Alfredo Manuel Gouveia da Costa

Relações entre a dinâmica de operadores implícitos e a estrutura de grupos finitos

Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
Março / 2003

Alfredo Manuel Gouveia da Costa

Relações entre a dinâmica de operadores implícitos e a estrutura de grupos finitos

Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
Março / 2003

Alfredo Manuel Gouveia da Costa

Relações entre a dinâmica de operadores implícitos e a estrutura de grupos finitos

Tese submetida à Faculdade de Ciências da Universidade do Porto
para obtenção do grau de Mestre em Matemática / Fundamentos e Aplicações

Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
Março / 2003

Resumo

Um operador implícito n-ário sobre uma pseudovariedade V é um n-uplo de operações implícitas n-árias sobre V. A interpretação de um operador implícito numa álgebra pró-V é a transformação n-ária cujas componentes são as interpretações das operações implícitas que definem esse operador.

Abordamos dois temas envolvendo a relação entre a dinâmica de operadores implícitos e a estrutura de grupos finitos. O primeiro desses temas debruça-se sobre operadores implícitos invertíveis; neste caso somos levados a um estudo prévio de algumas propriedades aritméticas do limite projectivo dos anéis dos restos módulo um número natural, o qual é um anel onde o anel dos inteiros está mergulhado. Por exemplo, mostramos que um elemento desse limite projectivo é invertível se e só se não for divisível por nenhum primo inteiro.

O segundo tema incide sobre os comutadores de Engel. A primeira componente da n-ésima iteração do operador $([x,y],y)$ é um comutador de Engel. Uma questão que acaba por revelar-se importante reside na escolha de uma definição para o comutador $[x,y]$ entre as opções $xyx^{-1}y^{-1}$ e $x^{-1}y^{-1}xy$. Se adoptarmos a primeira opção então os grupos finitos onde o operador $([x,y],y)$ é aperiódico são precisamente os grupos nilpotentes finitos. Se adoptarmos a segunda definição então encontramos exemplos de grupos finitos não nilpotentes onde $([x,y],y)$ é aperiódico (por exemplo, o grupo simétrico em três letras); mostramos que esses grupos são divisíveis pelo grupo simétrico em três letras. Entre outras questões relacionadas com o comportamento dinâmico do operador $([x,y],y)$, destacamos o estudo dos grupos diedrais.

Abstract

An n-ary implicit operator over a pseudovariety V is an n-tuple of n-ary implicit operations over V. The interpretation of an implicit operator on a pro-V algebra is an n-ary transformation whose components are the interpretations of the implicit operations which define that operator.

We study two subjects concerning the relationship between the dynamics of implicit operators and the structure of finite groups. The first of those subjects concerns invertible implicit operators; in this case we first study some arithmetical properties of the projective limit of the rings of integers modulo a natural number, which is a ring where the ring of the integers is embedded. For instance, we prove that an element of that projective limit is invertible if and only if it is not divisible by any prime integer.

The second subject falls upon Engel commutators. The first component of the n-th iterate of the operator $([x,y],y)$ is an Engel commutator. A question that becomes important is that of the choice of definition for the commutator $[x,y]$ between the two options $xyx^{-1}y^{-1}$ and $x^{-1}y^{-1}xy$. If we adopt the first one then the finite groups in which the operator $([x,y],y)$ is aperiodic are precisely the finite nilpotent groups. If instead we adopt the second definition then we find some examples of finite groups that are not nilpotent and where the operator $([x,y],y)$ is aperiodic (for example, the symmetric group on three letters); we show that such groups are divisible by the symmetric group on three letters. Among other questions related with the dynamical behavor of the operator $([x,y],y)$, deserves special mention our study of dihedral groups.

Résumé

Un opérateur implicite n-aire sur une pseudovariété V est un n-uple de opérations implicites n-aires sur V. L'interprétation d'un opérateur implicite dans une algèbre pro-V est la transformation n-aire dont les composantes sont des interprétations des opérations implicites qui le définissent.

Nous voulons approcher deux thèmes concernant la relation entre la dynamique des opérateurs implicites et la structure des groupes finis. Le premier de ceux thèmes s'occupe des opérateurs implicites invertibles; dans ce cas nous sommes emportés a une étude préliminaire de quelques propriétés arithmétiques du limite projectif des anneaux des restes module un nombre naturel, qui est un anneau où l'anneau des entiers est plongé. Par exemple, on prouve qu'un élément du limite projectif est invertible si et seulement s'il n'est pas divisible par aucun premier entier.

Le second sujet s'occupe des commutateurs d'Engel. La première composante de la n-ième itération de l'opérateur $([x, y], y)$ est un commutateur d'Engel. Une question importante dans ce sujet est celle qui se rapporte à la définition du commutateur $[x, y]$ entre les options $xyx^{-1}y^{-1}$ et $x^{-1}y^{-1}xy$. Si on adopte la première option alors les groupes finis dont l'opérateur $([x, y], y)$ est apériodique sont précisément les groupes nilpotents finis. Si on adopte la deuxième option alors on trouve des groupes finis non nilpotents où $([x, y], y)$ est apériodique (par exemple, le groupe symétrique en trois lettres); on montre que ces groupes sont divisibles par le groupe symétrique en trois lettres. Parmi d'autres questions rapportées avec le comportement dynamique de l'opérateur $([x, y], y)$, nous détachons l'étude des groupes diédraux.

Aos meus Pais

Agradecimentos

Gostaria de agradecer ao Professor Jorge Almeida pela sua generosa disponibilidade, pelas suas sugestões e pelo seu estímulo. A todos aqueles que se interessaram pelo meu trabalho, o meu obrigado.

Índice

Introdução

A primeira motivação para este trabalho surgiu do artigo [16]. O ponto de partida de tal artigo é o conceito de *grafo de comutação* de um grupo. Dado um grupo G, o seu grafo de comutação é o grafo cujos vértices estão indexados pelos elementos de G diferentes de 1, e onde dois vértices $x, y \in G \setminus \{1\}$ estão unidos por uma aresta se e só se x e y comutam e são distintos. Dito de outro modo, dois vértices do grafo de comutação estão ligados por uma aresta se e só se estão na relação binária de comutação, na qual dois elementos estão relacionados se e só se comutam. Tal como nos é dito pelos seus autores, o grafo de comutação revelou-se um instrumento muito útil na resolução de alguns problemas que são referidos no início do artigo. B. Plotkin sugeriu que se generalizasse o conceito de grafo de comutação, nomeadamente considerando grafos orientados de nilpotência e de solubilidade. De acordo com esta proposta, escolhida uma relação binária $\mathcal{R}$ adequada à definição do grafo, dois elementos x e y de $G \setminus \{1\}$ ficam unidos por uma aresta orientada de x para y se e só se $x\mathcal{R}y$ e $x \neq y$. A orientação do grafo deve-se à possibilidade de $\mathcal{R}$ não ser simétrica.[1] O primeiro exemplo que aí nos é dado é o de um grafo de nilpotência construído à custa das *palavras* ou *comutadores de Engel*. Tais palavras generalizam o conceito de comutador. Se definirmos o comutador entre x e y como sendo

$$[x, y] = x^{-1}y^{-1}xy,$$

então os comutadores de Engel são os termos

$$v_1(x, y) = [x, y],\ v_2(x, y) = [v_1(x, y), y], \ldots, v_n(x, y) = [v_{n-1}(x, y), y], \ldots.$$

A relação $\mathcal{R}$ que consideramos neste caso é aquela em que dois elementos distintos x e y de $G \setminus \{1\}$ estão relacionados se e só se existe algum $n \in \mathbb{N}$ tal que $v_n(x, y) = 1$. Esta relação pode ser considerada como uma relação de nilpotência, quer pela forma como se definem os subgrupos da série central descendente, quer pelo Teorema de Zorn [35, 30], o qual nos diz que um grupo finito G é nilpotente se e só se existe algum $n \in \mathbb{N}$ para o qual a lei $v_n(x, y) = 1$ é válida em G. Isto quer dizer que um grupo finito é nilpotente se e só se o grafo associado à relação $\mathcal{R}$ tem diâmetro 1. Observemos que se $v_n(x, y) = 1$ então para m maior do que n também se verifica $v_m(x, y) = 1$.

[1] Os autores do artigo também mostram interesse pelo grafo não orientado subjacente, obtido pela retirada de orientação às arestas e pela indentificação de cada par de arestas múltiplas numa única aresta.

Para obter grafos de solubilidade com o máximo de paralelismos com o grafo de nilpotência que acabámos de definir, coloca-se naturalmente o problema de encontrar uma sequência de palavras $(w_n(x,y))_{n\in\mathbb{N}}$ em duas variáveis x e y tal que se $w_n(x,y)=1$ então para m maior do que n também se verifica $w_m(x,y)=1$, e tal que um grupo finito G é solúvel se e só se existe algum $n\in\mathbb{N}$ para o qual a lei $w_n(x,y)=1$ é válida em G. B. Plotkin propôs três sequências que conjecturou que satisfizessem esta última condição. A mais simples dessas sequências define-se recursivamente do seguinte modo:

$$e_0(x,y)=[x,y],\ldots,e_n(x,y)=[[e_{n-1}(x,y),x],[e_{n-1}(x,y),y]],\ldots.$$

Notemos que a igualdade $e_n(x,y)=1$ é verificada se G tiver grau de solubilidade menor ou igual a $n+1$, e que ela de facto implica a igualdade $e_m(x,y)=1$ para $m\geq n$. Uma vez que um grupo satisfaz uma identidade com n variáveis se e só se todo o subgrupo gerado por n elementos satisfaz essa identidade, uma consequência imediata da validade da conjectura de B. Plotkin sobre a sequência $e_n(x,y)$, ou mais geralmente, da existência de uma sequência $(w_n(x,y))_{n\in\mathbb{N}}$ com as condições anteriormente mencionadas, é a de que um grupo finito é solúvel se e só se todo o subgrupo gerado por dois elementos é solúvel. Ora este é um dos mais importantes corolários da classificação realizada por J. Thompson dos grupos finitos simples cujos subgrupos próprios são solúveis [33]. A tarefa de classificação realizada por Thompson é bem conhecida pela sua extraordinária dificuldade e extensão (mais de 400 páginas). Uma demonstração independente de que um grupo finito é solúvel se e só se todo o subgrupo gerado por dois elementos é solúvel foi feita recentemente por P. Flavell [14]. Trata-se de uma demonstração de poucas páginas e elementar, no sentido em que não depende de nenhum resultado da ordem de complexidade do mencionado trabalho de Thompson. No entanto, nem Thompson nem Flavell nos deram leis em duas variáveis que permitam caracterizar os grupos solúveis finitos.

Em [16], o primeiro artigo que mencionámos, podemos encontrar várias referências a resultados anteriormente publicados que relacionam identidades em duas variáveis envolvendo os comutadores de Engel $v_n(x,y)$ e a estrutura de grupos finitos: se um grupo finito satisfaz uma identidade $v_1(x,y)=v_n(x,y)$, com $n>1$, então é Abeliano; se satisfaz uma identidade $v_2(x,y)=v_n(x,y)$, com $n>2$, então é solúvel; se satisfaz uma identidade $v_n(x,y)=v_{n+k}(x,y)$ com k ímpar então é solúvel. Estes resultados, bem como o Teorema de Zorn e a conjectura de Plotkin sobre a sequência de palavras $(e_n(x,y))_{n\in\mathbb{N}}$, podem ser vistos de um ponto de vista dinâmico. A própria definição dos termos $v_n(x,y)$ e $e_n(x,y)$ tem um carácter dinâmico. Se considerarmos o operador binário

$$\xi(x,y)=([x,y],y)$$

e o operador ternário

$$\psi(x,y,z)=([[x,y],[x,z]],y,z)$$

verificamos que $v_n(x,y)$ é a primeira componente de $\xi^n(x,y)$ e que $e_n(x,y)$ é a primeira componente de $\psi^n([x,y],x,y)$. Assim, o Teorema de Zorn estabelece uma relação entre a nilpotência ou não de um grupo finito e o tipo de órbita de ξ nesse grupo: os grupos

finitos nilpotentes são precisamente os grupos finitos em que todas as órbitas por ξ caem num ponto fixo cuja primeira coordenada é 1. Do mesmo modo, podemos dizer que a conjectura de Plotkin estabelece uma caracterização dos grupos solúveis finitos em termos do comportamento dinâmico de ψ: os grupos finitos solúveis são os grupos finitos onde as órbitas por ψ dos pontos $([x,y],x,y)$ caem no ponto fixo $(1,x,y)$. Esta perspectiva dinâmica desenvolveu-se no autor após a leitura dos artigos [3, 5, 2]. A sua leitura sensibilizou-o para o problema mais geral da relação entre certo tipo de operadores algébricos n-ários — os operadores implícitos n-ários — e a estrutura de grupos finitos. Pretende-se que esta relação seja feita ao nível das pseudovariedades de grupos finitos. Uma das razões para isto é que as classes dos grupos finitos com determinadas propriedades estruturais relevantes como a dos grupos Abelianos finitos, a dos grupos nilpotentes finitos e a dos grupos solúveis finitos são pseudovariedades, isto é, são classes fechadas para imagens homomorfas, produtos finitários e subgrupos dos seus elementos. Outra razão para fazermos o estudo ao nível das pseudovariedades é que assim podemos aproveitar a maquinaria da Álgebra Universal Finita, a qual tem o conceito de pseudovariedade como um dos mais fundamentais.

Esta monografia está organizada em quatro capítulos e um epílogo. Procurámos fazer um texto que fosse auto-contido nos resultados demonstrados.

O primeiro capítulo é dedicado à introdução de alguns tópicos preliminares sobre Álgebra Universal. A ênfase é posta nos conceitos de álgebra, termo, identidade, homomorfismo, variedade, pseudovariedade e álgebra livre.

No segundo capítulo são desenvolvidos alguns temas do domínio da Álgebra Universal Finita a partir do conceito de operação implícita. A exploração dos assuntos é feita tendo como horizonte o estudo que será realizado nos dois últimos capítulos acerca da relação entre algumas pseudovariedades de grupos finitos e a dinâmica de certos operadores implícitos. Ao longo do capítulo vão surgindo conceitos adequados ao estudo de pseudovariedades, conceitos esses que são paralelos a alguns dos que foram introduzidos no primeiro capítulo: os conceitos de operação implícita, álgebra pró-V e álgebra pró-V livre, em contraponto aos de termo, álgebra e álgebra livre. Na última secção deste capítulo preocupamo-nos em detalhar algumas das propriedades do grupo profinito livre monogénico, enquanto anel das operações implícitas unárias sobre a pseudovariedade dos grupos finitos.

O terceiro capítulo começa com um pequeno apontamento sobre comutadores, prossegue com a recapitulação de algumas definições e resultados bem conhecidos da Teoria dos Grupos, e termina com uma secção sobre operadores implícitos invertíveis, com destaque para aqueles que são invertíveis na pseudovariedade dos grupos nilpotentes finitos.

O quarto e último capítulo é dedicado ao estudo de igualdades envolvendo os comutadores de Engel, numa perspectiva dinâmica. Aí mostramos que se um grupo não nilpotente satisfaz para algum $n \in \mathbb{N}$ a igualdade $v_n(x,y) = v_{n+1}(x,y)$ então é divisível por S_3; julgamos que este resultado é original. Um dos objectivos deste capítulo é o

estudo das implicações da mudança da definição de comutador entre dois elementos x e y (de $x^{-1}y^{-1}xy$ para $xyx^{-1}y^{-1}$) nas questões relacionadas com os operadores de Engel.

O desenvolvimento de cada um dos capítulos é precedido por uma introdução mais detalhada, onde são mencionadas as referências bibliográficas mais significativas.

Capítulo 1

Preliminares

É notória a semelhança entre os Teoremas do Isomorfismo para grupos, anéis e módulos. A Álgebra Universal é uma área de estudo que providencia a unificação não só destas três séries de teoremas como também de um importante leque de conceitos fundamentais de várias teorias algébricas. Ao longo deste capítulo abordaremos alguns conceitos básicos da Álgebra Universal, com o duplo objectivo de adquirir uma capacidade de abstracção que permita a compreensão dos aspectos essenciais de problemas que serão estudados mais tarde e de preparar o terreno para o posterior desenvolvimento de algumas ferramentas da Álgebra Universal Finita (que é o ramo da Álgebra Universal que se ocupa do estudo das estruturas algébricas finitas). A redacção deste primeiro capítulo baseou-se em [1, 12].

1.1 Álgebras

1.1.1 Definições

Um *tipo algébrico*, ou *linguagem algébrica*, é um par ordenado $\tau = (\mathcal{F}, \alpha)$ formado por um conjunto $\mathcal{F}$ e uma função $\alpha : \mathcal{F} \to \mathbb{N}_0$. Os elementos de $\mathcal{F}$ são os *símbolos funcionais* ou *operações fundamentais* de τ; α é a *função de aridade* de τ, sendo, para cada $f \in \mathcal{F}$, o inteiro $\alpha(f)$ a *aridade* de f. Se $\alpha(f) = n$ dizemos que f é uma operação fundamental *n-ária*. No caso particular em que $n = 0$ também podemos dizer que f é uma *operação fundamental nulária* ou que f é um *símbolo constante*, ou simplesmente uma *constante*; para $n = 1, 2$ ou 3 adoptamos, em vez do atributo *n-ária*, os adjectivos convencionais *unária*, *binária* e *ternária*. O conjunto das operações fundamentais n-árias é denotado por $\mathcal{F}_n$.

Uma *álgebra de tipo τ* é um par ordenado $\mathcal{A} = (A, F)$ constituído por um conjunto não vazio A, dito o *universo* de $\mathcal{A}$, e uma família $F = \left(f_{\mathcal{A}} : A^{\alpha(f)} \to A\right)_{f \in \mathcal{F}}$ de *operações fundamentais* de $\mathcal{A}$. A função $f_{\mathcal{A}}$ é a *interpretação* de f em $\mathcal{A}$. O significado de A^0 é

aquele que encontramos na Teoria dos Conjuntos: $A^0 = \{\emptyset\}$ é o conjunto das funções $\emptyset \to A$. Portanto, se f é um símbolo constante podemos identificar $f_{\mathcal{A}}$ com $f_{\mathcal{A}}(\emptyset)$.

Uma álgebra diz-se *infinita*, *finita*, ou *trivial* conforme o cardinal do seu universo seja infinito, finito, ou um, respectivamente.

Por simplicidade, e sempre que não haja perigo de confusão, adoptamos as seguintes convenções:

- a menção do tipo pode não ser feita, e se nos referimos a várias álgebras em simultâneo então estamos a admitir que são todas do mesmo tipo;
- a interpretação $f_{\mathcal{A}}$ pode ser abusivamente denotada por f;
- se o conjunto $\mathcal{F}$ for finito e $f_1, f_2, \ldots, f_k$ forem os seus elementos, em vez de designarmos a álgebra $\mathcal{A}$ pelo par (A, F), designamo-la pela expressão $(A; f_1, f_2, \ldots, f_k)$;
- a referência a uma álgebra $\mathcal{A} = (A, F)$ pode ser feita com omissão do conjunto F, identificando-se $\mathcal{A}$ com o seu universo A.
- se $\cdot$ for uma operação binária, em vez de $\cdot(a, b)$ escrevemos $a \cdot b$ ou mesmo ab.

Diremos que uma álgebra $(A; f_1, f_2, \ldots, f_k)$ tem *aridade* $(n_1, n_2, \ldots, n_k)$ se $\alpha(f_i) = n_i$ $(i = 1, \ldots, k)$.

1.1.2 Alguns exemplos

Um grupóide é uma álgebra $(G; \cdot)$ de aridade (2). A estrutura de um grupóide pode ser bastante complicada. Fixado um tipo com apenas uma operação fundamental $\cdot$, binária, importa portanto considerar classes mais restritas de grupóides. A mais elementar de entre as mais estudadas dessas classes é a dos semigrupos. Um semigrupo caracteriza-se por satisfazer a propriedade associativa, expressa pela seguinte identidade:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

Os monóides e os grupos podem ser definidos como membros de subclasses da classe dos semigrupos: por exemplo, a classe dos monóides pode ser definida como a classe dos grupóides satisfazendo as fórmulas

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$\exists e : \; x \cdot e = e \cdot x = x$$

No entanto, para que aproveitemos eficentemente alguns dos resultados clássicos da Álgebra Universal, preferiremos fórmulas que sejam simplesmente identidades. Assim, para nos libertarmos dos quantificadores, adoptamos a perspectiva alternativa de

considerar um monóide como uma álgebra $(M; \cdot, 1)$ de aridade $(2, 0)$ satisfazendo as identidades

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$x \cdot 1 = 1 \cdot x = x$$

De modo semelhante, um grupo é uma álgebra $(G; \cdot, {}^{-1}, 1)$ de aridade $(2, 1, 0)$ que satisfaz as identidades

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$x \cdot 1 = 1 \cdot x = x$$

$$x \cdot x^{-1} = x^{-1} \cdot x = 1$$

A classe dos grupos Abelianos é uma subclasse dos grupos cujos elementos se caracterizam por satisfazerem adicionalmente a identidade $x \cdot y = y \cdot x$.

Um anel[1] é uma álgebra $(R; +, \cdot, -, 0, 1)$ de aridade $(2, 2, 1, 0, 0)$ com as seguintes propriedades:

1. $(R; +, -, 0)$ é um grupo Abeliano;
2. $(R, \cdot, 1)$ é um monóide;
3. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ e $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ (distributividade de $\cdot$ relativamente a $+$).

As estruturas de *semianel* [6] e de *semianel com zero* constituem variações da estrutura de anel. Um semianel é uma álgebra $(R; +, \cdot, 1)$ de aridade $(2, 2, 0)$ tal que $(R; +)$ é um semigrupo e que verifica as propriedades 2 e 3 de um anel.[2] Um semianel com zero é uma álgebra $(R; +, \cdot, 0, 1)$ de aridade $(2, 2, 0, 0)$ tal que $(R; +, 0)$ é um monóide e que também verifica as propriedades 2 e 3. Por exemplo, para a adição e multiplicação usuais, $\mathbb{N}$ é um semianel e $\mathbb{N}_0$ é um semianel com zero. São ambos comutativos (a multiplicação é comutativa).

Dado um anel R, um R-módulo é uma álgebra $(M; +, -, 0, (r\cdot)_{r \in R})$[3] tal que $+$ é binária, 0 é nulária, e as restantes operações são unárias, e que satisfaz as seguintes propriedades:

1. $(M; +, -, 0)$ é um grupo Abeliano;
2. $1 \cdot x = x$;
3. $r \cdot (x + y) = r \cdot x + r \cdot y$, $\forall r \in R$;

[1] Nesta monografia *anel* será sempre um sinónimo de *anel com unidade*.

[2] Na definição dada em [6] não se exige que a operação $\cdot$ tenha um elemento neutro.

[3] Reparemos que, de certo modo, estamos a estender a um caso em que o conjunto das operações fundamentais pode ser infinito a convenção de escrita que tínhamos adoptado para quando esse conjunto era finito.

4. $(r+s)\cdot x = r\cdot x + s\cdot x$, $\forall r,s \in R$;

5. $r\cdot(s\cdot x) = (rs)\cdot x$, $\forall r,s \in R$.

Não obstante não necessitarmos da estrutura de R-módulo para os nossos propósitos, a sua presença aqui tem o mérito de fornecer exemplos simples e familiares de álgebras com uma infinidade de operações fundamentais, no caso de R ser infinito. Para mais exemplos de álgebras de grande importância mas que não serão invocadas neste trabalho, veja-se [12].

1.2 Termos e Identidades

Fixemos um tipo algébrico $\tau = (\mathcal{F}, \alpha)$. Consideremos agora dois outros conjuntos X e P com as seguintes características: $\mathcal{F}$, X e P são disjuntos dois a dois, o cardinal de P é três e $X \cup \mathcal{F}_0 \neq \emptyset$. Os elementos de X serão a partir de agora referidos como as *variáveis*. Cada um dos elementos de P tem uma designação especial: *parênteses esquerdo*, *parênteses direito* e *vírgula*; os símbolos que representam cada um deles, e que a seguir apresentamos pela ordem respectiva e entre aspas, estão de acordo com a sua designação: "(" , ")", e ",". Seja $S(X)$ o conjunto das sequências finitas de elementos de $X \cup \mathcal{F} \cup P$; o conjunto $S(X)$ é sugestivamente referido como o *conjunto das palavras no alfabeto* $X \cup \mathcal{F} \cup P$. Identificando as sequências de comprimento um com os elementos que as definem, podemos considerar $X \cup \mathcal{F} \cup P$ como subconjunto de $S(X)$.

Definimos indutivamente uma sequência $(T_n(X))_{n\in\mathbb{N}_0}$ de subconjuntos de $S(X)$ pela seguinte fórmula de recorrência:

$$\begin{cases} T_0(X) = X \cup \mathcal{F}_0 \\ T_{n+1}(X) = T_n(X) \cup \left(\bigcup_{k\in\mathbb{N}} \{f(t_1,\ldots,t_k) \in S(X) : f \in \mathcal{F}_k;\ t_1,\ldots,t_k \in T_n(X)\}\right) \end{cases}$$

O subconjunto $T(X) = \bigcup_{n\in\mathbb{N}_0} T_n(X)$ de $S(X)$ é o conjunto dos *termos* de tipo τ em X. De forma muito natural, podemos fazer de $T(X)$ o universo de uma álgebra $\mathcal{T}(X)$, a álgebra dos termos de tipo τ em X, dando a cada elemento f de $\mathcal{F}_0$ a interpretação $f_{\mathcal{T}(X)} = f$, e a cada elemento f de $\mathcal{F}_n$, $n > 0$, a interpretação

$$\begin{aligned} f_{\mathcal{T}(X)} : \quad T(X)^n &\longrightarrow T(X) \\ (t_1,\ldots,t_n) &\longmapsto f(t_1,\ldots,t_n) \end{aligned}$$

Dado $p \in T(X)$ podemos escrever $p = p(x_1,\ldots,x_n)$ se o conjunto das variáveis que ocorrem na sequência constituinte de p estiver contido no conjunto de variáveis distintas $\{x_1,\ldots,x_n\}$, $(n > 0)$. Diremos que um termo p é um *termo n-ário* se o número de variáveis distintas que nele ocorrem for menor ou igual a n $(n \geq 0)$.[4]

[4]Obviamente, se $m \geq n$ então um termo n-ário é um termo m-ário, mas se $m < n$ tal pode não acontecer.

Sejam $p(x_1, \ldots, x_n) \in T_k(X)$ um termo n-ário, A uma álgebra de tipo τ e $(a_1, \ldots, a_n)$ um elemento de A^n, sendo p, A e $(a_1, \ldots, a_n)$ arbitrários. Vamos definir um elemento $p_A(a_1, \ldots, a_n)$ de A por recursividade sobre k, do modo que se segue:

- se $p = x_i \in X$ $(i = 1, \ldots, n)$, então $p_A(a_1, \ldots, a_n) = a_i$, e se $p = f \in \mathcal{F}_0$, então $p_A(a_1, \ldots, a_n) = f_A$;
- se $p \in T_k(X) \setminus T_{k-1}(X)$, $k > 0$, então existem $r \in \mathbb{N}$, $f \in \mathcal{F}_r$, $p_1, \ldots, p_r \in T_{k-1}(X)$ tais que $p = f(p_1, \ldots, p_r)$, e assim, supondo feita a definição para inteiros menores que k, definimos

$$p_A(a_1, \ldots, a_n) = f_A((p_1)_A(a_1, \ldots, a_n), \ldots, (p_r)_A(a_1, \ldots, a_n)).$$

Temos portanto a seguinte operação n-ária em A:

$$\begin{aligned} p_A : \quad A^n &\longrightarrow A \\ (a_1, \ldots, a_n) &\longmapsto p_A(a_1, \ldots, a_n) \end{aligned}$$

O conceito de termo n-ário generaliza o de operação fundamental n-ária. Com efeito, se $x_1, \ldots, x_n$ forem variáveis distintas, f for uma operação fundamental n-ária e p o termo $f(x_1, \ldots, x_n)$, então para qualquer álgebra A temos $p_A = f_A$.

Vimos como algumas classes de álgebras se caracterizam por satisfazer determinadas identidades. Temos agora uma oportunidade para dar um significado matemático preciso a esta utilização do verbo "satisfazer" e do substantivo "identidade". Uma *identidade* de tipo τ num conjunto X define-se como sendo um par ordenado (p, q) de termos de tipo τ em X. O par (p, q) é usualmente denotado pela igualdade formal $p = q$. Dizemos que uma álgebra A *satisfaz* uma identidade $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$, e escrevemos $A \models p = q$, se $p_A(a_1, \ldots, a_n) = q_A(a_1, \ldots, a_n)$ para todo o elemento $(a_1, \ldots, a_n)$ de A^n; se $\mathcal{K}$ for uma classe de álgebras de tipo τ então $\mathcal{K} \models p = q$ significa que todos os elementos de $\mathcal{K}$ satisfazem a identidade $p = q$; e se Σ for um conjunto de identidades de tipo τ então $\mathcal{K} \models \Sigma$ significa que todos os elementos de $\mathcal{K}$ satisfazem todas as identidades de Σ. A classe das álgebras que satisfazem um conjunto de identidades Σ é denotada $[\Sigma]$; é claro que para $\Sigma = \{p = q\}$ estaremos à vontade para omitir as chavetas, escrevendo apenas $[p = q]$.

Exemplo 1.1. *Consideremos um tipo algébrico com uma única operação binária* $\cdot$. *Sejam* x, y *e* z *três elementos distintos de um conjunto de variáveis* X. *Aplicando a convenção de simplificação fixada para as operações binárias,* $p = (x \cdot y) \cdot z$ *e* $q = x \cdot (y \cdot z)$ *são termos ternários nas variáveis* x, y *e* z. *A classe dos semigrupos é a classe* $[p = q]$.

Sejam $x_1, \ldots, x_n$ variáveis distintas de X. Um *operador polinomial n-ário*[5] de tipo τ nas variáveis $x_1, \ldots, x_n$ é um elemento $(p_1, \ldots, p_n)$ de $T(\{x_1, \ldots, x_n\})^n$. Dados

[5] Esta definição e as que a seguir lhe dão sequência são da responsabilidade do autor, embora com base em [3].

elementos $f = (p_1, \ldots, p_n)$ e $g = (q_1, \ldots, q_n)$ de $T(\{x_1, \ldots, x_n\})^n$, a *identidade de operadores polinomiais* $f = g$ é o conjunto de identidades $p_i = q_i$ $(i = 1, \ldots, n)$.

Dada uma álgebra A de tipo τ, podemos considerar a seguinte função de $T(\{x_1, \ldots, x_n\})^n$ no monóide $(A^n)^{A^n}$ das funções $A^n \to A^n$ (a operação do monóide é a composição de funções, evidentemente):

$$\begin{aligned} \epsilon_A : T(\{x_1, \ldots, x_n\})^n &\longrightarrow (A^n)^{A^n} \\ f = (p_1, \ldots, p_n) &\longmapsto f_A = ((p_1)_A, \ldots, (p_n)_A) \end{aligned}$$

A imagem de ϵ_A é um submonóide de $(A^n)^{A^n}$. A função $\epsilon_{T(\{x_1,\ldots,x_n\})}$ permite-nos definir em $T(\{x_1, \ldots, x_n\})^n$ uma operação de composição que o torna num monóide: se f e g são operadores polinomiais n-ários em $x_1, \ldots, x_n$, então a sua composta $f \circ g$ é $\epsilon_{T(\{x_1,\ldots,x_n\})}(f)(g)$.

1.3 Homomorfismos

Um *homomorfismo* $\varphi : \mathcal{A} \to \mathcal{B}$ entre duas álgebras $\mathcal{A} = (A, F)$ e $\mathcal{B} = (B, G)$ do mesmo tipo é uma função $\varphi : A \to B$ que torna o diagrama (1.1)[6] comutativo, para todo $f \in \mathcal{F}_n$ e para todo $n \in \mathbb{N}_0$.

$$\begin{array}{ccc} A^n & \xrightarrow{f_A} & A \\ {\scriptstyle \varphi^{(n)}}\downarrow & & \downarrow{\scriptstyle \varphi} \\ B^n & \xrightarrow{f_B} & B \end{array} \tag{1.1}$$

Exemplo 1.2. *Se $\mathcal{G} = (G; \cdot)$ e $\mathcal{H} = (H; \cdot)$ são dois grupóides, então um homomorfismo $\varphi : \mathcal{G} \to \mathcal{H}$ é uma função $\varphi : G \to H$ tal que $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, quaisquer que sejam os elementos a e b de G.*

Exemplo 1.3. *Se $\mathcal{G} = (G; \cdot, {}^{-1}, 1)$ e $\mathcal{H} = (H; \cdot, {}^{-1}, 1)$ são álgebras de aridade $(2, 1, 0)$, então um homomorfismo $\varphi : \mathcal{G} \to \mathcal{H}$ é uma função $\varphi : G \to H$ tal que*

1. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, $\forall a, b \in G$;
2. $\varphi(1) = 1$;
3. $\varphi(a^{-1}) = \varphi(a)^{-1}$, $\forall a \in G$.

Como é bem sabido, as condições 2 e 3 são surpérfluas se $\mathcal{G}$ e $\mathcal{H}$ forem grupos.

[6] É possível que o símbolo $\varphi^{(n)}$ cause alguma estranheza; assim convém esclarecer que se h é uma função $Y \to Z$, então $h^{(n)}$ designa a função $(y_1, \ldots, y_n) \in Y^n \to (h(y_1), \ldots, h(y_n)) \in Z^n$.

Exemplo 1.4. *Se* $\mathcal{R} = (R; +, \cdot, -, 0, 1)$ *e* $\mathcal{S} = (S; +, \cdot, -, 0, 1)$ *são álgebras de aridade* $(2, 2, 1, 0, 0)$, *então um homomorfismo* $\varphi : \mathcal{R} \to \mathcal{S}$ *é uma função* $\varphi : R \to S$ *tal que*

1. φ *é um homomorfismo entre* $(R; +, -, 0)$ *e* $(S; +, -, 0)$ *(ver exemplo 1.3);*
2. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b), \forall a, b \in G;$
3. $\varphi(1) = 1.$

Dizemos que uma álgebra B é uma *imagem homomorfa* de uma álgebra A se existir algum homomorfismo sobrejectivo $\varphi : A \to B$.

Usando um argumento indutivo baseado no modo recursivo como definimos o conjunto dos termos num conjunto de variáveis, podemos mostrar que se p é um termo n-ário então

$$\varphi(p_A(a_1, \ldots, a_n)) = p_B(\varphi(a_1), \ldots, \varphi(a_n)),\ \forall\, (a_1, \ldots, a_n) \in A^n$$

ou seja, o diagrama (1.2) comuta:

$$\begin{array}{ccc} A^n & \xrightarrow{p_A} & A \\ {\scriptstyle \varphi^{(n)}}\downarrow & & \downarrow{\scriptstyle \varphi} \\ B^n & \xrightarrow{p_B} & B \end{array} \tag{1.2}$$

O diagrama (1.2) tem o diagrama (1.1) como caso particular.

Um *isomorfismo* é um homomorfismo bijectivo (a inversa de um isomorfismo ainda é um isomorfismo), um *endomorfismo* é um homomorfismo cujo domínio é igual ao conjunto de chegada, e um *automorfismo* é um endomorfismo bijectivo. As álgebras A e B são *isomorfas*, e escrevemos $A \simeq B$, se existir algum isomorfismo entre elas.

Podemos considerar a classe das álgebras de tipo $\tau = (\mathcal{F}, \alpha)$ como a classe dos objectos de uma categoria $\mathscr{C}_\tau$, a *categoria das álgebras de tipo* τ, cujos morfismos são os homomorfismos entre álgebras.

Seja $\tilde{\tau} = (\tilde{\mathcal{F}}, \tilde{\alpha})$ um outro tipo algébrico. Suponhamos que os conjuntos $\mathcal{F}_n$ e $\tilde{\mathcal{F}}_n$ têm a mesma cardinalidade para todo o $n \in \mathbb{N}_0$. Isto é equivalente a dizer que existe uma bijecção $\rho : \mathcal{F} \to \tilde{\mathcal{F}}$ tal que, para todo o $n \in \mathbb{N}_0$, $\rho(\mathcal{F}_n) = \tilde{\mathcal{F}}_n$, ou seja, tal que $\tilde{\alpha} \circ \rho = \alpha$. Dada uma álgebra $\mathcal{A} = (A, F)$ de $\mathscr{C}_\tau$, se $\tilde{F} = \left(f_{\mathcal{A}} : A^{\alpha(f)} \to A\right)_{\rho(f) \in \tilde{\mathcal{F}}}$ então $\tilde{\mathcal{A}} = (A, \tilde{F})$ é uma álgebra de $\mathscr{C}_{\tilde{\tau}}$. A álgebra $\tilde{\mathcal{A}}$ caracteriza-se portanto pela interpretação $(\rho(f))_{\tilde{\mathcal{A}}} = f_{\mathcal{A}}$, para cada $f \in \mathcal{F}$. Ficou assim definido o functor

$$\begin{array}{rccc} H_\rho : & \mathscr{C}_\tau & \longrightarrow & \mathscr{C}_{\tilde{\tau}} \\ & \mathcal{A} & \longmapsto & \tilde{\mathcal{A}} \\ & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ & \mathcal{B} & \longmapsto & \tilde{\mathcal{B}} \end{array}$$

Este functor é um isomorfismo de categorias ($H_\rho \circ H_{\rho^{-1}} = 1_{\mathscr{C}_{\bar{\tau}}}$, $H_{\rho^{-1}} \circ H_\rho = 1_{\mathscr{C}_\tau}$). Esta propriedade expressa o facto, que já tem estado presente neste texto, de que o que verdadeiramente caracteriza um tipo algébrico $\tau = (\mathcal{F}, \alpha)$ é a cardinalidade dos conjuntos $\mathcal{F}_n$ de operações fundamentais n-árias. Assim, por exemplo, todos os tipos algébricos que consistem numa única operação binária são, para efeitos do estudo de álgebras, essencialmente o mesmo, o que torna legítimo o uso do artigo definido ao referirmo-nos a um desses tipos como *o* tipo algébrico dos semigrupos. O nome que atribuímos a este tipo é um pouco falacioso, pois uma álgebra do tipo dos semigrupos não tem que ser um semigrupo; o nome reflecte a importância que atribuímos a uma determinada classe de álgebras desse tipo. De modo análogo, podemos dizer que na subsecção 1.1.2 foram introduzidos, além do tipo dos semigrupos, *o* tipo dos monóides, *o* dos grupos, *o* dos anéis, *o* dos semianéis, *o* dos semianéis com zero, e *o* dos R-módulos.

1.4 Operadores de classes

1.4.1 Subálgebras

Dizemos que B é um *subuniverso* de uma álgebra A se B for um subconjunto não vazio de A tal que $f_A(B^n) \subseteq B$ para qualquer operação fundamental n-ária f, onde n é um elemento arbitrário de $\mathbb{N}_0$.

Exemplo 1.5. *Seja $\varphi : A \to B$ um homomorfismo. Então* $\operatorname{Im}\varphi$ *é um subuniverso de B, e se U for um subuniverso de B então $\varphi^{-1}(U)$ é também um subuniverso de A.*

Uma *subálgebra* B de uma álgebra A é um subuniverso B de A munido da estrutura de álgebra obtida pela restrição a B das operações fundamentais de A. Notemos que se B é um subconjunto da álgebra A munido de uma estrutura de álgebra, então B é uma subálgebra de A se e só se a inclusão $j : B \to A$ é um homomorfismo.

Seja X um conjunto infinito numerável de variáveis. Dada uma álgebra A, se S for um subconjunto tal que $S \cup \mathcal{F}_0 \neq \emptyset$, então o subconjunto

$$\langle S \rangle = \bigcup_{n \in \mathbb{N}_0} \{p_A(a_1, \ldots, a_n) \in A : p \text{ é um termo } n\text{-ário de } T(X);\ (a_1, \ldots, a_n) \in S^n\}$$

é um subuniverso de A e qualquer subuniverso de A que contém S também contém $\langle S \rangle$; munido da respectiva estrutura de álgebra, $\langle S \rangle$ é a subálgebra de A *gerada* por S. Se $\langle S \rangle = A$ então dizemos que A é gerada por S e que S é um *subconjunto gerador* de A. Por exemplo, para qualquer conjunto de variáveis X, a álgebra dos termos $T(X)$ é gerada por X.

Lema 1.6. *Sejam A e B duas álgebras (do mesmo tipo) e seja S um subconjunto gerador de A. Sejam $\psi : A \to B$ e $\eta : A \to B$ homomorfismos tais que $\psi_{|S} = \eta_{|S}$. Então $\psi = \eta$.*

Demonstração. Decorre imediatamente da definição de subálgebra gerada e da comutatividade entre homomorfismos e termos, expressa no diagrama (1.2). □

1.4.2 Produto directo de álgebras

Seja $(A_i)_{i\in I}$ uma família de álgebras (do mesmo tipo); o seu *produto directo* é a álgebra cujo universo é o produto cartesiano $\prod_{i\in I} A_i$, e onde a interpretação de cada operação fundamental é feita componente a componente:

$$f_{\prod_{i\in I} A_i}(a_1,\ldots,a_n) = (f_{A_i}((a_1)_i,\ldots,(a_n)_i))_{i\in I},\ \forall\,(a_1,\ldots,a_n)\in\left(\prod_{i\in I}A_i\right)^n,\ f\in\mathcal{F}_n,$$

onde $(a_k)_i$ representa a i-ésima componente de a_k.

