de grupos consideradas e iremos demonstrar o Princípio do Produto em Coroa de Straubing, o qual nos fornece uma descrição das linguagens reconhecidas pelo produto em coroa de dois monóides. Além disso, apresentaremos uma versão deste princípio para variedades de linguagens. Será ainda considerado o produto de linguagens com contador e descrita a operação entre monóides que lhe está associada .

Palavras-chave: Linguagem, Pseudovariedade, Variedade de Linguagens, Grupos Super-Resolúveis.

Abstract

The main subject of this work is to give a description of the languages recognized by finite super-soluble groups. That description will be done in two distinct ways. The first one uses the modular concatenation product, more precisely, we will prove that such a language is in the Boolean algebra generated by the concatenated modular products of elementary commutative languages. In the second one we prove that the languages recognized by super-soluble groups are Boolean combinations of languages that take the form of $r\tau^{-1}$, where p is a prime number, $r \in \mathbb{Z}_p$ and $\tau : A^* \to \mathbb{Z}_p$ is a function realized by some transductor in the strict triangular form.

In view of that study, we will analyse in detail the pseudovarieties of super-soluble groups as well as other pseudovarieties of groups, in particular we will consider the pseudovariety of p-groups and the pseudovariety of abelian groups whose exponent divides a given natural n. We will also characterize the product of pseudovarieties, dedicating particular attention to the pseudovariety $\mathbf{G}_p * \mathbf{Ab}^{p-1}$.

We will study the varieties of languages associated with the pseudovarieties of groups considered and will prove the Straubing's Wreath Product Principle, which gives us a description of the languages recognized by the wreath product of two monoids. In addition, we will present a version of this principle applied to varieties of languages. The product of languages with counter will also be considered and the associated operation between monoids will be described.

Key words: Language, Pseudovariety, Variety of Languages, Supersoluble Groups.

Conteúdo

Introdução

A interligação entre Semigrupos, Autómatos e Linguagens Formais, com as suas principais raízes nos trabalhos de Schützenberger e Eilenberg dos anos 60 e 70, tem sido objecto de vasto estudo pondo em evidência a importância da ligação entre a Álgebra e a Teoria da Computação, sendo que a Teoria das Linguagens Formais é uma das bases da Ciência da Computação Teórica. Um problema abordado por esta teoria tem sido, desde a sua origem nos anos 60, a classificação das linguagens racionais. Uma ferramenta muito aplicada nesta tarefa é o monóide sintáctico, $Syn(L)$, de uma linguagem racional L sobre um alfabeto finito A, visto que muitas propriedades combinatoriais de L correspondem a propriedades algébricas de $Syn(L)$. O facto de certas subclasses de linguagens racionais corresponderem a determinadas classes de monóides, ou de semigrupos, foi ilustrado primeiramente por Schützenberger (ver [22]). Em 1975, Eilenberg sistematizou esta correspondência mostrando que existe uma relação bijectiva entre certas famílias de monóides finitos, ditas pseudovariedades, e determinadas famílias de linguagens racionais, ditas variedades de linguagens. Mais concretamente, o chamado Teorema da Variedade de Eilenberg diz que, dada uma pseudovariedade de monóides $\mathbf{V}$, a classe das linguagens $\mathcal{V}$ cujo monóide sintáctico pertence a $\mathbf{V}$ é uma variedade de linguagens e a correspondência $\mathbf{V} \to \mathcal{V}$ entre pseudovariedades de monóides e variedades de linguagens é uma bijecção. Este teorema pode pois ser usado em ambos os sentidos: dada uma pseudovariedade de monóides podemos querer procurar uma descrição combinatorial da correspondente variedade de linguagens, ou, dada uma variedade de linguagens podemos pretender analisar a correspondente pseudovariedade de monóides. Muitos casos particulares desta correspondência têm sido estudados. Como exemplos temos, entre outros, o caso das linguagens sem estrela que estão em correspondência com os monóides aperiódicos (ver, por exemplo, [16]) e o das linguagens testáveis por pedaços que estão em correspondência com os monóides $\mathcal{J}$-triviais (ver, por exemplo, [17]).

O principal objectivo deste trabalho consiste em dar uma caracterização da variedade de linguagens associada à pseudovariedade dos grupos super-resolúveis, isto é, dos grupos que possuem uma série normal com factores cíclicos [9].

Dedicamos o primeiro capítulo deste trabalho à apresentação de conceitos e resultados gerais da Teoria dos Semigrupos e da Teoria dos Grupos, bem como a resultados sobre Álgebras, Representações e Módulos necessários para uma boa compreensão dos capítulos seguintes.

O Capítulo 2 destina-se ao estudo de algumas pseudovariedades de grupos. Começamos por estudar duas caracterizações alternativas da pseudovariedade produto, a primeira utilizando produtos semidirectos (Teorema de Kalouzñin-Krasner) e a segunda, que sai como corolário da primeira, usando produtos em coroa. Seguidamente, damos uma caracterização da pseudovariedade $\mathbf{Ab}^n$ dos grupos abelianos cujo expoente divide um dado natural n. Mostramos que esta pseudovariedade é gerada pelo grupo cíclico $\mathbb{Z}_n$ e determinamos identidades que a definem. Na secção seguinte, caracterizamos a pseudovariedade $\mathbf{G}_p$ dos p-grupos finitos de dois modos distintos: o primeiro em termos de identidades que a definem e o segundo usando p-grupos expressos como quocientes de um monóide livre por uma relação de congruência. Na quarta secção, dada uma potência q de um número primo p, caracterizamos a pseudovariedade $\mathbf{G}_p * \mathbf{Ab}^{q-1}$, em termos de pseudoidentidades. Mostramos também que no caso particular $q = p$ esta pseudovariedade de grupos pode ser descrita utilizando os subgrupos standard de Borel $B_n(\mathbb{Z}_p)$. Os resultados principais deste capítulo aparecem na última secção e destinam-se a caracterizar a pseudovariedade dos grupos super-resolúveis, a qual pode descrever-se, por exemplo, como sendo o supremo de todas as pseudovariedades $\mathbf{G}_p * \mathbf{Ab}^{p-1}$, em que p percorre o conjunto dos números primos. A segunda caracterização apresentada diz que a pseudovariedade dos grupos super-resolúveis é gerada pelos subgrupos de Borel $B_n(\mathbb{Z}_p)$, para todo o natural n e todo o número primo p.

No Capítulo 3 descrevemos algumas variedades de linguagens associadas a certas classes de grupos, em particular às pseudovariedades $\mathbf{Ab}^n$ e $\mathbf{G}_p$, o que nos prepara para a caracterização das linguagens reconhecidas pelos grupos super-resolúveis. Começamos por apresentar duas caracterizações das linguagens reconhecidas por grupos em $\mathbf{Ab}^n$: a primeira diz-nos que uma tal linguagem pertence à álgebra de Boole gerada pelas linguagens da forma $F(a, k, n) = \{u \in A^* : |u|_a \equiv k \pmod{n}\}$, em que $a \in A$ e $0 \leq k < n$, e a segunda diz que é união disjunta de linguagens comutativas n-elementares. Na secção seguinte caracterizamos a variedade de linguagens associada à pseudovariedade de grupos $\mathbf{G}_p$, mostrando que uma linguagem de A^* é reconhecida por um p-grupo se e só se é uma combinação Booleana de linguagens da forma $S(u, r, p) = \{w \in A^* : \binom{w}{u} \equiv r \pmod{p}\}$, em que $u \in A^*$ e $0 \leq r < p$. É objectivo da terceira secção demonstrar o Princípio do Produto em Coroa de Straubing, que nos fornece uma descrição das linguagens reconhecidas pelo produto em coroa de dois monóides, e apresentar uma versão deste resultado para variedades de linguagens. Este princípio tem numerosas aplicações, incluindo a caracterização de Schützenberger das

linguagens sem estrela.

Recordemos que o Teorema da Variedade de Eilenberg nos diz que, de uma certa forma, as variedades de linguagens racionais estão em correspondência bijectiva com as pseudovariedades de monóides. Esta correspondência estende-se a operações entre linguagens e entre monóides. Na última secção deste capítulo, consideramos o caso especial do produto de linguagens com contador, que foi apresentado pela primeira vez por Straubing (ver [23]), e descrevemos a operação associada entre monóides.

Finalmente, o último capítulo deste trabalho é dedicado à caracterização das linguagens reconhecidas por grupos super-resolúveis. Essa caracterização será feita de dois modos distintos: primeiro, mostramos que uma tal linguagem pertence à álgebra de Boole gerada por produtos modulares concatenados de linguagens comutativas elementares; segundo, provamos que as linguagens reconhecidas por grupos super-resolúveis são combinações Booleanas de linguagens da forma $r\tau^{-1}$, em que p é um número primo, $r \in \mathbb{Z}_p$ e $\tau : A^* \to \mathbb{Z}_p$ é uma função realizada por algum transdutor na forma triangular estrita.

O trabalho desenvolvido nesta dissertação teve por base o artigo de O. Carton, J.-E. Pin e X. S.-Escrivà [9], tendo requerido um vasto estudo de conceitos e resultados que surgem em diversas áreas da Álgebra, por vezes adaptados para poderem ser aplicados no estudo de [9].

Capítulo 1

Preliminares

O objectivo deste capítulo consiste em dar as principais definições e resultados necessárias ao longo deste trabalho. Tentaremos expôr os assuntos de forma a tornar o texto o mais autocontido possível. Apresentaremos no final todas as referências bibliográficas onde tais resultados podem ser encontrados.

Os semigrupos e monóides que iremos considerar em toda esta dissertação são finitos ou livres e os grupos são finitos.

1.1 Semigrupos e Monóides

Nesta secção apresentaremos alguns conceitos matemáticos necessários posteriormente. Nela revemos as definições de semigrupo, monóide, grupo, morfismo e congruência, bem como a construção de uma operação em monóides, o produto semidirecto, que será de grande utilidade no que se segue.

Se A é um conjunto finito denotamos o seu *cardinal* por $|A|$ ou $\text{card}(A)$.

Sejam A e B conjuntos. Uma *relação* ρ de A para B é um subconjunto do produto cartesiano $A \times B$. Diz-se que a e b estão *ρ-relacionados* se $(a, b) \in \rho$. Geralmente escreve-se $a\rho b$ em vez de $(a, b) \in \rho$.

Uma relação $\rho \subseteq A \times A$ diz-se uma *relação de equivalência* se, para quaisquer $a, b, c \in A$,

(1) $a\rho a$ (*reflexividade*);

(2) se $a\rho b$ então $b\rho a$ (*simetria*);

(3) se $a\rho b$ e $b\rho c$ então $a\rho c$ (*transitividade*).

Seja ρ uma relação de equivalência em A e $a \in A$. Define-se *classe de equivalência*, ou *ρ-classe*, contendo a por

$$[a]_\rho = \{x \in A : x\rho a\}.$$

Por vezes também se denota a ρ-classe de um elemento $a \in A$ por $a\rho$.

Observe-se que o conjunto de todas as ρ-classes forma uma *partição* do conjunto A, no sentido em que cada elemento de A pertence a uma e uma só ρ-classe.

As noções de relação de equivalência e de partição estão completamente interligadas. Dada uma equivalência ρ em A, denota-se por A/ρ o conjunto das ρ-classes de A, isto é,

$$A/\rho = \{[a]_\rho : a \in A\}.$$

Pelo que foi dito atrás, A/ρ constitui uma partição do conjunto A e designamos este conjunto por *conjunto quociente de A por ρ*.

Diz-se que uma relação φ de A para B é uma *aplicação* se, para todo o $a \in A$, existe um único $b \in B$ tal que $(a, b) \in \varphi$. O único b que corresponde a um dado a chama-se *imagem* de a pela aplicação φ e denota-se por $(a)\varphi$. Em geral escrevemos simplesmente $a\varphi$ para simplificar a escrita. O conjunto A designa-se por *domínio* de φ e denota-se por $dom\varphi$. Para indicar que φ é uma aplicação escrevemos $\varphi : A \to B$ em vez de $\varphi \subseteq A \times B$. Diz-se que $\varphi : A \to A$ é uma *função* se dom$\varphi \subseteq A$.

Uma aplicação $\varphi : A \to B$ diz-se *injectiva* se, para quaisquer $a, b \in A$,

$$a_1\varphi = a_2\varphi \Rightarrow a_1 = a_2.$$

Uma aplicação $\varphi : A \to B$ diz-se *sobrejectiva* se

$$\forall b \in B\ \exists a \in A \quad a\varphi = b.$$

Uma aplicação φ diz-se *bijectiva* se é simultaneamente injectiva e sobrejectiva, isto é:

$$\forall b \in B\ \exists! a \in A \quad a\varphi = b.$$

Se $\varphi : A \to B$ e $\psi : B \to C$ são aplicações, então a *composição* de φ e ψ, que se denota por $\varphi \circ \psi$, é uma aplicação de A para C definida por:

$$a(\varphi \circ \psi) = (a\varphi)\psi, \qquad \text{para todo o } a \in A.$$

Note-se que escrevemos o símbolo das aplicações do lado direito. Deste modo, para calcular a composição $\varphi \circ \psi$, aplicamos primeiro φ seguido de ψ. Em geral escrevemos simplesmente $\varphi\psi$.

Para finalizar recordemos que associado a uma aplicação $\varphi : A \to B$ temos a relação de equivalência em A definida por

$$\ker \varphi = \{(a, a') \in A \times A : a\varphi = a'\varphi\},$$

que se designa por *equivalência nuclear de* φ.

Seja S um conjunto não vazio e suponhamos que está definida em S uma *operação binária*, isto é, uma aplicação $\beta : S \times S \to S$.

Usualmente utilizam-se as notações multiplicativa $x \cdot y$ (ou simplesmente xy) e aditiva $x + y$, e a operação designa-se por "multiplicação" e "adição", respectivamente. Para o que se segue fixemos a notação multiplicativa. Diz-se que $(S, \cdot)$, ou simplesmente S, é um *semigrupo* se a operação binária $\cdot$ é *associativa*, isto é, se

$$(a \cdot b) \cdot c = a \cdot (b \cdot c), \qquad \text{para quaisquer } a, b, c \in S.$$

Um semigrupo $(S, \cdot)$ diz-se um *monóide*, se existe um elemento $1 \in S$ tal que

$$1 \cdot a = a = a \cdot 1, \qquad \text{para qualquer } a \in S.$$

O elemento 1 designa-se por *elemento identidade de* S.

Seja $(S, \cdot)$ um semigrupo tal que $|S| \geq 2$. Um elemento $0 \in S$ diz-se um *zero de* S se,

$$0 \cdot a = 0 = a \cdot 0, \qquad \text{para qualquer } a \in S.$$

Note-se que existe, quando muito, um elemento identidade e um zero em S.

Para subconjuntos A e B de um semigrupo S definimos

$$AB = \{ab : a \in A,\, b \in B\}.$$

Se um dos conjuntos A ou B é singular podemos simplificar a notação: se A e B são subconjuntos de S e a e b são elementos de S, então

$$Ab = \{ab : a \in A\},\ aB = \{ab : b \in B\}.$$

Se S é um semigrupo, um subconjunto $T \neq \emptyset$ de S diz-se um *subsemigrupo de* S se é fechado em relação à operação, isto é, se

$$a, b \in T \Rightarrow a \cdot b \in T.$$

Se S é um monóide, diz-se que um subsemigrupo T de S é um *submonóide* de S se $1 \in S$.

Um monóide G diz-se um *grupo* se verifica a seguinte condição

$$\forall x \in G\ \exists y \in G: \qquad xy = 1 = yx.$$

O elemento y é de facto univocamente determinado pelo elemento x. Assim, por vezes denota-se o elemento y associado deste modo a x por x^{-1} e designa-se por *inverso de* x.

Diz-se que $(G, \cdot)$ é um *grupo comutativo ou abeliano* se a operação binária é comutativa, isto é, se

$$a \cdot b = b \cdot a, \qquad \text{para quaisquer } a, b \in S.$$

Se o conjunto G for finito, diz-se que G é um *grupo finito* e chama-se *ordem* de G a $|G|$. Caso contrário, diz-se que G é um *grupo infinito*.

A um subsemigrupo H de um semigrupo G que seja ele próprio um grupo dá-se o nome de *subgrupo de* G e denota-se por $H \leq G$. Se $H \leq G$ e $H \neq G$ escrevemos $H < G$ e dizemos que H é *subgrupo próprio de* G.

Num semigrupo S um elemento $e \in S$ com a propriedade $e^2 = e$ designa-se por *idempotente de* S. Claramente tais elementos são tais que $e = e^2 = e^3 = \ldots$.

A análise das potências dos elementos num semigrupo finito leva-nos ao seguinte resultado:

Teorema 1.1.1. [16, 20] *Todo o elemento num semigrupo finito tem uma potência que é um idempotente.*

Sejam S e T semigrupos. Uma aplicação $\varphi : S \to T$ diz-se um *morfismo de semigrupos*, ou simplesmente um *morfismo*, se para quaisquer $x, y \in S$,

$$(xy)\varphi = (x\varphi)(y\varphi). \tag{1.1}$$

Se $S = T$ diz-se que φ é um *endomorfismo*. Se φ é um morfismo injectivo (respectivamente sobrejectivo, bijectivo) então diz-se que φ é um *monomorfismo* (respectivamente *epimorfismo, isomorfismo*) de semigrupos. Se existir um isomorfismo entre os semigrupos S e T, estes dizem-se *isomorfos* e escrevemos $S \simeq T$. Se φ é um endomorfismo bijectivo diz-se que φ é um *automorfismo*.

Se S e T são monóides com elementos identidade 1_S e 1_T, respectivamente, então $\varphi : S \to T$ diz-se um *morfismo de monóides* se verifica (1.1) e, além disso,

$$1_S\varphi = 1_T.$$

Dados S e T semigrupos, designa-se por *produto directo* (*externo*) de S e T o semigrupo que se obtém considerando no produto cartesiano $S \times$

T a operação dada por $(s_1, t_1)(s_2, t_2) = (s_1 s_2, t_1 t_2)$, para todos os pares $(s_1, t_1), (s_2, t_2) \in S \times T$. Esta operação mune $S \times T$ com estrutura de semigrupo que se denota simplesmente por $S \times T$.

Se S e T são monóides, $S \times T$ é um monóide em que o elemento identidade é o par $(1_S, 1_T)$, sendo 1_S e 1_T os elementos identidade de S e T, respectivamente.

Mais geralmente, se I é um conjunto, $(S_i)_{i \in I}$ é uma família de semigrupos, designa-se por *produto directo* da família $(S_i)_{i \in I}$, e denota-se por

$$\prod_{i \in I} S_i,$$

o produto cartesiano dos semigrupos S_i, munido da operação definida por

$$(s_i)_{i \in I}(s'_i)_{i \in I} = (s_i s'_i)_{i \in I}.$$

Sejam S e T monóides. Por *acção* (*à esquerda*) de T sobre S entende-se uma aplicação

$$\begin{array}{rcl} T \times S & \longrightarrow & S \\ (t, s) & \longmapsto & t \cdot s \end{array}$$

satisfazendo as propriedades seguintes:

(1) $1_T \cdot s = s$, para qualquer $s \in S$;

(2) $t_1 \cdot (t_2 \cdot s) = (t_1 t_2) \cdot s$, para quaisquer $s \in S$ e $t_1, t_2 \in T$.

Dualmente definimos *acção* (*à direita*) de T sobre S.

Diz-se que T actua sobre S *por endomorfismos* se a acção também verifica a condição

$$t \cdot (s_1 s_2) = (t \cdot s_1)(t \cdot s_2), \text{ para } t \in T \text{ e } s_1, s_2 \in S, \tag{1.2}$$

isto é, cada $t \in T$ define um endomorfismo de T.

Tenha-se presente que a propriedade (1.2) em notação aditiva se traduz por $t \cdot (s_1 + s_2) = (t \cdot s_1) + (t \cdot s_2)$.

A acção diz-se *unitária à direita* se $t \cdot 1_S = 1_S$, para qualquer $t \in T$.

Podemos agora definir uma outra operação entre monóides.

Sejam S e T monóides. Considere-se uma acção (à esquerda) de T sobre S por endomorfismos e unitária à direita. Define-se em $S \times T$ uma operação binária por

$$(s_1, t_1)(s_2, t_2) = (s_1(t_1 \cdot s_2), t_1 t_2), \text{ para } s_1, s_2 \in S \text{ e } t_1, t_2 \in T.$$

Com esta operação $S \times T$ é um monóide em que a identidade é o elemento $(1_S, 1_T)$. Este monóide designa-se por *produto semidirecto* (*externo*) dos monóides S e T e denota-se por $S \rtimes T$.

Uma relação de equivalência ρ num semigrupo S diz-se uma *relação de congruência* se respeita o produto, i.e. se, para quaisquer $a, b, c \in S$,

$$a\rho b \Rightarrow ca\rho cb,\ ac\rho bc.$$

Alternativamente, uma equivalência ρ é uma congruência se, para quaisquer $a, b, c, d \in S$,

$$a\rho b,\ c\rho d \Rightarrow ac\rho bd.$$

Seja ρ uma relação de congruência num semigrupo ou num monóide S e considere-se o conjunto quociente S/ρ constituído por todas as ρ-classes $[a]_\rho$ (para cada $a \in S$). A propriedade de congruência permite definir uma operação binária $\cdot$ em S/ρ por, para cada $a, b \in S$,

$$[a]_\rho \cdot [b]_\rho = [ab]_\rho.$$

Esta operação é claramente associativa pelo que S/ρ é também um semigrupo. Mais, se S é um monóide com elemento identidade 1_S, então S/ρ é um monóide com elemento identidade $[1_S]_\rho$.

Um exemplo clássico e muito importante de relação de congruência é a *congruência aritmética* $\equiv_n$ $(n \geq 2)$ em $S = (\mathbb{Z}, +)$ e também em $(\mathbb{Z}, \cdot)$ definida por, para $a, b \in \mathbb{Z}$,

$$a \equiv_n b \Longleftrightarrow a \equiv b \pmod{n},$$

ou seja,

$$a \equiv_n b \Leftrightarrow n \text{ divide } b - a \Leftrightarrow \exists k \in \mathbb{Z} \quad b - a = kn.$$

Diz-se que $a, b \in \mathbb{Z}$ são *congruentes módulo* n se $a \equiv b \pmod{n}$. É fácil verificar que qualquer inteiro é congruente, módulo n, com um e um só dos inteiros $0, 1, 2, \ldots, n-1$. Assim, o conjunto quociente $\mathbb{Z}/\equiv_n$ tem exactamente n classes. Este quociente designa-se por $\mathbb{Z}_n$ e utilizaremos a notação seguinte

$$\mathbb{Z}_n = \{\overline{0}, \overline{1} \ldots, \overline{n-1}\}.$$

Em $\mathbb{Z}_n$ define-se uma "adição" e uma "multiplicação" da seguinte forma, para $a, b \in \mathbb{Z}$,

$$\overline{a} + \overline{b} = \overline{a+b}$$

$$\overline{a} \cdot \overline{b} = \overline{ab}$$

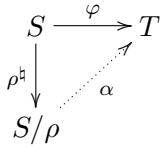
Dado um semigrupo S e uma congruência ρ em S, a aplicação $\rho^\natural : S \to S/\rho$ definida por $a\rho^\natural = [a]_\rho$, para cada $a \in S$, é um morfismo sobrejectivo,

usualmente designado por *epimorfismo canónico*. É claro que a equivalência nuclear associada a $\rho^\natural$ é exactamente ρ:

$$\ker \rho^\natural = \{(x,y) \in S \times S : x\rho^\natural = y\rho^\natural\} = \{(x,y) \in S \times S : x\rho y\} = \rho.$$

Assim, se por um lado, uma congruência ρ num semigrupo S conduz de forma natural a um morfismo $\rho^\natural$, um morfismo de semigrupos $\varphi : S \to T$ define uma relação de congruência $\ker \varphi$ em S.

Teorema 1.1.2 (Teorema do Homomorfismo)**.** [16, 20] *Sejam S e T monóides, $\varphi : S \to T$ um morfismo e $\rho = \ker \varphi$. Então existe um morfismo injectivo $\alpha : S/\rho \to T$ com $im\alpha = im\varphi$ e tal que o seguinte diagrama*



é comutativo, isto é, $\varphi = \rho^\natural\alpha$.

Seja $(\sim_i)_{i\in I}$ uma família de congruências sobre um monóide S, denota-se por $\sim = \bigcap_{i\in I} \sim_i$ a sua intersecção. Temos $u \sim v$ se e só se $u \sim_i v$ para todo o $i \in I$, com $u, v \in S$.

Proposição 1.1.3. [20] *Sejam S um monóide, $(\sim_i)_{i\in I}$ uma família de congruências sobre S e $\sim = \bigcap_{i\in I} \sim_i$ a sua intersecção. Então $S/\sim$ é isomorfo a um submonóide de*

$$\prod_{i\in I} S/\sim_i .$$

Se S e T são monóides, diz-se que S *divide* T, e escreve-se $S \mid T$, se existe um submonóide U de T e um morfismo sobrejectivo $\varphi : U \twoheadrightarrow S$. Note-se que a relação divide é uma relação binária reflexiva e transitiva.

1.2 Semigrupos e Monóides Livres

As estruturas livres são fundamentais na Teoria das Linguagens Formais. Aqui apresentamos os conceitos de semigrupo e de monóide livres, bem como a importância algébrica destas estruturas, que se traduz pela Propriedade Universal que satisfazem.

No contexto seguinte, é frequente referirmo-nos a um conjunto $A \neq \emptyset$ por um *alfabeto* e aos seus elementos por *letras*. Se A é um alfabeto, define-se A^+ como sendo o conjunto das sequências finitas

$$(a_1, a_2, \ldots, a_n), \text{ em que } a_1, a_2, \ldots, a_n \in A\, (n \geq 1).$$

O conjunto A^+ torna-se um semigrupo se nele se definir uma operação binária por $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_m) = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m)$, para $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$.

É fácil verificar que esta operação é associativa. Além disso, as sequências de comprimento 1 geram o semigrupo A^+ pois cada elemento $(a_1, a_2, \ldots, a_n)$ escreve-se como produto finito das sequências de comprimento 1 de A^+ $(a_1), (a_2), \ldots, (a_n)$.

É conveniente encarar os elementos de A^+ como sendo as *palavras* $a_1 a_2 \ldots a_n$ no alfabeto A.

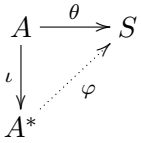
A multiplicação definida em cima corresponde apenas a uma justaposição $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_m) = a_1 a_2 \ldots a_n b_1 b_2 \ldots b_m$, esta operação chama-se *concatenação*.

O semigrupo A^+ é designado por *semigrupo livre no conjunto* A.

É frequente adicionar um elemento identidade 1 a A^+ de forma a obter um monóide A^*, que se designa por *monóide livre no conjunto* A. Interpreta-se 1 como sendo a *palavra vazia* (sem letras) no alfabeto A.

Algebricamente, a importância dos monóides livres reside na *propriedade universal sobre* A que satisfazem, que pode ser enunciada do seguinte modo:

Teorema 1.2.1. [16] *Sejam A um alfabeto, $(S, \cdot, 1)$ um monóide, $\theta : A \to S$ uma aplicação e $\iota : A \to A^*$, $a \to a$. Então existe um único morfismo $\varphi : A^* \to S$ tal que o seguinte diagrama*



é comutativo, isto é, $\theta = \iota\varphi$.

No teorema anterior a condição "o diagrama é comutativo" significa que φ coincide com θ no conjunto A. Nestas condições diz-se que φ *estende* θ, ou que θ *é a restrição* $\varphi_{|_A}$ *de* φ *a* A.

Um resultado análogo é válido para semigrupos, com A^+ no lugar de A^*.

Dado um alfabeto finito A chama-se *linguagem* (*formal*) *sobre* A a qualquer subconjunto do monóide livre A^*.

Se $A = \{a\}$ escreve-se simplesmente a^* e a^+ em vez de $\{a\}^*$ e $\{a\}^+$, respectivamente. Assim, $a^* = \{1, a, a^2, \cdots\}$ e $a^+ = \{a, a^2, a^3, \cdots\}$.

Se $\omega \in A^*$, escreve-se $|\omega|$ para representar o *comprimento de* ω definido do seguinte modo:

$$\begin{cases} |1| = 0 \\ |a_1 a_2 \ldots a_n| = n, \qquad n \in \mathbb{N},\ a_1, a_2, \ldots, a_n \in A \end{cases}$$

Note-se que se $\omega, z \in A^*$, então $|\omega z| = |\omega| + |z|$.

Se $\omega \in A^*$ e $a \in A$ então $|\omega|_a$ denota o *número de ocorrências de a em* ω, que se define recursivamente do seguinte modo:

$$\begin{cases} |1|_a = 0 \\ |vb|_a = \begin{cases} |v|_a & \text{, se } a \neq b \\ |v|_a + 1 & \text{, se } a = b \end{cases} \end{cases} \quad \text{, para } v \in A^*,\ b \in A.$$

1.3 Autómatos finitos e o Teorema de Kleene

O estudo das linguagens racionais está intrinsecamente relacionado com o estudo dos autómatos finitos. Nesta secção definimos os conceitos de autómato, linguagem reconhecível e linguagem racional e enunciamos o Teorema de Kleene, o qual nos garante que as linguagens reconhecidas por autómatos finitos são precisamente as linguagens racionais.

Um *autómato* é um quíntuplo $\mathcal{A} = (Q, A, E, I, F)$, em que

- Q é um conjunto de *estados*;
- A é um alfabeto (conjunto finito e não vazio);
- $E \subseteq Q \times A \times Q$ é o conjunto das *transições*;
- $I \subseteq Q$ é o conjunto dos *estados iniciais*;
- $F \subseteq Q$ é o conjunto dos *estados finais*.

Se Q for finito, diz-se que o autómato $\mathcal{A}$ é *finito*.
Uma transição $(p, a, q) \in E$ pode ser representada por $p \xrightarrow{a} q$.
Duas transições (p, a, q) e (p', a', q') dizem-se *consecutivas* se $p = q'$.

$$p \xrightarrow{a} q = p' \xrightarrow{a'} q'.$$

Um *caminho* é uma sequência finita de transições consecutivas,

$$(q_0, a_1, q_1)(q_1, a_2, q_2) \dots (q_{n-1}, a_n, q_n)$$

também representado por

$$q_0 \xrightarrow{a_1} q_1 \xrightarrow{a_2} q_2 \longrightarrow \cdots \longrightarrow q_{n-1} \xrightarrow{a_n} q_n,$$

a q_0 dá-se o nome de *origem* do caminho, a q_n de *extremidade*, a n de *comprimento* e a $a_1 a_2 \dots a_n$ de *etiqueta* do caminho.

Note-se que uma transição é um caminho de comprimento um. Convenciona-se que, para cada $q \in Q$, $(q, 1, q)$ é também um caminho que tem

etiqueta 1 e comprimento zero, mas não é uma transição.

Um *caminho* em $\mathcal{A}$ diz-se *bem sucedido* se a sua origem for um estado inicial e a sua extremidade um estado final.

Diz-se que uma palavra $w \in A^*$ é *reconhecida pelo autómato* $\mathcal{A}$ se for etiqueta de um caminho bem sucedido.

Define-se *linguagem reconhecida por um autómato* $\mathcal{A}$ como sendo a linguagem

$$L(\mathcal{A}) = \{w \in A^* : w \text{ é reconhecida por } \mathcal{A}\}.$$

Uma linguagem $L \subseteq A^*$ diz-se *reconhecida por um autómato finito* se existe um autómato finito $\mathcal{A}$ que a reconhece, isto é, tal que $L = L(\mathcal{A})$.

Uma linguagem diz-se *reconhecível* se é reconhecida por um autómato finito.

Dois autómatos $\mathcal{A}$ e $\mathcal{B}$ sobre o mesmo alfabeto finito A dizem-se *equivalentes* se reconhecem a mesma linguagem, isto é, se $L(\mathcal{A})$=$L(\mathcal{B})$.

Um autómato $\mathcal{A} = (Q, A, E, I, F)$ em que o conjunto dos estados iniciais é um conjunto singular $I = \{i\}$ diz-se *determinista* se verificar a condição seguinte:

Para quaisquer $p \in Q$ e $a \in A$, existe no máximo uma transição da forma (p, a, q).

Um autómato que não seja determinista diz-se *não determinista*.

Sejam $\mathcal{A} = (Q, A, E, \{i\}, F)$ um autómato determinista e

$$\begin{aligned} P &= \{(p, a) : \text{existe em } \mathcal{A} \text{ uma transição da forma } (p, a, q)\} \\ &= \{(p, a) : \exists q \in Q \quad (p, a, q) \in E\}, \end{aligned}$$

podemos considerar a aplicação

$$\begin{aligned} \varphi : P &\longrightarrow Q \\ (p, a) &\longrightarrow (p, a)\varphi, \end{aligned}$$

em que $(p, a)\varphi$ é o único estado $q \in Q$ tal que $(p, a, q) \in E$.

Habitualmente, representa-se φ por $\cdot$ e $(p, a)\varphi$ por $p \cdot a$ ou simplesmente pa. Designa-se φ por *função de transição* de $\mathcal{A}$.

Um autómato determinista será representado por um quíntuplo $\mathcal{A} = (Q, A, \cdot, i, F)$, sendo $\cdot$ a função de transição e i o único estado inicial.

É possível "prolongar" a função de transição às palavras: dados $p \in Q$, $u \in A^*$ e $a \in A$,

$$\begin{cases} p \cdot 1 = p \\ p \cdot (ua) = (p \cdot u) \cdot a \qquad \text{, se } p \cdot u \text{ e } (p \cdot u) \cdot a \text{ estiverem definidos} \end{cases}$$

Assim, se $\mathcal{A} = (Q, A, \cdot, i, F)$ é um autómato determinista tem-se

$$L(\mathcal{A}) = \{u \in A^* : i \cdot u \text{ está definida e } i \cdot u \in F\}.$$

Um autómato $\mathcal{A} = (Q, A, E, I, F)$ diz-se *completo* se, para quaisquer $p \in Q$ e $a \in A$, existe pelo menos uma transição da forma (p, a, q).

Note-se que se $\mathcal{A}$ for determinista e completo, a função de transição tem domínio $Q \times A$, isto é, a acção de uma letra qualquer sobre um estado qualquer existe e está univocamente determinada.

Por vezes pode ser conveniente resumir a acção de A sobre Q por meio de uma tabela. Por exemplo, se $Q = \{1, 2, 3\}$ e $A = \{a, b\}$ pode usar-se a tabela

	a	b
1	2	3
2	3	3
3	3	3

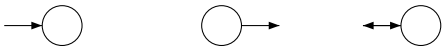
que resume a informação seguinte:

$$1 \cdot a = 2, \qquad 1 \cdot b = 3, \qquad 2 \cdot a = 2 \cdot b = 3, \qquad 3 \cdot a = 3 \cdot b = 3.$$

De uma forma mais conveniente, um autómato pode ser representado graficamente por meio de um diagrama que não é mais do que um grafo orientado etiquetado cujos vértices são os elementos de Q e no qual

$$p \xrightarrow{a} q \qquad \text{é uma aresta se e só se} \qquad p \cdot a = q.$$

Os estados iniciais, finais e simultaneamente iniciais e finais representam-se respectivamente por



Desta forma, o exemplo anterior corresponde ao diagrama para $\mathcal{A} = (\{1, 2, 3\}, \{a, b\}, 1, \{3\})$ representado na figura 1.1. Esse autómato reconhece a linguagem $\{a^2, ab, b\}A^*$.

Seja $A \neq \emptyset$ um conjunto finito. Prova-se muito facilmente (ver [20]) que todos os subconjuntos finitos de A^* são reconhecíveis, no entanto nem todo o subconjunto de A^* é reconhecível. O objectivo desta secção é dar uma descrição das linguagens reconhecíveis.

Dadas linguagens $L_1, L_2 \subseteq A^*$, define-se o seu *produto* (*concatenado*) L_1L_2 da seguinte forma:

$$L_1L_2 = \{uv : u \in L_1, v \in L_2\}.$$

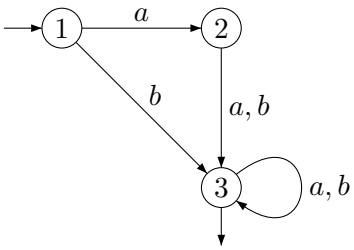


Figura 1.1: Um autómato que reconhece a linguagem $\{a^2, ab, b\}A^*$.

Dada uma linguagem $L \subseteq A^*$ define-se

$$L^* = \{u_1 u_2 \dots u_n : n \geq 0, u_1, u_2, \dots, u_n \in L\},$$

isto é, L^* é o submonóide de A^* gerado por L, esta operação designa-se por *operação estrela* (*de Kleene*).

Uma linguagem $L \subseteq A^*$ diz-se *racional* se pode ser obtida de subconjuntos finitos de A^* através de um número finito de operações de união, produto e estrela.

O conjunto de todos os subconjuntos racionais de A^* denota-se por $\mathrm{Rac}A^*$.

O último resultado desta secção é fundamental no estudo das linguagens racionais:

Teorema 1.3.1 (Teorema de Kleene)**.** [16] *Sejam A um alfabeto finito e $L \subseteq A^*$ uma linguagem de A^*. Então L é um conjunto reconhecível* (*por um autómato finito*) *se e só se L é racional.*

1.4 O Monóide Sintáctico

Um problema abordado pela Teoria das Linguagens Formais tem sido a classificação das linguagens racionais. Uma ferramenta muito importante aplicada nesta tarefa é o monóide sintáctico, que definimos, na primeira parte desta secção, através da noção de congruência sintáctica. Recordamos que, num certo sentido, o monóide sintáctico é o "melhor" monóide que reconhece uma dada linguagem. Na segunda parte, apresentamos as noções de monóide de transformações, bem como uma operação entre estruturas deste tipo. Por fim, definimos monóide de transformações associado a um autómato finito.

1.4.1 A Congruência Sintáctica

Dado um alfabeto finito A e uma linguagem $L \subseteq A^*$ define-se uma congruência em A^* por:

$$\sigma_L = \{(w,z) \in A^* \times A^* : \forall u,v \in A^* \quad uwv \in L \text{ sse } uzv \in L.\}$$

Esta relação designa-se por *congruência sintáctica em* A^*. De facto σ_L é uma relação de congruência. Mais geralmente tem-se o seguinte resultado:

Teorema 1.4.1. [16] *Para qualquer monóide* M *e cada* $P \subseteq M$ *a relação*

$$\sigma_P = \{(x,y) \in M \times M : \forall u,v \in A^* \quad uxv \in P \text{ sse } uyv \in P\} \tag{1.3}$$

é uma relação de congruência em M.

Retomando o caso $M = A^*$ e $L \subseteq A^*$, se σ_L for a congruência sintáctica associada a L define-se o *monóide sintáctico de* L como sendo o monóide quociente

$$Syn(L) = A^*/\sigma_L.$$

Uma nova noção de linguagem reconhecível, neste caso por um monóide, é a seguinte:

Dado um alfabeto finito A e um monóide M, uma linguagem $L \subseteq A^*$ diz-se *reconhecida pelo monóide* M se existem um morfismo $\varphi : A^* \to M$ e um subconjunto $P \subseteq M$ tais que $L = P\varphi^{-1}$. Também se diz que o monóide M *reconhece* L e que o morfismo φ *reconhece* L.

Note-se que uma linguagem $L \subseteq A^*$ é claramente reconhecida pelo seu monóide sintáctico $Syn(L) = A^*/\sigma_L$ pois, considerando o epimorfismo canónico $\sigma_L^\natural : A^* \twoheadrightarrow A^*/\sigma_L$, tem-se

$$P = L\sigma_L^\natural \subseteq A^*/\sigma_L \quad \text{é tal que} \quad P(\sigma_L^\natural)^{-1} = (L\sigma_L^\natural)(\sigma_L^\natural)^{-1} = L.$$

O seguinte resultado demonstra a importância do monóide sintáctico.

Teorema 1.4.2. [16] *Sejam* A *um alfabeto finito e* $L \subseteq A^*$. *As seguintes afirmações são equivalentes:*

(1) L *é uma linguagem racional de* A^*;

(2) *Syn(L) é finito;*

(3) L *é reconhecida por um monóide finito* M.

Veremos no próximo resultado que o monóide sintáctico de uma linguagem L é o "melhor" monóide que a reconhece.

Teorema 1.4.3. [20] *Sejam* A *um alfabeto finito,* $L \subseteq A^*$ *e* M *e* N *monóides. Tem-se:*

(1) M *reconhece* L *se e só se Syn(L) divide* M.

(2) *Se* M *reconhece* L *e* M *divide* N *então* N *reconhece* L.

1.4.2 Monóides de Transformações

Seja Q um conjunto. Denota-se por $\mathcal{T}(Q)$ o conjunto das aplicações $f : Q \to Q$. Se se munir $\mathcal{T}(Q)$ com a operação de composição de aplicações tem-se, de facto, um monóide em que o elemento identidade é a aplicação identidade.

Sejam $(S, \cdot, 1)$ um monóide e Q um conjunto sobre o qual S actua à direita. Se $\cdot : Q \times S \to Q$ é uma acção (à direita) de S sobre Q, então a aplicação $\xi : S \to \mathcal{T}(Q)$ definida por, para cada $s \in S$, $s\xi : Q \to Q$ tal que $(q)s\xi = q \cdot s$, para todo o $q \in Q$, é um morfismo. Por vezes escreve-se ξ_s em vez de $s\xi$ de forma a simplificar a notação.

Se ξ for injectivo, $im\xi$ é um submonóide de $\mathcal{T}(Q)$ e diz-se que (Q, S) é um *monóide de transformações*.

Note-se que o conjunto

$$\tau = \{(s, s') \in S \times S : \forall q \in Q,\ q \cdot s = q \cdot s'\}$$

é uma congruência em S. De facto, $\tau = \ker \xi$. Portanto (Q, S) é um monóide de transformações se $\tau = \{(s, s) : s \in S\}$, a congruência identidade.

Vamos agora apresentar a definição de uma operação em monóides de transformações que será útil no Capítulo 3 e que está intrinsecamente relacionada com a noção de produto semidirecto de monóides definido na Secção 1.1.

Sejam (P, S) e (Q, T) monóides de transformações. Estão definidas duas acções (à direita) de S sobre P e de T sobre Q

$$\begin{array}{rcl} P \times S & \longrightarrow & P \\ (p, s) & \longmapsto & p \cdot s \end{array}$$

e

$$\begin{array}{rcl} Q \times T & \longrightarrow & Q \\ (q, t) & \longmapsto & q \cdot t \end{array}$$

Seja S^Q o conjunto das aplicações de Q em S e nele considere-se uma operação binária definida pelo produto das imagens, i.e. quaisquer que sejam $f_1, f_2 \in S^Q$, $f_1 f_2$ é tal que para todo o $q \in Q$,

$$q(f_1 f_2) = (qf_1)(qf_2).$$

Esta operação mune S^Q com uma estrutura de monóide em que a identidade 1_{S^Q} é a aplicação de Q em S que transforma qualquer elemento q de Q na identidade de S, o qual existe pois S é um monóide.

Definimos uma acção à esquerda de T sobre S^Q da seguinte forma:

$$\begin{array}{rcl} T \times S^Q & \longrightarrow & S^Q \\ (t, f) & \longmapsto & t \cdot f \end{array}$$

em que

$$\begin{array}{rcl} t \cdot f : Q & \longrightarrow & S \\ q & \longmapsto & (q \cdot t)f, \end{array}$$

isto é, $q(t \cdot f) = (q \cdot t)f$, qualquer que seja $q \in Q$.

Note-se que esta acção de T sobre S^Q é uma acção por endomorfismos e é unitária à direita.

No produto cartesiano $S^Q \times T$ consideremos a operação definida por

$$(f_1, t_1)(f_2, t_2) = (f_1(t_1 \cdot f_2), t_1 t_2), \text{ para } f_1, f_2 \in S^Q,\ t_1, t_2 \in T. \qquad (1.4)$$

Obtemos um produto semidirecto externo, $S^Q \rtimes T$.

Seja $(P, S) \circ (Q, T) = (P \times Q, W)$, sendo $W = S^Q \rtimes T$ o produto semidirecto dos monóides S^Q e T que acabámos de definir.

Defina-se agora uma acção à direita de $P \times Q$ sobre $S^Q \rtimes T$ por

$$\begin{array}{rcl} (P \times Q) \times (S^Q \rtimes T) & \longrightarrow & P \times Q \\ ((p, q), (f, t)) & \longmapsto & (p \cdot (qf), q \cdot t) \end{array}$$

É fácil mostrar que esta acção define um morfismo injectivo de $S^Q \rtimes T$ em $\mathcal{T}(P \times Q)$, logo $S^Q \rtimes T$ pode ser encarado como um submonóide de $\mathcal{T}(P \times Q)$. Portanto esta acção define, de facto, um monóide de transformações. Ao monóide $(P, S) \circ (Q, T)$ dá-se o nome de *produto em coroa* dos monóides de transformações (P, S) e (Q, T). Um caso particular que nos vai interessar é aquele em que os monóides de transformações são (S, S) e (T, T), em que as acções são as operações binárias nos monóides. Neste caso, obtemos $(P, S) \circ (Q, T) = (P \times Q, W)$, em que $W = S^T \rtimes T$. O monóide $S^T \rtimes T$, em que a acção de T sobre S^T é a definida acima, designa-se por *produto em coroa* dos monóides S e T e denota-se por $S \circ T$.