1.4.3 Álgebras quocientes

Uma *congruência* θ numa álgebra A é uma relação de equivalência em A compatível com as operações fundamentais em A, no seguinte sentido:

$$\text{se } a_i\ \theta\ b_i\ (i=1,\ldots,n),\ \text{então } f_A(a_1,\ldots,a_n)\ \theta\ f_A(b_1,\ldots,b_n),\ \forall a_i,b_i\in A, f\in\mathcal{F}_n.$$

O conjunto quociente A/θ fica, de modo natural, munido de uma estrutura de álgebra: como θ é uma congruência, a interpretação $f_{A/\theta}(a_1/\theta,\ldots,a_n/\theta) = f_A(a_1,\ldots,a_n)/\theta$ de um símbolo $f\in\mathcal{F}_n$ está bem definida.

Exemplo 1.7. *A relação de equivalência total ∇ e a relação de igualdade Δ constituem exemplos triviais de congruências; a álgebra A/∇ é trivial e a álgebra A/Δ é isomorfa a A.*

Exemplo 1.8. *Se G é um grupo, então podemos estabelecer uma correspondência biunívoca natural entre congruências em G e subgrupos normais de G: se θ é uma congruência em G, então $1/\theta$ é um subgrupo normal de G; reciprocamente, se K é um subgrupo normal de G então a relação definida por $g_1\ \theta_K\ g_2 \Leftrightarrow g_1K = g_2K$ é uma congruência, e $K = 1/\theta_K$; e como $g/\theta = h/\theta \Leftrightarrow gh^{-1}\in 1/\theta$, se ϑ e ϱ forem congruências tais que $1/\vartheta = 1/\varrho$ então ϑ e ϱ são iguais. Situações semelhantes ocorrem com os ideais de um anel e os submódulos de um módulo, onde as congruências são determinadas por uma das suas subclasses.*

Se $\varphi : A\to B$ for um homomorfismo de álgebras, então o conjunto

$$\operatorname{Ker}\varphi = \{(a_1,a_2)\in A\times A : \varphi(a_1)=\varphi(a_2)\},$$

referido como o *núcleo* de φ, é uma congruência em A. A tradição da Teoria de Grupos já se apropriou da denominação e da notação desta congruência, o que faz com que no caso do tipo algébrico dos grupos a definição que acabámos de fazer seja ambígua.

No entanto esta ambiguidade fica resolvida pela correspondência que assinalámos no exemplo 1.8: o núcleo do homomorfismo φ segundo a definição usual da Teoria de Grupos é a classe de 1 na relação de equivalência que definimos.

Uma congruência θ numa álgebra A é o núcleo do homomorfismo canónico

$$\begin{aligned} \nu : \quad A &\longrightarrow A/\theta \\ a &\longmapsto a/\theta \end{aligned}$$

Portanto, toda a congruência numa álgebra é o núcleo de algum homomorfismo.

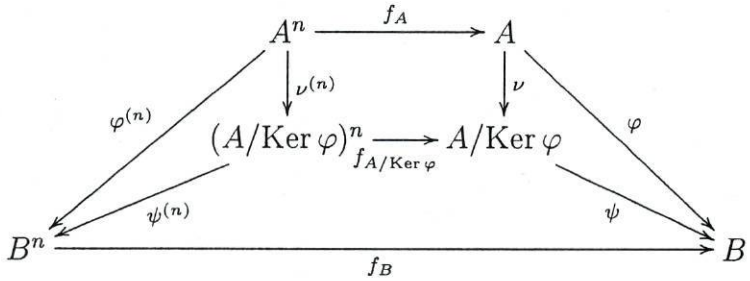
Estão agora reunidos os ingredientes para enunciar e demonstrar os Teoremas do Isomorfismo para álgebras arbitrárias, o que permite a unificação dos já conhecidos Teoremas do Isomorfismo para grupos, anéis e módulos. Nesta monografia realizaremos esta tarefa apenas para o primeiro desses teoremas, também conhecido como Teorema do Homomorfismo, por ser o único que nos aproveitará. Para o estudo dos restantes teoremas remetemos, por exemplo, para [12].

Teorema 1.9 (Teorema do Homomorfismo). *Se $\varphi : A \to B$ é um homomorfismo então $A/\mathrm{Ker}\,\varphi \simeq \mathrm{Im}\,\varphi$.*

Demonstração. Seja

$$\begin{aligned} \psi : \quad A/\mathrm{Ker}\,\varphi &\longrightarrow \mathrm{Im}\,\varphi \\ a/\mathrm{Ker}\,\varphi &\longmapsto \varphi(a) \end{aligned}$$

Vamos demonstrar o teorema provando que ψ é um isomorfismo. Uma vez que $a/\mathrm{Ker}\,\varphi = b/\mathrm{Ker}\,\varphi$ se e só se $\varphi(a) = \varphi(b)$, a função ψ está bem definida e é injectiva; por outro lado, ψ é claramente sobrejectiva. Resta-nos mostrar que ψ é um homomorfismo. No diagrama (1.3) (onde ν é o homomorfismo canónico e f é uma operação fundamental n-ária) o trapézio exterior, o rectângulo e os triângulos laterais comutam;



(1.3)

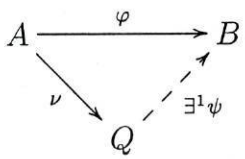
logo, como $\nu^{(n)}$ é sobrejectiva, o trapézio interior também comuta, i.e., ψ é um homomorfismo. □

Provámos a existência de um único homomorfismo $\psi : A/\mathrm{Ker}\,\varphi \to B$ tal que $\psi \circ \nu = \varphi$ e vimos que ψ é um homomorfismo injectivo. A próxima proposição é uma generalização deste resultado.

Proposição 1.10. *Sejam $\nu : A \to Q$ e $\varphi : A \to B$ dois homomorfismos, sendo ν sobrejectivo.*

1. *A existência de um único homomorfismo $\psi : Q \to B$ tal que $\psi \circ \nu = \varphi$ é equivalente à inclusão* $\operatorname{Ker}\nu \subseteq \operatorname{Ker}\varphi$.

2. *A existência de um único homomorfismo injectivo $\psi : Q \to B$ tal que $\psi \circ \nu = \varphi$ é equivalente à igualdade* $\operatorname{Ker}\nu = \operatorname{Ker}\varphi$.



Demonstração. A implicação directa de 1 é imediata. Mostremos a implicação recíproca. Se $\operatorname{Ker}\nu \subseteq \operatorname{Ker}\varphi$ então fica bem definida a função

$$\begin{aligned} \psi : \quad Q &\longrightarrow B \\ \nu(a) &\longmapsto \varphi(a) \end{aligned}$$

Temos de facto $\psi \circ \nu = \varphi$. Se agora no diagrama (1.3) substituirmos $A/\operatorname{Ker}\varphi$ por Q, obtemos ainda um diagrama comutativo, pelo que ψ é um homomorfismo. Uma vez provada a parte 1, não há qualquer dificuldade em demonstrar a parte 2. □

1.4.4 Variedades e Pseudovariedades

Parafraseando Burris e Sankappanavar [12], um dos assuntos mais importantes da Álgebra Universal é o estudo de classes de álgebras fechadas para certos géneros de operadores sobre classes de álgebras. Um *operador unário de classes de álgebras* O é simplesmente uma correspondência de classes que associa a cada classe $\mathcal{K}$ de álgebras do mesmo tipo uma outra classe de álgebras $\mathrm{O}(\mathcal{K})$ desse mesmo tipo. Num encadeamento lógico com as subsecções anteriores, temos como exemplos cruciais de operadores unários de álgebras os operadores S, H, I e P que a cada classe $\mathcal{K}$ associam, respectivamente:

- a classe $\mathrm{S}(\mathcal{K})$ das subálgebras de elementos de $\mathcal{K}$;
- a classe $\mathrm{H}(\mathcal{K})$ das imagens homomorfas de elementos de $\mathcal{K}$;
- a classe $\mathrm{I}(\mathcal{K})$ das álgebras isomorfas a elementos de $\mathcal{K}$;
- a classe $\mathrm{P}(\mathcal{K})$ dos produtos directos de famílias de elementos de $\mathcal{K}$.

O operador P não satisfaz as necessidades da Álgebra Universal Finita, uma vez que, em geral, transforma classes de álgebras finitas em classes com álgebras infinitas. Consideramos por isso o operador $\mathrm{P_{fin}}$ que a cada classe $\mathcal{K}$ associa a classe $\mathrm{P_{fin}}(\mathcal{K})$ dos produtos de famílias constituídas por um número finito de elementos de $\mathcal{K}$ (os quais não têm que ser finitos!).

Se $\mathrm{O_1}$ e $\mathrm{O_2}$ forem dois operadores unários de classes de álgebras, $\mathrm{O_1O_2}$ denota a sua composição: $\mathrm{O_1O_2}(\mathcal{K}) = \mathrm{O_1}(\mathrm{O_2}(\mathcal{K}))$. Reparemos que a composição de operadores é associativa. Escrevemos $\mathrm{O_1} \leq \mathrm{O_2}$ se para qualquer classe $\mathcal{K}$ tivermos $\mathrm{O_1}(\mathcal{K}) \subseteq \mathrm{O_2}(\mathcal{K})$.

Um operador O é *idempotente* se $\mathrm{O}^2 = \mathrm{O}$.

Lema 1.11. *As desigualdades* $\mathrm{SH} \leq \mathrm{HS}$, $\mathrm{SI} \leq \mathrm{IS}$, $\mathrm{OS} \leq \mathrm{SO}$ *e* $\mathrm{OH} \leq \mathrm{HO}$ *são válidas para* $\mathrm{O} \in \{\mathrm{P}, \mathrm{P_{fin}}\}$, *e os operadores* H, S, IP, HP *e* HS *são idempotentes.*

A demonstração das desigualdades e das idempotências mais não são do que exercícios rotineiros. Nesta monografia só será utilizada a desigualdade $\mathrm{SH} \leq \mathrm{HS}$ e a idempotência de HS. Por essa razão, demonstramos somente estes dois resultados:

Demonstração. Seja $A \in \mathrm{SH}(\mathcal{K})$; então existem uma álgebra C de $\mathcal{K}$ e um homomorfismo sobrejectivo $\varphi : C \to B$ tais que A é uma subálgebra de B; é claro que A é imagem homomorfa de $\varphi^{-1}(A)$, que por sua vez é uma subálgebra de C; logo $A \in \mathrm{HS}(\mathcal{K})$.

Uma vez que toda a álgebra é subálgebra e imagem homomorfa de si mesma, $\mathrm{HS} \leq \mathrm{HSHS}$. Pela mesma razão, os operadores S e H são idempotentes. Por outro lado, pela desigualdade $\mathrm{SH} \leq \mathrm{HS}$ e pela idempotência de S e H, $\mathrm{HSHS} \leq \mathrm{HHSS} = \mathrm{HS}$. □

Dizemos que uma álgebra B é um *divisor* da álgebra A se B for imagem homomorfa de uma subálgebra de A, ou seja, se $B \in \mathrm{HS}\{A\}$. Nesse caso dizemos também que B *divide* A e que A é *divisível* por B. Podemos deste modo definir uma relação "divide" entre álgebras do mesmo tipo; pela idempotência de HS, esta relação é transitiva. A álgebra B é um divisor *próprio* de A se B dividir A mas A não dividir B. Se A e B forem álgebras finitas tais que B divide A, então as seguintes condições são equivalentes:

1. B é um divisor próprio de A;
2. B e A não são isomorfas;
3. o cardinal de B é menor do que o de A.

As implicações $1 \Rightarrow 3$, $2 \Rightarrow 3$ e $2 \Rightarrow 1$ podem não ser válidas quando as álgebras A e B não são finitas. O grupo $\mathbb{Z}$ é um divisor próprio do grupo $\mathbb{Q}$ e no entanto $\mathbb{Z}$ e $\mathbb{Q}$ têm o mesmo cardinal. Temos como exemplo da impossibilidade de estender a última implicação a álgebras infinitas arbitrárias os grupos $\mathbb{Z}^{\mathbb{N}}$ e $\mathbb{Z}_2 \times \mathbb{Z}^{\mathbb{N}}$. Estes grupos não

são isomorfos, uma vez que $([1]_2, (0)_{n\in\mathbb{N}})$ é um elemento de ordem dois de $\mathbb{Z}_2 \times \mathbb{Z}^{\mathbb{N}}$ e $\mathbb{Z}^{\mathbb{N}}$ não tem elementos de ordem finita diferente de um; por outro lado, o grupo $\mathbb{Z}^{\mathbb{N}}$ divide o grupo $\mathbb{Z}_2 \times \mathbb{Z}^{\mathbb{N}}$, bastando para tal considerar a projecção canónica do segundo no primeiro, e $\mathbb{Z}_2 \times \mathbb{Z}^{\mathbb{N}}$ divide $\mathbb{Z}^{\mathbb{N}}$, pois a função

$$\begin{aligned} \mathbb{Z}^{\mathbb{N}} &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}^{\mathbb{N}} \\ (a_n)_{n\in\mathbb{N}} &\longmapsto ([a_1]_2, (a_{n+1})_{n\in\mathbb{N}}) \end{aligned}$$

é um homomorfismo sobrejectivo.

Uma *variedade* de tipo τ é uma classe de álgebras de tipo τ fechada para os operadores S, H e P. Se Σ for um conjunto de identidades de tipo τ, então $[\Sigma]$ é uma variedade. Na verdade, todas as variedades se obtêm deste modo:

Teorema 1.12 (Birkhoff). *Seja X um conjunto numerável. Se $\mathcal{V}$ é uma variedade e $\Sigma_{\mathcal{V}}$ é o conjunto das identidades em X válidas em $\mathcal{V}$, então $\mathcal{V} = [\Sigma_{\mathcal{V}}]$.*

A inclusão $\mathcal{V} \subseteq [\Sigma_{\mathcal{V}}]$ é trivial, o que não acontece com a demonstração da inclusão recíproca. O lugar mais indicado para essa demonstração seria no final da próxima secção, no entanto vamos omiti-la, preferindo apenas assinalar a estreita relação entre os conceitos de variedade e de identidade.

A classe $\mathfrak{G}_\sigma$ das álgebras do tipo σ dos semigrupos que são grupos não é uma variedade do tipo σ: por exemplo, $\mathbb{Z}$ é um grupo e $\mathbb{N}$ é um subsemigrupo de $\mathbb{Z}$ que não é grupo. Já a classe $\mathfrak{G}_\gamma$ das álgebras do tipo γ dos grupos que são grupos é uma variedade do tipo γ, pois

$$\mathfrak{G}_\gamma = [(x \cdot y) \cdot y = x \cdot (y \cdot z),\ x \cdot 1 = x,\ 1 \cdot x = x,\ x \cdot x^{-1} = 1,\ x^{-1} \cdot x = 1].$$

De seguida, apresentamos mais alguns exemplos importantes de variedades do tipo γ. A propósito das classes apresentadas, veja-se [23, 31, 30]. Voltaremos a falar com mais detalhe dos grupos nilpotentes e dos solúveis, a partir do capítulo 3.

$\mathfrak{A}$: classe dos grupos Abelianos;

$\mathfrak{A}_n$: classe dos grupos Abelianos de expoente n;

$\mathfrak{N}_c$: classe dos grupos nilpotentes com classe de nilpotência menor ou igual a c;

$\mathfrak{S}_d$: classe dos grupos solúveis com grau de solubilidade menor ou igual a d.

Em contraste, não são variedades do tipo γ:

$\mathfrak{N}$: classe dos grupos nilpotentes;

$\mathfrak{S}$: classe dos grupos solúveis.

Para $\tau \in \{\sigma, \gamma\}$, onde σ é o tipo dos semigrupos e γ é o tipo dos grupos, consideremos a classe $\mathfrak{G}_\tau$ como a classe dos objectos de uma subcategoria plena[7] $\mathscr{G}_\tau$ de $\mathscr{C}_\tau$. O functor

$$\begin{array}{rccc} F: & \mathscr{G}_\gamma & \longrightarrow & \mathscr{G}_\sigma \\ & (A;\cdot,^{-1},1) & \longmapsto & (A;\cdot) \\ & \downarrow\varphi & & \downarrow\varphi \\ & (B;\cdot,^{-1},1) & \longmapsto & (B;\cdot) \end{array}$$

que preserva a interpretação da operação binária é um isomorfismo de categorias.

Uma *pseudovariedade* de tipo τ é uma classe de álgebras finitas fechada para os operadores S, H e $\mathrm{P_{fin}}$. A classe G das álgebras finitas de tipo γ que são grupos é uma pseudovariedade de tipo γ. Embora não seja fechada para o operador S, a classe $\mathfrak{G}_\sigma$ é fechada para os operadores H e P; e como um subsemigrupo de um grupo finito ainda é um grupo, a subclasse $F(\mathsf{G})$ de $\mathfrak{G}_\sigma$ dos grupos finitos é uma pseudovariedade de tipo σ. Em geral, se V é uma subpseudovariedade de G então $F(\mathsf{V})$ é uma subpseudovariedade de $F(\mathsf{G})$. Isto torna legítimo que em geral se possa fazer a identificação de V com $F(\mathsf{V})$ e dizer que V é uma pseudovariedade sem explicitar se é do tipo σ ou γ. Podemos estabelecer um tipo de relação semelhante entre o tipo dos monóides e o tipo dos grupos. Tal já não é possível entre o tipo dos semigrupos e o tipo dos monóides, uma vez que um subsemigrupo de um monóide finito não é necessariamente um monóide.

Temos os seguintes exemplos de pseudovariedades de grupos:

G: classe dos grupos finitos;

Ab: classe dos grupos Abelianos finitos;

Ab_n: classe dos grupos Abelianos finitos de expoente n;

$\mathsf{G}_{\mathsf{nil}}$: classe dos grupos nilpotentes finitos;

$\mathsf{G}_{\mathsf{sol}}$: classe dos grupos solúveis finitos;

G_π: classe dos π-grupos finitos (onde π é um conjunto de primos);

$\mathsf{G}_{\mathsf{nil},\pi} = \mathsf{G}_{\mathsf{nil}} \cap \mathsf{G}_\pi$;

$\mathsf{G}_{\mathsf{sol},\pi} = \mathsf{G}_{\mathsf{sol}} \cap \mathsf{G}_\pi$.

Dada uma classe $\mathcal{K}$ de álgebras do tipo τ, existe uma variedade que a contém (por exemplo, a variedade de todas as álgebras de tipo τ). Como a intersecção de variedades ainda é uma variedade, a intersecção de todas as variedades que contêm $\mathcal{K}$ ainda é uma variedade que contém $\mathcal{K}$. Essa variedade designa-se como *variedade gerada por* $\mathcal{K}$ e é

[7]Uma subcategoria $\mathscr{D}$ de uma categoria $\mathscr{C}$ diz-se *plena* se o conjunto de morfismos de $\mathscr{D}$ entre dois objectos de $\mathscr{D}$ for igual ao conjunto de morfismos de $\mathscr{C}$ entre esses dois objectos.

denotada por $\mathrm{V}(\mathcal{K})$. Deste modo definimos um novo operador unário V de classes de álgebras do mesmo tipo. Analogamente, como toda a classe K de álgebras finitas está contida nalguma pseudovariedade e como a intersecção de pseudovariedades ainda é uma pseudovariedade, a intersecção das pseudovariedades que contêm K ainda é uma pseudovariedade, justamente denominada *pseudovariedade gerada por* K e denotada $\mathrm{V}_{\mathrm{fin}}(\mathsf{K})$. Ficou assim definido o operador $\mathrm{V}_{\mathrm{fin}}$ de classes de álgebras finitas do mesmo tipo. O lema 1.11 faz da demonstração das seguintes igualdades entre operadores um exercício fácil:

- $\mathrm{V} = \mathrm{HSP}$;
- $\mathrm{V}_{\mathrm{fin}} = \mathrm{HSP}_{\mathrm{fin}}$ (apenas para classes de álgebras finitas).

Exemplo 1.13. *Consideremos o tipo dos grupos. Para cada primo p de $\mathbb{N}$, a pseudovariedade $\mathrm{V}_{\mathrm{fin}}(\{\mathbb{Z}_p\})$ é a pseudovariedade Ab_p dos p-grupos Abelianos elementares finitos. Os grupos $\mathbb{Z}_p^n$, $n \in \mathbb{N}_0$, são representantes das suas classes de isomorfismo.*

Um outro paralelismo entre as variedades e as pseudovariedades diz respeito ao Teorema de Birkhoff. Com efeito, existe um análogo do Teorema de Birkhoff para pseudovariedades, o Teorema de Reiterman. Voltaremos a este assunto num momento mais apropriado, na secção 2.6.

1.5 Álgebras livres

Fixemos um tipo algébrico τ e um conjunto de variáveis X. A álgebra $T(X)$ dos termos em X tem a seguinte propriedade: se $\varphi : X \to A$ for uma função cujo conjunto de chegada é uma álgebra de tipo τ, então existe um único homomorfismo $\hat{\varphi} : T(X) \to A$ cuja restrição a X é a função φ (ver diagrama (1.4)). Com efeito, a função

$$\begin{aligned} \hat{\varphi} : \quad & T(X) \longrightarrow A \\ & p = p(x_1, \ldots, x_n) \longmapsto p_A(\varphi(x_1), \ldots, \varphi(x_n)) \end{aligned}$$

é um homomorfismo, pois se $f \in \mathcal{F}_n$ e $(p_1, \ldots, p_n) \in T(X)^n$, então

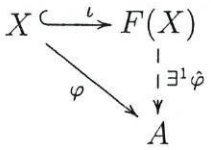
$$\begin{aligned} \hat{\varphi}(f(p_1, \ldots, p_n)) &= f_A((p_1)_A(\varphi(x_1), \ldots, \varphi(x_n)), \ldots, (p_n)_A(\varphi(x_1), \ldots, \varphi(x_n))) \\ &= f_A(\hat{\varphi}(p_1), \ldots, \hat{\varphi}(p_n)). \end{aligned}$$

E é imediato que a restrição de $\hat{\varphi}$ a X é φ e que $\hat{\varphi}$ é o único homomorfismo nestas condições, ilustradas no diagrama (1.4):

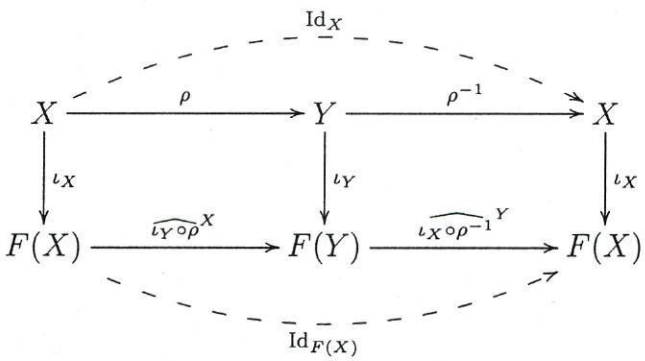
$$\begin{array}{ccc} X & \hookrightarrow & T(X) \\ & \searrow^{\varphi} & \downarrow \exists^1 \hat{\varphi} \\ & & A \end{array} \tag{1.4}$$

Esta propriedade de $T(X)$ leva-nos a um modo alternativo de descrever a operação n-ária $p_A : A^n \to A$. Dado um vector $(a_1, \ldots, a_n) \in A^n$ e uma qualquer função $\varphi : X \to A$ tal que $\varphi(x_i) = a_i$, temos $p_A(a_1, \ldots, a_n) = \hat{\varphi}(p)$: ou seja, "substituir" em p as variáveis $x_1, \ldots, x_n$ por $a_1, \ldots, a_n$, respectivamente, mais não é do que aplicar a p um homomorfismo $T(X) \to A$ que respeite a correspondência $x_i \mapsto a_i$. Ao adoptarmos esta perspectiva, ressalta desde logo a propriedade de que uma álgebra A de tipo τ satisfaz a identidade $p = q$ se e só se para todo o homomorfismo $\varphi : T(X) \to A$ tivermos $\varphi(p) = \varphi(q)$.

Façamos, no contexto das álgebras de tipo τ, a abstracção da propriedade de $T(X)$ que acabamos de descrever. Seja $\mathcal{K}$ uma classe de álgebras (de tipo τ). Sejam $F(X)$ uma álgebra (ainda de tipo τ) e $\iota : X \to F(X)$ uma função geradora, i.e., tal que $\iota(X)$ gera $F(X)$. Diremos que o par $(F(X), \iota)$ tem a *propriedade universal para $\mathcal{K}$ sobre X* se para toda a álgebra A de $\mathcal{K}$ e para toda a função $\varphi : X \to A$ existir um único homomorfismo $\varphi : F(X) \to A$ tal que $\hat{\varphi} \circ \iota = \varphi$.[8] Poderemos abusar da notação e falar da álgebra $F(X)$ no lugar do par $(F(X), \iota)$.



Se $\mathcal{K}$ contém alguma álgebra não trivial, então ι é injectiva. Se $F(X)$ é um elemento da classe $\mathcal{K}$, então é a menos de isomorfismo o único elemento de $\mathcal{K}$ com a propriedade universal para $\mathcal{K}$ sobre qualquer conjunto de cardinal igual ao de X (ver diagrama (1.5)).



(1.5)

Exemplo 1.14. *Se $j : X \to T(X)$ é a função de inclusão, o par $(T(X), j)$ tem a propriedade universal para a classe de todas as álgebras de tipo τ e sobre X. Logo se $|X| = |Y|$ então $T(X) \simeq T(Y)$.*

[8] Ao falarmos de um *único* homomorfismo estamos a ser enfáticos, pois se ψ e η são dois homomorfismos $F(X) \to A$ tais que $\psi \circ \iota = \eta \circ \iota$ então, como $\iota(X)$ gera $F(X)$, pelo lema 1.6 temos $\psi = \eta$.

Ainda não garantimos a existência de uma álgebra F com a propriedade universal para uma classe arbitrária $\mathcal{K}$ e sobre um conjunto X tal que $X \cup \mathcal{F}_0 \neq \emptyset$. Vamos fazer uma construção que vai dar-nos essa garantia. Associemos a $\mathcal{K}$ a congruência $\Theta_{\mathcal{K}}(X)$ em $T(X)$ constituída pelas identidades satisfeitas por $\mathcal{K}$. Notemos que $\mathcal{K}$ satisfaz uma identidade $p = q$ se e só se para toda a álgebra A de $\mathcal{K}$ e para todo o homomorfismo $\varphi : T(X) \to A$ tivermos $\varphi(p) = \varphi(q)$. Logo:

$$\begin{aligned}\Theta_{\mathcal{K}}(X) &= \{(p,q) \in T(X) \times T(X) : \mathcal{K} \models p = q\} \\ &= \bigcap \{\operatorname{Ker} \varphi : T(X) \xrightarrow{\varphi} A \text{ é um homomorfismo e } A \in \mathcal{K}\}.\end{aligned}$$

Denotemos por $\overline{p}$ o quociente $p/\Theta_{\mathcal{K}}(X)$, e por $\overline{X}$ o conjunto de quocientes $X/\Theta_{\mathcal{K}}(X)$.

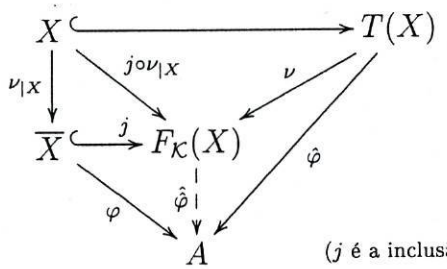
Lema 1.15. *Se $\mathcal{K}$ contém alguma álgebra não trivial então $x \in X \mapsto \overline{x} \in \overline{X}$ é uma bijecção; se $\mathcal{K}$ for uma classe vazia ou com apenas álgebras triviais, então $\overline{X}$ tem um só elemento.*

Demonstração. Se A é uma álgebra não trivial de $\mathcal{K}$ então, para quaisquer dois elementos x e y distintos de X, A não satisfaz a identidade $x = y$, pelo que $(x, y) \notin \Theta_{\mathcal{K}}(X)$, ou seja, $\overline{x} \neq \overline{y}$. Por outro lado, se $\mathcal{K}$ for uma classe vazia ou com apenas álgebras triviais, então todas as identidades são satisfeitas por $\mathcal{K}$, e portanto $\Theta_{\mathcal{K}}(X)$ é a relação de equivalência total. □

A álgebra quociente $T(X)/\Theta_{\mathcal{K}}(X)$ é denotada $F_{\mathcal{K}}(X)$ e é referida como a *$\mathcal{K}$-álgebra livre sobre X*.

Teorema 1.16. *A álgebra $F_{\mathcal{K}}(X)$ tem a propriedade universal para $\mathcal{K}$ sobre $\overline{X}$.*

Demonstração. Sejam $\nu : T(X) \to F_{\mathcal{K}}(X)$ o homomorfismo canónico e $\varphi : \overline{X} \to A$ uma função arbitrária numa álgebra arbitrária A de $\mathcal{K}$. Pela propiedade universal de $T(X)$, existe um homomorfismo $\hat{\varphi} : T(X) \to A$ cuja restrição a X é $\varphi \circ \nu_{|X}$.



Como $A \in \mathcal{K}$, temos $\operatorname{Ker} \hat{\varphi} \supseteq \Theta_{\mathcal{K}}(X) = \operatorname{Ker} \nu$. Pela proposição 1.10 (1), existe um homomorfismo $\hat{\hat{\varphi}} : F_{\mathcal{K}}(X) \to A$ tal que $\hat{\varphi} = \hat{\hat{\varphi}} \circ \nu$. Donde, se $x \in X$ então

$$\hat{\hat{\varphi}}(\overline{x}) = \hat{\hat{\varphi}} \circ \nu(x) = \hat{\varphi}(x) = \varphi \circ \nu(x) = \varphi(\overline{x}),$$

ou seja, $\hat{\hat{\varphi}}_{|\overline{X}} = \varphi$. □

Pelo lema 1.15, o par $(F_{\mathcal{K}}(X), j \circ \nu_{|X})$ tem a propriedade universal sobre X.

Lema 1.17. *Se* $|X| = |X'|$ *então* $F_{\mathcal{K}}(X) \simeq F_{\mathcal{K}}(X')$.

Demonstração. Como observámos no exemplo 1.14, existe um isomorfismo $\zeta : T(X) \to T(X')$. Sejam $\nu : T(X) \to F_{\mathcal{K}}(X)$ e $\nu' : T(X') \to F_{\mathcal{K}}(X')$ os homomorfismos canónicos.

$$\begin{array}{ccc} T(X) & \xrightarrow{\quad\nu\quad} & F_{\mathcal{K}}(X) \\ & {\scriptstyle \nu' \circ \zeta} \searrow \quad \nearrow {\scriptstyle \exists^1 \psi} & \\ & F_{\mathcal{K}}(X') & \end{array} \tag{1.6}$$

A igualdade $\operatorname{Ker} \nu = \operatorname{Ker}(\nu' \circ \zeta)$ mostra-se de forma rotineira. Pela proposição 1.10 (2), as álgebras $F_{\mathcal{K}}(X)$ e $F_{\mathcal{K}}(X')$ são isomorfas (ver diagrama (1.6): o homomorfismo ψ é injectivo, e como a função ν é sobrejectiva, ψ é uma bijecção). □

Lema 1.18. *A álgebra* $F_{\mathcal{K}}(X)$ *é isomorfa a uma subálgebra de um produto de elementos de* $\mathcal{K}$.

Demonstração. Consideremos o conjunto de congruências em $T(X)$

$$\Lambda = \{\operatorname{Ker} \varphi : T(X) \xrightarrow{\varphi} A \text{ é homomorfismo e } A \in \mathcal{K}\}.$$

Para cada $\theta \in \Lambda$, sejam A_θ um elemento de $\mathcal{K}$ e $\varphi_\theta : T(X) \to A_\theta$ um homomorfismo tais que $\operatorname{Ker} \varphi_\theta = \theta$. Consideremos agora o homomorfismo

$$\begin{aligned} \psi : T(X) &\longrightarrow \textstyle\prod_{\theta \in \Lambda} A_\theta \\ p &\longmapsto (\varphi_\theta(p))_{\theta \in \Lambda} \end{aligned}$$

Temos $\operatorname{Ker} \psi = \bigcap_{\theta \in \Lambda} \operatorname{Ker} \varphi_\theta = \bigcap_{\theta \in \Lambda} \theta = \Theta_{\mathcal{K}}(X)$. Logo $F_{\mathcal{K}}(X) \simeq \operatorname{Im} \psi$. □

Corolário 1.19. *Se* $\mathcal{K}$ *é uma variedade então* $F_{\mathcal{K}}(X)$ *é um elemento de* $\mathcal{K}$, *e é, a menos de isomorfismo, o único elemento de* $\mathcal{K}$ *com a propriedade universal para* $\mathcal{K}$ *sobre* X.

Proposição 1.20. *Se* V *é uma pseudovariedade gerada por um único elemento e se* X *for um conjunto de variáveis finito então* $F_{\mathsf{V}}(X)$ *é um elemento de* V.

Demonstração. Seja A uma álgebra que gera V. Consideremos o conjunto Λ dos homomorfismos que têm $T(X)$ como domínio e A como conjunto de chegada. Um elemento de Λ fica completamente determinado pela sua restrição a X, pelo que o cardinal de Λ é menor ou igual ao conjunto das funções de domínio X e conjunto de chegada A. Como X e A são finitos, Λ também é finito. Consideremos o seguinte homomorfismo:

$$\begin{aligned} \psi : T(X) &\longrightarrow \textstyle\prod_{\varphi \in \Lambda} \operatorname{Im} \varphi \\ p &\longmapsto (\varphi(p))_{\varphi \in \Lambda} \end{aligned}$$

Como Λ é finito, o produto $\prod_{\varphi\in\Lambda} \operatorname{Im}\varphi$ é um elemento de V, bem como a respectiva subálgebra $\operatorname{Im}\psi$. Temos $\psi(p) = \psi(q)$ se e só se $A \models p = q$. Como A gera V, $A \models p = q$ se e só se $\mathsf{V} \models p = q$. Logo $\operatorname{Ker}\psi = \Theta_{\mathsf{V}}(X)$ e portanto $F_{\mathsf{V}}(X)$ é isomorfo a $\operatorname{Im}\psi$. □

A próxima proposição diz-nos que $F_{\mathcal{K}}(X)$ satisfaz precisamente as identidades em X satisfeitas por $\mathcal{K}$. Logo se X for um conjunto infinito, um único objecto, $F_{\mathcal{K}}(X)$, reúne toda a informação sobre $\mathcal{K}$ que pode ser codificada por identidades satisfeitas por todos os elementos de $\mathcal{K}$.

Proposição 1.21. *Para cada $p, q \in T(X)$, $\mathcal{K} \models p = q$ se e só se $F_{\mathcal{K}}(X) \models p = q$.*

Demonstração. Para a implicação directa basta invocar o lema 1.18. Seja $\nu : T(X) \to F_{\mathcal{K}}(X)$ o homomorfismo canónico. Se $F_{\mathcal{K}}(X) \models p = q$, então $\varphi(p) = \varphi(q)$ para todo o homomorfismo $\varphi : T(X) \to F_{\mathcal{K}}(X)$; em particular $\nu(p) = \nu(q)$. Ora $\operatorname{Ker}\nu = \Theta_{\mathcal{K}}(X) = \{(p, q) \in T(X) \times T(X) : \mathcal{K} \models p = q\}$. □

Consideremos no tipo dos semigrupos um conjunto de variáveis X. Seja Σ o conjunto das identidades em X satisfeitas pelos semigrupos. Para cada $x \in T(X)$ e $n \in \mathbb{N}$, designemos por x^n o termo definido recursivamente pelas regras $x^1 = x$ e $x^{n+1} = x^n \cdot x$. O conjunto $R(X)$ das sequências finitas da forma

$$w = (\cdots((x_{i_1}^{n_{i_1}} \cdot x_{i_2}^{n_{i_2}}) \cdot x_{n_{i_3}}^{n_{i_3}}) \cdot \cdots \cdot x_{i_k}^{n_{i_k}}), \qquad n_{i_j} \in \mathbb{N},\ x_{i_j} \in X,\ x_{i_j} \neq x_{i_{j+1}}$$

é um sistema completo de representantes das classes de equivalência da congruência Σ (i.e., todo o elemento de $T(X)$ é equivalente a um único elemento de $R(X)$). A omissão em w dos parênteses e do símbolo funcional produz uma nova sequência

$$w^{\mathcal{S}} = x_{i_1}^{n_{i_1}} x_{i_2}^{n_{i_2}} x_{i_3}^{n_{i_3}} \cdots x_{i_k}^{n_{i_k}}$$

onde agora $x_{i_j}^{n_{i_j}}$ é uma abreviatura para a repetição de x_{i_j} consecutivamente por n_{i_j} vezes. O conjunto $X^{\mathcal{S}}$ das sequências finitas de elementos de X é constituído por elementos da forma $w^{\mathcal{S}}$, $w \in R(X)$. Em $X^{\mathcal{S}}$, existe uma operação binária de concatenação de sequências:

$$(x_1 \cdots x_n) \cdot (y_1 \cdots y_m) = x_1 \cdots x_n y_1 \cdots y_m$$

Esta operação é obviamente associativa, fazendo portanto de $X^{\mathcal{S}}$ um semigrupo. Trata-se de um semigrupo livre, o que se pode concluir observando que a função

$$\begin{aligned} \rho^{\mathcal{S}} : \quad T(X)/\Sigma &\longrightarrow X^{\mathcal{S}} \\ \overline{w}\ (w \in R(X)) &\longmapsto w^{\mathcal{S}} \end{aligned}$$

é um isomorfismo de álgebras.

Acrescentando a $X^{\mathcal{S}}$ a sequência vazia, denotada por 1, obtemos um conjunto $X^{\mathcal{M}}$ que é um monóide livre para a operação que estende a de $X^{\mathcal{S}}$ da seguinte forma: $w \cdot 1 = 1 \cdot w = w$, $w \in R(X)$ e $1 \cdot 1 = 1$.

Finalmente, considerando o tipo dos grupos, vamos também exibir um modelo sugestivo para o grupo livre sobre um conjunto X de variáveis. Seja então Σ o conjunto das identidades em X satisfeitas pelos grupos. Para cada $x \in T(X)$ e $n \in \mathbb{N}$, designemos por x^n o termo definido pelas regras $x^1 = x$ e $x^{n+1} = x^n \cdot x$; e por x^{-n} o termo $(x^{-1})^n$ (note-se que não há ambiguidade entre o inteiro -1 e o símbolo unário $^{-1}$). O conjunto $R(X)$ formado pelo símbolo 1 (também denotado por x^0) e pelos termos da forma

$$w = (\cdots((x_{i_1}^{n_{i_1}} \cdot x_{i_2}^{n_{i_2}}) \cdot x_{n_{i_3}}^{n_{i_3}}) \cdot \cdots \cdot x_{i_k}^{n_{i_k}}), \qquad n_{i_j} \in \mathbb{Z} \setminus \{0\},\ x_{i_j} \in X,\ x_{i_j} \neq x_{i_{j+1}}$$

é um sistema completo de representantes de $T(X)/\Sigma$ (veja-se, por exemplo, [30, 31] para uma justificação). A omissão em w dos parênteses e do símbolo binário produz uma nova sequência

$$w^{\mathcal{G}} = x_{i_1}^{n_{i_1}} x_{i_2}^{n_{i_2}} x_{i_3}^{n_{i_3}} \cdots x_{i_k}^{n_{i_k}}$$

onde agora $x_{i_j}^{n_{i_j}}$ é uma abreviatura para a repetição de x_{i_j} ou $x_{i_j}^{-1}$ (conforme $n_{i_j} > 0$ ou $n_{i_j} < 0$) consecutivamente por $|n_{i_j}|$ vezes. Designando a sequência vazia por $1^{\mathcal{G}}$, consideremos o conjunto $X^{\mathcal{G}}$ das sequências da forma $w^{\mathcal{G}}$, com $w \in R(X)$. A função

$$\begin{aligned} \rho^{\mathcal{G}} : \quad T(X)/\Sigma &\longrightarrow X^{\mathcal{G}} \\ \overline{w}\ (w \in R(X)) &\longmapsto w^{\mathcal{G}} \end{aligned}$$

é uma bijecção, deste modo definindo em $X^{\mathcal{G}}$ uma operação binária que faz dele um grupo livre. Esta operação não é a simples concatenação: o produto de dois elementos de $X^{\mathcal{G}}$ é a sequência que se obtém da sua concatenação e das sucessivas cancelações de termos consecutivos mutuamente inversos. O elemento neutro de $X^{\mathcal{G}}$ é a sequência vazia $1^{\mathcal{G}}$.

Na prática, quando passamos a lidar apenas com classes de grupos (respectivamente, semigrupos, monóides), em vez de trabalharmos com os termos em X torna-se mais simples trabalharmos com elementos do grupo livre $X^{\mathcal{G}}$ (respectivamente, semigrupo livre $X^{\mathcal{G}}$, monóide livre $X^{\mathcal{M}}$). Deste modo, se Γ for um conjunto de identidades nas variáveis x e y tais que $[\Gamma]$ é a variedade dos grupos, então, por exemplo, $[y^{-1}xy = yx]$ designa a variedade $[\{(y^{-1} \cdot x) \cdot y = y \cdot x\} \cup \Gamma]$.

A *frequência* da variável x num termo p do tipo dos grupos (respectivamente, semigrupos, monóides) tal que $\rho^{\mathcal{G}}(\overline{p})$ (respectivamente, $\rho^{\mathcal{S}}(\overline{p})$, $\rho^{\mathcal{M}}(\overline{p})$) é igual a

$$x_{i_1}^{n_{i_1}} x_{i_2}^{n_{i_2}} x_{i_3}^{n_{i_3}} \cdots x_{i_k}^{n_{i_k}}$$

é o inteiro $\sum_{i_j : x_{i_j} = x} n_{i_j}$, o qual é igual a 0 se $\{i_j : x_{i_j} = x\} = \emptyset$.

Capítulo 2

Operações implícitas

O conceito fundamental que unifica os tópicos abordados ao longo deste capítulo é o de operação implícita. A primeira secção tem um duplo objectivo: a motivação para a introdução deste conceito e, até como meio de fazer esta motivação, a apresentação da noção de potência ómega de um elemento de um semigrupo finito. Serão também abordadas outras operações unárias relacionadas. Ao longo desta monografia iremos apercebermo-nos do modo como a ideia de potência ómega surge naturalmente no contexto do estudo de fenómenos de periodicidade de operadores implícitos sobre álgebras (pro)finitas. A primeira secção servirá por isso também como plataforma de preparação do estudo de tais fenómenos em alguns operadores, estudo este que será efectuado nos dois capítulos seguintes.

Na segunda secção serão concretizadas de forma abstracta as ideias entretanto esboçadas na primeira secção. Embora o nosso interesse último se circunscreva a um leque muito restrito de tipos algébricos, julgamos que se neste caso nos mantivermos sob um registo razoavelmente abstracto então a compreensão dos conceitos abordados será facilitada. Isto porque a especificação do tipo algébrico e da pseudovariedade não será relevante, nem a sua abstracção causará dificuldades adicionais de compreensão, uma vez assimilados os conceitos expostos no primeiro capítulo. No entanto, teremos a preocupação de exibir exemplos concretos, alguns dos quais serão retomados posteriormente. Como o título desta secção indica, as operações implícitas n-árias serão apresentadas como elementos de uma álgebra. Veremos algumas propriedades desta álgebra, nomeadamente de natureza categórica e topológica.

A secção seguinte, a terceira, é o prolongamento natural do estudo topológico da álgebra das operações implícitas. Nesta secção introduziremos a noção de álgebra topológica, bem como a noção mais restrita de álgebra pró-V.

Nas quarta e quinta secções exploramos a propriedade universal da álgebra das operações implícitas n-árias. Esta propriedade começa por ser abordada na segunda secção, mas agora estendemos o âmbito da sua aplicação a todas as álgebras pró-V. Isto permite-nos fazer uma reinterpretação do conceito de operação implícita, alargando a

sua aplicabilidade às álgebras pró-V, tornando deste modo possível a composição de operações implícitas, como veremos.

Na sexta secção damos finalmente uma definição de pseudoidentidade e precisamos a razão (já aflorada na primeira secção) pela qual as pseudoidentidades são uma forma de descrição de pseudovariedades mais adequada do que as identidades.

Na sétima secção introduzimos a noção de operador implícito, para logo a utilizarmos como processo de construção de mais exemplos de operações implícitas. Nesta secção vamos lidar com monóides profinitos de (interpretações de) operadores. Esta é mais uma razão para unificarmos o estudo dos diversos tipos algébricos. Ainda encontramos mais uma outra razão para esta unificação na oitava e última secção, dedicada às álgebras das operações implícitas unárias sobre as pseudovariedades dos semigrupos, monóides, grupos finitos, respectivamente; elas são, respectivamente, um semianel, um semianel com zero e um anel profinito. O conhecimento de alguns aspectos aritméticos do anel profinito $\overline{\Omega}_1\mathsf{G}$ das operações implícitas unárias sobre a pseudovariedade dos grupos finitos, e que é uma extensão de $\mathbb{Z}$, será necessário para o posterior estudo (a realizar no terceiro capítulo) de operadores implícitos invertíveis em determinadas pseudovariedades de grupos. O trabalho efectuado na sétima secção permitirá que na última secção possamos dar alguns exemplos interessantes de elementos de $\overline{\Omega}_1\mathsf{G}$, e de relações aritméticas entre eles. Estaremos então motivados para analisar alguns aspectos básicos da aritmética do anel $\overline{\Omega}_1\mathsf{G}$, de que destacamos uma condição necessária e suficiente para a invertibilidade de um elemento e a exibição de um sistema completo de primos não associados entre si. Esta análise de $\overline{\Omega}_1\mathsf{G}$ foi feita sem o auxílio de uma bibliografia (para além daquela que trata dos anéis em geral), não obstante na pesquisa efectuada terem-se encontrados apontamentos sobre outras propriedades relevantes de $\overline{\Omega}_1\mathsf{G}$, mas que não tinham o pendor aritmético que procurávamos. Esta situação parece indiciar que a aritmética de $\overline{\Omega}_1\mathsf{G}$ já foi estudada há muito tempo, tendo entretanto caído no esquecimento. Ao fazermos o estudo de $\overline{\Omega}_1\mathsf{G}$ também retiraremos algumas conclusões a respeito dos semianéis $\overline{\Omega}_1\mathsf{S}$ e $\overline{\Omega}_1\mathsf{M}$ das operações implícitas sobre as pseudovariedades dos semigrupos finitos e dos monóides finitos, respectivamente. A sustentação bibliográfica de parte da última secção é portanto um problema por cuja resolução humildemente aguardamos, numa espera activa.

As referências bibliográficas mais significativas para a sustentação deste capítulo são: [1, 27] para a primeira secção; [4] para as quatro secções seguintes; [3, 5, 2] para as duas últimas. Outras referências pontuais serão dadas na devida altura.

2.1 A potência ómega

Como seria de esperar, no estudo de álgebras finitas ganham particular relevo as propriedades combinatórias dos conjuntos finitos [1]. Vamos dar a seguir um exemplo disso.

Proposição 2.1. *Seja S um semigrupo. Dado um elemento a de S que gera um subsemigrupo finito, existem inteiros positivos n e k tais que $a^n = a^{n+k}$ e que verificam as seguintes propriedades:*

1. *Para todo $l \in \mathbb{N}_0$, o resto r da divisão de l por k é o único elemento do conjunto $\{0, 1, \ldots, k-1\}$ tal que $a^{n+l} = a^{n+r}$;*
2. *Para todos $m \in \mathbb{N}$, $l_1, l_2 \in \mathbb{N}_0$, se $a^{m+l_1} = a^{m+l_2}$ então $l_1 \equiv l_2 \pmod{k}$;*
3. *Para todos os inteiros m, l positivos, $a^m = a^{m+l}$ se e só se m é maior ou igual a n e k divide l;*
4. *O subsemigrupo $\langle a \rangle$ tem $n + k - 1$ elementos e $\langle a \rangle = \{a, a^2, \ldots, a^{n+k-1}\}$.*

Demonstração. Como o subsemigrupo gerado por a é finito, existem inteiros positivos m e l tais que $a^m = a^{m+l}$. Seja n o menor desses inteiros positivos m, e seja k o menor dos inteiros positivos l tais que $a^n = a^{n+l}$. Se $l \geq k$, então $l = qk + r$ para alguns inteiros q e r tais que $q \geq 1$ e $0 \leq r < k$. Então,

$$a^{n+l} = a^{n+qk+r} = a^{n+k+(q-1)k+r} = a^{n+(q-1)k+r} = \ldots = a^{n+r}.$$

Em particular, se k divide l então $a^{n+l} = a^n$. Para a demonstração da alínea 1 ficar completa, falta apenas provar a unicidade de r, o que será feito em simultâneo com a demonstração da alínea 2.

Suponhamos então que $a^{m+l_1} = a^{m+l_2}$, $m \in \mathbb{N}_0$, $l_2 > l_1 \geq 0$. Seja $t \in \mathbb{N}$ tal que $n + tk > m + l_1$. Multiplicando ambos os membros da igualdade $a^{m+l_1} = a^{m+l_2}$ por $a^{n+tk-(m+l_1)}$ obtemos $a^{n+tk} = a^{n+tk+l_2-l_1}$. Seja r o resto da divisão de $l_2 - l_1$ por k. Então, pelo que já demonstrámos no parágrafo precedente, $a^n = a^{n+r}$. Pela minimalidade de k, $r = 0$. Isto termina a demonstração das alíneas 1 e 2.

A implicação directa da alínea 3 resulta da minimalidade de n e da alínea 2; a recíproca resulta da alínea 1.

A igualdade $\langle a \rangle = \{a, a^2, \ldots, a^{n+k-1}\}$ é uma consequência imediata da alínea 1. Suponhamos que i e j são elementos de $\{1, 2, \ldots, n+k-1\}$ tais que $i < j$ e $a^i = a^j$. Pela minimalidade de n, $i \geq n$. Como $a^{n+(i-n)} = a^{n+(j-n)}$, pela alínea 2, k divide $j - i$. Mas $n \leq i < j \leq n + k - 1 \Rightarrow 0 < j - i < k$, pelo que k não divide $j - i$, o que é uma contradição. Logo $|\langle a \rangle| = n + k - 1$. □

Se S é um semigrupo e $a \in S$ gera um subsemigrupo finito, então os menores inteiros positivos n e k tais que $a^n = a^{n+k}$ são referidos como o *índice* e o *período* de a, respectivamente. Vamos agora supor que S também tem uma estrutura de monóide. O menor elemento m de $\mathbb{N}_0$ para o qual existe $l \in \mathbb{N}$ tal que $a^m = a^{m+l}$ é igual ao índice de a se o elemento neutro 1 de S não pertencer ao subsemigrupo de S gerado por a, e é igual a 0 se 1 pertencer a esse subsemigrupo.[1] O inteiro m será referido como sendo o *pré-período* de a. Notemos que o menor inteiro positivo l tal que $a^m = a^{m+l}$ é precisamente o período de a: no caso em que $m = 0$ isto é verdade

[1] Como é usual, a potência de expoente nulo a^0 designa o elemento neutro 1.

porque $1 = a^l \Leftrightarrow a = a^{1+l}$; com efeito, se $r \in \mathbb{N}$ for tal que $a^r = 1$, então temos $a = a^{1+l} \Rightarrow a^{r-1}a = a^{r-1}a^{l+1} \Rightarrow 1 = a^l$. Observemos também que as três primeiras propriedades da proposição 2.1 permanecem válidas mesmo quando $n = 0$ ou $m = 0$, e que, pela mesma proposição, o submonóide de S gerado por a tem $n + k$ elementos (se o elemento neutro de S não pertencer ao subsemigrupo gerado por a então basta acrescentar uma unidade à ordem desse subsemigrupo; se, pelo contrário, pertencer, então basta observar que nesse caso o índice é igual a 1).

Os fenómenos de periodicidade que temos vindo a descrever podem ser vistos como fenómenos de periodicidade de transformações de um conjunto nele próprio. Aquilo que nos permite fazer a passagem para este ponto de vista é o facto de que, dado um monóide M, se M^M designar o monóide das funções $M \to M$, então a função

$$\begin{aligned} \varrho_M : M &\longrightarrow M^M \\ a &\longmapsto \rho_a : x \in M \mapsto ax \end{aligned}$$

é um homomorfismo injectivo de monóides. Neste sentido, todo o monóide é um submonóide de um monóide de transformações.[2] A função ϱ_M permite concretizar a descrição dos fenómenos de periodicidade do submonóide de M gerado por um seu elemento a enquanto fenómenos de periodicidade de uma função, ou de uma órbita de um ponto por uma função, pois

$$a^m = a^{m+l} \Leftrightarrow \rho_{a^m} = \rho_{a^{m+l}} \Leftrightarrow \rho_a^m = \rho_a^{m+l}$$

e a sucessão das sucessivas potências de a é precisamente a órbita de 1 por ρ_a.

Este tipo de considerações pode ser alargado ao âmbito mais geral dos semigrupos através da seguinte construção típica. Dado um semigrupo S, consideramos um monóide S^1 cujo universo é constituído por S e por um elemento 1 que não está em S, e cuja operação binária estende a de S e tem 1 como elemento neutro. Como ϱ_{S^1} é um homomorfismo injectivo de monóides, e portanto de semigrupos, o semigrupo S é isomorfo ao subsemigrupo $\varrho_{S^1}(S)$ de $(S^1)^{S^1}$. Neste sentido, podemos dizer que todo o semigrupo é um subsemigrupo de um semigrupo de funções.

Dada uma função $f : A \to A$ e um elemento a de A, os elementos da órbita de a por f formam um monóide $\mathcal{O}_a(f)$ para operação $*$ seguinte:

$$f^i(a) * f^j(a) = f^{i+j}(a),\ i, j \in \mathbb{N}_0.$$

A i-ésima potência de $f(a)$ em $\mathcal{O}_a(f)$ é precisamente $f^i(a)$. O elemento neutro deste monóide é a. Se $\mathcal{O}_a(f)$ for finito, então o pré-período e o período da órbita de f por a são, respectivamente, o pré-período e o período de $f(a)$ em $\mathcal{O}_a(f)$.

Lema 2.2. *Consideremos um conjunto finito A e uma função $f : A \to A$. Sejam n e k o pré-período e o período de f, respectivamente. Para cada $a \in A$, sejam n_a e k_a o pré-período e o período da órbita de a por f, respectivamente. Então,*

$$n = \max\{n_a : a \in A\} \quad e \quad k = \text{m. m. c.}\{k_a : a \in A\}.$$

[2] Trata-se de um análogo do Teorema de Cayley da Teoria dos Grupos, o qual nos diz que todo o grupo é um subgrupo de um grupo de permutações.

Demonstração. Sejam então $n_0 = \max\{n_a : a \in A\}$ e $k_0 = \text{m.m.c.}\{k_a : a \in A\}$. Fixemos $a \in A$. Em $\mathcal{O}_a(f)$ temos a igualdade

$$f(a)^{n_0} = f(a)^{n_0+k_0},$$

ou seja,

$$f^{n_0}(a) = f^{n_0+k_0}(a).$$

Como a é arbitrário, $f^{n_0} = f^{n_0+k_0}$, pelo que $n \leq n_0$ e k divide k_0. Por outro lado, para qualquer $a \in A$ temos

$$f^n(a) = f^{n+k}(a),$$

ou seja, em $\mathcal{O}_a(f)$ verifica-se a seguinte igualdade:

$$f(a)^n = f(a)^{n+k}.$$

Logo $n_a \leq n$ e k_a divide k. Como a é arbitrário, $n_0 \leq n$ e k_0 divide k. Logo $n_0 = n$ e $k_0 = k$. □

Um outro exemplo da importância da Combinatória no estudo das álgebras finitas, e que vem na sequência da proposição 2.1, é o da existência de idempotentes em semigrupos finitos. Um idempotente de um semigrupo S é um elemento e tal que $e^2 = e$.

Proposição 2.3. *Se S é um semigrupo gerado por um dos seus elementos, então S é isomorfo a $(\mathbb{N}, +)$, ou então é finito e tem um único idempotente.*

Demonstração. Seja a um gerador de S. Se todas as potências de a forem distintas, então é claro que $a^n \in S \mapsto n \in \mathbb{N}$ é um isomorfismo. Senão, S é finito. Nesse caso, sejam n o índice e k o período de a. O conjunto $G = \{a^{n+i} : i \in \mathbb{N}_0\}$ é um subsemigrupo de S. Pela proposição 2.1, a função

$$\begin{aligned} G &\longrightarrow \mathbb{Z}_k \\ a^{n+i}, i \in \mathbb{N}_0 &\longmapsto [n+i]_k \end{aligned}$$

está bem definida. Esta função é um homomorfismo de semigrupos, e segue directamente da proposição 2.1 que se trata de uma bijecção. Logo G é um grupo, e o seu elemento neutro e é um idempotente de S. Se b é um elemento de S, então $b^n \in G$; em particular, se f é um idempotente de S, então $f = f^n \in G$ e portanto $f = e$. □

Notemos que na proposição 2.3 a condição de finitude é crucial para a existência de um idempotente: o semigrupo aditivo $\mathbb{N}$ não tem idempotentes.

Ainda sob a hipótese de que o elemento a gera um subsemigrupo finito do semigrupo S, denotemos por a^ω o único idempotente de $\langle a \rangle$, literalmente a *potência ómega de a*. Seja $t \in \mathbb{N}$ tal que $a^\omega = a^t$. Como a^ω é um idempotente, $a^\omega = a^t = (a^t)^r = a^{tr}$ para todo $r \geq 1$. Em particular, $a^\omega = a^{m!}$ se $m \geq t$. Logo a sucessão $(a^{m!})_{m \in \mathbb{N}}$ é quase-constante

igual a a^ω, o que é equivalente a dizer que converge para a^ω na topologia discreta de S. Decorre da demonstração da proposição 2.3 que o conjunto

$$G = \{a^m : m \text{ é maior igual ao índice de } a\}$$

é um grupo[3] cujo elemento neutro é a^ω. Se $k \in \mathbb{N}$, então $a^\omega a^k$ é um elemento de G; designamo-lo por $a^{\omega+k}$, e ao seu inverso em G por $a^{\omega-k}$. Esta convenção de notações estende-se naturalmente a $k = 0$: $a^{\omega+0}$ designa a^ω. Para qualquer $k \in \mathbb{Z}$, a sucessão $(a^{m!+k})_{m>|k|}$ converge para $a^{\omega+k}$ na topologia discreta de S.

Notemos que se S for um grupo então $a^\omega = 1$, uma vez que o elemento neutro é o único idempotente de um grupo. Em geral, a invertibilidade[4] de um elemento de um monóide finito está relacionada com a sua potência ómega:

Lema 2.4. *Sejam M um monóide finito e x um elemento de M. As seguintes condições são equivalentes:*

1. *x é invertível;*
2. *existe $y \in M$ tal que $yx = 1$;*
3. *existe $y \in M$ tal que $xy = 1$;*
4. *$x^\omega = 1$.*

Demonstração. As implicações $1 \Rightarrow 2$ e $1 \Rightarrow 3$ são triviais. Suponhamos que existe $y \in M$ tal que $yx = 1$. Então a função $z \in M \mapsto xz \in M$ é injectiva, pois

$$xu = xv \Rightarrow yxu = yxv \Rightarrow u = v.$$

Como M é finito, essa mesma função é sobrejectiva, pelo que existe $z \in M$ tal que $xz = 1$. Ora $z = (yx)z = y(xz) = y$, o que mostra a implicação $2 \Rightarrow 1$. A demonstração da implicação $3 \Rightarrow 1$ é análoga.

Suponhamos agora que existe $y \in M$ tal que $xy = yx = 1$. Como x e y comutam, $x^k y^k = (xy)^k = 1$, para qualquer $k \in \mathbb{N}$. Então, e como x^ω é um idempotente,

$$x^\omega = x^\omega x^\omega y^\omega = x^\omega y^\omega = 1$$

o que mostra $1 \Rightarrow 4$. Finalmente, se $x^\omega = 1$ então $x^{\omega-1}$ é inverso de x. □

Se o semigrupo S for finito, então para cada $k \in \mathbb{Z}$ podemos considerar em S a operação unária

$$\begin{aligned} (\pi_k)_S : S &\longrightarrow S \\ s &\longmapsto s^{\omega+k} \end{aligned}$$

[3]Todo o subsemigrupo de $\langle a \rangle$ que é um grupo está contido em G, o qual, por essa razão, é normalmente designado como o *subgrupo maximal* de $\langle a \rangle$.

[4]Um elemento x de um monóide M é invertível se e só se existe $y \in M$ tal que $xy = yx = 1$. O elemento y, que facilmente se mostra ser único, é o inverso de x.

Se $\varphi : S \to T$ for um homomorfismo entre semigrupos finitos, então

$$\varphi(a^{\omega+k}) = \varphi(\lim_{m\to+\infty} a^{m!+k}) = \lim_{m\to+\infty} \varphi(a^{m!+k}) = \lim_{m\to+\infty} \varphi(a)^{m!+k} = \varphi(a)^{\omega+k}.$$

Ou seja, o diagrama (2.1) é comutativo.

$$\begin{array}{ccc} S & \xrightarrow{(\pi_k)_S} & S \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ T & \xrightarrow{(\pi_k)_T} & T \end{array} \tag{2.1}$$

A comutatividade do diagrama (2.1) impõe a seguinte questão: existirá algum termo unário p do tipo dos semigrupos tal que $p_S = (\pi_k)_S$ para todo o semigrupo finito S? No caso particular da operação π_0 é fácil fazer a ligação entre esta questão e o conceito de pseudovariedade equacional. Uma pseudovariedade V de tipo τ diz-se *equacional* se existir alguma variedade $\mathcal{V}$ de tipo τ tal que V é a classe $\mathcal{V}^F$ das álgebras finitas de $\mathcal{V}$. Pelo teorema de Birkhoff, uma pseudovariedade é equacional se e só se existe um conjunto Σ de identidades para o qual, qualquer que seja a álgebra finita A, nós temos $A \in \mathsf{V} \Leftrightarrow A \models \Sigma$. Se existisse algum termo unário p do tipo dos semigrupos tal que $p_S(a) = a^\omega$ para todo o elemento a de todo o semigrupo finito S, então, encarando p como um termo do tipo dos monóides, a pseudovariedade do tipo dos monóides dos grupos finitos seria equacional: com efeito, pelo lema 2.4 teríamos $\mathsf{G} = [p = 1]^F$. Vamos ver que tal não acontece:

Lema 2.5. *Seja τ o tipo algébrico dos grupos, dos monóides ou dos semigrupos. Sejam p e q termos de tipo τ num conjunto de variavéis X. Se existir uma infinidade de grupos finitos de ordem prima onde a identidade $p = q$ é válida, então todas as variáveis de X têm a mesma frequência em p e q.*

Demonstração. Para cada $i \in \{1, \ldots, n\}$, sejam ε_i e δ_i a frequência de x_i em p e q, respectivamente. Seja k um primo tal que $\mathbb{Z}_k \models p = q$. Então, substituindo em p e q as variáveis distintas de x_i por $[0]_k$ e a variável x_i por $[1]_k$, obtemos a igualdade $[\varepsilon_i]_k = [\delta_i]_k$. Ou seja, k divide $\varepsilon_i - \delta_i$. Como $\varepsilon_i - \delta_i$ é divisível por uma infinidade de primos, $\varepsilon_i = \delta_i$. □

Corolário 2.6. *Seja τ o tipo algébrico dos grupos, dos monóides ou dos semigrupos. Sejam p e q termos de tipo τ num conjunto de variavéis X. Se existir uma infinidade de grupos finitos de ordem prima onde a identidade $p = q$ é válida, então todas as álgebras comutativas de tipo τ satisfazem a identidade $p = q$.*

Como existem monóides comutativos finitos que não são grupos, a pseudovariedade do tipo dos monóides G não é equacional. Consequentemente, G também não é equacional enquanto pseudovariedade do tipo dos semigrupos. Concluímos também que não existe nenhum termo unário p do tipo dos semigrupos tal que $p_S = (\pi_0)_S$. Podemos aliás da forma que se segue concluir directamente que, para qualquer $k \in \mathbb{Z}$, não existe nenhum

termo unário p do tipo dos semigrupos tal que $p_S = (\pi_k)_S$. Com efeito, se existisse, um tal p seria da forma x^n, onde x é uma variável e $n \in \mathbb{N}$. Consequentemente, para qualquer elemento a de um semigrupo finito teríamos $a^{\omega+k} = a^n$. Mas tal não se verifica se a tiver índice maior do que n.

Apesar da pseudovariedade dos grupos finitos não ser equacional nos tipos dos semigrupos e dos monóides, ela fica completamente caracterizada à custa da operação π_0, pela igualdade $x^\omega = 1$, a qual, no caso do tipo dos semigrupos, é uma abreviatura da cadeia de igualdades $x^\omega y = yx^\omega = y$, onde y é uma variável distinta de x; observemos também que a operação π_0 comuta com homomorfismos. Este exemplo mostra-nos como os conceitos de termo e de identidade são de certa forma inadequados como meio de descrição de pseudovariedades.

Terminamos com mais um exemplo desta falta de adequação, com a diferença de que agora vamos estar perante uma operação binária. Este exemplo é de particular interesse para a segunda parte desta monografia. Dado um grupo G, consideremos a função

$$\begin{aligned} f: \quad G^2 &\longrightarrow G^2 \\ (x,y) &\longmapsto (xyx^{-1}y^{-1}, y) \end{aligned}$$

Esta função é um elemento do monóide $(G^2)^{G^2}$ das funções $G^2 \to G^2$. Se G for finito, então $(G^2)^{G^2}$ também o é, pelo que f admite uma potência ómega. Seja $[x, {}_\omega y]$ a primeira componente de $f^\omega(x,y)$. A operação binária $(x,y) \mapsto [x, {}_\omega y]$, definível em grupos finitos, comuta com homomorfismos. Iremos mostrar no capítulo 4 que a pseudovariedade $\mathsf{G_{nil}}$ dos grupos nilpotentes finitos caracteriza-se pela propriedade $[x, {}_\omega y] = 1$. Contudo, $\mathsf{G_{nil}}$ não é equacional no tipo dos grupos, pois Baumslag demonstrou em [7] que se uma identidade do tipo dos grupos é válida em todos os p-grupos finitos, então é válida em todos os grupos.

2.2 A álgebra das operações implícitas n-árias

A secção anterior deu-nos a motivação para o percurso que vamos efectuar ao longo do resto deste capítulo.

Fixemos uma pseudovariedade V. Como cada membro de V é finito, podemos formar um conjunto $\mathsf{V_0}$ que seja um sistema completo de representantes das classes de isomorfismo de elementos de V (i.e., todo o elemento de V é isomorfo a um único elemento de $\mathsf{V_0}$). Para cada $n \in \mathbb{N}$, também podemos formar o conjunto $\mathrm{Imp}_n \mathsf{V_0}$ de todas as famílias $(\pi_A)_{A \in \mathsf{V_0}}$ de funções $\pi_A : A^n \to A$ que tornam o diagrama (2.2) comutativo para qualquer homomorfismo $\varphi : A \to B$ entre elementos de $\mathsf{V_0}$.

$$\begin{array}{ccc} A^n & \xrightarrow{\pi_A} & A \\ {\scriptstyle \varphi^{(n)}}\downarrow & & \downarrow{\scriptstyle \varphi} \\ B^n & \xrightarrow{\pi_B} & B \end{array} \tag{2.2}$$

Lema 2.7. *Cada família* $(\pi_A)_{A\in \mathsf{V}_0}$ *é uma subfamília de uma única família* $(\pi_A)_{A\in \mathsf{V}}$ *de funções* $\pi_A : A^n \to A$ *que tornam o diagrama* (2.2) *comutativo para quaisquer elementos de* V.

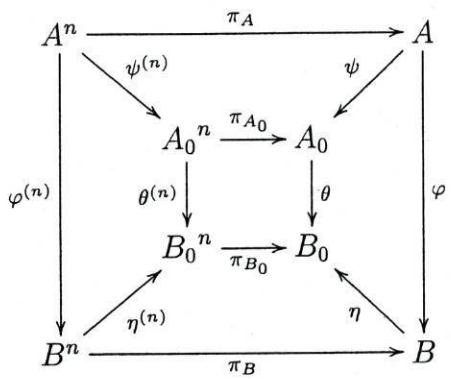
Demonstração. Se $A \in \mathsf{V}$ e $\psi : A \to A_0 \in \mathsf{V}_0$ é um isomorfismo, então π_A tem uma única definição possível, como se constata no diagrama (2.3).

$$\begin{array}{ccc} {A_0}^n & \xrightarrow{\pi_{A_0}} & A_0 \\ \uparrow{\scriptstyle \psi^{(n)}} & & \uparrow{\scriptstyle \psi} \\ A^n & \xrightarrow[\pi_A=\psi^{-1}\circ\pi_{A_0}\circ\psi^{(n)}]{} & A \end{array} \tag{2.3}$$

Esta definição não depende de ψ. Se $\eta : A \to A_0$ também for um isomorfismo, então como $\eta \circ \psi^{-1}$ é um automorfismo de A_0 e $A_0 \in \mathsf{V}_0$, o quadrado exterior do diagrama (2.4) comuta, e como tal também acontece com o rectângulo superior, ainda acontece com o inferior:

$$\begin{array}{ccc} {A_0}^n & \xrightarrow{\pi_{A_0}} & A_0 \\ \uparrow{\scriptstyle \psi^{(n)}} & & \downarrow{\scriptstyle \psi^{-1}} \\ A^n & \xrightarrow[\psi^{-1}\circ\pi_{A_0}\circ\psi^{(n)}]{} & A \\ \uparrow{\scriptstyle (\eta^{-1})^{(n)}} & & \downarrow{\scriptstyle \eta} \\ {A_0}^n & \xrightarrow{\pi_{A_0}} & A_0 \end{array} \tag{2.4}$$

Finalmente, seja B outro elemento de V e sejam B_0 a álgebra de V_0 isomorfa a B e $\eta : B \to B_0$ um isomorfismo. Então, para todo o homomorfismo $\varphi : A \to B$, se θ for o homomorfismo $\eta \circ \varphi \circ \psi^{-1}$, o quadrado exterior do diagrama (2.5) comuta, pois todos os polígonos interiores comutam:



(2.5)

□

Uma família $(\pi_A)_{A\in \mathsf{V}}$ que comuta com homomorfismos é denominada de *operação implícita n-ária* sobre V. Pelo lema 2.7, podemos formar o conjunto $\mathrm{Imp}_n \mathsf{V}$ de todas

as operações implícitas n-árias sobre V e afirmar que

$$(\pi_A)_{A\in\mathsf{V}} \in \mathrm{Imp}_n\,\mathsf{V} \mapsto (\pi_A)_{A\in\mathsf{V}_0} \in \mathrm{Imp}_n\,\mathsf{V}_0$$

é uma bijecção.

Se p for um termo n-ário, então $(p_A)_{A\in\mathsf{V}} \in \mathrm{Imp}_n\,\mathsf{V}$ e se q também for um termo n-ário então $(p_A)_{A\in\mathsf{V}} = (q_A)_{A\in\mathsf{V}}$ se e só se $\mathsf{V} \models p = q$. A uma operação implícita n-ária $(p_A)_{A\in\mathsf{V}}$ obtida a partir de um termo n-ário p (que, como vimos, não é necessariamente único), chamamos *operação explícita n-ária.* Podem existir operações implícitas que não são explícitas. Exemplos disso são as operações unárias $x^{\omega+k}$, $k \in \mathbb{Z}$, na pseudovariedade dos semigrupos finitos, ou a operação binária $[x, {}_\omega y]$ na pseudovariedade dos grupos finitos.

Fixemos um conjunto $X = \{x_1, \ldots, x_n\}$ de n variáveis distintas. Podemos identificar o conjunto A^n com o conjunto A^X das funções $X \to A$, identificando o vector $\vec{a} = (a_1, \ldots, a_n) \in A^n$ com a função $\alpha : x_i \in X \to a_i \in A$. Reparemos que ao fazermos esta identificação entre A^X e A^n estamos de certo modo a ordenar os elementos de X. Dadas funções $f : A^n \to A$ e $\varphi : A \to B$ usaremos as notações $f(\alpha)$ e $\varphi \circ \alpha$ para $f(\vec{a})$ e $\varphi^{(n)}(\vec{a})$, respectivamente.

Vimos como uma operação implícita n-ária $\pi = (\pi_A)_{A\in\mathsf{V}}$ fica determinada se conhecermos as funções $\pi_A : A^n \to A$, $A \in \mathsf{V}_0$. Por outro lado, quando A é uma álgebra de V, a função $\pi_A : A^n \to A$ fica determinada se para cada $\alpha \in A^X$ conhecermos $\pi_A(\alpha)$; além disso $\pi_A(\alpha) = \pi_{\langle\alpha(X)\rangle}(\alpha)$ pois π comuta com o homomorfismo de inclusão $\langle\alpha(X)\rangle \to A$. Isto leva-nos a considerar o conjunto I dos pares (A, α) formado por álgebras de V_0 e funções geradoras $\alpha : X \to A$. Ao pormos em evidência a propriedade que caracteriza a família $(\pi_A)_{A\in\mathsf{V}}$ como operação implícita n-ária, verificamos que $\pi = (\pi_A(\alpha))_{(A,\alpha)\in I}$ é elemento dos conjuntos

$$F_{((B,\beta),(C,\gamma))} = \{(x_{(A,\alpha)})_{(A,\alpha)\in I} \in \prod_{(A,\alpha)\in I} A : \theta_{C,B}(x_{(C,\gamma)}) = x_{(B,\beta)}$$
$$\text{se } \theta_{C,B} : C \to B \text{ é um homomorfismo tal que } \theta_{C,B} \circ \gamma = \beta\}$$

e que portanto é elemento da sua intersecção

$$\overline{\Omega}_X\mathsf{V}_0 = \bigcap_{\substack{(B,\beta)\in I\\(C,\gamma)\in I}} F_{((B,\beta),(C,\gamma))}.$$

Pelo lema 1.6, como γ gera C, o homomorfismo $\theta_{C,B}$ se existir é único. É um exercício de rotina mostrar que $\overline{\Omega}_X\mathsf{V}_0$ é uma subálgebra de $\prod_{(A,\alpha)\in I} A$.

Lema 2.8. *A função*

$$\begin{aligned}\zeta_{\mathsf{V}_0} : \ \mathrm{Imp}_n\,\mathsf{V} &\longrightarrow \overline{\Omega}_X\mathsf{V}_0\\ (\pi_A)_{A\in\mathsf{V}} &\longmapsto (\pi_A(\alpha))_{(A,\alpha)\in I}\end{aligned}$$

é uma bijecção.

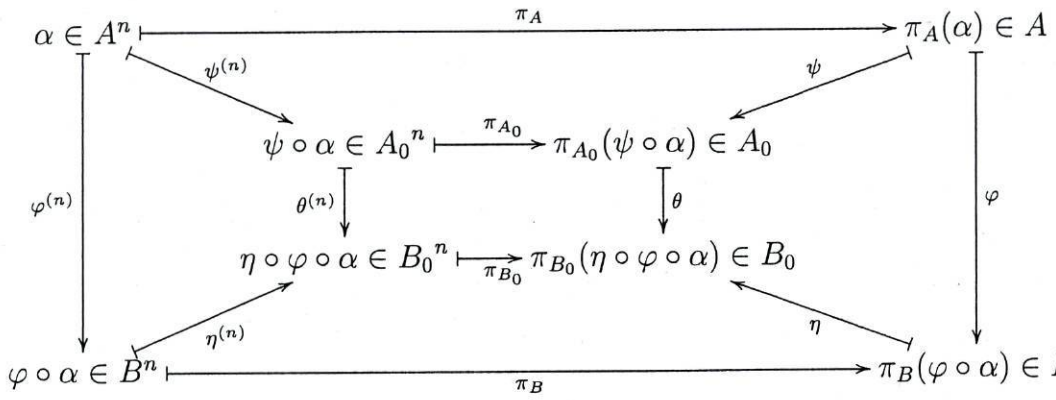
Demonstração. Seja $(x_{(A,\alpha)})_{(A,\alpha)\in I} \in \overline{\Omega}_X \mathsf{V}_0$. Vamos definir uma família $(\pi_A)_{A\in\mathsf{V}}$ de funções $\pi_A : A^n \to A$ através dos seguintes dois passos:

1. Se $(A,\alpha) \in I$ então $\pi_A(\alpha) = x_{(A,\alpha)}$.
2. Se $A \in V$, $\alpha \in A^X \approx A^n$ e $\psi : \langle \alpha(X)\rangle \to A_0 \in \mathsf{V}_0$ for um isomorfismo, então $\pi_A(\alpha) = \psi^{-1}(\pi_{A_0}(\psi \circ \alpha))$.[5]

Esta definição não depende da escolha de ψ, como ilustra o diagrama (2.6), o qual é uma emulação da comutatividade do diagrama (2.4)[6]: o quadrado exterior comuta porque $(A_0, \psi\circ\alpha), (A_0, \eta\circ\alpha) \in I$ e $(x_{(A,\alpha)})_{(A,\alpha)\in I} \in \overline{\Omega}_X \mathsf{V}_0$, e como o rectângulo superior comuta, tal também acontece com o inferior, ou seja, $\eta(\psi^{-1}(\pi_{A_0}(\psi \circ \alpha))) = \pi_A(\eta \circ \alpha)$.

$$\begin{array}{ccc}
\psi \circ \alpha \in {A_0}^n & \xrightarrow{\pi_{A_0}} & \pi_{A_0}(\psi \circ \alpha) \in A_0 \\
{\scriptstyle \psi^{(n)}}\uparrow & & \downarrow{\scriptstyle \psi^{-1}} \\
\alpha \in A^n & \xrightarrow[\psi^{-1}\circ\pi_{A_0}\circ\psi^{(n)}]{} & \psi^{-1}(\pi_{A_0}(\psi \circ \alpha)) \in A \\
{\scriptstyle (\eta^{-1})^{(n)}}\uparrow & & \downarrow{\scriptstyle \eta} \\
\eta \circ \alpha \in {A_0}^n & \xrightarrow{\pi_{A_0}} & \pi_{A_0}(\eta \circ \alpha) \in A_0
\end{array} \tag{2.6}$$

Dados um par de álgebras $A, B \in \mathsf{V}$, um homomorfismo $\varphi : A \to B$, e um elemento α de $A^X \approx A^n$, sejam $\psi : \langle \alpha(X)\rangle \to A_0 \in \mathsf{V}_0$ e $\eta : \langle \varphi \circ \alpha(X)\rangle \to B_0 \in \mathsf{V}_0$ isomorfimos. Para $\theta = \eta \circ \varphi \circ \psi^{-1}$, o diagrama (2.7) comuta, logo $(\pi_A)_{A\in\mathsf{V}} \in \mathrm{Imp}_n \mathsf{V}$.



(2.7)

Por construção, $\zeta_{\mathsf{V}_0}^{-1}(\{(x_{(A,\alpha)})_{(A,\alpha)\in I}\}) = \{(\pi_A)_{A\in\mathsf{V}}\}$. □

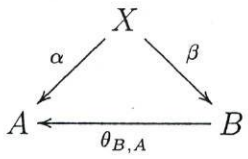
Se V_1 for um outro sistema completo de representantes das classes de isomorfismo de elementos de V, a bijecção $\zeta_{\mathsf{V}_1}^{-1} \circ \zeta_{\mathsf{V}_0} : \overline{\Omega}_X \mathsf{V}_0 \to \overline{\Omega}_X \mathsf{V}_1$ é um isomorfismo. Estamos

[5] A_0 depende portanto de α.

[6] A dependência de A_0 em relação a α impede uma utilização directa da comutatividade do quadrado exterior do diagrama (2.4).

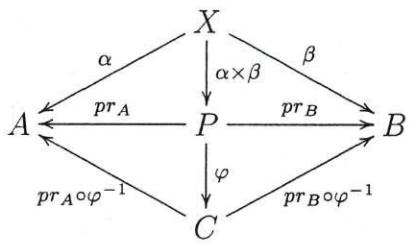
então justificados para denotar $\overline{\Omega}_X \mathsf{V}_0$ por $\overline{\Omega}_X \mathsf{V}$ e designar os seus elementos como operações implícitas n-árias, identificando-os com os elementos de $\mathrm{Imp}_n \mathsf{V}$ através da bijecção ζ_{V_0}. A álgebra $\overline{\Omega}_X \mathsf{V}$ é a *álgebra das operações implícitas n-árias sobre* V.

O conjunto I admite a ordem parcial $\leq$ se estipularmos que $(A, \alpha) \leq (B, \beta)$ se e só se existe um (único) homomorfismo $\theta_{B,A} : B \to A$ que torne comutativo o diagrama (2.8).



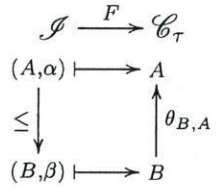
(2.8)

Dados $(A, \alpha), (B, \beta) \in I$, se P for a subálgebra de $A \times B$ gerada pela função $\alpha \times \beta$ e se $\varphi : P \to C \in \mathsf{V}_0$ for um isomorfismo então $\gamma = \varphi \circ (\alpha \times \beta)$ é tal que $(C, \gamma) \in I$, $(A, \alpha) \leq (C, \gamma)$ e $(B, \beta) \leq (C, \gamma)$, como se depreende do diagrama (2.9) (onde pr_A e pr_B são as projecções canónicas). Concluímos que o conjunto ordenado $(I, \leq)$ é *dirigido*, ou *filtrante* [21].