Dados uma linguagem $L \subseteq A^*$ e um monóide de transformações (Q, S), diz-se que L *é reconhecida por* (Q, S), ou que (Q, S) *reconhece* L, se existe um morfismo de monóides $\varphi : A^* \to S$, um estado $q_0 \in Q$ e um conjunto $F \subseteq Q$ tais que

$$L = \{u \in A^* : q_0 \cdot (u\varphi) \in F\}.$$

Terminamos esta subsecção com a definição de monóide de transformações de um autómato.

Observemos em primeiro lugar que todo o autómato é equivalente a um autómato determinista e completo (ver [16]).

Seja $\mathcal{A} = (Q, A, \cdot, i, F)$ um autómato determinista e completo. A aplicação $Q \times A \to Q$, $(q, a) \mapsto q \cdot a$ define uma acção à direita de Q sobre A. Esta acção prolonga-se de forma natural a A^* pelo que se tem um morfismo

$\xi : A^* \to \mathcal{T}(Q)$ definido por, para cada $u \in A^*$, $u\xi : Q \to Q$ é tal que $(q)u\xi = q \cdot u$, para todo o $q \in Q$. Tem-se

$$\tau = \{(u, v) \in A^* \times A^* : \forall q \in Q,\ q \cdot u = q \cdot v\} = \ker \xi$$

e do Teorema do Homomorfismo (1.1.2) resulta que $A^*/\tau \simeq A^*\xi$. Portanto $(Q, A^*/\tau)$ é um monóide de transformações que se designa por *monóide de transformações do autómato* $\mathcal{A}$.

1.5 Pseudovariedades

O objectivo desta secção é apresentar a noção de pseudovariedade de monóides. Referimos também dois resultados que caracterizam as pseudovariedades de monóides geradas por uma família de monóides.

Uma classe $\mathbf{V}$ de monóides finitos diz-se uma *pseudovariedade de monóides* se $\{1\} \in \mathbf{V}$ e além disso verifica as condições seguintes:

(1) Se $A \in \mathbf{V}$ e B é um submonóide de A então $B \in \mathbf{V}$;

(2) Se $A \in \mathbf{V}$, B é um monóide e $\varphi : A \twoheadrightarrow B$ é um epimorfismo então $B \in \mathbf{V}$;

(3) Se $A, B \in \mathbf{V}$ então $A \times B \in \mathbf{V}$.

Note-se que a propriedade dada por (3) estende-se a produtos directos finitos arbitrários:

$$\text{Se } A_1, A_2, \ldots, A_n \in \mathbf{V} \text{ então } A_1 \times A_2 \times \cdots \times A_n \in \mathbf{V}.$$

Por vezes pode ser útil juntar as propriedades (1) e (2), que podem ser substituídas pela seguinte:

$$\text{Se } A \in \mathbf{V} \text{ e } B \text{ divide } A \text{ então } B \in \mathbf{V}.$$

Seja $I \neq \emptyset$ um conjunto (finito ou infinito). Seja $(\mathbf{V}_i)_{i \in I}$ uma família de pseudovariedades de monóides. Então

$$\mathbf{V} = \bigcap_{i \in I} \mathbf{V}_i$$

é também uma pseudovariedade de monóides.

Considere-se agora uma família de monóides finitos $(M_j)_{j \in J}$, em que J pode ser finito ou infinito mas $J \neq \emptyset$. Seja $\mathbf{V}$ a intersecção de todas as pseudovariedades contendo a família $(M_j)_{j \in J}$. Note-se que a colecção de pseudovariedades que contêm todos os M_j é não vazia uma vez que, no caso mais extremo, ela contém a classe de todos os monóides finitos que

é uma pseudovariedade de monóides. Pelo que foi dito atrás, $\mathbf{V}$ é uma pseudovariedade contendo todos os M_j, e é a mais pequena pseudovariedade com esta propriedade.

Designa-se a mais pequena pseudovariedade que contém uma dada família de monóides finitos $(M_j)_{j\in J}$ por *pseudovariedade gerada* pelos monóides M_j e escreve-se

$$\mathbf{V} = \mathbf{V}\langle M_j : j \in J\rangle .$$

O seguinte resultado dá uma caracterização dos monóides desta pseudovariedade:

Teorema 1.5.1. [16] *Seja $\boldsymbol{V}\langle M_j : j \in J\rangle$ a pseudovariedade gerada pela família de monóides finitos $(M_j)_{j\in J}$. Então $A \in \boldsymbol{V}\langle M_j : j \in J\rangle$ se e só se existem $j_1, j_2, \ldots, j_n \in J$ tais que A divide $M_{j_1} \times M_{j_2} \times \cdots \times M_{j_n}$.*

Tendo em conta o teorema anterior concluímos que

$$\begin{aligned}&\mathbf{V}\langle M_j : j \in J\rangle = \\ &= \{M : \exists n \geq 0, \exists M_{j_1}, M_{j_2}, \ldots, M_{j_n}, M \mid M_{j_1} \times M_{j_2} \times \cdots \times M_{j_n}\}.\end{aligned}$$

Sejam $X = \{x_1, x_2, \ldots\}$ um alfabeto numerável (finito ou infinito) e $u, v \in X^*$ elementos distintos de X^*. Diz-se que um monóide M *satisfaz a identidade* $u = v$ se $u\varphi = v\varphi$, para qualquer morfismo de monóides $\varphi : X^* \to M$.

Se $((u_n, v_n))_{n\geq 1}$ é uma sequência (finita ou infinita) de pares de elementos distintos de X^*, então pode considerar-se a classe $\mathcal{C}$ de todos os monóides finitos que satisfazem as identidades $u_n = v_n$ $(n \geq 1)$. Diz-se que a classe $\mathcal{C}$ é *definida pelas identidades* $u_n = v_n$ $(n \geq 1)$. Facilmente se verifica que $\mathcal{C}$ é uma pseudovariedade que se denota por

$$\mathbf{V}\left[u_n = v_n\,(n \geq 1)\right].$$

Uma classe $\mathcal{C}$ de monóides finitos diz-se *ultimamente definida pelas identidades* $u_n = v_n$ $(n \geq 1)$ se consiste precisamente nos monóides finitos que satisfazem as identidades $u_n = v_n$, para todo o n a partir de certa ordem.

Trata-se, de facto, de uma pseudovariedade de monóides que denotamos por

$$\mathbf{V}\left[\!\left[u_n = v_n\,(n \geq 1)\right]\!\right].$$

Para mais pormenores ver [16].

Um resultado que vai ser útil posteriormente é o seguinte:

Proposição 1.5.2. [20] *Toda a pseudovariedade de monóides gerada por um único monóide é definida por uma sequência de identidades.*

1.6 Variedades de Linguagens

O Teorema da Variedade de Eilenberg, que irá ser enunciado posteriormente, permite classificar as linguagens reconhecíveis por meio das propriedades dos seus monóides sintácticos. Nesta secção apresentamos a noção de variedade de linguagens bem como algumas formas de descrever uma classe específica de linguagens racionais.

Se $\mathbf{V}$ é uma pseudovariedade de monóides e se A é um alfabeto finito, denota-se por $A^*\mathcal{V}$ o conjunto das linguagens de A^* cujo monóide sintáctico está em $\mathbf{V}$, isto é:

$$A^*\mathcal{V} = \{L \subseteq A^* : Syn(L) \in \mathbf{V}\}.$$

Note-se que, pelo Teorema 1.4.2, as linguagens de $A^*\mathcal{V}$ são racionais, desde que os seus monóides sintácticos sejam finitos.

Um outro critério para uma dada linguagem pertencer a $A^*\mathcal{V}$ é o seguinte:

Teorema 1.6.1. [16, 20] *Sejam $\boldsymbol{V}$ uma pseudovariedade de monóides, A um alfabeto finito e $A^*\mathcal{V}$ o conjunto das linguagens de A^* cujo monóide sintáctico está em $\boldsymbol{V}$. Então $L \in A^*\mathcal{V}$ se e só se L é reconhecida por um monóide em $\boldsymbol{V}$.*

Uma *classe de linguagens racionais* é uma aplicação $\mathcal{C}$ que associa a cada alfabeto finito A um conjunto $A^*\mathcal{C}$ de linguagens racionais de A^*, isto é, $A^*\mathcal{C} \subseteq Rac(A^*)$.

A correspondência $\mathbf{V} \to \mathcal{V}$ permite associar a cada pseudovariedade de monóides uma classe de linguagens racionais.

Se M é um monóide, $X \subseteq M$ arbitrário, $u \in M$, define-se o *residual esquerdo de X por u*

$$u^{-1}X = \{s \in M : us \in X\}.$$

De forma análoga define-se $Xu^{-1} = \{s \in M : su \in X\}$.

Uma *variedade de linguagens* é uma classe de linguagens racionais $\mathcal{V}$ tal que:

(1) Para todo o alfabeto finito A, a classe $A^*\mathcal{V}$ contém A^* e é fechada para as operações de união e complementação ($A^*\mathcal{V}$ forma uma álgebra de Boole);

(2) Se A e B são alfabetos finitos, $\varphi : A^* \to B^*$ é um morfismo de monóides livres e $L \in B^*\mathcal{V}$ então $L\varphi^{-1} \in A^*\mathcal{V}$;

(3) Se A é um alfabeto finito, $L \in A^*\mathcal{V}$ e $a \in A$ então $a^{-1}L, La^{-1} \in A^*\mathcal{V}$.

Note-se que a condição (1) implica que $A^*\mathcal{V}$ é também fechado para a intersecção. A condição (3) implica que, se $L \in A^*\mathcal{V}$ e $u \in A^*$, então $u^{-1}L, Lu^{-1} \in A^*\mathcal{V}$.

Teorema 1.6.2. [20, 16] *Sejam $\boldsymbol{V}$ uma pseudovariedade de monóides e $\mathcal{W}$ uma variedade de linguagens. Então:*

(1) *Para cada alfabeto finito A, se $A^*\mathcal{V}$ é a classe de todas as linguagens de A^* cujo monóide sintáctico está em $\boldsymbol{V}$, então $\mathcal{V}$ é uma variedade de linguagens.*

(2) *Se $\boldsymbol{W}$ é a classe de todos os monóides sintácticos das linguagens de $A^*\mathcal{W}$, para todo o alfabeto finito A, então $\boldsymbol{W}$ é uma pseudovariedade de monóides.*

Teorema 1.6.3 (Teorema da Variedade de Eilenberg)**.** [20, 16] *A correspondência $\boldsymbol{V} \to \mathcal{V}$ é uma bijecção entre a classe de todas as pseudovariedades de monóides e a classe de todas as variedades de linguagens. Mais ainda, tem-se:*

$$\boldsymbol{V} \subseteq \boldsymbol{W} \Longleftrightarrow A^*\mathcal{V} \subseteq A^*\mathcal{W}, \text{ para qualquer alfabeto finito } A.$$

Na prática pode ser um pouco difícil descrever as linguagens de $A^*\mathcal{V}$, para uma pseudovariedade de monóides $\mathbf{V}$ arbitrária, mas tal não é o caso quando $\mathbf{V}$ é uma pseudovariedade gerada por um único monóide.

Teorema 1.6.4. [16, 20] *Seja $\boldsymbol{V} = \boldsymbol{V}\langle M\rangle$ a pseudovariedade de monóides gerada pelo monóide M, e seja A um alfabeto finito. Então $A^*\mathcal{V}$ é a álgebra de Boole gerada pelas linguagens $z\varphi^{-1}$, para todo o $z \in M$ e para todo o morfismo $\varphi : A^* \to M$.*

1.7 Reticulados

Nesta secção apresentamos os resultados da Teoria dos Reticulados que vão ser necessários posteriormente.

Seja A um conjunto. Diz-se que uma relação $\leq$ sobre A é uma *relação de ordem parcial* se, quaisquer que sejam $a, b, c \in A$,

(1) $a \leq a$ (*reflexividade*);

(2) se $a \leq b$ e $b \leq a$ então $a = b$ (*anti-simetria*);

(3) se $a \leq b$ e $b \leq c$ então $a \leq c$ (*transitividade*).

Um conjunto com uma relação de ordem parcial chama-se um *conjunto parcialmente ordenado.*

Seja A um conjunto parcialmente ordenado e $X \subseteq A$.

(1) Um elemento $m \in A$ diz-se *maximal* se, para qualquer $a \in A$ se tem que
$$m \leq a \Rightarrow a = m.$$
Um elemento $n \in A$ diz-se *minimal* se, para qualquer $a \in A$ se tem que
$$a \leq n \Rightarrow a = n.$$

(2) Diz-se que $a \in A$ é um *majorante* de X se $x \leq a$, para qualquer $x \in X$. Diz-se que $b \in A$ é um *minorante* de X se $b \leq x$, para qualquer $x \in X$.

(3) Diz-se que $a \in A$ é *máximo* de X se for majorante de X e $a \in X$ e que $b \in A$ é *mínimo* de X se for minorante de X e $b \in X$.

(4) Além disso, diz-se que $a \in A$ é o *supremo* de X se a for o mínimo do conjunto dos majorantes de X e que $b \in A$ é o *ínfimo* de X se b for o máximo do conjunto dos minorantes de X, denota-se a e b, respectivamente, por $\bigvee X$ e $\bigwedge X$.

Chama-se *reticulado* a um conjunto parcialmente ordenado em que existe supremo e ínfimo de qualquer conjunto com dois elementos $\{a, b\}$, que representamos, respectivamente, por $a \vee b$ e $a \wedge b$.

Um reticulado R diz-se *completo* se, para qualquer conjunto $X \subseteq R$, existem $\bigvee X$ e $\bigwedge X$.

Sejam P e Q conjuntos parcialmente ordenados. Uma aplicação sobrejectiva $f : P \to Q$ tal que para quaisquer $a, b \in P$ se tenha
$$a \leq b \Leftrightarrow af \leq bf$$
diz-se que é um *isomorfismo de ordem.*

Tem-se o seguinte resultado:

Proposição 1.7.1. [13] *Sejam S e R reticulados e $f : R \to S$ um isomorfismo de ordem. Se R é completo então dada uma família $(r_i)_{i \in I}$ de elementos de R tem-se*
$$\left(\bigvee_{i \in I} r_i \right) f = \bigvee_{i \in I} (r_i f),$$
consequentemente S é completo.

1.8 Grupos

A Teoria dos Grupos dentro da Álgebra é um ramo muito útil e com muitas aplicações em diversas áreas. No nosso trabalho pretendemos estudar certas classes de grupos pelo que necessitaremos rever alguns resultados desta teoria. Recordaremos nesta secção os principais factos necessários para uma boa compreensão do Capítulo 2.

Seja G um grupo. Um subgrupo próprio H de G diz-se um *subgrupo maximal* de G, e escrevemos $H <\cdot G$, se é maximal entre os subgrupos próprios de G.

Um subgrupo $\{1\} \neq H \leq G$ diz-se um *subgrupo minimal* de G, e escrevemos $H \cdot\leq G$, se é minimal entre os subgrupos não triviais de G.

É claro que $\{1\}$ e G são subgrupos de G. A $\{1\}$ chamamos *subgrupo trivial de* G.

Proposição 1.8.1. [8] *Sejam G um grupo e $x \in G$ um elemento fixo. Então todas as potências x^k, com $k \in \mathbb{Z}$, são distintas ou existe um natural $n_x \in \mathbb{N}$, mínimo tal que $x^{n_x} = 1$. Este natural n_x tem a propriedade seguinte: se $m \in \mathbb{Z}$, estão $x^m = 1$ se e só se $n_x \mid m$.*

Nas condições da proposição anterior, se existe, o natural n_x chama-se *ordem de x*; caso contrário, diz-se que x tem *ordem infinita*. Designamos a ordem de x por $|x|$.

Seja G um grupo e suponhamos que $\emptyset \neq S \subseteq G$. Define-se

$$\langle S\rangle = \{g : \text{existem } n \in \mathbb{N},\ s_i \in S \text{ e } k_i \in \mathbb{Z} \text{ tais que } g = s_1^{k_1} s_2^{k_2} \dots s_n^{k_n}\}.$$

Mostra-se que $\langle S\rangle$ é subgrupo de G e que, de facto, é o menor subgrupo de G que contém S, ou seja,

$$\langle S\rangle = \bigcap_{\substack{H\leq G \\ H\supseteq S}} H.$$

A $\langle S\rangle$ dá-se o nome de *subgrupo de G gerado por S*.

Dado um grupo G, diz-se que G é *cíclico* se existir $x \in G$ tal que $G = \langle x\rangle$. Portanto, qualquer $x \in G$ gera um *subgrupo cíclico* de G

$$\langle x\rangle = \{x^k : k \in \mathbb{Z}\}.$$

Note-se que todo o grupo cíclico é necessariamente abeliano.

No caso em que x tem ordem n finita, tem-se

$$\langle x\rangle = \{x, x^2, \dots, x^{n-1}, x^n = 1\}.$$

De facto tem-se $|\langle x\rangle| = n = |x|$.

Seja G um grupo finito. Define-se o *expoente* $\exp(G)$ *de* G como sendo o mínimo múltiplo comum das ordens dos elementos de G:

$$\exp(G) = \text{mmc}(|g| : g \in G).$$

Exemplo 1.8.2. (1) Seja G um grupo. Dados $x, y \in G$ define-se o *comutador* $[x, y]$ de x e y do seguinte modo: $[x, y] = x^{-1}y^{-1}xy \in G$. É claro que $xy = yx$ se e só se $[x, y] = 1$. O subgrupo $G' = \langle [x, y] : x, y \in G\rangle$ de G chama-se *subgrupo derivado* de G. É fácil verificar que G é abeliano se e só se $G' = \{1\}$.

(2) Definimos também o subgrupo

$$Z(G) = \{z \in G : zg = gz, \forall g \in G\}$$

que se chama o *centro* de G. Um grupo G é abeliano se e só se $Z(G) = G$.

Dados um grupo G e um seu subgrupo H, podemos definir uma relação de equivalência $\sim$ em G do seguinte modo: para $a, b \in G$,

$$a \sim b \text{ se e só se } Ha = Hb,$$

tendo-se $[a]_\sim = Ha$. Assim, os subconjuntos Ha e aH designam-se por *classe lateral direita de* H *em* G e *classe lateral esquerda de* H *em* G, respectivamente, sendo a um *representante* dessas classes laterais.

Teorema 1.8.3 (Teorema de Lagrange)**.** [8] *Sejam G um grupo finito e $H \leq G$. Então $|H|$ divide $|G|$ e tem-se $|G| = |H|[G : H]$, em que $[G : H]$ designa o número de classes laterais direitas de H em G.*

A versão do Teorema de Lagrange para classes laterais esquerdas também é válida, pelo que o número de classes laterais esquerdas é igual ao número de classes laterais direitas e designa-se por *índice* de H em G.

Os seguintes resultados são consequências imediatas do Teorema de Lagrange:

Teorema 1.8.4. [8] *Sejam G um grupo finito e $x \in G$. Então $|x| \mid |G|$.*

Corolário 1.8.5. [8] *Sejam G um grupo finito e $x \in G$. Então $x^{|G|} = 1$.*

Teorema 1.8.6. [8] *Seja G um grupo finito com $|G| = p$, em que p é um número primo. Então G é cíclico.*

A proposição seguinte permite dar uma correspondência entre os divisores da ordem e os subgrupos de um grupo cíclico.

Proposição 1.8.7. [8] *Seja G um grupo cíclico finito de ordem n. Se $m \in \mathbb{N}$ é tal que $m \mid n$, então G tem um único subgrupo de ordem m, e esse subgrupo é cíclico.*

Seja G um grupo. Um subgrupo N de G diz-se *normal* se $Ng = gN$, qualquer que seja $g \in G$. Escrevemos $N \trianglelefteq G$. Se N é subgrupo próprio de G e é normal em G escrevemos $N \lhd G$.

Um grupo G diz-se *simples* se não possui subgrupos normais além de $\{1\}$ e G.

Uma caracterização alternativa dos subgrupos normais é a seguinte:

Proposição 1.8.8. [8] *Sejam G um grupo e $H \leq G$. Então,*

$$H \trianglelefteq G \text{ se e só se } g^{-1}Hg \subseteq H, \text{ qualquer que seja } g \in G.$$

Claramente, dado um grupo G, tem-se $\{1\}, G \trianglelefteq G$. Mais ainda, o subgrupo derivado G' e o centro $Z(G)$ de G são normais em G.

Sejam G um grupo e H um subgrupo próprio de G. Diz-se que H é *normal maximal* em G, e escrevemos $H \lhd\cdot\, G$, se $H \lhd G$ e é maximal entre os subgrupos normais próprios de G.

Um subgrupo $\{1\} \neq H \leq G$ diz-se *normal minimal* em G, e escrevemos $H \cdot\trianglelefteq G$, se $H \trianglelefteq G$ e é minimal entre os subgrupos normais não triviais de G.

Sejam G um grupo e $H, K \leq G$, nem sempre HK é um subgrupo de G mas tem-se:

Proposição 1.8.9. [8, 18] *Sejam G um grupo e $H, K \leq G$. Se $H \trianglelefteq G$ ou $K \trianglelefteq G$ então, $HK \leq G$.*

Além disso, se $H \trianglelefteq G$ e $K \leq G$ então $H \cap K \trianglelefteq K$.

A construção seguinte é muito importante na teoria de grupos:

Sejam G um grupo e $N \trianglelefteq G$. No conjunto G/H das classes laterais de N em G (como $N \trianglelefteq G$, é indiferente falar em classes laterais esquerdas ou direitas), define-se uma operação binária $*$ do seguinte modo:

$$(aN) * (bN) = (ab)N, \text{ se } a, b \in G.$$

Na prática, não há ambiguidade se se omitir o símbolo "$*$" e escrevermos simplesmente $(aN)(bN)$ em vez de $(aN) * (bN)$, porque de facto a classe de ab é o produto dos subconjuntos aN e bN.

Proposição 1.8.10. [8] *Sejam G um grupo e $N \trianglelefteq G$. Então G/N é um grupo com elemento identidade $N = 1N$ e o inverso de um elemento $aN \in G/N$ é o elemento $a^{-1}N \in G/N$.*

A forma dos subgrupos normais de um grupo quociente é descrita no seguinte resultado:

Proposição 1.8.11. [18] *Sejam G um grupo e N um subgrupo normal de G. Então o conjunto dos subgrupos normais de G/N é*

$$\{H/N : N \subseteq H,\ H \trianglelefteq G\}.$$

É importante ter presente que, se G é um grupo cíclico e $N \trianglelefteq G$, então também G/N é cíclico e também que:

Proposição 1.8.12. [8, 10] *Seja G um grupo e G' o seu subgrupo derivado. Se $N \trianglelefteq G$ é tal que $G' \leq N$ então G/N é abeliano. Em particular, G/G' é abeliano. Reciprocamente, se $N \trianglelefteq G$ é tal que G/N é abeliano, então $G' \leq N$.*

Sejam G e H grupos. Uma aplicação $\varphi : G \to H$ diz-se um *morfismo de grupos* se satisfaz a propriedade

$$(xy)\varphi = (x\varphi)(y\varphi),$$

para todo o $x, y \in G$, i.e. é um morfismo de semigrupos. É consequência da definição que um morfismo entre grupos aplica a identidade de G na identidade de H e que, para qualquer $x \in G$, se tem $(x^{-1})\varphi = (x\varphi)^{-1}$.

O conjunto

$$Aut(G) = \{\varphi : \varphi \text{ é um automorfismo de } G\}$$

é um grupo com respeito à composição de aplicações.

Seja p um número primo. Um automorfismo φ do grupo G diz-se um *p-automorfismo* se p é o único número primo que divide a sua ordem, enquanto elemento do grupo $Aut(G)$, e diz-se um *p'-automorfismo* se a sua ordem não é divisível por p.

Caracterizamos agora o grupo $Aut(G)$ no caso em que G é um grupo cíclico:

Teorema 1.8.13. [8] *Seja p um número primo e C_p um grupo cíclico de ordem p. Então $Aut(C_p) \simeq C_{p-1}$, o grupo cíclico de ordem $p-1$.*

Recordemos também que:

Proposição 1.8.14. *Sejam G e H grupos tais que $G \simeq H$. Então $Aut(G) \simeq Aut(H)$.*

Dado um grupo G e $x \in G$ definimos uma aplicação $\alpha_x : G \to G$ por $g\alpha_x = x^{-1}gx$, qualquer que seja $g \in G$, que é um automorfismo de G dito o *automorfismo interior de G induzido pelo elemento x*. Seja

$$Inn(G) = \{\alpha_x \in Aut(G) : x \in G\}.$$

Mostra-se que $Inn(G)$ é um subgrupo de $Aut(G)$.

Dizemos que $N \leq G$ é um *subgrupo característico* de G, e escrevemos N *char* G, se $N\varphi = N$, qualquer que seja $\varphi \in Aut(G)$.

Note-se que $N \trianglelefteq G$ se $N\alpha_x = N$, para todo o $x \in G$. Pelo que se N *char* G então $N \trianglelefteq G$.

Claramente, se G é um grupo, o subgrupo trivial $\{1\}$ e G são subgrupos característicos de G. Mais ainda, o centro $Z(G)$ de G e o subgrupo derivado G' de G são também subgrupos característicos de G.

Segue-se uma propriedade dos subgrupos característicos:

Proposição 1.8.15. [10] *Sejam G um grupo e H, K subgrupos de G. Se H char K e $K \trianglelefteq G$ então $H \trianglelefteq G$.*

Dado um morfismo de grupos $\varphi : G \to H$ define-se o *kernel de* φ e a *imagem de* φ do seguinte modo:

$$\ker \varphi = \{g \in G : g\varphi = 1_H\}$$
$$G\varphi = im\varphi = \{h \in H : \exists g \in G \text{ tal que } h = g\varphi\}.$$

Proposição 1.8.16. [18] *Sejam G, H grupos e $\varphi : G \to H$ um morfismo. Então φ é um monomorfismo se e só se* $\ker \varphi = \{1\}$.

Os três teoremas seguintes são bem conhecidos na teoria de grupos:

Teorema 1.8.17 (Teorema do Homomorfismo)**.** [8] (a) *Sejam G, H grupos e $\varphi : G \to H$ um morfismo. Então* $\ker \varphi \trianglelefteq G$, $im\varphi \leq H$ *e*

$$im\varphi \simeq G/\ker \varphi.$$

(b) *Se $N \trianglelefteq G$ então a aplicação $\pi : G \twoheadrightarrow G/N$ definida por $g\pi = gN$ é um epimorfismo cujo kernel é N e com imagem G/N.*

Se na alínea (a) do teorema anterior φ é injectivo tem-se, pela proposição anterior, $\ker \varphi = \{1\}$ donde

$$im\varphi \simeq G/\{1\} \simeq G.$$

Nestas condições também se diz que φ é um *mergulho* e que G se *mergulha* em H, escrevendo-se

$$G \lesssim H.$$

Teorema 1.8.18 (1º Teorema do Isomorfismo)**.** [8] *Sejam G um grupo, $H \leq G$ e $K \trianglelefteq G$. Então $HK \leq G$, $H \cap K \trianglelefteq H$ e*

$$HK/K \simeq H/(H \cap K).$$

Teorema 1.8.19 (2º Teorema do Isomorfismo)**.** [8] *Sejam G um grupo e $H \leq G$, $N \trianglelefteq G$ tais que $N \leq H$. Então $H/N \trianglelefteq G/N$ e*

$$(G/N)/(H/N) \simeq G/H.$$

Sejam G e H grupos. Consideremos definida no produto cartesiano $G \times H$ a operação produto componente a componente apresentada na Secção 1.1 para semigrupos. Com essa operação, o conjunto $G \times H$ torna-se um grupo com elemento identidade $(1_G, 1_H)$ em que o inverso de um elemento (g, h) é o elemento (g^{-1}, h^{-1}), sendo g^{-1} o inverso de g em G e h^{-1} o inverso de h em H. O grupo $G \times H$ designa-se por *produto directo* (*externo*) de G e H.

Note-se que se G e H são ambos abelianos então $G \times H$ é também abeliano.

À semelhança do que foi feito para semigrupos, também a noção de produto directo externo de grupos se pode estender a produtos com mais de dois grupos. Em particular se $(G_i)_{i=1,\ldots,m}$ é uma família finita de grupos, denotamos o *produto directo externo* da família $(G_i)_{i=1,\ldots,m}$ por

$$G_1 \times \cdots \times G_m \text{ ou por } \prod_{i=1}^{m} G_i.$$

Analogamente ao que acontece para o caso $m = 2$, o elemento $(1, \ldots, 1)$ é a identidade de $G_1 \times \cdots \times G_m$ e cada $(g_1, \ldots, g_m) \in G_1 \times \cdots \times G_m$ tem inverso $(g_1^{-1}, \ldots, g_m^{-1})$.

Sejam G um grupo e $M, N \leq G$. Diz-se que G é *produto directo interno* dos subgrupos M e N se

(1) $G = MN$,

(2) $M, N \trianglelefteq G$ e

(3) $M \cap N = \{1\}$

e neste caso escrevemos $G = M \dot{\times} N$.

Vejamos que a noção de produto directo interno também se pode estender a produtos com mais de dois grupos. Sejam G um grupo, m um inteiro positivo e, para cada $i \in \{1, \ldots, m\}$, $N_i \trianglelefteq G$ um subgrupo normal de G. Atendendo à associatividade do produto de subgrupos, é possível definir o produto

$$N_1 \cdots N_m.$$

Pela Proposição 1.8.9 e utilizando um raciocínio de indução, tem-se $N_1 \cdots N_m$ subgrupo de G. Diz-se que $G = N_1 \cdots N_m$ é *produto directo interno* dos subgrupos N_i se todo o elemento g de G se escreve, de modo único, na forma,

$$g = n_1 \cdots n_m, \text{ com } n_i \in N_i \text{ e } i = 1, \ldots, m.$$

Denotaremos o produto directo interno de $N_1, \ldots, N_m$ por

$$\dot{\prod_{i=1}^{m}} N_i.$$

De facto, este conceito de produto directo interno de subgrupos generaliza o correspondente conceito de produto directo de dois subgrupos, apesar de esta última noção ter anteriormente aparecido de uma forma um pouco diferente.

O próximo resultado relaciona o produto directo interno com o externo:

Teorema 1.8.20. [10] *Sejam G um grupo e $N_1, \ldots, N_m \trianglelefteq G$ tais que G é produto directo interno dos grupos $N_1, \ldots, N_m$. Então*

$$G \simeq N_1 \times \cdots \times N_m.$$

Seja p um número primo. Um grupo P diz-se um *p-grupo* finito se é finito e $|P| = p^n$, em que $n \in \mathbb{N}_0$. Diz-se que P é um *p'-grupo* se $p \nmid |P|$.

Um subgrupo H de um grupo finito G diz-se um *p-subgrupo de G* se a sua ordem é uma potência do número primo p e diz-se um *p-subgrupo de Sylow* de G se $|H| = p^n$, sendo p^n a maior potência de p que divide $|G|$. O conjunto dos p-subgrupos de Sylow de G será denotado por $\mathrm{Syl}_p(G)$.

Se p é um número primo, G é um grupo finito e $\{P\} = \mathrm{Syl}_p(G)$ então P é um subgrupo característico de G.

Note-se para referência futura que muitas vezes se denota $\bigcap_{P \in \mathrm{Syl}_p(G)} P$ por $O_p(G)$.

Um dos resultados fundamentais na teoria dos p-grupos finitos reside no Teorema de Sylow:

Teorema 1.8.21 (Teorema de Sylow)**.** [8, 10] *Sejam p um número primo e G um grupo finito. Então:*

(1) *O grupo G contém um p-subgrupo de Sylow;*

(2) *Todo o p-subgrupo de G está contido num p-subgrupo de Sylow de G.*

Como consequência deste resultado temos:

Corolário 1.8.22. [10] *Sejam G um grupo finito e S um p-subgrupo de Sylow de G. Então, $S \trianglelefteq G$ se e só se S é o único p-subgrupo de Sylow de G.*

Corolário 1.8.23 (Teorema de Cauchy)**.** [10] *Sejam p um número primo e G um grupo finito. Se $p \mid |G|$ então existe um elemento $g \in G$ tal que $|g| = p$.*

Corolário 1.8.24. [10] *Um grupo finito G é um p-grupo se e só se a ordem de todos os seus elementos é uma potência de p.*

Outro resultado muito importante na teoria dos p-grupos finitos e que vai ser de alguma utilidade posteriormente é o seguinte:

Teorema 1.8.25. [10] *Sejam p um número primo e P um p-grupo finito não trivial. Então $Z(P) > \{1\}$.*

Como consequência tem-se:

Corolário 1.8.26. [10] *Todo o p-grupo finito simples é abeliano e tem ordem p.*

Os grupos abelianos finitos descrevem-se à custa dos seus p-grupos cíclicos:

Teorema 1.8.27. [10] *Seja G um grupo finito abeliano. Então*

$$G = \prod_{i=1}^{n}{}^{\cdot} C_i,$$

em que os subgrupos C_i são p-grupos para vários primos p.

Note-se que se $G_1, \ldots, G_n$ são grupos e σ é uma bijecção de $\{1, \ldots, n\}$, então

$$G_1 \times \cdots \times G_n \simeq G_{(1)\sigma} \times \cdots \times G_{(n)\sigma}.$$

Sejam G um grupo e $M \trianglelefteq G$ um subgrupo normal de G. Se existe um subgrupo K de G tal que

(1) $G = MK$;

(2) $K \cap M = \{1\}$,

diz-se que G se *decompõe sobre* M, que M é *complementado* por K em G e que K é um *complemento* de M em G.

Um subgrupo K de um grupo finito G diz-se um *subgrupo de Hall* de G se $\text{mdc}(|G|, [G : K]) = 1$. Se K é um complemento de um subgrupo normal M de G e além disso é um subgrupo de Hall diz-se que K é um *complemento de Hall* de M em G.

O resultado seguinte garante-nos a existência de complemento em certas condições:

Teorema 1.8.28 (Teorema de Schur e Zassenhaus)**.** [8] *Sejam G um grupo finito e $H \trianglelefteq G$ um subgrupo de Hall normal de G. Então existe um complemento K para H em G.*

Sejam H e G grupos e

$$\begin{array}{rcl} \alpha : G & \longrightarrow & Aut(H) \\ g & \longmapsto & \alpha_g \end{array}$$

um morfismo de grupos. Definindo $g \cdot h = (h)\alpha_{g^{-1}}$, para cada $g \in G$ e $h \in H$, obtemos uma acção à esquerda de G sobre H por endomorfismos e unitária à direita. Note-se que, como G e H são grupos, a acção é de facto

por *automorfismos*. Podemos considerar o produto semidirecto associado o qual denotamos por $H \overset{\alpha}{\rtimes} G$ ou simplesmente $H \rtimes G$. Trata-se de um grupo com elemento identidade $(1_H, 1_G)$ e em que o inverso de um elemento $(h, g) \in H \times G$ é o elemento $(g^{-1} \cdot h^{-1}, g^{-1})$.

Facilmente se verifica que, se H é um grupo e G_1 e G_2 são grupos que actuam sobre H tais que $G_1 \simeq G_2$, então $H \rtimes G_1 \simeq H \rtimes G_2$.

Observação 1.8.29. (1) Um caso particular de produto semidirecto externo de grupos é o seguinte:

Sejam G e H grupos e consideremos o morfismo de grupos definido por

$$\begin{array}{rcl} \alpha : G & \longrightarrow & Aut(H) \\ g & \longmapsto & id_H \end{array}$$

logo $g \cdot h = (h)\alpha_{g^{-1}} = h$, para quaisquer $g \in G$ e $h \in H$. O produto em $H \overset{\varphi}{\rtimes} G$ é tal que

$$(h, g)(h', g') = (h(g \cdot h'), gg') = (hh', gg'),$$

quaisquer que sejam $(g, h), (g', h') \in G \times H$. Assim $H \overset{\varphi}{\rtimes} G = H \times G$, o produto directo externo dos grupos H e G.

(2) Se G é um grupo, $M \trianglelefteq G$ e K é um complemento de M em G então todo o elemento g de G se escreve de modo único como produto mk de um elemento $m \in M$ por um $k \in K$. Uma vez que $M \trianglelefteq G$, cada $k \in K$ induz, por conjugação, um automorfismo α_k de M dado por $(m)\alpha_k = k^{-1}mk$, qualquer que seja $m \in M$. A seguinte aplicação é um morfismo de grupos

$$\begin{array}{rcl} \alpha : K & \longrightarrow & Aut(M) \\ k & \longmapsto & \alpha_k \end{array}$$

pelo que podemos considerar $M \overset{\alpha}{\rtimes} K$ e a aplicação $\theta : G \to M \overset{\alpha}{\rtimes} K$, $g = mk \mapsto (m, k)$.

Como, para quaisquer $m_1, m_2 \in M$ e $k_1, k_2 \in K$,

$$(m_1k_1)(m_2k_2) = m_1k_1m_2k_1^{-1}k_1k_2 = (m_1(m_2)\alpha_{k_1^{-1}})(k_1k_2)$$

conclui-se facilmente que G é isomorfo a $M \overset{\alpha}{\rtimes} K$. Nestas condições dizemos que G é *produto semidirecto interno* de M e K.

Outra noção de produto de grupos intrinsecamente relacionada com a noção de produto semidirecto e que já foi definida na Secção 1.4 para monóides é a seguinte:

Sejam H e G grupos e H^G o conjunto das aplicações de G em H. Com a operação definida pelo produto das imagens H^G é um grupo, em que o elemento identidade é a aplicação de G em H que transforma qualquer elemento g de G no elemento identidade de H e o inverso de uma aplicação $f \in H^G$ é a aplicação $f' \in H^G$ tal que, qualquer que seja $g \in G$, se tenha $gf' = (gf)^{-1}$.

Considerando a acção à esquerda de G sobre H^G, definida na Secção 1.4, construímos um produto semidirecto $H^G \rtimes G$ que é um grupo e se designa por *produto em coroa* de H por G, o qual denotamos por $H \circ G$.

Seja G um grupo. Uma *série* para G é uma cadeia de subgrupos $H_i \leq G$, $0 \leq i \leq n$, tais que

(1) $H_0 = \{1\}$ e $H_n = G$;

(2) $H_i \trianglelefteq H_{i+1}$, $i = 0, \ldots, n-1$.

Os grupos quociente H_{i+1}/H_i designam-se por *factores* da série. A série diz-se *normal* se $H_i \trianglelefteq G$, para cada $i = 0, \ldots, n$. Uma série normal diz-se *normal maximal* se cada subgrupo H_i é maximal entre os subgrupos próprios normais de H_{i+1}, para cada $i = 0, \ldots, n-1$. Note-se que numa série normal maximal os seus factores são simples. Observemos também que, dado que os nossos grupos são finitos, existe sempre uma série normal maximal para cada grupo não trivial.

Uma série normal diz-se *central* se os seus factores são centrais, isto é,

$$H_{i+1}/H_i \leq Z(G/H_i), \quad \text{com} \quad i = 0, \ldots, n-1.$$

Um grupo G diz-se *resolúvel* se possui uma série normal com factores abelianos, isto é, se existem subgrupos normais $H_1, \ldots, H_{n-1} \trianglelefteq G$ tais que

$$\{1\} = H_0 \trianglelefteq \cdots \trianglelefteq H_n = G$$

e cada H_{i+1}/H_i é abeliano, para $i = 0, \ldots, n-1$.

Proposição 1.8.30. [10] *Sejam G um grupo e $N \leq G$. Se G é resolúvel então N é resolúvel.*

Proposição 1.8.31. [10] *Sejam G um grupo e $N \trianglelefteq G$. Se N e G/N são resolúveis, então G é resolúvel.*

Um grupo G diz-se *abeliano elementar* se existe um número primo p tal que $G \simeq C_p \times \cdots \times C_p \neq \{1\}$, em que C_p é um grupo cíclico de ordem p.

Proposição 1.8.32. [10] *Sejam G um grupo e $\{1\} \neq N \cdot \trianglelefteq G$. Se N é finito e resolúvel então é um grupo abeliano elementar.*

Tal como o Teorema de Schur e Zassenhaus (1.8.28), também o próximo resultado nos garante a existência de um complemento, neste caso para certos grupos finitos resolúveis.

Teorema 1.8.33 (Teorema de Hall)**.** [10] *Seja G um grupo finito e resolúvel de ordem mn, em que* $\mathrm{mdc}(m,n)=1$. *Seja $M \trianglelefteq G$ de ordem m. Então M admite um complemento em G.*

Um grupo G diz-se *nilpotente* se possui uma série central, isto é, se existem subgrupos normais $H_1, \ldots, H_{n-1} \trianglelefteq G$ tais que

$$\{1\} = H_0 \trianglelefteq \cdots \trianglelefteq H_n = G$$

com $H_{i+1}/H_i \leq Z(G/N_i)$, para $i = 0, \ldots, n-1$.

Note-se que os grupos nilpotentes são resolúveis. Além disso, se G é abeliano então G é nilpotente e resolúvel.

Proposição 1.8.34. [10] *Subgrupos e grupos quociente de grupos nilpotentes são nilpotentes.*

Proposição 1.8.35. [10] *Os p-grupos finitos são nilpotentes. Consequentemente são resolúveis.*

Recordemos duas caracterizações dos grupos nilpotentes:

Teorema 1.8.36. [10] *Seja G um grupo finito. São equivalentes:*

(1) *G é nilpotente;*

(2) *Todo o subgrupo de Sylow de G é normal em G;*

(3) *G é produto dos seus subgrupos de Sylow.*

Teorema 1.8.37. [15] *Seja G um grupo resolúvel. Então o subgrupo derivado G' de G é nilpotente.*

Terminamos esta secção com a definição do *subgrupo de Frattini* $\Phi(G)$ de um grupo finito G:

$$\Phi(G) = \bigcap_{M < G} M,$$

a intersecção de todos os subgrupos maximais de G.

Por convenção define-se $\Phi(\{1\}) = \{1\}$. Tem-se $\Phi(G)$ *char* G, donde $\Phi(G) \trianglelefteq G$ e podemos considerar o *quociente de Frattini* $G/\Phi(G)$.

Proposição 1.8.38. [8] *Seja p um número primo e P um p-grupo finito. Então o quociente de Frattini $P/\Phi(P)$ é um p-grupo abeliano elementar.*

Usaremos mais à frente o seguinte facto:

Teorema 1.8.39 (Teorema de Burnside)**.** [14] *Seja φ um p'-automorfismo de um p-grupo P e suponhamos que φ induz a identidade em $P/\Phi(P)$, isto é, $(g\varphi)\Phi(P) = g\Phi(P)$, para todo o $g \in P$. Então φ é o automorfismo identidade de P.*

1.9 Álgebra Linear: Anéis, Corpos e Espaços Vectoriais

Nesta secção vamos recordar vários conceitos e resultados sobre anéis, corpos e espaços vectoriais que necessitamos posteriormente.

Um *anel* é uma estrutura constituída por um conjunto A e duas operações binárias definidas em A, usualmente designadas por "adição",$+$, e "multiplicação",$\cdot$, tais que:

(1) $(A, +)$ é um grupo abeliano;

(2) $(A, \cdot)$ é um semigrupo;

(3) São válidas as *leis distributivas* da multiplicação em relação à adição, isto é, para $a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{e} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Um anel diz-se *comutativo* se a operação de multiplicação é comutativa. Diz-se ainda que A é *anel com identidade* se existe em A um elemento, designado por 1, que é a identidade para a multiplicação.

Num anel com identidade, os elementos que possuem inverso para a multiplicação dizem-se *invertíveis*, por vezes são designados por *unidades*. O conjunto das unidades de um anel A com identidade forma um grupo para a multiplicação, que denotamos usualmente por $\mathcal{U}(A)$.

A um anel comutativo, com identidade no qual todo o elemento não nulo é invertível dá-se o nome de *corpo*. Assim sendo, o grupo das unidades de um corpo K é $K \setminus \{0\}$.

Um importante exemplo de anel a que já nos referimos na Secção 1.1 é o conjunto $\mathbb{Z}_n$, para cada $n \in \mathbb{N}$, com as respectivas operações de adição e multiplicação. Recordemos que $\mathbb{Z}_p$ é corpo (finito) se e só se o número p é primo. Portanto, se p é um número primo, $\mathcal{U}(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\}$.

Sejam A e B aneis. Uma aplicação $f : A \to B$ diz-se um *morfismo*, ou um *morfismo de anéis*, se verifica as condições seguintes, quaisquer que sejam $a, a' \in A$:

(1) $(a + a')f = (af) + (a'f)$;

(2) $(aa')f = (af)(a'f)$.

Tal como noutras estruturas, um morfismo injectivo (respectivamente sobrejectivo, bijectivo) chama-se um *monomorfismo* (respectivamente *epimorfismo*, *isomorfismo*).