(2.9)

Somos levados a considerar o seguinte functor F da categoria $\mathscr{I}$ do conjunto ordenado $(I, \leq)$ na categoria $\mathscr{C}_\tau$ das álgebras de tipo τ:



O functor F constitui um sistema projectivo, e a álgebra $\overline{\Omega}_X \mathsf{V}$ é o limite projectivo de F:

$$\overline{\Omega}_X \mathsf{V} = \varprojlim_{(A,\alpha) \in I} A$$

Exemplo 2.9. *Na pseudovariedade* G *dos grupos finitos, consideremos um sistema de representantes que inclua os grupos cíclicos* $\mathbb{Z}_n$, $n \in \mathbb{N}$. *A álgebra das operações implícitas n-árias sobre* G *é o grupo* $\varprojlim_{(\mathbb{Z}_n,\alpha) \in I} \mathbb{Z}_n$. *Como a escolha dos geradores de* $\mathbb{Z}_n$ *é simétrica, é natural que consideremos o subconjunto* J *de* I *formado pelos pares constituídos por um grupo* $\mathbb{Z}_n$ *e pelo gerador* $[1]_n$ *de* $\mathbb{Z}_n$. *Este subconjunto é cofinal*[7]

[7]Um subconjunto J de um conjunto ordenado $(I, \leq)$ é *cofinal* em I se $\forall i \in I, \exists j \in J : i \leq j$.

em I, pelo que a projecção canónica é um isomorfismo entre o grupo $\varprojlim_{(\mathbb{Z}_n,\alpha)\in I} \mathbb{Z}_n$ e o grupo $\widehat{\mathbb{Z}} = \varprojlim_{(\mathbb{Z}_n,[1]_n)\in J} \mathbb{Z}_n$. Notemos que existe um homomorfismo $\theta_{n,m}$ de $\mathbb{Z}_n$ para $\mathbb{Z}_m$ tal que $\theta_{n,m}([1]_n) = [1]_m$ se e só se m divide n. Se m divide n então $\theta_{n,m}([k]_n) = [k]_m$. Em [28] podemos encontrar algumas informações interessantes sobre $\widehat{\mathbb{Z}}$. O cardinal deste grupo é $2^{\aleph_0}$.

Exemplo 2.10. *Seja p um primo de $\mathbb{N}$. Os grupos $\mathbb{Z}_p^n$, $n \in \mathbb{N}_0$, formam um sistema de representantes das classes de isomorfismo da pseudovariedade dos p-grupos Abelianos elementares finitos Ab_p, gerada pelo grupo $\mathbb{Z}_p$. Todos os grupos desta pseudovariedade que são gerados por n dos seus elementos são imagens homomorfas de $\mathbb{Z}_p^n$. Logo, se e_i for o i-ésimo vector canónico do $\mathbb{Z}_p$-espaço vectorial $\mathbb{Z}_p^n$, então o conjunto constituído apenas pelo par $(\mathbb{Z}_p^n, (e_1, \ldots, e_n))$ é cofinal em I, pelo que a álgebra das operações implícitas n-árias sobre V é isomorfa ao grupo $\mathbb{Z}_p^n$.*

Seja $\iota : X \to \overline{\Omega}_X\mathsf{V}$ a função cujas componentes são as funções geradoras das respectivas componentes, i.e., ι define-se pelas igualdades $\iota(x_i) = (\alpha(x_i))_{(A,\alpha)\in I}$. Consideremos em qualquer álgebra finita a topologia discreta e em $\overline{\Omega}_X\mathsf{V}$ a topologia induzida da topologia produto de $\prod_{(A,\alpha)\in I} A$. Então a projecção canónica na coordenada (A, α) é o único homomorfismo contínuo $\hat{\alpha} : \overline{\Omega}_X\mathsf{V} \to A$ que torna o diagrama (2.10) comutativo para qualquer $(A, \alpha) \in I$. Trata-se evidentemente de um homomorfismo sobrejectivo. Nem todo o homomorfismo $\overline{\Omega}_X\mathsf{V} \to A$ tem que ser contínuo: é o caso do exemplo 6.3 de [4].

$$\begin{array}{ccc} X & \xrightarrow{\iota} & \overline{\Omega}_X\mathsf{V} \\ & \searrow^{\alpha} & \downarrow \hat{\alpha} \\ & & A \end{array} \tag{2.10}$$

Constitui um pequeno passo adicional mostrar que o diagrama (2.10) também comuta para qualquer álgebra de V (e não apenas de V_0), e para qualquer função $\alpha : X \to A$ (não necessariamente geradora). Daqui resulta imediatamente que se $\Omega_X\mathsf{V}$ for a subálgebra gerada por $\iota(X)$, então $(\Omega_X\mathsf{V}, \iota)$ tem a propriedade universal para V sobre X. É natural que nos perguntemos se $\Omega_X\mathsf{V}$ é a V-álgebra livre sobre X. A resposta é afirmativa:

Lema 2.11. $F_{\mathsf{V}}(X) \simeq \Omega_X\mathsf{V}$.

Demonstração. Consideremos o homomorfismo sobrejectivo

$$\begin{aligned} \varphi : \quad T(X) &\longrightarrow \Omega_X\mathsf{V} \\ p(x_1, \ldots, x_n) &\longmapsto p_{\overline{\Omega}_X\mathsf{V}}(\iota(x_1), \ldots, \iota(x_n)) \end{aligned}$$

Temos

$$\begin{aligned} p_{\overline{\Omega}_X\mathsf{V}}(\iota(x_1), \ldots, \iota(x_n)) &= p_{\overline{\Omega}_X\mathsf{V}}((\alpha(x_1))_{(A,\alpha)\in I}, \ldots, \alpha(x_n)_{(A,\alpha)\in I}) \\ &= (p_A(\alpha))_{(A,\alpha)\in I} \approx (p_A)_{A\in\mathsf{V}}, \end{aligned}$$

onde o símbolo $\approx$ serve para significar a identificação que já assinalámos.

Logo $(p,q) \in \operatorname{Ker}\varphi \Leftrightarrow (p_A)_{A\in\mathsf{V}} = (q_A)_{A\in\mathsf{V}} \Leftrightarrow \mathsf{V} \models p = q \Leftrightarrow (p,q) \in \Theta_{\mathsf{V}}(X)$. □

Uma forma alternativa de mostrar que $\Omega_X\mathsf{V}$ e $F_{\mathsf{V}}(X)$ são álgebras isomorfas consistiria em provar que estas álgebras têm a propriedade universal sobre X para a variedade gerada por V.

Como resulta da demonstração do lema 2.11, os elementos de $\Omega_X\mathsf{V}$ são as operações explícitas n-árias. Por isso $\Omega_X\mathsf{V}$ é referida como a *álgebra das operações explícitas n-árias sobre* V. Se V contém álgebras não triviais, então ι é injectiva, pelo que podemos abusar da notação e designar a operação $\iota(x_i)$ por x_i; com esta identificação, $\Omega_X\mathsf{V}$ é gerada pelas variáveis $x_1, \ldots, x_n$. Devido ao modo como é interpretada numa qualquer álgebra de V, a operação explícita x_i é designada como a *projecção na i-ésima componente.*

Se π é uma operação implícita n-ária então, considerando π como elemento de $\overline{\Omega}_X\mathsf{V}$, temos $\pi_A(\alpha) = \hat{\alpha}(\pi)$. É claro que se π e ρ forem elementos distintos de $\overline{\Omega}_X\mathsf{V}$, existem uma álgebra A sobre V e um homomorfismo contínuo $\varphi : \overline{\Omega}_X\mathsf{V} \to A$ tais que $\varphi(\pi) \neq \varphi(\rho)$, bastando para tal tomar $A \in \mathsf{V}_0$ e $\alpha \in A^n$ tais que $\pi_A(\alpha) \neq \rho_A(\alpha)$ e considerar a projecção de $\overline{\Omega}_X\mathsf{V}$ sobre (A,α). Esta simples propriedade é da maior importância. Iremos aproveitá-la mais adiante para o estudo de pseudovariedades de grupos finitos. No entanto para que o possamos fazer precisamos conhecer algumas características topológicas de $\overline{\Omega}_X\mathsf{V}$.

Proposição 2.12.

1. *$\overline{\Omega}_X\mathsf{V}$ é um espaço topológico Hausdorff;*
2. *$\overline{\Omega}_X\mathsf{V}$ é um subconjunto fechado de $\prod_{(A,\alpha)\in I} A$;*
3. *$\overline{\Omega}_X\mathsf{V}$ é compacto;*
4. *A subálgebra $\Omega_X\mathsf{V}$ é densa em $\overline{\Omega}_X\mathsf{V}$.*

Demonstração. **1:** $\overline{\Omega}_X\mathsf{V}$ é subespaço do produto $\prod_{(A,\alpha)\in I} A$ de espaços Hausdorff.

2: Os subconjuntos de $\prod_{(A,\alpha)\in I} A$ que têm um número finito de coordenadas fixadas[8] e as restantes coordenadas livres[9] formam uma base $\mathfrak{b}$ da topologia de $\prod_{(A,\alpha)\in I} A$. O subconjunto $F_{((B,\beta),(C,\gamma))}$ de $\prod_{(A,\alpha)\in I} A$ é união de um número

[8]Um subconjunto S de um produto $\prod_{\lambda\in\Lambda} X_\lambda$ tem a coordenada λ_0 *fixada* se a imagem de S pela projecção canónica $S \to X_{\lambda_0}$ tiver um único elemento.

[9]Um subconjunto $S = \prod_{\lambda\in\Lambda} S_\lambda$ de um produto $X = \prod_{\lambda\in\Lambda} X_\lambda$ tem a coordenada λ_0 *livre em* X se $S_{\lambda_0} = X_{\lambda_0}$.

finito de elementos de $\mathfrak{b}$, uma vez que existem subconjuntos B_0 de B e C_0 de C tais que

$$F_{((B,\beta),(C,\gamma))} = \left(\prod_{\substack{(A,\alpha)\in I \\ (A,\alpha)\neq(B,\beta),(C,\gamma)}} A \right) \times B_0 \times C_0.$$

Como os elementos de $\mathfrak{b}$ também são fechados, o conjunto $F_{((B,\beta),(C,\gamma))}$ é fechado. Logo $\overline{\Omega}_X\mathsf{V} = \bigcap_{\substack{(B,\beta)\in I \\ (C,\gamma)\in I}} F_{((B,\beta),(C,\gamma))}$ é um fechado de $\prod_{(A,\alpha)\in I} A$.

3: O Teorema de Tychonoff diz-nos que o produto de espaços topológicos compactos é ainda compacto. Logo $\prod_{(A,\alpha)\in I} A$ é compacto, e portanto o subconjunto fechado $\overline{\Omega}_X\mathsf{V}$ também o é.

4: Seja $\mathcal{U}$ um qualquer elemento de $\mathfrak{b}$ tal que $\mathcal{U} \cap \overline{\Omega}_X\mathsf{V} \neq \emptyset$. Queremos mostrar que $\mathcal{U} \cap \Omega_X\mathsf{V} \neq \emptyset$. Como $\mathcal{U} \cap \overline{\Omega}_X\mathsf{V} \neq \emptyset$, existem $(A_1,\alpha_1),\ldots,(A_k,\alpha_k) \in I$ e $a_1 \in A_1,\ldots,a_k \in A_k$ tais que

$$\mathcal{U} \cap \overline{\Omega}_X\mathsf{V} = \{(x_{(A,\alpha)})_{(A,\alpha)} \in \overline{\Omega}_X\mathsf{V} : x_{(A_1,\alpha_1)} = a_1,\ldots,x_{(A_k,\alpha_k)} = a_k\}.$$

Sejam P a subálgebra de $A_1\times\cdots\times A_k$ gerada por $\alpha_1\times\cdots\times\alpha_k$ e $\varphi : P \to A_0 \in \mathsf{V}_0$ um isomorfismo. Se $\alpha_0 = \varphi\circ(\alpha_1\times\cdots\times\alpha_k)$ então $(A_0,\alpha_0) \in I$, $(A_i,\alpha_i) \leq (A_0,\alpha_0)$ e $\theta_{A_0,A_i} = pr_{A_i}\circ\varphi^{-1}$, $(i \in \{1,\ldots,k\})$, onde $pr_{A_i} : P \to A_i$ é a projecção canónica. O conjunto

$$\Lambda = \bigcap_{i=1,\ldots,k} \{a \in A_0 : \theta_{A_0,A_i}(a) = a_i\}$$

é não vazio, pois $\varphi(a_1,\ldots,a_k) \in \Lambda$. Temos

$$\bigcup_{a\in\Lambda} \{(x_{(A,\alpha)})_{(A,\alpha)} \in \Omega_X\mathsf{V} : x_{(A_0,\alpha_0)} = a\} \subseteq \mathcal{U} \cap \Omega_X\mathsf{V}.$$

A projecção canónica $\hat{\alpha}_{|\Omega_X\mathsf{V}} : \Omega_X\mathsf{V} \to A_0$ na coordenada (A_0,α_0) é sobrejectiva, pois $\hat{\alpha_0}_{|\Omega_X\mathsf{V}} \circ \iota = \alpha$ (ver diagrama (2.10)). Logo, para todo $a \in A_0$,

$$\{(x_{(A,\alpha)})_{(A,\alpha)} \in \Omega_X\mathsf{V} : x_{(A_0,\alpha_0)} = a\} \neq \emptyset. \quad \square$$

Corolário 2.13. *A álgebra $\overline{\Omega}_X\mathsf{V}$ é finita se e só se a subálgebra $\Omega_X\mathsf{V}$ é finita. Se $\overline{\Omega}_X\mathsf{V}$ e $\Omega_X\mathsf{V}$ forem finitas então são iguais.*

Demonstração. Num espaço Hausdorff os conjuntos finitos são fechados. Pela sua densidade em $\overline{\Omega}_X\mathsf{V}$, se $\Omega_X\mathsf{V}$ for finita então é igual a $\overline{\Omega}_X\mathsf{V}$. $\square$

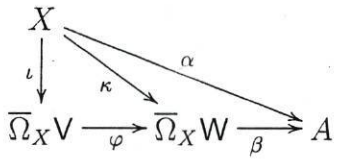
Corolário 2.14. *Se $A \in \mathsf{V}$, então para qualquer $\pi \in \overline{\Omega}_X\mathsf{V}$ existe $p \in \Omega_X\mathsf{V}$ tal que $\pi_A = p_A$.*

Demonstração. Seja $\pi \in \overline{\Omega}_X\mathsf{V}$. Consideremos a pseudovariedade W gerada por A e sejam ι e κ as funções geradoras de $\overline{\Omega}_X\mathsf{V}$ e $\overline{\Omega}_X\mathsf{W}$, respectivamente. Pela proposição 1.20, a álgebra $\Omega_X\mathsf{W}$ é um elemento de W, e portanto também de V. Pelo corolário 2.13,

$\overline{\Omega}_X\mathsf{W} = \Omega_X\mathsf{W}$. Assim existe um único homomorfismo contínuo $\varphi : \overline{\Omega}_X\mathsf{V} \to \overline{\Omega}_X\mathsf{W}$ tal que $\varphi \circ \iota = \kappa$. Temos então

$$\varphi(\overline{\Omega}_X\mathsf{V}) = \overline{\kappa(X)} = \overline{\Omega}_X\mathsf{W} = \Omega_X\mathsf{W} = \kappa(X) = \varphi(\Omega_X\mathsf{V}).$$

Logo existe $p \in \Omega_X\mathsf{V}$ tal que $\varphi(\pi) = \varphi(p)$. Seja α um qualquer elemento de A^X. Sabemos que existe um único homomorfismo contínuo $\beta : \overline{\Omega}_X\mathsf{W} \to A$ tal que $\beta \circ \kappa = \alpha$. O homomorfismo $\beta \circ \varphi$ é o único homomorfismo contínuo $\psi : \overline{\Omega}_X\mathsf{V} \to A$ tal que $\psi \circ \iota = \alpha$.



Logo

$$\pi_A(\alpha) = \beta \circ \varphi(\pi) = \beta(\varphi(\pi)) = \beta(\varphi(p)) = \beta \circ \varphi(p) = p_A(\alpha).$$

Como α é arbitrário, $\pi_A = p_A$. □

Com a proposição 2.12, podemos justificar a barra que surge no símbolo $\overline{\Omega}_X\mathsf{V}$, pois ela adquire o significado topológico da densidade de $\Omega_X\mathsf{V}$ em $\overline{\Omega}_X\mathsf{V}$.

Retomemos o exemplo 2.9. Pela compacidade de $\varprojlim_{(\mathbb{Z}_n,\alpha)\in I} \mathbb{Z}_n$ e pela propriedade Hausdorff de $\widehat{\mathbb{Z}} = \varprojlim_{(\mathbb{Z}_n,[1]_n)\in J} \mathbb{Z}_n$, a projecção canónica do primeiro grupo no segundo, além de ser um isomorfismo de grupos é um homeomorfismo de espaços topológicos.

2.3 Álgebras pró-V

A parte final da secção anterior leva-nos a focar a nossa atenção na interacção entre propriedades algébricas e topológicas de determinados objectos. Os conceitos que se seguem tornam precisas as características que pretendemos para esses objectos.

Uma *álgebra topológica* é uma álgebra munida de uma topologia para a qual as operações fundamentais são contínuas. Os morfismos entre álgebras topológicas são os homomorfismos contínuos. Logo, os isomorfismos de álgebras topológicas são os isomorfismos de álgebras que são homeomorfismos. Uma função *geradora* de uma álgebra topológica A é uma função $\iota : X \to A$ tal que a subálgebra $\langle \iota(X) \rangle$ é densa em A. Os conceitos de *função geradora de uma álgebra* e de *função geradora de uma álgebra topológica* são distintos, embora análogos. A álgebra topológica A é *finitamente gerada* se existir alguma função geradora de A que tenha domínio finito.

Uma *álgebra compacta* é uma álgebra topológica compacta e Hausdorff. Uma *álgebra pró-*V é uma álgebra compacta A com a seguinte propriedade: dados quaisquer dois elementos distintos $u, v \in A$ existem uma álgebra F de V e um homomorfismo contínuo $\varphi : A \to F$ tais que $\varphi(u) \neq \varphi(v)$. Uma álgebra topológica (não necessariamente

compacta) com esta propriedade diz-se *residual em* V. Observemos que os conjuntos $\varphi^{-1}(\varphi(u))$ e $\varphi^{-1}(\varphi(v))$ são abertos e disjuntos: são abertos porque $\{\varphi(u)\}$ e $\{\varphi(v)\}$ são abertos[10] de F e φ é contínua, e são disjuntos porque $\{\varphi(u)\}$ e $\{\varphi(v)\}$ têm intersecção vazia. Como $u \in \varphi^{-1}(\varphi(u))$ e $v \in \varphi^{-1}(\varphi(v))$, isto implica que as componentes conexas de A sejam os conjuntos singulares (i.e., só com um elemento). Recordemos que um espaço topológico cujas componentes conexas são os conjuntos singulares diz-se *totalmente desconexo*. Ora, um espaço topológico compacto e Hausdorff é totalmente desconexo se e só se possui uma base constituida apenas por abertos-fechados[11] [34]. Um espaço topológico com uma tal base diz-se *zero-dimensional*. Evidentemente, os espaços topológicos discretos são totalmente desconexos e zero-dimensionais. Assim, as propriedades das álgebras pró-V aproximam-nas das álgebras de V. Aliás, as álgebras de V munidas da topologia discreta são exemplos de álgebras pró-V. A álgebra $\overline{\Omega}_X\mathsf{V}$ também é um exemplo de uma álgebra pró-V, não necessariamente finita. Quando V é a pseudovariedade de todas as álgebras finitas, usamos o atributo *profinito* no lugar de pró-V.

A propriedade da residualidade em V das álgebras pró-V implica uma outra propriedade que a generaliza, a qual expressamos no próximo lema.

Lema 2.15. *Seja A uma álgebra pró-*V*. Se K e L forem subconjuntos compactos disjuntos de A, então existem uma álgebra F de* V *e um homomorfismo contínuo $\varphi : A \to F$ tais que $\varphi(K) \cap \varphi(L) = \emptyset$.*

Demonstração. Seja $v \in L$. Para cada $u \in K$ existem uma álgebra $F_{\{u,v\}}$ de V e um homomorfismo contínuo $\varphi_{\{u,v\}} : A \to F_{\{u,v\}}$ tais que $\varphi_{\{u,v\}}(u) \neq \varphi_{\{u,v\}}(v)$. A família $\varphi^{-1}_{\{u,v\}}(\varphi_{\{u,v\}}(u))_{u\in K}$ é uma cobertura aberta de K. Pela compacidade de K, admite uma subcobertura finita $\varphi^{-1}_{\{u_i,v\}}(\varphi_{\{u_i,v\}}(u_i))_{u_1,\ldots,u_n\in K}$. Consideremos o homomorfismo contínuo

$$\begin{aligned} \varphi_v = \textstyle\prod_{i=1}^n \varphi_{\{u_i,v\}} : \ A &\longrightarrow F_v = \textstyle\prod_{i=1}^n F_{\{u_i,v\}} \\ a &\longmapsto (\varphi_{u_i,v}(a))_{i=1,\ldots,n} \end{aligned}$$

Seja $u \in K$. Existe $i \in \{1,\ldots,n\}$ tal que $u \in \varphi^{-1}_{\{u_i,v\}}(\varphi_{\{u_i,v\}}(u_i))$, pelo que $\varphi_{\{u_i,v\}}(u) = \varphi_{\{u_i,v\}}(u_i) \neq \varphi_{\{u_i,v\}}(v)$. Logo $\varphi_v(u) \neq \varphi_v(v)$ e portanto $\varphi_v(K) \cap \varphi_v(\{v\}) = \emptyset$.

Por sua vez, a cobertura aberta $\varphi_v^{-1}(\varphi_v(v))_{v\in L}$ de L também admite uma subcobertura finita $\varphi^{-1}_{v_i}(\varphi_{v_i}(v_i))_{v_1,\ldots,v_m\in L}$. O homomorfismo contínuo

$$\begin{aligned} \varphi = \textstyle\prod_{i=1}^m \varphi_v : \ A &\longrightarrow F = \textstyle\prod_{i=1}^m F_{v_i} \\ a &\longmapsto (\varphi_{v_i}(a))_{i=1,\ldots,m} \end{aligned}$$

e a álgebra F estão nas condições pretendidas. □

[10] Também são fechados.

[11] Como o nome indica, um aberto-fechado é um conjunto aberto e fechado.

Corolário 2.16. *Seja A uma álgebra pró-*V*. Qualquer que seja o subconjunto aberto-fechado K de A, existe algum homomorfismo contínuo $\varphi : A \to F$ de A numa álgebra F de* V *tal que $K = \varphi^{-1}(\varphi(K))$.*

Demonstração. Seja então K um subconjunto aberto-fechado de A. A inclusão não trivial é $\varphi^{-1}(\varphi(K)) \subseteq K$. Como K e $A \setminus K$ são subconjuntos fechados de um espaço compacto, são também eles mesmos subespaços compactos. Pelo lema 2.15, sabemos que existem uma álgebra F de V e um homomorfismo contínuo $\varphi : A \to F$ tais que $\varphi(K) \cap \varphi(A \setminus K) = \emptyset$. Logo $A \setminus K \cap \varphi^{-1}(\varphi(K)) = \emptyset$ e portanto $\varphi^{-1}(\varphi(K)) \subseteq K$. □

Vamos terminar esta secção com um resumo de algumas das mais relevantes propriedades topológicas das álgebras pró-V finitamente geradas. Seja A uma álgebra topológica com topologia $\mathcal{T}$. Fixada a pseudovariedade V, consideremos para cada $(u, v) \in A \times A$ o conjunto $\mathfrak{C}$ dos cardinais de álgebras F de V para as quais existe algum homomorfismo contínuo $\varphi : A \to F$ tal que $\varphi(u) \neq \varphi(v)$. Definimos o elemento $r(u, v)$ de $\mathbb{N} \cup \{+\infty\}$ como sendo igual ao mínimo de $\mathfrak{C}$ se este conjunto for não vazio e igual a $+\infty$ caso contrário. Observemos que $r(u, v)$ nunca pode ser igual a 1 e que A é residual em V se e só se $u \neq v \Rightarrow r(u, v) \neq +\infty$. Consideremos agora o número

$$d(u, v) = 2^{-r(u,v)}$$

considerando $2^{-\infty} = 0$. Verificam-se as seguintes propriedades:

1. $d(u, v) \geq 0$;
2. $u = v \Rightarrow d(u, v) = 0$;
3. $d(u, w) \leq \max\{d(u, v), d(v, w)\}$.

As propriedades 1 e 2 são triviais, e mesmo a última propriedade é quase imediata: dados $u, v, w \in A$, se $\varphi : A \to F \in$ V for um homomorfismo contínuo tal que $\varphi(u) \neq \varphi(w)$, então $\varphi(v) \neq \varphi(u)$ ou $\varphi(v) \neq \varphi(w)$, pelo que $r(u, w) \geq \min\{r(u, v), r(v, w)\}$. Conforme já observamos, se A for uma álgebra pró-V então a implicação recíproca de 2 também é válida, pelo que nesse caso d é uma ultramétrica.[12] Como veremos, se A for finitamente gerada então a topologia $\mathcal{T}$ é metrizável por d.

Dizer que a álgebra topológica A é finitamente gerada é o mesmo que dizer que existe um subconjunto finito $\mathcal{X}$ de A tal que $\overline{\langle \mathcal{X} \rangle} = A$. Para cada $F \in$ V seja $\mathrm{Homc}(A, F)$ o conjunto dos homomorfismos contínuos de domínio A e conjunto de chegada F. Os elementos de $\mathrm{Homc}(A, F)$ ficam completamente determinados pela sua restrição a $\mathcal{X}$. Como $\mathcal{X}$ é finito, concluímos que $\mathrm{Homc}(A, F)$ também é um conjunto finito (de cardinal menor ou igual ao de $\mathcal{X}$).

Um tipo algébrico finito é um tipo com um número finito de operações fundamentais.

[12] Uma ultramétrica é uma métrica que verifica o axioma mais forte $d(u, w) \leq \max\{d(u, v), d(v, w)\}$.

Proposição 2.17. *Consideremos uma pseudovariedade* V *num tipo algébrico finito. Seja* A *uma álgebra pró-*V *para a topologia* $\mathcal{T}$*. A topologia* $\mathcal{T}$ *é metrizável por* d*.*

Demonstração. Consideremos um elemento v de A. Para a métrica d, a bola aberta de centro v e raio $\varepsilon > 0$ é o conjunto

$$\begin{aligned} B(v;\varepsilon) &= \{u \in A : d(u,v) < \varepsilon\} \\ &= \{u \in A : 2^{-r(u,v)} < \varepsilon\} \\ &= \{u \in A : r(u,v) > -\log_2 \varepsilon\}. \end{aligned}$$

Portanto, os elementos do conjunto das bolas abertas de centro v são os conjuntos

$$B_n(v) = \{u \in A : r(u,v) > n\}, \quad n \in \mathbb{N}.$$

Vamos começar por mostrar que $B_n(v)$ é um elemento de $\mathcal{T}$. Seja V_0 um sistema completo de representantes das classes de isomorfismo dos elementos de V. Consideremos o conjunto

$$I = \{(F,\varphi) \in \mathsf{V}_0 \times \textstyle\prod_{G \in \mathsf{V}_0} \mathrm{Homc}(A,G) : |F| \leq n \text{ e } \varphi \in \mathrm{Homc}(A,F)\}.$$

Como o tipo algébrico é finito, o conjunto $\{F \in \mathsf{V}_0 : |F| \leq L\}$ é finito. Como A é finitamente gerada, $\mathrm{Homc}(A,F)$ é finito, para qualquer $F \in \mathsf{V}$. Então o conjunto I também é finito. Logo o produto

$$P = \prod_{(F,\varphi) \in I} F$$

é um elemento de V. A função

$$\Phi = \prod_{(F,\varphi) \in I} \varphi$$

é um elemento de $\mathrm{Homc}(A,P)$. Se $r(u,v) > n$ então $\varphi(u) = \varphi(v)$ para todo $(F,\varphi) \in I$, pois $|F| \leq n$ se $(F,\varphi) \in I$. Logo $\Phi(u) = \Phi(v)$. Por outro lado, se $r(u,v) \leq n$ então existe uma álgebra F de cardinal menor ou igual a n e um homomorfismo contínuo $\varphi : A \to F$ tais que $\varphi(u) \neq \varphi(v)$. É claro que podemos supor $F \in \mathsf{V}_0$, ou seja, $(F,\varphi) \in I$. Então $\Phi(u) \neq \Phi(v)$. Resumindo,

$$r(u,v) > n \Leftrightarrow \Phi(u) = \Phi(v).$$

Como $\Phi(u) = \Phi(v) \Leftrightarrow u \in \Phi^{-1}(\Phi(v))$, daqui se retira que

$$B_n(v) = \Phi^{-1}(\Phi(v)).$$

Pela continuidade de Φ, o conjunto $B_n(v)$ é um elemento de $\mathcal{T}$. A topologia $\mathcal{T}_d$ definida pela métrica gerada por d é a topologia gerada pela família de conjuntos $(B_n(v))_{v \in A, n \in \mathbb{N}}$. Logo $\mathcal{T}_d \subseteq \mathcal{T}$.

Como a álgebra topológica A é zero-dimensional, existe uma base $\mathfrak{b}$ de $\mathcal{T}$ constituída por abertos-fechados. Vamos mostrar a inclusão $\mathcal{T} \subseteq \mathcal{T}_d$ provando a inclusão $\mathfrak{b} \subseteq \mathcal{T}_d$.

Consideremos então um elemento K de $\mathfrak{b}$. Pelo corolário 2.16, existem uma álgebra F de V e um homomorfismo contínuo $\varphi : A \to F$ tais que $K = \varphi^{-1}(\varphi(K))$. Seja $v \in K$. Se $r(u,v) > |F|$ então $\varphi(u) = \varphi(v)$, donde

$$B_{|F|}(v) \subseteq \varphi^{-1}(\varphi(v)) \subseteq \varphi^{-1}(\varphi(K)) = K.$$

Como v é um elemento arbitrário de K, o conjunto K é um aberto para a métrica d. □

De agora em diante, em todos os resultados que envolvam a utilização da ultramétrica d estaremos a assumir implicitamente que o tipo algébrico é finito.

Lema 2.18. *Uma álgebra pró-*V *é uma álgebra topológica isomorfa a uma subálgebra topológica de um produto de álgebras pró-*V.

Demonstração. Dada uma álgebra A pró-V, consideremos o conjunto $\mathcal{P}_2(A)$ dos subconjuntos de A com cardinal igual a 2. Então, para cada $\{u,v\} \in \mathcal{P}_2(A)$ existem uma álgebra $F_{\{u,v\}}$ de V e um homomorfismo contínuo $\varphi_{\{u,v\}} : A \to F_{\{u,v\}}$ tais que $\varphi_{\{u,v\}}(u) \neq \varphi_{\{u,v\}}(v)$. Consideremos a função

$$\begin{aligned} \varphi = \textstyle\prod_{\{u,v\}\in\mathcal{P}_2(A)} \varphi_{\{u,v\}} : A &\longrightarrow \textstyle\prod_{\{u,v\}\in\mathcal{P}_2(A)} F_{\{u,v\}} \\ a &\longmapsto (\varphi_{\{u,v\}}(a))_{\{u,v\}\in\mathcal{P}_2(A)} \end{aligned}$$

Esta função é um homomorfismo contínuo e injectivo.[13] Então a função

$$a \in A \overset{\varphi_0}{\mapsto} \varphi(a) \in \operatorname{Im}\varphi$$

é uma bijecção contínua. Pela compacidade de A e pela propriedade Hausdorff de $\operatorname{Im}\varphi$, o homomorfismo φ_0 é um homeomorfismo. □

Decorre da demonstração do lema anterior que uma álgebra pró-V finita é isomorfa a uma subálgebra de um produto de um número finito de elementos de V. Logo as álgebras de V são as únicas álgebras pró-V finitas.

O lema 2.18 tem dois corolários enunciados a seguir e cuja utilidade é ilustrada no exemplo subsequente.

Corolário 2.19. *Sejam A uma álgebra pró-*V *e $(u_n)_n$ uma sucessão de elementos de A. A sucessão $(u_n)_n$ converge em A se e só se para todo o homomorfismo contínuo $\varphi : A \to F$ de A numa álgebra F de V a sucessão $(\varphi(u_n))_n$ é quase-constante.*

Demonstração. A implicação directa é imediata. Pelo lema 2.18, para algum conjunto V_0 de álgebras de V, a álgebra topológica A pode ser considerada como um subespaço fechado do produto $\prod_{B\in\mathsf{V}_0} B$. Ora num produto $\prod_{i\in I} X_i$ de espaços topológicos X_i uma sucessão $(f_n)_{n\in\mathbb{N}}$ converge se e só se as sucessões $(f_n(i))_{n\in\mathbb{N}}$ convergem em X_i, qualquer que seja o elemento i de I [34]. Assim para mostrarmos a implicação recíproca os homomorfismos contínuos que nos basta considerar são as restrições a A das projecções canónicas de $\prod_{B\in\mathsf{V}_0} B$ em elementos de V_0. □

[13] $u, v \in A$ e $u \neq v \Rightarrow \varphi_{\{u,v\}}(u) \neq \varphi_{\{u,v\}}(v) \Rightarrow \varphi(u) \neq \varphi(v)$.

Corolário 2.20. *Sejam A uma álgebra pró-V e $(u_n)_n$ uma sucessão de elementos de A. A sucessão $(u_n)_n$ converge em A para u se e só se para todo o homomorfismo contínuo $\varphi : A \to F$ de A numa álgebra F de V a sucessão $(\varphi(u_n))_n$ é quase-constante igual a $\varphi(u)$.*

Demonstração. A demonstração deste corolário é análoga à do corolário anterior; neste caso a observação a fazer é a de que num produto $\prod_{i\in I} X_i$ de espaços topológicos X_i uma sucessão $(f_n)_{n\in\mathbb{N}}$ converge para g se e só se as sucessões $(f_n(i))_{n\in\mathbb{N}}$ convergem em X_i para $g(i)$, qualquer que seja o elemento i de I [34]. □

Exemplo 2.21. *Consideremos a pseudovariedade S dos semigrupos finitos. A sucessão de operações explícitas unárias $(x^{n!+k})_{n\geq|k|}$ converge em $\overline{\Omega}_{\{x\}}\mathsf{S}$ para a operação implícita $x^{\omega+k}$, uma vez que para qualquer homomorfismo contínuo $\varphi : \overline{\Omega}_{\{x\}}\mathsf{S} \to S$ num semigrupo finito S temos*

$$\lim_{n\to\infty} \varphi(x^{n!+k}) = \varphi(\lim_{n\to\infty} x^{n!+k}) = \varphi(x^{\omega+k}).$$

2.4 $\overline{\Omega}_n\mathsf{V}$ enquanto álgebra pró-V livre

O próximo teorema generaliza para qualquer álgebra A pró-V a comutatividade do diagrama (2.10).

Teorema 2.22. *Para toda a álgebra A pró-V e para toda a função $\alpha : X \to A$, existe um único homomorfismo contínuo $\hat{\alpha} : \overline{\Omega}_X\mathsf{V} \to A$ tal que $\hat{\alpha} \circ \iota = \alpha$.*

Demonstração. Sejam A uma álgebra pró-V e $\alpha : X \to A$ uma função. Consideremos o conjunto $\mathcal{P}_2(A)$ dos subconjuntos de A com cardinal igual a 2. Então, para cada $\{u, v\} \in \mathcal{P}_2(A)$ existem uma álgebra $F_{\{u,v\}}$ de V e um homomorfismo contínuo $\varphi_{\{u,v\}} : A \to F_{\{u,v\}}$ tais que $\varphi_{\{u,v\}}(u) \neq \varphi_{\{u,v\}}(v)$. Seja $\theta_{\{u,v\}} : \overline{\Omega}_X\mathsf{V} \to F_{\{u,v\}}$ o único homomorfismo contínuo tal que $\theta_{\{u,v\}} \circ \iota = \varphi_{\{u,v\}} \circ \alpha$.

$$\begin{array}{ccc} X & \xrightarrow{\iota} & \overline{\Omega}_X\mathsf{V} \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\theta_{\{u,v\}}} \\ A & \xrightarrow[\varphi_{\{u,v\}}]{} & F_{\{u,v\}} \end{array}$$

Sejam agora $F = \prod_{\{u,v\}\in\mathcal{P}_2(A)} F_{\{u,v\}}$, $\theta : \overline{\Omega}_X\mathsf{V} \to F$ o homomorfismo $\prod_{\{u,v\}\in\mathcal{P}_2(A)} \theta_{\{u,v\}}$ e $\varphi : A \to F$ o homomorfismo $\prod_{\{u,v\}\in\mathcal{P}_2(A)} \varphi_{\{u,v\}}$. Temos $\theta \circ \iota = \varphi \circ \alpha$.

$$\begin{array}{ccc} X & \xrightarrow{\iota} & \overline{\Omega}_X\mathsf{V} \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\theta} \\ A & \xrightarrow[\varphi]{} & F \end{array}$$

A função

$$a \in A \overset{\varphi_0}{\mapsto} \varphi(a) \in \operatorname{Im}\varphi$$

é uma bijecção contínua e portanto, pela compacidade de A e pela propriedade Hausdorff de $\operatorname{Im}\varphi$, é um homeomorfismo. Basta-nos pois mostrar que $\operatorname{Im}\theta \subseteq \operatorname{Im}\varphi$ e tomar $\hat{\varphi} = \varphi_0^{-1} \circ \theta$ para completarmos a demonstração. Como $\operatorname{Im}\varphi$ é um subconjunto compacto do espaço Hausdorff F,

$$\begin{aligned}\operatorname{Im}\varphi = \overline{\operatorname{Im}\varphi} &\supseteq \overline{\varphi(\langle\alpha(X)\rangle)} = \overline{\langle\varphi(\alpha(X))\rangle} \\ &= \overline{\langle\theta(\iota(X))\rangle} = \overline{\theta(\langle\iota(X)\rangle)} = \overline{\theta(\Omega_X\mathsf{V})} \\ &= \theta(\overline{\Omega_X\mathsf{V}}) = \theta(\overline{\Omega}_X\mathsf{V}) = \operatorname{Im}\theta.\end{aligned}$$

Demonstrada a existência do homomorfismo $\hat{\alpha}$, a unicidade é quase imediata: se φ e ψ forem homomorfismos $\overline{\Omega}_X\mathsf{V} \to A$ tais que $\varphi \circ \iota = \psi \circ \iota$, então pelo lema 1.6 $\varphi_{|\Omega_X\mathsf{V}} = \psi_{|\Omega_X\mathsf{V}}$; se além do mais φ e ψ forem contínuos, então, como $\Omega_X\mathsf{V}$ é denso em $\overline{\Omega}_X\mathsf{V}$, $\varphi = \psi$. □

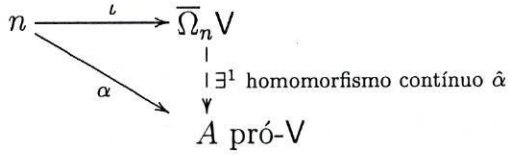
Vamos abstrair a propriedade descrita no teorema 2.22. Se F for uma álgebra pró-V e $\iota : X \to F$ for uma função tal que $\overline{\langle\iota(X)\rangle} = F$, dizemos que F é uma *álgebra pró-V livre* sobre X, relativamente a ι, se para toda a álgebra pró-V e para toda a função $\alpha : X \to A$ existir um único homomorfismo contínuo $\hat{\alpha} : \overline{\Omega}_X\mathsf{V} \to A$ tal que $\hat{\alpha} \circ \iota = \alpha$. Se X for um conjunto finito não vazio[14], então $\overline{\Omega}_X\mathsf{V}$ é uma álgebra pró-V livre sobre X. Mimetizando um raciocínio já utilizado no capítulo 1, concluímos que, a menos de isomorfismo de álgebras topológicas, existe uma única álgebra pró-V livre sobre um conjunto de cardinal n. Escolhemos o conjunto $n = \{0, \ldots, n-1\}$, para falarmos na álgebra pró-V livre $\overline{\Omega}_n\mathsf{V}$ das operações implícitas n-árias sobre V, e na subálgebra densa $\Omega_n\mathsf{V}$ das operações explícitas n-árias sobre V. Em geral, por simplicidade, continuamos a denotar por x_i a imagem de $i-1$ pela função geradora de $\overline{\Omega}_n\mathsf{V}$.

2.5 Operações implícitas em álgebras pró-V e composição de operações implícitas

Libertemo-nos do modelo que construímos para $\overline{\Omega}_n\mathsf{V}$ (e que permitiu provar a sua existência), tirando proveito da definição de álgebra pró-V livre, expressa no dia-

[14]Na verdade esta é uma condição supérflua. Apesar de termos construído $\overline{\Omega}_X\mathsf{V}$ partindo do pressuposto de que X é um conjunto finito não vazio, a finitude de X não foi relevante para essa construção. A opção por supor X finito deveu-se a três razões: apenas nos será útil o estudo de operações implícitas com aridade finita, se X for finito então, como vimos, $\overline{\Omega}_X\mathsf{V}$ tem propriedades topológicas muito úteis, e ainda sob a hipótese da finitude de X a aquisição de conceitos é, na nossa opinião, feita com menos esforço e maior apoio da intuição (nomeadamente através da identificação $A^X \approx A^{|X|}$).

grama (2.11).