No caso em que $B = A$, diz-se que f é um *endomorfismo*, se fôr simultaneamente isomorfismo toma o nome de *automorfismo*.

Uma parte I não vazia de um anel A diz-se um *ideal* de A se verifica as seguintes propriedades:

(1) $x, y \in I \Rightarrow x + y \in I$;

(2) $x \in I \Rightarrow -x \in I$;

(3) $x \in I \Rightarrow xa, ax \in I$, para qualquer $a \in A$.

Proposição 1.9.1. [18] *Sejam A e B anéis e $f : A \to B$ um morfismo de anéis. Se f é um epimorfismo e I é um ideal de A então If é um ideal de B.*

Sejam A um anel e $I \subseteq A$ um ideal de A. Considere-se uma relação definida em A do seguinte modo:

$$a \equiv b \pmod{I} \Leftrightarrow a - b \in I$$

Esta relação é, de facto, uma relação de congruência nos semigrupos $(A, +)$ e $(A, \cdot)$ no sentido da definição dada na Secção 1.1, pelo que podemos construir o respectivo anel quociente A/I.

Sejam V um conjunto não vazio e K um corpo. Diz-se que V é um *espaço vectorial* sobre o corpo K se:

(1) Está definida em V uma operação binária que se designa por *adição*,+, tal que $(V, +)$ é grupo abeliano;

(2) Está definida uma aplicação de $V \times K$ para V, designada por *produto escalar*, que a cada par $(x, \lambda) \in V \times K$ faz corresponder um elemento $x\lambda$ de V tal que, para $\lambda, \mu \in K$ e $x, y \in V$,

   (a) $(x + y)\lambda = x\lambda + y\lambda$;
   (b) $x(\lambda + \mu) = x\lambda + x\mu$;
   (c) $(x\lambda)\mu = x(\lambda\mu)$;
   (d) $x1_K = x$.

Um subconjunto não vazio U de um espaço vectorial V sobre um corpo K diz-se um *subespaço vectorial* de V, e escrevemos $U \leq_K V$, se fôr espaço vectorial para as operações induzidas o que equivale a dizer que, para $x, y \in U$ e $\lambda \in K$,

(1) $x + y \in U$;

(2) $x\lambda \in U$.

Sejam V um espaço vectorial sobre um corpo K e U, W subespaços vectoriais de V. Dizemos que V é *soma directa* de U e W, e escrevemos $V = U \oplus W$, se:

(1) $V = U + W$;

(2) $U \cap W = \{0_V\}$.

Sejam V e V' espaços vectoriais sobre o mesmo corpo K e $f : V \to V'$ uma aplicação. Diz-se que φ é uma *aplicação linear* sobre K se satisfaz as seguintes propriedades, para quaisquer $x, y \in V$, $\lambda \in K$,

(1) $(x + y)\varphi = (x\varphi) + (y\varphi)$;

(2) $(x\lambda)\varphi = (x\varphi)\lambda$,

diz-se que φ é um *isomorfismo* se é bijectiva e um *automorfismo* se $V = V'$ e φ é bijectiva.

Se V e V' são espaços vectoriais tais que existe $\varphi : V \to V'$ isomorfismo dizemos que V e V' são *isomorfos* e escrevemos $V \simeq V'$.

Note-se que todo o espaço vectorial de dimensão finita $n \in \mathbb{N}$ sobre um corpo K é isomorfo ao produto directo $K \times \cdots \times K$ de n cópias do corpo K.

É claro como se define o produto directo de anéis ou de corpos depois de termos visto esse conceito para semigrupos e grupos.

Proposição 1.9.2. [8] *Sejam p um número primo e $P \neq \{1\}$ um p-grupo abeliano elementar de ordem p^n, em que $n \in \mathbb{N}$. Então P tem estrutura de espaço vectorial de dimensão n sobre o corpo finito $\mathbb{Z}_p$ de ordem p. As operações são definidas do seguinte modo, em que $\cdot$ representa a operação no grupo P: dados $g, h \in P$ e $\overline{\lambda} \in \mathbb{Z}_p$ com $\lambda \in \mathbb{N}$,*

$$\textit{Adição do espaço vectorial: } g + h = g \cdot h,$$

$$\textit{Multiplicação escalar: } g\overline{\lambda} = g \cdot \ldots \cdot g \ (\lambda \textit{ vezes}).$$

Os subgrupos do grupo P são precisamente os subespaços de P encarado como espaço vectorial. Mais ainda, uma aplicação bijectiva $\varphi : P \to P$ é morfismo se e só se é aplicação linear sobre $\mathbb{Z}_p$.

1.10 Álgebras, Representações e Módulos

A Teoria das Representações está intrinsecamente relacionada com a Teoria dos Grupos. Os resultados que apresentamos aqui são bem conhecidos e só os enunciamos para uma melhor compreensão do que irá ser feito posteriormente no Capítulo 2. Recordaremos também alguns resultados sobre Álgebras e Módulos.

Note-se que as designações álgebra-K, módulo-G e módulo-A para as estruturas que iremos apresentar nesta secção são propositadas. Elas devem-se ao facto de estarmos a considerar acções à direita.

Seja K um corpo. Uma *álgebra-K* é um conjunto A com as seguintes propriedades:

(1) A é um espaço vectorial de dimensão finita sobre K;

(2) A é um anel com identidade;

(3) A multiplicação escalar e a multiplicação do anel são relacionadas por

$$(ab)k = a(bk) = (ak)b, \text{ para } a, b \in A \text{ e } k \in K.$$

Dados um corpo K e um espaço vectorial $V \neq \{0\}$ de dimensão n sobre K, sejam

$$End_K(V) = \{\varphi \mid \varphi : V \to V \text{ é aplicação linear sobre } K\},$$

$$GL(V) = \{\varphi \in End_K(V) : \varphi \text{ é um automorfismo}\},$$

$$M_n(K) = \{M : M \text{ é matriz } n \times n \text{ sobre } K\},$$

$$Gl_n(K) = \{M \in M_n(K) : M \text{ é invertível}\}.$$

Note-se que por vezes se denota $GL(V)$ por $Aut_K(V)$ ou simplesmente por $Aut(V)$.

Em relação à composição $GL(V)$ é um grupo; em relação ao produto, $Gl_n(K)$ é também um grupo; com as operações usuais de adição e multiplicação de matrizes e multiplicação por um escalar, $M_n(K)$ é uma álgebra-K; $End_K(V)$ é álgebra-K para as operações seguintes:

(1) Adição: se $\varphi, \theta \in End_K(V)$, define-se $\varphi + \theta : V \to V$, $v \mapsto (v\varphi) + (v\theta)$;

(2) Multiplicação (composição): se $\varphi, \theta \in End_K(V)$, define-se $\varphi\theta : V \to V$, $v \mapsto (v\varphi)\theta$;

(3) Multiplicação escalar: se $\varphi \in End_K(V)$ e $k \in K$, define-se $\varphi k : V \to V$, $v \mapsto (v\varphi)k$.

Sejam A e B álgebras-K. Um *morfismo de álgebras-K* de A para B é uma aplicação $\tau : A \to B$ tal que

(1) $\tau : A \to B$ é uma aplicação linear sobre K;

(2) $(a_1a_2)\tau = (a_1\tau)(a_2\tau)$, para $a_1, a_2 \in A$;

(3) $1_A\tau = 1_B$.

Mais uma vez, tal como atrás, se $A = B$ diz-se que τ é um *endomorfismo de álgebras-K*. Um *isomorfismo de álgebras-K* de A para B é um morfismo de álgebras-K que é bijectivo.

Dado $\tau : A \to B$ um morfismo de álgebras-K, define-se o *kernel de* τ por

$$\ker \tau = \{a \in A : a\tau = 0_B\}.$$

Seja A uma álgebra-K. Um subconjunto $I \subseteq A$ diz-se um *ideal de* A se I é um ideal de A encarado como anel e é fechado para a multiplicação escalar, isto é, $x\mu \in I$, quaisquer que sejam $x \in I$ e $\mu \in K$.

Sejam A e B álgebras-K e $\tau : A \to B$ um morfismo de álgebras-K. Então $\ker \tau$ é um ideal de A.

Seja K um corpo.

(1) Seja G um grupo finito. Uma *representação de G sobre K* é um morfismo de grupos
$$\rho : G \longrightarrow GL(V),$$
em que V é um espaço vectorial de dimensão finita sobre K. Se ρ é um monomorfismo diz-se que ρ é uma representação *fiel* de G;

(2) Uma *representação de G sobre K por matrizes* é um morfismo de grupos
$$\varphi : G \longrightarrow Gl_n(K).$$
Ao natural n dá-se o nome de *grau* de φ. Diz-se que φ é uma representação *fiel* de G se é um monomorfismo.

(3) Seja A uma álgebra-K. Uma *representação de A sobre o espaço vectorial V sobre K* é um morfismo de álgebras-K
$$\pi : A \longrightarrow End_K(V).$$

Sejam G um grupo finito e K um corpo. Seja $K[G]$ o conjunto de todas as somas formais

$$\sum_{g \in G} \lambda_g g, \tag{1.5}$$

em que $\lambda_g \in K$. Podemos encarar a soma formal (1.5) como sendo a aplicação

$$\begin{array}{ccc} G & \longrightarrow & K \\ g & \longmapsto & \lambda_g \end{array}$$

Por definição, duas somas formais $\sum_{g \in G} \lambda_g g$ e $\sum_{g \in G} \mu_g g$ são iguais se e só se $\lambda_g = \mu_g$, para todo o $g \in G$.

Definem-se adição, multiplicação escalar de K e multiplicação em $K[G]$ do seguinte modo:

$$\sum_{g\in G}\lambda_g g+\sum_{g\in G}\mu_g g=\sum_{g\in G}(\lambda_g+\mu_g)g, \tag{1.6}$$

$$\Big(\sum_{g\in G}\lambda_g g\Big)\mu=\sum_{g\in G}(\lambda_g\mu)g, \tag{1.7}$$

$$\Big(\sum_{g\in G}\lambda_g g\Big)\Big(\sum_{g\in G}\mu_g g\Big)=\sum_{g\in G}\Big(\sum_{h\in G}\lambda_h\mu_{h^{-1}g}\Big)g,$$

em que $\lambda_g,\mu_g,\mu\in K$. O conjunto $K[G]$ é uma álgebra-K tal que o elemento zero é $\sum_{g\in G}0_K g$ e o elemento um é $\sum_{g\in G}\delta_{1g}g$, sendo δ_{ab} o símbolo de Kronecker definido por: $\delta_{ab}=1$ se $a=b$ e $\delta_{ab}=0$ se $a\neq b$.

Identificamos um elemento $h\in G$ com o elemento $\sum_{g\in G}\delta_{hg}g\in K[G]$. Assim podemos encarar G como sendo um subconjunto de $K[G]$; a multiplicação original em G é a restrição da multiplicação em $K[G]$.

A $K[G]$ dá-se o nome de *álgebra de grupo* e o conjunto G é uma base de $K[G]$ sobre K, encarando

$$G=\{h:h\in G\}=\{\sum_{g\in G}\delta_{hg}g:h\in G\}.$$

Mais geralmente, se S é um monóide, podemos definir de modo análogo uma *álgebra de monóide* como sendo o conjunto $K[S]$, em que a adição e multiplicação escalar em $K[S]$ são definidas como em (1.6) e (1.7) e a multiplicação é dada por

$$\Big(\sum_{s\in S}\lambda_s s\Big)\Big(\sum_{s\in S}\mu_s s\Big)=\sum_{s,t\in S}(\lambda_s\mu_t)st,$$

em que $\lambda_s,\mu_s\in K$.

Note-se que S pode ser finito ou infinito pois vamos considerar que cada elemento $x\in K[S]$ tem uma expansão na forma

$$x=\sum_{s\in S}\lambda_s s$$

com apenas um número finito de coeficientes $\lambda_s\neq 0$.

Proposição 1.10.1. [8, 10] *Sejam K um corpo, G um grupo, V um espaço vectorial de dimensão finita sobre K e $\rho:G\to GL(V)$ uma representação de G sobre K. Então ρ induz uma representação única $\bar{\rho}$ de $K[G]$ sobre o espaço vectorial V sobre K tal que $\bar{\rho}_{|G}=\rho$, definida por*

$$\begin{array}{rcl}\bar{\rho}:K[G] & \longrightarrow & End_K(V)\\ \sum_{g\in G}\lambda_g g & \longmapsto & \sum_{g\in G}(g\rho)\lambda_g.\end{array}$$

Sejam G um grupo finito, K um corpo e V um espaço vectorial sobre K de dimensão $n \in \mathbb{N}$. Diz-se que V é um *módulo-G à direita* se G actua à direita sobre $(V, +)$ por endomorfismos $(1, 2, 3)$ e se a acção respeita o produto por escalar (4), i.e.

(1) $v(gh) = (vg)h$, para $v \in V$, $g, h \in G$;

(2) $v1 = v$, para $v \in V$;

(3) $(v + w)g = vg + wg$, para $v, w \in V$, $g \in G$;

(4) $(v\lambda)g = (vg)\lambda$, para $v \in V$, $g \in G$, $\lambda \in K$.

Se $U \subseteq V$ é um subespaço de V e V é um módulo-G, diz-se que U é *G-invariante* se

$$Ug \subseteq U, \quad \text{para qualquer } g \in G.$$

Sejam K um corpo, G um grupo e V um módulo-G (à direita). Um *submódulo-G* de V é um subespaço U de V que é G-invariante; escrevemos $U \leq_G V$.

Proposição 1.10.2. [8] *Sejam V um espaço vectorial de dimensão finita sobre um corpo K e G um grupo finito.*

(1) *Se $\rho : G \to GL(V)$ é uma representação de G sobre V, então V é um módulo-G com respeito à acção definida por*

$$vg = v(g\rho), \text{ para } g \in G, \, v \in V.$$

(2) *Se V é um módulo-G, então a aplicação $g\rho : V \to V$, $v \mapsto vg$, pertence a $GL(V)$. Mais ainda, a aplicação*

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL(V) \\ g & \longmapsto & g\rho \end{array}$$

é um morfismo de grupos, portanto uma representação de G sobre V.

Sejam K um corpo, A uma álgebra-K e V um espaço vectorial sobre K de dimensão $n \in \mathbb{N}_0$. Diz-se que V é um *módulo-A à direita* se A actua à direita sobre $(V, +)$ por endomorfismos e se a acção respeita as operações definidas em A, i.e.

(1) $v(ab) = (va)b$, para $v \in V$, $a, b \in A$;

(2) $v1 = v$, para $v \in V$;

(3) $(v + w)a = va + wa$, para $v, w \in V$, $a \in A$;

(4) $v(a + b) = va + vb$, para $v \in V$, $a, b \in A$;

(5) $(v\lambda)a = (va)\lambda$, para $v \in V$, $a \in A$, $\lambda \in K$.

Sejam K um corpo e A uma álgebra-K. Pretendemos transformar A num módulo-A, para tal definimos uma acção de A sobre A do seguinte modo: dado $\alpha \in A$ (espaço vectorial) e $a \in A$ (álgebra-K),

$$\alpha \cdot a = \alpha a.$$

Verifica-se que A é módulo-A à direita com respeito a esta acção, chamado *módulo regular à direita de A*.

Observação 1.10.3. Vamos agora construir um módulo-$K[G]$ associado a uma representação de G sobre K. Sejam G um grupo finito, V um espaço vectorial de dimensão $n \in \mathbb{N}$ sobre um corpo K e $\rho : G \to GL(V)$ uma representação de G. Munimos V com uma estrutura de módulo-$K[G]$ definida a partir de ρ pela adição usual em V e pela acção definida por

$$vx = v(x\bar{\rho}),\ \forall v \in V,\ \forall x \in K[G],$$

sendo $\bar{\rho} : K[G] \to End_K(V)$ o único endomorfismo tal que $\bar{\rho}_{|_G} = \rho$, que sabemos existir pela Proposição 1.10.1.

Sejam K um corpo, G um grupo e tomemos módulos-$K[G]$ (à direita) V e W. Consideremos ρ, σ as representações de G proporcionadas por V e W, respectivamente.

(1) Um *submódulo-$K[G]$* U de V é um subespaço de V tal que $ux \in U$, quaisquer que sejam $u \in U$ e $x \in K[G]$; escrevemos $U \leq_{K[G]} V$.

(2) Diz-se que V é um módulo-$K[G]$ *irredutível* se $V \neq \{0\}$ e os seus únicos submódulos-$K[G]$ são $\{0\}$ e V.

(3) Diz-se que ρ é uma *representação irredutível de G* se V é um módulo-$K[G]$ irredutível.

Seja K um corpo, A uma álgebra-K e V um módulo-A. Uma *série de composição* de V é uma cadeia de submódulos

$$\{0\} = V_0 < V_1 < \cdots < V_r = V$$

tal que cada quociente V_i/V_{i-1} é irredutível como módulo-A, para $i \in \{1, \ldots, r\}$.

Observemos que, dado que os nossos módulos-A são sempre de dimensão finita sobre K, cada módulo-A não nulo tem (pelo menos) uma série de composição.

Proposição 1.10.4. [11] *Sejam K um corpo de característica p, em que p é um número primo, G um grupo e V um módulo-$K[G]$ irredutível. Então*

$$C_V(O_p(G)) = \{v \in V : vx = v, \forall x \in O_p(G)\}$$

é um submódulo de V. Logo $C_V(O_p(G)) = V$, pois V é módulo-$K[G]$ irredutível.

Proposição 1.10.5. [8] *Sejam G um grupo finito e K um corpo de característica zero ou característica prima p tal que p não divide a ordem de G. Seja $V \neq \{0\}$ um módulo-$K[G]$. Então $V = V_1 \oplus \cdots \oplus V_t$, em que todos os V_i são submódulos-$K[G]$ irredutíveis de V.*

Proposição 1.10.6. [8] *Sejam K um corpo e A uma álgebra-K. Então cada módulo-A irredutível é cíclico.*

No que se segue representamos por $K[t]$ o anel de polinómios em t com coeficientes em K.

Proposição 1.10.7. [8] *Seja G um grupo finito abeliano cujo expoente divide n. Sejam K um corpo e V um módulo-$K[G]$ irredutível. Suponhamos que $t^n - 1$ se decompõe em $K[t]$ como produto de factores de grau 1. Então a dimensão de V sobre K é 1.*

1.11 Transdutores

Neste trabalho será útil utilizarmos conceitos mais gerais do que o de autómato, nomeadamente os de transdutor e transdutor subsequencial.

Um *transdutor* (sobre um anel R) é um quíntuplo $\mathcal{T} = (Q, A, R, E, I, F)$, em que

- Q é um conjunto finito de estados;
- A é um alfabeto finito de entradas;
- R é um anel de saída (pode ser infinito);
- $E \subseteq Q \times A \times R \times Q$ (finito) é o conjunto de transições;
- $I \subseteq Q$ é o conjunto dos estados iniciais;
- $F \subseteq Q$ é o conjunto dos estados finais.

Intuitivamente, uma transição (p, a, r, q) pode ser interpretada do seguinte modo:

Encontrando-se o transdutor no estado p ao receber a entrada a move-se para o estado q e produz a saída r.

Por vezes, analogamente ao que acontece nos autómatos, pode ser conveniente representar a transição (p, a, r, q) por uma seta $p \xrightarrow{a|r} q$. A representação dos estados iniciais e dos estados finais é feita como nos autómatos.

Um *caminho bem sucedido* é uma sequência de transições consecutivas da forma

$$q_0 \xrightarrow{a_1|r_1} q_1 \xrightarrow{a_2|r_2} q_2 \cdots q_{n-1} \xrightarrow{a_n|r_n} q_n,$$

em que as extremidades q_0 e q_n são um estado inicial e um final, respectivamente.

A *etiqueta* do caminho é a palavra $a_1a_2 \ldots a_n$. A *saída* é o produto $r_1r_2 \ldots r_n$. A *função realizada por* $\mathcal{T}$ (*transdução*) transforma cada palavra $u \in A^*$ na soma das saídas de todos os caminhos bem sucedidos de etiqueta u.

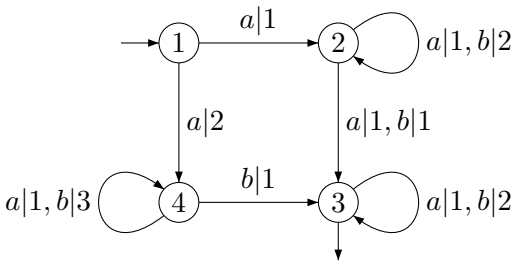


Figura 1.2: Um transdutor com saídas em $\mathbb{Z}$.

Por exemplo, se τ é a transdução realizada pelo transdutor da figura 1.2, existem quatro caminhos bem sucedidos com etiqueta *abba*:

$$(1)1 \xrightarrow{a|1} 2 \xrightarrow{b|2} 2 \xrightarrow{b|2} 2 \xrightarrow{a|1} 3 \quad (2)1 \xrightarrow{a|1} 2 \xrightarrow{b|2} 2 \xrightarrow{b|1} 3 \xrightarrow{a|1} 3$$

$$(3)1 \xrightarrow{a|2} 4 \xrightarrow{b|3} 4 \xrightarrow{b|1} 3 \xrightarrow{a|1} 3 \quad (4)1 \xrightarrow{a|2} 4 \xrightarrow{b|1} 3 \xrightarrow{b|2} 3 \xrightarrow{a|1} 3$$

A saída do primeiro caminho é $1 \times 2 \times 2 \times 1 = 4$ e as saídas dos restantes caminhos são respectivamente $2, 6$ e 4. Tem-se então $(abba)\tau = 4+2+6+4 = 16$.

Se $I = \{q_0\} \subseteq Q$ e $\mathcal{T}$ é tal que, para quaisquer $q \in Q$ e $a \in A$ existe no máximo uma transição da forma $(q, a, r, q') \in E$, podemos considerar o seguinte subconjunto de $Q \times A$

$$P = \{(q, a) : \exists q' \in Q,\ \exists r \in R,\ (q, a, r, q') \in E\}$$

e as aplicações

$$\begin{aligned} \cdot : P &\longrightarrow Q \\ (q, a) &\longmapsto q \cdot a \end{aligned}$$

e

$$\begin{aligned} * : P &\longrightarrow R \\ (q, a) &\longmapsto q * a \end{aligned}$$

sendo $q \cdot a$ o único estado $q' \in Q$ tal que $(q, a, r, q') \in E$ e $q * a$ o único elemento $r \in R$ tal que $(q, a, r, q') \in E$. Estas restrições à definição geral de transdutor motivam a seguinte noção de transdutor:

Um *transdutor subsequencial* (sobre um monóide R) é um octúplo $\mathcal{T} = (Q, A, R, q_0, \cdot, *, m, \rho)$, em que

- Q é um conjunto finito de estados;
- A é um alfabeto finito de entradas;
- R é um monóide de saída (pode ser infinito);
- $q_0 \in Q$ é o estado inicial;
- $(q, a) \mapsto q \cdot a \in Q$ (*função de transição*), $(q, a) \mapsto q * a \in R$ (*função de saída*) são funções com o mesmo domínio contido em $Q \times A$;
- $m \in R$ é o prefixo inicial;
- $\rho : Q \to R$ (*função terminal*) é uma função.

Note-se que as funções de transição e de saída não são necessariamente aplicações pois a imagem de um elemento qualquer de $Q \times A$ pode nem sempre estar definida. O mesmo sucede com a função terminal que tem domínio contido em Q.

As funções de transição e de saída prolongam-se a funções $Q \times A^* \to Q$ e $Q \times A^* \to R$ do seguinte modo:

Para cada $u \in A^*$ e $a \in A$,

$q \cdot 1 = q$	$q * 1 = 1$
$q \cdot (ua) = (q \cdot u) \cdot a$	se $q \cdot u$ e $(q \cdot u) \cdot a$ estão definidos
$q * (ua) = (q * u)((q \cdot u) * a)$	se $q * u$, $q \cdot u$ e $(q \cdot u) * a$ estão definidos

Introduzem-se algumas regras de prioridade nos operadores de forma a simplificar a escrita. Dá-se a maior prioridade ao produto (concatenado), depois à operação ponto ($\cdot$) e por fim à operação estrela ($*$). Assim escrevemos, por exemplo, $q \cdot ua$ em vez de $q \cdot (ua)$, $q * ua$ em vez de $q * (ua)$ e $q \cdot u * a$ em vez de $(q \cdot u) * a$.

A *função realizada pelo transdutor subsequencial* $\mathcal{T}$ é a função $\varphi : A^* \to R$ definida por

$$u\varphi = m(q_0 * u)(q_0 \cdot u)\rho, \quad \text{para todo o } u \in A^*.$$

Uma *função subsequencial* é uma função que pode ser realizada por um transdutor subsequencial.

O *monóide de transformações de um transdutor subsequencial* $\mathcal{T} = (Q, A, R, q_0, \cdot, *, m, \rho)$ é, por definição, o monóide de transformações do autómato $(Q, A, \cdot, q_0, \emptyset)$.

Um *transdutor sequencial* é uma versão mais simplificada do anterior, sem prefixo inicial nem função terminal. Mais precisamente é um transdutor subsequencial em que o prefixo inicial é $m = 1$ e a função terminal transforma todo o estado em 1, i.e. $q\rho = 1$, para todo o $q \in Q$. Neste caso, escrevemos $\mathcal{T} = (Q, A, R, q_0, \cdot, *)$ e a *função realizada por* $\mathcal{T}$ é a função $\varphi : A^* \to R$ definida por

$$u\varphi = q_0 * u, \quad \text{para todo o } u \in A^*.$$

Uma *função sequencial* é uma função que pode ser realizada por um transdutor sequencial.

Capítulo 2

Pseudovariedades de Grupos

Neste capítulo pretendemos descrever a pseudovariedade dos grupos super-resolúveis. Com vista a essa descrição abordaremos diversas classes de grupos, nomeadamente as pseudovariedades: produto de pseudovariedades de grupos; dos grupos abelianos cujo expoente divide um dado natural n; dos p-grupos.

Uma classe $\mathbf{G}$ de grupos finitos diz-se uma *pseudovariedade de grupos* se $\{1\} \in \mathbf{G}$ e além disso verifica as condições seguintes:

(1) Se $A \in \mathbf{G}$ e B é um subgrupo de A então $B \in \mathbf{G}$;

(2) Se $A \in \mathbf{G}$, B é um grupo e $\varphi : A \twoheadrightarrow B$ é um epimorfismo então $B \in \mathbf{G}$;

(3) Se $A, B \in \mathbf{G}$ então $A \times B \in \mathbf{G}$.

Note-se que toda a pseudovariedade de grupos é uma pseudovariedade de monóides uma vez que todo o submonóide de um grupo finito é, ele próprio, um grupo, pois todo o elemento num semigrupo (monóide) finito tem uma potência que é um idempotente. Reciprocamente, é claro que toda a pseudovariedade de monóides cujos elementos são grupos é uma pseudovariedade de grupos.

Assim sendo, podemos aplicar os resultados já conhecidos sobre pseudovariedades de monóides às pseudovariedades de grupos.

A classe de todas as pseudovariedades de grupos forma um reticulado completo para a inclusão, logo existe supremo (e ínfimo) de qualquer família de pseudovariedades de grupos. De facto, dada uma família $(\mathbf{H}_i)_{i\in I}$ de pseudovariedades de grupos, o seu supremo é a pseudovariedade $\bigvee_{i\in I} \mathbf{H}_i$ dos grupos G tais que $G \simeq H/N$, em que

$$H \leq H_1 \times \cdots \times H_n \text{ com } H_k \in \mathbf{H}_{i_k}, \text{ para } k \in \{1, \ldots, n\},\ i_k \in I \text{ e } N \trianglelefteq H,$$

i.e. dos grupos G que são isomorfos a quocientes de subgrupos de produtos directos finitos de elementos das pseudovariedades $\mathbf{H}_i$.

As pseudovariedades que vão ter um papel importante ao longo de todo este trabalho são as seguintes:

Dado um número primo p, denote-se por $\mathbf{G}_p$ a classe de todos os p-grupos finitos. Verifica-se facilmente que $\mathbf{G}_p$ é uma pseudovariedade de grupos.

Dada uma pseudovariedade de grupos $\mathbf{H}$, a classe dos grupos de $\mathbf{H}$ cuja ordem não é divisível por p forma também uma pseudovariedade que denotamos por $\mathbf{H}_{p'}$.

São também exemplos de pseudovariedades de grupos a classe $\mathbf{Ab}$ de todos os grupos abelianos, a classe $\mathbf{S}$ de todos os grupos resolúveis e a classe $\mathbf{N}$ de todos os grupos nilpotentes. Dado $n \in \mathbb{N}$, a classe $\mathbf{Ab}^n$ de todos os grupos abelianos cujo expoente divide n é outro exemplo de pseudovariedade de grupos.

2.1 A pseudovariedade produto

Dadas duas pseudovariedades de grupos $\mathbf{U}$ e $\mathbf{V}$, define-se a *pseudovariedade produto* $\mathbf{U} * \mathbf{V}$ do seguinte modo:

$$G \in \mathbf{U} * \mathbf{V} \quad \text{sse} \quad \exists U \in \mathbf{U}, \quad U \trianglelefteq G \quad \text{tal que} \quad G/U \in \mathbf{V}.$$

É fácil verificar que $\mathbf{U} * \mathbf{V}$ é de facto uma pseudovariedade de grupos.

No que se segue é útil ter presente duas caracterizações alternativas da pseudovariedade produto. Para estabelecer essas caracterizações precisamos de dois resultados auxiliares. O primeiro diz-nos o seguinte:

Lema 2.1.1. *Sejam G um grupo e $H \trianglelefteq G$. Então o grupo G mergulha-se em $H \circ (G/H)$.*

Demonstração. Escolhemos um conjunto completo de representantes das classes de G/H denotando, para cada $u \in G$, por $\overline{u}$ o representante da sua classe Hu. Assim, $Hu = H\overline{u}$. Essa escolha será feita de tal forma que $\overline{1} = 1$.

Para cada $u \in G$, definimos

$$\begin{array}{rcl} f_u : G/H & \longrightarrow & H \\ H\overline{v} & \longmapsto & \overline{v}\, u\, \overline{vu}^{-1} \end{array}$$

Provemos que f_u é uma aplicação.

Sejam $u \in G$ e $H\overline{v} \in G/H$. Tem-se:

$H(\overline{v}\, u\, \overline{vu}^{-1}) = H\overline{v}Hu H\overline{vu}^{-1} = HvHu(Hvu)^{-1} = Hvu(vu)^{-1} = H$. Portanto $\overline{v}\, u\, \overline{vu}^{-1} \in H$.

Tomemos $H\overline{v_1}, H\overline{v_2} \in G/H$ tais que $H\overline{v_1} = H\overline{v_2}$. Então:

$H\overline{v_1 u} = Hv_1u = Hv_1Hu = H\overline{v_1}Hu = H\overline{v_2}Hu = Hv_2Hu = Hv_2u = H\overline{v_2 u}$. Portanto tem-se $\overline{v_1 u} = \overline{v_2 u}$, atendendo ao modo como escolhemos os representantes, pelo que se conclui que $\overline{v_1}\, u\, \overline{v_1 u}^{-1} = \overline{v_2}\, u\, \overline{v_2 u}^{-1}$. Logo f_u é uma aplicação.

Consideremos agora a seguinte aplicação

$$\begin{array}{rcl} \varphi : G & \longrightarrow & H \circ (G/H) = H^{G/H} \rtimes G/H \\ u & \longmapsto & (f_u, H\overline{u}) \end{array}$$

Vejamos que se trata de um monomorfismo de grupos:

Sejam $u, v \in G$. Tem-se

$$(uv)\varphi = (f_{uv}, H\overline{uv})$$

e

$$(u\varphi)(v\varphi) = (f_u, H\overline{u})(f_v, H\overline{v}) = (f_u(H\overline{u} \cdot f_v), H\overline{u}H\overline{v}).$$

Ora, $H\overline{u}H\overline{v} = HuHv = Huv = H\overline{uv}$ e, para qualquer $H\overline{w} \in G/H$,

$$\begin{array}{rcl} (H\overline{w})(f_u(H\overline{u} \cdot f_v)) & = & (H\overline{w})f_u(H\overline{w})(H\overline{u} \cdot f_v) \\ & = & (H\overline{w})f_u(H\overline{w}H\overline{u})f_v \\ & = & (H\overline{w})f_u(H\overline{wu})f_v \\ & = & (\overline{w}\, u\, \overline{wu}^{-1})(\overline{wu}\, v\, \overline{wuv}^{-1}) \\ & = & \overline{w}\, uv\, \overline{wuv}^{-1} = (H\overline{w})f_{uv}, \end{array}$$

donde $(uv)\varphi = (u\varphi)(v\varphi)$, quaisquer que sejam $u, v \in G$. Consequentemente φ é um morfismo de grupos.

De facto φ é um monomorfismo. Mostremos que $\ker\varphi = \{1_G\}$. Recordemos que a identidade de $H \circ (G/H)$ é $(1_{H^{G/H}}, H\overline{1})$, em que $1_{H^{G/H}}$ é a aplicação de G/H em H que transforma qualquer elemento Hg de G/H na identidade de H. Fixemos $u \in G$ e $h = Hf_u$. Temos $h = (H\overline{1})f_u = \overline{1}\, u\, \overline{1u}^{-1} = u\,\overline{u}^{-1}$ pelo que $h\overline{u} = u$. Ora,

$$\ker\varphi = \{u \in G : (f_u, H\overline{u}) = (1_{H^{G/H}}, H\overline{1})\},$$

donde se $u \in \ker\varphi$ então $H\overline{u} = H\overline{1}$, logo $\overline{u} = \overline{1} = 1$ e portanto $h = u$. Mas $h = Hf_u = (H)1_{H^{G/H}} = 1_H$ pelo que $u = h = 1_H = 1_G$. Portanto $\ker\varphi = \{1_G\}$, pelo que φ é um monomorfismo, como pretendido. □

O segundo resultado que precisamos diz-nos o seguinte:

Lema 2.1.2. *Sejam S e T grupos. Então $S \rtimes T$ mergulha-se em $S^T \rtimes T$.*

Demonstração. Para cada $s \in S$, definimos uma aplicação $f_s : T \to S$ por $tf_s = t \cdot s$, para todo o $t \in T$, em que $\cdot$ denota a acção proveniente do produto semidirecto $S \rtimes T$.

Consideremos agora a aplicação dada por

$$\begin{array}{rcl} \theta : S \rtimes T & \longrightarrow & S^T \rtimes T \\ (s,t) & \longrightarrow & (f_s, t) \end{array}$$

A aplicação θ é claramente injectiva pois, se $(f_{s_1}, t_1) = (f_{s_2}, t_2)$ então $t_1 = t_2$ e $f_{s_1} = f_{s_2}$, pelo que $s_1 = 1 \cdot s_1 = 1f_{s_1} = 1f_{s_2} = 1 \cdot s_2 = s_2$.

Mais, para quaisquer $s_1, s_2 \in S$ e $t_1, t_2, t \in T$,

$$\begin{array}{rcl} t(f_{s_1}(t_1 \cdot f_{s_2})) & = & tf_{s_1}(tt_1)f_{s_2} = (t \cdot s_1)((tt_1) \cdot s_2) \\ & = & (t \cdot s_1)(t \cdot (t_1 \cdot s_2)) = t \cdot (s_1(t_1 \cdot s_2)) \\ & = & tf_{s_1(t_1 \cdot s_2)}, \end{array}$$

donde $f_{s_1}(t_1 \cdot f_{s_2}) = f_{s_1(t_1 \cdot s_2)}$. Portanto

$$(f_{s_1}, t_1)(f_{s_2}, t_2) = (f_{s_1}(t_1 \cdot f_{s_2}), t_1t_2) = (f_{s_1(t_1 \cdot s_2)}, t_1t_2),$$

quaisquer que sejam $s_1, s_2 \in S$ e $t_1, t_2 \in T$.

Portanto θ é um monomorfismo. □

Estamos agora em condições de demonstrar a primeira caracterização alternativa da pseudovariedade produto:

Teorema 2.1.3 (Teorema de Kaloužnin-Krasner)**.** *Sejam* $\boldsymbol{U}$ *e* $\boldsymbol{V}$ *pseudovariedades de grupos. Então*

$$\boldsymbol{U} * \boldsymbol{V} = \{G \textit{ grupo} : G \lesssim A \rtimes B, \textit{ com } A \in \boldsymbol{U} \textit{ e } B \in \boldsymbol{V}\}.$$

Demonstração. Seja

$$X = \{G \text{ grupo} : G \lesssim A \rtimes B, \text{ com } A \in \mathbf{U} \text{ e } B \in \mathbf{V}\}.$$

Seja $G \in X$. Existe H tal que $G \simeq H$, com $H \leq A \rtimes B$, em que $A \in \mathbf{U}$ e $B \in \mathbf{V}$.

Ora, $A \times \{1\} \trianglelefteq A \rtimes B$, $A \times \{1\} \simeq A \in \mathbf{U}$, logo $A \times \{1\} \in \mathbf{U}$, e $\{1\} \times B \simeq B \in \mathbf{V}$, logo $\{1\} \times B \in \mathbf{V}$. Mais, a aplicação

$$\begin{array}{rcl} A \rtimes B & \longrightarrow & \{1\} \times B \\ (a,b) & \longrightarrow & (1,b) \end{array}$$

é um epimorfismo cujo kernel é o grupo $A \times \{1\}$ logo, pelo Teorema do Homomorfismo (1.8.17), tem-se

$$\{1\} \times B \simeq \frac{A \rtimes B}{A \times \{1\}}.$$

Portanto $A \rtimes B \in \mathbf{U} * \mathbf{V}$.

Então $G \simeq H$, $H \leq A \rtimes B$ e $A \rtimes B \in \mathbf{U} * \mathbf{V}$, pelo que $G \in \mathbf{U} * \mathbf{V}$.

Reciprocamente, tomemos $G \in \mathbf{U} * \mathbf{V}$. Existe $N \trianglelefteq G$, $N \in \mathbf{U}$ tal que $G/N \in \mathbf{V}$. Pelo Lema 2.1.1, G mergulha-se em $N \circ (G/N) = N^{G/N} \rtimes G/N$, isto é, $G \lesssim N^{G/N} \rtimes G/N$. Mas $N \in \mathbf{U}$ e G/N é finito logo $N^{G/N} \in \mathbf{U}$. Portanto $G \in X$. □

Note-se que a demonstração deste teorema permite também concluir que, se $A \in \mathbf{U}$ e $B \in \mathbf{V}$, em que $\mathbf{U}$ e $\mathbf{V}$ são pseudovariedades de grupos, então $A \rtimes B \in \mathbf{U} * \mathbf{V}$.

Como consequência obtém-se uma outra caracterização da pseudovariedade produto:

Corolário 2.1.4. *Sejam $\boldsymbol{U}$ e $\boldsymbol{V}$ pseudovariedades de grupos. Tem-se*

$$\boldsymbol{U} * \boldsymbol{V} = \{G \textit{ grupo} : G \mid (S \circ T), \textit{ tal que } S \in \boldsymbol{U} \textit{ e } T \in \boldsymbol{V}\}.$$

Demonstração. Sejam G um grupo, $S \in \mathbf{U}$ e $T \in \mathbf{V}$ tais que $G \mid (S \circ T)$. Então $S^T \simeq S^{|T|}$ e $S^{|T|} \in \mathbf{U}$, pois T é finito, pelo que $S^T \in \mathbf{U}$. Portanto $S \circ T = S^T \rtimes T \in \mathbf{U} * \mathbf{V}$, donde $G \in \mathbf{U} * \mathbf{V}$.

Reciprocamente, seja $G \in \mathbf{U} * \mathbf{V}$. Pelo Teorema de Kaloužnin-Krasner (2.1.3) tem-se $G \lesssim S \rtimes T$, em que $S \in \mathbf{U}$ e $T \in \mathbf{V}$. Mas, pelo Lema 2.1.2, tem-se $S \rtimes T \lesssim S^T \rtimes T = S \circ T$, pelo que $G \lesssim S \circ T$. Em particular, $G \mid (S \circ T)$. □

Note-se que o produto semidirecto de monóides é uma operação não associativa. No entanto, a operação $*$ entre pseudovariedades já é associativa. Para demonstrar este facto vamos precisar do seguinte lema técnico:

Lema 2.1.5. *Sejam A, B e C grupos. Tem-se:*

$$(A \circ B) \circ C \simeq A^{B \times C} \rtimes (B \circ C)\,.$$

Demonstração. Note-se que

$$(A \circ B) \circ C = (A^B \rtimes B)^C \rtimes C \;\text{ e }\; A^{B\times C} \rtimes (B \circ C) = A^{B\times C} \rtimes (B^C \rtimes C).$$

Consideremos

$$\begin{array}{rcl} \theta : \left(A^B \rtimes B\right)^C \rtimes C & \longrightarrow & A^{B\times C} \rtimes \left(B^C \rtimes C\right) \\ (f, c) & \longmapsto & (g, (h, c)) \end{array}$$

em que, para cada $c' \in C$, $c'f = (k^{(c')}, b')$, $k^{(c')} : B \to A$ é uma aplicação e $b' \in B$. Definimos $g : B \times C \to A$ por $(b, c')g = bk^{(c')}$, em que $b \in B$, e $h : C \to B$ por $c'h = b'$. Portanto $c'f = (k^{(c')}, b') = (k^{(c')}, c'h)$.

Sejam $f_1, f_2 \in \big(A^B \rtimes B\big)^C$, $c_1, c_2 \in C$ tais que $(f_1, c_1) = (f_2, c_2)$. Então, para qualquer $c' \in C$ tem-se

$$(k_1^{(c')}, c'h_1) = c'f_1 = c'f_2 = (k_2^{(c')}, c'h_2).$$

Logo $k_1^{(c')} = k_2^{(c')}$ e $h_1 = h_2$. Mas $bk_1^{(c')} = (b, c')g_1$ e $bk_2^{(c')} = (b, c')g_2$, qualquer que seja $b \in B$, pelo que $g_1 = g_2$. Assim θ é uma aplicação.

Vejamos que θ é um isomorfismo.

Sejam $f_1, f_2 \in \big(A^B \rtimes B\big)^C$, $c_1, c_2 \in C$, $(f_1, c_1)\theta = (g_1, (h_1, c_1))$ e $(f_2, c_2)\theta = (g_2, (h_2, c_2))$ em que, para quaisquer $b \in B$ e $c' \in C$, os elementos $c'f_1 = (k_1^{(c')}, c'h_1)$ e $c'f_2 = (k_2^{(c')}, c'h_2)$ são tais que $bk_1^{(c')} = (b, c')g_1$ e $bk_2^{(c')} = (b, c')g_2$.

Vamos definir uma acção à esquerda de $B^C \rtimes C = B \circ C$ sobre $A^{B\times C}$ que irá definir um produto semidirecto externo $A^{B\times C} \rtimes (B \circ C)$:

$$\begin{array}{rcl} (B^C \rtimes C) \times A^{B\times C} & \longrightarrow & A^{B\times C} \\ ((h, c), g) & \longmapsto & (h, c) \cdot g \end{array}$$

sendo,

$$\begin{array}{rcl} (h, c) \cdot g : B \times C & \longrightarrow & A \\ (b, c') & \longmapsto & (b(c'h), c'c)g \end{array} \tag{2.1}$$

É fácil verificar que esta aplicação define uma acção por automorfismos e é unitária à direita, condições essas que permitem definir um produto semidirecto externo.

Ora,

$$\begin{array}{rcl} (f_1, c_1)\theta(f_2, c_2)\theta & = & \big(g_1, (h_1, c_1)\big)\big(g_2, (h_2, c_2)\big) \\ & = & \Big(g_1\big((h_1, c_1) \cdot g_2\big), (h_1, c_1)(h_2, c_2)\Big) \\ & = & \Big(g_1\big((h_1, c_1) \cdot g_2\big), \big(h_1(c_1 \cdot h_2), c_1c_2\big)\Big) \end{array}$$

e $(f_1, c_1)(f_2, c_2) = (f_1(c_1 \cdot f_2), c_1c_2)$. Mas, para qualquer $c' \in C$, tem-se

$$\begin{array}{rcl} c'\big(f_1(c_1 \cdot f_2)\big) & = & c'f_1(c'c_1)f_2 \\ & = & \Big(k_1^{(c')}, c'h_1\Big)\Big(k_2^{(c'c_1)}, (c'c_1)h_2\Big) \\ & = & \Big(k_1^{(c')}\Big(c'h_1 \cdot k_2^{(c'c_1)}\Big), c'h_1(c'c_1)h_2\Big) \\ & = & \Big(k_1^{(c')}\Big(c'h_1 \cdot k_2^{(c'c_1)}\Big), c'\Big(h_1(c_1 \cdot h_2)\Big)\Big) \end{array}$$

Além disso, para qualquer $b \in B$,

$$\begin{aligned} b\Big(k_1^{(c')}\Big(c'h_1 \cdot k_2^{(c'c_1)}\Big)\Big) &= bk_1^{(c')}(b(c'h_1))k_2^{(c'c_1)} \\ &= (b,c')g_1(b(c'h_1),c'c_1)g_2 \\ &\overset{(2.1)}{=} (b,c')g_1(b,c')\big((h_1,c_1)\cdot g_2\big) \\ &= (b,c')\big(g_1\big((h_1,c_1)\cdot g_2\big)\big) \end{aligned}$$

Portanto $(f_1,c_1)\theta(f_2,c_2)\theta = ((f_1,c_1)(f_2,c_2))\theta$ e, consequentemente, θ é um morfismo.

Sejam $f_1, f_2 \in \big(A^B \rtimes B\big)^C$ e $c_1, c_2 \in C$ tais que $(f_1,c_1)\theta = (f_2,c_2)\theta$. Então $(g_1,(h_1,c_1)) = (g_2,(h_2,c_2))$ donde, para qualquer $c' \in C$,

$$c'f_1 = \Big(k_1^{(c')}, c'h_1\Big) = \Big(k_2^{(c')}, c'h_2\Big) = c'f_2$$

Logo $c_1 = c_2$ e $f_1 = f_2$, pelo que θ é injectiva.

Sejam $g \in A^{B\times C}$, $h \in B^C$ e $c \in C$. Definimos

$$\begin{aligned} f : C &\longrightarrow A^B \rtimes B \\ c' &\longmapsto (k^{(c')}, c'h) \end{aligned}$$

em que $bk^{(c')} = (b,c')g$, para cada $b \in B$. Pela forma como definimos θ, a imagem de (f,c) através de θ é precisamente $(g,(h,c))$. Portanto, θ é sobrejectiva. Concluimos que θ é um isomorfismo, como se pretendia. □

Podemos então provar a associatividade da operação $*$ entre pseudovariedades.

Teorema 2.1.6. *Dadas* $\boldsymbol{U}$, $\boldsymbol{V}$ *e* $\boldsymbol{W}$ *pseudovariedades de grupos, tem-se*

$$\boldsymbol{U} * (\boldsymbol{V} * \boldsymbol{W}) = (\boldsymbol{U} * \boldsymbol{V}) * \boldsymbol{W}.$$

Demonstração. Seja $B \in \mathbf{U} * (\mathbf{V} * \mathbf{W})$. Pela definição de $\mathbf{U} * (\mathbf{V} * \mathbf{W})$ existe $B' \in \mathbf{U}$ tal que $B' \trianglelefteq B$ e $B/B' \in \mathbf{V} * \mathbf{W}$. Pela definição de $\mathbf{V} * \mathbf{W}$ existe $B''/B' \trianglelefteq B/B'$, sendo $B'' \trianglelefteq B$ tal que $B' \subseteq B''$, com $B''/B' \in \mathbf{V}$ e $(B/B')/(B''/B') \in \mathbf{W}$.

Ora, $B' \trianglelefteq B$ é tal que $B' \subseteq B''$ pelo que $B' \trianglelefteq B''$. Logo existe $B' \trianglelefteq B''$, $B' \in \mathbf{U}$ e $B''/B' \in \mathbf{V}$, donde $B'' \in \mathbf{U} * \mathbf{V}$. Assim, existe $B'' \trianglelefteq B$ tal que $B'' \in \mathbf{U}*\mathbf{V}$ e $B/B'' \in \mathbf{W}$ porque $B/B'' \simeq (B/B')(B''/B')$, pelo 2º Teorema do Isomorfismo (1.8.19), portanto $B \in (\mathbf{U} * \mathbf{V}) * \mathbf{W}$.

Reciprocamente, seja $B \in (\mathbf{U} * \mathbf{V}) * \mathbf{W}$. Pelo Corolário 2.1.4, existem $T \in \mathbf{U}*\mathbf{V}$ e $W \in \mathbf{W}$ tais que $B \mid (T \circ W)$. Uma vez que $T \in \mathbf{U}*\mathbf{V}$, novamente pelo Corolário 2.1.4, existem $U \in \mathbf{U}$ e $V \in \mathbf{V}$ tais que $T \mid (U \circ V)$.

Portanto, existem $K \leq U \circ V$ e $\psi : K \twoheadrightarrow T$ um epimorfismo. Muito facilmente se conclui que $K \circ W \leq (U \circ V) \circ W$. Defina-se uma aplicação por

$$\begin{array}{rcl} \theta : K \circ W & \longrightarrow & T \circ W \\ (f, w) & \longrightarrow & (f\psi, w) \end{array}$$

Sejam $(f_1, w_1), (f_2, w_2) \in K \circ W$. Para qualquer $w \in W$, tem-se

$$\begin{array}{rcl} w(f_1\psi(w_1 \cdot f_2\psi)) & = & (wf_1)\psi((ww_1)f_2)\psi = ((wf_1)(ww_1)f_2)\psi \\ & = & ((wf_1)w(w_1 \cdot f_2))\psi = (w(f_1(w_1 \cdot f_2)))\psi \\ & = & w(f_1(w_1 \cdot f_2)\psi). \end{array}$$

Portanto,

$$\begin{array}{rcl} ((f_1, w_1)(f_2, w_2))\theta & = & (f_1(w_1 \cdot f_2), w_1w_2)\theta = (f_1(w_1 \cdot f_2)\psi, w_1w_2) \\ & = & (f_1\psi(w_1 \cdot f_2\psi), w_1w_2) = (f_1\psi, w_1)(f_2\psi, w_2) \\ & = & (f_1, w_1)\theta(f_2, w_2)\theta. \end{array}$$

Concluímos que θ é um morfismo. Provemos agora que θ é sobrejectivo. Seja $(g, w) \in T \circ W$. Como ψ é um epimorfismo, pelo Teorema do Homomorfismo (1.8.17),

$$\begin{array}{rcl} K/\ker\psi & \longrightarrow & T \\ k\ker\psi & \longrightarrow & k\psi \end{array}$$

é um isomorfismo. Consideremos $K' \subseteq K$ um conjunto de representantes de $K/\ker\psi$ tal que o representante da classe $\ker\psi$ seja o elemento 1_K. Vamos definir uma aplicação $f : W \to K$ do seguinte modo:

Dado $w_1 \in W$, como $w_1g \in T$ existe um único $k' \in K' \subseteq K$ tal que $k'\psi = w_1g$, definimos $w_1f = k'$. Tem-se $(f, w)\theta = (f\psi, w) = (g, w)$, pois $w_1(f\psi) = k'\psi = w_1g$, para cada $w_1 \in W$. Portanto θ é sobrejectivo e $T \circ W \mid (U \circ V) \circ W$. Mais, como $B \mid T \circ W$, pela propriedade transitiva da relação divide, $B \mid (U \circ V) \circ W$. Mas, pelo Lema 2.1.5, tem-se $(U \circ V) \circ W \simeq U^{V \times W} \rtimes (V \circ W) = U^{V \times W} \rtimes (V^W \rtimes W)$. Ora, $V \times W$ é finito logo $U^{V \times W} \in \mathbf{U}$. Analogamente, $V^W \in \mathbf{V}$. Assim $U^{V \times W} \rtimes (V^W \rtimes W) \in \mathbf{U} * (\mathbf{V} * \mathbf{W})$. Portanto, $(U \circ V) \circ W \in \mathbf{U} * (\mathbf{V} * \mathbf{W})$ donde $B \in \mathbf{U} * (\mathbf{V} * \mathbf{W})$.

Concluímos pois que $\mathbf{U} * (\mathbf{V} * \mathbf{W}) = (\mathbf{U} * \mathbf{V}) * \mathbf{W}$. □

2.2 A pseudovariedade $\mathbf{Ab}^n$

Nesta secção daremos uma caracterização da pseudovariedade $\mathbf{Ab}^n$, dos grupos abelianos cujo expoente divide um dado natural n, a qual será considerada posteriormente no Capítulo 4.

Recordemos que, para cada natural $n \in \mathbb{N}$, o grupo $(\mathbb{Z}_n, +)$ é cíclico de ordem n e é abeliano.

Proposição 2.2.1. *Seja n um natural. A pseudovariedade dos grupos abelianos cujo expoente divide n é gerada pelo grupo $\mathbb{Z}_n$, isto é,*

$$\boldsymbol{Ab}^n = \boldsymbol{V}\langle \mathbb{Z}_n \rangle .$$

Demonstração. Esta prova será feita em dois passos:

1º) Mostramos que $\mathbf{Ab}^n = \mathbf{V}\,[xy = yx, x^n = 1]$;

2º) Mostramos que $\mathbf{V}\,\langle \mathbb{Z}_n \rangle = \mathbf{V}\,[xy = yx, x^n = 1]$.

1º) Seja $G \in \mathbf{Ab}^n$. Então G é abeliano pelo que satisfaz a identidade $xy = yx$. Uma vez que $\text{mmc}(|g| : g \in G) = \exp(G)$ e $\exp(G) \mid n$, tem-se que $|g| \mid n$, donde $g^n = 1$, para todo o $g \in G$. Logo G satisfaz a identidade $x^n = 1$.

Reciprocamente, suponhamos que G satisfaz as identidades $xy = yx$ e $x^n = 1$. Então G é abeliano e, para todo o $g \in G$, tem-se $g^n = 1$, donde $|g| \mid n$, pelo que $\exp(G) = \text{mmc}(|g| : g \in G) \mid n$. Assim $G \in \mathbf{Ab}^n$.

2º) Defina-se $\mathbf{V} = \mathbf{V}\,\langle \mathbb{Z}_n \rangle$. Pela Proposição 1.5.2, $\mathbf{V}$ é definida por uma sequência de identidades. Como $\mathbb{Z}_n$ é um grupo cíclico de ordem n abeliano, $\mathbb{Z}_n \in \mathbf{V}\,[xy = yx, x^n = 1]$ pelo que

$$\mathbf{V} \subseteq \mathbf{V}\,[xy = yx, x^n = 1]\,.$$

Suponhamos que $\mathbf{V} \neq \mathbf{V}\,[xy = yx, x^n = 1]$. Então existiria uma identidade $u = v$ satisfeita por $\mathbf{V}$ mas que não se deduziria de $xy = yx$ nem de $x^n = 1$.

Escolhamos uma tal identidade $u = v$ tal que $|u| + |v|$ seja mínimo, sendo assim u e v contêm no máximo $n - 1$ ocorrências de cada letra pois, caso contrário, usar-se-iam as identidades $xy = yx$ e $x^n = 1$ para obter uma identidade $u = v$ com $|u| + |v|$ menor (por exemplo, $u = u_1 x u_2 x u_3 \ldots x u_n x u_{n+1}$ implicaria $u = u_1 x^n u_2 u_3 \ldots u_{n+1} = u_1 u_2 u_3 \ldots u_{n+1}$).

Queremos provar que u e v contém exactamente as mesmas letras. Seja x uma letra de u. Suponhamos, por absurdo, que x não é uma letra de v, isto é, $|v|_x = 0$. Seja $|u|_x = k$. Recordemos que a identidade $u = v$ é satisfeita por $\mathbf{V}$, logo por $\mathbb{Z}_n$. Substituindo cada ocorrência de x em $u = v$ por $\overline{1}$ e as ocorrências das restantes letras por $\overline{0}$ obtemos $\overline{k} = \overline{0}$, o que é absurdo pois $0 < k \leq n - 1$, uma vez que u contém no máximo $n - 1$ ocorrências de cada letra. Portanto toda a letra de u tem uma ocorrência em v. Analogamente, toda a letra de v tem uma ocorrência em u. Consequentemente, u e v contêm exactamente as mesmas letras.

Como a identidade $u = v$ não se deduz de $xy = yx$ resulta que, para qualquer letra x de u, e consequentemente de v, se tem $|u|_x \neq |v|_x$, caso

contrário, a identidade $u = v$ deduzir-se-ia de $xy = yx$, o que contradiz a hipótese. Seja x uma letra de u. Sem perda de generalidade suponhamos que $|u|_x < |v|_x$. Note-se que $|v|_x \leq n-1$. Tomemos $|u|_x = k$ e $|v|_x = t$. Substituindo todas as ocorrências de x em $u = v$ por $\overline{1}$ e as ocorrências das outras letras por $\overline{0}$, concluímos que $\overline{k} = \overline{t}$ em $\mathbb{Z}_n$, o que é absurdo pois $k < t \leq n-1$.

Assim $\mathbf{V} = \mathbf{V}\,[xy = yx, x^n = 1]$. □

2.3 A pseudovariedade $\mathbf{G}_p$

É objectivo desta secção apresentar duas descrições da pseudovariedade $\mathbf{G}_p$ dos p-grupos finitos, para um dado número primo p. A primeira em termos de identidades que a definem e a segunda usando p-grupos definidos como quocientes de um monóide livre por uma relação de congruência. Esta segunda caracterização será de particular interesse no Capítulo 3, quando se descreverem as linguagens reconhecidas pelos p-grupos.

Proposição 2.3.1. *Dado um número primo p, a pseudovariedade dos p-grupos finitos é a pseudovariedade de grupos ultimamente definida pelas identidades $x^{p^k} = 1$, em que $k \geq 0$, isto é,*

$$\boldsymbol{G}_p = \boldsymbol{V}\left[\!\left[x^{p^k} = 1\,(k \geq 0)\right]\!\right].$$

Demonstração. Se $G \in \mathbf{G}_p$, então $|G| = p^k$, para algum $k \geq 0$. Portanto, para qualquer $g \in G$, temos $g^{p^k} = 1$. Mais ainda, para qualquer $k' \geq k$ tem-se $g^{p^{k'}} = (g^{p^k})^{p^{k'-k}} = 1$, logo G satisfaz as identidades $x^{p^k} = 1$ a partir de certo $k \geq 0$, isto é, $G \in \mathbf{V}\left[\!\left[x^{p^k} = 1\,(k \geq 0)\right]\!\right]$.

Reciprocamente, seja $G \in \mathbf{V}\left[\!\left[x^{p^k} = 1\,(k \geq 0)\right]\!\right]$. Então existe $k \geq 0$ tal que $g^{p^{k'}} = 1$, para quaisquer $g \in G$ e $k' \geq k$, logo $g^{p^k} = 1$, donde $|g| \mid p^k$, para qualquer $g \in G$. Portanto G é um p-grupo. □

Da proposição anterior conclui-se então que

$$\mathbf{G}_p = \bigcup_{k \geq 0} \mathbf{G}_{p,k}, \tag{2.2}$$

sendo $\mathbf{G}_{p,k} = \mathbf{V}\left[x^{p^k} = 1\right]$ a pseudovariedade dos grupos de expoente p^k.

Vamos agora apresentar a segunda caracterização da pseudovariedade $\mathbf{G}_p$. Para isso iremos precisar de alguns resultados auxiliares que passamos a apresentar.

Sejam $u, w \in A^*$ tais que $u = u_1 u_2 \ldots u_n$. O *coeficiente binomial* $\binom{w}{u}$ é definido como sendo o número de factorizações de w na forma $w =$

$v_0u_1v_1u_2\dots v_{n-1}u_nv_n$, com $v_0,\dots,v_n \in A^*$. Portanto o coeficiente binomial conta o número de factorizações de w em que u aparece como subpalavra.

Têm-se as seguintes propriedades do coeficiente binomial:

Proposição 2.3.2. *Seja A um alfabeto finito. Temos*

(1) $\binom{w_1w_2}{u} = \sum_{u=u_1u_2}\binom{w_1}{u_1}\binom{w_2}{u_2}$, *para quaisquer* $w_1, w_2, u, u_1, u_2 \in A^*$;

(2) $\binom{a}{u} = \begin{cases} 1 & , \text{ se } u = 1 \text{ ou } u = a \\ 0 & , \text{ caso contrário,} \end{cases}$ *para quaisquer* $a \in A$, $u \in A^*$;

(3) $\binom{1}{u} = \begin{cases} 1 & , \text{ se } u = 1 \\ 0 & , \text{ caso contrário,} \end{cases}$ *para qualquer* $u \in A^*$.

Note-se que estas propriedades podem ser usadas para definir o coeficiente binomial por indução em $|w|$. Mais, se $w = a^p$ e $u = a^q$, com $q \leq p$, tem-se

$$\binom{w}{u} = \binom{p}{q} = \frac{p!}{q!(p-q)!}.$$

Seja p um número primo. Dada uma palavra $u \in A^*$, define-se uma relação $\sim_u$ em A^* por, para $w_1, w_2 \in A^*$,

$$w_1 \sim_u w_2 \Leftrightarrow \binom{w_1}{v} \equiv \binom{w_2}{v} \pmod{p},$$

para qualquer $v \in A^*$ tal que $u \in A^*vA^*$.

A condição $u \in A^*vA^*$ expressa o facto de v ser um factor de u. A relação $\sim_u$ é uma relação de equivalência.

Proposição 2.3.3. *Para qualquer $u \in A^*$, a relação de equivalência $\sim_u$ é uma relação de congruência em A^*.*

Além disso, $G_u = A^*/\sim_u$ é um p-grupo de expoente $p^{|u|}$.

Demonstração. O facto de $\sim_u$ ser relação de congruência resulta facilmente da definição e da Proposição 2.3.2.

Como esta congruência tem um número finito de classes, pois $|u|$ é finito, resulta que G_u é um monóide finito. Para mostrar que G_u é um p-grupo de expoente $p^{|u|}$ é suficiente mostrar, recordando a notação da página 58, que $G_u \in \mathbf{G}_{p,|u|} = \mathbf{V}\left[x^{p^{|u|}} = 1\right]$, isto é,

$$\forall w \in A^*, \quad ([w]_{\sim_u})^{p^{|u|}} = [1]_{\sim_u},$$

ou, equivalentemente,

$$\forall w \in A^*, \quad w^{p^{|u|}} \sim_u 1.$$

Se provarmos que, para quaisquer $w \in A^*$, $k \in \mathbb{N}$ e $v \in A^*$ tal que $0 < |v| \leq k$, se tem que $\binom{w^{p^k}}{v} \equiv 0 \pmod{p}$ o resultado fica provado. Façamos a demonstração por indução em k:

Se $k = 1$ então v é uma letra e tem-se $\binom{w^p}{v} = |w^p|_v = p|w|_v \equiv 0 \pmod{p}$.

Por indução assumimos que o resultado é válido para qualquer y tal que $0 < |y| \leq k$. Suponhamos que v é tal que $|v| = k + 1$. Tem-se então, pela Proposição 2.3.2 (1) generalizada,

$$\binom{w^{p^{k+1}}}{v} = \sum_{v=v_1 \ldots v_p} \binom{w^{p^k}}{v_1} \cdots \binom{w^{p^k}}{v_p},$$

em que $v_1, \ldots, v_p \in A^*$. Para $i \in \{1, \ldots, p\}$ tal que $0 < |v_i| \leq k$, por hipótese de indução, tem-se $\binom{w^{p^k}}{v_i} \equiv 0 \pmod{p}$ e a parcela $\binom{w^{p^k}}{v_1} \ldots \binom{w^{p^k}}{v_p}$ pode ser omitida. Sobram então as parcelas em que algum $v_i = v$ e os restantes v_j são 1. Neste caso a parcela $\binom{w^{p^k}}{v_1} \ldots \binom{w^{p^k}}{v_p}$ reduz-se a $\binom{w^{p^k}}{v}$. Existem exactamente p parcelas desta forma. Portanto $\binom{w^{p^{k+1}}}{v} = p\binom{w^{p^k}}{v} \equiv 0 \pmod{p}$ como pretendido. Concluímos que G_u é um p-grupo de expoente $p^{|u|}$. □

Dado um alfabeto finito A e um inteiro $k \geq 0$ define-se a congruência

$$\sim_k = \bigcap_{|u|=k} \sim_u .$$

Portanto, para $w_1, w_2 \in A^*$,

$$w_1 \sim_k w_2 \Leftrightarrow \binom{w_1}{v} \equiv \binom{w_2}{v} \pmod{p},$$

para qualquer $v \in A^*$ tal que $|v| \leq k$.

Seja $G_{r,k} = A^*/\sim_k$, em que $r = \text{card}(A)$. Segue-se, do que acabámos de ver e da Proposição 1.1.3, que $G_{r,k}$ é um subgrupo do produto

$$\prod_{\substack{u \in A^* \\ |u|=k}} G_u,$$

pelo que $G_{r,k}$ é um p-grupo de expoente p^k.

Vamos agora dar uma descrição mais algébrica e menos combinatorial dos grupos $G_{r,k}$.

Dados um monóide S (finito ou infinito) e um corpo $\mathbb{F}$, considere-se a álgebra de monóide $\mathbb{F}[S]$ definida na Secção 1.10. Recorde-se que cada elemento $x \in \mathbb{F}[S]$ tem uma expansão na forma

$$x = \sum_{s \in S} \lambda_s s,$$

com apenas um número finito de coeficientes $\lambda_s \neq 0$.

Notemos que o conjunto

$$I = \left\{ \sum_{s \in S} \lambda_s s \in \mathbb{F}[S] : \sum_{s \in S} \lambda_s = 0_{\mathbb{F}} \right\}$$

é um ideal de $\mathbb{F}[S]$. De facto, $I \subseteq \mathbb{F}[S]$ e é tal que $0_{\mathbb{F}[S]} \in I$, pois $0_{\mathbb{F}} = \sum_{s \in S} 0_{\mathbb{F}}$. Mais, quaisquer que sejam $x, y \in I$, tem-se $x = \sum_{s \in S} \lambda_s s$ e $y = \sum_{s \in S} \mu_s s$, donde $x - y = \sum_{s \in S} (\lambda_s - \mu_s) s$, em que

$$\sum_{s \in S} (\lambda_s - \mu_s) = \sum_{s \in S} \lambda_s - \sum_{s \in S} \mu_s = 0_{\mathbb{F}}.$$

Portanto $x - y \in I$. Tomemos $t \in \mathbb{F}[S]$. Então $t = \sum_{s \in S} \mu_s s$, donde $xt = \sum_{s,s' \in S} (\lambda_s \mu_{s'}) ss'$, em que

$$\sum_{s,s' \in S} \lambda_s \mu_{s'} = \sum_{s \in S} \left(\sum_{s' \in S} \lambda_s \right) \mu_{s'} = 0_{\mathbb{F}}$$

pelo que $xt \in I$. Analogamente provamos que $tx \in I$. Além disso, se $\mu \in \mathbb{F}$ obtemos $x\mu = \left(\sum_{s \in S} \lambda_s s \right) \mu = \sum_{s \in S} (\lambda_s \mu) s$, logo

$$\sum_{s \in S} \lambda_s \mu = \left(\sum_{s \in S} \lambda_s \right) \mu = 0_{\mathbb{F}},$$

pelo que $x\mu \in I$. Concluímos então que I é um ideal de $\mathbb{F}[S]$.

Mais ainda, I é o ideal de $\mathbb{F}[S]$ gerado pelos elementos de $\mathbb{F}[S]$ da forma $1 - s$, com $s \in S$:

Seja $s \in S$. Se $s = 1$ então $1 - s = 0_{\mathbb{F}[S]} \in I$. Se $s \neq 1$ então $s = \sum_{t \in S} \delta_{ts} t$ e $1 = \sum_{t \in S} \delta_{t1} t$, em que

$$\delta_{ab} = \begin{cases} 0 & \text{se } a \neq b \\ 1 & \text{se } a = b \end{cases}$$

Portanto $1 - s = \sum_{t \in S} (\delta_{t1} - \delta_{ts}) t$, em que

$$\delta_{t1} - \delta_{ts} = \begin{cases} 1 & \text{se } t = 1 \\ -1 & \text{se } t = s \\ 0 & \text{se } t \neq 1, s \end{cases}$$

logo $\sum_{t \in S} (\delta_{t1} - \delta_{ts}) = 1 - 1 = 0_{\mathbb{F}}$, donde $1 - s \in I$, qualquer que seja $s \in S$. Assim $\{1 - s : s \in S\} \subseteq I$.

Consideremos agora um ideal J de $\mathbb{F}[S]$ tal que $\{1 - s : s \in S\} \subseteq J$. Vamos provar que $I \subseteq J$. Notemos que em $\mathbb{F}[S]$, para qualquer $s \in S$,

$$s 0_{\mathbb{F}} = 0_{\mathbb{F}[S]} \tag{2.3}$$

pois, de $s = \sum_{t\in S} \delta_{ts} t$ obtemos

$$\begin{aligned} s0_{\mathbb{F}} &= \left(\sum_{t\in S} \delta_{ts} t\right) 0_{\mathbb{F}} = \sum_{t\in S} (\delta_{ts} 0_{\mathbb{F}}) t \\ &= \sum_{t\in S} 0_{\mathbb{F}} t = 0_{\mathbb{F}[S]} \end{aligned}$$

Seja $x \in I$, com $x = \sum_{s\in S} \lambda_s s$ tal que $\sum_{s\in S} \lambda_s = 0_{\mathbb{F}}$. No que se segue convém ter presente que podemos escrever

$$\sum_{t\in S} \lambda_t = 0_{\mathbb{F}}. \tag{2.4}$$

Obtemos então

$$\begin{aligned} x &= \sum_{s\in S} \lambda_s s = \sum_{s\in S} \lambda_s s - 0_{\mathbb{F}[S]} \overset{(2.3)}{=} \sum_{s\in S} \lambda_s s - 1_S 0_{\mathbb{F}} \overset{(2.4)}{=} \sum_{s\in S} \lambda_s s - 1_S \left(\sum_{t\in S} \lambda_t\right) \\ &= \sum_{s\in S} \lambda_s s - \left(\sum_{s\in S} \delta_{s1} s\right) \left(\sum_{t\in S} \lambda_t\right) = \sum_{s\in S} \lambda_s s - \sum_{t\in S} \left(\left(\sum_{s\in S} \delta_{s1} s\right) \lambda_t\right) \\ &= \sum_{s\in S} \lambda_s s - \sum_{t\in S} \left(\sum_{s\in S} (\delta_{s1}\lambda_t) s\right) = \sum_{s\in S} \lambda_s s - \sum_{s\in S} \left(\sum_{t\in S} (\delta_{s1}\lambda_t)\right) s \\ &= \sum_{s\in S} \left(\lambda_s - \sum_{t\in S} (\delta_{s1}\lambda_t)\right) s, \end{aligned}$$

pelo que

$$x = \sum_{s\in S} \left(\lambda_s - \sum_{t\in S} (\delta_{s1}\lambda_t)\right) s. \tag{2.5}$$

Então

$$\begin{aligned} \sum_{\substack{t\in S \\ t\neq 1}} (t - 1_S)\lambda_t &= \sum_{\substack{t\in S \\ t\neq 1}} \left(\left(\sum_{s\in S} \delta_{st} s - \sum_{s\in S} \delta_{s1} s\right) \lambda_t\right) \\ &= \sum_{\substack{t\in S \\ t\neq 1}} \left(\left(\sum_{s\in S} (\delta_{st} s - \delta_{s1}) s\right) \lambda_t\right) \\ &= \sum_{\substack{t\in S \\ t\neq 1}} \left(\sum_{s\in S} \big((\delta_{st} - \delta_{s1})\lambda_t\big) s\right) \\ &= \sum_{s\in S} \left(\sum_{\substack{t\in S \\ t\neq 1}} (\delta_{st} - \delta_{s1})\lambda_t\right) s \end{aligned} \tag{2.6}$$

Se $s = 1$, tem-se

$$\lambda_1 - \sum_{t\in S}(\delta_{1,1}\lambda_t) = \lambda_1 - \sum_{t\in S}\lambda_t = -\sum_{\substack{t\in S\\ t\neq 1}}\lambda_t,$$

além disso

$$\sum_{\substack{t\in S\\ t\neq 1}}(\delta_{1t} - \delta_{11})\lambda_t = -\sum_{\substack{t\in S\\ t\neq 1}}\lambda_t.$$

Se $s \neq 1$ tem-se

$$\sum_{\substack{t\in S\\ t\neq 1}}(\delta_{st} - \delta_{s1})\lambda_t = \sum_{\substack{t\in S\\ t\neq 1}}\delta_{st}\lambda_t = \lambda_s.$$

Tendo em conta as fórmulas (2.5) e (2.6), obtém-se

$$x \overset{(2.5)}{=} \sum_{s\in S}\left(\lambda_s - \sum_{t\in S}(\delta_{s1}\lambda_t)\right)s = \sum_{s\in S}\left(\sum_{\substack{t\in S\\ t\neq 1}}(\delta_{st} - \delta_{s1})\lambda_t\right)s \overset{(2.6)}{=} \sum_{\substack{t\in S\\ t\neq 1}}(t - 1_S)\lambda_t.$$

Portanto $x \in J$. Logo $I \subseteq J$. Concluímos pois que I é o ideal de $\mathbb{F}[S]$ gerado pelos elementos da forma $1 - s$, com $s \in S$.

Se $S = A^*$, em que $A = \{a_1, \ldots, a_r\}$ é um alfabeto com r letras, então $\mathbb{F}[S]$ é o anel de polinómios $\mathbb{F}[a_1, \ldots, a_r]$ com variáveis não comutativas $a_1, \ldots, a_r$ e coeficientes em $\mathbb{F}$.

No que se segue $\mathbb{F}$ será o corpo finito $\mathbb{Z}_p$ com p elementos, em que p é um número primo.

Lema 2.3.4. *Seja A um alfabeto finito. Então $\mathbb{Z}_p[A^*]$ é a álgebra-$\mathbb{Z}_p$ livre gerada pelo conjunto A, isto é, existe uma aplicação $\iota : A \to \mathbb{Z}_p[A^*]$ tal que, para qualquer monóide M e qualquer aplicação $f : A \to \mathbb{Z}_p[M]$, existe um e um só morfismo $\theta : \mathbb{Z}_p[A^*] \to \mathbb{Z}_p[M]$ tal que o diagrama*

$$\begin{array}{ccc} A & \xrightarrow{\iota} & \mathbb{Z}_p[A^*] \\ & \searrow^{f} & \downarrow{\scriptstyle \theta} \\ & & \mathbb{Z}_p[M] \end{array} \tag{2.7}$$

é comutativo, ou seja, $\iota\theta = f$.

Demonstração. Consideremos a aplicação

$$\begin{array}{rcl} \iota : A & \longrightarrow & \mathbb{Z}_p[A^*] \\ a & \longmapsto & \displaystyle\sum_{u\in A^*}\delta_{ua}u = a \end{array}$$

Tomemos um monóide M e uma aplicação $f : A \to \mathbb{Z}_p[M]$ arbitrários. Vamos construir um morfismo $\theta : \mathbb{Z}_p[A^*] \to \mathbb{Z}_p[M]$ do seguinte modo:

Para cada $u \in A^*$, seja $r_u = |u| \in \mathbb{N}_0$ e decomponhamos u como produto de letras de A tal que $u = a_1 \dots a_{r_u}$. Queremos um morfismo θ tal que $(1_{\mathbb{Z}_p[A^*]})\theta = 1_{\mathbb{Z}_p[M]}$ e $af = a(\iota\theta) = (a\iota)\theta = \left(\sum_{u\in A^*} \delta_{ua} u\right)\theta$. Notemos primeiro que, dado $x = \sum_{u\in A^*} \lambda_u u \in \mathbb{Z}_p[A^*]$, se tem

$$\begin{aligned}
\sum_{u\in A^*} \lambda_u u &= \sum_{u\in A^*} \left(\sum_{v\in A^*} (\delta_{vu}\lambda_u) v \right) \\
&= \sum_{u\in A^*} \left(\sum_{v_1,\dots,v_{r_u}\in A^*} \big((\delta_{a_1 v_1} \dots \delta_{a_{r_u} v_{r_u}})\lambda_u\big) v_1 \dots v_{r_u} \right) \\
&= \sum_{u\in A^*} \left(\sum_{v_1,\dots,v_{r_u}\in A^*} (\delta_{a_1 v_1} \dots \delta_{a_{r_u} v_{r_u}}) v_1 \dots v_{r_u} \right) \lambda_u \\
&\quad \sum_{u\in A^*} \left(\sum_{v_1\in A^*} \delta_{a_1 v_1} v_1 \dots \sum_{v_{r_u}\in A^*} \delta_{a_{r_u} v_{r_u}} v_{r_u} \right) \lambda_u
\end{aligned}$$

pelo que pretendemos ter

$$\begin{aligned}
\left(\sum_{u\in A^*} \lambda_u u\right)\theta &= \left(\sum_{u\in A^*} \left(\sum_{v_1\in A^*} \delta_{a_1 v_1} v_1 \dots \sum_{v_{r_u}\in A^*} \delta_{a_{r_u} v_{r_u}} v_{r_u} \right) \lambda_u \right) \theta \\
&= \left(\left(\sum_{u\in A^*} \left(\sum_{v_1\in A^*} \delta_{a_1 v_1} v_1 \dots \sum_{v_{r_u}\in A^*} \delta_{a_{r_u} v_{r_u}} v_{r_u} \right) \right) \theta \right) \lambda_u \\
&= \sum_{u\in A^*} \left(\left(\sum_{v_1\in A^*} \delta_{a_1 v_1} v_1 \right) \theta' \dots \left(\sum_{v_{r_u}\in A^*} \delta_{a_{r_u} v_{r_u}} v_{r_u} \right) \theta' \right) \lambda_u \\
&= \sum_{u\in A^*} \Big((a_1 f) \dots (a_{r_u} f) \Big) \lambda_u \in \mathbb{Z}_p[M].
\end{aligned}$$

Tomemos então θ definida deste modo e verifiquemos que se trata de um morfismo de álgebras-$\mathbb{Z}_p$.

Sejam $x = \sum_{u\in A^*} \lambda_u u,\ y = \sum_{u\in A^*} \mu_u u \in \mathbb{Z}_p[A^*]$ e $\lambda \in \mathbb{Z}_p$. Tem-se

$$\begin{aligned}
(x+y)\theta &= \left(\sum_{u\in A^*} \lambda_u u + \sum_{u\in A^*} \mu_u u \right) \theta = \left(\sum_{u\in A^*} (\lambda_u + \mu_u) u \right) \theta \\
&= \sum_{u\in A^*} \Big((a_1 f) \dots (a_{r_u} f) \Big) (\lambda_u + \mu_u) \\
&= \sum_{u\in A^*} \Big((a_1 f) \dots (a_{r_u} f) \Big) \lambda_u + \sum_{u\in A^*} \Big((a_1 f) \dots (a_{r_u} f) \Big) \mu_u \\
&= (x\theta) + (y\theta)
\end{aligned}$$

e

$$\begin{aligned}(x\lambda)\theta &= \left(\left(\sum_{u\in A^*}\lambda_u u\right)\lambda\right)\theta = \left(\sum_{u\in A^*}(\lambda_u\lambda)u\right)\theta \\ &= \sum_{u\in A^*}\Big((a_1 f)\dots(a_{r_u}f)\Big)(\lambda_u\lambda) \\ &= \left(\sum_{u\in A^*}\Big((a_1 f)\dots(a_{r_u}f)\Big)\lambda_u\right)\lambda \\ &= x(\theta\lambda).\end{aligned}$$

Além disso,

$$\begin{aligned}(xy)\theta &= \left(\left(\sum_{u\in A^*}\lambda_u u\right)\left(\sum_{u\in A^*}\mu_u u\right)\right)\theta = \left(\sum_{u,v\in A^*}(\lambda_u\mu_v)uv\right)\theta \\ &= \sum_{u,v\in A^*}\Big((a_1 f)\dots(a_{r_u}f)(b_1 f)\dots(b_{r_v}f)\Big)\lambda_u\mu_v \\ &= \sum_{u,v\in A^*}\left(\Big((a_1 f)\dots(a_{r_u}f)\Big)\lambda_u\right)\left(\Big((b_1 f)\dots(b_{r_v}f)\Big)\mu_v\right) \\ &= \left(\sum_{u\in A^*}\Big((a_1 f)\dots(a_{r_u}f)\Big)\lambda_u\right)\left(\sum_{v\in A^*}\Big((b_1 f)\dots(b_{r_v}f)\Big)\mu_v\right) \\ &= (u\theta)(v\theta).\end{aligned}$$

Portanto θ é um morfismo de álgebras-$\mathbb{Z}_p$.

O diagrama (2.7) comuta pelo modo como definimos θ e também, pela mesma razão, θ é único.

Assim $\mathbb{Z}_p[A^*]$ é a álgebra-$\mathbb{Z}_p$ livre gerada pelo conjunto A. □

Podemos agora apresentar outra descrição da congruência $\sim_k$.

Proposição 2.3.5. *Sejam A um alfabeto finito e $w_1, w_1 \in A^*$. Então*

$$w_1 \sim_k w_2 \quad \textit{se e só se} \quad w_1 - w_2 \in I^{k+1},$$

em que $I = \big\{\sum_{s\in S}\lambda_s s \in \mathbb{Z}_p[A^*] : \sum_{s\in S}\lambda_s = 0\big\}$.

Demonstração. Seja $A = \{a_1, \dots, a_r\}$. Como $\mathbb{Z}_p[A^*]$ é a álgebra-$\mathbb{Z}_p$ livre gerada pelos elementos $a_1, \dots, a_r$, em particular, existe um e um só endomorfismo $\pi : \mathbb{Z}_p[A^*] \to \mathbb{Z}_p[A^*]$ tal que $a_i\pi = 1 - a_i$, para todo o $i \in \{1, \dots, r\}$.

Ora, $a_i(\pi\pi) = (1 - a_i)\pi = 1\pi - a_i\pi = 1 - (1 - a_i) = a_i$, para qualquer $i \in \{1, \dots, r\}$, donde $\pi\pi$ é o automorfismo identidade. Então a condição $w_1 - w_2 \in I^{k+1}$ é equivalente a $w_1\pi - w_2\pi \in J^{k+1}$, em que $J = I\pi$. Calculemos então o ideal J.

O ideal I é gerado pelos elementos $1-w$, com $w \in A^+$. Mas $1-w_1w_2 = (1-w_1)+w_1(1-w_2)$, donde I é o ideal de $\mathbb{Z}_p[A^*]$ gerado pelos elementos $1-a$, com $a \in A$. Portanto, J é o ideal de $\mathbb{Z}_p[A^*]$ gerado pelos elementos $(1-a)\pi = 1\pi - a\pi = 1-(1-a) = a$, com $a \in A$.

Conclui-se então que J^{k+1} é o ideal gerado pelos elementos $v \in A^*$ tais que $|v| > k$.

Vamos agora estabelecer a seguinte identidade

$$w\pi = \sum_{u \in A^*} (-1)^{|u|} \binom{w}{u} u, \tag{2.8}$$

começando por notar que este somatório é finito pois $\binom{w}{u} = 0$ sempre que $|w| < |u|$. Utilizando a Proposição 2.3.2, tem-se a igualdade (2.8) para $w = 1$ e $w = a$, pois

$$\sum_{u \in A^*} (-1)^{|u|} \binom{w}{u} u = \sum_{u \in A^*} (-1)^{|u|} \binom{1}{u} u = (-1)^0 1 \cdot 1 = 1 = 1\pi$$

e

$$\sum_{u \in A^*} (-1)^{|u|} \binom{w}{u} u = \sum_{u \in A^*} (-1)^{|u|} \binom{a}{u} u = (-1)^0 1 \cdot 1 + (-1)^1 1a = 1 - a = a\pi.$$

Por indução sobre o comprimento de w, suponhamos que a igualdade (2.8) é válida para qualquer $w \in A^*$ tal que $|w| \leq t$. Suponhamos que $w = w_1w_2$ com $w_1 \in A$, $w_2 \in A^*$ e $|w_2| = t$. Então

$$\begin{aligned}
w\pi = (w_1w_2)\pi &= \left(\sum_{u_1 \in A^*} (-1)^{|u_1|} \binom{w_1}{u_1} u_1 \right) \left(\sum_{u_2 \in A^*} (-1)^{|u_2|} \binom{w_2}{u_2} u_2 \right) \\
&= \sum_{u_1, u_2 \in A^*} (-1)^{|u_1|+|u_2|} \binom{w_1}{u_1} \binom{w_2}{u_2} u_1u_2 \\
&= \sum_{u_1, u_2 \in A^*} (-1)^{|u_1u_2|} \binom{w_1}{u_1} \binom{w_2}{u_2} u_1u_2 \\
&= \sum_{u \in A^*} \left((-1)^{|u|} \sum_{u = u_1u_2} \binom{w_1}{u_1} \binom{w_2}{u_2} \right) u \\
&= \sum_{u \in A^*} (-1)^{|u|} \binom{w_1w_2}{u} u \\
&= \sum_{u \in A^*} (-1)^{|u|} \binom{w}{u} u
\end{aligned}$$

Atendendo ao princípio de indução, fica demonstrada a fórmula (2.8).

De (2.8) deduzimos que, para qualquer $w \in A^*$,

$$w\pi = \sum_{u \in A^*} (-1)^{|u|} \binom{w}{u} u \equiv \sum_{|u| \leq k} (-1)^{|u|} \binom{w}{u} u \pmod{J^{k+1}}, \tag{2.9}$$

pois J^{k+1} é ideal gerado pelos elementos $v \in A^*$ com $|v| > k$. Recordemos que a relação de congruência mod J^{k+1} está definida na Secção 1.9.

Como vimos atrás, para quaisquer $w_1, w_2 \in A^*$,

$$w_1 \sim_k w_2 \Leftrightarrow \binom{w_1}{v} \equiv \binom{w_2}{v} \pmod{p}, \text{ para qualquer } v \text{ com } |v| \leq k,$$

e, por (2.9), temos

$$w_1\pi - w_2\pi \equiv \sum_{|v| \leq k} (-1)^{|v|} \left(\binom{w_1}{v} - \binom{w_2}{v} \right) v \pmod{J^{k+1}}. \tag{2.10}$$

Tem-se então

$$w_1\pi - w_2\pi \in J^{k+1} \Leftrightarrow w_1\pi \equiv w_2\pi \pmod{J^{k+1}} \Leftrightarrow w_1 \sim_k w_2,$$

em que a condição necessária da última equivalência resulta de se ter $\binom{w_1}{v} \equiv \binom{w_2}{v} \pmod{p}$, para qualquer v com $|v| \leq k$, donde, utilizando a hipótese,

$$\sum_{|v| \leq k} (-1)^{|v|} \left(\binom{w_1}{v} - \binom{w_2}{v} \right) v \equiv 0 \pmod{p},$$

e tem-se $w_1\pi \equiv w_2\pi \pmod{J^{k+1}}$; quanto à condição suficiente, da hipótese e de (2.10) obtemos $\sum_{|v| \leq k} (-1)^{|v|} \left(\binom{w_1}{v} - \binom{w_2}{v} \right) v \in J^{k+1}$ e como J^{k+1} é o ideal de $\mathbb{Z}_p[A^*]$ gerado pelos elementos $v \in A^*$ com $|v| > k$, vem $\binom{w_1}{v} \equiv \binom{w_2}{v} \pmod{p}$, para qualquer v com $|v| \leq k$, ou seja, $w_1 \sim_k w_2$. □

Proposição 2.3.6. *Sejam p um número primo e q uma potência de p. Se G é um p-grupo finito de ordem q e I_G é o ideal de $\mathbb{Z}_p[G]$ gerado pelos elementos da forma $1 - g$, com $g \in G$, então ${I_G}^q = \{0\}$.*

Demonstração. A demonstração será feita por indução na ordem de G.

Se $q = 1$, isto é, $G = \{1\}$ então I_G é gerado por 0, logo ${I_G}^1 = I_G = \{0\}$.

Se $G \neq \{1\}$ então G tem centro $Z(G)$ não-trivial, pelo Teorema 1.8.25. Uma vez que $Z(G) \leq G$, pelo Teorema de Lagrange (1.8.3), $|Z(G)|$ é uma potência de p. Pelo Teorema de Cauchy (1.8.23), concluímos que existe $C \leq Z(G)$ com $|C| = p$. Note-se que uma vez que $C \leq Z(G)$ então $C \trianglelefteq G$. Tomemos $H = G/C$ e $\pi : G \twoheadrightarrow H$ o epimorfismo canónico, o qual se estende de forma natural a um morfimo de álgebras-$\mathbb{Z}_p$

$$\bar{\pi} : \mathbb{Z}_p[G] \to \mathbb{Z}_p[H].$$

Tomemos $K = \ker \bar{\pi}$. Sabemos que K é um ideal de $\mathbb{Z}_p[G]$. Mostremos que $K = (1-c)\mathbb{Z}_p[G]$, em que c é um gerador de C.

É claro que $(1-c)\mathbb{Z}_p[G] \subseteq K$.

Como π é sobrejectiva podemos escolher uma aplicação $\varphi : H \to G$ tal que $\varphi\pi = id_H$. Estendemos essa aplicação a um morfismo de álgebras-$\mathbb{Z}_p$ $\psi : \mathbb{Z}_p[H] \to \mathbb{Z}_p[G]$, cuja existência está garantida após considerarmos um conjunto de representantes das classes de $H = G/C$. Além disso, como $\varphi\pi = id_H$ tem-se também $\psi\bar{\pi} = id_{\mathbb{Z}_p[H]}$.

Como $H = G/C$ e tendo em conta o modo como se constrói a aplicação φ, resulta que qualquer $g \in G$ se escreve na forma $g = c^i(h\varphi)$, para alguns $h \in H$ e $1 \leq i \leq p$. Logo todo o x em $\mathbb{Z}_p[G]$ tem a forma

$$x = \sum_{i=1}^{p} c^i(x_i\psi), \quad \text{para alguns } x_1, \ldots, x_p \in \mathbb{Z}_p[H],$$

donde $x\bar{\pi} = \sum_{i=1}^{p}(c^i\bar{\pi})x_i(\psi\bar{\pi}) = \sum_{i=1}^{p} x_i$, pois $c^i\bar{\pi} = C$ e $x_i(\psi\bar{\pi}) = x_i$, pelo que $x \in K = \ker\bar{\pi}$ se e só se $\sum_{i=1}^{p} x_i = 0$.