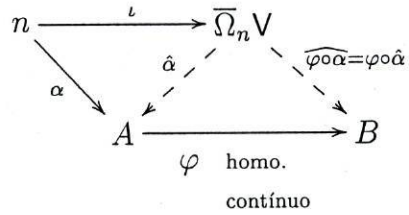


(2.11)

Seja π um elemento de $\overline{\Omega}_n\mathsf{V}$. A existência e unicidade do homomorfismo $\hat{\alpha}$ torna possível a interpretação de π numa qualquer álgebra A pró-V como a operação n-ária

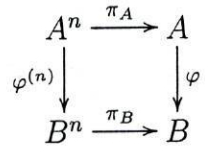
$$\begin{aligned} \pi_A : A^n &\longrightarrow A \\ \alpha &\longmapsto \hat{\alpha}(\pi) \end{aligned}$$

Ainda pela unicidade dos homomorfismos $\hat{\alpha}$, esta interpretação comuta com homomorfismos contínuos:



$$\varphi(\pi_A(\alpha)) = \varphi(\hat{\alpha}(\pi)) = \widehat{\varphi \circ \alpha}(\pi) = \pi_B(\varphi \circ \alpha).$$

Dito de outro modo, o diagrama (2.12) comuta para qualquer homomorfismo contínuo $\varphi : A \to B$ entre álgebras pró-V.



(2.12)

Já sabíamos que a família $\pi = (\pi_A)_{A \in V}$ tornava o diagrama (2.12) comutativo para qualquer homomorfismo entre álgebras de V. A novidade reside em π admitir uma interpretação nas álgebras pró-V que estende naturalmente o conceito de operação implícita sobre V ao de operação implícita na classe das álgebras pró-V.

Exemplo 2.23. *Num semigrupo profinito S, a potência $a^{\omega+k}$ define-se como sendo a imagem de a pela interpretação em S da operação implícita unária $x^{\omega+k}$. Já tínhamos visto no exemplo 2.21 que a sucessão de operações explícitas $(x^{n!+k})_{n \geq |k|}$ converge para $x^{\omega+k}$. Logo, se φ for o único homomorfismo contínuo $\overline{\Omega}_1\mathsf{S} \to S$ que envia*[15] *x em a, então*

$$a^{\omega+k} = \varphi(x^{\omega+k}) = \varphi(\lim_{n \to +\infty} x^{n!+k}) = \lim_{n \to +\infty} \varphi(x)^{n!+k} = \lim_{n \to +\infty} a^{n!+k}.$$

O próximo lema, que generaliza o lema 2.4, vem no seguimento deste exemplo.

[15]Em conformidade com a convenção geral que adoptámos, denotamos por x a imagem de 0 pela função geradora $\iota : 1 = \{0\} \to \overline{\Omega}_1\mathsf{V}$.

Lema 2.24. *Sejam M um monóide profinito e x um elemento de M. As seguintes condições são equivalentes:*

1. *x é invertível;*
2. *existe $y \in M$ tal que $yx = 1$;*
3. *existe $y \in M$ tal que $xy = 1$;*
4. *$x^\omega = 1$.*

Demonstração. Com excepção das implicações $2 \Rightarrow 1$ e $3 \Rightarrow 1$, a demonstração é inteiramente análoga à do lema 2.4. Suponhamos que $yx = 1$. Seja $\varphi : M \to F$ um homomorfismo contínuo num monóide finito F. Então $\varphi(y)\varphi(x) = 1$. Decorre da demonstração do lema 2.4 que $\varphi(x)\varphi(y) = 1$, ou seja, que $\varphi(xy) = \varphi(1)$. Como φ e F são arbitrários e M é profinito, $xy = 1$, o que mostra a implicação $2 \Rightarrow 1$. Analogamente, se $xy = 1$ então x é invertível. □

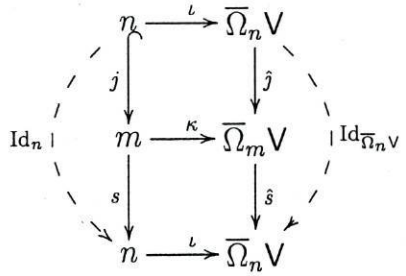
A interpretação em álgebras pró-V de operações implícitas sobre uma pseudovariedade V tem como aplicação importante o facto de ser um meio expedito de as compor. Se $w \in \overline{\Omega}_n\mathsf{V}$ for uma operação implícita n-ária sobre V e $v_1, \ldots, v_n \in \overline{\Omega}_m\mathsf{V}$ forem operações implícitas m-árias sobre V, então definimos a operação implícita composta $w(v_1, \ldots, v_n)$ como sendo a operação implícita m-ária $u = w_{\overline{\Omega}_m\mathsf{V}}(v_1, \ldots, v_n)$. Esta definição é adequada, pois se A é uma álgebra pró-V e $\alpha : m \to A$ é um elemento de A^m, então $u_A(\alpha)$ é igual a $w_A((v_1)_A(\alpha), \ldots, (v_n)_A(\alpha))$, como a seguir se deduz:

$$\begin{aligned} u_A(\alpha) &= \hat{\alpha}(u) \\ &= \hat{\alpha}(w_{\overline{\Omega}_m\mathsf{V}}(v_1, \ldots, v_n)) \\ &= w_A(\hat{\alpha}(v_1), \ldots, \hat{\alpha}(v_n)) \\ &= w_A((v_1)_A(\alpha), \ldots, (v_n)_A(\alpha)). \end{aligned}$$

Como exemplo muito particular, temos a igualdade $\pi = \pi(x_1, \ldots, x_n)$, para todo $\pi \in \overline{\Omega}_n\mathsf{V}$.

Se $n \leq m$, a álgebra $\overline{\Omega}_n\mathsf{V}$ pode ser mergulhada em $\overline{\Omega}_m\mathsf{V}$, do modo que a seguir descrevemos. Sejam $j : n \to m$ a inclusão de n em m, e $s : m \to n$ uma função tal que $s \circ j = \mathrm{Id}_n$. Sejam ι e κ as funções geradoras de $\overline{\Omega}_n\mathsf{V}$ e $\overline{\Omega}_m\mathsf{V}$, respectivamente. Se $\hat{\jmath}$ e $\hat{s}$ forem os únicos homomorfismos contínuos que tornam comutativos os quadrados interiores do diagrama (2.13), então, pela sua unicidade, o homomorfismo contínuo $\hat{s} \circ \hat{\jmath}$ é a identidade, como ilustra o mesmo diagrama (2.13). Logo $\hat{\jmath}$ é um homomorfismo

injectivo.



(2.13)

Notemos que se $m = n$ então $\hat{\jmath}$ é a identidade. O homomorfismo $\hat{\jmath}$ envia a operação implícita n-ária $\pi \in \overline{\Omega}_n\mathsf{V}$ na operação implícita m-ária sobre V que transforma um m-uplo $(a_1, \ldots, a_n, a_{n+1}, \ldots, a_m)$ de elementos de uma álgebra A pró-V em $\pi_A(a_1, \ldots, a_n)$, como a seguir se deduz:

$$\begin{aligned}\hat{\jmath}(\pi) &= \hat{\jmath}(\pi_{\overline{\Omega}_n\mathsf{V}}(\iota(0), \ldots, \iota(n-1))) \\ &= \pi_{\overline{\Omega}_m\mathsf{V}}(\hat{\jmath}(\iota(0)), \ldots, \hat{\jmath}(\iota(n-1))) \\ &= \pi_{\overline{\Omega}_m\mathsf{V}}(\kappa(0), \ldots, \kappa(n-1))\end{aligned}$$

Verifica-se, como consequência imediata da injectividade de $\hat{\jmath}$, a seguinte propriedade, válida para elementos π e ρ, de $\overline{\Omega}_n\mathsf{V}$ e para $m \geq n$:

$$\pi_{\overline{\Omega}_m\mathsf{V}} = \rho_{\overline{\Omega}_m\mathsf{V}} \Leftrightarrow \pi = \rho.$$

2.6 Pseudoidentidades

Uma *pseudoidentidade* em V é um par ordenado (π, ρ) de operações implícitas sobre V com a mesma aridade. O par (π, ρ) é usualmente denotado pela igualdade formal $\pi = \rho$. Dizemos que uma álgebra A pró-V satisfaz a pseudoidentidade $\pi = \rho$, e escrevemos $A \models \pi = \rho$, se $\pi_A = \rho_A$; se K for uma classe de álgebras pró-V então $\mathsf{K} \models \pi = \rho$ significa que todos os elementos de K satisfazem a pseudoidentidade $\pi = \rho$; e se Σ for um conjunto de pseudoidentidades em V então $\mathsf{K} \models \Sigma$ significa que todos os elementos de K satisfazem todas as pseudoidentidades de Σ. A classe das álgebras de V que satisfazem um conjunto de pseudoidentidades Σ em V é denotada $[\![\Sigma]\!]_{\mathsf{V}}$; caso seja $\Sigma = \{\pi = \rho\}$ estaremos à vontade para omitir as chavetas, escrevendo apenas $[\![\pi = \rho]\!]_{\mathsf{V}}$.

Exemplo 2.25. *Consideremos, no tipo algébrico dos monóides, as pseudovariedades* M *dos monóides finitos e* G *dos grupos finitos; temos* $\mathsf{G} = [\![x^\omega = 1]\!]_{\mathsf{M}}$.

Consideremos o tipo algébrico dos semigrupos e a pseudovariedade S dos semigrupos finitos. Se X é um conjunto de $n-1$ variáveis, $\pi \in \overline{\Omega}_X\mathsf{S}$ e y é uma variável que não ocorre em X, então usamos a igualdade formal $\pi^\omega = 1$ como abreviatura da cadeia $\pi^\omega y = y\pi^\omega = y$ de pseudoidentidades entre operações implícitas n-árias.

Exemplo 2.26. *Se* G *for a subpseudovariedade de* S *constituída pelos grupos finitos então* $\mathsf{G} = [\![x^\omega = 1]\!]_\mathsf{S}$.

Como as operações implícitas comutam com homomorfismos entre elementos de V, a classe $[\![\Sigma]\!]_\mathsf{V}$ é uma subpseudovariedade de V. De facto, em flagrante analogia com o Teorema de Birkhoff, todas as subpseudovariedades são desta forma:

Teorema 2.27 (Reiterman). *Se* W *é uma subpseudovariedade de uma pseudovariedade* V *e se* Σ_W *é o conjunto das pseudoidentidades em* V *válidas em* W, *então* $\mathsf{W} = [\![\Sigma_\mathsf{W}]\!]_\mathsf{V}$.

Em [4] podemos encontrar uma demonstração do Teorema de Reiterman que, na nossa opinião, se enquadra bem no modo como nesta monografia temos abordado o conceito de operação implícita.

De agora em diante, caso fique claro que as pseudovariedades com que trabalhamos são subpseudovariedades de V, escrevemos $[\![\Sigma]\!]$ em vez de $[\![\Sigma]\!]_\mathsf{V}$. Em geral V será a pseudovariedade das álgebras finitas.

O Teorema de Reiterman permite-nos dizer que as pseudoidentidades são um instrumento adequado para descrever pseudovariedades, colmatando a insuficiência das identidades, manifestada pelo facto de nem todas as pseudovariedades serem equacionais. O poder descritivo das pseudoidentidades confere grande importância e poder de síntese às álgebras pró-V livres finitamente geradas: se Σ for um conjunto de pseudoidentidades constituído por operações implícitas n-árias sobre V (i.e., se Σ estiver contido em $\overline{\Omega}_n\mathsf{V} \times \overline{\Omega}_n\mathsf{V}$), então $\overline{\Omega}_n\mathsf{V} \models \Sigma$ se e só se $\mathsf{V} \models \Sigma$.

2.7 Operadores implícitos

Um *operador implícito* (respectivamente, *explícito*) n-ário sobre uma pseudovariedade V é um elemento de $(\overline{\Omega}_n\mathsf{V})^n$ (respectivamente, $(\Omega_n\mathsf{V})^n$). Os operadores implícitos unários são portanto precisamente as operações implícitas unárias. O conceito de operador implícito encontra-se desenvolvido em [3, 5]. Em [3] os resultados sobre operadores implícitos que entretanto são aí alcançados desempenham um papel importante no estudo de questões relacionadas com a decidibilidade de pseudovariedades de semigrupos finitos.[16] Uma parte do conteúdo destes dois artigos serviu de base para o que vamos fazer até ao final deste capítulo.

Se $f = (\pi_1, \ldots, \pi_n)$ e $g = (\rho_1, \ldots, \rho_n)$ forem operadores implícitos n-ários sobre V, então a *pseudoidentidade de operadores* $f = g$ é o conjunto das pseudoidentidades $\pi_i = \rho_i$ $(i = 1, \ldots, n)$.

[16] Uma pseudovariedade de semigrupos finitos diz-se *decidível* se existir algum algoritmo que permita testar se um semigrupo finito pertence a ela ou não [1].

Dados um operador implícito n-ário $f = (\pi_1, \ldots, \pi_n)$ sobre V e uma álgebra A pró-V, a *interpretação de f em A* é a função $f_A = ((\pi_1)_A, \ldots, (\pi_n)_A)$ de A^n em A^n. É claro que se g for um outro operador implícito sobre A então $f_A = g_A$ se e só se A satisfaz a pseudoidentidade de operadores $f = g$. O conjunto $\mathscr{O}(A^n)$ das interpretações em A de operadores implícitos n-ários sobre V é um submonóide do monóide das funções $A^n \to A^n$, para a operação de composição. Um elemento de $\mathscr{O}(A^n)$ é um *operador implícito sobre A*. A ultramétrica natural de $\overline{\Omega}_n\mathsf{V}$ induz a ultramétrica em $\mathscr{O}(A^n)$ definida do seguinte modo:

$$d(T, U) = \sum_{i=1}^{n} \inf\{d(\pi, \rho) : \pi, \rho \in \overline{\Omega}_n\mathsf{V}, \pi_A = T_i,\ \rho_A = U_i\}$$

onde T_i e U_i são as funções componentes de T e U, respectivamente. O monóide $\mathscr{O}(A^n)$ é topológico, um facto que enunciamos sob a forma de lema, demonstrando-o de seguida:

Lema 2.28. *Seja A uma álgebra pró-V. A composição de operadores implícitos sobre A é uma operação contínua.*

Demonstração. Sejam $u, u', v_1, \ldots, v_n, v'_1, \ldots, v'_n$ elementos de $\overline{\Omega}_n\mathsf{V}$. Comecemos por supor que $r(u(v_1, \ldots, v_n), u'(v'_1, \ldots, v'_n)) \in \mathbb{N}$, ou seja, que $u(v_1, \ldots, v_n) \neq u'(v'_1, \ldots, v'_n)$. Sejam então F um elemento de V tal que $r(u(v_1, \ldots, v_n), u'(v'_1, \ldots, v'_n)) = |F|$ e φ um homomorfismo contínuo $\overline{\Omega}_n\mathsf{V} \to F$ tal que $\varphi(u(v_1, \ldots, v_n)) \neq \varphi(u'(v'_1, \ldots, v'_n))$. Ora

$$\begin{aligned}\varphi(u(v_1, \ldots, v_n)) \neq \varphi(u'(v'_1, \ldots, v'_n)) &\Leftrightarrow \varphi(u_{\overline{\Omega}_n\mathsf{V}}(v_1, \ldots, v_n)) \neq \varphi(u'_{\overline{\Omega}_n\mathsf{V}}(v'_1, \ldots, v'_n)) \\ &\Leftrightarrow u_F(\varphi(v_1), \ldots, \varphi(v_n)) \neq u'_F(\varphi(v'_1), \ldots, \varphi(v'_n)).\end{aligned}$$

Se $u_F \neq u'_F$, então existe $\alpha \in F^n$ tal que $u_F(\alpha) \neq u'_F(\alpha)$ e portanto $\hat{\alpha}(u) \neq \hat{\alpha}(u')$. Por outro lado, se $u_F = u'_F$ então existe $i \in \{1, \ldots, n\}$ tal que $\varphi(v_i) \neq \varphi(v'_i)$. Assim, mesmo que $r(u(v_1, \ldots, v_n), u'(v'_1, \ldots, v'_n)) = +\infty$, verifica-se a desigualdade $\min_{i=1,\ldots,n}\{r(u, u'), r(v_i, v'_i)\} \leq r(u(v_1, \ldots, v_n), u'(v'_1, \ldots, v'_n))$, ou seja,

$$d(u(v_1, \ldots, v_n), u'(v'_1, \ldots, v'_n)) \leq \max_{i=1,\ldots,n}\{d(u, u'), d(v_i, v'_i)\}.$$

Consideremos agora os elementos $f = (\pi_1, \ldots, \pi_n)$, $g = (\rho_1, \ldots, \rho_n)$, $f' = (\pi'_1, \ldots, \pi'_n)$ e $g' = (\rho'_1, \ldots, \rho'_n)$ de $(\overline{\Omega}_n\mathsf{V})^n$. Sejam também $u_i, v_i, u'_i, v'_i \in \overline{\Omega}_n\mathsf{V}$ tais que $(u_i)_A = (\pi_i)_A$, $(u'_i)_A = (\pi'_i)_A$, $(v_i)_A = (\rho_i)_A$ e $(v'_i)_A = (\rho'_i)_A$ $(i = 1, \ldots, n)$. Consideremos em $\mathscr{O}(A^n) \times \mathscr{O}(A^n)$ a métrica da soma. Então,

$$
\begin{aligned}
d(f_A \circ g_A, f'_A \circ g'_A) &\leq \sum_{i=1}^{n} d(u_i(v_1, \ldots, v_n), u'_i(v'_1, \ldots, v'_n)) \\
&\leq \sum_{i=1}^{n} \max_{j=1,\ldots,n} \{d(u_i, u'_i), d(v_j, v'_j)\} \\
&\leq \sum_{i=1}^{n} \left(d(u_i, u'_i) + \sum_{j=1}^{n} d(v_j, v'_j) \right) \\
&= \sum_{i=1}^{n} d(u_i, u'_i) + n \sum_{i=1}^{n} d(v_i, v'_i).
\end{aligned}
$$

Logo

$$
d(f_A \circ g_A, f'_A \circ g'_A) \leq d(f_A, f'_A) + n\, d(g_A, g'_A) \leq n\, d((f_A, g_A), (f'_A, g'_A)),
$$

pelo que a composição é uma operação uniformemente contínua em $\mathscr{O}(A^n)$. □

Seja B uma álgebra pró-V que é imagem da álgebra A pró-V por um homomorfismo contínuo.[17] Então a função

$$
\begin{aligned}
\epsilon_{A,B} : \quad & \mathscr{O}(A^n) \longrightarrow \mathscr{O}(B^n) \\
& f_A \,(f \in (\overline{\Omega}_n \mathsf{V})^n) \longmapsto f_B
\end{aligned}
$$

está bem definida e é um homomorfismo de monóides. De facto é um morfismo de álgebras topológicas. Com efeito, o conjunto $\{\pi \in \overline{\Omega}_n \mathsf{V} : \pi_A = \rho_A\}$ está contido no conjunto $\{\pi \in \overline{\Omega}_n \mathsf{V} : \pi_B = \rho_B\}$, pelo que a função $\epsilon_{A,B}$ é contractiva ($d(f_B, g_B) \leq d(f_A, g_A)$) e portanto contínua. Daqui resulta facilmente que $\mathscr{O}(A^n)$ é um monóide profinito: se $f = (\pi_1, \ldots, \pi_n)$ e $g = (\rho_1, \ldots, \rho_n)$ são operadores implícitos n-ários sobre V tais que $f_A \neq g_A$, então existem $i \in \{1, \ldots, n\}$ e $\alpha \in A^n$ tais que $(\pi_i)_A(\alpha) \neq (\rho_i)_A(\alpha)$; como A é pró-V, existe um homomorfismo contínuo $\varphi : A \to F \in \mathsf{V}$ tal que $\varphi((\pi_i)_A(\alpha)) \neq \varphi((\rho_i)_A(\alpha))$, o que é equivalente à desigualdade $(\pi_i)_F(\varphi \circ \alpha) \neq (\rho_i)_F(\varphi \circ \alpha)$; logo $\epsilon_{A,F}(f_A) \neq \epsilon_{A,F}(g_A)$. A função

$$
\begin{aligned}
\epsilon_A : \quad & (\overline{\Omega}_n \mathsf{V})^n \longrightarrow \mathscr{O}(A^n) \\
& f = (\pi_1, \ldots, \pi_n) \longmapsto f_A = ((\pi_1)_A, \ldots, (\pi_n)_A)
\end{aligned}
$$

[17] Uma álgebra B que é imagem de uma álgebra A pró-V por um homomorfismo contínuo pode não ser profinita; contudo, se acrescentarmos a condição de que B é profinita, então já temos a garantia de que B é pró-V: veja-se a proposição 4.3 de [4] e o comentário que se lhe segue.

também é contractiva (considerando em $\overline{\Omega}_n\mathsf{V}$ a métrica da soma), e é um homeomorfismo no caso em que $A = \overline{\Omega}_n\mathsf{V}$. Como tal, $\epsilon_{\overline{\Omega}_n\mathsf{V}}$ induz no espaço métrico $(\overline{\Omega}_n\mathsf{V})^n$ uma operação de composição que o torna num monóide topológico isomorfo a $\mathscr{O}((\overline{\Omega}_n\mathsf{V})^n)$. Explicitemos essa operação de composição: se $(\pi_1, \ldots, \pi_n)$ e $(\rho_1, \ldots, \rho_n)$ são elementos de $(\overline{\Omega}_n\mathsf{V})^n$, a composta $(\pi_1, \ldots, \pi_n) \circ (\rho_1, \ldots, \rho_n)$ é o operador cuja i-ésima componente é $\pi_i(\rho_1, \ldots, \rho_n)$.

Como $\mathscr{O}(A^n)$ é um monóide profinito, os seus elementos admitem uma potência ómega. No caso particular em que $n = 1$ e V é a pseudovariedade dos semigrupos finitos, levanta-se logo um problema: x^ω representa a operação implícita "potência ómega" ou é a potência ómega do operador explícito x? O dois conceitos não coincidem, pois a potência ómega do operador x é x. Para contornar este problema, no caso em que f é um operador unário sobre uma pseudovariedade de semigrupos, denotaremos a potência ómega de f por $f^{\circ\omega}$, pondo-se assim em destaque o facto de estarmos a considerar a operação de composição.

Se $f \in (\overline{\Omega}_n\mathsf{V})^n$, e A é uma álgebra pró-V, então pela continuidade de ϵ_A temos $(f^\omega)_A = (f_A)^\omega$. Logo $(x_i)_{\overline{\Omega}_n\mathsf{V}}(f^\omega)$ é a operação implícita $(x_i \circ (f_A)^\omega)_{A\in\mathsf{V}}$.

Exemplo 2.29. *Seja* S *a pseudovariedade dos semigrupos finitos. Dado* $n \in \mathbb{N}$, *consideremos o operador implícito unário* $\pi(x) = x^n$ *sobre* S. *Aplicando a potência ómega ao operador* π, *obtemos a operação implícita*

$$\pi^{\circ\omega}(x) = \lim_{k\to+\infty} x^{n^{k!}}.$$

a qual é naturalmente denotada por x^{n^ω}. *Pelo pequeno Teorema de Fermat, se o primo* p *não divide* n, *a pseudoidentidade* $x^{n^\omega} = x$ *é válida na pseudovariedade* G_p *dos* p*-grupos finitos. Por outro lado,* $\mathsf{G}_p = [\![x^{p^\omega} = 1]\!]$.

Exemplo 2.30. *Ainda na pseudovariedade* S *dos semigrupos finitos, consideremos o operador implícito binário* $f(x, y) = (xyx^{\omega-1}y^{\omega-1}, y)$. *Para cada* $k \in \mathbb{N}$, *denotemos por* $[x, {}_k y]$ *a primeira componente de* f^k. *Observemos que* $[x, {}_{k+1} y] = [[x, {}_k y], y]$. *A primeira componente da potência ómega do operador* f *é a operação implícita*

$$[x, {}_\omega y] = \lim_{k\to+\infty} [x, {}_{k!} y].$$

Notemos que $[x, {}_1 x] = x^\omega$, *e que, por indução,* $[x, {}_k x] = x^\omega$. *Logo* $[x, {}_\omega x] = x^\omega$. *Daqui se retira que se um semigrupo satisfaz a pseudoidentidade* $[x, {}_\omega y] = 1$ *então é um grupo. Iremos mostrar no capítulo 4 que os grupos que satisfazem a pseudoidentidade* $[x, {}_\omega y] = 1$ *são precisamente os grupos nilpotentes finitos. Este resultado deve-se a M. Zorn [35].*

Estes exemplos ilustram o papel desempenhado pelos operadores implícitos enquanto meio de obtenção de novas operações implícitas a partir de outras que são previamente dadas.

2.8 Operações implícitas unárias nas pseudovariedades S, M e G

A composição $\circ$ de operações implícitas unárias é uma operação binária em $\overline{\Omega}_1\mathsf{V}$. A consideração de uma operação de composição vai permitir-nos enriquecer a estrutura de $\overline{\Omega}_1\mathsf{V}$ de uma forma que é particularmente interessante nos casos em que V é a pseudovariedade S, M ou G dos semigrupos, monóides ou grupos finitos, respectivamente.

Proposição 2.31. *Interpretando em $\overline{\Omega}_1\mathsf{S}$, $\overline{\Omega}_1\mathsf{M}$ e $\overline{\Omega}_1\mathsf{G}$ a operação binária $\cdot$ do correspondente tipo algébrico como uma adição e a composição $\circ$ como uma multiplicação, temos sucessivamente:*

1. *em $\overline{\Omega}_1\mathsf{S}$ uma estrutura de semianel comutativo profinito;*
2. *em $\overline{\Omega}_1\mathsf{M}$ uma estrutura de semianel com zero comutativo profinito;*
3. *em $\overline{\Omega}_1\mathsf{G}$ uma estrutura de anel comutativo profinito;*

Além disso,

1. *o subsemianel $\Omega_1\mathsf{S}$ de $\overline{\Omega}_1\mathsf{S}$ é isomorfo a $\mathbb{N}$;*
2. *o subsemianel com zero $\Omega_1\mathsf{M}$ de $\overline{\Omega}_1\mathsf{M}$ é isomorfo a $\mathbb{N}_0$;*
3. *o subanel $\Omega_1\mathsf{G}$ de $\overline{\Omega}_1\mathsf{G}$ é isomorfo a $\mathbb{Z}$.*

Demonstração. Seja então $\mathsf{V} \in \{\mathsf{S}, \mathsf{M}, \mathsf{G}\}$. Seja R o semianel $\mathbb{N}$, o semianel com zero $\mathbb{N}_0$ ou o anel $\mathbb{Z}$, conforme $\mathsf{V} = \mathsf{S}$, M ou G.

$\diamond$ *O grupóide $(\overline{\Omega}_1\mathsf{V}; \cdot)$ é comutativo.* Como $\Omega_1\mathsf{V}$ é um subespaço denso do espaço métrico $\overline{\Omega}_1\mathsf{V}$, para cada $\pi, \rho \in \overline{\Omega}_n\mathsf{V}$ existem sucessões $(x^{a_n})_n$ e $(x^{b_n})_n$ de elementos de $\Omega_n\mathsf{V}$ convergentes para π e ρ, respectivamente ($a_n, b_n \in R$). Logo, da continuidade da operação $\cdot$ resulta o seguinte:

$$\begin{aligned}\pi \cdot \rho &= \lim x^{a_n} \cdot \lim x^{b_n} = \lim (x^{a_n} \cdot x^{b_n}) = \lim x^{a_n + b_n} \\ &= \lim x^{b_n + a_n} = \lim (x^{b_n} \cdot x^{a_n}) = \lim x^{b_n} \cdot \lim x^{a_n} \\ &= \rho \cdot \pi\end{aligned}$$

Uma justificação igualmente simples para a comutatividade de $\cdot$ é a de que o modelo que construímos para $\overline{\Omega}_1\mathsf{V}$ é um limite projectivo de álgebras comutativas. No entanto a demonstração que demos usa uma técnica que vamos continuar a aplicar.

$\diamond$ *A operação de composição é contínua em $\overline{\Omega}_1\mathsf{V}$.* Este facto mais não é do que um caso particular do lema 2.28.

$\diamond$ *O monóide* $(\overline{\Omega}_1\mathsf{V}; \circ, x)$ *é comutativo.* Para cada $\pi, \rho \in \overline{\Omega}_1\mathsf{V}$, sejam $(x^{a_n})_n$ e $(x^{b_n})_n$ sucessões de elementos de $\Omega_n\mathsf{V}$ convergentes para π e ρ, respectivamente $(a_n, b_n \in R)$. Pela continuidade da composição em $\overline{\Omega}_1\mathsf{V}$,

$$\begin{aligned}\pi \circ \rho &= \lim x^{a_n} \circ \lim x^{b_n} = \lim (x^{a_n} \circ x^{b_n}) = \lim x^{a_n \times b_n} \\ &= \lim x^{b_n \times a_n} = \lim (x^{b_n} \circ x^{a_n}) = \lim x^{b_n} \circ \lim x^{a_n} \\ &= \rho \circ \pi\end{aligned}$$

$\diamond$ *A operação* $\circ$ *é distributiva relativamente à multiplicação* $\cdot$ *do grupóide* $\overline{\Omega}_1\mathsf{V}$. Sejam $u, v, w \in \overline{\Omega}_1\mathsf{V}$ e seja $(x^{a_n})_n$ uma sucessão de elementos de $\Omega_1\mathsf{V}$ convergente para u $(a_n \in R)$. Então,

$$\begin{aligned}u \circ (v \cdot w) &= \lim (x^{a_n} \circ (v \cdot w)) \qquad \text{(por } \circ \text{ ser contínua)} \\ &= \lim (x^{a_n}_{\overline{\Omega}_1\mathsf{V}}(v \cdot w)) \\ &= \lim (v \cdot w)^{a_n} \\ &= \lim (v^{a_n} \cdot w^{a_n}) \qquad \text{(por } \cdot \text{ ser comutativa)} \\ &= \lim v^{a_n} \cdot \lim w^{a_n} \qquad \text{(por } \cdot \text{ ser contínua)} \\ &= \lim (x^{a_n} \circ v) \cdot \lim (x^{a_n} \circ w) \\ &= (u \circ v) \cdot (u \circ w) \qquad \text{(novamente por } \circ \text{ ser contínua),}\end{aligned}$$

ficando assim provada a distributividade à direita. Graças à comutatividade de $\cdot$ e de $\circ$, a distributividade à esquerda resulta imediatamente da distributividade à direita.

$\diamond$ *O semianel* $\overline{\Omega}_1\mathsf{S}$*, o semianel com zero* $\overline{\Omega}_1\mathsf{M}$ *e o anel* $\overline{\Omega}_1\mathsf{G}$ *são profinitos.* Na verdade, vamos provar um resultado mais geral: os homomorfismos contínuos sobrejectivos de semigrupos, monóides ou grupos (conforme V seja igual a S, M ou G) de domínio $\overline{\Omega}_1\mathsf{V}$ e conjunto de chegada numa álgebra pró-V são homomorfismos de semianéis, semianéis com zero, anéis, respectivamente. Sejam A uma álgebra pró-V e φ um homomorfismo contínuo e sobrejectivo $\overline{\Omega}_1\mathsf{V} \to A$. Sejam $(u, u'), (v, v') \in \operatorname{Ker}\varphi$. Então

$$\varphi(u \circ v) = \varphi(u(v)) = u_A(\varphi(v)) = u_A(\varphi(v')) = \varphi(u \circ v').$$

Pela comutatividade de $\circ$, e por simetria,

$$\varphi(u \circ v') = \varphi(v' \circ u) = \varphi(v' \circ u') = \varphi(u' \circ v'),$$

pelo que $\varphi(u \circ v) = \varphi(u' \circ v')$, o que mostra a compatibilidade de $\circ$ com $\operatorname{Ker}\varphi$. Logo a álgebra A, isomorfa a $\overline{\Omega}_1\mathsf{V}/\operatorname{Ker}\varphi$, admite uma estrutura de semianel, semianel com zero ou anel (conforme V seja igual a S, M ou G), a qual torna φ num homomorfismo de semianéis, semianéis com zero, anéis, respectivamente.

$\diamond$ $\Omega_1\mathsf{V} \simeq R$. A função

$$\begin{aligned}\phi : R &\longrightarrow \Omega_1\mathsf{V} \\ k &\longmapsto x^k\end{aligned}$$

é um isomorfismo entre R e $\Omega_1\mathsf{V}$ (de facto, este isomorfismo é único). □

Torna-se muitas vezes mais cómodo considerar R como subálgebra de $\overline{\Omega}_1\mathsf{V}$ através do isomorfismo ϕ. Esta identificação de R com $\Omega_1\mathsf{V}$ dá-nos a motivação para fazer a seguinte convenção: se dada uma operação implícita π de $\overline{\Omega}_1\mathsf{V}$ adoptarmos algum símbolo ν para denotar π por x^ν, diremos que ν é um *expoente profinito* de π. Por exemplo, em G, -5 é um expoente profinito de x^{-5}, e 2^ω é um expoente profinito de x^{2^ω}. Estendemos formalmente a adição e a multiplicação em R a todos os expoentes profinitos de elementos de $\overline{\Omega}_1\mathsf{V}$, fazendo corresponder a adição à multiplicação $\cdot$ de operações implícitas, e a multiplicação à composição: se ν e μ forem expoentes profinitos, então $\nu+\mu$ é o expoente profinito de $x^\nu \cdot x^\mu$ e $\nu\mu$ é o de $x^\nu \circ x^\mu$. Por exemplo, em $\overline{\Omega}_1\mathsf{V}$, $\omega+\omega=\omega$ e $\omega\times\omega=\omega$. Os expoentes profinitos são uma forma prática de representar operações implícitas unárias e de com elas efectuar operações aritméticas. Há que ter cuidado com o símbolo 1: pode significar o expoente profinito de x ou o elemento neutro de $\overline{\Omega}_1\mathsf{M}$ ou de $\overline{\Omega}_1\mathsf{G}$ (cujo expoente profinito é 0).

Exemplo 2.32. *Consideremos o operador implícito unário $\pi(x)=x^n$ sobre S. Mais atrás já havíamos estabelecido a notação x^{n^ω} para $\pi^{\circ\omega}(x)$. Em geral, convencionamos denotar por x^{n^ν} a operação implícita $\pi^{\circ\nu}(x)$, para qualquer expoente profinito ν em $\overline{\Omega}_1\mathsf{M}$. Sob a representação de expoentes profinitos, eis alguns exemplos de relações aritméticas entre operações implícitas unárias sobre S:*

$$\begin{aligned}
&n^\omega \times n^\omega = n^{\omega+\omega} = n^\omega;\\
&n^{\omega-k} \times n^\omega = n^{(\omega-k)+\omega} = n^{\omega-k},\ k\in\mathbb{N};\\
&n^k \times n^{\omega-k} = n^{k+(\omega-k)} = n^\omega,\ k\in\mathbb{N}.
\end{aligned}$$

Exemplo 2.33. *Dois exemplos em $\overline{\Omega}_1\mathsf{G}$:*

$$(3^\omega-1)3^\omega = 3^\omega\times 3^\omega - 3^\omega = 3^{\omega+\omega}-3^\omega = 0;$$

$$\begin{aligned}
(2^{\omega-1}-1)(2^\omega+1) &= 2^{\omega-1}\times 2^\omega + 2^{\omega-1} - 2^\omega - 1\\
&= 2^{\omega-1+\omega} + 2^{\omega-1} - 2^\omega - 1\\
&= 2^{\omega-1} + 2^{\omega-1} - 2^\omega - 1\\
&= 2\times 2^{\omega-1} - 2^\omega - 1\\
&= 2^\omega - 2^\omega - 1\\
&= -1.
\end{aligned}$$

O exemplo precedente mostrou que o anel $\overline{\Omega}_1\mathsf{G}$ não é um domínio de integridade, e que tem outros invertíveis além de 1 e de -1.

Já $\overline{\Omega}_1\mathsf{S}$ e $\overline{\Omega}_1\mathsf{M}$ têm 1 como único elemento invertível. Para vermos que assim é, vamos supor que π é uma operação implícita em S (em M) distinta de x; então existe uma sucessão $(a_n)_n$ de elementos de $\mathbb{N}\setminus\{1\}$ (respectivamente, de $\mathbb{N}_0\setminus\{1\}$) tal que $(x^{a_n})_n$

converge para π em $\overline{\Omega}_1\mathsf{S}$ (respectivamente, em $\overline{\Omega}_1\mathsf{M}$); logo se M for o monóide de 3 elementos gerado por um elemento s tal que $s^2 = s^3$ então $\pi_M(1) = 1$ e $\pi_M(s) = \pi_M(s^2) \in \{1, s^2\}$, e portanto π_M não é invertível.

Também é fácil justificar que se em $\overline{\Omega}_1\mathsf{M}$ tivermos $\nu\mu = 0$ então $\nu = 0$ ou $\mu = 0$.

Para cada $n \in \mathbb{N}$, existe um único homomorfismo contínuo $\varphi_n : \overline{\Omega}_1\mathsf{V} \to \mathbb{Z}_n$ tal que $\varphi_n(x) = [1]_n$. Trata-se de um homomorfismo de semianéis, semianéis com zero ou anéis, conforme $\mathsf{V} = \mathsf{S}$, M ou G. Com justiça, podemos dizer que este é o homomorfismo canónico entre $\overline{\Omega}_1\mathsf{V}$ e $\mathbb{Z}_n$. Escreveremos por vezes $\pi \equiv \rho \pmod{n}$ quando $\varphi_n(\pi) = \varphi_n(\rho)$. Pelo argumento de unicidade habitual, se m divide n então $\varphi_m = \theta_{n,m} \circ \varphi_n$, onde $\theta_{n,m} : \mathbb{Z}_n \to \mathbb{Z}_m$ é o homomorfismo já apresentado no exemplo 2.9 e que, recordemos, associa $[k]_n$ a $[k]_m$.

No caso da pseudovariedade dos grupos finitos, as imagens pelos homomorfismos φ_n determinam completamente uma operação implícita: com efeito, se π e ρ forem operações implícitas unárias sobre G distintas, então existe um homomorfismo contínuo sobrejectivo $\psi : \overline{\Omega}_1\mathsf{G} \to F \in \mathsf{G}$ tal que $\psi(\pi) \neq \psi(\rho)$; sendo F um grupo cíclico, existe um isomorfismo $\eta : F \to \mathbb{Z}_n$, para algum $n \in \mathbb{N}$; pela sua unicidade, φ_n é igual a $\eta \circ \psi$, pelo que $\varphi_n(\pi) \neq \varphi_n(\rho)$. O que acabámos de descrever não pode ser estendido às pseudovariedades S e M: nesses casos, a operação implícita $x^{\omega+1}$ é distinta de x, e no entanto $\varphi_n(x^{\omega+1}) = \varphi_n(x) = [1]_n$ para todo $n \in \mathbb{N}$.

De agora em diante, até ao final deste capítulo, V designará uma das pseudovariedades S, M ou G.

Lema 2.34. *Para cada $n \in \mathbb{N}$, o conjunto dos múltiplos de n em $\overline{\Omega}_1\mathsf{V}$ é o núcleo de φ_n.*

Demonstração. O núcleo de φ_n é um fechado de $\overline{\Omega}_1\mathsf{V}$, donde $\overline{\operatorname{Ker}\varphi_n \cap \Omega_1\mathsf{V}} \subseteq \operatorname{Ker}\varphi_n$. Por outro lado, o núcleo de φ_n também é um aberto de $\overline{\Omega}_1\mathsf{V}$, pelo que, como a subálgebra $\Omega_1\mathsf{V}$ é densa, $\operatorname{Ker}\varphi_n \subseteq \overline{\operatorname{Ker}\varphi_n \cap \Omega_1\mathsf{V}}$. Tendo em atenção a continuidade da composição, concluímos que

$$\operatorname{Ker}\varphi_n = \overline{\operatorname{Ker}\varphi_n \cap \Omega_1\mathsf{V}} = \overline{\operatorname{Ker}\varphi_{n|\Omega_1\mathsf{V}}} = \overline{x^n \circ \Omega_1\mathsf{V}} = x^n \circ \overline{\Omega_1\mathsf{V}} = x^n \circ \overline{\Omega}_1\mathsf{V}.$$

Ou seja, para toda operação implícita π de $\overline{\Omega}_1\mathsf{V}$, π é um múltiplo de x^n se e só se $\varphi_n(\pi) = 0$. □

Definimos um *primo* de um anel, semianel, ou semianel com zero A como sendo um elemento π de A não invertível e diferente de zero tal que

$$\pi \text{ divide } ab \text{ implica que } \pi \text{ divide } a \text{ ou que } \pi \text{ divide } b, \quad \forall a, b \in A.$$

Uma vez munidos desta definição, podemos enunciar o seguinte corolário do lema 2.34:

Corolário 2.35. *Os primos de $\mathbb{N}$ são primos de $\overline{\Omega}_1\mathsf{V}$.*

Demonstração. Seja p um primo de $\mathbb{N}$. Suponhamos que π e ρ são elementos de $\overline{\Omega}_1\mathsf{V}$ tais que p divide o seu produto. Então, $0 = \varphi_p(\pi \circ \rho) = \varphi_p(\pi)\varphi_p(\rho)$. Como $\mathbb{Z}_p$ é um domínio de integridade, $\varphi_p(\pi) = 0$ ou $\varphi_p(\rho) = 0$, isto é, p divide π ou ρ. Resta-nos observar que p não é invertível: com efeito, se existisse $\rho \in \overline{\Omega}_1\mathsf{V}$ tal que $x = x^p \circ \rho$, então teríamos $[1]_p = (p\varphi_p(x))\varphi(\rho) = [0]_p$. □

Num anel, semianel ou semianel com zero, dois elementos a e b dizem-se *associados* se existir um invertível u tal que $a = ub$. A relação "associado" é uma relação de equivalência. Um elemento é primo se e só se todos os seus associados são primos. Veremos mais à frente que nem todos os primos de $\overline{\Omega}_1\mathsf{V}$ são associados de primos de $\mathbb{N}$.