Portanto se $x \in K$ então $x = \sum_{i=1}^{p}(c^i - 1)(x_i\psi)$, visto que $\sum_{i=1}^{p}(x_i\phi) = 0$. Mas, para $1 \leq i \leq p$, temos $c^i - 1 \in (1-c)\mathbb{Z}_p[G]$, donde $x \in (1-c)\mathbb{Z}_p[G]$. Concluímos assim que $K \subseteq (1-c)\mathbb{Z}_p[G]$. Logo $K = (1-c)\mathbb{Z}_p[G]$.

Por indução podemos assumir que ${I_W}^t = \{0\}$, para qualquer p-grupo W com ordem $1 \leq t < q$. Então, como H é p-grupo e $|H| = r = q/p < q$, temos ${I_H}^r = \{0\}$.

Obtemos então ${I_G}^r\bar{\pi} = (I_G\bar{\pi})^r = {I_H}^r = \{0\}$, pelo que ${I_G}^r \subseteq \ker\bar{\pi}$ donde ${I_G}^r \subseteq (1-c)\mathbb{Z}_p[G]$.

Logo ${I_G}^q = ({I_G}^r)^p \subseteq (1-c)^p\mathbb{Z}_p[G]$.

Ora, na expansão binomial de $(1-c)^p$ todos os coeficientes binomiais $\binom{p}{i}$, com $0 < i < p$, são divisíveis pelo número primo p, portanto $(1-c)^p = 1 - c^p = 0$, donde ${I_G}^q \subseteq \{0\}$. Concluímos então que ${I_G}^q = \{0\}$. O resultado fica demonstrado pelo princípio de indução. □

O mais pequeno inteiro $n \geq 1$ tal que $I_G^{n+1} = \{0\}$ chama-se o *índice de nilpotência* do p-grupo G.

Proposição 2.3.7. *Sejam G um p-grupo com índice de nilpotência n, A um alfabeto com cardinal r e $\varphi : A^* \to G$ um morfismo. Então φ admite uma factorização*

$$A^* \xrightarrow{\tau} G_{r,n} = A^*/\sim_n \xrightarrow{\psi} G,$$

em que τ é o morfismo natural correspondente à congruência $\sim_n$ de A^* e ψ é um morfismo. Mais ainda, se φ é sobrejectivo então ψ também o é.

Demonstração. Recordemos que $\sim_n$ está definida por, para cada $w_1, w_2 \in A^*$,

$$w_1 \sim_n w_2 \Leftrightarrow \binom{w_1}{v} \equiv \binom{w_2}{v} \pmod{p}, \text{ para qualquer } v \in A^* \text{ com } |v| \leq n.$$

O morfismo φ induz de forma natural um morfismo de álgebras-$\mathbb{Z}_p$

$$\varphi : \mathbb{Z}_p[A^*] \longrightarrow \mathbb{Z}_p[G].$$

Tem-se $I\varphi \subseteq I_G$, em que I é o ideal de $\mathbb{Z}_p[A^*]$ gerado pelos elementos da forma $1-u$, com $u \in A^+$ e I_G é o ideal de $\mathbb{Z}_p[G]$ gerado pelos elementos da forma $1-g$, com $g \in G$. Resulta então que $I^{n+1}\varphi \subseteq I_G^{n+1} = \{0\}$, pois G tem índice de nilpotência n.

Sejam $w_1, w_2 \in A^*$ tais que $w_1 \sim_n w_2$. Pela Proposição 2.3.5, tem-se $w_1 - w_2 \in I^{n+1}$. Portanto $w_1\varphi - w_2\varphi \in I^{n+1}\varphi = \{0\}$. Assim podemos definir ψ por $([w]_{\sim_n})\psi = w\varphi$, para $w \in A^*$. Obtemos $\varphi = \tau\psi$.

É fácil ver que ψ é morfismo e é claro que se φ é sobrejectivo ψ também o é. □

Dado um grupo finito G definimos *rank de* G, e denotamos por $\mathrm{rank}(G)$, como sendo o menor dos cardinais dos conjuntos de geradores de G.

Proposição 2.3.8. *Seja G um p-grupo tal que $\mathrm{rank}(G) \leq r$ e índice de nilpotência n. Então G é um grupo quociente de $G_{r,n}$.*

Demonstração. Como $\mathrm{rank}(G) \leq r$, o grupo G é gerado por elementos $g_1, \ldots, g_r$ (elementos não necessariamente distintos), logo existe um morfismo sobrejectivo $\varphi : A^* \twoheadrightarrow G$, em que A é um alfabeto com r letras. O morfismo natural $\tau : A^* \twoheadrightarrow A^*/\sim_n$ associado à congruência $\sim_n$ é sobrejectivo logo, pela Proposição 2.3.7, o morfismo $\psi : G_{r,n} \twoheadrightarrow G$ é sobrejectivo e tem-se

$$G \simeq \frac{G_{r,n}}{\ker \psi},$$

como pretendíamos. □

Como consequência destas proposições obtemos as seguintes caracterizações da pseudovariedade $\mathbf{G}_p$ dos p-grupos finitos:

Corolário 2.3.9. *A pseudovariedade de grupos $\boldsymbol{G}_p$ é gerada pelos grupos $G_{r,n}$, para todos os inteiros $r \geq 1$ e $n \geq 1$.*

Demonstração. Claramente $\mathbf{V}\langle G_{r,n} : r, n \geq 1\rangle \subseteq \mathbf{G}_p$ pois $G_{r,n} \in \mathbf{G}_p$, para quaisquer r e $n \geq 1$.

Seja $G \in \mathbf{G}_p$. Ora, G é tal que $\mathrm{rank}(G) \leq r$, para um certo r, e tem um determinado índice de nilpotência n. Pela demonstração da Proposição 2.3.8, resulta que $\psi : G_{r,n} \twoheadrightarrow G$ é um epimorfismo logo, pelo Teorema 1.5.1, $G \in \mathbf{V}\langle G_{r,n} : r, n \geq 1\rangle$. □

Corolário 2.3.10. *A pseudovariedade de grupos $\boldsymbol{G}_p$ é gerada pelos grupos G_u, para todo o $u \in A^*$ e todo o alfabeto finito A.*

Demonstração. Claramente $\mathbf{V}\langle G_u : u \in A^*, A \text{ alfabeto finito}\rangle \subseteq \mathbf{G}_p$ pois, pela Proposição 2.3.3, resulta que G_u é um p-grupo, para todo o alfabeto finito A e todo o $u \in A^*$.

Seja $G \in \mathbf{G}_p$. Como vimos no corolário anterior, existe um epimorfismo $\psi : G_{r,n} \twoheadrightarrow G$, em que $G_{r,n}$ é um subgrupo do produto directo

$$\prod_{\substack{u \in A^* \\ |u|=n}} G_u,$$

pelo que foi visto na página 60. Portanto

$$G \in \mathbf{V}\langle G_u : u \in A^*, A \text{ alfabeto finito}\rangle,$$

como pretendíamos. □

2.4 A pseudovariedade $\mathbf{G}_p * \mathbf{Ab}^{p-1}$

Pretendemos, agora, descrever a pseudovariedade $\mathbf{G}_p * \mathbf{Ab}^{p-1}$ através de pseudoidentidades.

A noção de identidade como igualdade formal entre duas palavras sobre um alfabeto numerável (finito ou infinito) $X = \{x_1, x_2, \ldots\}$, apresentada na secção 1.5, pode ser estendida à noção de *pseudoidentidade* (que não iremos definir aqui), o mesmo acontecendo com a noção de satisfação de uma identidade por um monóide, de forma que as pseudovariedades de monóides sejam precisamente as classes de monóides que satisfazem um conjunto de pseudoidentidades.

Temos como exemplo de pseudoidentidade a igualdade

$$(x_1x_2)^\omega = (x_1x_2)^\omega x_1. \tag{2.11}$$

Um monóide M com ℓ elementos satisfaz a pseudoidentidade (2.11) se e só se para qualquer substituição das variáveis x_1 e x_2 por elementos de M e do símbolo ω por $\ell!$ obtemos uma igualdade em M, isto é, para qualquer morfismo de monóides $\varphi : X^* \to M$ se tem $\left((x_1x_2)^{\ell!}\right)\varphi = \left((x_1x_2)^{\ell!}x_1\right)\varphi$.

Grosso modo, as pseudoidentidades que vão surgir são igualdades formais entre certas sequências construídas a partir de letras do alfabeto e utilizando um símbolo especial ω e a operação de exponenciação, onde o símbolo ω é interpretado em cada monóide M com cardinal ℓ como sendo $\ell!$.

Como exemplo, fixando um número primo p, um grupo G com ordem ℓ satisfaz a pseudoidentidade $(x_1^{p-1}x_2^{p-1})^{p^\omega} = 1$ se e só se para qualquer

morfismo $\varphi : X^* \to G$ se tem $((x_1^{p-1}x_2^{p-1})^{p^{\ell!}})\varphi = 1\varphi$. Equivalentemente, G satisfaz $(x_1^{p-1}x_2^{p-1})^{p^\omega} = 1$ se e só se $(a^{p-1}b^{p-1})^{p^{\ell!}} = 1$, para quaisquer $a, b \in G$.

Lema 2.4.1. *Em todo o grupo G que satisfaça a identidade $(x^s y^s)^r = 1$, em que r e s são primos entre si, o conjunto $H = \{g \in G : |g| \mid r\}$ é um subgrupo normal de G.*

Demonstração. É claro que $1_G \in H$, pois $|1_G| = 1 \mid r$.

Seja $h \in H$. Então $|h| \mid r$. Portanto $h^r = 1$. Mas $(h^{-1})^r = (h^r)^{-1} = 1$, donde $|h^{-1}| \mid r$, pelo que $h^{-1} \in H$.

Sejam agora $a, b \in H$. Então $|a|, |b| \mid r$. Logo $a^r = 1$ e $b^r = 1$. Como r e s são primos entre si, pela igualdade de Bézout, existem $x, y \in \mathbb{Z}$ tais que $1 = xr + ys$. Portanto $a = a^{xr+ys} = a^{xr}a^{ys} = (a^r)^x(a^y)^s = (a^y)^s$, pois $a^r = 1$. Analogamente, tem-se $b = (b^y)^s$. Assim $(ab)^r = ((a^y)^s(b^y)^s)^r = 1$, visto que $a^y, b^y \in G$ e G satisfaz a identidade $(x^s y^s)^r = 1$. Concluímos que $|ab| \mid r$, pelo que $ab \in H$. Provámos que $H \leq G$.

Sejam $g \in G$ e $h \in H$. Então $|h| \mid r$ e $h^r = 1$. Por um argumento simples de indução, mostra-se que $(g^{-1}hg)^n = g^{-1}h^n g$, para qualquer natural $n \in \mathbb{N}$. Logo $(g^{-1}hg)^r = g^{-1}h^r g = g^{-1}g = 1$. Portanto $|g^{-1}hg| \mid r$ resultando que $g^{-1}hg \in H$. Concluímos que $H \trianglelefteq G$, como pretendíamos. □

Seja p um número primo e q uma potência de p.

Vamos determinar pseudoidentidades que definem a pseudovariedade de grupos $\mathbf{G}_p * \mathbf{Ab}^{q-1}$, interessando-nos particularmente o caso $q = p$.

Consideremos as seguintes pseudoidentidades sobre o alfabeto $\{x, y\}$:

$$(x^{q-1}y^{q-1})^{p^\omega} = 1 \tag{2.12}$$

$$(x^{\omega-1}y^{\omega-1}xy)^{p^\omega} = 1 \tag{2.13}$$

Teorema 2.4.2. *A pseudovariedade $\boldsymbol{G}_p * \boldsymbol{Ab}^{q-1}$ é a classe de todos os grupos finitos definidos pelas pseudoidentidades* (2.12) *e* (2.13)*, isto é,*

$$\boldsymbol{G}_p * \boldsymbol{Ab}^{q-1} = \boldsymbol{V}\left[(x^{q-1}y^{q-1})^{p^\omega} = 1, (x^{\omega-1}y^{\omega-1}xy)^{p^\omega} = 1\right].$$

Demonstração. Seja $G \in \mathbf{G}_p * \mathbf{Ab}^{q-1}$. Então existe $H \trianglelefteq G$ tal que $H \in \mathbf{G}_p$ e $G/H \in \mathbf{Ab}^{q-1}$.

Ora, para quaisquer $a, b \in G$, temos $a^{q-1}b^{q-1}H = a^{q-1}Hb^{q-1}H = H$, pois G/H é um grupo cujo expoente divide $q-1$, donde $a^{q-1}b^{q-1} \in H$. Mais, $a^{-1}b^{-1}abH = a^{-1}Hb^{-1}HaHbH = a^{-1}HaHb^{-1}HbH = H$, pois G/H é grupo abeliano, donde $a^{-1}b^{-1}ab \in H$.

Suponhamos que $|G| = \ell$. Então $a^{\ell!} = a^{\ell(\ell-1)!} = 1$, para qualquer $a \in G$, pelo que $a^{-1} = a^{\ell!-1}$. Mais, como H é um p-grupo, $h^{p^{\ell!}} = 1$, para todo o

$h \in H$. Tem-se então, para quaisquer $a, b \in G$ e $h \in H$,

$$a^{q-1}b^{q-1} \in H \tag{2.14}$$
$$a^{-1}b^{-1}ab \in H \tag{2.15}$$
$$a^{-1} = a^{\ell!-1} \tag{2.16}$$
$$h^{p^{\ell!}} = 1 \tag{2.17}$$

Assim, por (2.14) e (2.17), o grupo G satisfaz $(x^{q-1}y^{q-1})^{p^{\ell!}} = 1$ e, por (2.15), (2.16) e (2.17), G satisfaz $(x^{\ell!-1}y^{\ell!-1}xy)^{p^{\ell!}} = 1$. Portanto, G satisfaz as pseudoidentidades (2.12) e (2.13).

Reciprocamente, suponhamos que o grupo G é tal que $|G| = \ell$ e satisfaz as pseudoidentidades (2.12) e (2.13). Pela nossa interpretação das ω-palavras, de (2.12) e (2.13) obtemos

$$(a^{q-1}b^{q-1})^{p^{\ell!}} = 1 \quad \text{e} \quad (a^{\ell!-1}b^{\ell!-1}ab)^{p^{\ell!}} = 1, \quad \text{para quaisquer } a, b \in G.$$

Note-se que q é uma potência de p logo $\text{mdc}(q-1, p^{\ell!}) = 1$. Além disso, pelo Lema 2.4.1 tem-se $H = \{a \in G : |a| \mid p^{\ell!}\} \trianglelefteq G$. De facto $H \in \mathbf{G}_p$ pois todos os seus elementos têm ordem uma potência de p.

Por (2.12), para qualquer $g \in G$, temos $(g^{q-1})^{p^{\ell!}} = (g^{q-1}1^{q-1})^{p^{\ell!}} = 1$ pelo que $|g^{q-1}| \mid p^{\ell!}$. Portanto, pela definição de H, obtemos $g^{q-1}H = H$, para todo o $g \in G$. Portanto G/H satisfaz a identidade $x^{q-1} = 1$.

Além disso, por (2.13), para quaisquer $a, b \in G$, $(a^{\ell!-1}b^{\ell!-1}ab)^{p^{\ell!}} = 1$, donde $|a^{\ell!-1}b^{\ell!-1}ab| \mid p^{\ell!}$, pelo que $a^{\ell!-1}b^{\ell!-1}abH = H$, novamente pela definição de H. Logo G/H satisfaz $x^{\ell!-1}y^{\ell!-1}xy = 1$. Mas, é claro que o expoente de um grupo de ordem menor ou igual a ℓ divide $\ell!$. Portanto G/H satisfaz $x^{\ell!} = 1$, ou seja, satisfaz $x^{\ell!-1} = x^{-1}$.

Assim, da expressão $x^{\ell!-1}y^{\ell!-1}xy = 1$ deduz-se $x^{-1}y^{-1}xy = 1$, donde G/H satisfaz $[x, y] = 1$ pelo que é um grupo abeliano.

Mais ainda, pelo que já vimos G/H satisfaz $x^{q-1} = 1$, donde $|gH| \mid q-1$, qualquer que seja $g \in G$ e, atendendo à definição de expoente de um grupo, conclui-se que $\exp(G/H) \mid q-1$, donde $G/H \in \mathbf{Ab}^{q-1}$. Concluímos que $G \in \mathbf{G}_p * \mathbf{Ab}^{q-1}$.

Portanto $\mathbf{G}_p * \mathbf{Ab}^{q-1} = \mathbf{V}\left[(x^{q-1}y^{q-1})^{p^\omega} = 1, (x^{\omega-1}y^{\omega-1}xy)^{p^\omega} = 1\right]$. □

Seja K um corpo. No grupo

$$Gl_n(K) = \{M \in M_n(K) : M \text{ é invertível}\}$$

consideremos o subgrupo $B_n(K)$ das matrizes invertíveis triangulares superiores, que é conhecido por *subgrupo standard de Borel*, e também $U_n(K)$ o grupo das matrizes unitriangulares de $B_n(K)$, i.e. matrizes triangulares superiores com uns na diagonal.

É agora nosso objectivo dar uma caracterização da pseudovariedade $\mathbf{G}_p * \mathbf{Ab}^{p-1}$ utilizando os subgrupos standard de Borel $B_n(\mathbb{Z}_p)$, para o que vamos precisar do seguinte lema técnico:

Lema 2.4.3. *Dado um número primo p, tem-se*

$$\boldsymbol{G}_p * \boldsymbol{Ab} = \boldsymbol{G}_p * \boldsymbol{Ab}_{p'}.$$

Demonstração. A inclusão $\mathbf{G}_p * \mathbf{Ab}_{p'} \subseteq \mathbf{G}_p * \mathbf{Ab}$ é evidente.

Seja então $H \in \mathbf{G}_p * \mathbf{Ab}$. Pelo Teorema de Kalužnin-Krasner (2.1.3), $H \lesssim G \rtimes W$, em que $G \in \mathbf{G}_p$ e $W \in \mathbf{Ab}$.

Como $W \in \mathbf{Ab}$, do Teorema 1.8.27 resulta $W = \prod_{i=1}^{r} C_i$ em que $C_i \leq W$ são p_i-grupos cíclicos. Portanto, pelo Teorema 1.8.20, obtemos

$$W = \prod_{i=1}^{r} C_i \simeq C_1 \times \cdots \times C_r. \tag{2.18}$$

Suponhamos que $C_1, \ldots, C_l$ são p-grupos e $C_{l+1}, \ldots, C_r$ são p'-grupos (note-se que se pode sempre "reordenar" os grupos C_i a menos de isomorfismo). Uma vez que os grupos cíclicos são abelianos e $\mathbf{G}_p$ e $\mathbf{Ab}$ são pseudovariedades de grupos resulta que $C_1 \times \cdots \times C_l \in \mathbf{G}_p$ e $C_{l+1} \times \cdots \times C_r \in \mathbf{Ab}_{p'}$.

Assim,

$$\begin{aligned} G \rtimes W &= G \rtimes \left(\prod_{i=1}^{r} C_i \right) \\ &\overset{(2.18)}{\simeq} G \rtimes ((C_1 \times \cdots \times C_l) \times (C_{l+1} \times \cdots \times C_r)) \in \mathbf{G}_p * (\mathbf{G}_p * \mathbf{Ab}_{p'}). \end{aligned}$$

Pela associatividade do produto de pseudovariedades tem-se

$$\mathbf{G}_p * (\mathbf{G}_p * \mathbf{Ab}_{p'}) = (\mathbf{G}_p * \mathbf{G}_p) * \mathbf{Ab}_{p'} \subseteq \mathbf{G}_p * \mathbf{Ab}_{p'},$$

pois $\mathbf{G}_p * \mathbf{G}_p \subseteq \mathbf{G}_p$. Portanto, $H \in \mathbf{G}_p * \mathbf{Ab}_{p'}$.

Conclui-se que $\mathbf{G}_p * \mathbf{Ab} \subseteq \mathbf{G}_p * \mathbf{Ab}_{p'}$, pelo que se tem a igualdade pretendida. □

Tendo em conta que $\mathbf{Ab}^{p-1} \subseteq \mathbf{Ab}$, podemos agora afirmar que

$$\mathbf{G}_p * \mathbf{Ab}^{p-1} \subseteq \mathbf{G}_p * \mathbf{Ab} = \mathbf{G}_p * \mathbf{Ab}_{p'}. \tag{2.19}$$

Teorema 2.4.4. *Um grupo pertence à pseudovariedade $\boldsymbol{G}_p * \boldsymbol{Ab}^{p-1}$ se e só se é isomorfo a um subgrupo do subgrupo standard de Borel $B_n(\mathbb{Z}_p)$, para algum número natural n.*

Demonstração. Seja G um grupo de $\mathbf{G}_p * \mathbf{Ab}^{p-1}$. Então existe $N \trianglelefteq G$ tal que $N \in \mathbf{G}_p$ e $G/N \in \mathbf{Ab}^{p-1}$. Note-se que, como $G/N \in \mathbf{Ab}^{p-1}$, tem-se que $\exp(G) \mid p-1$, donde $|gN| \mid p-1$, para qualquer $g \in G$, pelo que não existe em G/N um elemento de ordem p. Por outro lado, pelo Teorema de Cauchy (1.8.23), todo o grupo cuja ordem seja divisível por p possui um elemento de ordem p, donde $p \nmid |G/N|$. Então $N \in \mathrm{Syl}_p(G)$. Assim, pelo Teorema de

Schur e Zassenhaus (1.8.28), existe um subgrupo $C \leq G$ tal que $G = NC$ e $C \simeq G/N$. Note-se que $N \trianglelefteq G$ e $N \in \mathrm{Syl}_p(G)$, donde $\mathrm{Syl}_p(G) = \{N\}$. Assim

$$O_p(G) = \bigcap_{P \in \mathrm{Syl}_p(G)} P = N.$$

Pela Proposição 1.10.4, resulta que se V é um módulo-$\mathbb{Z}_p[G]$ irredutível então $C_V(O_p(G)) = \{v \in V : vn = v,\ \forall n \in N\} = V$. Provemos que V é um módulo-$\mathbb{Z}_p[G]$ irredutível se e só se V é um módulo-$\mathbb{Z}_p[C]$ irredutível. Se V é um módulo-$\mathbb{Z}_p[G]$ irredutível então, para quaisquer $v \in V$ e $n \in N$,

$$vn = v. \tag{2.20}$$

Suponhamos, com vista a um absurdo, que V não é irredutível sobre $\mathbb{Z}_p[C]$. Então existe W submódulo-$\mathbb{Z}_p[C]$ de V tal que $\{0\} <_{\mathbb{Z}_p} W <_{\mathbb{Z}_p} V$. Por W ser submódulo-$\mathbb{Z}_p[C]$ de V resulta que W é C-invariante. Assim, quaisquer que sejam $g \in G$ e $w \in W$, temos $g = nc$, com $n \in N$ e $c \in C$, donde, por (2.20), tem-se $wg = wnc = wc \in W$, portanto W é G-invariante. Como G é uma base de $\mathbb{Z}_p[G]$, se considerarmos $G = \{g_1, \ldots, g_n\}$, dados $x \in \mathbb{Z}_p[G]$ e $w \in W$, existem $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_p$ tais que $x = \sum_{i=1}^n g_i\alpha_i$, pelo que $wx = \sum_{i=1}^n (wg_i)\alpha_i \in W$. Portanto W é módulo-$\mathbb{Z}_p[G]$ o que é absurdo. Reciprocamente, se V é módulo-$\mathbb{Z}_p[C]$ irredutível então é claro que V é módulo-$\mathbb{Z}_p[G]$ irredutível.

Note-se que, se considerarmos $\mathcal{U}(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\}$, o grupo das unidades de $\mathbb{Z}_p$, como $|\mathcal{U}(\mathbb{Z}_p)| = p - 1$, pelo Corolário 1.8.5 tem-se $z^{p-1} = 1$, qualquer que seja $z \in \mathcal{U}(\mathbb{Z}_p)$. Portanto o polinómio $t^{p-1} - 1$ factoriza-se em $\mathbb{Z}_p$ em polinónios de grau 1. Uma vez que $C \in \mathbf{Ab}^{p-1}$, pois $C \simeq G/N$ e $G/N \in \mathbf{Ab}^{p-1}$, pela Proposição 1.10.7, obtém-se que todo o módulo-$\mathbb{Z}_p[C]$ irredutível V tem dimensão 1 enquanto espaço vectorial sobre $\mathbb{Z}_p$. Portanto, todo o módulo-$\mathbb{Z}_p[G]$ irredutível tem também dimensão 1 sobre $\mathbb{Z}_p$.

Seja V o módulo regular sobre $\mathbb{Z}_p[G]$, definido na Secção 1.10. Seja

$$\{0\} = V_0 < V_1 < \cdots < V_n = V$$

uma série de composição de V como módulo-$\mathbb{Z}_p[G]$. Vamos usar esta série para escolher uma base de V sobre $\mathbb{Z}_p$. Por definição de série de composição, todo o factor V_{i+1}/V_i é um módulo-$\mathbb{Z}_p[G]$ irredutível e pelo que acabámos de ver, $dim_{\mathbb{Z}_p}(V_{i+1}/V_i) = 1$, para todo o $i \in \{0, \ldots, n-1\}$.

Escolhemos $b_1 \in V_1/V_0 = V_1/\{0\}$ base de V_1/V_0 sobre $\mathbb{Z}_p$, $b_2 + V_1 \in V_2/V_1$ base de V_2/V_1 sobre $\mathbb{Z}_p$. Note-se que $b_2 \notin V_1$, caso contrário, $b_2 + V_1 = V_1$ e $b_2 + V_1$ não constituiria uma base. Assim, $\{b_1, b_2\}$ é conjunto linearmente independente sobre $\mathbb{Z}_p$ pois, se assim não fosse, existiria $\alpha \in \mathcal{U}(\mathbb{Z}_p)$ tal que $b_2 = b_1\alpha \in V_1$, o que é absurdo. Sucessivamente, podemos construir $\{b_1, \ldots, b_n\}$ linearmente independente tal que $b_{i+1} + V_i$ é base de V_{i+1}/V_i

com $i = 0, \ldots, n-1$. Então $\mathcal{B} = \{b_1, \ldots, b_n\}$ é uma base de V sobre $\mathbb{Z}_p$. Assim, $V_1 = \langle b_1 \rangle, \ldots, V_n = \langle b_1, \ldots, b_n \rangle$ são submódulos-$\mathbb{Z}_p[G]$ do módulo regular V, logo são espaços G-invariantes, isto é, para cada i temos $v_i g \in V_i$, quaisquer que sejam $v_i \in V_i$ e $g \in G$. Consideremos a acção de G sobre V que a cada $v = \sum_{g \in G} \lambda_g g \in V$ e a cada $g_0 \in G$ faz corresponder o elemento $vg_0 = \sum_{g \in G} \lambda_g (gg_0) \in V$. Note-se que se tem

$$X = \{g_0 \in G : vg_0 = v, \forall v \in V\} = \{1\},$$

pois, para cada $g_0 \in X$, se considerarmos $g_0^{-1} = \sum_{g \in G} \delta_{g_0^{-1} g} g \in V$, temos $g_0^{-1} g_0 = g_0^{-1}$, uma vez que $g_0 \in X$. Mais ainda, $g_0^{-1} g_0 = \sum_{g \in G} \delta_{g_0^{-1} g} (gg_0) = 1$, donde $g_0 = 1$ e obtém-se a igualdade pretendida.

Note-se que V, enquanto espaço vectorial sobre $\mathbb{Z}_p$, pode ser encarado como módulo-G à direita com a acção definida anteriormente. Pela Proposição 1.10.2 (2), resulta que

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL(V) \\ g_0 & \longmapsto & g_0 \rho \end{array}$$

em que $v(g_0\rho) = vg_0$, para cada $v \in V$, é um morfismo injectivo pois $X = \{1\}$.

Em seguida vamos construir uma representação $\varphi : G \to Gl_n(\mathbb{Z}_p)$ de G. Sabemos que os grupos $GL(V)$ e $Gl_n(\mathbb{Z}_p)$ são isomorfos: de facto considerando a base $\mathcal{B}$ de V sobre $\mathbb{Z}_p$ construída acima, a aplicação

$$\begin{array}{rcl} \theta : GL(V) & \longrightarrow & Gl_n(\mathbb{Z}_p) \\ f & \longmapsto & A_f \end{array}$$

em que $A_f = (a_{ij})_{i,j}$ é a matriz da aplicação linear f em relação à base $\mathcal{B}$, é um isomorfismo. Então $\varphi = \rho\theta : G \to Gl_n(\mathbb{Z}_p)$ é um monomorfismo, donde φ é uma representação fiel de G. Pela construção da base $\mathcal{B}$ e tendo em conta que os espaços V_i são G-invariantes, concluímos que, para cada $g \in G$, $g\varphi \in Gl_n(\mathbb{Z}_p)$ é uma matriz triangular superior, logo $g\varphi \in B_n(\mathbb{Z}_p)$. Portanto $G \lesssim B_n(\mathbb{Z}_p)$.

Para mostrarmos a condição reciproca, basta provar que os grupos $B_n(\mathbb{Z}_p)$ pertencem à pseudovariedade $\mathbf{G}_p * \mathbf{Ab}^{p-1}$, para qualquer natural n.

Seja π o morfismo que transforma cada matriz de $B_n(\mathbb{Z}_p)$ no vector de $\mathbb{Z}_p^n$ correspondente à sua diagonal. Note-se que π é um morfismo pois as matrizes de $B_n(\mathbb{Z}_p)$ são triangulares superiores.

A imagem de π é o grupo $(\mathcal{U}(\mathbb{Z}_p))^n = (\mathbb{Z}_p \setminus \{0\})^n$, o qual é abeliano, e $|(\mathcal{U}(\mathbb{Z}_p))^n| = (p-1)^n$ logo, pela definição de expoente de um grupo, resulta que $\exp((\mathcal{U}(\mathbb{Z}_p))^n) \mid p-1$, donde $(\mathcal{U}(\mathbb{Z}_p))^n \in \mathbf{Ab}^{p-1}$. Além disso, por definição de π, obtemos $\ker \pi = U_n(\mathbb{Z}_p)$ o qual é claramente um p-grupo, portanto $\ker \pi \in \mathbf{G}_p$.

Ora, $\ker \pi \trianglelefteq B_n(\mathbb{Z}_p)$, $\ker \pi \in \mathbf{G}_p$ e, pelo Teorema do Homomorfismo (1.8.17), $(\mathcal{U}(\mathbb{Z}_p))^n = (B_n(\mathbb{Z}_p))\pi \simeq B_n(\mathbb{Z}_p)/\ker \pi$. Uma vez que $(\mathcal{U}(\mathbb{Z}_p))^n \in \mathbf{Ab}^{p-1}$, obtém-se $B_n(\mathbb{Z}_p) \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$. □

Concluímos esta secção com a seguinte caracterização da pseudovariedade de grupos $\mathbf{G}_p * \mathbf{Ab}^{p-1}$, para cada número primo p:

Corolário 2.4.5. *Para cada número primo p, a pseudovariedade $\boldsymbol{G}_p * \boldsymbol{Ab}^{p-1}$ é gerada pelos subgrupos standard de Borel $B_n(\mathbb{Z}_p)$, para todo o natural n.*

Demonstração. Seja $G \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$. Pelo Teorema 2.4.4 tem-se $G \lesssim B_n(\mathbb{Z}_p)$, para algum natural n, logo existe um monomorfismo $\theta : G \to B_n(\mathbb{Z}_p)$. Portanto $G \simeq G\theta \leq B_n(\mathbb{Z}_p)$. Em particular, $G \mid B_n(\mathbb{Z}_p)$ pelo que $G \in \mathbf{V}\langle B_n(\mathbb{Z}_p) : n \in \mathbb{N}\rangle$.

Reciprocamente, seja $G \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$. Então, pelo Teorema 1.5.1, existem $n_1, \ldots, n_t \in \mathbb{N}$ tais que $G \mid B_{n_1}(\mathbb{Z}_p) \times \cdots \times B_{n_t}(\mathbb{Z}_p)$. Na demonstração do Teorema 2.4.4 concluímos que $B_n(\mathbb{Z}_p) \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$, qualquer que seja $n \in \mathbb{N}$, donde, por definição de pseudovariedade, concluímos que $B_{n_1}(\mathbb{Z}_p) \times \cdots \times B_{n_t}(\mathbb{Z}_p) \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$, pelo que $G \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$. Portanto

$$\mathbf{G}_p * \mathbf{Ab}^{p-1} = \mathbf{V}\langle B_n(\mathbb{Z}_p) : n \in \mathbb{N}\rangle,$$

como pretendíamos. □

2.5 A pseudovariedade dos grupos super-resolúveis

Nesta secção vamos apresentar uma nova pseudovariedade de grupos: a pseudovariedade dos grupos super-resolúveis.

Um grupo G diz-se *super-resolúvel* se possui uma série normal com factores cíclicos, isto é, se existem subgrupos normais $G_1, \ldots, G_{n-1} \trianglelefteq G$ tais que

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G,$$

e cada G_{i+1}/G_i é cíclico, para $i = 0, \ldots, n-1$.

Proposição 2.5.1. *A classe **Su** de todos os grupos super-resolúveis é uma pseudovariedade de grupos.*

Demonstração. (1) Se $G \in \mathbf{Su}$ e $H \leq G$, então $H \in \mathbf{Su}$:

Pela definição de **Su**, existe uma série normal $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$ com factores cíclicos.

Considere-se $H_i = G_i \cap H$, para cada $i \in \{0, \ldots, n\}$.

Ora, pelo 1º Teorema do Isomorfismo (1.8.18) tem-se

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

pois $G_i \subseteq G_i(G_{i+1} \cap H)$, $G_i \trianglelefteq G_{i+1}$ e $G_{i+1} \cap H \leq G_{i+1}$, donde $G_i(G_{i+1} \cap H) \leq G_{i+1}$. Note-se que $H_i = G_i \cap H \trianglelefteq G_{i+1} \cap H = H_{i+1}$, pois $G_i \trianglelefteq G_{i+1}$. Se $G_i \trianglelefteq G$ e $H \leq G$, então $H_i = G_i \cap H \trianglelefteq H$.

Uma vez que G_{i+1}/G_i é cíclico, tem-se $G_i(G_{i+1} \cap H)/G_i$ cíclico, por ser subgrupo de um grupo cíclico. Logo H_{i+1}/H_i também é cíclico.

Ora $H_0 = G_0 \cap H = \{1\} \cap H = \{1\}$ e $H_n = G_n \cap H = G \cap H = H$, pelo que

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = H$$

é uma série normal de H com factores cíclicos. Portanto $H \in \mathbf{Su}$.

(2) Se $G \in \mathbf{Su}$ e $\varphi : G \twoheadrightarrow H$ é um epimorfismo então $H \in \mathbf{Su}$:

Pelo Teorema do Homomorfismo (1.8.17), $H = G\varphi \simeq G/\ker\varphi$. Seja $N = \ker\varphi \trianglelefteq G$ e $\psi : G/N \to G\varphi$ um isomorfismo.

Como $G \in \mathbf{Su}$, existe uma série normal $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$ com factores cíclicos. Provemos que $G/N \in \mathbf{Su}$:

Consideremos $T_i = G_iN/N$, em que $i \in \{0, \ldots, n\}$. Note-se que $T_0 = G_0N/N = \{1\}N/N = N/N = \{N\}$ e $T_n = G_nN/N = GN/N = G/N$. Como $N \trianglelefteq G_iN$ resulta que T_i é grupo. Mais, $G_i \trianglelefteq G_{i+1}$ e $N \subseteq G_iN$ implicam $G_iN \trianglelefteq G_{i+1}N$ e $T_i = G_iN/G \trianglelefteq G_{i+1}N/G = T_{i+1}$.

Ora, $G_iN \trianglelefteq G$, pois $N, G_i \trianglelefteq G$, e $N \subseteq G_iN$ pelo que $G_iN/N \trianglelefteq G/N$, para todo o $i \in \{0, \ldots, n\}$. Portanto

$$\{N\} = T_0 \trianglelefteq T_1 \trianglelefteq \cdots \trianglelefteq T_{n-1} \trianglelefteq T_n = G/N$$

é uma série normal de G/N. Vejamos que os seus factores são cíclicos. Pelos 1º e 2º Teoremas do Isomorfismo (1.8.18 e 1.8.19) resulta que

$$\frac{T_{i+1}}{T_i} = \frac{\frac{G_{i+1}N}{N}}{\frac{G_iN}{N}} \simeq \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \simeq \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \simeq \frac{\frac{G_{i+1}}{G_i}}{\frac{G_{i+1} \cap (G_iN)}{G_i}},$$

Como $\frac{G_{i+1}}{G_i}$ é um grupo cíclico, $\frac{\frac{G_{i+1}}{G_i}}{\frac{G_{i+1} \cap (G_iN)}{G_i}}$ também é cíclico, donde $\frac{T_{i+1}}{T_i}$ é cíclico.

Concluímos que $G/N \in \mathbf{Su}$. Provemos então que $H \in \mathbf{Su}$. Vejamos que

$$\{1_H\} = \{1_G\varphi\} = \{T_0\psi\} \trianglelefteq T_1\psi \trianglelefteq \cdots \trianglelefteq T_{n-1}\psi \trianglelefteq T_n\psi = G\varphi = H$$

é uma série normal de H com factores cíclicos. Como $T_i \trianglelefteq G/N$ e ψ é morfismo sobrejectivo, $T_i\psi \trianglelefteq G\varphi = H$. Além disso, $T_i\psi \trianglelefteq T_{i+1}\psi$ pois $T_i \trianglelefteq T_{i+1}$ e $T_{i+1}/T_i \simeq T_{i+1}\psi/T_i\psi$, pois ψ é isomorfismo. Uma vez que T_{i+1}/T_i é cíclico também $T_{i+1}\psi/T_i\psi$ é cíclico. Logo $H \in \mathbf{Su}$.

(3) Se $G, H \in \mathbf{Su}$ então $G \times H \in \mathbf{Su}$:

Sejam G e H grupos super-resolúveis. Pela definição, existem séries normais para G e H com factores cíclicos

$$\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G \quad \text{e} \quad \{1_H\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_m = H.$$

Consideremos a cadeia

$$\{(1_G, 1_H)\} \trianglelefteq G_1 \times \{1_H\} \trianglelefteq \cdots \trianglelefteq G_n \times \{1_H\} \trianglelefteq G_n \times H_1 \trianglelefteq \cdots \trianglelefteq G_n \times H_m = G \times H,$$

é claro que cada um destes grupos é normal no seguinte e todos são normais em $G \times H$. Além disso, para todo o $i \in \{0, \ldots, n-1\}$,

$$\frac{G_{i+1} \times \{1_H\}}{G_i \times \{1_H\}} \simeq \frac{G_{i+1}}{G_i}$$

e, como G_{i+1}/G_i é cíclico, o grupo $(G_{i+1} \times \{1_H\})/(G_i \times \{1_H\})$ é cíclico. Mais, para todo o $j \in \{0, \ldots, m-1\}$,

$$\frac{G \times H_{j+1}}{G \times H_j} \simeq \frac{G}{G} \times \frac{H_{j+1}}{H_j} \simeq \{G\} \times \frac{H_{j+1}}{H_j} \simeq \frac{H_{j+1}}{H_j}.$$

Sendo H_{j+1}/H_j cíclico, também o grupo $(G \times H_{j+1})/(G \times H_j)$ é cíclico. Concluímos pois que $G \times H \in \mathbf{Su}$.

Portanto, $\mathbf{Su}$ constitui uma pseudovariedade de grupos. □

Recordemos que, dado um grupo G, um seu subgrupo normal $M \neq \{1\}$ diz-se *normal minimal* em G se dado $\{1\} \neq N \trianglelefteq G$ tal que $N \subseteq M$ então $N = M$.

Um grupo G diz-se *monolítico* se possui um único subgrupo M normal minimal, a esse subgrupo damos o nome de *monolito* de G.

Lema 2.5.2. *Seja G um grupo monolítico com monolito M. Então*

$$M = \bigcap_{\{1\} \neq N \trianglelefteq G} N.$$

Demonstração. Seja G um grupo monolítico. Consideremos $\{1\} \neq N \trianglelefteq G$. Se N é normal minimal em G então, pela unicidade do monolito, $N = M$.

Se N não é normal minimal em G, então existe $\{1\} \neq N_1 \trianglelefteq G$ tal que $\{1\} \neq N_1 \triangleleft N$. Como G é finito pode repetir-se o processo até encontrar $\{1\} \neq N_k$ normal minimal em G tal que

$$\{1\} \neq N_k \trianglelefteq \cdots \trianglelefteq N_1 \trianglelefteq N,$$

da unicidade do monolito resulta que $M = N_k \subseteq N$.

Conclui-se então que, para qualquer subgrupo $\{1\} \neq N \trianglelefteq G$, se tem $M \subseteq N$, donde $M \subseteq \bigcap_{\{1\} \neq N \trianglelefteq G} N$. Como $\{1\} \neq M \trianglelefteq G$, obtemos

$$M = \bigcap_{\{1\} \neq N \trianglelefteq G} N. \qquad \square$$

Lema 2.5.3. *Seja* $\mathbf{V}$ *uma pseudovariedade de grupos. Então:*

(1) $\mathbf{V} \subseteq \mathbf{S}$ *se e só se todos os grupos monolíticos em* $\mathbf{V}$ *têm monolitos abelianos;*

(2) $\mathbf{V} \subseteq \mathbf{Su}$ *se e só se todos os grupos monolíticos em* $\mathbf{V}$ *têm monolitos cíclicos.*

Em particular, $\mathbf{N} \subseteq \mathbf{Su} \subseteq \mathbf{S}$.

Demonstração. Demonstremos apenas a condição (2), já que a prova de (1) é análoga.

Suponhamos que $\mathbf{V} \subseteq \mathbf{Su}$.

Seja $G \in \mathbf{V}$ um grupo monolítico com monolito M. Mostremos que M é cíclico.

Por hipótese $\mathbf{V} \subseteq \mathbf{Su}$ donde $G \in \mathbf{Su}$, pelo que existe uma série normal com factores cíclicos

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

Consideremos $M_i = G_i \cap M$, para $i \in \{0, \dots n\}$.

Temos $M_i = G_i \cap M \trianglelefteq G_{i+1} \cap M = M_{i+1}$, pois $G_i \trianglelefteq G_{i+1}$, para $i \in \{0, \dots, n-1\}$. Além disso, $G_i \trianglelefteq G$ e $M \trianglelefteq G$ pelo que $M_i = G_i \cap M \trianglelefteq G$, para $i \in \{0, \dots, n\}$.

Tomemos então a série normal

$$\{1\} = M_0 \trianglelefteq M_1 \trianglelefteq \cdots \trianglelefteq M_n = M.$$

Note-se que, para qualquer $i \in \{0, \dots, n\}$, temos $M_i = \{1\}$ ou $M_i = M$, por M ser normal minimal. Seja $i \in \{0, \dots, n\}$ tal que $M_i = \{1\}$ e $M_{i+1} = M$.

Tem-se M_{i+1}/M_i isomorfo a um subgrupo de G_{i+1}/G_i cíclico, donde M_{i+1}/M_i é cíclico. Ora, $M_{i+1}/M_i = M/\{1\} \simeq M$ pelo que M é cíclico.

Reciprocamente, seja $G \in \mathbf{V}$ e suponhamos que todo o grupo monolítico em $\mathbf{V}$ tem monolitos cíclicos.

Por G ser finito, existe uma série normal maximal

$$\{1\} \lhd\cdot\, G_1 \lhd\cdot\, G_2 \lhd\cdot\, \cdots \lhd\cdot\, G_{n-1} \lhd\cdot\, G. \tag{2.21}$$

Vejamos que cada factor desta série é monolítico em $\mathbf{V}$:

Consideremos os epimorfismos canónicos $\pi_i : G_{i+1} \twoheadrightarrow G_{i+1}/G_i$. Ora, $G_{i+1} \leq G$, $G \in \mathbf{V}$ donde $G_{i+1} \in \mathbf{V}$, portanto $G_{i+1}/G_i \in \mathbf{V}$.

A série (2.21) é normal maximal portanto tem factores simples donde G_{i+1}/G_i é o único subgrupo normal não trivial (logo também é o único subgrupo normal minimal) de G_{i+1}/G_i. Deste modo, trata-se de um grupo monolítico cujo monolito é o próprio. Portanto, por hipótese, G_{i+1}/G_i é cíclico. Assim, $G \in \mathbf{Su}$.

Resta mostrar que $\mathbf{N} \subseteq \mathbf{Su} \subseteq \mathbf{S}$. É claro que $\mathbf{Su} \subseteq \mathbf{S}$. Mostremos então que $\mathbf{N} \subseteq \mathbf{Su}$. Recordemos que $\mathbf{N}$ é a pseudovariedade dos grupos nilpotentes.

Tendo em conta (2), tomemos um grupo G monolítico de $\mathbf{N}$. Mostremos que o seu monolito M é cíclico.

Como G é nilpotente, pelo Teorema 1.8.36, todos os seus subgrupos de Sylow são normais. Suponhamos que existem números primos p_1 e p_2, distintos, divisores da ordem de G. Sejam $P_1 \in \mathrm{Syl}_{p_1}(G)$ e $P_2 \in \mathrm{Syl}_{p_2}(G)$. Ora, $\{1\} \neq P_1, P_2 \trianglelefteq G$ pelo que, pelo Lema 2.5.2,

$$\{1\} \neq M = \bigcap_{\{1\} \neq N \trianglelefteq G} N \subseteq P_1, P_2.$$

Pelo Teorema de Lagrange (1.8.3), a ordem de M divide as ordens dos grupos P_1 e P_2 o que é absurdo, pois $\{1\} \neq M$ e p_1 e p_2 são números primos distintos. Portanto G é um p-grupo, para algum número primo p.

Sendo G um p-grupo finito não trivial, tem centro $Z(G)$ não trivial. Mais, $Z(G) \trianglelefteq G$ donde, pelo Lema 2.5.2, temos $M \subseteq Z(G)$.

Provemos que M é simples. Seja $\{1\} \neq H \trianglelefteq M$. Então $H \subseteq Z(G)$ pelo que $\{1\} \neq H \trianglelefteq G$. Assim, novamente pelo Lema 2.5.2, obtemos $M \subseteq H$ donde $H = M$. Logo M é simples. Como M é um p-grupo simples, pelo Corolário 1.8.26, M tem ordem prima logo, pelo Teorema 1.8.6, M é cíclico. Portanto $G \in \mathbf{Su}$. Fica pois provado que $\mathbf{N} \subseteq \mathbf{Su}$. □

O nosso objectivo seguinte consiste em dar uma decomposição da pseudovariedade dos grupos super-resolúveis em termos das pseudovariedades $\mathbf{G}_p * \mathbf{Ab}^{p-1}$. Para isso iremos precisar de alguns resultados auxiliares que passamos a apresentar.

A próxima proposição é uma consequência do Teorema de Hall.

Proposição 2.5.4. *Todo o grupo em $\boldsymbol{G}_p * \boldsymbol{S}_{p'}$ é isomorfo a um produto semidirecto $P \rtimes H$, em que P é o (único) p-subgrupo de Sylow de G e $H \in \boldsymbol{S}_{p'}$ é um complemento de Hall de P.*

Demonstração. Seja $G \in \mathbf{G}_p * \mathbf{S}_{p'}$. Então existe um p-grupo $P \in \mathbf{G}_p$ tal que $P \trianglelefteq G$ e $G/P \in \mathbf{S}_{p'}$, logo G/P é resolúvel e $p \nmid |G/P|$. Como P é um p-grupo, $p \mid |G|$. Conclui-se pois que P tem de ser um p-subgrupo de Sylow de G, por a sua ordem ser a maior potência de p que divide $|G|$. Mais ainda, como $P \trianglelefteq G$, pelo Corolário 1.8.22 concluímos que o grupo P tem de ser o único p-subgrupo de Sylow de G.

Ora, P é um p-grupo logo, pela Proposição 1.8.35, P também é resolúvel. Mas G/P é resolúvel donde, pela Proposição 1.8.31, concluímos que G é resolúvel. Pelo Teorema de Hall (1.8.33), P admite um complemento H em G que, por ser subgrupo de um grupo resolúvel, é resolúvel. Temos $G = PH$ tal que $P \cap H = \{1\}$. Como $|H| = |G/P|$, conclui-se que $p \nmid |H|$, donde

$H \in \mathbf{S}_{p'}$. Mais, mdc($|H|$,$[G : H]$)= 1, pelo que H é um complemento de Hall de P. Assim, pela Observação 1.8.29 (2), G é isomorfo a um produto semidirecto $P \rtimes H$. □

Para a próxima caracterização dos grupos super-resolúveis monolíticos precisamos de dois lemas auxiliares:

Lema 2.5.5. *Todo o grupo monolítico em $\mathbf{N}*\mathbf{Ab}$ pertence à pseudovariedade $\mathbf{G}_p * \mathbf{Ab}$, para algum número primo p.*

Demonstração. Sejam $G \in \mathbf{N}*\mathbf{Ab}$ um grupo monolítico e M o seu monolito. Então existe $N \in \mathbf{N}$ tal que $N \trianglelefteq G$ e $G/N \in \mathbf{Ab}$.

Se G é abeliano, então $G \in \mathbf{G}_p * \mathbf{Ab}$ porque $\{1\} \trianglelefteq G$ é um p-grupo e $G/\{1\} \simeq G$ é abeliano.

Se G não é abeliano, considere-se $G' = [G, G]$, o subgrupo derivado de G. Tem-se $N \trianglelefteq G$ e G/N abeliano logo, pela Proposição 1.8.12, $[G, G] \leq N$. Mas N é um grupo nilpotente pelo que G' também é nilpotente. Assim, G' é produto dos seus subgrupos de Sylow, pelo Teorema 1.8.36. O mesmo teorema ainda nos garante que todo o subgrupo de Sylow de G' é normal em G', donde só existe um p-subgrupo de Sylow de G' para cada número primo p, divisor da ordem de G', atendendo ao Corolário 1.8.22. Portanto, os subgrupos de Sylow de G' são característicos em G' (ver página 31). Tem-se também G' *char* G, donde $G' \trianglelefteq G$, pelo que os subgrupos de Sylow de G' são normais em G, pela Proposição 1.8.15. Claramente existe pelo menos um p-subgrupo de Sylow não trivial de G', pois $G' \neq \{1\}$ uma vez que G é não abeliano. Seja $P \neq \{1\}$ um subgrupo de Sylow de G'. Usando a fórmula dada no Lema 2.5.2 prova-se que o monolito M de G é um subconjunto (logo um subgrupo) de todo o subgrupo de Sylow não trivial de G'. Pelo Teorema de Lagrange (1.8.3), conclui-se que a ordem de M divide a ordem de todo o subgrupo de Sylow de G' não trivial. Como $M \neq \{1\}$, conclui-se que só pode existir um subgrupo de Sylow de G'. Caso contrário, se existissem $P \in \mathrm{Syl}_p(G')$ e $Q \in \mathrm{Syl}_q(G')$, com $p \neq q$, resultaria que $|M| = 1$, o que é absurdo. Logo G' é um p-grupo não trivial, para algum número primo p, donde $G' \in \mathbf{G_p}$. Da Proposição 1.8.12 resulta que G/G' é abeliano. Portanto $G \in \mathbf{G}_p * \mathbf{Ab}$, para algum número primo p. □

Lema 2.5.6. *Se um produto semidirecto de grupos $P \rtimes H$, com $P \neq \{1\}$, é monolítico, então o morfismo $\alpha : H \to Aut(P)$ que define a acção é injectivo.*

Demonstração. Seja $P \neq \{1\}$ um grupo e suponhamos que o produto semidirecto $P \rtimes H$ é monolítico com monolito $\{(1, 1)\} \neq M \trianglelefteq P \rtimes H$. Tem-se

$$\begin{aligned} \ker \alpha &= \{h \in H : \alpha_h = id_P\} \\ &= \{h \in H : (p)\alpha_h = p,\ \forall p \in P\} \\ &= \{h \in H : h^{-1} \cdot p = p,\ \forall p \in P\}. \end{aligned}$$

Tem-se $\ker\alpha \trianglelefteq H$ e também $\{1\}\times\ker\alpha \trianglelefteq P\rtimes H$. De facto, para quaisquer $(p,h)\in P\rtimes H$ e $(1,h_1)\in\{1\}\times\ker\alpha$,

$$\begin{aligned}(p,h)^{-1}(1,h_1)(p,h) &= (h^{-1}\cdot p^{-1},h^{-1})(1(h_1\cdot p),h_1h)\\ &= \Big(\big(h^{-1}\cdot p^{-1}\big)\big(h^{-1}\cdot(h_1\cdot p)\big),h^{-1}(h_1h)\Big)\\ &= \big((h^{-1}\cdot p^{-1})(h^{-1}\cdot p),h^{-1}h_1h\big) \qquad (2.22)\\ &= \big(h^{-1}\cdot(p^{-1}p),h^{-1}h_1h\big)\\ &= (h^{-1}\cdot 1,h^{-1}h_1h)=(1,h^{-1}h_1h)\in\{1\}\times\ker\alpha,\end{aligned}$$

em que a igualdade (2.22) se deve ao facto de se ter $h_1\cdot p=p$, para qualquer $p\in P$, uma vez que $h_1^{-1}\in\ker\alpha$ visto que $h_1\in\ker\alpha$.

De uma forma análoga, mostra-se que $P\times\{1\}\trianglelefteq P\rtimes H$ resultando que $(\{1\}\times\ker\alpha)\cap(P\times\{1\})=\{(1,1)\}$.

Suponhamos, por absurdo, que $K=\{1\}\times\ker\alpha\neq\{(1,1)\}$. Pelo Lema 2.5.2, o monolito de um grupo é a intersecção de todos os seus subgrupos normais não triviais donde $M\subseteq K$, mas também $M\subseteq P\times\{1\}$, pelo que $M\subseteq K\cap(P\times\{1\})=\{(1,1)\}$, o que é absurdo. Portanto $\{1\}\times\ker\alpha=\{(1,1)\}$, pelo que $\ker\alpha=\{1\}$, donde α é injectivo. □

Observação 2.5.7. Recordemos alguns resultados elementares de teoria de representação de grupos, que aplicaremos a seguir.

Seja G um grupo e V um espaço vectorial sobre o corpo $\mathbb{Z}_p$. Note-se que V é um p-grupo abeliano elementar uma vez que V é isomorfo ao produto $\mathbb{Z}_p\times\cdots\times\mathbb{Z}_p$ de n cópias de $\mathbb{Z}_p$, sendo $n=dim_{\mathbb{Z}_p}V$. Suponhamos que G actua em V por automorfismos. Pela Proposição 1.9.2, resulta que os subespaços de V são exactamente os subgrupos de G e os automorfismos de espaços vectoriais são precisamente os automorfismos de grupos. A acção por automorfismos de G sobre V define um produto semidirecto $V\rtimes G$. Observemos agora que dado $H\subseteq V\times\{1\}$, tem-se $H\trianglelefteq V\rtimes G$ se e só se, para quaisquer $(v,g)\in V\rtimes G$ e $(v',1)\in H$,

$$\begin{aligned}(v,g)^{-1}(v',1)(v,g) &= (g^{-1}\cdot(-v),g^{-1})(v'+(1\cdot v),1g)\\ &= ((g^{-1}\cdot(-v))+g^{-1}\cdot(v'+(1\cdot v)),g^{-1}g)\\ &= ((g^{-1}\cdot(-v))+g^{-1}\cdot(v'+v),1)\\ &= (g^{-1}\cdot(-v+v'+v),1)=(g^{-1}\cdot v',1)\in H,\end{aligned}$$

pelo que dado $T\subseteq V$,

$$T\times\{1\}\trianglelefteq V\rtimes G \text{ se e só se } g^{-1}\cdot T\subseteq T, \text{ para qualquer } g\in G.$$

Notemos então que, se considerarmos o morfismo $\alpha: G\to Aut(V)$ que define a acção em $V\rtimes G$, tendo em conta a definição de produto semidirecto externo $V\rtimes G$, para verificarmos a condição $g^{-1}\cdot T\subseteq T$ basta ver que $(T)\alpha_g\subseteq T$.

Estamos então em condições de demonstrar o próximo resultado que caracteriza os grupos super-resolúveis monolíticos.

Proposição 2.5.8. *Todo o grupo super-resolúvel monolítico pertence à pseudovariedade* $\boldsymbol{G}_p * \boldsymbol{Ab}^{p-1}$*, para algum número primo* p*.*

Demonstração. Seja G um grupo super-resolúvel monolítico com monolito M.

Se G é abeliano então é um p-grupo. De facto, pelo Lema 2.5.2, tem-se $M = \bigcap_{\{1\}\neq N \trianglelefteq G} N = \bigcap_{\{1\}\neq P \leq G} P$ pois, como G é abeliano, todos os subgrupos de G são normais. Além disso, novamente por G ser abeliano, resulta que G é nilpotente, donde G é produto directo dos seus subgrupos de Sylow, pelo Teorema 1.8.36. Tendo em conta a igualdade acima, tem-se $M \subseteq P$, logo $M \leq P$, para todo o subgrupo P de Sylow de G. Pelo Teorema de Lagrange (1.8.3), conclui-se que a ordem de M divide a ordem de todo o subgrupo de Sylow de G não trivial. Como $M \neq \{1\}$, conclui-se que só pode existir um subgrupo de Sylow de G. Caso contrário, se existissem $P \in \mathrm{Syl}_p(G)$ e $Q \in \mathrm{Syl}_q(G)$, com $p \neq q$, resultaria que $|M| = 1$, o que é absurdo. Logo G é um p-grupo, para algum número primo p. Portanto $G \in \mathbf{G}_p$ e claramente $G/G = \{G\} \in \mathbf{Ab}^{p-1}$, pelo que $G \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$.

Se G é não abeliano, uma vez que G é super-resolúvel então G é resolúvel, pelo Lema 2.5.3. Pelo Teorema 1.8.37, $G' = [G, G]$ é nilpotente. Obtém-se $G' \trianglelefteq G$, $G' \in \mathbf{N}$ e, pela Proposição 1.8.12, $G/G' \in \mathbf{Ab}$, donde $G \in \mathbf{N} * \mathbf{Ab}$.

Ora, G é monolítico e $G \in \mathbf{N} * \mathbf{Ab}$ donde, pelo Lema 2.5.5, temos $G \in \mathbf{G}_p * \mathbf{Ab}$, para algum número primo p. Mas, pelo Lema 2.4.3, $\mathbf{G}_p * \mathbf{Ab} = \mathbf{G}_p * \mathbf{Ab}_{p'}$, logo $G \in \mathbf{G}_p * \mathbf{Ab}_{p'}$ pelo que existe $P \in \mathbf{G}_p$ e $P \trianglelefteq G$ tal que $G/P \in \mathbf{Ab}_{p'}$ e como os grupos abelianos são resolúveis $G/P \in \mathbf{S}_{p'}$. Pela demonstração da Proposição 2.5.4, existe $H \leq G$ tal que $G = PH$ e $P \cap H = \{1\}$. Assim $G/P \simeq H$ e H é p'-grupo abeliano. Portanto $G \simeq P \rtimes H$, em que P é um p-grupo não trivial, pois G é não abeliano, e H é um p'-grupo abeliano.

Como G é um grupo monolítico, $P \rtimes H$ é monolítico e, pelo Lema 2.5.6, o morfismo $\alpha : H \to Aut(P)$ que define a acção associada a $P \rtimes H$ é injectivo, donde H pode ser encarado como um subgrupo de $Aut(P)$. Vamos "identificar" um elemento $h \in H$ com um elemento de $Aut(P)$, mais precisamente com o elemento $\alpha_h \in Aut(P)$. Considere-se $\rho : H \to Aut(P/\Phi(P))$, que transforma cada automorfismo $h \in H$ no automorfismo $\overline{h}$ induzido por h no quociente de Frattini $P/\Phi(P)$, isto é,

$$\begin{array}{rcl} \overline{h} : P/\Phi(P) & \longrightarrow & P/\Phi(P) \\ p\,\Phi(P) & \longrightarrow & (ph)\,\Phi(P) \end{array}$$

Vejamos que ρ é injectivo. Temos

$$\ker \rho = \{h \in H : h\rho = id_{P/\Phi(P)}\} = \{h \in H : \overline{h} = id_{P/\Phi(P)}\}.$$

Seja $h \in H$ encarado como um automorfismo do p-grupo P. Suponhamos que $\overline{h} = id_{P/\Phi(P)}$, isto é, h induz a identidade em $P/\Phi(P)$. Note-se que H é um p'-grupo, logo h é um p'-automorfismo. Pelo Teorema de Burnside (1.8.39), resulta que h é o automorfismo identidade de P o que implica que $\ker \rho = \{1_H\}$, ou seja, ρ é injectivo.

Seja $V = P/\Phi(P)$. Pela Proposição 1.8.38, V é um p-grupo abeliano elementar e, portanto, pela Proposição 1.9.2, V é um espaço vectorial sobre $\mathbb{Z}_p$.

Note-se que $\Phi(P) \times \{1\} \subseteq P \times \{1\}$ é tal que, para todo o $h \in H$, $(\Phi(P))\alpha_h = \Phi(P)$, pois $\Phi(P)$ *char* P, donde $\Phi(P) \times \{1\} \trianglelefteq P \rtimes H$, pela Observação 2.5.7. Consideremos então o grupo $(P \rtimes H)/(\Phi(P) \times \{1\})$. Para facilidade da escrita vamos apenas escrever $(P \rtimes H)/\Phi(P)$. O objectivo agora é mostrar que

$$\frac{P \rtimes H}{\Phi(P)} \simeq \frac{P}{\Phi(P)} \rtimes H.$$

Considere-se a seguinte correspondência

$$\begin{array}{rccc} \varphi: & \dfrac{P \overset{\alpha}{\rtimes} H}{\Phi(P)} & \longrightarrow & \dfrac{P}{\Phi(P)} \overset{\rho}{\rtimes} H \\ & (p,h)\,\Phi(P) & \longrightarrow & (p\,\Phi(P), h) \end{array}$$

Mostremos que φ é um isomorfismo. Tem-se

$$\begin{array}{rcl} (p_1,h_1)\Phi(P) = (p_2,h_2)\Phi(P) & \Leftrightarrow & (p_1,h_1)(h_2^{-1}\cdot p_2^{-1}, h_2^{-1}) \in \Phi(P) \\ & \Leftrightarrow & (p_1(h_1\cdot(h_2^{-1}\cdot p_2^{-1})), h_1h_2^{-1}) \in \Phi(P) \\ & \Leftrightarrow & (p_1((h_1h_2^{-1})\cdot p_2^{-1})), h_1h_2^{-1}) \in \Phi(P) \\ & \Leftrightarrow & p_1((h_1h_2^{-1})\cdot p_2^{-1}) \in \Phi(P),\ h_1h_2^{-1} = 1 \\ & \Leftrightarrow & p_1(1\cdot p_2^{-1}) \in \Phi(P),\ h_1 = h_2 \\ & \Leftrightarrow & p_1p_2^{-1} \in \Phi(P),\ h_1 = h_2 \\ & \Leftrightarrow & (p_1\Phi(P), h_1) = (p_2\Phi(P), h_2) \end{array}$$

Portanto φ é uma aplicação injectiva. Claramente φ é sobrejectiva. Vejamos que é um morfismo:

$$\begin{array}{rcll} ((p_1,h_1)\Phi(P))\varphi((p_2,h_2)\Phi(P))\varphi & = & (p_1\Phi(P),h_1)(p_2\Phi(P),h_2) & \\ & = & (p_1\Phi(P)(h_1\cdot p_2\Phi(P)), h_1h_2) & \\ & = & (p_1\Phi(P)(p_2)h_1^{-1}\Phi(P), h_1h_2) & \\ & = & (p_1(p_2)h_1^{-1}\Phi(P), h_1h_2) & \\ & = & ((p_1(p_2)h_1^{-1}, h_1h_2)\Phi(P))\varphi & \\ & = & ((p_1(p_2)\alpha_{h_1^{-1}}, h_1h_2)\Phi(P))\varphi & (2.23) \\ & = & ((p_1,h_1)(p_2,h_2)\Phi(P))\varphi & (2.24) \\ & = & ((p_1,h_1)\Phi(P)(p_2,h_2)\Phi(P))\varphi, & \end{array}$$

em que a igualdade (2.23) resulta da identificação feita entre os elementos $h \in H$ e os elementos $\alpha_h \in Aut(V)$, enquanto que a igualdade (2.24) resulta de se ter $(p_1, h_1)(p_2, h_2) = (p_1(h_1 \cdot p_2), h_1 h_2) = (p_1(p_2)\alpha_{h_1^{-1}}, h_1 h_2)$, quaisquer que sejam $p_1, p_2 \in P$ e $h_1, h_2 \in H$.

Concluimos pois que φ é um isomorfismo.

Uma vez que G é um grupo super-resolúvel e $G \simeq P \rtimes H$, resulta que $P \rtimes H$ é super-resolúvel pelo que $(P \rtimes H)/\Phi(P)$ é super-resolúvel. Portanto $V \rtimes H$ é super-resolúvel.

Ora, o morfismo $\rho : H \to Aut(V)$ é injectivo, logo ρ é representação fiel de H, donde, pela Proposição 1.10.1, existe um morfismo $\bar{\rho} : \mathbb{Z}_p[H] \to End_{\mathbb{Z}_p}(V)$ definido por, para cada $x = \sum_{h \in H} \lambda_h h \in \mathbb{Z}_p[H]$,

$$x\bar{\rho} = \sum_{h \in H} \overline{h}\lambda_h = \sum_{h \in H} (h\rho)\lambda_h.$$

Vamos, em seguida, munir o espaço vectorial $V (\simeq \mathbb{Z}_p^n)$ com uma estrutura de módulo-$\mathbb{Z}_p[H]$, a partir de ρ pela adição usual em $\mathbb{Z}_p^n$ e o produto escalar definido por: dados $v \in V$ e $x \in \mathbb{Z}_p[H]$, $vx = v(x\bar{\rho})$, pela Observação 1.10.3.

O grupo H é finito, $\mathbb{Z}_p$ é um corpo de característica p prima, em que $p \nmid |H|$, pois H é p'-grupo, e $V \neq \{0\}$ é módulo-$\mathbb{Z}_p[H]$, donde pela Proposição 1.10.5, tem-se $V = V_1 \oplus \cdots \oplus V_t$, sendo os V_i submódulos-$\mathbb{Z}_p[H]$ de V irredutíveis. Consequentemente as respectivas representações associadas $\rho_i : H \to Aut(V_i)$ são irredutíveis.

Ora, V_i é submódulo-$\mathbb{Z}_p[H]$ de V donde, para cada $x \in \mathbb{Z}_p[H]$ e cada $v_i \in V_i$,

$$v_i x = \sum_{h \in H} (v_i)\overline{h}\lambda_h \in V_i.$$

Resulta então que $V_i \times \{1\} \subseteq V \times \{1\}$ é tal que, para cada $v_i \in V_i$ e cada $h \in H$, se tem $(v_i)\overline{h} \in V_i$, isto é, $(V_i)\overline{h} \subseteq V_i$, para todo o $h \in H$, logo $V_i \times \{1\} \trianglelefteq V \rtimes H$. Veja-se a Observação 2.5.7. Pela Proposição 1.10.6, tem-se V_i cíclico, qualquer que seja $i \in \{1, \ldots, t\}$, pelo que V_i tem dimensão 1 enquanto espaço vectorial sobre $\mathbb{Z}_p$. Assim V_i é um grupo cíclico de ordem p, pelo que $V_i \simeq \mathbb{Z}_p$. Então $t = n = dim_{\mathbb{Z}_p}(V)$.

Uma vez que ρ é uma representação fiel, H mergulha-se em $(\mathbb{Z}_{p-1})^n$. De facto, tendo em conta que cada subespaço V_i de V é tal que, para todo o $h \in H$, se tem $(V_i)\overline{h} \subseteq V_i$, resulta facilmente que a seguinte aplicação é um monomorfismo

$$\begin{array}{rcl} \psi : H & \longrightarrow & Aut(V_1) \times \cdots \times Aut(V_n) \\ h & \longrightarrow & (\overline{h}^{(1)}, \ldots, \overline{h}^{(n)}) \end{array}$$

sendo, para cada i, o automorfismo $\overline{h}^{(i)} : V_i \to V_i$ definido por $(v_i)\overline{h}^{(i)} = (0 + \cdots + v_i + \cdots + 0)\overline{h}$, para todo o $v_i \in V_i$.

Ora $Aut(V_i) \simeq Aut(\mathbb{Z}_p)$, para todo o $i \in \{1, \ldots, n\}$, pois $V_i \simeq \mathbb{Z}_p$, donde $Aut(V_1) \times \cdots \times Aut(V_n) \simeq (Aut(\mathbb{Z}_p))^n$. Uma vez que $\mathbb{Z}_p$ é grupo cíclico de ordem p, pelo Teorema 1.8.13, $Aut(\mathbb{Z}_p)$ é um grupo cíclico de ordem $p-1$ pelo que $Aut(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$. Portanto, $(Aut(\mathbb{Z}_p))^n \simeq (\mathbb{Z}_{p-1})^n$. Então $Aut(V_1) \times \cdots \times Aut(V_n) \simeq (\mathbb{Z}_{p-1})^n$, pelo que H se mergulha em $(\mathbb{Z}_{p-1})^n$. Portanto existe um monomorfismo $\bar{\psi} : H \to (\mathbb{Z}_{p-1})^n$.

Como $(\mathbb{Z}_{p-1})^n$ é um grupo abeliano, H também o é. Assim, dado $h \in H$, tem-se $|h| = |h\bar{\psi}|$. Mas $h\bar{\psi} \mid |\mathbb{Z}_{p-1}| = p-1$, logo $|h| \mid p-1$. Portanto $\exp(H) \mid p-1$, pelo que $H \in \mathbf{Ab}^{p-1}$. Concluimos que $P \rtimes H \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$. Como $G \simeq P \rtimes H$, tem-se que $G \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$, como se pretendia. □

Recordemos que, por (2.19), tem-se $\mathbf{G}_p * \mathbf{Ab}^{p-1} \subseteq \mathbf{G}_p * \mathbf{Ab}_{p'}$. Mas $\mathbf{Ab} \subseteq \mathbf{S}$, donde

$$\mathbf{G}_p * \mathbf{Ab}^{p-1} \subseteq \mathbf{G}_p * \mathbf{S}_{p'}.$$

Para o próximo resultado precisamos do seguinte lema:

Lema 2.5.9. *Todo o grupo não abeliano em $\boldsymbol{G}_p * \boldsymbol{Ab}^{p-1}$ é isomorfo a um produto semidirecto $P \rtimes H$, em que P é um p-grupo não trivial e $H \in \boldsymbol{Ab}^{p-1}$.*

Demonstração. Seja $G \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$ um grupo não abeliano. Temos $G \in \mathbf{G}_p * \mathbf{Ab}^{p-1} \subseteq \mathbf{G}_p * \mathbf{S}_{p'}$ donde, pela Proposição 2.5.4, temos $G \simeq P \rtimes H$, em que $P \in \mathrm{Syl}_p(G)$ e $H \in \mathbf{S}_{p'}$ é um complemento de Hall de G. Note-se que, por G não ser abeliano, $P \neq \{1\}$ pois, caso contrário, $G \simeq \{1\} \rtimes H \simeq H \in \mathbf{Ab}^{p-1}$, o que é absurdo.

Mostremos agora que $H \in \mathbf{Ab}^{p-1}$:

Pela demonstração da Proposição 2.5.4, tem-se $G = PH$, $P \cap H = \{1\}$ e $H \simeq G/P \in \mathbf{S}_{p'}$.

Seja $\ell = |G|$. Pelo Teorema 2.4.2,

$$G \in \mathbf{G}_p * \mathbf{Ab}^{p-1} = \mathbf{V}\left[(x^{p-1}y^{p-1})^{p^\omega} = 1, (x^{\omega-1}y^{\omega-1}xy)^{p^\omega} = 1\right],$$

portanto G satisfaz as pseudoidentidades

$$(x^{p-1}y^{p-1})^{p^\omega} = 1, \tag{2.25}$$

$$(x^{\omega-1}y^{\omega-1}xy)^{p^\omega} = 1 \tag{2.26}$$

Ora, para qualquer $g \in G$, por (2.25), tem-se $1 = (g^{p-1}1^{p-1})^{p^{\ell!}} = (g^{p-1})^{p^{\ell!}}$, donde $((gP)^{p-1})^{p^{\ell!}} = P$. Mas $G/P \simeq H$. Assim, resulta que, para todo o $h \in H$,

$$(h^{p-1})^{p^{\ell!}} = 1. \tag{2.27}$$

Mas, para qualquer $h \in H$, temos $h^{p-1} \in H$ logo, por (2.27), obtemos $|h^{p-1}| \mid p^{\ell!}$. Por hipótese $H \in \mathbf{S}_{p'}$, donde $p \nmid |H|$. Então $p \nmid |h^{p-1}|$, logo $|h^{p-1}| = 1$, para todo o $h \in H$. Assim, para todo o $h \in H$, tem-se $h^{p-1} = 1$, pelo que $|h| \mid p-1$. Conclui-se que $\exp(H) \mid p-1$.

Para quaisquer $g_1, g_2 \in G$, por (2.26), tem-se $(g_1^{\ell!-1} g_2^{\ell!-1} g_1 g_2)^{p^{\ell!}} = 1$. Portanto $((g_1P)^{\ell!-1}(g_2P)^{\ell!-1} g_1 P g_2 P)^{p^{\ell!}} = P$, donde

$$|(g_1P)^{\ell!-1}(g_2P)^{\ell!-1} g_1 P g_2 P| \mid p^{\ell!}.$$

Novamente de $G/P \simeq H$, resulta, para quaisquer $h_1, h_2 \in H$,

$$|h_1^{\ell!-1} h_2^{\ell!-1} h_1 h_2| \mid p^{\ell!}$$

e, do mesmo modo que foi visto atrás, conclui-se que $h_1^{\ell!-1} h_2^{\ell!-1} h_1 h_2 = 1$, quaisquer que sejam $h_1, h_2 \in H$.

Ora, para todo o $g \in G$, tem-se $(gP)^{\ell!} = g^{\ell!}P = P$, pois $|G| = \ell$, donde $h^{\ell!} = 1$, para todo o $h \in H$. Logo $h^{\ell!-1} = h^{-1}$. Obtemos então que $1 = h_1^{\ell!-1} h_2^{\ell!-1} h_1 h_2 = h_1^{-1} h_2^{-1} h_1 h_2 = [h_1, h_2]$, para quaisquer $h_1, h_2 \in H$, donde $H' = \{1\}$, pelo que H é abeliano. Portanto $H \in \mathbf{Ab}^{p-1}$. □

Proposição 2.5.10. *Todo o grupo em $\boldsymbol{G}_p * \boldsymbol{Ab}^{p-1}$ é super-resolúvel.*

Demonstração. Mostremos que $\mathbf{G}_p * \mathbf{Ab}^{p-1} \subseteq \mathbf{Su}$ usando o Lema 2.5.3.

Seja $G \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$ um grupo monolítico com monolito M.

Se G é abeliano, então G é nilpotente logo é super-resolúvel, pelo Lema 2.5.3. Novamente pelo Lema 2.5.3, sabemos que M é cíclico.

Se G é não abeliano, pelo Lema 2.5.9, temos $G \simeq P \rtimes H$, em que P é um p-grupo não trivial e $H \in \mathbf{Ab}^{p-1}$.

Pode então considerar-se M como monolito de um produto semidirecto $P \rtimes H$, em que $P \in \mathbf{G}_p$ e $H \in \mathbf{Ab}^{p-1}$. Pelo Lema 2.5.3, basta mostrar que M é cíclico.

Tem-se $\{(1,1)\} \neq P \times \{1\} \trianglelefteq P \rtimes H$ donde, pelo Lema 2.5.2, $M \leq P \times \{1\}$. Portanto M é um p-grupo. Logo M é nilpotente pelo que é resolúvel, pela Proposição 1.8.35. Resulta da Proposição 1.8.32 que M é um p-grupo abeliano elementar.

Facilmente se verifica que $Z(P) \times \{1\} = Z(P \times \{1\})$, donde

$$Z(P) \times \{1\} \; char \; P \times \{1\}.$$

Uma vez que $P \times \{1\} \trianglelefteq P \rtimes H$, pela Proposição 1.8.15, obtém-se $Z(P) \times \{1\} \trianglelefteq P \rtimes H$. Ora, P é um p-grupo não trivial portanto, pelo Teorema 1.8.25, tem-se $Z(P) \neq \{1\}$. Então $\{(1,1)\} \neq Z(P) \times \{1\} \trianglelefteq P \rtimes H$ donde, pelo Lema 2.5.2, $M \subseteq Z(P) \times \{1\} = Z(P \times \{1\})$.

Note-se que $\{(1,1)\} \neq P \times \{1\} \trianglelefteq P \rtimes H$ logo, pelo Lema 2.5.2 tem-se $M \leq P \times \{1\}$.

Seja $\rho : H \to Aut(P)$ o morfismo que define a acção em $P \rtimes H$. Denotemos também por ρ o morfismo que transforma cada $h \in H$ no automorfismo $h\rho_{|_M} \in Aut(M)$. Uma vez que $M \subseteq P \times \{1\}$ é tal que $M \trianglelefteq P \rtimes H$ tem-se, pela Observação 2.5.7, $M(h\rho) = M$, para todo o $h \in H$, pelo que, de facto, $h\rho_{|_M} \in Aut(M)$, qualquer que seja $h \in H$.

Note-se que, uma vez que M é um p-grupo abeliano elementar, pela Proposição 1.9.2, pode ser encarado como um espaço vectorial sobre $\mathbb{Z}_p$. Mais, tal como foi visto na demonstração da Proposição 2.5.8, M pode ser visto como um módulo-$\mathbb{Z}_p[H]$, com o produto escalar definido de forma análoga ao definido na referida demonstração. Vejamos que M é irredutível enquanto módulo-$\mathbb{Z}_p[H]$.

Seja $V \neq \{0\}$ um submódulo-$\mathbb{Z}_p[H]$ de M. Então V é um subespaço vectorial de M sobre o corpo $\mathbb{Z}_p$, logo V é um subgrupo de M, pela Proposição 1.9.2. Uma vez que V é um submódulo-$\mathbb{Z}_p[H]$ de M tem-se, para quaisquer $v \in V$ e $x \in \mathbb{Z}_p[H]$,

$$vx = \sum_{h \in H} v(h\rho)\, \lambda_h \in V.$$

Então, para quaisquer $h \in H$ e $v \in V$, obtemos $v(h\rho) \in V$, logo $V(h\rho) \subseteq V$, para qualquer $h \in H$.

Note-se que, se N é tal que $\{1\} \neq N < M \leq P \times \{1\}$ e $N(h\rho) \subseteq N$, qualquer que seja $h \in H$, tem-se $N \trianglelefteq P \rtimes H$, pela Observação 2.5.7. Então $\{1\} \neq N < M$ e $N \trianglelefteq P \rtimes H$ o que é absurdo, pois sendo M monolito de $P \rtimes H$ é subgrupo normal minimal.

Conclui-se então que $V = M$ e, portanto, M é irredutível enquanto módulo-$\mathbb{Z}_p[H]$. De forma análoga ao que foi feito na demonstração do Teorema 2.4.4, concluímos que M tem dimensão 1 enquanto espaço vectorial sobre $\mathbb{Z}_p$. Portanto M é cíclico, como se pretendia. □

Estão portanto reunidas as condições necessárias para demonstrarmos o resultado principal desta secção, que se obtém como consequência da Proposição 2.5.10:

Corolário 2.5.11. *A pseudovariedade dos grupos super-resolúveis é o supremo*

$$\bigvee_{p \in \mathbb{P}} \boldsymbol{G}_p * \boldsymbol{A}\boldsymbol{b}^{p-1}.$$

Demonstração. Pela Proposição 2.5.10, tem-se $\mathbf{G}_p * \mathbf{A}\mathbf{b}^{p-1} \subseteq \mathbf{Su}$, para qualquer número primo p. Portanto, por definição de supremo,

$$\bigvee_{p \in \mathbb{P}} \mathbf{G}_p * \mathbf{A}\mathbf{b}^{p-1} \subseteq \mathbf{Su}.$$

Para concluirmos a outra inclusão, vamos mostrar que todo o grupo super-resolúvel G é isomorfo a um subgrupo H de um produto directo $\prod_{i \in I} G_i$, em que os grupos G_i são monolíticos, e para qualquer $j \in I$,

$$\pi_{j_{|H}} : H \twoheadrightarrow G_j \quad \text{é um epimorfismo.}$$

Seja G um grupo super-resolúvel. Suponhamos que $G = \{g_1, \ldots, g_n\}$. Sejam $g_i, g_j \in G$ tais que $g_i \neq g_j$. Como $\{N : N \trianglelefteq G\}$ é finito pois G

é finito, existe $N_{i,j} \trianglelefteq \cdot G$ normal maximal tal que $g_i N_{i,j} \neq g_j N_{i,j}$, donde $G/N_{i,j} \neq \{G\}$. Note-se que se tem, no mínimo, $N_{i,j} = \{1\}$. Tome-se

$$\prod_{g_i \neq g_j} G/N_{i,j}.$$

Como $N_{i,j} \trianglelefteq \cdot G$ é normal maximal, $G/N_{i,j}$ é simples não trivial, logo $G/N_{i,j}$ é monolítico. Vejamos que $G \lesssim \prod_{g_i \neq g_j} G/N_{i,j}$:

Tome-se $\psi : G \to \prod_{g_i \neq g_j} G/N_{i,j}$ definido por $g\psi = (gN_{i,j})_{i,j}$.

Pela definição de produto directo, ψ é morfismo. Mais, ψ é de facto um monomorfismo:

Sejam $g, h \in G$ tais que $g\psi = h\psi$. Existem $k, t \in \{1, \ldots, n\}$ tais que $g = g_k$ e $h = g_t$. Suponhamos que $(gN_{i,j})_{i,j} = (hN_{i,j})_{i,j}$, isto é, $(g_k N_{i,j})_{i,j} = (g_t N_{i,j})_{i,j}$. Então $g_k N_{i,j} = g_t N_{i,j}$, para quaisquer $i, j \in \{1, \ldots, n\}$. Em particular, $g_k N_{k,t} = g_t N_{k,t}$ logo, por definição de $N_{k,t}$, tem-se $g_k = g_t$. Concluimos que ψ é injectivo.

Considere-se $\pi_{i,j} : \prod_{g_k \neq g_t} G/N_{k,t} \to G/N_{i,j}$ e $G\psi \leq \prod_{g_i \neq g_j} G/N_{i,j}$. Tem-se, para todos os $i, j \in \{1, \ldots, n\}$,

$$\pi_{i,j_{|G\psi}} : G\psi \to G/N_{i,j} \text{ um epimorfismo.}$$

Note-se que, por definição, $((g_{k,t}N_{k,t})_{k,t})\pi_{i,j} = g_{i,j}N_{i,j}$, qualquer que seja $(g_{k,t}N_{k,t})_{k,t} \in \prod_{g_k \neq g_t} G/N_{k,t}$. Logo, para qualquer $gN_{i,j} \in G/N_{i,j}$, tomando $g\psi \in G\psi$, obtemos $(g\psi)\pi_{i,j_{|G\psi}} = ((gN_{k,t})_{k,t})\pi_{i,j_{|G\psi}} = gN_{i,j}$.

Uma vez que G é super-resolúvel, $G\psi$ é super-resolúvel. Além disso, $\pi_{i,j_{|G\psi}}$ é epimorfismo, pelo que também $G/N_{i,j}$ é super-resolúvel, quaisquer que sejam $i, j \in \{1, \ldots, n\}$. Como $G/N_{i,j}$ é monolítico, pela Proposição 2.5.8, tem-se

$$G/N_{i,j} \in \mathbf{G}_{p_{i,j}} * \mathbf{Ab}^{p_{i,j}-1} \subseteq \bigvee_{p \in \mathbb{P}} \mathbf{G}_p * \mathbf{Ab}^{p-1},$$

para algum número primo $p_{i,j}$.

Como $\bigvee_{p \in \mathbb{P}} \mathbf{G}_p * \mathbf{Ab}^{p-1}$ é pseudovariedade de grupos,

$$\prod_{g_i \neq g_j} G/N_{i,j} \in \bigvee_{p \in \mathbb{P}} \mathbf{G}_p * \mathbf{Ab}^{p-1},$$

donde

$$G \in \bigvee_{p \in \mathbb{P}} \mathbf{G}_p * \mathbf{Ab}^{p-1},$$

e assim se conclui a demonstração. □

Notemos que já depois do nosso estudo estar terminado surgiu uma nova demonstração do corolário anterior dada em [9] por O. Carton, J.-E. Pin e X.

S.-Escrivà. Por se tratar de uma demonstração que envolve novos conceitos não tratados neste trabalho, decidimos manter a demonstração original que, apesar de ter exigido um grande número de resultados auxiliares, nos parece muito clara e interessante. A nova demonstração usa o facto da classe de todos os grupos super-resolúveis ser uma classe Schunk, isto é, uma classe de grupos cujas imagens epimorfas primitivas estão todas nessa classe.

Uma outra caracterização da pseudovariedade dos grupos super-resolúveis, que se baseia num resultado da secção anterior, é a seguinte:

Proposição 2.5.12. *A pseudovariedade dos grupos super-resolúveis é gerada pelos subgrupos standard de Borel $B_n(\mathbb{Z}_p)$, para todo o natural n e todo o número primo p.*

Demonstração. Seja G um grupo super-resolúvel. Pelo Corolário 2.5.11,

$$G \in \bigvee_{p\in\mathbb{P}} \mathbf{G}_p * \mathbf{Ab}^{p-1}.$$

Por definição de supremo de pseudovariedades de grupos, existem $H \leq H_1 \times \cdots \times H_k$ e $N \trianglelefteq H$ tais que, para qualquer $i \in \{1,\ldots,k\}$, $H_i \in \mathbf{G}_{p_i} * \mathbf{Ab}^{p_i-1}$, $p_i \in \mathbb{P}$ e $G \simeq H/N$.

Ora, para cada $i \in \{1,\ldots,k\}$, $H_i \in \mathbf{G}_{p_i} * \mathbf{Ab}^{p_i-1}$ logo, pelo Teorema 2.4.4, existe $n_i > 0$ tal que $H_i \lesssim B_{n_i}(\mathbb{Z}_{p_i})$, logo existe um monomorfismo $\psi_i : H_i \to B_{n_i}(\mathbb{Z}_{p_i})$. Considere-se a aplicação

$$\begin{array}{rcl} \psi : H_1 \times \cdots \times H_k & \longrightarrow & B_{n_1}(\mathbb{Z}_{p_1}) \times \cdots \times B_{n_k}(\mathbb{Z}_{p_k}) \\ (h_1,\ldots,h_k) & \longmapsto & (h_1\psi_1,\ldots,h_k\psi_k) \end{array}$$

É claro que ψ é um monomorfismo, pois cada ψ_i é um monomorfismo. Uma vez que $H \leq H_1 \times \cdots \times H_k$, tem-se $H\psi \leq B_{n_1}(\mathbb{Z}_{p_1}) \times \cdots \times B_{n_k}(\mathbb{Z}_{p_k})$.

A aplicação seguinte é claramente um epimorfismo de grupos

$$\begin{array}{rcl} \theta : H\psi & \longrightarrow & H/N \\ h\psi & \longmapsto & hN \end{array}$$

Portanto, existe um epimorfismo de $H\psi$ para G, pois $G \simeq H/N$. Assim $G \mid B_{n_1}(\mathbb{Z}_{p_1}) \times \cdots \times B_{n_k}(\mathbb{Z}_{p_k})$ e, pelo Teorema 1.5.1, sai que $G \in \mathbf{V}\langle B_n(\mathbb{Z}_p) : (n,p) \in \mathbb{N}\times\mathbb{P}\rangle$.

Reciprocamente, seja $G \in \mathbf{V}\langle B_n(\mathbb{Z}_p) : (n,p) \in \mathbb{N}\times\mathbb{P}\rangle$. Então existem $(n_1,p_1),\ldots,(n_k,p_k) \in \mathbb{N}\times\mathbb{P}$ tais que $G \mid B_{n_1}(\mathbb{Z}_{p_1}) \times \cdots \times B_{n_k}(\mathbb{Z}_{p_k})$. Logo existem $T \leq B_{n_1}(\mathbb{Z}_{p_1}) \times \cdots \times B_{n_k}(\mathbb{Z}_{p_k})$ e $\varphi : T \twoheadrightarrow G$ epimorfismo. Pelo Teorema do Homomorfismo (1.8.17), $G = T\varphi \simeq T/\ker\varphi$.

Tome-se $N = \ker\varphi \trianglelefteq T$. Uma vez que $B_{n_i}(\mathbb{Z}_{p_i}) \in \mathbf{G}_{p_i} * \mathbf{Ab}^{p_i-1}$ para qualquer $i \in \{1,\ldots,k\}$, por definição de supremo de pseudovariedades obtém-se $G \in \bigvee_{p\in\mathbb{P}} \mathbf{G}_p * \mathbf{Ab}^{p-1} = \mathbf{Su}$. Portanto G é um grupo super-resolúvel. □

Capítulo 3

Variedades de Linguagens

No Capítulo 1 apresentámos a noção de variedade de linguagens e a cada pseudovariedade de monóides $\mathbf{V}$ fizemos corresponder uma variedade de linguagens $\mathcal{V}$. Exibimos uma condição necessária e suficiente para uma dada linguagem pertencer a essa variedade (Teorema 1.6.1) e, no caso das pseudovariedades de monóides geradas por um único monóide, demos uma forma de caracterizar a respectiva variedade de linguagens associada (Teorema 1.6.4). Neste capítulo descreveremos as variedades de linguagens associadas à pseudovariedade dos grupos abelianos cujo expoente divide um certo natural n e à pseudovariedade dos p-grupos finitos, para um dado número primo p. Estes resultados preparar-nos-ão para tratar o principal objectivo deste trabalho que consiste em descrever a variedade de linguagens associada à pseudovariedade dos grupos super-resolúveis, o que será tratado no último capítulo.