No próximo exemplo representaremos as operações implícitas sob a forma dos seus expoentes profinitos. Parece-nos assim que obtemos uma maior transparência dos conteúdos. Até ao final deste capítulo, a regra será a representação de operações implícitas sob esta forma. A excepção a esta regra ficará patente quando, por exemplo, usarmos o sinal de composição $\circ$ para a multiplicação em $\overline{\Omega}_1\mathsf{V}$.

Exemplo 2.36. *Seja p um primo de $\mathbb{N}$. Consideremos em $\overline{\Omega}_1\mathsf{V}$ a operação implícita $p^\omega + (\omega - 1)$ (recordemos que se $\mathsf{V} = \mathsf{G}$ então $\omega = 0$). A sucessão $(p^{k!} + (k! - 1))_k$ converge para $p^\omega + (\omega - 1)$. Pelo pequeno teorema de Fermat, para todo o primo q de $\mathbb{N}$ distinto de p e para $k \geq q - 1$ a operação implícita $p^{k!} - 1$ é divisível por q, pelo que $p^{k!} + (k! - 1)$ é divisível por q se $k \geq q$. Como o conjunto dos múltiplos de q em $\overline{\Omega}_1\mathsf{V}$ é fechado, $p^\omega + (\omega - 1)$ é divisível por todos os primos de $\mathbb{N}$ distintos de p. Logo, a operação implícita $p^{\omega+1} + (\omega - 1)p$ é divisível por todos os primos de $\mathbb{N}$. E no entanto $p^{\omega+1} + (\omega - 1)p$ é diferente de zero, pois $\varphi_{p^2}(p^{\omega+1} + (\omega - 1)p) = [-p]_{p^2} \neq [0]_{p^2}$.*

Dada uma operação implícita ν sobre V e um primo p de $\mathbb{N}$, consideremos o conjunto não vazio

$$E_{\nu,p} = \{n \in \mathbb{N}_0 : p^n \text{ divide } \nu\}.$$

Vamos definir o expoente profinito

$$\operatorname{ord}_p \nu \in \mathbb{N}_0 \mathbin{\mathring{\cup}} \{\omega\}$$

do seguinte modo:

- se $E_{\nu,p}$ for limitado superiormente, então $\operatorname{ord}_p \nu$ é o máximo de $E_{\nu,p}$;
- se $E_{\nu,p}$ não for limitado superiormente, ou seja, se for igual a $\mathbb{N}_0$, então $\operatorname{ord}_p \nu = \omega$.

O expoente profinito $\operatorname{ord}_p \nu$ será uma ferramenta muito útil para organizarmos uma breve descrição de algumas propriedades aritméticas elementares de $\overline{\Omega}_1\mathsf{V}$. No que diz respeito a este desiderato, o nosso objectivo será o de obter propriedades que estejam próximas de algumas das propriedades básicas de um domínio de factorização única.

Lema 2.37. *Dados $\nu \in \overline{\Omega}_1\mathsf{V}$ e um primo p de $\mathbb{N}$, existe $\alpha \in \overline{\Omega}_1\mathsf{V}$ tal que $\nu = \alpha p^{\operatorname{ord}_p \nu}$ e p não divide α.*

Demonstração. Seja $n \in \mathbb{N}_0$ tal que p^n divide ν. Então existe $\alpha \in \overline{\Omega}_1\mathsf{V}$ tal que $\nu = \alpha p^n$. Se p dividir α então p^{n+1} divide ν, pelo que $n \neq \mathrm{ord}_p\, \nu$. Isto mostra o lema no caso em que $\mathrm{ord}_p\, \nu \in \mathbb{N}$. Suponhamos agora que $\mathrm{ord}_p\, \nu = \omega$, o que é equivalente a dizer que qualquer potência p^n ($n \in \mathbb{N}$) divide ν. Então existe uma sucessão $(u_n)_n$ de elementos de $\overline{\Omega}_1\mathsf{V}$ tal que

$$\nu = u_n p^{n!}.$$

Como $\overline{\Omega}_1\mathsf{V}$ é um espaço métrico compacto, a sucessão $(u_n)_n$ admite uma subsucessão $(u_{n_k})_k$ convergente para algum $u \in \overline{\Omega}_1\mathsf{V}$. Assim se mostra que p^ω divide ν:

$$\nu = \lim_{k \to +\infty} u_{n_k} p^{n_k!} = u p^\omega. \tag{2.14}$$

Se u não for divisível por p, então tomamos $\alpha = u$ e a demonstração termina aqui. Caso contrário, consideramos a operação implícita

$$\alpha = u + p^\omega + (\omega - 1).$$

Seja s um elemento de um qualquer semigrupo finito. Então, para k suficientemente grande,

$$\begin{aligned} s^{\alpha p^\omega} &= s^{(u+p^{k!}+(k!-1))p^{k!}} \\ &= s^{up^{k!}} \cdot s^{p^{k!}p^{k!}} \cdot s^{(k!-1)p^{k!}} \\ &= s^{up^{k!}} \cdot s^{p^{k!}} \cdot s^{k!p^{k!}-p^{k!}} \\ &= s^{up^{k!}+p^{k!}+k!p^{k!}-p^{k!}} \\ &= s^{up^\omega} s^{\omega p^\omega}. \end{aligned} \tag{2.15}$$

Ora s^{p^ω} é um elemento do subgrupo maximal do subsemigrupo gerado por s. Logo s^{up^ω} também é um elemento desse subgrupo maximal, cujo elemento neutro é s^ω, donde por (2.15) e por (2.14) concluímos que $s^{\alpha p^\omega} = s^\nu$. Como s é arbitrário,

$$\alpha p^\omega = \nu.$$

Ora,

$$\varphi_p(\alpha) = \varphi_p(u) + \varphi_p(p^\omega + (\omega - 1)) = \varphi_p(p^\omega + (\omega - 1)) = [-1]_p \neq [0]_p,$$

pelo que α não é divisível por p. □

Decorre da demonstração do lema 2.37 que $\mathrm{ord}_p\, \nu = \omega$ se e só se p^ω divide ν. De forma inteiramente análoga, para qualquer $k \in \mathbb{Z}$, concluiríamos que $\mathrm{ord}_p\, \nu = \omega$ se e só se $p^{\omega+k}$ divide ν.

Exemplo 2.38. *Para qualquer $k \in \mathbb{Z}$, temos $\mathrm{ord}_p\, p^{\omega+k} = \omega$. Em $\overline{\Omega}_1\mathsf{G}$ as operações implícitas*

$$u = p^{\omega+k} + (p^\omega - 1) \quad e \quad v = p^{\omega-k} + (p^\omega - 1)$$

são mutuamente inversas ($uv = 1$) *e são tais que*

$$p^{\omega+k} = up^{\omega} \quad e \quad p^{\omega} = vp^{\omega+k}.$$

Logo p^{ω} *e* $p^{\omega+k}$ *são elementos de* $\overline{\Omega}_1\mathsf{G}$ *associados. Considerando* $\nu = p^{\omega+k}$ *e* $\alpha = u$, *a igualdade* $p^{\omega+k} = up^{\omega}$ *exemplifica o lema 2.37: uma vez que a relação "divide" é transitiva, um elemento que divide um invertível também divide* 1, *logo* u *não é divisível por* p. *Por sua vez, a igualdade* $p^{\omega} = vp^{\omega+k}$ *permite-nos concluir que, no caso em que* $\operatorname{ord}_p \nu = \omega$, *o lema 2.37 permanece válido se tivermos* $\omega + k$ *no lugar de* $\operatorname{ord}_p \nu$; *isto porque* $\nu = \alpha p^{\omega}$ *implica* $\nu = \alpha v p^{\omega+k}$ *e* αv *não é divisível por* p *se* α *não for divisível por* p, *uma vez que* p *é um primo de* $\overline{\Omega}_1\mathsf{G}$ *e o invertível* v *também não é divisível por* p.

O próximo lema afirma a validade do recíproco do lema 2.37.

Lema 2.39. *Sejam* $\nu \in \overline{\Omega}_1\mathsf{V}$ *e* p *um primo de* $\mathbb{N}$. *Se* e *for um elemento de* $\mathbb{N}_0 \mathbin{\mathring{\cup}} \{\omega\}$ *para o qual existe* $\alpha \in \overline{\Omega}_1\mathsf{V}$ *tal que* $\nu = \alpha p^e$ *e* α *não é divisível por* p, *então* $e = \operatorname{ord}_p \nu$.

Demonstração. Consideremos o conjunto não vazio

$$E_{\nu,p} = \{n \in \mathbb{N}_0 : p^n \text{ divide } \nu\}$$

a partir do qual definimos $\operatorname{ord}_p \nu$. Se $e = \omega$ então $E_{\nu,p} = \mathbb{N}_0$ e portanto $\operatorname{ord}_p \nu = \omega = e$. Suponhamos agora que $e \in \mathbb{N}_0$. Seja $n \in E_{\nu,p}$. Consideremos também um elemento a de $\mathbb{N}$ tal que $\varphi_{p^n}(\alpha) = [a]_{p^n}$. Então,

$$[0]_{p^n} = \varphi_{p^n}(\nu) = \varphi_{p^n}(\alpha)\varphi_{p^n}(p^e) = [a]_{p^n}[p^e]_{p^n} = [ap^e]_{p^n},$$

ou seja, p^n divide ap^e. Por hipótese, $\varphi_p(\alpha) \neq [0]_p$. Ora

$$[a]_p = \theta_{p^n,p}([a]_{p^n}) = \theta_{p^n,p}(\varphi_{p^n}(\alpha)) = \varphi_p(\alpha),$$

pelo que p não divide a. Como p^n divide ap^e, isto implica $n \leq e$. Logo e majora $E_{\nu,p}$. Como $e \in E_{\nu,p}$, concluímos que $e = \operatorname{ord}_p \nu$. □

Em $\mathbb{N}_0 \mathbin{\mathring{\cup}} \{\omega\}$ vamos considerar uma operação binária $\oplus$ que estende a adição usual de $\mathbb{N}_0$ e onde ω é um elemento absorvente (isto é, $\omega \oplus e = e \oplus \omega = \omega$, $\forall e \in \mathbb{N}_0 \mathbin{\mathring{\cup}} \{\omega\}$).

Lema 2.40. *Seja* p *um primo de* $\mathbb{N}$. *Então*

$$\operatorname{ord}_p(\nu\mu) = \operatorname{ord}_p \nu \oplus \operatorname{ord}_p \mu$$

para quaisquer $\nu, \mu \in \overline{\Omega}_1\mathsf{V}$.

Demonstração. Pelo lema 2.37, existem $\alpha, \beta, u \in \overline{\Omega}_1\mathsf{V}$ não divisíveis por p tais que $\nu = \alpha p^{\mathrm{ord}_p \nu}$, $\mu = \beta p^{\mathrm{ord}_p \mu}$ e $p^{\mathrm{ord}_p \nu + \mathrm{ord}_p \mu} = u p^{\mathrm{ord}_p \nu \oplus \mathrm{ord}_p \mu}$.[18] Então

$$\nu\mu = \alpha\beta u p^{\mathrm{ord}_p \nu \oplus \mathrm{ord}_p \mu}.$$

Como α, β e u não são divisíveis por p e como p é um primo de $\overline{\Omega}_1\mathsf{V}$, o produto $\alpha\beta u$ também não é divisível por p. Do lema 2.39 deduzimos que

$$\mathrm{ord}_p(\nu\mu) = \mathrm{ord}_p \nu \oplus \mathrm{ord}_p \mu. \quad \square$$

Corolário 2.41. *Se p é um primo de $\mathbb{N}$ então p^ω é um primo de $\overline{\Omega}_1\mathsf{V}$ que não é associado de nenhum primo de $\mathbb{N}$.*

Demonstração. Sejam $\nu, \mu \in \overline{\Omega}_1\mathsf{V}$ tais que p^ω divide $\nu\mu$. Pelo lema anterior,

$$\mathrm{ord}_p \nu \oplus \mathrm{ord}_p \mu = \omega.$$

Esta igualdade implica $\mathrm{ord}_p \nu = \omega$ ou $\mathrm{ord}_p \mu = \omega$, ou seja, p^ω divide ν ou divide μ. Logo p^ω é um primo de $\overline{\Omega}_1\mathsf{V}$. Um associado de p^ω é divisível, por exemplo, por p^2, pelo que p^ω não é associado de nenhum primo de $\mathbb{N}$. $\square$

Segue-se uma proposição que podemos encarar como uma espécie de teorema de factorização única dos elementos de $\overline{\Omega}_1\mathsf{V}$ num produto de primos de $\mathbb{N}$.

Proposição 2.42. *Seja $(p_n)_{n\in\mathbb{N}}$ uma sucessão injectiva constituída por todos os primos de $\mathbb{N}$. Dado $\nu \in \overline{\Omega}_1\mathsf{V}$, consideremos em $\overline{\Omega}_1\mathsf{V}$ a sucessão*

$$z_n = \prod_{i=1}^{n} p_i^{\mathrm{ord}_{p_i} \nu}.$$

Para qualquer ponto de acumulação z de $(z_n)_n$ existe um elemento u de $\overline{\Omega}_1\mathsf{V}$ tal que $\nu = uz$ e u não é divisível por nenhum primo de $\mathbb{N}$.

Para cada primo p de $\mathbb{N}$ seja e_p um elemento de $\mathbb{N}_0 \mathbin{\mathring{\cup}} \{\omega\}$ e suponhamos que a sucessão em $\overline{\Omega}_1\mathsf{V}$

$$y_n = \prod_{i=1}^{n} p_i^{e_{p_i}}$$

tem um ponto de acumulação y para o qual existe um elemento v de $\overline{\Omega}_1\mathsf{V}$ tal que v não é divisível por nenhum primo de $\mathbb{N}$ e $\nu = vy$. Então, para qualquer primo p de $\mathbb{N}$ temos $e_p = \mathrm{ord}_p \nu$.

A propósito deste enunciado e antes de passarmos à sua demonstração, convém recordar que qualquer sucessão em $\overline{\Omega}_1\mathsf{V}$ tem um ponto de acumulação, uma vez que $\overline{\Omega}_1\mathsf{V}$ é um espaço métrico compacto.

[18] Se $(\mathrm{ord}_p \nu, \mathrm{ord}_p \mu) \in \mathbb{N}_0 \times \mathbb{N}_0 \mathbin{\mathring{\cup}} \{(\omega, \omega)\}$ então tomamos $u = 1$.

Demonstração da proposição 2.42. Vamos mostrar por indução sobre n que, para cada $n \in \mathbb{N}$, existe $u_n \in \overline{\Omega}_1 \mathsf{V}$ tal que

$$\nu = u_n z_n \text{ e } u_n \text{ não é divisível por } p_i,\ i = 1, \ldots, n. \tag{2.16}$$

O passo inicial é apenas o lema 2.37. Suponhamos que temos (2.16). Então, pelo lema 2.40,

$$\operatorname{ord}_{p_{n+1}}(\nu) = \operatorname{ord}_{p_{n+1}}(u_n) \oplus \left(\bigoplus_{i=1}^{n} \operatorname{ord}_{p_{n+1}}(p_i^{\operatorname{ord}_{p_i} \nu}) \right). \tag{2.17}$$

Se p e q são primos distintos de $\mathbb{N}$ então para qualquer $e \in \mathbb{N}_0 \mathbin{\mathring{\cup}} \{\omega\}$ a potência p^e não é divisível por q (para o caso em que $e = \omega$ basta invocar o exemplo 2.36: temos $p^\omega \equiv 1 \pmod{q}$). Logo se $i \leq n$ então $\operatorname{ord}_{p_{n+1}}(p_i^{\operatorname{ord}_{p_i} \nu}) = 0$. Por (2.17),

$$\operatorname{ord}_{p_{n+1}}(\nu) = \operatorname{ord}_{p_{n+1}}(u_n).$$

Daí que, pelo lema 2.37, existe um elemento u_{n+1} de $\overline{\Omega}_1 \mathsf{V}$ que não é divisível por p_{n+1} e tal que

$$u_n = u_{n+1} p_{n+1}^{\operatorname{ord}_{p_{n+1}}(\nu)}.$$

Substituindo em (2.16) obtemos

$$\nu = u_{n+1} z_{n+1} \text{ e } u_{n+1} \text{ não é divisível por } p_i,\ i = 1, \ldots, n, n+1.$$

Isto conclui o passo indutivo.

Seja $(z_{n_k})_k$ uma subsucessão convergente de $(z_n)_n$. Como $\overline{\Omega}_1 \mathsf{V}$ é um espaço métrico compacto, a sucessão $(u_{n_k})_k$ tem uma subsucessão $(u_{n_{k_l}})_l$ convergente para $u \in \overline{\Omega}_1 \mathsf{V}$. Então,

$$\nu = \lim_{l \to +\infty} u_{n_{k_l}} z_{n_{k_l}} = u \lim_{k \to +\infty} z_{n_k}.$$

Seja p um primo de $\mathbb{N}$. Provado (2.16), podemos dizer que existe uma ordem a partir da qual os termos da sucessão $(u_n)_n$ estão contidos em $\varphi_p^{-1}(\mathbb{Z}_p \setminus \{0\})$. Como este conjunto é fechado, u pertence-lhe. Logo u não é divisível por nenhum primo de $\mathbb{N}$.

Concluída a demonstração da primeira parte da proposição, passemos à segunda parte. Fixemos um primo p de $\mathbb{N}$. Seja $k \in \mathbb{N}$ tal que $p_k = p$. Então

$$n \geq k \Rightarrow \operatorname{ord}_p y_n = \bigoplus_{i=1}^{n} \operatorname{ord}_p(p_i^{e_{p_i}}) = e_p.$$

Ou seja,

$$n \geq k \Rightarrow \begin{cases} y_n \in \varphi_{p^{e_p}}^{-1}(0) \cap \varphi_{p^{e_p+1}}^{-1}(\mathbb{Z}_{p^{e_p+1}} \setminus \{0\}) & \text{se } e_p \in \mathbb{N}_0 \\ y_n \in \bigcap_{s \in \mathbb{N}} \varphi_{p^s}^{-1}(0) & \text{se } e_p = \omega \end{cases}$$

Pela continuidade de φ_m para qualquer $m \in \mathbb{N}$, os conjuntos

$$\varphi_{p^{e_p}}^{-1}(0) \cap \varphi_{p^{e_p+1}}^{-1}(\mathbb{Z}_{p^{e_p+1}} \setminus \{0\}) \quad \text{e} \quad \bigcap_{s \in \mathbb{N}} \varphi_{p^s}^{-1}(0)$$

são fechados, pelo que

$$\begin{cases} y \in \varphi_{p^{e_p}}^{-1}(0) \cap \varphi_{p^{e_p+1}}^{-1}(\mathbb{Z}_{p^{e_p+1}} \setminus \{0\}) & \text{se } e_p \in \mathbb{N} \\ y \in \bigcap_{s\in\mathbb{N}} \varphi_{p^s}^{-1}(0) & \text{se } e_p = \omega \end{cases}$$

ou seja, $\operatorname{ord}_p y = e_p$. Por outro lado $\operatorname{ord}_p \nu = \operatorname{ord}_p v \oplus \operatorname{ord}_p y = \operatorname{ord}_p y$, uma vez que v não é divisível por p. Logo $\operatorname{ord}_p \nu = e_p$. □

Exemplo 2.43. *Em $\overline{\Omega}_1\mathsf{G}$, para qualquer primo de $\mathbb{N}$ temos $\operatorname{ord}_p 0 = \omega$. A sucessão*

$$z_1 = 2^\omega, \quad z_2 = 2^\omega \times 3^\omega, \quad z_3 = 2^\omega \times 3^\omega \times 5^\omega, \quad z_4 = 2^\omega \times 3^\omega \times 5^\omega \times 11^\omega, \ldots$$

cujo n-ésimo termo é o produto das potências ómega dos n primeiros primos de $\mathbb{N}$ converge para 0, pois um grupo finito de ordem k satisfaz a pseudoidentidade $x^{z_n} = 1$ se $n \geq k$.

Mais geralmente, em $\overline{\Omega}_1\mathsf{S}$ e em $\overline{\Omega}_1\mathsf{M}$ a sucessão z_n converge para ω. Com efeito, se s é um elemento de um semigrupo finito então s^{z_n} é um elemento do subgrupo maximal G do subsemigrupo gerado por s, pelo que

$$n \geq |G| \Rightarrow s^{z_n} = (s^{z_n})^{z_n} = \textit{elemento neutro de } G = s^\omega,$$

pois $z_n \times z_n = z_n$; isto mostra que $(s^{z_n})_n$ é quase-constante igual a a^ω.

Exemplo 2.44. *Consideremos em $\overline{\Omega}_1\mathsf{V}$ a sucessão*

$$y_1 = 3, \quad y_2 = 3 \times 5, \quad y_3 = 3 \times 5 \times 7, \quad y_4 = 3 \times 5 \times 7 \times 11, \ldots$$

cujo n-ésimo termo é o produto dos n primeiros primos ímpares de $\mathbb{N}$. Se ν for um ponto de acumulação de $(y_n)_n$ então $\operatorname{ord}_2 \nu = 0$ e $\operatorname{ord}_p \nu = 1$ para qualquer primo ímpar p de $\mathbb{N}$. A sucessão $(y_n)_n$ é a subsucessão $(z_{n+1})_n$ da sucessão $(z_n)_n$ da proposição 2.42 que se obtém a partir de ν e da sucessão de números primos cujo n-ésimo termo é o n-ésimo número primo de $\mathbb{N}$. Vejamos agora que $(y_n)_n$ diverge. Para qualquer primo ímpar p de $\mathbb{N}$ temos a congruência $p \equiv \pm 1 \pmod 4$. Mais do que isso, existe uma infinidade desses primos que verificam $p \equiv -1 \pmod 4$, facto este que é um caso particular do bem conhecido teorema de Dirichlet sobre primos numa progressão aritmética[19] *[20]. Logo, a sucessão $(y_n)_n$ tem uma infinidade de termos no conjunto $\varphi_4^{-1}([-1]_4)$ e uma infinidade de termos no conjunto $\varphi_4^{-1}([1]_4)$. Como estes conjuntos são abertos disjuntos, concluímos que a sucessão $(y_n)_n$ é divergente em $\overline{\Omega}_1\mathsf{V}$.*

Estes exemplos ilustram alguns dos limites das nossas tentativas de aproximação de $\overline{\Omega}_1\mathsf{V}$ aos domínios de factorização única: o número de factores primos distintos de um elemento diferente de zero pode ser infinito, e a sucessão z_n da proposição 2.42 pode não ser convergente. Um outro ângulo do problema da procura de semelhanças

[19] Diz-nos este teorema que se a e b forem inteiros primos entre si, então existe uma infinidade de termos da progressão aritmética $an + b$ que são primos. A demonstração para o caso em que $a = 4$ e $b = 3$ (que é o que nos interessa neste momento) é um exercício simples.

entre $\overline{\Omega}_1\mathsf{V}$ e os domínios de factorização única consiste em saber em que medida é possível ir mais além no enunciado da proposição 2.42 substituindo a condição de u não ser divisível por nenhum primo de $\mathbb{N}$ pela mais forte de u ser invertível. A próxima proposição dá-nos uma resposta completa a esta questão no caso $\mathsf{V} = \mathsf{G}$, resposta essa que efectivamente vai no sentido da aproximação aos domínios de factorização única.

Proposição 2.45. *Um elemento de $\overline{\Omega}_1\mathsf{G}$ é invertível se e só se não é divisível por nenhum primo de $\mathbb{N}$.*

Demonstração. A implicação directa resulta do simples facto de um elemento de um anel dividir um invertível se e só se for ele mesmo um invertível. Reciprocamente, suponhamos que π não é divisível por nenhum primo de $\mathbb{N}$. Arbitrado $n \in \mathbb{N}$, seja $a \in \mathbb{N}$ tal que $\varphi_n(\pi) = [a]_n$. Seja p um qualquer primo de $\mathbb{N}$ que divide n. Como $[a]_p = \theta_{n,p}(\varphi_n(\pi)) = \varphi_p(\pi) \neq [0]_p$, os inteiros a e n são primos entre si. Logo o conjunto

$$A_n = \{z \in \mathbb{Z}_n : \varphi_n(\pi)z = [1]_n\}$$

é não vazio.[20] Consideremos k elementos $n_1, \ldots, n_k$ de $\mathbb{N}$, e seja m o seu produto. Uma vez que A_m é não vazio e φ_m é um homomorfismo sobrejectivo, podemos considerar um elemento ρ_m de $\varphi_m^{-1}(A_m)$. Aplicando a ambos os membros da igualdade $\varphi_m(\pi)\varphi_m(\rho_m) = [1]_m$ o homomorfismo θ_{m,n_i} obtemos $\varphi_{n_i}(\pi)\varphi_{n_i}(\rho_m) = [1]_{n_i}$. Logo ρ_m é um elemento de $\bigcap_{i=1}^{k} \varphi_{n_i}^{-1}(A_{n_i})$. Então a intersecção de qualquer subfamília finita da família de fechados $(\varphi_n^{-1}(A_n))_n$ é não vazia, e portanto pela compacidade de $\overline{\Omega}_1\mathsf{G}$,

$$\bigcap_{n\in\mathbb{N}} \varphi_n^{-1}(A_n) \neq \emptyset.$$

Existe portanto $\rho \in \overline{\Omega}_1\mathsf{V}$ tal que para todo $n \in \mathbb{N}$ se tem $\varphi_n(\pi)\varphi_n(\rho) = [1]_n$, ou seja, tal que

$$\varphi_n(\pi \circ \rho) = \varphi_n(x), \quad \forall n \in \mathbb{N}.$$

Ora, como já observámos na página 71, os elementos de $\overline{\Omega}_1\mathsf{G}$ ficam completamente determinados pelas suas imagens através dos homomorfismos φ_n, pelo que $\pi \circ \rho = x$. Logo π é invertível. □

Exemplo 2.46. *Como vimos no exemplo 2.36, se p for um primo de $\mathbb{N}$ então a operação implícita unária $p^{\omega+1} - p$ sobre G é divisível por todos os primos de $\mathbb{N}$. Assim, $p^{\omega+1} - p + 1 \equiv 1 \pmod{q}$, para todo o primo q de $\mathbb{N}$. Logo, a operação implícita $p^{\omega+1} - p + 1$ é um invertível de $\overline{\Omega}_1\mathsf{G}$ distinto de ± 1.*

Corolário 2.47. *Seja $(p_n)_{n\in\mathbb{N}}$ uma sucessão injectiva constituída por todos os primos de $\mathbb{N}$. Dado $\nu \in \overline{\Omega}_1\mathsf{G}$, consideremos em $\overline{\Omega}_1\mathsf{G}$ a sucessão*

$$z_n = \prod_{i=1}^{n} p_i^{\operatorname{ord}_{p_i}\nu}.$$

[20] Ou seja, a equação $\varphi_n(\pi)z = 1$ em $\mathbb{Z}_n$ tem solução na variável z, para qualquer $n \in \mathbb{N}$. Em [4] J. Almeida mostrou um teorema geral de compacidade do qual resulta a existência de soluções da equação $\pi z = 1$ em $\overline{\Omega}_1\mathsf{G}$ (estamos a referirmo-nos ao primeiro teorema da oitava secção desse artigo). No entanto preferimos utilizar um argumento mais elementar para demonstrar esta proposição.

Para qualquer ponto de acumulação z de $(z_n)_n$ existe um elemento u de $\overline{\Omega}_1\mathsf{G}$ tal que $\nu = uz$ e u é invertível.

Para cada primo p de $\mathbb{N}$ seja e_p um elemento de $\mathbb{N}_0 \mathring{\cup} \{\omega\}$ e suponhamos que a sucessão em $\overline{\Omega}_1\mathsf{G}$

$$y_n = \prod_{i=1}^{n} p_i^{e_{p_i}}$$

tem um ponto de acumulação y para o qual existe um elemento v de $\overline{\Omega}_1\mathsf{G}$ tal que v é invertível e $\nu = vy$. Então, para qualquer primo p de $\mathbb{N}$ temos $e_p = \operatorname{ord}_p \nu$.

Demonstração. Resulta imediatamente das proposições 2.42 e 2.45. □

Corolário 2.48. *Se ν é um primo de $\overline{\Omega}_1\mathsf{G}$, então existe um primo p de $\mathbb{N}$ tal que ν é associado de p ou de p^ω.*

Demonstração. Seja ν um primo de $\overline{\Omega}_1\mathsf{G}$. Pela proposição 2.45, existe um primo p de $\mathbb{N}$ que divide ν. Pelo lema 2.37, existem $e \in \mathbb{N} \mathring{\cup} \{\omega\}$ e $a \in \overline{\Omega}_1\mathsf{G}$ tais que $\nu = ap^e$ e p não divide a. Suponhamos que existe um primo q de $\mathbb{N}$ que divide a. Necessariamente, $q \neq p$. Como ν é primo, ν divide a ou ν divide p^e. Se ν divide a, então p divide a, o que é contraditório; se ν divide p^e então q divide p^e, o que é absurdo porque $q \neq p$. Logo a não é divisível por nenhum primo de $\mathbb{N}$ e portanto, pela proposição 2.45, é invertível. Concluímos assim que ν é um elemento associado de p^e em $\overline{\Omega}_1\mathsf{G}$. Então p^e é um primo de $\overline{\Omega}_1\mathsf{G}$, pelo que $e = 1$ ou $e = \omega$. □

Embora a implicação directa da proposição 2.45 seja válida em $\overline{\Omega}_1\mathsf{S}$ e em $\overline{\Omega}_1\mathsf{M}$, a recíproca já não o é. Um exemplo é dado pela operação implícita $\omega + 1$. Como em $\overline{\Omega}_1\mathsf{S}$ e $\overline{\Omega}_1\mathsf{M}$ esta operação é diferente do expoente profinito 1, ela não é invertível nem em $\overline{\Omega}_1\mathsf{S}$ nem em $\overline{\Omega}_1\mathsf{M}$. Ora, para todo o $n \in \mathbb{N}$, a imagem de $\omega + 1$ por $\varphi_n : \overline{\Omega}_1\mathsf{V} \to \mathbb{Z}_n$, $\mathsf{V} \in \{\mathsf{S}, \mathsf{M}\}$ é $[1]_n$, pelo que $\omega + 1$ não é divisível por nenhum elemento de $\mathbb{N}$.

A operação implícita $\omega + 1$ também serve para mostrar que o corolário 2.47 deixa de ser verdadeiro se nele substituirmos $\overline{\Omega}_1\mathsf{G}$ por $\overline{\Omega}_1\mathsf{S}$ ou $\overline{\Omega}_1\mathsf{M}$. Com efeito, para $\nu = \omega + 1$, como $\operatorname{ord}_p(\omega + 1) = 0$ para todo o primo p de $\mathbb{N}$, o elemento u da proposição 2.42 é a própria operação implícita $\omega + 1$, a qual não é invertível nem em $\overline{\Omega}_1\mathsf{S}$ nem em $\overline{\Omega}_1\mathsf{M}$.

Pelo lema 2.40, se p é um primo de $\mathbb{N}$ então as potências $p^{\omega+k}$ $(k \in \mathbb{Z})$ são primos de $\overline{\Omega}_1\mathsf{V}$, $\mathsf{V} \in \{\mathsf{G}, \mathsf{S}, \mathsf{M}\}$. Se $\mathsf{V} = \mathsf{G}$ então essas potências de p são associadas entre si (exemplo 2.38, ou então corolário 2.48). Pelo contrário, quaisquer dois elementos distintos de $\overline{\Omega}_1\mathsf{S}$ e de $\overline{\Omega}_1\mathsf{M}$ não são associados entre si, pois o expoente profinito 1 é o único invertível de $\overline{\Omega}_1\mathsf{S}$ e de $\overline{\Omega}_1\mathsf{M}$. Deixamos em aberto a seguinte questão: quais são os primos de $\overline{\Omega}_1\mathsf{S}$ e de $\overline{\Omega}_1\mathsf{M}$? Existe algum primo de $\overline{\Omega}_1\mathsf{S}$ ou de $\overline{\Omega}_1\mathsf{M}$ que não seja um primo p de $\mathbb{N}$ e que não seja da forma $p^{\omega+k}$?

Capítulo 3

Relance sobre a pseudovariedade dos grupos nilpotentes finitos

No presente capítulo, cruzam-se os temas desenvolvidos no capítulo anterior e aqueles que serão desenvolvidos no próximo, onde estudaremos a dinâmica de uma família muito particular de operadores, e onde as questões relacionadas com a nilpotência de um grupo finito desempenharão um papel alargado. Na terceira e última secção deste capítulo veremos uma condição necessária e suficiente para que um operador implícito seja invertível na pseudovariedade dos grupos nilpotentes finitos. Em contraste, os operadores implícitos sobre grupos finitos de que nos ocuparemos no próximo capítulo apenas são invertíveis no grupo trivial. Dada a relevância dos grupos nilpotentes na terceira secção deste capítulo e, mais ainda, no próximo capítulo, temos a precedê-la uma secção onde se dão algumas informações bem conhecidas e úteis sobre grupos nilpotentes e também sobre grupos solúveis. A primeira secção ocupa-se do comutador (ou, como veremos, dos comutadores) entre dois elementos, uma operação binária essencial (até para a elaboração de algumas definições básicas) em questões de nilpotência e solubilidade. A questão da definição de comutador, aflorada nesta secção, será posteriormente desenvolvida no próximo capítulo.

Resumindo, estamos perante um capítulo que ocupa uma posição de centralidade nesta monografia, enquanto ponto de cruzamento entre os capítulos adjacentes (o que, há que dizê-lo, porventura lhe confere um certo carácter heterogéneo).

3.1 Comutadores

A definição do comutador $[x, y]$ de dois elementos x e y de um grupo não está estabilizada na literatura da Teoria dos Grupos. Enquanto que nalguns livros e artigos a definição é

$$[x, y] = x^{-1}y^{-1}xy$$

já noutros é

$$[x, y] = xyx^{-1}y^{-1}.$$

É claro que segundo qualquer uma destas definições, x e y comutam se e só se o seu comutador é 1. Estaremos interessados em confrontar estas duas definições, pelo que nos convém distingui-las na nomenclatura e na notação. Assim, definimos o *comutador clássico* $[x, y]_c$ de x e y pela igualdade

$$[x, y]_c = x^{-1}y^{-1}xy$$

e o *comutador transposto* $[x, y]_t$ pela igualdade

$$[x, y]_t = xyx^{-1}y^{-1}$$

A relação entre estes dois tipos de comutadores é muito simples:

$$[x, y]_t = [x^{-1}, y^{-1}]_c.$$

A definição de *conjugado de um elemento* também varia na literatura conforme a definição de comutador adoptado. Adoptaremos aquela que está associada ao comutador clássico: ou seja, para nós o conjugado x^y de x por y é $y^{-1}xy$. Se $n \in \mathbb{Z}$ então x^{ny} designa o elemento $(x^y)^n$. A proposição seguinte exibe algumas das propriedades do comutador clássico e as correspondentes do comutador transposto.

Lema 3.1. *Se x, y e z são elementos de um grupo então:*

1. $[x, y]_c = [y, x]_c^{-1}$;
2. $[x, y]_c = [x, y^{-1}]_c^{-y} = [x^{-1}, y]_c^{-x}$;
3. $[xy, z]_c = [x, z]_c^y [y, z]_c$;
4. $[x, yz]_c = [x, z]_c[x, y]_c^z$;
5. $[x, y]_t = [y, x]_t^{-1}$;
6. $[x, y]_t = [x, y^{-1}]_t^{-y^{-1}} = [x^{-1}, y]_t^{-x^{-1}}$;
7. $[xy, z]_t = [y, z]_t^{x^{-1}} [x, z]_t$;
8. $[x, yz]_t = [x, y]_t[x, z]_t^{y^{-1}}$.

Sejam H e K subgrupos de um grupo G; o *subgrupo comutador* de H e K é o subgrupo $[H, K]$ de G gerado pelo conjunto dos comutadores clássicos de elementos de H com elementos de K:

$$[H, K] = \langle \{[h, k]_c : h \in H,\ k \in K\} \rangle.$$

Como $[h, k]_t = [h^{-1}, k^{-1}]_c$, podíamos ter escolhido para a definição de $[H, K]$ o comutador transposto no lugar do clássico:

$$[H, K] = \langle \{[h, k]_t : h \in H,\ k \in K\} \rangle.$$

Além disso, como $[h, k]_c = [k, h]_c^{-1}$, temos $[H, K] = [K, H]$.

A distinção que fizemos entre comutador clássico e transposto é da nossa exclusiva responsabilidade, e deve-se ao facto de não existir uma uniformidade de definições entre diversos artigos estudados, cujos conteúdos serão abordados no capítulo 4. Esta

situação surpreendeu o autor, pois, como verificaremos, a escolha do tipo de comutador não é inocente; e, no entanto, a leitura cruzada de apenas alguns dos artigos leva-nos a pensar que o era. Por exemplo, R. Brandl em [10] utiliza a definição do comutador clássico (sem no entanto o explicitar); de forma independente, D. Nikolova em [26] estuda o problema que ocupou R. Brandl em [10], mas agora sob a forma do comutador transposto, e no artigo conjunto [11] estes dois autores juntam esforços e utilizam de forma não explícita a definição de comutador clássico, sem que no entanto seja explicado o que se mantêm e o que se altera se mudarmos a definição de comutador.

3.2 Alguns resultados úteis sobre grupos nilpotentes ou solúveis

Nesta secção vamos fazer um sumário de algumas definições e resultados bem conhecidos sobre grupos nilpotentes e grupos solúveis. Para mais detalhes, remetemos o leitor para [30, 31].

Uma *série subnormal* de um grupo G é uma sequência de subgrupos

$$G = G_0 \geq G_1 \geq \ldots \geq G_n = 1 \tag{3.1}$$

tal que $G_{i+1} \lhd G_i$, $i \in \{0, \ldots, n-1\}$. Se $G_i \lhd G$, $i \in \{0, \ldots, n\}$, então estamos perante uma *série normal*. Os *factores* da série (3.1) são os grupos quocientes G_i/G_{i+1}. O inteiro n é o *comprimento* da série (3.1).

Sejam H e K subgrupos normais de G tais que K é um subgrupo de H. Dizemos que H/K é um *factor central* de G se H/K está contido no centro de G/K, o que é equivalente a $[H, G] \leq K$. Um grupo G *nilpotente* é um grupo que possui uma *série central*, que é uma série normal cujos factores são centrais. O menor inteiro que é comprimento de alguma série central de G é a *classe de nilpotência* de G. Assim, o grupo trivial é o único cuja classe de nilpotência é 0, e os grupos Abelianos não triviais são precisamente aqueles que têm classe de nilpotência igual a 1.

A *série central ascendente* de G é a sequência

$$1 = \zeta_0(G) \leq \zeta_1(G) \leq \zeta_2(G) \leq \ldots \tag{3.2}$$

cujos elementos se definem recursivamente pela regra de que $\zeta_{i+1}(G)/\zeta_i(G)$ é o centro de $G/\zeta_i(G)$. Reparemos que $\zeta_1(G)$ é igual a $Z(G)$, o centro de G. O conjunto

$$\zeta_\omega(G) = \bigcup_{i \in \mathbb{N}_0} \zeta_i(G)$$

é um subgrupo de G que é igual a G se e só se G é nilpotente. Se G for nilpotente, então a classe de nilpotência de G é o menor inteiro c tal que $\zeta_c(G) = G$.

A *série central descendente* de G é a sequência

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \gamma_3(G) \geq \dots \tag{3.3}$$

cujos elementos se definem recursivamente pela regra $\gamma_{i+1}(G) = [\gamma_i(G), G]$. Reparemos que $\gamma_2(G) = G'$, o subgrupo derivado de G. O conjunto

$$\gamma_\omega(G) = \bigcap_{i \in \mathbb{N}} \gamma_i(G)$$

é um subgrupo de G que é igual a 1 se e só se G é nilpotente. Se G for nilpotente, então a classe de nilpotência de G é o menor inteiro c tal que $\gamma_{c+1}(G) = 1$.

Recordemos que o normalizador de um subgrupo H de G é o subgrupo

$$N_G(H) = \{g \in G : H^g = H\}.$$

O número de subgrupos de G conjugados de H é o índice de $N_G(H)$. Um subgrupo K normaliza H se $K \leq N_G(H)$, o que é equivalente a $[H, K] \leq H$. Um grupo satisfaz a *condição do normalizador* se todo o subgrupo próprio estiver estritamente contido no seu normalizador.

Proposição 3.2.