A classe de todas as variedades de linguagens forma um reticulado completo para a inclusão. De facto, dada uma família $(\mathcal{H}_i)_{i\in I}$ de variedades de linguagens, o seu supremo é a variedade $\bigvee_{i\in I}\mathcal{H}_i$, sendo $A^*\left(\bigvee_{i\in I}\mathcal{H}_i\right)$ a álgebra de Boole gerada pelas linguagens de $\bigcup_{i\in I}A^*\mathcal{H}_i$, para cada alfabeto finito A.

Pelo Teorema da Variedade de Eilenberg (1.6.3), sabemos que a correspondência $\mathbf{V}\to\mathcal{V}$ é uma bijecção e que, além disso,

$$\mathbf{V}\subseteq\mathbf{W}\Longleftrightarrow A^*\mathcal{V}\subseteq A^*\mathcal{W},\text{ para qualquer alfabeto finito }A.$$

Portanto obtemos um isomorfismo de ordem entre o reticulado de todas as pseudovariedades de grupos e o reticulado de todas as variedades de linguagens. Assim, dada uma família de pseudovariedades de grupos $(\mathbf{V}_i)_{i\in I}$, se $\mathcal{V}$ for a variedade de linguagens associada à pseudovariedade de grupos $\bigvee_{i\in I}\mathbf{V}_i$, pela Proposição 1.7.1 tem-se

$$\mathcal{V}=\bigvee_{i\in I}\mathcal{V}_i,$$

em que $\mathcal{V}_i$ é a variedade de linguagens associada à pseudovariedade de grupos $\mathbf{V}_i$, para cada $i \in I$, ou seja, para qualquer alfabeto finito A,

$$A^*\mathcal{V} = A^*\left(\bigvee_{i\in I} \mathcal{V}_i\right).$$

Para cada número primo p, seja $\mathcal{U}_p$ a variedade de linguagens associada à pseudovariedade de grupos $\mathbf{G}_p * \mathbf{Ab}^{p-1}$ e seja $\mathcal{U}$ a variedade de linguagens associada à pseudovariedade dos grupos super-resolúveis $\mathbf{Su}$. Pelo que acabámos de notar e tendo em conta o Corolário 2.5.11, concluímos que

$$\mathcal{U} = \bigvee_{p\in\mathbb{P}} \mathcal{U}_p. \tag{3.1}$$

3.1 Linguagens reconhecidas por grupos abelianos

Nesta secção vamos descrever, para cada natural n, a variedade $\mathcal{A}b^n$ das linguagens reconhecidas pelos grupos de $\mathbf{Ab}^n$. Uma caracterização desta variedade de linguagens é dada pela seguinte proposição:

Proposição 3.1.1. *Seja A um alfabeto finito. Então $A^*\mathcal{A}b^n$ é a álgebra de Boole gerada pelas linguagens da forma*

$$F(a,k,n) = \{u \in A^* : |u|_a \equiv k \pmod{n}\},$$

em que $a \in A$ e $0 \leq k < n$.

Demonstração. Seja $a \in A$. Defina-se $\varphi : A^* \to \mathbb{Z}_n$ por

$$a\varphi = 1, \quad b\varphi = 0,\ \forall b \in A \setminus \{a\}.$$

É claro que φ é um morfismo tal que, para cada $0 \leq k < n$,

$$k\varphi^{-1} = \{u \in A^* : |u|_a \equiv k \pmod{n}\} = F(a,k,n).$$

Portanto, para cada $a \in A$ e cada $k \in \{0,\ldots,n-1\}$, a linguagem $F(a,k,n)$ é reconhecida por $\mathbb{Z}_n \in \mathbf{Ab}^n$. Logo, pelo Teorema 1.6.1, $F(a,k,n) \in A^*\mathcal{A}b^n$.

Concluímos que $A^*\mathcal{A}b^n$ contém a álgebra de Boole gerada pelas linguagens $F(a,k,n)$.

Reciprocamente, vamos usar o Teorema 1.6.4 e ter em conta que, pela Proposição 2.2.1, $\mathbf{Ab}^n = \mathbf{V}\langle\mathbb{Z}_n\rangle$.

Sejam $\varphi : A^* \to \mathbb{Z}_n$ um morfismo e $m \in \mathbb{Z}_n$. Então

$$\begin{aligned} u \in m\varphi^{-1} &\Leftrightarrow u\varphi = m \\ &\Leftrightarrow \left(\sum_{a\in A}(a\varphi)|u|_a\right) \equiv m \pmod{n} \\ &\Leftrightarrow \forall a \in A\ \exists k_a \in \{0,\ldots,n-1\} \quad |u|_a \equiv k_a \pmod{n} \\ &\quad \text{e} \quad \left(\sum_{a\in A}(a\varphi)k_a\right) \equiv m \pmod{n} \\ &\Leftrightarrow u \in \bigcap_{a\in A} F(a,k_a,n), \end{aligned}$$

em que a escolha dos inteiros k_a é tal que

$$\sum_{a\in A}(a\varphi)k_a \equiv m \pmod{n}.$$

Portanto cada $m\varphi^{-1}$ está na álgebra de Boole gerada pelos conjuntos $F(a,k,n)$, em que $a \in A$ e $0 \leq k < n$. □

Vamos agora exibir uma outra descrição da variedade de linguagens $\mathcal{A}b^n$, para o que vamos precisar de um novo tipo de linguagens.

Seja $A = \{a_1,\ldots,a_s\}$ um alfabeto finito. Chamamos *linguagem comutativa n-elementar* a uma linguagem da forma

$$F(r_1,\ldots,r_s,n) = \{u \in A^* : |u|_{a_1} \equiv r_1 \pmod{n},\ \ldots,\ |u|_{a_s} \equiv r_s \pmod{n}\},$$

em que, $r_1\ldots,r_s \in \{0,\ldots,n-1\}$.

Com a notação da Proposição 3.1.1, tem-se

$$F(r_1,\ldots,r_s,n) = F(a_1,r_1,n) \cap \ldots \cap F(a_s,r_s,n). \tag{3.2}$$

Consideremos o alfabeto $A = \{a,b\}$ e o natural $n = 2$. Então

$$F(0,0,2) = \{u \in A^* : |u|_a \equiv 0 \pmod{2},\ |u|_b \equiv 0 \pmod{2}\}$$

é o conjunto das palavras de A^* que têm um número par de ocorrências de cada uma das letras a e b.

Além disso, $F(0,0,2) = F(a,0,2) \cap F(b,0,2)$ em que

$$F(a,0,2) = \{u \in A^* : |u|_a \equiv 0 \pmod{2}\}$$

e

$$F(b,0,2) = \{u \in A^* : |u|_b \equiv 0 \pmod{2}\}$$

são, respectivamente, os conjuntos das palavras de A^* que têm um número par de ocorrências da letra a e um número par de ocorências da letra b.

Proposição 3.1.2. *Uma linguagem é reconhecida por um grupo em $\boldsymbol{Ab}^n$ se e só se é união disjunta de linguagens comutativas n-elementares.*

Demonstração. Sejam $A = \{a_1, \ldots, a_s\}$ um alfabeto e $G \in \mathbf{Ab}^n$. Seja L uma linguagem reconhecida por G. Então existem um morfismo $\varphi : A^* \to G$ e $P \subseteq G$ tais que $P\varphi^{-1} = L$.

Tomemos $a_1\varphi = g_1, \ldots, a_s\varphi = g_s$. Para $u \in A^*$ e $i \in \{1, \ldots, s\}$, sejam $|u|_{a_i} \equiv r_i \pmod{n}$.

Adoptando a notação aditiva para G (por G ser abeliano) temos

$$u\varphi = \sum_{1 \leq i \leq s} |u|_{a_i} g_i = \sum_{1 \leq i \leq s} r_i g_i.$$

Portanto

$$u \in L \text{ sse } u\varphi \in P \text{ sse } \sum_{1 \leq i \leq s} r_i g_i \in P.$$

Concluímos então que

$$L = \bigcup_{(r_1, \ldots, r_s) \in E} F(r_1, \ldots, r_s, n),$$

sendo

$$E = \left\{ (r_1, \ldots, r_s) : \sum_{1 \leq i \leq s} r_i g_i \in P \right\}.$$

Ora, por definição, $F(r_1, \ldots, r_s, n)$ são linguagens comutativas n-elementares e são claramente disjuntas duas a duas.

Reciprocamente, por (3.2), tem-se $F(r_1, \ldots, r_s, n) = F(a_1, r_1, n) \cap \ldots \cap F(a_s, r_s, n)$ logo, pela Proposição 3.1.1, obtemos $F(r_1, \ldots, r_s, n) \in A^*\mathcal{A}b^n$. □

3.2 Linguagens reconhecidas por p-grupos

Dado um número primo p, denotemos por $\mathcal{G}_p$ a variedade de linguagens associada à pseudovariedade de grupos $\mathbf{G}_p$, isto é, $A^*\mathcal{G}_p$ denota o conjunto das linguagens de A^* cujo monóide sintáctico está em $\mathbf{G}_p$, para cada alfabeto finito A. Nesta secção vamos descrever esta variedade e para tal será útil ter presente o que foi visto na Secção 2.3.

O teorema seguinte permite caracterizar as linguagens reconhecidas pelos grupos de $\mathbf{G}_p$:

Teorema 3.2.1. *Seja A um alfabeto finito. Então $A^*\mathcal{G}_p$ a álgebra de Boole gerada pelas linguagens da forma*

$$S(u, r, p) = \{w \in A^* : \binom{w}{u} \equiv r \pmod{p}\},$$

em que $u \in A^*$ e $0 \leq r < p$.

Demonstração. Sejam $u \in A^*$ e $0 \leq r \leq p$. Mostremos, por definição de $A^*\mathcal{G}_p$, que $Syn(S(u,r,p)) \in \mathbf{G}_p$. Para facilitar a notação seja $L = S(u,r,p)$.

Recordemos que na Secção 2.3 definimos a relação de congruência $\sim_u$ por, para $w_1, w_2 \in A^*$,

$$w_1 \sim_u w_2 \Leftrightarrow \binom{w_1}{v} \equiv \binom{w_2}{v} \pmod{p},$$

para qualquer $v \in A^*$ tal que $u \in A^*vA^*$.

Consideremos a seguinte correspondência

$$\begin{array}{rcl} \varphi : G_u = A^*/\sim_u & \longrightarrow & Syn(L) = A^*/\sigma_L \\ [w]_{\sim_u} & \longmapsto & [w]_{\sigma_L} \end{array}$$

Suponhamos que $[w_1]_{\sim_u} = [w_2]_{\sim_u}$. Tem-se $w_1 \sim_u w_2$, ou seja, $\binom{w_1}{v} \equiv \binom{w_2}{v} \pmod{p}$, para todo o factor v de u.

Sejam $v_1, v_2 \in A^*$. Então

$$\begin{array}{rcl} v_1w_1v_2 \in L & \Leftrightarrow & \binom{v_1w_1v_2}{u} \equiv r \pmod{p} \\ & \Leftrightarrow & \left(\sum_{u=u_1u_2u_3} \binom{v_1}{u_1}\binom{w_1}{u_2}\binom{v_2}{u_3}\right) \equiv r \pmod{p} \\ & \Leftrightarrow & \left(\sum_{u=u_1u_2u_3} \binom{v_1}{u_1}\binom{w_2}{u_2}\binom{v_2}{u_3}\right) \equiv r \pmod{p} \\ & \Leftrightarrow & \binom{v_1w_2v_2}{u} \equiv r \pmod{p} \\ & \Leftrightarrow & v_1w_2v_2 \in L \end{array}$$

Portanto φ é uma aplicação. Pelas definições de monóide quociente e de φ, resulta que φ é um morfismo. Mais ainda, φ é sobrejectiva.

Uma vez que G_u é um p-grupo, como φ é epimorfismo e $\mathbf{G}_p$ é pseudovariedade, resulta que $Syn(L) \in \mathbf{G}_p$. Portanto $L = S(u,r,p) \in A^*\mathcal{G}_p$.

Reciprocamente, tomemos agora $L \subseteq A^*$ tal que $Syn(L) \in \mathbf{G}_p$.

Consideremos o epimorfismo canónico $\sigma_L^\natural : A^* \twoheadrightarrow A^*/\sigma_L$. Seja $r = \mathrm{card}(A)$ e n o índice de nilpotência de $Syn(L)$. Pela Proposição 2.3.7, o morfismo $\sigma_L^\natural$ admite uma factorização na forma

$$A^* \xrightarrow{\tau} G_{r,n} = A^*/\sim_n \xrightarrow{\psi} Syn(L),$$

com $\sigma_L^\natural = \tau\psi$.

Ora, $L = (L\sigma_L^\natural)(\sigma_L^\natural)^{-1}$, donde $L = L'\tau^{-1}$, sendo $L' = L(\sigma_L^\natural\psi^{-1})$.

Portanto L é união de classes de equivalência de $\sim_n$. Recordemos que a congruência $\sim_n$ foi definida (Secção 2.3) por, para $w_1, w_2 \in A^*$,

$$w_1 \sim_n w_2 \Leftrightarrow \binom{w_1}{v} \equiv \binom{w_2}{v} \pmod{p},$$

para qualquer $v \in A^*$ tal que $|v| \leq n$.

Como cada classe de congruência de $\sim_n$ é, por definição de $\sim_n$, intersecção de conjuntos da forma $S(u, r, p)$, com $0 \leq r < p$, resulta que L é uma combinação Booleana de linguagens do tipo pretendido. □

Como consequência imediata do resultado anterior e do Teorema 1.6.1, tem-se o seguinte corolário:

Corolário 3.2.2. *Uma linguagem de A^* é reconhecida por um p-grupo se e só se é uma combinação Booleana de linguagens da forma*

$$S(u, r, p) = \{w \in A^* : \binom{w}{u} \equiv r \pmod{p}\},$$

em que $u \in A^*$ e $0 \leq r < p$.

3.3 Linguagens reconhecidas por produtos em coroa

Nesta secção daremos uma demonstração do Princípio do Produto em Coroa de Straubing que permite descrever as linguagens reconhecidas pelos produtos em coroa de dois monóides. Daremos também uma versão deste resultado para variedades de linguagens.

Começamos por descrever a relação existente entre as noções de linguagem reconhecida por um monóide de transformações e por um monóide.

Proposição 3.3.1. *Seja T um monóide e (Q, T) um monóide de transformações. Tem-se:*

(1) *Se $L \subseteq A^*$ é reconhecida por (Q, T), então L é reconhecida pot T;*

(2) *$L \subseteq A^*$ é reconhecida por (T, T) se e só se L é reconhecida pot T;*

(3) *Se $L \subseteq A^*$ é reconhecida por T, então L é uma combinação Booleana de linguagens reconhecidas por (Q, T).*

Demonstração. (1) Suponhamos que $L \subseteq A^*$ é reconhecida por (Q, T). Então existem um morfismo $\varphi : A^* \to T$, um estado $q_0 \in Q$ e um conjunto de estados $F \subseteq Q$ tais que

$$L = \{r \in A^* : q_0 \cdot (r\varphi) \in F\}.$$

Seja $P = \{t \in T : q_0 \cdot t \in F\} \subseteq T$. Tem-se

$$r \in L \Leftrightarrow q_0 \cdot (r\varphi) \in F \Leftrightarrow r\varphi \in P \Leftrightarrow r \in P\varphi^{-1}.$$

Portanto $L = P\varphi^{-1}$ e L é reconhecida por T.

(2) Suponhamos que L é reconhecida por T. Existem um morfismo $\varphi : A^* \to T$ e um subconjunto P de T tais que $L = P\varphi^{-1}$. Note-se que quando consideramos o monóide de transformações (T, T) estamos a considerar a acção definida pelo produto em T.

Tomemos $1 \in T$ e $F \subseteq T$. Tem-se

$$L = P\varphi^{-1} = \{r \in A^* : r\varphi \in P\} = \{r \in A^* : 1 \cdot (r\varphi) \in P\},$$

portanto L é reconhecida por (T, T).

A condição recíproca resulta de (1).

(3) Admitamos que L é reconhecida por T. Existem um morfismo $\varphi : A^* \to T$ e um subconjunto P de T tais que $L = P\varphi^{-1}$. Vamos mostrar que

$$L = \bigcup_{p \in P} \bigcap_{q \in Q} L_{p,q}, \tag{3.3}$$

em que $L_{p,q} = \{r \in A^* : q \cdot (r\varphi) = q \cdot p\}$.

Claramente $L \subseteq \bigcup_{p \in P} \bigcap_{q \in Q} L_{p,q}$ pois $L = P\varphi^{-1}$.

Seja $r \in \bigcup_{p \in P} \bigcap_{q \in Q} L_{p,q}$. Então existe $p \in P$ tal que $q\xi_{r\varphi} = q \cdot (r\varphi) = q \cdot p = q\xi_p$, qualquer que seja $q \in Q$ (ver notação da Subsecção 1.4.2), ou seja, $\xi_{r\varphi} = \xi_p$. Como ξ é morfismo injectivo, pois (Q, T) é monóide de transformações, tem-se $r\varphi = p \in P$, portanto $r \in P\varphi^{-1} = L$. Fica estabelecida a igualdade (3.3). Para concluir o que se pretende basta mostrar que cada linguagem $L_{p,q}$ é reconhecida por (Q, T).

Sejam $p \in P$ e $q \in Q$. Considerando o morfismo $\varphi : A^* \to T$, $q \in Q$ estado inicial, $F_{p,q} = \{q \cdot p\} \subseteq Q$ conjunto de estados finais, temos

$$L_{p,q} = \{r \in A^* : q \cdot (r\varphi) = q \cdot p\} = \{r \in A^* : q \cdot (r\varphi) \in F_{p,q}\},$$

pelo que cada linguagem $L_{p,q}$ é reconhecida por (Q, T). □

Apenas para o próximo resultado precisamos fazer algumas restrições ao trandutor subsequencial $\mathcal{T} = (Q, A, R, q_0, \cdot, *, m, \rho)$. Suponhamos que $\mathcal{T}$ é tal que as funções de transição $\cdot$ e de saída $*$ são, de facto, aplicações. Assim, o autómato $(Q, A, \cdot, q_0, \emptyset)$ é determinista e completo pelo que podemos considerar o seu monóide de transformações.

Teorema 3.3.2. *Seja $\sigma : A^* \to R$ a função subsequencial realizada pelo transdutor subsequencial $\mathcal{T} = (Q, A, R, q_0, \cdot, *, m, \rho)$ e (Q, T) o monóide de transformações de $\mathcal{T}$. Se $L \subseteq R$ é reconhecida pelo monóide de transformações (P, S), então $L\sigma^{-1}$ é reconhecida pelo produto em coroa $(P, S) \circ (Q, T)$.*

Demonstração. Suponhamos que $L \subseteq R$ é reconhecida por (P, S). Então existem um morfismo $\varphi : R \to S$, um estado $p_0 \in P$ e um conjunto de estados $F \subseteq P$ tais que

$$L = \{r \in R : p_0 \cdot (r\varphi) \in F\}. \tag{3.4}$$

Ora, $(P,S)\circ(Q,T)=(P\times Q,W)$, em que $W=S^Q\rtimes T$. Defina-se $\psi:A^*\to W$ do seguinte modo: para cada $u\in A^*$, $u\psi$ é tal que, para qualquer $(p,q)\in P\times Q$,

$$(p,q)\cdot(u\psi)=(p\cdot(q*u)\varphi,q\cdot u).$$

Para cada $u\in A^*$, tome-se $f_u:Q\to S$ definida por $qf_u=(q*u)\varphi$, para qualquer $q\in Q$. É claro que ψ está bem definida. Note-se que $u\psi=(f_u,u)$, para cada $u\in A^*$.

Sejam $u,v\in A^*$ e $q\in Q$. Tem-se

$$\begin{aligned} q(f_u(u\cdot f_v)) &= qf_u(q\cdot u)f_v=(q*u)\varphi((q\cdot u)*v)\varphi \\ &= ((q*u)((q\cdot u)*v))\varphi=(q*(uv))\varphi \\ &= qf_{uv}. \end{aligned}$$

Portanto $f_u(u\cdot f_v)=f_{uv}$, para quaisquer $u,v\in A^*$, pelo que se conclui que ψ é um morfismo.

Seja $I=\{(p,q)\in P\times dom\rho:p\cdot(q\rho)\varphi\in F\}\subseteq P\times Q$.

Por definição de ψ, para $p_0\in P$, $q_0\in Q$ e $m\in R$ obtemos

$$(p_0\cdot(m\varphi),q_0)\cdot(u\psi)=((p_0\cdot(m\varphi))\cdot(q_0*u)\varphi,q_0\cdot u)=(p_0\cdot(m\varphi(q_0*u)\varphi),q_0\cdot u).$$

Assim, por (3.4) e pelas definições de σ e de I,

$$\begin{aligned} L\sigma^{-1} &= \{u\in A^*:u\sigma\in L\} \\ &= \{u\in A^*:p_0\cdot(u\sigma)\varphi\in F\} \\ &= \{u\in A^*:p_0\cdot(m(q_0*u)(q_0\cdot u)\rho)\varphi\in F\} \\ &= \{u\in A^*:p_0\cdot\big(m\varphi(q_0*u)\varphi((q_0\cdot u)\rho)\varphi\big)\in F\} \\ &= \{u\in A^*:(p_0\cdot(m\varphi),q_0)\cdot(u\psi)\in I\}. \end{aligned}$$

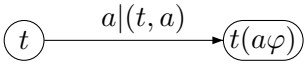
Ora $(p_0\cdot(m\varphi),q_0)\in P\times Q$, pelo que $L\sigma^{-1}$ é reconhecida por $(P\times Q,W)=(P,S)\circ(Q,T)$, como se pretendia. □

Para descrever as linguagens reconhecidas por produtos em coroa de dois monóides de transformações precisamos apresentar uma ferramenta auxiliar: o conceito de *transdutor sequencial de um morfismo*.

Sejam A um alfabeto finito, T um monóide e $\varphi:A^*\twoheadrightarrow T$ um morfismo sobrejectivo de monóides. Considere-se $B_T=T\times A$ e $\mathcal{T}_\varphi=(T,A,B_T^*,1,\cdot,*)$ o transdutor sequencial definido por: dados $t\in T$ e $a\in A$,

$$t\cdot a=t(a\varphi)\ \text{ e }\ t*a=(t,a).$$

As suas transições são dadas pelo seguinte diagrama:



Note-se que o monóide de transformações de $\mathcal{T}_\varphi$ é (T, T). De facto, o seu monóide de transformações é o monóide de transformações do autómato $\mathcal{A}_{\mathcal{T}_\varphi} = (T, A, \cdot, 1, \emptyset)$, ou seja, $(T, A^*/\tau)$, em que

$$\begin{aligned} \tau &= \{(w, z) \in A^* \times A^* : \forall t \in T,\ t(w\varphi) = t(z\varphi)\} \\ &= \{(w, z) \in A^* \times A^* : w\varphi = z\varphi\} \\ &= \ker \varphi. \end{aligned}$$

Uma vez que φ é um morfismo sobrejectivo de monóides, pelo Teorema do Homomorfismo (1.1.2), temos $T \simeq A^*/\ker\varphi = A^*/\tau$. Portanto (T, T) é, de facto, o monóide de transformações de $\mathcal{T}_\varphi$.

Observe-se que o autómato $\mathcal{A}_{\mathcal{T}_\varphi}$ é determinista e completo. Logo podemos efectivamente falar no seu monóide de transformações.

A função sequencial $\sigma_\varphi : A^* \to B_T^*$ realizada por $\mathcal{T}_\varphi$ designa-se por *função sequencial associada a* φ e é tal que, para quaisquer $a_1 \ldots, a_n \in A$,

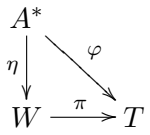
$$(a_1 \ldots a_n)\sigma_\varphi = (1, a_1)(a_1\varphi, a_2) \ldots ((a_1 \ldots a_{n-1})\varphi, a_n).$$

Note-se que a função σ_φ assim definida é de facto uma aplicação pois a imagem de cada palavra $u \in A^*$ está definida.

Sejam $X = (P, S)$ e $Y = (Q, T)$ monóides de transformações. Consideremos $Z = X \circ Y = (P \times Q, W)$, em que $W = S^Q \rtimes T$, o seu produto em coroa. Seja $L \subseteq A^*$ uma linguagem reconhecida por Z. Por definição existem um estado (inicial) $(p_0, q_0) \in P \times Q$, um subconjunto $F \subseteq P \times Q$ e um morfismo de monóides $\eta : A^* \to W$ tais que

$$L = \{u \in A^* : (p_0, q_0) \cdot (u\eta) \in F\}. \tag{3.5}$$

Tomemos $\pi : W \to T$ a projecção natural definida por $(f, t)\pi = t$, que é um epimorfismo, e $\varphi = \eta\pi : A^* \to T$. O seguinte diagrama é comutativo



Seja $B_Q = Q \times A$. Definimos uma aplicação $\sigma : A^* \to B_Q^*$ por

$$(a_1 a_2 \ldots a_n)\sigma = (q_0, a_1)(q_0 \cdot (a_1\varphi), a_2) \ldots (q_0 \cdot (a_1 \ldots a_{n-1})\varphi, a_n),$$

para quaisquer $a_1, a_2, \ldots, a_n \in A$, $n \geq 0$.

Para cada $q \in Q$, definimos uma aplicação $\lambda_q : B_T \to B_Q^*$ por

$$(t, a)\lambda_q = (q \cdot t, a),$$

para cada $(t, a) \in B_T$. Note-se que λ_q pode ser prolongada de forma natural a um morfismo $\lambda_q : B_T^* \to B_Q^*$.

Então λ_{q_0} serve de "ponte" entre σ e σ_φ, pois $\sigma = \sigma_\varphi \lambda_{q_0}$, ou seja, o seguinte diagrama é comutativo

$$\begin{array}{ccc} A^* & & \\ {\scriptstyle \sigma_\varphi}\downarrow & \searrow^{\sigma} & \\ B_T^* & \xrightarrow{\lambda_{q_0}} & B_Q^* \end{array} \tag{3.6}$$

Note-se que σ é também uma função sequencial, realizada pelo transdutor $\mathcal{T}_\sigma = (Q, A, B_Q^*, q_0, \cdot, *)$, em que dados $q \in Q$ e $a \in A$,

$$q \cdot a = q \cdot (a\varphi) \quad \text{e} \quad q * a = (q, a).$$

Com estas definições tem-se o seguinte:

Teorema 3.3.3. *A linguagem L é uma união finita de linguagens da forma $U \cap (V\sigma_\varphi^{-1})$, sendo $U \subseteq A^*$ reconhecida por T e $V \subseteq B_T^*$ reconhecida por $X = (P, S)$.*

Demonstração. De acordo com o que temos em cima, $F \subseteq P \times Q$ logo, por (3.5), tem-se

$$\begin{aligned} L &= \{u \in A^* : (p_0, q_0) \cdot (u\eta) \in F\} \\ &= \bigcup_{(p,q)\in F} \{u \in A^* : (p_0, q_0) \cdot (u\eta) = (p, q)\}. \end{aligned} \tag{3.7}$$

Consideremos $\eta : A^* \to W$ definido, para cada letra $a \in A$, por $a\eta = (f_a, t_a)$, em que $a\varphi = t_a$, o que faz sentido porque $\varphi = \eta\pi$. Assim sendo tem-se $t_{ab} = t_a t_b$, para quaisquer $a, b \in A$, pois φ é morfismo.

Definimos uma aplicação $\alpha : B_Q \to S$ por $(q, a)\alpha = qf_a$, para $(q, a) \in B_Q$. Pela propriedade universal dos monóides livres α estende-se a um morfismo (que designaremos também por α) de monóides $\alpha : B_Q^* \to S$.

Tome-se $\gamma = \lambda_{q_0}\alpha$, então o seguinte diagrama é comutativo

$$\begin{array}{ccc} B_T^* & \xrightarrow{\lambda_{q_0}} & B_Q^* \\ & {\scriptstyle \gamma}\searrow & \downarrow{\scriptstyle \alpha} \\ & & S \end{array} \tag{3.8}$$

Compondo os diagramas (3.6) e (3.8) obtemos outro diagrama comutativo

$$\begin{array}{ccc} A^* & & \\ {\scriptstyle \sigma_\varphi}\downarrow & \searrow^{\sigma} & \\ B_T^* & \xrightarrow{\lambda_{q_0}} & B_Q^* \\ & {\scriptstyle \gamma}\searrow & \downarrow{\scriptstyle \alpha} \\ & & S \end{array}$$

Seja $u = a_1 a_2 \dots a_n \in A^*$ uma palavra. Tem-se

$$\begin{aligned}
(p_0, q_0) \cdot (u\eta) &= (p_0, q_0) \cdot ((a_1\eta)(a_2\eta)\dots(a_n\eta)) \\
&= (p_0, q_0) \cdot ((f_{a_1}, t_{a_1})(f_{a_2}, t_{a_2})\dots(f_{a_n}, t_{a_n})) \\
&= (p_0 \cdot ((q_0 f_{a_1})\dots(q_0 \cdot (t_{a_1}\dots t_{a_{n-1}}))f_{a_n}), q_0 \cdot (t_{a_1}\dots t_{a_n})) \\
&= (p_0 \cdot ((q_0)f_{a_1}\dots(q_0 \cdot (a_1\dots a_{n-1})\varphi)f_{a_n}), q_0 \cdot (u\varphi)) \\
&= (p_0 \cdot ((q_0, a_1)\alpha\dots(q_0 \cdot (a_1\dots a_{n-1})\varphi, a_n)\alpha), q_0 \cdot (u\varphi)) \\
&= (p_0 \cdot ((q_0, a_1)\dots(q_0 \cdot (a_1\dots a_{n-1})\varphi, a_n))\alpha, q_0 \cdot (u\varphi)) \\
&= (p_0 \cdot ((a_1\dots a_n)\sigma)\alpha, q_0 \cdot (u\varphi)) \\
&= (p_0 \cdot (u\sigma_\varphi)\gamma, q_0 \cdot (u\varphi))
\end{aligned}$$

Portanto, fixado $(p, q) \in F$, obtemos $(p_0, q_0) \cdot (u\eta) = (p, q)$ se e só se

$$p_0 \cdot (u\sigma_\varphi)\gamma = p \tag{3.9}$$

e

$$q_0 \cdot (u\varphi) = q \tag{3.10}$$

Tomemos $U = \{u \in A^* : q_0 \cdot (u\varphi) = q\}$ e $V = \{v \in B_T^* : p_0 \cdot (v\sigma_\varphi)\gamma = p\}$. Então a condição (3.9) pode ser reformulada por $u\sigma_\varphi \in V$, isto é, $u \in \sigma_\varphi^{-1}$ e a condição (3.10) pode ser reformulada por $u \in U$.

Considerando $q_0 \in Q$ como estado inicial, o morfismo $\varphi : A^* \to T$, o conjunto $\{q\} \subseteq Q$ como conjunto de estados finais e tendo em conta a definição de U, concluímos que U é reconhecida por (Q, T). Logo, pela Proposição 3.3.1, U é reconhecida por T.

Tomando $p_0 \in P$ como estado inicial, o morfismo $\gamma : B_T^* \to S$, o conjunto $\{p\} \subseteq P$ como conjunto de estados finais e tendo em conta a definição de V, temos V reconhecida por (P, S). Atendendo à igualdade (3.7), tem-se o pretendido. □

Quando os monóides de transformação X e Y são ambos monóides, como consequência do teorema anterior obtemos o *Princípio do Produto em Coroa*:

Corolário 3.3.4. *Dados um alfabeto finito A e monóides S e T, toda a linguagem de A^* reconhecida por $S \circ T$ é combinação Booleana finita de linguagens da forma $U \cap (V\sigma_\varphi^{-1})$, em que $\varphi : A^* \to T$ é um morfismo de monóides, $U \subseteq A^*$ é reconhecida por T (pelo morfismo φ) e $V \subseteq B_T^*$ é reconhecida por S.*

Demonstração. Seja $L \subseteq A^*$ uma linguagem reconhecida por $S \circ T$. Pela Proposição 3.3.1 (3), resulta que L é combinação Booleana finita de linguagens reconhecidas por $(S \times T, S \circ T) = (S \times T, S^T \rtimes T)$.

Tomemos $Z = (S \times T, S \circ T)$. Então $Z = X \circ Y$, em que $X = (S, S)$ e $Y = (T, T)$. Pelo Teorema 3.3.3, cada linguagem reconhecida por Z é união finita de linguagens da forma $U \cap (V\sigma_\varphi^{-1})$, em que $\varphi : A^* \to T$ é um

morfismo, tendo-se que T reconhece $U \subseteq A^*$ e $V \subseteq B_T^*$ é reconhecida por $X = (S, S)$. A linguagem V é reconhecida por S, pela Proposição 3.3.1 (2), pelo que se obtém o resultado pretendido. □

O seguinte resultado, que resulta do corolário anterior, fornece-nos uma descrição das linguagens que são reconhecidas pelos monóides pertencentes a uma pseudovariedade produto.

Corolário 3.3.5. *Sejam $\boldsymbol{V}$ e $\boldsymbol{W}$ pseudovariedades de monóides, $\mathcal{V}$ e $\mathcal{W}$ as respectivas variedades de linguagens associadas e $\mathcal{U}$ a variedade de linguagens associada a $\boldsymbol{V} * \boldsymbol{W}$. Então, para todo o alfabeto finito A, o conjunto de linguagens $A^*\mathcal{U}$ é a mais pequena álgebra de Boole que contém $A^*\mathcal{W}$ e também as linguagens da forma $V\sigma_\varphi^{-1}$, em que σ_φ é a função sequencial associada ao morfismo $\varphi : A^* \to T$, com $T \in \boldsymbol{W}$, e $V \in B_T^*\mathcal{V}$.*

Demonstração. Note-se que $\mathbf{W} \subseteq \mathbf{V} * \mathbf{W}$ pois, dado $G \in \mathbf{W}$, como $\{1\} \in \mathbf{V}$ e $G/\{1\} \simeq G \in \mathbf{W}$ temos $G \in \mathbf{V} * \mathbf{W}$. Assim, pelo Teorema da Variedade de Eilenberg (1.6.3), para todo o alfabeto finito A, tem-se $A^*\mathcal{W} \subseteq A^*\mathcal{U}$.

Seja $V \subseteq B_T^*$ uma linguagem reconhecida por um monóide $S \in \mathbf{V}$, isto é, $V \in B_T^*\mathcal{V}$. Uma vez que (T, T) é o monóide de transformações de $\mathcal{T}_\varphi$ e V é reconhecida por S, pela Proposição 3.3.1, V é reconhecida por (S, S) donde, atendendo ao Teorema 3.3.2, $V\sigma_\varphi^{-1}$ é reconhecida por $(S, S) \circ (T, T) = (S \times S, S \circ T)$. Novamente pela Proposição 3.3.1 concluímos que $V\sigma_\varphi^{-1} \subseteq A^*$ é reconhecida por $S \circ T \in \mathbf{V} * \mathbf{W}$, pelo que $V\sigma_\varphi^{-1} \in A^*\mathcal{U}$.

Reciprocamente, pelo Corolário 2.1.4 tem-se

$$\mathbf{V} * \mathbf{W} = \{G : G \mid (S \circ T),\ S \in \mathbf{V}, T \in \mathbf{W}\}.$$

Como toda a linguagem $L \in A^*\mathcal{U}$ é reconhecida por um monóide $G \in \mathbf{V} * \mathbf{W}$, existem $S \in \mathbf{V}$ e $T \in \mathbf{W}$ tais que $G \mid (S \circ T)$. Pelo Teorema 1.4.3, a linguagem L é reconhecida por $S \circ T$. Pelo corolário anterior, tem-se o pretendido. □

3.4 Produto de linguagens com contador

Recordemos que o Teorema da Variedade de Eilenberg diz-nos que, de uma certa forma, as variedades de linguagens racionais estão em correspondência bijectiva com as pseudovariedades de monóides (finitos). Esta correspondência estende-se a operações entre linguagens e entre monóides. Nesta secção vamos considerar o caso especial do produto de linguagens com contador e descreveremos a operação associada a esta em monóides.

Vamos agora estudar a seguinte operação de produto de linguagens com contador, também designado por *produto modular concatenado*,

$$L_1, \ldots, L_k \longrightarrow (L_1 a_1 L_2 \ldots a_{k-1} L_k)_{r,p},$$

em que $L_1, \ldots, L_k$ são linguagens, $a_1, \ldots, a_{k-1}$ são letras, r, p são inteiros e $(L_1 a_1 L_2 \ldots a_{k-1} L_k)_{r,p}$ é o conjunto das palavras u tais que o número de factorizações de u na forma $u = u_1 a_1 u_2 \ldots a_{k-1} u_k$, com $u_i \in L_i$, para $i \in \{1, \ldots, k\}$, é congruente com r módulo p.

Temos como objectivo seguinte descrever a operação entre monóides associada a esta operação produto entre linguagens. Essa operação é o produto de Schützenberger que passamos a descrever.

Seja p um número primo e $\mathbb{Z}_p$ o corpo dos inteiros módulo p. Sejam $k \geq 2$ e $G_1, \ldots, G_k$ grupos.

Denotamos por K a álgebra de grupo $\mathbb{Z}_p[G_1 \times \cdots \times G_k]$ de $G_1 \times \cdots \times G_k$ sobre $\mathbb{Z}_p$, trata-se de um anel de polinómios sobre $G_1 \times \cdots \times G_k$ com coeficientes em $\mathbb{Z}_p$.

Denotamos por $\mathbb{Z}_p \Diamond_k(G_1, \ldots, G_k)$ o *produto de Schützenberger* sobre $\mathbb{Z}_p$ dos grupos $G_1, \ldots, G_k$ que se define como sendo o subgrupo de $Gl_k(K)$ sobre $\mathbb{Z}_p$ constituído por todas as matrizes $m = (m_{i,j})_{i,j \in \{1,\ldots,k\}}$ satisfazendo as três condições seguintes:

(1) se $i > j$ então $m_{i,j} = 0$;

(2) se $i = j$ então $m_{i,j} = (1, \ldots, 1, g_i, 1, \ldots, 1)$ para algum $g_i \in G_i$;

(3) se $i < j$ então $m_{i,j} \in \mathbb{Z}_p[1 \times \cdots \times 1 \times G_i \times G_{i+1} \times \cdots \times G_j \times 1 \times \cdots \times 1]$.

Os elementos de $\mathbb{Z}_p \Diamond_k(G_1, \ldots, G_k)$ são matrizes triangulares superiores cuja i-ésima entrada da diagonal "é" um elemento de G_i e cuja (i, j)-entrada, com $i < j$, é um polinómio com "suporte" $G_i \times G_{i+1} \times \cdots \times G_j$.

Observemos que a definição de produto de Schützenberger $\mathbb{Z}_p \Diamond_k(G_1, \ldots, G_k)$ que acabámos de dar generaliza a definição de produto de Schützenberger de grupos $\Diamond_k(G_1, \ldots, G_k)$ a qual pode ser encontrada, por exemplo, em [20, 24 ou 25].

Sejam $a_1, \ldots, a_{k-1} \in A$ e $L_1, \ldots, L_k \subseteq A^*$ linguagens reconhecidas por $G_1, \ldots, G_k$, respectivamente. Para cada $i \in \{1, \ldots, k\}$, seja $\eta_i : A^* \to G_i$ um morfismo que reconhece a linguagem L_i. Existem $P_i \subseteq G_i$ tais que $L_i = P_i \eta_i^{-1}$.

Vamos definir uma aplicação $\mu : A \to \mathbb{Z}_p \Diamond_k(G_1, \ldots, G_k)$ do seguinte modo:

Para cada letra $a \in A$, a matriz $a\mu \in \mathbb{Z}_p \Diamond_k(G_1, \ldots, G_k)$ é dada por

$a\mu_{i,i} = (1, \ldots, 1, a\eta_i, 1, \ldots, 1)$, se $1 \leq i \leq k$;

$a\mu_{i,j} = (1, \ldots, 1)$, se $j = i + 1$, $a = a_i$ e $1 \leq i < k$;

$a\mu_{i,j} = 0$, caso contrário.

Pela propriedade universal do monóide livre A^*, a aplicação μ estende-se de forma natural a um morfismo $\mu : A^* \to \mathbb{Z}_p \Diamond_k(G_1, \ldots, G_k)$.

Lema 3.4.1. *Seja $w \in A^+$. Tem-se:*

(1) *Se $1 \leq j < i \leq k$, então $w\mu_{i,j} = 0$;*

(2) *Se $1 \leq i \leq k$, então $w\mu_{i,i} = w\eta_i$;*

(3) *Se $1 \leq i < j \leq k$, então $w\mu_{i,j} = \sum \lambda_g g$, em que a soma é estendida aos elementos da forma $g = (1, \ldots, 1, g_i, g_{i+1}, \ldots, g_j, 1, \ldots, 1)$ (em que $g_h \in G_h$, para todo o h) e λ_g é o número (calculado em $\mathbb{Z}_p$) de factorizações de w na forma $w = w_i a_i w_{i+1} \ldots a_{j-1} w_j$, com $w_i\eta_i = g_i, \ldots, w_j\eta_j = g_j$.*

Demonstração. Seja $w = b_1 \ldots b_m$, com $m \geq 1$ e $b_1, \ldots, b_m \in A$.

Tem-se $w\mu = (b_1\mu) \ldots (b_m\mu)$. Como as matrizes $a\mu$, com $a \in A$, são triangulares superiores e o produto de matrizes triangulares superiores é triangular superior, as afirmações (1) e (2) relativas a $w\mu_{i,j}$, com $j < i$ ou $j = i$, são imediatas.

Se $1 \leq i < j \leq k$, então

$$w\mu_{i,j} = \sum_{i=h_0 \leq \cdots \leq h_m = j} (b_1\mu_{h_0,h_1}) \ldots (b_m\mu_{h_{m-1},h_m}),$$

portanto

$$\begin{aligned} w\mu_{i,j} = \sum \; & (1, \ldots, 1, (b_1 \ldots b_{q_i - 1})\mu_i, (b_{q_i+1} \ldots b_{q_{i+1}-1})\mu_{i+1}, \\ & \ldots, (b_{q_{j-1}+1} \ldots b_m)\mu_j, 1, \ldots, 1), \end{aligned}$$

sendo a soma estendida a todas as sequências $1 \leq q_i < q_{i+1} < \cdots < q_j \leq m$ tais que $b_{q_s} = a_s$, para todo o $i \leq s \leq j$.

Sejam $w_i = b_1 \ldots b_{q_i - 1}, w_{i+1} = b_{q_i+1} \ldots b_{q_{i+1}-1}, \ldots, w_j = b_{q_{j-1}+1} \ldots b_m$ e $g_i = (w_i\mu_i), g_{i+1} = (w_{i+1}\mu_{i+1}), \ldots, g_j = (w_j\mu_j)$. Tem-se então

$$w\mu_{i,j} = \sum (1, \ldots, 1, g_i, g_{i+1}, \ldots, g_j, 1, \ldots, 1). \qquad \square$$

Estamos agora em condições de demonstrar o seguinte teorema que permite caracterizar as linguagens reconhecidas por produtos modulares concatenados:

Teorema 3.4.2. *Sejam $k \geq 2$, $p \geq 1$, $p \in \mathbb{P}$ inteiros, $G_1, \ldots, G_k$ grupos e $a_1, \ldots, a_{k-1} \in A$. Suponhamos que $L_1, \ldots, L_k \subseteq A^*$ são linguagens reconhecidas por $G_1, \ldots, G_k$, respectivamente. Então, para todo o $r \geq 0$, a linguagem $(L_1 a_1 L_2 \ldots a_{k-1} L_k)_{r,p}$ é reconhecida por $\mathbb{Z}_p \Diamond_k (G_1, \ldots, G_k)$.*

Demonstração. Sejam $r \geq 0$, $P = P_1 \times \cdots \times P_k$ e

$$Q = \{g \in \mathbb{Z}_p \Diamond_k (G_1, \ldots, G_k) : g_{1,k} = \sum_{s \in G_1 \times \cdots \times G_k} \lambda_s s \quad \text{e} \quad \sum_{s \in P} \lambda_s \equiv r \pmod{p}\}.$$

Dado $w \in A^*$,

$$w \in Q\mu^{-1} \Leftrightarrow w\mu_{1,k} = \sum_s \lambda_s s \quad \text{é tal que} \quad \sum_{s\in P} \lambda_s \equiv r \pmod p,$$

em que, pelo Lema 3.4.1, $s = (s_1, \ldots, s_k)$ com $s_h \in G_h$, para todo o $h \in \{1, \ldots, k\}$, e λ_s é o número de factorizações (calculadas em $\mathbb{Z}_p$) da forma $w = w_1 a_1 w_2 \ldots a_{k-1} w_k$, em que $w_h \eta_h = s_h$, para todo o $h \in \{1, \ldots, k\}$. Ora, para qualquer $h \in \{1, \ldots, k\}$, $P_h \eta_h^{-1} = L_h$. Portanto

$$w \in Q\mu^{-1} \Leftrightarrow w \in (L_1 a_1 L_2 \ldots a_{k-1} L_k)_{r,p}.$$

Assim, $Q\mu^{-1} = (L_1 a_1 L_2 \ldots a_{k-1} L_k)_{r,p}$, em que $Q \subseteq \mathbb{Z}_p \Diamond_k (G_1, \ldots, G_k)$ e $\mu : A^* \to \mathbb{Z}_p \Diamond_k (G_1, \ldots, G_k)$ é um morfismo.