1. *Se G é um grupo nilpotente e $1 \neq N \lhd G$, então $N \cap Z(G) \neq 1$.*
2. *Todo o grupo nilpotente satisfaz a condição do normalizador.*
3. *Todo o subgrupo maximal de um grupo nilpotente é normal.*

Como caso particular da condição 1, um grupo nilpotente não trivial tem centro não trivial. O recíproco de qualquer destas três condições não é verdadeiro. Tal no entanto não acontece com as duas últimas se nos restringirmos à classe dos grupos finitos. Os grupos nilpotentes finitos estão bem caracterizados pela próxima proposição:

Proposição 3.3. *Seja G um grupo finito. As seguintes propriedades são equivalentes:*

1. *G é nilpotente.*
2. *G satisfaz a condição do normalizador.*
3. *Todo o subgrupo maximal de G é normal.*
4. *G é o produto directo dos seus subgrupos de Sylow.*[1]

[1]Neste texto, subgrupo de Sylow será sempre sinónimo de p-subgrupo de Sylow, para algum primo p.

Dado um grupo G, o subgrupo gerado pelos seus subgrupos normais nilpotentes designa-se por *subgrupo de Fitting de* G e é denotado por $\mathrm{Fit}(G)$. Evidentemente, $\mathrm{Fit}(G)$ é um subgrupo normal. Se G for finito então $\mathrm{Fit}(G)$ é nilpotente.

Um grupo *solúvel* é um grupo que possui uma *série solúvel*, que é uma série subnormal cujos factores são Abelianos. Trivialmente, todo o grupo nilpotente é solúvel; por outro lado, o grupo S_3 das permutações em três letras é solúvel mas não é nilpotente. O menor inteiro que é comprimento de alguma série solúvel de um grupo solúvel G é o *grau de solubilidade* de G. Assim, o grupo trivial é o único cujo grau de solubilidade é 0, e os grupos Abelianos não triviais são precisamente aqueles que têm grau de solubilidade igual a 1. Um grupo diz-se *metabeliano* se o seu grau de solubilidade for menor ou igual a 2.

A *série derivada* de G é a sequência

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \dots \tag{3.4}$$

cujos elementos se definem recursivamente pela regra $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. Reparemos que $G^{(1)} = G'$, o subgrupo derivado de G. O conjunto

$$G^{(\omega)} = \bigcap_{i \in \mathbb{N}_0} G^{(i)}$$

é um subgrupo de G que é igual a 1 se e só se G é solúvel. Se G for solúvel, então o grau de solubilidade de G é o menor inteiro d tal que $G^{(d)} = 1$.

Apesar das classes dos grupos nilpotentes e solúveis não serem variedades, elas são fechadas para os operadores H e S. No caso da solubilidade, este facto tem uma espécie de recíproco:

Proposição 3.4. *Se H é um subgrupo normal de G tal que H e G/H são ambos solúveis, então G é solúvel.*

A transcrição da proposição 3.4 para grupos nilpotentes não é possível: A_3 e S_3/A_3 são ambos Abelianos, e no entanto S_3 não é nilpotente. O critério de P. Hall dá-nos uma condição análoga à da proposição 3.4 e que, embora um pouco mais fraca, é de grande importância:

Proposição 3.5 (Critério de P. Hall). *Se H é um subgrupo normal de G tal que H e G/H' são ambos nilpotentes, então G é nilpotente.*

Como assinala J. Rotman em [31, pág. 111], num comentário a uma demonstração, muitos teoremas da Teoria dos Grupos têm a estrutura lógica "a classe de grupos finitos $\mathcal{K}$ está contida na classe de grupos finitos $\mathcal{L}$", sendo a sua demonstração feita por redução ao absurdo do seguinte modo: se $\mathcal{K} \nsubseteq \mathcal{L}$, então existe um elemento G de $\mathcal{K} \setminus \mathcal{L}$ que tem ordem mínima; procuramos então produzir uma contradição a partir das características de G decorrentes da minimalidade da sua ordem. Por exemplo,

suponhamos que $\mathcal{L}$ é a pseudovariedade $\mathsf{G_{nil}}$ dos grupos nilpotentes finitos e que $\mathcal{K}$ é fechada para o operador S. Então G não é nilpotente e todos os seus subgrupos são elementos de $\mathcal{K}$; como G é um elemento de ordem mínima de $\mathcal{K} \setminus \mathsf{G_{nil}}$, todos os seus subgrupos próprios são nilpotentes. Neste ponto, torna-se útil o conhecimento da estrutura dos grupos finitos que não são nilpotentes e cujos subgrupos próprios são todos nilpotentes; são os chamados *grupos não-nilpotentes minimais*. A próxima proposição dá-nos informações valiosas sobre a sua estrutura:

Proposição 3.6 (O. J. Schmidt, [30]). *Suponhamos que G é um grupo não-nilpotente minimal. Então:*

1. *G é solúvel;*
2. *$|G| = p^m q^n$, onde p e q são primos distintos;*
3. *existe um único p-subgrupo de Sylow, e todo o q-subgrupo de Sylow é cíclico.*

Como todos os subgrupos de Sylow com a mesma ordem são conjugados entre si, dizer que o p-subgrupo de Sylow P de G é o seu único p-subgrupo de Sylow é o mesmo que dizer que P é um subgrupo normal de G; e dizer que todo o q-subgrupo de Sylow é cíclico, é o mesmo que dizer que algum q-subgrupo de Sylow Q é cíclico. Note-se também que $G = PQ$.

Voltemos ao exemplo genérico que antecedeu e motivou a exposição da proposição 3.6. Uma situação típica com que nos defrontaremos é aquela em que a classe $\mathcal{K}$ além de ser fechada para o operador S também é fechada para o operador H. Ou seja, dito de outro modo, em que $\mathcal{K}$ contém os divisores dos seus elementos. Nesse caso, se G é um elemento de ordem mínima da classe $\mathcal{K} \setminus \mathsf{G_{nil}}$, então todos os seus divisores próprios são nilpotentes. Daí o nosso interesse pela próxima proposição:

Proposição 3.7. *Suponhamos que G é um grupo finito não-nilpotente cujos divisores próprios são nilpotentes. Então:*

1. *G é um grupo não-nilpotente minimal;*
2. *todo o subgrupo normal próprio de G é Abeliano;*
3. *todos os subgrupos de Sylow de G são Abelianos;*
4. *$Z(G) = 1$.*

Demonstração. 1: Trivial.

2: Seja H um subgrupo normal próprio de G. Tal como qualquer subgrupo próprio, H é nilpotente. Suponhamos agora que $H' \neq 1$. Então G/H' é um divisor próprio de G, sendo por isso nilpotente. Mas então, pelo critério de P. Hall (proposição 3.5) o grupo G é nilpotente, o que é contraditório. Logo H é Abeliano.

3: Pela proposição 3.6, $G = PQ$, onde P é um p-subgrupo de Sylow normal e Q é um q-subgrupo de Sylow cíclico. Pela alínea anterior, P é Abeliano.

4: Se $Z(G) \neq 1$, então $G/Z(G)$ é um divisor próprio e portanto nilpotente, o que implica a nilpotência de G. Logo $Z(G) = 1$. □

Exemplo 3.8. *O grupo S_3 é um grupo que não é nilpotente mas cujos divisores próprios são nilpotentes. O grupo T de ordem 12 gerado por dois elementos a e b tais que $a^6 = 1$ e $b^2 = a^3 = (ab)^2$ [31] é um grupo não-nilpotente minimal que tem um divisor próprio que não é nilpotente: S_3.*

Uma outra situação frequente é aquela em que estamos perante a necessidade de demonstrar que uma determinada classe $\mathcal{K}$ de grupos finitos fechada para os operadores H e S está contida na pseudovariedade $\mathsf{G_{sol}}$ dos grupos solúveis finitos. Vamos supor que $\mathcal{K} \setminus \mathsf{G_{sol}} \neq \emptyset$. Então existe um elemento G de $\mathcal{K} \setminus \mathsf{G_{sol}}$ de ordem mínima. Como $\mathcal{K}$ é fechada para os operadores H e S, todos os divisores próprios de G estão em $\mathcal{K}$ e portanto, pela minimalidade da ordem de G, são solúveis. Mas então G é um grupo simples, pois se tivesse algum subgrupo normal próprio não trivial então, pela proposição 3.4, o grupo G seria solúvel. Por esta razão, mostrar que a classe $\mathcal{K}$ está contida em $\mathsf{G_{sol}}$ é o mesmo que mostrar que nenhum grupo finito simples não solúvel[2] cujos subgrupos próprios são solúveis está contido em $\mathcal{K}$. A lista dos grupos finitos simples não solúveis cujos subgrupos próprios são solúveis, grupos esses geralmente designados como *grupos simples minimais*, é um dos mais importantes produtos do famoso artigo em 6 partes ([33] é a primeira parte) de Thompson onde é feita a classificação dos grupos finitos simples não Abelianos cujos subgrupos locais são solúveis (um subgrupo local é o normalizador de algum subgrupo não trivial solúvel). Este trabalho de Thompson, além de ser considerado de inusitada dificuldade, tem a particularidade de prolongar-se por mais de 400 páginas. Em [15] encontramos comentários, referências e um enquadramento teórico das técnicas e resultados presentes no artigo mencionado.

3.3 Operadores invertíveis

Esta secção assenta estruturalmente em dois resultados: o primeiro deles dá-nos condições necessárias e suficientes para que um operador implícito sobre a pseudovariedade dos grupos finitos seja invertível na pseudovariedade dos p-grupos finitos; o segundo resultado é um corolário do primeiro, e dá-nos condições necessárias e suficientes para que um operador implícito sobre a pseudovariedade dos grupos finitos seja invertível na pseudovariedade dos grupos nilpotentes finitos. Em ambos os casos, uma dessas condições é de grande utilidade prática, pois permite-nos saber se o operador é invertível ou não na pseudovariedade em causa apenas com o cálculo de um

[2]Os grupos finitos simples solúveis são os grupos finitos simples Abelianos, ou seja, os grupos de ordem prima.

determinante. A dificuldade da demonstração do primeiro dos resultados mencionados reside essencialmente na suficiência das condições, o que será possível após a demonstração de um lema bastante geral que relaciona a invertibilidade de um operador implícito n-ário sobre uma pseudovariedade V com a subálgebra de $\overline{\Omega}_n\mathsf{V}$ gerada pelas componentes desse operador. Este lema é por si só deveras interessante. Os resultados que surgem ao longo desta secção são fruto do labor que deu corpo ao capítulo 2. Eles encontram-se expostos em [2], onde antecedem alguns resultados acerca de operadores implícitos sobre a pseudovariedade dos grupos finitos cuja potência ómega tem as duas coordenadas iguais em certas pseudovariedades de grupos finitos.

Mas comecemos então por fazer uma caracterização básica dos operadores invertíveis. Um operador implícito n-ário diz-se *invertível* se admitir inverso no monóide profinito $(\overline{\Omega}_n\mathsf{V})^n$.

Lema 3.9. *As seguintes condições são equivalentes para um qualquer operador implícito n-ário f:*

1. *f é invertível;*
2. *para toda a álgebra A pró-V, a transformação f_A é invertível;*
3. *para toda a álgebra A de V, a transformação f_A é invertível;*
4. *existe $g \in (\overline{\Omega}_n\mathsf{V})^n$ tal que $gf = 1$;*
5. *existe $g \in (\overline{\Omega}_n\mathsf{V})^n$ tal que $fg = 1$;*
6. *$f^\omega = 1$.*

Demonstração. A cadeia de equivalências $1 \Leftrightarrow 4 \Leftrightarrow 5 \Leftrightarrow 6$ é uma consequência do lema 2.24. Recordemos que a função

$$\begin{aligned} \epsilon_A : (\overline{\Omega}_n\mathsf{V})^n &\longrightarrow \mathscr{O}(A^n) \\ h &\longmapsto h_A \end{aligned}$$

é um homomorfismo (contínuo) de monóides, qualquer que seja a álgebra A pró-V. Este facto justifica a implicação $1 \Rightarrow 2$. A implicação $2 \Rightarrow 3$ é trivial. Vamos concluir com a justificação da implicação $3 \Rightarrow 6$. Seja A uma álgebra de V. Como o homomorfismo ϵ_A é contínuo, $(f^\omega)_A = (f_A)^\omega$. Ora o operador f é invertível em A se e só se $(f_A)^\omega = \mathrm{Id}_A$. Logo 3 é equivalente a

$$(f^\omega)_A = \mathrm{Id}_A, \quad \forall A \in \mathsf{V},$$

ou seja, é equivalente a que f^ω seja o operador identidade. □

Observemos que se f é invertível então o seu inverso é $f^{\omega-1}$.

Gostaríamos de sublinhar na demonstração do lema anterior a invocação do argumento de que os elementos de $\overline{\Omega}_n\mathsf{V}$ ficam completamente determinados pelas suas interpretações nos elementos de (um sistema de representantes de) V. O próximo lema evidencia esta possibilidade de sintetizar num só objecto — a álgebra $\overline{\Omega}_n\mathsf{V}$ — informação que diz respeito a todos os elementos de uma pseudovariedade, tirando depois proveito das características desse objecto.

Lema 3.10. *Um operador implícito $(w_1, \ldots, w_n)$ sobre V é invertível se e só se a subálgebra $\langle w_1, \ldots, w_n\rangle$ é densa em $\overline{\Omega}_n\mathsf{V}$.*

Demonstração. Seja φ o único endomorfismo contínuo de $\overline{\Omega}_n\mathsf{V}$ que envia x_i em w_i. Temos $\langle w_1, \ldots, w_n\rangle = \varphi(\langle x_1, \ldots, x_n\rangle) = \varphi(\Omega_n\mathsf{V})$, donde $\overline{\langle w_1, \ldots, w_n\rangle} = \varphi(\overline{\Omega}_n\mathsf{V})$. Mas se $\pi \in \overline{\Omega}_n\mathsf{V}$, então $\pi = \pi(x_1, \ldots, x_n)$ e portanto $\varphi(\pi) = \pi(\varphi(x_1), \ldots, \varphi(x_n)) = \pi(w_1, \ldots, w_n)$ pelo que

$$\overline{\langle w_1, \ldots, w_n\rangle} = \{\pi(w_1, \ldots, w_n) : \pi \in \overline{\Omega}_n\mathsf{V}\}. \tag{3.5}$$

Pela alínea 4 do lema 3.9, o operador $(w_1, \ldots, w_n)$ é invertível se e só se existem $\pi_1, \ldots, \pi_n \in \overline{\Omega}_n\mathsf{V}$ tais que $(\pi_1, \ldots, \pi_n)(w_1, \ldots, w_n) = (x_1, \ldots, x_n)$, ou seja,

$$x_i = \pi_i(w_1, \ldots, w_n). \tag{3.6}$$

Se $(w_1, \ldots, w_n)$ for invertível, então qualquer que seja $\rho \in \overline{\Omega}_n\mathsf{V}$, existem $\pi_1, \ldots, \pi_n \in \overline{\Omega}_n\mathsf{V}$ tais que

$$\rho = \rho(x_1, \ldots, x_n) = \rho((\pi_1, \ldots, \pi_n)(w_1, \ldots, w_n)) = \rho(\pi_1, \ldots, \pi_n)(w_1, \ldots, w_n)$$

pelo que se $\pi = \rho(\pi_1, \ldots, \pi_n)$ temos $\rho = \pi(w_1, \ldots, w_n)$. Tendo em conta (3.6), concluímos que $(w_1, \ldots, w_n)$ é invertível se e só se para todo $\rho \in \overline{\Omega}_n\mathsf{V}$ existe $\pi \in \overline{\Omega}_n\mathsf{V}$ tal que $\rho = \pi(w_1, \ldots, w_n)$. Logo pela igualdade (3.5) o operador $(w_1, \ldots, w_n)$ é invertível se e só se $\overline{\langle w_1, \ldots, w_n\rangle} = \overline{\Omega}_n\mathsf{V}$. □

Seja V uma pseudovariedade de monóides. Dada uma operação implícita n-ária w em V, a *frequência* da variável x_j é a operação implícita unária

$$|w|_j = w_{\overline{\Omega}_n\mathsf{V}}(\underbrace{1, \ldots, 1}_{j-1}, x, 1, \ldots, 1).$$

Esta definição está de acordo com a definição de frequência de uma variável num termo do tipo dos monóides, ou dos grupos: se p for um termo de um desses dois tipos, então a frequência da variável x_j no termo p é o único inteiro k tal que $|p_{\overline{\Omega}_n\mathsf{V}}(x_1, \ldots, x_n)|_j = x^k$ (encarando agora $x_1, \ldots, x_n$ e x como operações implícitas sobre V).

Seja $f = (w_1, \ldots, w_n)$ um operador implícito sobre V. A *matriz de frequências* de f é a matriz $n \times n$ cuja entrada (i, j) é a operação implícita unária $|w_i|_j$. Esta matriz é denotada por $A(f)$.

Exemplo 3.11. *Consideremos na pseudovariedade* G *dos grupos finitos os seguintes operadores implícitos:*

1. $f_1 = (yx^2y^3x^2y, y^2x^{-2}y^3x^{-1})$;
2. $f_2 = (x^{2^\omega}y, yxy)$;
3. $f_3 = (y^{15^\omega}x^{2^{\omega-1}}yx^{-1}y, xy^{2^\omega}x^{-1}y)$;
4. $f_4 = (y^{-1}x^2y^2x^2z^2x^2z^{-1}, z^{5^\omega-2}x^{-1}zx^2z, y^{5^{\omega-1}}xz^{-1})$.

A suas matrizes de frequências são, respectivamente,

1. $A(f_1) = \begin{pmatrix} 4 & 5 \\ -3 & 5 \end{pmatrix}$
2. $A(f_2) = \begin{pmatrix} 2^\omega & 1 \\ 1 & 2 \end{pmatrix}$
3. $A(f_3) = \begin{pmatrix} 2^{\omega-1}-1 & 15^\omega+2 \\ 0 & 2^\omega+1 \end{pmatrix}$
4. $A(f_4) = \begin{pmatrix} 6 & 1 & 1 \\ 1 & 0 & 5^\omega \\ 1 & 5^{\omega-1} & -1 \end{pmatrix}$

Lema 3.12. *Seja* f *um operador implícito sobre a pseudovariedade dos grupos finitos. Para todo o primo* p *de* $\mathbb{Z}$*, o operador* $f_{\mathbb{Z}_p}$ *é uma transformação linear cujo determinante é a imagem do determinante de* $A(f)$ *pelo homomorfismo canónico de anéis* $\varphi_p : \overline{\Omega}_1\mathsf{G} \to \mathbb{Z}_p$.

Demonstração. Sejam $w_1, \ldots, w_n$ as componentes de f. A linearidade de $f_{\mathbb{Z}_p}$ é equivalente à linearidade de $(w_i)_{\mathbb{Z}_p}$, para todo $i \in \{1, \ldots, n\}$. Pelo corolário 2.14, existe $u_i \in \Omega_1\mathsf{G}$ tal que $(w_i)_{\mathbb{Z}_p} = (u_i)_{\mathbb{Z}_p}$. A linearidade de $(u_i)_{\mathbb{Z}_p}$ não oferece dificuldades.

Como φ_p é um homomorfismo de anéis,

$$\begin{aligned} \varphi_p(\det A(f)) &= \varphi_p(\det(|w_i|_j)_{i,j}) = \det(\varphi_p(|w_i|_j))_{i,j} \\ &= \det(\varphi_p(|w_i|_j(x)))_{i,j} = \det((|w_i|_j)_{\mathbb{Z}_p}(\varphi_p(x)))_{i,j} \\ &= \det((|w_i|_j)_{\mathbb{Z}_p}([1]_p))_{i,j} = \det f_{\mathbb{Z}_p} \end{aligned}$$

sendo a última igualdade válida simplesmente porque $(|w_i|_j)_{\mathbb{Z}_p}([1]_p)$ é a imagem por $(w_i)_{\mathbb{Z}_p}$ do j-ésimo vector canónico do espaço vectorial $\mathbb{Z}_p^n$. □

Teorema 3.13. *Sejam* f *um operador implícito sobre a pseudovariedade dos grupos finitos e* p *um primo de* $\mathbb{N}$*. As seguintes condições são equivalentes:*

1. f *é invertível em* G_p;
2. f *é invertível em* Ab_p;
3. f *é invertível em* $\mathbb{Z}_p$;
4. $\det A(f) \not\equiv 0 \pmod{p}$.

Demonstração. A validade da cadeia $1 \Rightarrow 2 \Rightarrow 3$ decorre imediatamente da cadeia de inclusões $\mathsf{G}_p \supseteq \mathsf{Ab}_p \supseteq \{\mathbb{Z}_p\}$.

Diz-nos o lema 2.34 que os múltiplos de p em $\overline{\Omega}_1\mathsf{G}$ são os elementos do núcleo do homomorfismo canónico $\varphi_p : \overline{\Omega}_1\mathsf{G} \to \mathbb{Z}_p$. Donde, pelo lema 3.12, o determinante de $A(f)$ é divisível por p se e só se $f_{\mathbb{Z}_p}$ não é uma transformação linear invertível.

Falta-nos mostrar $3 \Rightarrow 1$, o que faremos na versão do contra-recíproco. Suponhamos então que $f = (w_1, \ldots, w_n)$ não é invertível em G_p. Pelo lema 3.10, encarando $w_1, \ldots, w_n$ como operações implícitas sobre G_p, sabemos que $H = \overline{\langle w_1, \ldots, w_n \rangle}$ é um subgrupo topológico próprio de $\overline{\Omega}_n\mathsf{G}_p$. Então do lema 2.15 resulta a existência de um p-grupo finito F e de um homomorfismo contínuo e sobrejectivo $\varphi : \overline{\Omega}_n\mathsf{G}_p \to F$ tais que $\varphi(H)$ é um subgrupo próprio de F. Por ser próprio, o subgrupo $\varphi(H)$ está contido num subgrupo maximal K de F. Os subgrupos maximais de p-grupos finitos são normais e têm indíce p. Sabemos então que existe um homomorfismo $\eta : F \to \mathbb{Z}_p$ cujo núcleo é K. Detenhamo-nos no diagrama (3.7):

$$\begin{array}{ccc} n & \xrightarrow{\iota} & \overline{\Omega}_n\mathsf{G}_p \\ & \searrow^{(\eta\circ\varphi)\circ\iota} & \downarrow{\scriptstyle \eta\circ\varphi} \\ & & \mathbb{Z}_p \end{array} \tag{3.7}$$

Como $\eta\circ\varphi$ é um homomorfismo contínuo, da comutatividade do diagrama (3.7) resulta que

$$(w_i)_{\mathbb{Z}_p}((\eta \circ \varphi) \circ \iota) = \eta \circ \varphi(w_i) = \eta(0) = 0$$

sendo a penúltima igualdade justificada por $\varphi(w_i) \in \varphi(H) \leq K = \operatorname{Ker}\eta$. Logo $f_{\mathbb{Z}_p}((\eta \circ \varphi) \circ \iota) = \vec{0}$. Se $f_{\mathbb{Z}_p}$ for injectiva, então $(\eta \circ \varphi) \circ \iota = \vec{0}$. Como o homomorfismo nulo $\overline{\Omega}_n\mathsf{G}_p \to \mathbb{Z}_p$ é contínuo, pela sua propriedade de unicidade $\eta\circ\varphi$ é o homomorfismo nulo. Mas então $\eta(F) = (\eta \circ \varphi)(\overline{\Omega}_n\mathsf{V}) = \{0\}$, o que é absurdo pois $\operatorname{Ker}\eta = K < F$. Logo a transformação $f_{\mathbb{Z}_p}$ não é injectiva. □

É de assinalar o paralelismo da condição 4 do teorema anterior com a condição de invertibilidade de uma transformação linear num espaço vectorial de dimensão finita em termos do valor do respectivo determinante. Como vimos durante a demonstração do teorema, este paralelismo surge do lema 3.12. O próximo corolário também é muito sugestivo do ponto de vista do valor do determinante da matriz de frequências.

Corolário 3.14. *Sejam f um operador implícito sobre a pseudovariedade dos grupos finitos. As seguintes condições são equivalentes:*

1. *f é invertível em $\mathsf{G}_{\mathsf{nil}}$;*
2. *f é invertível em Ab;*
3. *$\det A(f)$ é invertível.*

Demonstração. Vamos fazer a demonstração através da cadeia $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$. A implicação $1 \Rightarrow 2$ resulta da inclusão $\mathsf{G}_{\mathsf{nil}} \supseteq \mathsf{Ab}$. Pela mesma ordem de ideias, se f é invertível em Ab então, para todo o primo p de $\mathbb{N}$, é invertível em $\mathbb{Z}_p$ e portanto, pelo teorema 3.13, temos as seguintes condições equivalentes:

a) $\det A(f) \not\equiv 0 \pmod{p}$, para todo o primo p de $\mathbb{N}$;

b) f é invertível em G_p, para todo o primo p de $\mathbb{N}$.

A proposição 2.45 diz-nos que a condição *a)* (e portanto também *b)*) é equivalente à invertibilidade de $\det A(f)$, o que mostra 2⇒3. Por outro lado, como todo o grupo nilpotente finito é o produto directo dos seus subgrupos de Sylow, a condição *b)* permite-nos concluir que f é invertível em $\mathsf{G}_{\mathsf{nil}}$. Como *b)* ⇔ *a)* ⇔ 3, isto mostra 3⇒1. □

Exemplo 3.15. *Consideremos os operadores do exemplo 3.11:*

1. $f_1 = (yx^2y^3x^2y, y^2x^{-2}y^3x^{-1})$;
2. $f_2 = (x^{2^\omega}y, yxy)$;
3. $f_3 = (y^{15^\omega}x^{2^{\omega-1}}yx^{-1}y, xy^{2^\omega}x^{-1}y)$;
4. $f_4 = (y^{-1}x^2y^2x^2z^2x^2z^{-1}, z^{5^\omega-2}x^{-1}zx^2z, y^{5^{\omega-1}}xz^{-1})$.

Como $\det A(f_1) = 35$, *pelo teorema 3.13 o operador* f_1 *não é invertível nem em* $\mathbb{Z}_5$ *nem em* $\mathbb{Z}_7$, *mas é invertível em* G_p *para todo o primo* p *de* $\mathbb{N}$ *diferente de* 5 *e de* 7. *Logo se* π *for o conjunto dos primos de* $\mathbb{N}$ *diferentes de* 5 *e de* 7, *o operador* f *é invertível em* $\mathsf{G}_{\mathsf{nil},\pi}$, *que é a pseudovariedade gerada pela família de pseudovariedades* $(\mathsf{G}_p)_{p\in\pi}$.

As matrizes de frequências dos operadores f_2, f_3 *e* f_4 *têm determinante igual a* $2^{\omega+1}-1$, -1 *e* 1, *respectivamente. Vimos no exemplo 2.46 que a operação implícita* $2^{\omega+1}-1$ *é invertível. Logo estes três operadores são invertíveis em* $\mathsf{G}_{\mathsf{nil}}$.

Exemplo 3.16. *O operador binário* $f = (x^{-1}y^{-1}xyx, y)$ *é invertível em* $\mathsf{G}_{\mathsf{nil}}$, *uma vez que o determinante da sua matriz de frequências é* 1. *No entanto não é invertível em* S_3: *a órbita do par de transposições* $((1,2),(1,3))$ *cai no ponto fixo* $((1,3),(1,3))$, *logo na primeira iteração.*

Capítulo 4

Operadores de Engel

Os *operadores de Engel* são os seguintes operadores polinomiais binários de grupos:

$$\xi_c = ([x,y]_c, y), \quad \xi_t = ([x,y]_t, y),$$

$$\xi_{c,d} = (x, [x,y]_c), \quad \xi_{t,d} = (x, [x,y]_t).$$

Os operadores ξ_c, ξ_t, $\xi_{c,d}$ e $\xi_{t,d}$ são referidos como operador de Engel *clássico*, *transposto*, *clássico direito* e *transposto direito*, respectivamente.

O Teorema de Zorn [35] é um dos resultados mais significativos desta monografia, e será demonstrado neste capítulo. O Teorema de Zorn estabelece uma relação entre a nilpotência de um grupo finito e o comportamento dinâmico dos operadores de Engel, fornecendo uma caracterização dinâmica da pseudovariedade dos grupos nilpotentes finitos. Esta caracterização exprime-se através de uma pseudoidentidade com duas variáveis. Nos anos sessenta, quase três décadas depois do aparecimento do Teorema de Zorn (1936), N. D. Gupta e H. Heineken contribuíram com novos resultados sobre a influência da dinâmica dos operadores de Engel em aspectos estruturais dos grupos, de que destacamos a solubilidade em grupos finitos [18, 17, 19]. Posteriormente, com preocupações semelhantes, salientam-se nos anos 80 os trabalhos de D. B. Nikolova e R. Brandl [24, 25, 26, 10, 8, 11].

Devemos chamar a atenção para o facto de que os trabalhos mencionados surgem sob uma aparência que, na nossa opinião, em maior ou menor grau, esconde a perspectiva dinâmica com que o autor desta monografia os vê (o artigo conjunto de N. D. Gupta e H. Heineken pode ser apontado como aquele que mais se aproxima desta perspectiva). Também não encontramos neles conceitos básicos da Álgebra Universal Finita, como os de pseudovariedade ou de operação implícita, o que em alguns dos artigos se justifica pelo simples facto do desenvolvimento e divulgação destes conceitos ser posterior à sua publicação. No entanto, parece-nos que a utilização da linguagem da Álgebra Universal Finita facilita a apresentação e compreensão do seu conteúdo.

Algum do trabalho recente de J. Almeida ([2, 5, 3]) chamou a atenção do autor para o carácter dinâmico de vários dos resultados dos artigos atrás mencionados.

A próxima secção pode ser considerada como um preâmbulo abstracto ao estudo dos fenómenos de periodicidade dos operadores de Engel. Poderíamos ter dispensado esta abstracção, mas somos da opinião de que não ganharíamos nada com isso, nem sequer em compreensibilidade. Pelo contrário, julgamos que a nossa abordagem permitirá focarmo-nos no que é essencial, estabelecendo também uma ligação com os capítulos anteriores, especialmente o precedente.

4.1 Operadores pré-periódicos

A invertibilidade da interpretação de um operador implícito m-ário f numa álgebra A pró-V é apenas um dos possíveis comportamentos interessantes que o sistema dinâmico (A^m, f_A) pode ter. Como acontece com qualquer sistema dinâmico num conjunto finito, se a álgebra A for finita então o subsemigrupo de $(A^m)^{A^m}$ gerado por f_A é (tal como $(A^m)^{A^m}$) finito e portanto o sistema (A^m, f_A) é periódico ou pré-periódico. Ainda sob a hipótese da finitude de A, notemos que a periodicidade de f_A é equivalente à sua invertibilidade. Mesmo que a álgebra A pró-V não seja finita, se a interpretação de f em A for uma transformação pré-periódica, então o par (n_A, k_A), constituído respectivamente pelo pré-período e pelo período de f_A, é um invariante por isomorfismos de álgebras topológicas: se B é uma álgebra topológica isomorfa a A, então $(n_A, k_A) = (n_B, k_B)$. Por esta razão dizemos que o par (n_A, k_A) é o *invariante* de f em A.

De acordo com o que vimos na primeira secção do capítulo 2, uma álgebra A pró-V satisfaz a pseudoidentidade de operadores $f^n = f^{n+k}$ (com $n \geq 0$ e $k > 0$) se e só se f_A é uma transformação pré-periódica com pré-período menor ou igual a n e período divisor de k. Naturalmente surge uma questão que terá um papel importante quando nas secções seguintes concretizarmos o estudo dos operadores de Engel: qual a influência dos parâmetros n e k na estrutura dos elementos da pseudovariedade $[\![f^n = f^{n+k}]\!]$? A próxima proposição permite-nos organizar a procura de uma resposta a esta questão. Com efeito, ela diz-nos nas suas partes 1 e 2 como colocar adequadamente o problema da influência que isoladamente cada um dos parâmetros tem, e diz-nos na sua parte 3 que fazer o estudo de ambos os parâmetros separadamente é o mesmo que fazê-lo em simultâneo.

Proposição 4.1. *Seja f um operador implícito sobre* V. *Verificam-se as seguintes igualdades ($n \in \mathbb{N}_0$ e $k \in \mathbb{N}$):*

1. $\bigcup_{n\in\mathbb{N}_0} [\![f^n = f^{n+k}]\!] = [\![f^\omega = f^{\omega+k}]\!]$;
2. $\bigcup_{k\in\mathbb{N}} [\![f^n = f^{n+k}]\!] = [\![f^n = f^{n+\omega}]\!]$;
3. $[\![f^n = f^{n+k}]\!] = [\![f^\omega = f^{\omega+k}]\!] \cap [\![f^n = f^{n+\omega}]\!]$.

Demonstração.

1 e 2: É imediato que $[\![f^\omega = f^{\omega+k}]\!] \subseteq \bigcup_{n\in\mathbb{N}_0}[\![f^{n!} = f^{n!+k}]\!]$ e que $[\![f^n = f^{n+\omega}]\!] \subseteq \bigcup_{k\in\mathbb{N}}[\![f^n = f^{n+k!}]\!]$. Reciprocamente, suponhamos que $A \in [\![f^n = f^{n+k}]\!]$. Então $A \models f^l = f^{l+k}$ para todo $l \geq n$; em particular, $A \models f^{l!} = f^{l!+k}$ para todo $l \geq n$, donde $A \models f^\omega = f^{\omega+k}$. Por outro lado, $A \models f^n = f^{n+kq}$, para todo $q \geq 1$; em particular, $A \models f^n = f^{n+q!}$, para todo $q \geq k$, pelo que $A \models f^n = f^{n+\omega}$.

3: A inclusão directa resulta de 1 e 2. Reciprocamente, se A pertence à pseudovariedade $[\![f^\omega = f^{\omega+k}]\!] \cap [\![f^n = f^{n+\omega}]\!]$ então f_A tem período divisor de k e pré-período menor ou igual a n, pelo que $A \models f^n = f^{n+k}$. □

Concluímos que a pseudovariedade $[\![f^\omega = f^{\omega+k}]\!]$ (respectivamente, a pseudovariedade $[\![f^n = f^{n+\omega}]\!]$) é a pseudovariedade das álgebras de V nas quais o período (respectivamente, o pré-período) da interpretação de f é divisor de k (respectivamente, menor ou igual a n).

Em analogia com o caso dos operadores implícitos, se f for um operador m-ário polinomial e A for uma álgebra qualquer onde f_A seja pré-periódico, então o par (n_A, k_A), formado respectivamente pelo pré-período e período de f_A, é um invariante por isomorfismos de álgebras. Dizemos que o par (n_A, k_A) é o *invariante* de f de A. Também é verdade que a álgebra A satisfaz a identidade de operadores polinomiais $f^n = f^{n+k}$ se e só se f_A é uma transformação pré-periódica com pré-período menor ou igual a n e período divisor de k.

4.2 Comutadores de Engel

Para cada $n \in \mathbb{N}_0$, sejam [29]:

- $[x, {}_n y]_c$ a primeira componente de ξ_c^n;
- $[x, {}_n y]_t$ a primeira componente de ξ_t^n;
- $[{}_n x, y]_c$ a segunda componente de $\xi_{c,d}^n$;
- $[{}_n x, y]_t$ a segunda componente de $\xi_{t,d}^n$.

A segunda componente de ξ_c^n e de ξ_t^n é o termo y e a primeira componente de $\xi_{c,d}^n$ e de $\xi_{t,d}^n$ é o termo x. Logo, o estudo do comportamento dinâmico de ξ_c e de ξ_t (respectivamente, $\xi_{c,d}$ e $\xi_{t,d}$) reduz-se ao estudo da primeira (respectivamente, segunda) componente das suas iterações. Os termos $[x, {}_n y]_c$, $[x, {}_n y]_t$, $[{}_n x, y]_c$ e $[{}_n x, y]_t$ são os n-ésimos comutadores de Engel *clássico*, *transposto*, *clássico direito* e *transposto direito*, respectivamente. Cada um destes termos satisfaz uma relação de recorrência

que decorre imediatamente da sua definição: para $l \in \{c, t\}$,

$$\begin{cases} [x, {}_0y]_l = x \\ [x, {}_ny]_l = [[x, {}_{n-1}y]_l, y]_l \quad \text{se } n \geq 1 \end{cases} \quad \text{e} \quad \begin{cases} [{}_0x, y]_l = y \\ [{}_nx, y]_l = [x, [{}_{n-1}x, y]_l]_l \quad \text{se } n \geq 1. \end{cases}$$

A próxima proposição apresenta seis relações entre estes quatro tipos de comutadores.

Proposição 4.2. *As seguintes identidades são válidas em qualquer grupo:*

1. $[x, {}_ny]_c = [{}_ny^{-1}, x]_c^{y^n}$, $n \geq 0$;
2. $[x, {}_ny]_t = [{}_ny^{-1}, x]_t^{y^{-n}}$, $n \geq 0$;
3. $[x, {}_ny]_t = [[{}_{n-1}y^{-1}, x^{-1}]_c, y^{-1}]_c$, $n \geq 1$;
4. $[{}_nx, y]_t = [x^{-1}, [y^{-1}, {}_{n-1}x^{-1}]_c]_c$, $n \geq 1$;
5. $[x, {}_ny]_t = [[x^{-1}, {}_{n-1}y]_c, y^{-1}]_c^{y^{-(n-1)}}$, $n \geq 1$;
6. $[{}_nx, y]_t = [x^{-1}, [{}_{n-1}x, y^{-1}]_c]_c^{x^{-(n-1)}}$, $n \geq 1$.

Demonstração. A demonstração das quatro primeiras alíneas faz-se por indução, sendo o passo inicial trivial. Façamos o passo indutivo de cada uma delas:

- $[x, {}_ny]_c = [{}_ny^{-1}, x]_c^{y^n}$, $n \geq 0$:

$$\begin{aligned} [x, {}_{n+1}y]_c &= [[x, {}_ny]_c, y]_c \\ &= [[{}_ny^{-1}, x]_c^{y^n}, y]_c \\ &= [[{}_ny^{-1}, x]_c, y]_c^{y^n} \\ &= [y, [{}_ny^{-1}, x]_c]_c^{-y^n} && \text{pela alínea 1 do lema 3.1} \\ &= [y^{-1}, [{}_ny^{-1}, x]_c]_c^{y^{n+1}} && \text{pela alínea 2 do lema 3.1} \\ &= [{}_{n+1}y^{-1}, x]_c^{y^{n+1}} \end{aligned}$$

- $[x, {}_ny]_t = [{}_ny^{-1}, x]_t^{y^{-n}}$, $n \geq 0$:

$$\begin{aligned} [x, {}_{n+1}y]_t &= [[x, {}_ny]_t, y]_c \\ &= [[{}_ny^{-1}, x]_t^{y^{-n}}, y]_t \\ &= [[{}_ny^{-1}, x]_t, y]_t^{y^{-n}} \\ &= [y, [{}_ny^{-1}, x]_t]_t^{-y^{-n}} && \text{pela alínea 5 do lema 3.1} \\ &= [y^{-1}, [{}_ny^{-1}, x]_t]_t^{y^{-(n+1)}} && \text{pela alínea 6 do lema 3.1} \\ &= [{}_{n+1}y^{-1}, x]_t^{y^{-(n+1)}} \end{aligned}$$

- $[x, {}_n y]_t = [[{}_{n-1}y^{-1}, x^{-1}]_c, y^{-1}]_c$, $n \geq 1$:

$$\begin{aligned}
[x, {}_{n+1}y]_t &= [[x, {}_n y]_t, y]_t \\
&= [[x, {}_n y]_t^{-1}, y^{-1}]_c \\
&= [[[{}_{n-1}y^{-1}, x^{-1}]_c^{-1}, y^{-1}]_c^{-1}, y^{-1}]_c \\
&= [[y^{-1}, [{}_{n-1}y^{-1}, x^{-1}]_c]_c, y^{-1}]_c \qquad \text{pela alínea 1 do lema 3.1} \\
&= [[{}_n y^{-1}, x^{-1}]_c, y^{-1}]_c
\end{aligned}$$

- $[{}_n x, y]_t = [x^{-1}, [y^{-1}, {}_{n-1}x^{-1}]_c]_c$, $n \geq 1$

$$\begin{aligned}
[{}_{n+1}x, y]_t &= [x, [{}_n x, y]_t]_t \\
&= [x^{-1}, [{}_n x, y]_t^{-1}]_c \\
&= [x^{-1}, [x^{-1}, [y^{-1}, {}_{n-1}x^{-1}]_c]_c^{-1}]_c \\
&= [x^{-1}, [[y^{-1}, {}_{n-1}x^{-1}]_c, x^{-1}]_c]_c]_c \qquad \text{pela alínea 1 do lema 3.1} \\
&= [x^{-1}, [y^{-1}, {}_n x^{-1}]_c]_c
\end{aligned}$$

A quinta alínea demonstra-se directamente a partir da terceira e da primeira:

$$[x, {}_n y]_t = [[{}_{n-1}y^{-1}, x^{-1}]_c, y^{-1}]_c = [[x^{-1}, {}_{n-1}y]_c^{y^{-(n-1)}}, y^{-1}]_c = [[x^{-1}, {}_{n-1}y]_c, y^{-1}]_c^{y^{-(n-1)}}.$$

Analogamente, a sexta alínea demonstra-se directamente a partir da quarta e da primeira:

$$[{}_n x, y]_t = [x^{-1}, [y^{-1}, {}_{n-1}x^{-1}]_c]_c = [x^{-1}, [{}_{n-1}x, y^{-1}]_c^{x^{-(n-1)}}]_c = [x^{-1}, [{}_{n-1}x, y^{-1}]_c]_c^{x^{-(n-1)}}.$$

□

As igualdades da proposição 4.2 permitem-nos facilmente demonstrar a seguinte proposição:

Proposição 4.3. *Seja $n \in \mathbb{N}_0$. Verificam-se as seguintes igualdades entre variedades de grupos:*

$$[[x, {}_n y]_c = 1] = [[x, {}_n y]_t = 1] = [[{}_n x, y]_c = 1] = [[{}_n x, y]_t = 1].$$

Demonstração. Seja $n \in \mathbb{N}$. Se $n = 0$ então a proposição é trivialmente verdadeira. Suponhamos que $n \geq 1$ e seja G um grupo. Pela alínea 1 da proposição 4.2,

$$\begin{aligned}
G \models [x, {}_n y]_c = 1 &\Leftrightarrow G \models [{}_n y^{-1}, x]_c^{y^n} = 1 \\
&\Leftrightarrow G \models [{}_n y^{-1}, x]_c = 1 \\
&\Leftrightarrow G \models [{}_n x, y]_c = 1.
\end{aligned}$$

tendo a última equivalência resultado da substituição de x e y por y e x^{-1}, respectivamente.