Concluímos que a linguagem $(L_1 a_1 L_2 \ldots a_{k-1} L_k)_{r,p}$ é reconhecida pelo grupo $\mathbb{Z}_p \Diamond_k (G_1, \ldots, G_k)$. □

Contrariamente ao produto concatenado, o produto modular concatenado não é distributivo em relação à união. Por exemplo, se $A = \{a\}$ é um alfabeto com apenas uma letra então

$$(\{a\}a\{a,1\})_{1,2} = \{aaa, aa\}, \quad (\{1\}a\{a,1\})_{1,2} = \{aa, a\}$$

$$\text{mas} \ \ (\{a,1\}a\{a,1\})_{1,2} = \{aaa, a\}$$

pois $aa = (a)a(1) = (1)a(a)$.

No entanto é válida uma propriedade mais fraca que irá ser útil posteriormente:

Proposição 3.4.3. *Sejam $L_0, \ldots, L_k$ linguagens de A^* e $i \in \{0, \ldots, k\}$. Suponhamos que L_i é união disjunta das linguagens $L_{i,1}, \ldots, L_{i,\ell}$. Então cada produto modular $(L_0 a_1 L_1 \ldots a_k L_k)_{r,p}$ é uma união de intersecções de linguagens da forma $(L_0 a_1 L_1 \ldots L_{i-1} a_i L_{i,j} a_{i+1} L_{i+1} \ldots a_k L_k)_{s,p}$, com $1 \leq j \leq \ell$ e $0 \leq s < p$.*

Demonstração. Vamos mostrar que $(L_0 a_1 L_1 \ldots a_k L_k)_{r,p}$ é igual a

$$\bigcup_{\substack{r_1+\cdots+r_\ell \equiv r \pmod p \\ 0 \leq r_1, \ldots, r_\ell < p}} \ \bigcap_{1 \leq j \leq \ell} (L_0 a_1 L_1 \ldots L_{i-1} a_i L_{i,j} a_{i+1} L_{i+1} \ldots a_k L_k)_{r_j,p} \quad (3.11)$$

De facto, se para uma dada palavra u, consideremos o conjunto $F(u)$ de todos os $k+1$-uplos $(u_0, u_1, \ldots, u_k)$ tais que $u = u_0 a_1 u_1 \ldots a_k u_k$, com $u_0 \in L_0, \ldots, u_k \in L_k$, então o conjunto $F(u)$ é a união disjunta dos conjuntos $F_j(u)$ definidos por

$$F_j(u) = \{(u_0, u_1, \ldots, u_k) \in F(u) : u_i \in L_{i,j}\}.$$

Segue-se que $|F(u)| = \sum_{1 \leq j \leq \ell} |F_j(u)|$ e, portanto, $|F(u)| \equiv r \pmod p$ se e só se existem $r_1, \ldots, r_\ell$ tais que $r_1 + \cdots + r_\ell \equiv r \pmod p$ e $|F_i(u)| \equiv r_i \pmod p$, para qualquer $i \in \{1, \ldots, \ell\}$. Isto prova (3.11) e a proposição. □

Voltando ao exemplo anterior, tem-se:

$$(\{a\}a\{a,1\})_{0,2} = A^* \setminus \{aaa, aa\}, \quad (\{1\}a\{a,1\})_{0,2} = A^* \setminus \{aa, a\}$$

Portanto

$$(\{a\}a\{a,1\})_{0,2} \cap (\{1\}a\{a,1\})_{1,2} = \{a\}$$
$$(\{a\}a\{a,1\})_{1,2} \cap (\{1\}a\{a,1\})_{0,2} = \{aaa\}$$

sendo a união destas duas linguagens $(\{a,1\}a\{a,1\})_{1,2}$.

Capítulo 4

Linguagens reconhecidas por grupos super-resolúveis

Neste capítulo iremos apresentar duas caracterizações da variedade de linguagens associada à pseudovariedade dos grupos super-resolúveis. Uma delas é dada através de produtos modulares concatenados e a outra usando funções realizadas por transdutores na forma triangular estrita.

4.1 Produtos modulares concatenados e linguagens reconhecidas por grupos super-resolúveis

Depois de todo o trabalho que foi feito para trás, estamos agora em condições de demonstrar o principal teorema que nos dará uma forma mais explícita de descrever as linguagens de $A^*\mathcal{U}_p$, para cada alfabeto finito A, isto é, as linguagens reconhecidas por grupos em $\mathbf{G}_p * \mathbf{Ab}^{p-1}$. Nesta secção daremos uma caracterização algébrica destas linguagens, a qual usa o conceito de produto modular concatenado já introduzido no capítulo anterior. Posteriormente obteremos uma caracterização das linguagens reconhecidas por grupos super-resolúveis finitos.

Um resultado dado em [2] por J. Almeida, S. Margolis, B. Steinberg e M. Volkov, o qual utiliza o produto de Mal'cev de pseudovariedades, permite obter uma demonstração alternativa do próximo teorema. No entanto, decidimos manter a demonstração inicial uma vez que a referência à nova demonstração foi apresentada após o nosso estudo estar terminado.

Teorema 4.1.1. *Seja L uma linguagem de A^*. As seguintes afirmações são equivalentes:*

(1) *L é reconhecida por um grupo em $\boldsymbol{G}_p * \boldsymbol{Ab}^{p-1}$;*

(2) *L é uma combinação Booleana de linguagens da forma $(L_0a_1\dots a_kL_k)_{r,p}$, em que cada L_i é uma linguagem comutativa $(p-1)$-elementar;*

(3) *L é uma combinação Booleana de linguagens da forma $(L_0a_1\dots a_kL_k)_{r,p}$, em que cada L_i é uma combinação Booleana de linguagens comutativas $(p-1)$-elementares.*

Demonstração. (2) $\Rightarrow$ (3) é trivial.

(3) $\Rightarrow$ (1). Cada combinação Booleana de linguagens comutativas $(p-1)$-elementares é, por (3.2), combinação Booleana de linguagens da forma $F(a,k,p-1)$ donde, pela Proposição 3.1.1, é reconhecida por um grupo em $\mathbf{Ab}^{p-1}$. Mais ainda, a Proposição 3.4.2 garante que, se cada linguagem L_i é reconhecida por um grupo G_i, então a linguagem $(L_0a_1L_1\dots a_kL_k)_{r,p}$ é reconhecida pelo grupo $G=\mathbb{Z}_p\Diamond_{k+1}(G_0,\dots,G_k)$.

Falta então provar que, se os grupos G_i estão em $\mathbf{Ab}^{p-1}$, então G está em $\mathbf{G}_p*\mathbf{Ab}^{p-1}$:

Seja $\pi: G\to G_0\times\cdots\times G_k$ o morfismo sobrejectivo que transforma cada matriz de G no produto dos elementos da sua diagonal, assim dado $m\in G$, $m\pi=m_{0,0}\dots m_{k,k}$. Mostremos que $\ker\pi$ é um p-grupo.

Se $m\in\ker\pi$ então $m_{i,j}=0$, para $i>j$, $m_{i,i}=(1,\dots,1)$ para $i=0,\dots,k$ e $m_{i,j}\in\mathbb{Z}_p[\{1\}\times\cdots\times\{1\}\times G_i\times\cdots\times G_j\times\{1\}\times\cdots\times\{1\}]$, para $i<j$.

Notemos que, para $i<j$, a entrada (i,j) da matriz m pode ser escrita como

$$m_{i,j}=\sum_{h\in G_i\times\cdots\times G_j}\lambda_h h,$$

para alguns $\lambda_h\in\mathbb{Z}_p$.

Assim existem exactamente $p^{|G_i|\dots|G_j|}$ elementos desta forma pelo que a ordem de $\ker\pi$ é uma potência de p. Portanto $\ker\pi\in\mathbf{G}_p$.

Pelo Teorema do Homomorfismo (1.8.17) tem-se

$$G_0\times\cdots\times G_k=G\pi\simeq\frac{G}{\ker\pi}$$

e, como $G_0,\dots,G_k\in\mathbf{Ab}^{p-1}$ obtemos $G_0\times\cdots\times G_k\in\mathbf{Ab}^{p-1}$, donde $G/\ker\pi\in\mathbf{Ab}^{p-1}$. Logo $G\in\mathbf{G}_p*\mathbf{Ab}^{p-1}$.

Portanto $(L_0a_1L_1\dots a_kL_k)_{r,p}$ é reconhecida por um grupo de $\mathbf{G}_p*\mathbf{Ab}^{p-1}$, pelo que pertence à variedade de linguagens $\mathcal{U}_p$. Mas, por hipótese, L é combinação Booleana de linguagens da forma $(L_0a_1L_1\dots a_kL_k)_{r,p}$, donde $L\in\mathcal{U}_p$, ou seja, é reconhecida por um grupo em $\mathbf{G}_p*\mathbf{Ab}^{p-1}$.

(1) $\Rightarrow$ (2). Com a notação do Corolário 3.3.5 aplicada à variedade de linguagens $\mathcal{U}_p$, é suficiente mostrar que as linguagens de $A^*\mathcal{A}b^{p-1}$ e as linguagens $V\sigma_\varphi^{-1}$ são da forma descrita em (2).

Seja $L \in A^*\mathcal{A}b^{p-1}$. Então L é reconhecida por um grupo em $\mathbf{Ab}^{p-1}$. Portanto, pela Proposição 3.1.2, L é união disjunta de linguagens comutativas $(p-1)$-elementares, mas estas são casos particulares de linguagens da forma $(L_0a_1L_1\ldots a_kL_k)_{r,p}$, em que só temos uma linguagem e $r=1$. Portanto L é combinação Booleana de linguagens da forma descrita em (2).

Consideremos agora as linguagens $V\sigma_\varphi^{-1}$, sendo $\sigma_\varphi : A^* \to B_G^*$ a função sequencial associada ao morfismo $\varphi : A^* \to G$, com $G \in \mathbf{Ab}^{p-1}$, e V uma linguagem de B_G^* reconhecida por um p-grupo.

Como σ_φ^{-1} comuta com as operações Booleanas, isto é, verifica para quaisquer $X, Y \subseteq B_G^*$,

$$\begin{aligned}(X\cup Y)\sigma_\varphi^{-1} &= (X\sigma_\varphi^{-1})\cup(Y\sigma_\varphi^{-1});\\ (X\cap Y)\sigma_\varphi^{-1} &= (X\sigma_\varphi^{-1})\cap(Y\sigma_\varphi^{-1});\\ (B_G^*\setminus X)\sigma_\varphi^{-1} &= A^*\setminus(X\sigma_\varphi^{-1}),\end{aligned}$$

pelo Teorema 3.2.1, basta provar que as linguagens da forma $V = S(u,r,p)$, com $0 \le r < p$ e $u \in B_G^*$, são tais que $V\sigma_\varphi^{-1}$ é do tipo descrito em (2).

Seja $u \in B_G^*$. Como $B_G = G\times A$, a palavra u é da forma $(g_1,c_1)\ldots(g_k,c_k)$, em que $g_1,\ldots,g_k \in G$, $c_1,\ldots,c_k \in A$. Portanto, $V = S(u,r,p)$ é o seguinte conjunto

$$\{v \in B_G^* : \mathrm{card}\{(v_0,\ldots,v_k) : v_0(g_1,c_1)v_1\ldots v_{k-1}(g_k,c_k)v_k = v\} \equiv r \pmod p\}$$

Vamos então calcular a linguagem $V\sigma_\varphi^{-1}$.

Dado $w = a_1\ldots a_n$, tem-se

$$w\sigma_\varphi = (1,a_1)(a_1\varphi,a_2)\ldots((a_1\ldots a_{n-1})\varphi,a_n),$$

donde, w pertence à linguagem $V\sigma_\varphi^{-1}$ se e só se

$$\mathrm{card}\{(v_0,\ldots,v_k) : v_0(g_1,c_1)v_1\ldots v_{k-1}(g_k,c_k)v_k = w\sigma_\varphi\} \equiv r \pmod p. \quad (4.1)$$

É nosso objectivo mostrar que

$$V\sigma_\varphi^{-1} = ((h_1\varphi^{-1})c_1(h_2\varphi^{-1})c_2\ldots(h_k\varphi^{-1})c_kA^*)_{r,p}, \quad (4.2)$$

em que $h_1 = g_1$, $h_2 = (g_1(c_1\varphi))^{-1}g_2,\ldots,h_k = (g_{k-1}(c_{k-1}\varphi))^{-1}g_k$.

Seja $w = a_1\ldots a_n$ tal que (4.1) se verifica. Então se

$$v_0(g_1,c_1)v_1\ldots v_{k-1}(g_k,c_k)v_k = (1,a_1)((a_1)\varphi,a_2)\ldots((a_1\ldots a_{n-1})\varphi,a_n),$$

para cada $j \in \{1,\ldots,k\}$ existe $i_j \in \{1,\ldots,k\}$ tal que

$$(g_j,c_j) = ((a_1\ldots a_{i_j-1})\varphi,a_{i_j}).$$

Tomando,

$$\begin{cases} u_0 = a_1 \dots a_{i_1-1} \\ u_1 = a_{i_1+1} \dots a_{i_2-1} \\ \vdots \\ u_{k-1} = a_{i_{k-1}+1} \dots a_{i_k-1} \\ u_k = a_{i_k+1} \dots a_n \end{cases}$$

tem-se $w = a_1 \dots a_n = u_0 c_1 u_1 c_2 \dots c_{k-1} u_{k-1} c_k u_k$.

Ora, $g_1 = (a_1 \dots a_{i_1-1})\varphi = u_0\varphi$ e, para cada $j \in \{1, \dots, k\}$, tem-se

$$\begin{aligned} (g_j(c_j\varphi))^{-1} g_{j+1} &= ((a_1 \dots a_{i_j-1})\varphi(a_{i_j}\varphi))^{-1}(a_1 \dots a_{i_{j+1}-1})\varphi \\ &= (a_{i_j+1} \dots a_{i_{j+1}-1})\varphi = u_j\varphi, \end{aligned}$$

portanto

$$\begin{cases} u_0 \in g_1\varphi^{-1} \\ u_1 \in ((g_1(c_1\varphi))^{-1} g_2)\varphi^{-1} \\ \vdots \\ u_{k-1} \in ((g_{k-1}(c_{k-1}\varphi))^{-1} g_k)\varphi^{-1} \\ u_k \in A^* \end{cases}$$

Conclui-se pois que $w \in ((h_1\varphi^{-1})c_1(h_2\varphi^{-1})c_2 \dots (h_k\varphi^{-1})c_k A^*)_{r,p}$, sendo os h_i da forma descrita atrás.

Reciprocamente suponhamos que $w = a_1 \dots a_n = u_0 c_1 u_1 \dots u_{k-1} c_k u_k$, em que

$$\begin{aligned} &u_0 \in g_i\varphi^{-1},\ u_k \in A^* \text{ e, para qualquer } j \in \{1, \dots, k-1\}, \\ &u_j \in ((g_j(c_j\varphi))^{-1} g_{j+1})\varphi^{-1}. \end{aligned} \tag{4.3}$$

Existem $i_j \in \{1, \dots, k\}$ tais que $c_j = a_{i_j}$, para cada $j \in \{1, \dots, k\}$. Mais ainda,

$$\begin{cases} u_0 = a_1 \dots a_{i_1-1} \\ u_1 = a_{i_1+1} \dots a_{i_2-1} \\ \vdots \\ u_{k-1} = a_{i_{k-1}+1} \dots a_{i_k-1} \\ u_k = a_{i_k+1} \dots a_n \end{cases}$$

Ora,

$$\begin{aligned} w\sigma_\varphi &= (1, a_1) \dots ((a_1 \dots a_{i_1-1})\varphi, a_{i_1}) \dots ((a_{i_1} \dots a_{i_k-1})\varphi, a_{i_k}) \dots \\ &\quad \dots ((a_1 \dots a_{n-1})\varphi, a_n). \end{aligned}$$

Por (4.3), concluímos que $u_0\varphi = g_1$ e

$$\begin{aligned} u_1\varphi &= (a_{i_1+1} \dots a_{i_2-1})\varphi = (g_1(c_1\varphi))^{-1} g_2 = ((a_1 \dots a_{i_1-1})\varphi(a_{i_1}\varphi))^{-1} g_2 \\ &= ((a_1 \dots a_{i_1-1} a_{i_1})\varphi)^{-1} g_2 = ((a_1 \dots a_{i_1})\varphi)^{-1} g_2, \end{aligned}$$

portanto $(a_{i_1+1} \dots a_{i_2-1})\varphi = ((a_1 \dots a_{i_1})\varphi)^{-1} g_2$, donde $g_2 = (a_1 \dots a_{i_2-1})\varphi$.

Por um argumento recursivo concluímos que, para cada $j \in \{1, \dots, k\}$, $g_j = (a_1 \dots a_{i_j-1})\varphi$. Logo tem-se (4.2). Como $\varphi : A^* \to G$ é um morfismo e, para qualquer $i \in \{1, \dots, k\}$, $\{h_i\} \subseteq G$ temos $L_i = h_i\varphi^{-1}$ reconhecida por G, um grupo de $\mathbf{Ab}^{p-1}$. Da Proposição 3.1.2 resulta que, para todo o $i \in \{1, \dots, k\}$, a linguagem $h_i\varphi^{-1}$ de A^* é união disjunta de linguagens comutativas $(p-1)$-elementares.

Suponhamos agora que, para cada $i \in \{1, \dots, k\}$, a linguagem $h_i\varphi^{-1} = L_i$ é união disjunta de $L_{i,1}, \dots, L_{i,\ell_i}$, em que $\ell_i \in \mathbb{N}$.

Pela Proposição 3.4.3, aplicada k vezes, obtém-se que o produto modular

$$V\sigma_\varphi^{-1} = (L_1 c_1 L_2 c_2 \dots c_{k-1} L_k c_k A^*)_{r,p}$$

é uma união de intersecções, logo é combinação Booleana, de linguagens da forma

$$(L_{1,j_1} c_1 L_{2,j_2} c_2 \dots c_{k-1} L_{k,j_k} c_k A^*)_{s,p},$$

em que $1 \leq j_i \leq \ell_i$ para $i \in \{1, \dots, k\}$ e $0 \leq s \leq p$ e, neste caso, as linguagens L_{i,j_i} já são linguagens comutativas $(p-1)$-elementares. □

O corolário seguinte dá-nos uma caracterização das linguagens reconhecidas pelos grupos de $\mathbf{G}_p * \mathbf{Ab}^{p-1}$.

Corolário 4.1.2. *Para todo o alfabeto finito A, o conjunto $A^*\mathcal{U}_p$ é a álgebra de Boole gerada pelas linguagens da forma $(L_0 a_1 L_1 \dots a_k L_k)_{r,p}$, sendo cada L_i uma linguagem comutativa $(p-1)$-elementar de A^*.*

Demonstração. Resulta da aplicação directa dos Teoremas 1.6.1 e 4.1.1. □

Podemos agora enunciar uma descrição das linguagens reconhecidas por grupos super-resolúveis finitos.

Corolário 4.1.3. *Para cada alfabeto finito A, o conjunto $A^*\mathcal{U}$ é a álgebra de Boole gerada pelas linguagens da forma $(L_0 a_1 L_1 \dots a_k L_k)_{r,p}$, sendo cada L_i uma linguagem comutativa $(p-1)$-elementar de A^*, para cada número primo p.*

Demonstração. Pela fórmula (3.1) tem-se, para cada alfabeto finito A,

$$A^*\mathcal{U} = A^* \left(\bigvee_{p \in \mathbb{P}} \mathcal{U}_p \right).$$

No início do Capítulo 3 referimos que $A^* \left(\bigvee_{p \in \mathbb{P}} \mathcal{U}_p \right)$ é a álgebra de Boole gerada pelas linguagens de $\bigcup_{p \in \mathbb{P}} A^*\mathcal{U}_p$. Portanto, pelo Corolário 4.1.2, temos o pretendido. □

4.2 Transdutores e linguagens reconhecidas por grupos super-resolúveis

Nesta secção será apresentada outra descrição das linguagens reconhecidas pelos grupos super-resolúveis.

Seja $\mathcal{T} = (Q, A, \mathbb{Z}_p, E, I, F)$ um transdutor com saídas em $\mathbb{Z}_p$. Diz-se que $\mathcal{T}$ está na *forma triangular estrita* se $Q = \{1, \ldots, n\}$, 1 é o único estado inicial, n é o único estado final e as suas transições satisfazem as três condições seguintes:

(1) não existe nenhuma transição de p para q tal que $p > q$;

(2) para $p < q$ e para cada letra $a \in A$, existe, quando muito, uma transição de p para q de etiqueta a;

(3) para cada letra $a \in A$ e para cada estado $q \in Q$, existe exactamente uma transição da forma $q \xrightarrow{a|r} q$, para algum $r \in \mathcal{U}(\mathbb{Z}_p)$.

Por exemplo, se considerarmos para alfabeto de entradas o conjunto $A = \{a, b\}$ e para conjunto de saídas o corpo $\mathbb{Z}_3$, o seguinte transdutor está na forma triangular estrita:

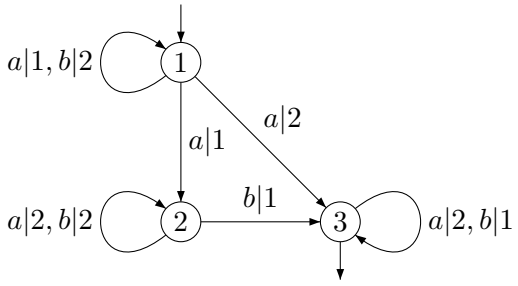


Figura 4.1: Um transdutor na forma triangular estrita

Do mesmo modo que foi dito no Capítulo 1, se τ é a transdução realizada pelo transdutor da figura 4.1, existem 5 caminhos bem sucedidos de etiqueta $aaba$, nomeadamente

$$(1)\ 1 \xrightarrow{a|1} 1 \xrightarrow{a|1} 1 \xrightarrow{b|2} 1 \xrightarrow{a|2} 3 \quad (2)\ 1 \xrightarrow{a|1} 1 \xrightarrow{a|2} 3 \xrightarrow{b|1} 3 \xrightarrow{a|2} 3$$

$$(3)\ 1 \xrightarrow{a|2} 3 \xrightarrow{a|2} 3 \xrightarrow{b|1} 3 \xrightarrow{a|2} 3 \quad (4)\ 1 \xrightarrow{a|1} 1 \xrightarrow{a|1} 2 \xrightarrow{b|1} 3 \xrightarrow{a|2} 3$$

$$(5)\ 1 \xrightarrow{a|1} 2 \xrightarrow{a|2} 2 \xrightarrow{b|1} 3 \xrightarrow{a|2} 3$$

A saída do primeiro caminho é $1 \times 1 \times 2 \times 2 \equiv 1 \pmod 3$ e as saídas dos restantes caminhos são, respectivamente, $1, 2, 2, 1$. Tem-se então $(aaba)\tau = 1 + 1 + 2 + 2 + 1 \equiv 1 \pmod 3$.

A cada transdutor na forma triangular estrita está associado um morfismo $\mu : A^* \to B_n(\mathbb{Z}_p)$, que designamos por *representação linear*, definido da seguinte forma:

Para cada letra $a \in A$, a entrada (p, q) da matriz $a\mu \in B_n(\mathbb{Z}_p)$ é dada por

$$a\mu_{p,q} = \begin{cases} 0 & \text{se não existe uma transição de } p \text{ para } q \text{ de etiqueta } a \\ r & \text{se } p \xrightarrow{a|r} q \text{ é a única transição de } p \text{ para } q \text{ de etiqueta } a \end{cases}$$

Observe-se que μ assim definida é, de facto, uma aplicação tendo em conta a definição de transdutor na forma triangular estrita. O facto de ser um morfismo resulta da propriedade universal dos monóides livres.

No exemplo anterior, obtém-se

$$a\mu = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}, b\mu = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}, (aaba)\mu = \begin{bmatrix} 2 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{bmatrix}.$$

Note-se que $(aaba)\tau = 1 = a\mu_{1,3}$. Não se trata de uma coincidência. De facto a representação linear dá-nos uma forma fácil de calcular a função realizada pelo transdutor, pois tem-se $u\tau = u\mu_{1,n}$. Para mais pormenores ver [6].

Reciprocamente, dado um morfismo $\mu : A^* \to B_n(\mathbb{Z}_p)$ é claro como se define um transdutor $\mathcal{T} = (\{1, \ldots, n\}, A, \mathbb{Z}_p, E, 1, \{n\})$ na forma triangular estrita. Associado ao trandutor $\mathcal{T}$ temos a função $\tau : A^* \to \mathbb{Z}_p$ realizada por $\mathcal{T}$ que é tal que $u\tau = u\mu_{1,n}$, para qualquer $u \in A^*$.

Recordemos que denotamos por $\mathcal{U}_p$ a variedade de linguagens associada à pseudovariedade de grupos $\mathbf{G}_p * \mathbf{Ab}^{p-1}$, isto é, para cada alfabeto finito A, denotamos por $A^*\mathcal{U}_p$ a classe das linguagens de A^* reconhecidas pelos grupos de $\mathbf{G}_p * \mathbf{Ab}^{p-1}$.

Lema 4.2.1. *Sejam p um número primo e A um alfabeto finito. Então $L \in A^*\mathcal{U}_p$ se e só se L é reconhecida por um subgrupo standard de Borel $B_n(\mathbb{Z}_p)$, para algum $n \in \mathbb{N}$.*

Demonstração. Se $L \in A^*\mathcal{U}_p$, então L é reconhecida por um grupo $G \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$, isto é, existem um morfismo $\varphi : A^* \to G$ e um conjunto $X \subseteq G$ tais que $L = X\varphi^{-1}$. Pelo Teorema 2.4.4, sabemos que $G \lesssim B_n(\mathbb{Z}_p)$, para algum $n \in \mathbb{N}$, logo existe um monomorfismo $\theta : G \to B_n(\mathbb{Z}_p)$. Portanto $X\theta \subseteq B_n(\mathbb{Z}_p)$ e $\varphi\theta$ é um morfismo de A^* em $B_n(\mathbb{Z}_p)$ tal que $(X\theta)(\varphi\theta)^{-1} = X\varphi^{-1} = L$, donde L é reconhecida por $B_n(\mathbb{Z}_p)$.

Reciprocamente, se L é reconhecida por um subgrupo standard de Borel $B_n(\mathbb{Z}_p)$ e uma vez que, pela demonstração do Teorema 2.4.4, se tem $B_n(\mathbb{Z}_p) \in \mathbf{G}_p * \mathbf{Ab}^{p-1}$, concluímos que $L \in A^*\mathcal{U}_p$. □

Estamos agora em condições de dar a última caracterização da variedade de linguagens $\mathcal{U}_p$.

Teorema 4.2.2. *Seja A um alfabeto finito. Uma linguagem pertence a $A^*\mathcal{U}_p$ se e só se é uma combinação Booleana de linguagens da forma $r\tau^{-1}$, em que $r \in \mathbb{Z}_p$ e $\tau : A^* \to \mathbb{Z}_p$ é uma função realizada por algum transdutor na forma triangular estrita.*

Demonstração. Sejam A um alfabeto finito e $\mathcal{B}$ a álgebra de Boole gerada pelas linguagens da forma $r\tau^{-1}$, em que $r \in \mathbb{Z}_p$ e $\tau : A^* \to \mathbb{Z}_p$ é uma função realizada por algum transdutor na forma triangular estrita. É nosso objectivo mostrar que

$$\mathcal{B} = A^*\mathcal{U}_p.$$

Consideremos uma função $\tau : A^* \to \mathbb{Z}_p$ realizada por um transdutor na forma triangular estrita. Seja $\mu : A^* \to B_n(\mathbb{Z}_p)$ a sua representação linear. Tomemos $r \in \mathbb{Z}_p$ e mostremos que a linguagem $r\tau^{-1}$ é reconhecida por $B_n(\mathbb{Z}_p)$.

Seja $R = \{m \in B_n(\mathbb{Z}_p) : m_{1,n} = r\} \subseteq B_n(\mathbb{Z}_p)$. Tem-se

$$u \in r\tau^{-1} \Leftrightarrow u\mu_{1,n} = r \Leftrightarrow u\mu \in R \Leftrightarrow u \in R\mu^{-1}.$$

Portanto $r\tau^{-1} = R\mu^{-1}$, em que $\mu : A^* \to B_n(\mathbb{Z}_p)$ é um morfismo e $R \subseteq B_n(\mathbb{Z}_p)$, pelo que a linguagem $r\tau^{-1}$ é reconhecida pelo grupo $B_n(\mathbb{Z}_p)$. Mas, na demonstração do Teorema 2.4.4, vimos que os subgrupos standard de Borel $B_n(\mathbb{Z}_p)$ são elementos da pseudovariedade de grupos $\mathbf{G}_p * \mathbf{Ab}^{p-1}$, pelo que a linguagem $r\tau^{-1}$ pertence a $A^*\mathcal{U}_p$.

Como, por definição de variedade de linguagens, $A^*\mathcal{U}_p$ é uma álgebra de Boole, tem-se $\mathcal{B} \subseteq A^*\mathcal{U}_p$.

Provemos agora que $A^*\mathcal{U}_p \subseteq \mathcal{B}$. Tome-se $L \in A^*\mathcal{U}_p$. Pelo Lema 4.2.1, L é reconhecida por um subgrupo standard de Borel $B_n(\mathbb{Z}_p)$, para algum $n \in \mathbb{N}$, logo existem um morfismo $\eta : A^* \to B_n(\mathbb{Z}_p)$ e um subconjunto $P \subseteq B_n(\mathbb{Z}_p)$ tais que $L = P\eta^{-1}$. Queremos mostrar que $L \in \mathcal{B}$. Ora,

$$L = P\eta^{-1} = \bigcup_{m \in P} m\eta^{-1},$$

pelo que basta demonstrar que, para cada $m \in P \subseteq B_n(\mathbb{Z}_p)$, temos $m\eta^{-1} \in \mathcal{B}$.

É claro que

$$m\eta^{-1} = \bigcap_{1 \leq i,j \leq n} L^m_{i,j},$$

em que $L^m_{i,j} = \{u \in A^* : u\eta_{i,j} = m_{i,j}\}$.

Fixemos $i, j \in \{1, \ldots, n\}$ e tomemos $t = j - i + 1$. Seja $\mu^{i,j} : A^* \to B_t(\mathbb{Z}_p)$ o morfismo definido por, dado $a \in A$,

$$a\mu^{i,j}_{k,\ell} = a\mu_{i+k-1,i+\ell-1}, \qquad \text{para } 1 \leq k, \ell \leq t.$$

Note-se que $a\mu_{k,\ell}^{i,j}$ é a submatriz de $a\eta$ cujo elemento do lado superior direito é $a\mu_{1,t}^{i,j} = a\eta_{i,j}$ e o elemento do lado inferior esquerdo é $a\mu_{t,1}^{i,j} = a\eta_{j,i}$, pelo que concluímos que, para todo o $u \in A^*$, se tem $u\mu_{1,t}^{i,j} = u\eta_{i,j}$.

Tomando $m_{i,j} = r$, obtemos

$$u \in L_{i,j}^m \Leftrightarrow u\eta_{i,j} = m_{i,j} \Leftrightarrow u\eta_{i,j} = r \Leftrightarrow u\mu_{1,t}^{i,j} = r,$$

portanto $L_{i,j}^m = r\tau_{i,j}^{-1}$, em que $\tau_{i,j}$ é a função realizada pelo transdutor na forma triangular estrita definido por $\mu^{i,j}$.

Tem-se então

$$L = \bigcup_{m \in P} \bigcap_{1 \leq i,j \leq n} L_{i,j}^m,$$

sendo as linguagens $L_{i,j}^m$ da forma descrita atrás. Além disso, vimos que, para cada $m \in P$ e cada $(i,j) \in \{1,\ldots,n\}^2$, temos $L_{i,j}^m = r\tau_{i,j}^{-1}$, em que $r \in \mathbb{Z}_p$ e $\tau_{i,j}$ é a função realizada pelo transdutor na forma triangular estrita definido por $\mu^{i,j}$. Portanto L é combinação Booleana de linguagens da forma pretendida, pelo que $L \in \mathcal{B}$. Concluímos que se tem a igualdade $\mathcal{B} = A^*\mathcal{U}_p$ e o teorema segue-se. □

Por fim podemos caracterizar as linguagens reconhecidas pelos grupos finitos super-resolúveis. Recordemos que denotamos por $\mathcal{U}$ a variedade de linguagens associada à pseudovariedade **Su** dos grupos super-resolúveis, isto é, para cada alfabeto finito A, denotamos por $A^*\mathcal{U}$ a classe das linguagens de A^* reconhecidas pelos grupos super-resolúveis finitos.

Corolário 4.2.3. *Seja A um alfabeto finito. Uma linguagem pertence a $A^*\mathcal{U}$ se e só se é uma combinação Booleana de linguagens da forma $r\tau^{-1}$, em que p é um número primo, $r \in \mathbb{Z}_p$ e $\tau : A^* \to \mathbb{Z}_p$ é uma função realizada por algum transdutor na forma triangular estrita.*

Demonstração. Pela fórmula (3.1) tem-se, para cada alfabeto finito A,

$$A^*\mathcal{U} = A^* \left(\bigvee_{p \in \mathbb{P}} \mathcal{U}_p \right).$$

No início do Capítulo 3, referimos que $A^* \left(\bigvee_{p \in \mathbb{P}} \mathcal{U}_p \right)$ é a álgebra de Boole gerada pelas linguagens de $\bigcup_{p \in \mathbb{P}} A^*\mathcal{U}_p$. Portanto, pelo Teorema 4.2.2, tem-se o pretendido. □

Bibliografia

[1] J. Almeida, *Finite Semigroups and Universal Algebra*, series in Algebra, volume 3, World Scientific.

[2] J. Almeida, S. W. Margolis, B. Steinberg e M. V. Volkov, *Representation Theory of Finite Semigroups, Semigroup Radicals and Formal Language Theory*, ArXiv Mathmatics E-Prints, Fev. 2007.

[3] J. Almeida, S. W. Margolis e M. V. Volkov, *The pseudovariety of semigroups of triangular matrices over a finite field*, Theor. Inform. Appl. 39,**1** (2005), 31-48.

[4] J. L. Alperin e R. B. Bell, *Groups and Representations*, Graduate Texts in Mathematics, vol 162, Springer, Berlin, 1995.

[5] K. Auinger e B. Steinberg, *Varieties of finite supersolvable groups with the M. Hall property*, Math. Ann. 335,**4** (2006), 853-877.

[6] J. Berstel, *Transductions and Context-Free Languages*, Teubner, 1979.

[7] M. Branco, Notas da disciplina *Elementos de Teoria da Computação*, DM, FCUL, 2006-2007.

[8] O. J. Brison, *Grupos e Representações*, Colecção Textos de Matemática do departamento de Matemática da FCUL, volume 12, 1ª Edição, 1999.

[9] O. Carton, J.-E. Pin e X. S.-Escrivà, *Languages recognized by finite supersoluble groups*, preprint.

[10] J. P. Dias da Silva, Notas da disciplina *Grupos e Representações*, DM, FCUL, 2006-2007.

[11] K. Doerk e T. Hawkes, *Finite Soluble Groups, de Gruyter Expositions in Mathematics*, vol. 4, Walter de Gruyter & Co., Berlin, 1992.

[12] S. Eilenberg, *Automata, Languages and Machines*, Vol. B, Academic Press [Harcourt Brace Jovanovich Publishers] New York, 1976. Pure and Applied Mathematica, vol. 59.

[13] P. J. Freitas, *Tópicos de Álgebra Superior*, Colecção Textos de Matemática do departamento de Matemática da FCUL, volume 19, 1ª Edição, 2005.

[14] D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968.

[15] M. Hall, *The Theory of Groups*, The Macmillan Co., New York, N. Y. 1959.

[16] J. M. Howie, *Automata and Languages*, Oxford Science Publications, 1991.

[17] R. McNaughton, *Algebraic decision procedures for local testability*, Math. Systems Theory **8** (1974) 60-76.

[18] A. J. Monteiro e I. T. Matos, *Álgebra, um primeiro curso*, Escolar Editora, 2ª Edição, 2001.

[19] H. Neumann, *Varieties of Groups*, Springer, Berlin Heidelberg New York, 1967.

[20] J.-E. Pin, *Varieties of Formal Languages*, North Oxford Academic, 1986.

[21] J.-E. Pin e P. Weil, *The wreath product principle for ordered semigroups*, Communications in Algebra 30 (2002), 5677-5713.

[22] M.-P. Schützenberger, *On finite monoids having only trivial subgroups*, Inform. and Control **8** (1965) 190-194.

[23] H. Straubing, *The wreath product and its applications*, in Formal properties of finite automata and applications (Ramatuelle, 1988), pp. 15-24, Lecture notes in Comput. Sci. vol 386, Springer, Berlin, 1989.

[24] P. Weil, *An extension of the Schützenberger product*, in Lattices, semigroups, and universal algebra (Lisbon, 1988), Plenum, New York, 1990.

[25] P. Weil, *Products of languages with counter*, Theoret. Comput. Sci. 76 (1990), 251-260.

Notações

Este índice está ordenado pelo número de página onde o símbolo surge pela primeira vez.

$\ker \varphi$	equivalência nuclear associada à aplicação φ, 7
$\|G\|$	ordem de G, 8
$H \leq G$	H é um subgrupo de G, 8
$H < G$	H é um subgrupo próprio de G, 8
$S \times T$	produto directo (externo) de S e T, 9
$S \rtimes T$	produto semidirecto externo de S e T, 10
S/ρ	conjunto quociente, 10
$\equiv_n$	congruência aritmética, 10
$a \equiv b \pmod{n}$	n divide $a - b$, 10
$\mathbb{Z}_n$	anel dos inteiros módulo n, 10
$\rho^\natural$	morfismo natural associado a uma congruência ρ, 10
$S \mid T$	S divide T, 11
A^+	o semigrupo livre sobre o conjunto A, 11
A^*	o monóide livre sobre o conjunto A, 12
$\|\omega\|$	comprimento de ω, 12
$\|\omega\|_a$	número de ocorrências de a em ω, 13
$\mathcal{A}$	um autómato, 13
$p \xrightarrow{a} q$	uma transição de um autómato, 13
$L(\mathcal{A})$	a linguagem reconhecida pelo autómato $\mathcal{A}$, 14
RacA^*	o conjunto das linguagens racionais de A^*, 16
σ_L	a congruência sintáctica de uma linguagem L, 17
Syn(L)	o monóide sintáctico de uma linguagem L, 17
$\mathcal{T}(Q)$	conjunto das aplicações de Q em Q, 18
(Q, S)	um monóide de transformações, 18
S^Q	conjunto das aplicações de Q em S, 18
$(P, S) \circ (Q, T)$	produto em coroa de monóides de transformações, 19
$S \circ T$	produto em coroa de monóides, 19
$\mathbf{V}$	uma pseudovariedade, 20
$\mathbf{V}\,\langle M_j : j \in J\rangle$	a pseudovariedade gerada pela família de monóides

	$(M_j)_{j\in J}$, 21
$\mathbf{V}\,[u_n = v_n\,(n \geq 1)]$	a pseudovariedade definida pelas identidades $u_n = v_n$, 21
$\mathbf{V}\,[\![u_n = v_n\,(n \geq 1)]\!]$	a pseudovariedade ultimamente definida pelas identidades $u_n = v_n$, 21
$A^*\mathcal{V}$	conjunto das linguagens de A^* cujo monóide sintáctico está em $\mathbf{V}$, 22
$u^{-1}X$	residual esquerdo de X por u, 22
$H <\cdot G$	H é um subgrupo maximal de G, 25
$H \cdot\leq G$	H é um subgrupo minimal de G, 25
$\|x\|$	ordem do elemento x, 25
$\langle S\rangle$	subgrupo gerado por S, 25
$\exp(G)$	expoente de G, 26
$[x, y] = x^{-1}y^{-1}xy$	comutador de x e y, 26
G'	subgrupo derivado de G, 26
$Z(G)$	centro de G, 26
Ha	classe lateral direita, 26
aH	classe lateral esquerda, 26
$[G : H]$	índice de H em G, 26
$N \trianglelefteq G$	H é um subgrupo normal de G, 27
$N \lhd G$	H é um subgrupo normal próprio de G, 27
$H \lhd\cdot G$	H é um subgrupo normal maximal de G, 27
$H \cdot\trianglelefteq G$	H é um subgrupo normal minimal de G, 27
G/H	grupo quociente de G por H, 27
$Aut(G)$	grupo dos automorfismos de G, 28
$Inn(G)$	grupo dos automorfismos interiores de G, 28
$N\ char\ G$	N é subgrupo característico de G, 29
$\ker\varphi$	kernel de um morfismo, 29
$G\varphi = im\varphi$	imagem de G por φ, 29
$G \lesssim H$	G mergulha-se em H, 29
$M \dot{\times} N$	produto directo interno de M e N, 30
$\prod_{i=1}^{m}{}^{\cdot} N_i$	produto directo interno de $N_1, \ldots, N_m$, 30
$\mathrm{Syl}_p(G)$	conjunto dos subgrupos de Sylow de G, 31
$O_p(G)$	$\bigcap_{P\in\mathrm{Syl}_p(G)} P$, 31
$H \rtimes G$,$H \overset{\alpha}{\rtimes} G$	produto semidirecto de H por G, 33
$H \circ G$	produto em coroa H por G, 34
$\Phi(G)$	subgrupo de Frattini de G, 35
$G/\Phi(G)$	quociente de Frattini, 35
$\mathcal{U}(A)$	grupo das unidades de A, 36
$U \oplus W$	soma directa de U e W, 38
$End_K(V)$	álgebra-K das aplicações lineares de V em V sobre K, 39

$GL(V)$	grupo dos automorfismos de V sobre K, 39
$M_n(K)$	álgebra-K das matrizes $n \times n$ sobre K, 39
$Gl_n(K)$	grupo das matrizes $n \times n$ invertíveis sobre K, 39
$Aut_K(V)$	$GL(V)$, 39
$Aut(V)$	$GL(V)$, 39
$\ker \tau$	kernel de um morfismo de álgebras-K, 40
$K[G]$	álgebra de grupo, 40
$K[S]$	álgebra de monóide, 41
$C_V(O_p(G))$	$\{v \in V : vx = v, \forall x \in O_p(G)\}$, 44
$K[t]$	anel de polinómios em t com coeficientes em K, 44
$a \vee b$	supremo de a e b, 24
$a \wedge b$	ínfimo de a e b, 24
$\mathcal{T}$	transdutor, 44
$p \xrightarrow{a\|r} q$	uma transição de um transdutor, 45
$\bigvee_{i\in I} \mathbf{H}_i$	supremo da família $(\mathbf{H}_i)_{i\in I}$ de pseudovariedades de grupos, 49
$\mathbf{G}_p$	pseudovariedade dos p-grupos, 50
$\mathbf{H}_{p'}$	pseudovariedade dos grupos em $\mathbf{H}$ cuja ordem não é divisível por p, 50
$\mathbf{Ab}$	pseudovariedade dos grupos abelianos, 50
$\mathbf{S}$	pseudovariedade dos grupos resolúveis, 50
$\mathbf{N}$	pseudovariedade dos grupos nilpotentes, 50
$\mathbf{Ab}^n$	pseudovariedade dos grupos abelianos cujo expoente divide n, 50
$\mathbf{U} * \mathbf{V}$	pseudovariedade produto, 50
$B_n(K)$	subgrupo standard de Borel, 72
$U_n(K)$	grupo das matrizes unitriangulares de $B_n(K)$, 72
$\bigvee_{i\in I} \mathcal{H}_i$	supremo da família $(\mathcal{H}_i)_{i\in I}$ de variedades de linguagens, 91
$F(r_1, \ldots, r_s, n)$	linguagem comutativa n-elementar, 93
$\binom{w}{u}$	coeficiente binomial, 58
$\mathcal{T}_\varphi$	transdutor sequencial de um morfismo, 98
$(L_1 a_1 L_2 \ldots a_{k-1} L_k)_{r,p}$	produto modular concatenado, 102
$\mathbb{Z}_p \Diamond_k (G_1, \ldots, G_k)$	produto de Schützenberger sobre $\mathbb{Z}_p$ dos grupos $G_1, \ldots, G_k$, 103

Índice