Analogamente, pela alínea 2 da proposição 4.2,

$$G \models [x, {}_n y]_t = 1 \Leftrightarrow G \models [{}_n x, y]_t = 1.$$

Finalmente, pela alínea 3 da proposição 4.2,

$$\begin{aligned} G \models [x, {}_n y]_t = 1 &\Leftrightarrow G \models [[{}_{n-1} y^{-1}, x^{-1}]_c, y^{-1}]_c = 1 \\ &\Leftrightarrow G \models [y^{-1}, [{}_{n-1} y^{-1}, x^{-1}]_c]_c = 1 \\ &\Leftrightarrow G \models [{}_n y^{-1}, x^{-1}]_c = 1 \\ &\Leftrightarrow G \models [{}_n x, y]_c = 1. \end{aligned}$$

tendo a última equivalência resultado da substituição de x e y por y^{-1} e x^{-1}, respectivamente. □

Um grupo da variedade $[[x, {}_n y]_c = 1]$ é um *n-grupo de Engel* [30, 29].

O conceito de n-ésimo comutador de Engel admite uma generalização profinita natural. Seja ν um expoente profinito da pseudovariedade dos monóides. As operações implícitas $[x, {}_\nu y]_c$ e $[x, {}_\nu y]_t$ são as primeiras componentes dos operadores implícitos $((\xi_c)_{\overline{\Omega}_2 \mathsf{G}})^\nu$ e $((\xi_t)_{\overline{\Omega}_2 \mathsf{G}})^\nu$, respectivamente; e as operações implícitas $[{}_\nu x, y]_c$ e $[{}_\nu x, y]_t$ são as segundas componentes dos operadores implícitos $(\xi_{c,d})^\nu$ e $(\xi_{t,d})^\nu$, respectivamente.

Em qualquer grupo G, se $n \geq i$ então os comutadores $[x, {}_n y]_c$, $[x, {}_n y]_t$, $[{}_n x, y]_c$, $[{}_n x, y]_t$ são elementos de $\gamma_{i+1}(G)$. Se G for um grupo profinito, então $[x, {}_\omega y]_c = \lim [x, {}_{n!} y]_c$; uma vez que os elementos da série central descendente de G são fechados, $[x, {}_\omega y]_c$ é um elemento de $\gamma_\omega(G)$. Do mesmo modo, $[x, {}_\omega y]_t$, $[{}_\omega x, y]_c$ e $[{}_\omega x, y]_t$ pertencem a $\gamma_\omega(G)$.

4.3 Identidades de Engel

Ao longo desta secção devemos ter bem presente o conteúdo da secção 4.1.

De forma muito sintética, podemos dizer que os trabalhos [18, 17, 19, 24, 25, 26, 11, 10, 8] preocupam-se com a influência dos invariantes dos operadores de Engel na estrutura dos grupos onde são pré-periódicos (especialmente nos grupos finitos), no que diz respeito à nilpotência e à solubilidade. Os dois primeiros itens da próxima proposição reduzem o estudo dos invariantes dos quatro operadores de Engel aos invariantes de apenas dois deles: ξ_c e ξ_t.

Proposição 4.4. *Sejam $n, k \in \mathbb{N}$. Verificam-se as seguintes igualdades entre variedades de grupos:*

1. $\left[[x, {}_n y]_c = [x, {}_{n+k} y]_c\right] = \left[[{}_n x, y]_t = [{}_{n+k} x, y]_t\right]$;
2. $\left[[x, {}_n y]_t = [x, {}_{n+k} y]_t\right] = \left[[{}_n x, y]_c = [{}_{n+k} x, y]_c\right]$;
3. $\left[[x, {}_n y]_c^{y^k} = [x, {}_{n+k} y]_c\right] = \left[[{}_n x, y]_c = [{}_{n+k} x, y]_c\right]$;
4. $\left[[x, {}_n y]_t^{y^{-k}} = [x, {}_{n+k} y]_t\right] = \left[[{}_n x, y]_t = [{}_{n+k} x, y]_t\right]$.

Demonstração. Seja G um grupo arbitrário. Aplicando a igualdade 4 da proposição 4.2, temos:

$$G \models [{}_n x, y]_t = [{}_{n+k} x, y]_t \Leftrightarrow$$

$$\Leftrightarrow G \models [x^{-1}, [y^{-1}, {}_{n-1} x^{-1}]_c]_c = [x^{-1}, [y^{-1}, {}_{n+k-1} x^{-1}]_c]_c$$

$$\Leftrightarrow G \models [y^{-1}, {}_{n-1} x^{-1}]_c^{-1} x^{-1} [y^{-1}, {}_{n-1} x^{-1}]_c = [y^{-1}, {}_{n+k-1} x^{-1}]_c^{-1} x^{-1} [y^{-1}, {}_{n+k-1} x^{-1}]_c$$

$$\Leftrightarrow G \models ([y^{-1}, {}_{n-1} x^{-1}]_c^{-1} x^{-1} [y^{-1}, {}_{n-1} x^{-1}]_c)^{-1} = ([y^{-1}, {}_{n+k-1} x^{-1}]_c^{-1} x^{-1} [y^{-1}, {}_{n+k-1} x^{-1}]_c)^{-1}$$

$$\Leftrightarrow G \models [y^{-1}, {}_{n-1} x^{-1}]_c^{-1} x [y^{-1}, {}_{n-1} x^{-1}]_c = [y^{-1}, {}_{n+k-1} x^{-1}]_c^{-1} x [y^{-1}, {}_{n+k-1} x^{-1}]_c$$

$$\Leftrightarrow G \models [y^{-1}, {}_{n-1} x^{-1}]_c^{-1} x [y^{-1}, {}_{n-1} x^{-1}]_c \, x^{-1} = [y^{-1}, {}_{n+k-1} x^{-1}]_c^{-1} x [y^{-1}, {}_{n+k-1} x^{-1}]_c \, x^{-1}$$

$$\Leftrightarrow G \models [y^{-1}, {}_n x^{-1}]_c = [y^{-1}, {}_{n+k} x^{-1}]_c$$

$$\Leftrightarrow G \models [x, {}_n y]_c = [x, {}_{n+k} y]_c.$$

Ficou assim provada a primeira igualdade de variedades. A segunda demonstra-se a partir da igualdade 3 da proposição 4.2 de forma análoga. Mostremos a terceira. Aplicando agora a igualdade 1 da proposição 4.2, temos:

$$G \models [{}_n x, y]_c = [{}_{n+k} x, y]_c \Leftrightarrow$$

$$\Leftrightarrow G \models [{}_n y^{-1}, x]_c = [{}_{n+k} y^{-1}, x]_c$$

$$\Leftrightarrow G \models [x, {}_n y]_c^{y^{-n}} = [x, {}_{n+k} y]^{y^{-(n+k)}}$$

$$\Leftrightarrow G \models ([x, {}_n y]_c^{y^{-n}})^{y^{n+k}} = ([x, {}_{n+k} y]_c^{y^{-(n+k)}})^{y^{n+k}}$$

$$\Leftrightarrow G \models [x, {}_n y]_c^{y^k} = [x, {}_{n+k} y]_c.$$

A última igualdade também se demonstra de forma análoga à terceira. □

Feita a redução do nosso estudo aos operadores ξ_c e ξ_t, designemos o invariante de ξ_c num grupo G como *invariante clássico de Engel* de G, e o invariante de ξ_t como *invariante transposto de Engel* de G.

A proposição 4.4 tem a seguinte versão profinita como corolário:

Proposição 4.5. *Sejam $n, k \in \mathbb{N}$. Verificam-se as seguintes igualdades entre pseudovariedades de grupos finitos:*

1. *(a)* $[\![[x, {}_\omega y]_c = [x, {}_{\omega+k} y]_c]\!] = [\![[{}_\omega x, y]_t = [{}_{\omega+k} x, y]_t]\!]$;
   (b) $[\![[x, {}_\omega y]_t = [x, {}_{\omega+k} y]_t]\!] = [\![[{}_\omega x, y]_c = [{}_{\omega+k} x, y]_c]\!]$;
   (c) $[\![[x, {}_\omega y]_c^{y^k} = [x, {}_{\omega+k} y]_c]\!] = [\![[{}_\omega x, y]_c = [{}_{\omega+k} x, y]_c]\!]$;
   (d) $[\![[x, {}_\omega y]_t^{y^{-k}} = [x, {}_{\omega+k} y]_t]\!] = [\![[{}_\omega x, y]_t = [{}_{\omega+k} x, y]_t]\!]$;
2. $[\![[x, {}_n y]_c = [x, {}_{n+\omega} y]_c]\!] = [\![[{}_n x, y]_c = [{}_{n+\omega} x, y]_c]\!] =$
   $[\![[x, {}_n y]_t = [x, {}_{n+\omega} y]_t]\!] = [\![[{}_n x, y]_t = [{}_{n+\omega} x, y]_t]\!]$.

Demonstração. A parte 1 resulta trivialmente da proposição 4.4, e a parte 2 surge também imediatamente da proposição 4.4 e do facto de que num grupo finito a potência ómega de um elemento qualquer ser o elemento neutro. □

Corolário 4.6. *Num grupo finito, o pré-período de ξ_c é igual ao pré-período de ξ_t.*

Demonstração. Sejam G um grupo finito, e n_l o pré-período de $(\xi_l)_G$, $l \in \{c, t\}$. O grupo G satisfaz a pseudoidentidade $[x, {}_{n_c} y]_c = [x, {}_{n_c+\omega} y]_c$. Então pela alínea 2 da proposição 4.5 também satisfaz a pseudoidentidade $[x, {}_{n_c} y]_t = [x, {}_{n_c+\omega} y]_t$. Logo $n_t \leq n_c$. Analogamente, $n_c \leq n_t$. □

Não obstante num grupo finito G o pré-período de ξ_c ser igual ao de ξ_t, as órbitas por ξ_c e por ξ_t de um ponto de $G \times G$ podem ter pré-períodos distintos. Obtivemos alguns exemplos deste fenómeno fazendo cálculos num computador com o GAP [32]. Neste programa a composição de permutações é feita aplicando primeiro a permutação da esquerda: se π e ρ são permutações do grupo simétrico S_n em n letras então $\pi\rho$ envia i em $\rho(\pi(i))$. A permutação cíclica de S_n que envia um elemento i_j do subconjunto $\{i_1, \ldots, i_r\}$ de cardinal r de $\{1, \ldots, n\}$ em i_{j+1} (com $i_{r+1} = i_1$) e deixa fixos os restantes elementos de $\{1, \ldots, n\}$ é denotada no GAP por $(i_1, i_2, \ldots, i_r)$. Os cálculos efectuados deram-nos como exemplo o grupo S_4 e o ponto $((2,3,4),(1,4,2,3))$ de $S_4 \times S_4$, cuja órbita por ξ_t tem pré-período igual a 1 (e período igual a 4), enquanto que a órbita do mesmo ponto por ξ_c tem pré-período igual a 2 (e período igual a 2).

Como consequência do corolário 4.6, o pré-período de ξ_c num grupo finito (igual ao de ξ_t) será designado apenas como *pré-período de Engel*. O grupo S_3 é um exemplo de um grupo finito cujo invariante clássico de Engel difere do invariante transposto de Engel: o primeiro é igual a $(2,1)$ e o segundo é igual a $(2,2)$.

Resumindo, a pseudovariedade $[\![[x, {}_n y]_c = [x, {}_{n+\omega} y]_c]\!]$ é a classe dos grupos finitos com pré-período de Engel menor ou igual a n, a pseudovariedade $[\![[x, {}_\omega y]_c = [x, {}_{\omega+k} y]_c]\!]$ é a classe dos grupos finitos onde o período de ξ_c é divisor de k e $[\![[x, {}_\omega y]_t = [x, {}_{\omega+k} y]_t]\!]$ é a classe daqueles onde o período de ξ_t é divisor de k.

4.4 Invariantes de Engel de alguns grupos

Se, para $l \in \{c, t\}$, no grupo G a transformação ξ_l é periódica, então existe $n \in \mathbb{N}$ tal que

$$(\xi_l)^n_G(x, y) = (x, y)$$

para quaisquer $x, y \in G$. Em particular,

$$\forall x \in G,\ (x, x) = (\xi_l)^n_G(x, x) = ([x, {}_n x]_l, x) = (1, x).$$

Ou seja, o grupo trivial é o único grupo onde os operadores de Engel são periódicos.

Na tabela 4.1 (ver página 103) estão indicados os invariantes de Engel de alguns grupos, que são identificados de acordo com as seguintes notações [31]:

- S_n para o grupo simétrico em n letras;
- A_n para o grupo alternado em n letras;
- D_{2n} para o grupo diedral de ordem $2n$;
- Q para o grupo dos quaterniões;
- T para o grupo de ordem 12 gerado por dois elementos a e b tais que $a^6 = 1$ e $b^2 = a^3 = (ab)^2$;
- $PSL(n, q)$ para o grupo projectivo unimodular (ou grupo projectivo especial linear [15]) de dimensão n sobre o corpo de Galois de ordem $q = p^l$, onde p é um primo.

O grupo projectivo unimodular $PSL(n, q)$ é simples se e só se $n = 2$ e $q \geq 4$ ou se $n \geq 3$. O grupo alternado A_n também é simples quando (e apenas quando) $n \neq 4$.

Não existem na tabela 4.1 pares de grupos finitos isomorfos entre si e nela estão representadas todas as classes de isomorfismo dos grupos finitos de ordem menor do que dezasseis.[1] Na sequência destas observações, convém assinalar os seguintes isomorfismos, os quais esgotam todos os isomorfismos envolvendo apenas grupos projectivos unimodulares ou grupos alternados [31]:

$$PSL(2,3) \simeq A_4; \qquad PSL(2,4) \simeq PSL(2,5) \simeq A_5; \qquad PSL(2,9) \simeq A_6;$$
$$PSL(2,7) \simeq PSL(3,2); \qquad PSL(4,2) \simeq A_8.$$

[1] Recordemos que existe uma única classe de isomorfismo de grupos não Abelianos de ordem seis. Nesta classe estão S_3, D_6 e $PSL(2,2)$.

A inclusão de alguns grupos projectivos unimodulares na tabela 4.1 vem a propósito de [11], onde é calculado o invariante transposto de Engel de $PSL(2,q)$ até $q = 13$, inclusivé. Ainda em [11] é mostrado que o pré-período de Engel de $PSL(2,q)$ é igual a 3 se e só se $q \in \{4,5,8\}$.

O cálculo dos invariantes de Engel dos grupos finitos da tabela 4.1 foi feito num computador utilizando o GAP [32], tendo sido confirmados os cálculos efectuados em [11]. O algoritmo que utilizámos é bastante simples e baseia-se no lema 2.2:

```
engt:=function(g)
    local n, k, x, y, nxy, kxy, c, list, stop, i;
    n:=0;
    k:=1;
    for x in g do
        for y in g do
            list:=[];
            stop:=0;
            nxy:=0;
            c:=x;
            while stop = 0 do
                list[nxy+1]:=c;
                c:=c*y*c^(-1)*y^(-1);
                for i in [0..nxy] do
                    if c = list[i+1] then
                        stop:=1;
                        kxy:=nxy+1-i;
                        break;
                    fi;
                od;
                nxy:=nxy+1;
            od;
            if nxy-kxy > n then
                n:=nxy-kxy;
            fi;
            k:=Lcm(k, kxy);
        od;
    od;
    return [n, k];
end;
```

Recordemos que o grupo diedral de ordem $2m$ é o único grupo desta ordem gerado por dois elementos a e b tais que

$$b^m = 1,\ a^2 = 1,\ \text{e}\ aba = b^{-1}.$$

Grupo	Ordem	Transposto	Clássico
Trivial	1	(0,1)	
Abeliano não trivial	$\neq 1$	(1,1)	
S_3	6	(2,2)	(2,1)
D_8	8	(2,1)	
Q	8	(2,1)	
D_{10}	10	(2,4)	
D_{12}	12	(2,2)	(2,1)
T	12	(2,2)	(2,1)
A_4	12	(2,3)	
D_{14}	14	(2,3)	(2,6)
A_5	60	(3,60)	
A_6	360	(4,120)	
A_7	2520	(15,35280)	
S_4	24	(2,12)	(2,6)
S_5	120	(3,60)	
S_6	720	(4,1320)	
S_7	5040	(21,388080)	
$PSL(2,7)$	168	(4,168)	
$PSL(2,8)$	504	(3,126)	
$PSL(2,11)$	660	(6,1980)	
$PSL(2,13)$	1092	(7,2184)	
$PSL(2,16)$	4080	(5,2040)	
$PSL(2,19)$	3420	(9,17100)	
$PSL(2,23)$	6072	(8,121440)	
$PSL(3,3)$	5616	(21,34320)	

Tabela 4.1: Invariantes de Engel de alguns grupos

Em [16] é feita uma referência ao cálculo feito na tese de Doutoramento [24] de D. Nikolova dos invariantes de Engel dos grupos D_{2p}, no caso em que p é um primo. No entanto, não encontrámos nenhuma referência ao conteúdo, na sua máxima força, da próxima proposição.

Proposição 4.7. *Para cada inteiro positivo m maior do que 2, sejam $\alpha \in \mathbb{N}_0$ e $\beta \in \mathbb{N}$ tais que β é ímpar e $m = 2^\alpha \beta$. Então o pré-período de Engel de D_{2m} é igual a $\max\{2, \alpha\}$, e os períodos de ξ_t e de ξ_c em D_{2m} são iguais à ordem de 2 e de -2 em $\mathbb{Z}_\beta^*$, respectivamente.*

Demonstração. Seja n o pré-período de Engel de D_{2m}. Para cada $l \in \{c, t\}$, designemos por k_l o período de ξ_l, e para cada ponto P de $D_{2m} \times D_{2m}$ designemos por $n_{P,l}$ e $k_{P,l}$ o pré-período e o período da órbita de P por ξ_l, respectivamente. O nosso propósito será utilizar o lema 2.2.

Sejam a e b dois elementos de D_{2m} tais que

$$D_{2m} = \langle a, b \rangle,\ b^m = 1,\ a^2 = 1,\ \text{e}\ aba = b^{-1}.$$

Todos os pontos de D_{2m} são da forma

$$a^\varepsilon b^i,\ \varepsilon \in \{0, 1\},\ i \in \{0, 1, \ldots, m-1\}.$$

Vamos estudar separadamente as órbitas dos pontos de cada um dos três seguintes subconjuntos de $D_{2m} \times D_{2m}$:

1. $E_1 = \{(a^\varepsilon b^i, b^j) : \varepsilon \in \{0, 1\},\ i, j \in \{0, 1, \ldots, m-1\}\}$;
2. $E_2 = \{(ab^i, ab^i) : i \in \mathbb{N}_0\} \cup \{(1, ab^i) : i \in \mathbb{N}_0\}$;
3. $E_3 = \{(a^\varepsilon b^i, ab^j) : \varepsilon \in \{0, 1\},\ i, j \in \{0, 1, \ldots, m-1\}\} \setminus E_2$.

Estes três conjuntos formam uma partição de $D_{2m} \times D_{2m}$.

A órbita por ξ_l dos pontos do conjunto E_1 tem pré-período menor igual a 2 e período igual a 1: uma vez que $\langle b \rangle \lhd D_{2m}$, temos $[a^\varepsilon b^i, b^j]_l \in \langle b \rangle$, e portanto

$$[a^\varepsilon b^i, {}_r b^j]_l = 1 \text{ se } r \geq 2.$$

Determinemos em particular o pré-período da órbita de (a, b). Temos

$$[a, b]_t = aba^{-1}b^{-1} = abab^{-1} = b^{-2};$$
$$[a, b]_c = a^{-1}b^{-1}ab = ab^{-1}ab = b^2.$$

Se $[a, {}_1 b]_l$ fosse igual a $[a, {}_r b]_l$ para algum $r \geq 2$, então teríamos $b^2 = 1$. Mas tal não acontece porque a ordem de b é igual m, que por hipótese é maior do que 2. Se, por outro lado, $[a, {}_1 b]_l$ fosse igual a $[a, {}_0 b]_l$, então teríamos $a = b^2$, contradizendo o facto

de que $a \notin \langle b \rangle$. E como para $r \geq 2$ também não podemos ter $[a, {}_0b]_l = [a, {}_rb]_l (= 1)$, concluímos que o pré-período da órbita de (a, b) por ξ_l é igual a 2. Logo, fixado l,

$$\max_{P \in E_1} n_{P,l} = 2.$$

Os dados sobre as órbitas dos elementos de E_2 extraem-se quase imediatamente: o pré-período de $n_{(1,1),l}$ é zero; se $P \in E_2 \setminus \{(1,1)\}$ então $n_{P,l} = 1$; e $k_{P,l} = 1$ para todo $P \in E_2$.

Fixemos agora um ponto $P = (a^\varepsilon b^i, ab^j)$ do conjunto E_3, com $\varepsilon \in \{0,1\}$, $i \in \{0, 1, \ldots, m-1\}$, e estudemos a sua órbita por ξ_t. Comecemos por mostrar por indução sobre $r \in \mathbb{N}$ que

$$[a^\varepsilon b^i, {}_rab^j]_t = b^{2^r(\varepsilon j + (-1)^\varepsilon i)}. \tag{4.1}$$

Vamos dividir o passo inicial em dois casos. No primeiro, supomos que $\varepsilon = 0$:

$$\begin{aligned} [b^i, ab^j]_t &= b^i ab^j b^{-i} (ab^j)^{-1} \\ &= b^i (ab^j b^{-i} b^{-j}) a \\ &= b^{2i}. \end{aligned} \tag{4.2}$$

No segundo caso, supomos que $\varepsilon = 1$:

$$\begin{aligned} [ab^i, ab^j]_t &= ab^i ab^j (ab^i)^{-1} (ab^j)^{-1} \\ &= ab^i (ab^j b^{-i} a) b^{-j} a \\ &= ab^i b^{-j+i} b^{-j} a \\ &= ab^{2i-2j} a \\ &= b^{2(j-i)}. \end{aligned}$$

Agora o passo indutivo:

$$\begin{aligned} [a^\varepsilon b^i, {}_{r+1}ab^j]_t &= [[a^\varepsilon b^i, {}_rab^j]_t, ab^j]_t \\ &= [b^{2^r(\varepsilon j + (-1)^\varepsilon i)}, ab^j]_t \\ &= b^{2 \times 2^r(\varepsilon j + (-1)^\varepsilon i)} \qquad \text{por (4.2)} \\ &= b^{2^{r+1}(\varepsilon j + (-1)^\varepsilon i)}. \end{aligned}$$

Uma vez provada a igualdade 4.1, temos:

$$\begin{aligned} [a^\varepsilon b^i, {}_rab^j]_t = [a^\varepsilon b^i, {}_{r+s}ab^j]_t &\Leftrightarrow b^{2^r(\varepsilon j + (-1)^\varepsilon i)} = b^{2^{r+s}(\varepsilon j + (-1)^\varepsilon i)} \\ &\Leftrightarrow b^{2^{r+s}(\varepsilon j + (-1)^\varepsilon i) - 2^r(\varepsilon j + (-1)^\varepsilon i)} = 1 \\ &\Leftrightarrow b^{2^r(\varepsilon j + (-1)^\varepsilon i)(2^s - 1)} = 1. \end{aligned}$$

Como a ordem de b é igual a m, esta última igualdade é equivalente a

$$2^r(\varepsilon j + (-1)^\varepsilon i)(2^s - 1) \equiv 0 \pmod{m}. \tag{4.3}$$

Suponhamos que $\varepsilon j + (-1)^{\varepsilon} i = 0$. Temos duas possibilidades: $\varepsilon = 0$ e $i = 0$, ou $\varepsilon = 1$ e $j = i$: em qualquer dos casos isto implica que P seja um elemento de E_2, o que é contraditório. Logo $\varepsilon j + (-1)^{\varepsilon} i \neq 0$. Existem portanto $\lambda_P \in \mathbb{N}_0$ e $\mu_P \in \mathbb{N}$ tais que μ_P é ímpar e $|\varepsilon j + (-1)^{\varepsilon} i| = 2^{\lambda_P} \mu_P$. Por (4.3), atendendo a que $m = 2^{\alpha}\beta$ e a que β é ímpar, temos então a seguinte a equivalência:

$$\xi_t^r(P) = \xi_t^{r+s}(P) \Leftrightarrow \begin{cases} 2^{r+\lambda_P} \equiv 0 \pmod{2^{\alpha}} \\ \mu_P(2^s - 1) \equiv 0 \pmod{\beta} \end{cases} \qquad \forall r, s \in \mathbb{N} \tag{4.4}$$

Logo,

$$n_{P,t} \neq 0 \Rightarrow n_{P,t} = \min\{r \in \mathbb{N} : 2^{r+\lambda_P} \equiv 0 \pmod{2^{\alpha}}\} = \max\{1, \alpha - \lambda_P\}; \tag{4.5}$$

$$k_{P,t} = \min\{s \in \mathbb{N} : \mu_P(2^s - 1) \equiv 0 \pmod{\beta}\}. \tag{4.6}$$

De (4.5) resulta

$$\max_{P \in E_3} n_{P,t} \leq \max\{1, \alpha\}. \tag{4.7}$$

O pré-período de P pode efectivamente ser igual a zero: com efeito, se $r \geq 1$, então

$$[a^{\varepsilon} b^i, {}_r ab^j]_t = a^{\varepsilon} b^i \Leftrightarrow b^{2^r(\varepsilon j + (-1)^{\varepsilon} i)} = a^{\varepsilon} b^i \Leftrightarrow b^{2^r(\varepsilon j + (-1)^{\varepsilon} i) - i} = a^{\varepsilon} \Leftrightarrow \varepsilon = 0 \text{ e } b^{(2^r - 1)i} = 1.$$

sendo a última equivalência válida porque $a \notin \langle b \rangle$. Logo um ponto P de E_3 tem pré-período igual a zero se e só se $\varepsilon = 0$ e existir $r \in \mathbb{N}$ tal que m divide $(2^r - 1)i$.[2]

Se o_2 for a ordem de 2 em $\mathbb{Z}_{\beta}^*$, então $\mu_P(2^{o_2} - 1) \equiv 0 \pmod{\beta}$, donde, pela equivalência (4.4),

$$\forall P \in E_3,\ k_{P,t} \text{ divide } o_2. \tag{4.8}$$

Consideremos em particular o ponto $P_0 = (a, ab) \in E_3$. De acordo com a observação que atrás fizemos sobre os pontos de E_3 que têm pré-período igual a zero, $n_{P_0,t} \neq 0$. Por outro lado, $\lambda_{P_0} = 0$ e $\mu_{P_0} = 1$, pelo que $n_{P_0,t} = \max\{1, \alpha\}$ e $k_{P_0,t} = o_2$, por (4.5) e (4.6), respectivamente. Logo, por (4.7) e (4.8),

$$\max_{P \in E_3} n_{P,t} = \max\{1, \alpha\} \quad \text{e} \quad \text{m. m. c.}_{P \in E_3} k_{P,t} = o_2.$$

[2]No caso em que $i = 1$, pelo conhecido teorema de Euler sobre congruências, um tal $r \in \mathbb{N}$ existe se e só se m é ímpar.

Então, pelo lema 2.2,

$$\begin{aligned} n &= \max\{n_{P,t} : P \in D_{2m} \times D_{2m}\} \\ &= \max\{\max_{P\in E_1} n_{P,t},\ \max_{P\in E_2} n_{P,t},\ \max_{P\in E_3} n_{P,t}\} \\ &= \max\{2, 1, \max\{1, \alpha\}\} \\ &= \max\{2, \alpha\}; \end{aligned}$$

$$\begin{aligned} k_t &= \text{m. m. c.}\{k_{P,t} : P \in D_{2m} \times D_{2m}\} \\ &= \text{m. m. c.}\{\underset{P\in E_1}{\text{m. m. c.}}\, k_{P,t},\ \underset{P\in E_2}{\text{m. m. c.}}\, k_{P,t},\ \underset{P\in E_3}{\text{m. m. c.}}\, k_{P,t}\} \\ &= \text{m. m. c.}\{1, 1, o_2\} \\ &= o_2. \end{aligned}$$

Falta-nos analisar o período das órbitas por ξ_c dos elementos de E_3. De modo análogo ao que foi feito quando lidámos com o operador ξ_t, podemos mostrar sucessivamente que

$$[a^\varepsilon b^i, {}_r ab^j]_c = b^{(-2)^r(i-\varepsilon j)} \quad \forall r \in \mathbb{N} \tag{4.9}$$

que para todo o ponto $P = (a^\varepsilon b^i, ab^j)$ de E_3

$$\xi_c^r(P) = \xi_c^{r+s}(P) \Leftrightarrow (-2)^r(i - \varepsilon j)((-2)^s - 1) \equiv 0 \pmod m, \quad \forall r, s \in \mathbb{N}$$

e que

$$\forall P \in E_3,\ k_{P,c} \text{ divide a ordem } o_{-2} \text{ de } -2 \text{ em } \mathbb{Z}_\beta^*.$$

Finalmente, $P = (a, ab) \Rightarrow i - \varepsilon j = -1 \Rightarrow k_{P,c} = o_{-2}$, e portanto $k_c = o_{-2}$. □

Uma consequência interessante da proposição 4.7 é que para qualquer elemento n de $\mathbb{N}_0$ existe um grupo finito cujo pré-período é igual a n. Em contraste, não existem grupos finitos onde ξ_c tenha período igual a dois, ou seja, as pseudovariedades $[\![[x, {}_\omega y]_c = [x, {}_{\omega+1} y]_c]\!]$ e $[\![[x, {}_\omega y]_c = [x, {}_{\omega+2} y]_c]\!]$ são iguais [8]. No entanto, para cada $l \in \{c, t\}$, existem grupos finitos de período arbitrariamente grande, como a partir da proposição 4.7 se mostra na proposição seguinte.

Proposição 4.8. *Seja $l \in \{c, t\}$. Para qualquer $r \in \mathbb{N}$ existe $k > r$ tal que k é igual ao período de ξ_l em algum grupo finito diedral. O inteiro k pode ser escolhido tanto entre os pares como entre os ímpares.*

Demonstração. Sejam p um primo ímpar, $k_{p,t}$ a ordem de 2 em $\mathbb{Z}_p^*$ e $k_{p,c}$ a ordem de -2 em $\mathbb{Z}_p^*$. Para qualquer $e \in \mathbb{N}$,

$$(\pm 2)^e \equiv 1 \pmod p \Rightarrow 2^{2e} = 4^e \equiv 1 \pmod p \Rightarrow 4^e > p.$$

Logo,

$$p > 4^r \Rightarrow k_{p,l} > r, \quad l \in \{c, t\}, \tag{4.10}$$

o que mostra a primeira parte da proposição. Vamos agora mostrar que para cada $l \in \{c, t\}$ podemos escolher $p > 4^r$ tal que $k_{p,l}$ tem uma paridade pré-fixada. Como a ordem de $\mathbb{Z}_p^*$ é $p-1$, o inteiro $k_{p,l}$ divide $p-1$. Se $k_{p,l}$ for ímpar então $k_{p,l}$ divide $\frac{p-1}{2}$. Logo,

$$k_{p,t} \text{ ímpar } \Rightarrow 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}; \tag{4.11}$$

$$k_{p,c} \text{ ímpar } \Rightarrow (-2)^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{4.12}$$

No quinto capítulo de [20] podemos encontrar a demonstração das seguintes equivalências, para qualquer primo ímpar p:

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow p \equiv 1 \text{ ou } 7 \pmod{8}; \tag{4.13}$$

$$(-2)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow p \equiv 1 \text{ ou } 3 \pmod{8}. \tag{4.14}$$

Então, por (4.13) e (4.11) e por (4.14) e (4.12), temos:

$$p \equiv 5 \pmod{8} \Rightarrow k_{p,l} \text{ par }. \tag{4.15}$$

Se $p = 8n+7$ para algum $n \in \mathbb{N}$ então $\frac{p-1}{2} = 4n+3$ e portanto, por (4.13), $2^{4n+3} \equiv 1 \pmod{p}$. Logo $k_{p,t}$ divide o ímpar $4n+3$, pelo que

$$p \equiv 7 \pmod{8} \Rightarrow k_{p,t} \text{ ímpar }. \tag{4.16}$$

Analogamente, por (4.14),

$$p \equiv 3 \pmod{8} \Rightarrow k_{p,c} \text{ ímpar }. \tag{4.17}$$

Pelo teorema de Dirichlet sobre primos numa progressão aritmética, para cada uma das progressões aritméticas $8n+3$, $8n+5$ e $8n+7$ sabemos que existe uma infinidade de primos entre os seus termos. Podemos portanto escolher primos que sejam maiores do que 4^r entre os termos de cada uma destas sucessões. Logo, fixado $l \in \{c, t\}$, por (4.10) e (4.15) o inteiro $k(= k_{p,l})$ pode ser escolhido entre os números pares; por (4.10) e por (4.16) ou (4.17), também pode ser escolhido entre os números ímpares. □

O grupo $D = \prod_{m \in \mathbb{N}} D_{2m}$ é um exemplo de um grupo onde nenhum dos operadores de Engel é pré-periódico: se, para $l \in \{c, t\}$, a transformação $(\xi_l)_D$ fosse pré-periódica, então, para qualquer $m \in \mathbb{N}$, o pré-período de $(\xi_l)_{D_{2m}}$ seria menor ou igual do que o de $(\xi_l)_D$, contradizendo o facto de que o conjunto dos naturais que são pré-período de algum grupo finito diedral é o conjunto $\mathbb{N}$.

Um outro exemplo de um grupo que não satisfaz nenhuma identidade de Engel é o grupo diedral infinito [30]. O grupo diedral infinito D_∞ pode ser descrito do seguinte

modo: se no grupo livre $F_{\mathcal{G}}(x,y)$ considerarmos o fecho normal[3] N dos termos x^2 e $xyxy$ então $D_\infty \simeq F(x,y)/N$. O grupo D_∞ é um grupo infinito gerado por dois elementos u e v tais que

$$u^2 = 1, \text{ e } uvu = v^{-1}.$$

As igualdades (4.1) e (4.9) que surgem na demonstração da proposição 4.7 foram deduzidas apenas à custa das relações $a^2 = 1$ e $aba = b^{-1}$. Logo essas igualdades também são válidas para os geradores u e v de D_∞. Em particular,

$$[v,_r uv]_t = v^{2^r}, \quad [v,_r uv]_c = v^{(-2)^r}, \quad \forall r \in \mathbb{N}_0. \tag{4.18}$$

Como a ordem de v não é finita, isto implica que para $l \in \{c,t\}$ tenhamos

$$[v,_r uv]_l \neq [v,_{r+s} uv]_l, \quad \forall r \in \mathbb{N}_0, \forall s \in \mathbb{N}. \tag{4.19}$$

Logo em D_∞ não é válida nenhuma identidade de Engel.[4] Este facto é referido de passagem em [9], sem que no entanto se dê qualquer justificação, o que não surpreende, pois somos facilmente levados às igualdades (4.18). Foram estas igualdades que motivaram a demonstração que aqui fizemos da proposição 4.7.

Para $n \geq 2$ não se conhece até ao momento uma caracterização completa da estrutura dos elementos da pseudovariedade $[\![[x,_n y]_c = [x,_{n+\omega} y]_c]\!]$ dos grupos finitos onde o pré-período de Engel é menor ou igual n. E para $k \geq 2$ também não se conhece a estrutura das pseudovariedades $[\![[x,_\omega y]_t = [x,_{\omega+k} y]_t]\!]$ e $[\![[x,_\omega y]_c = [x,_{\omega+k} y]_c]\!]$, as quais são, respectivamente, as classes dos grupos finitos onde ξ_t e ξ_c têm período divisor de k. Os grupos finitos onde estes operadores têm período igual a 1 serão o tema da próxima secção. Veremos que os grupos finitos onde ξ_t tem período 1 estão bem caracterizados (são precisamente os grupos nilpotentes finitos), e, embora não dispondo de uma caracterização completa, daremos algumas caraterizações parciais muito restritivas sobre aqueles onde ξ_c tem período 1. Estes desconhecimentos sobre a influência dos invariantes de Engel na estrutura de um grupo finito pode ser atestado no artigo mais recente [16]. No entanto, até ao final deste capítulo veremos mais alguns casos onde existem algumas caracterizações parciais interessantes dos grupos finitos onde os operadores de Engel têm uma determinada dinâmica.

4.5 Operadores de Engel aperiódicos

Comecemos por esclarecer o significado do título desta secção. Uma transformação aperiódica é uma transformação pré-periódica de período um.

[3]Num grupo G, o fecho normal $\langle X \rangle^G$ de um subconjunto X é a intersecção de todos os subgrupos normais de G que contêm X. O conjunto $\langle X \rangle^G$ é ele próprio um subgrupo normal de G, sendo por isso também designado como o subgrupo normal de G gerado por X. Se $X \neq \emptyset$, então $\langle X \rangle^G = \{x_1{}^{g_1} \cdots x_n{}^{g_n} : x_i \in X, g_i \in G, n \in \mathbb{N}\}$.

[4]Este exemplo é realmente distinto do exemplo anteriormente dado, o grupo $D = \prod_{m \in \mathbb{N}} D_{2m}$: enquanto que D_∞ é numerável, D tem cardinal $2^{\aleph_0}$.

O lema que se segue foi obtido pelo autor e por J. Almeida, em colaboração. Tendo em conta as proposições 3.6 e 3.7, o próximo lema é já um indício da importância que terá mais à frente o conhecimento da estrutura dos grupos finitos que não são nilpotentes mas cujos divisores próprios são nilpotentes.

Lema 4.9. *Suponhamos que G é um grupo finito com um subgrupo normal e Abeliano P e um subgrupo cíclico Q tais que $Z(PQ) = 1$. Seja y um gerador de Q. Para $l \in \{c, t\}$, se k_l for um múltiplo do período de $(\xi_l)_G$, então $[x, {}_{k_l}y]_l = x$, para todo o $x \in P$.*

Demonstração. Como $P \lhd G$, para todo o $x \in P$ temos $[x, y]_l \in P$. Portanto fica bem definida a transformação

$$\begin{aligned} \zeta_{l,y} : P &\longrightarrow P \\ x &\longmapsto [x, y]_l \end{aligned}$$

Sejam $x, z \in P$. Então

$$\begin{aligned} [x, y]_c = [z, y]_c &\Leftrightarrow x^{-1}y^{-1}xy = z^{-1}y^{-1}zy \\ &\Leftrightarrow x^{-1}y^{-1}x = z^{-1}y^{-1}z \\ &\Leftrightarrow zx^{-1}y^{-1}xz^{-1} = y^{-1} \\ &\Leftrightarrow (xz^{-1})^{-1}y^{-1}(xz^{-1}) = y^{-1}. \end{aligned}$$

Logo, se $\zeta_{c,y}(x) = \zeta_{c,y}(z)$ então xz^{-1} comuta com o gerador y^{-1} de Q, donde xz^{-1} é um elemento de P que comuta com todos os elementos de Q. Sendo P um grupo Abeliano, concluímos que $xz^{-1} \in Z(PQ)$. Ora $Z(PQ) = 1$, pelo que $x = z$ e $\zeta_{c,y}$ é injectiva, e mesmo bijectiva, pela finitude de P.

Por outro lado,

$$\begin{aligned} \zeta_{t,y}(x) = \zeta_{t,y}(z) &\Leftrightarrow [x, y]_t = [z, y]_t \\ &\Leftrightarrow [x^{-1}, y^{-1}]_c = [z^{-1}, y^{-1}]_c \\ &\Leftrightarrow \zeta_{c,y^{-1}}(x^{-1}) = \zeta_{c,y^{-1}}(z^{-1}) \\ &\Leftrightarrow x^{-1} = z^{-1} \\ &\Leftrightarrow x = z. \end{aligned}$$

Portanto também $\zeta_{t,y}$ é bijectiva. Por ser uma transformação invertível, $\zeta_{l,y}$ é periódica. Seja p_l o período de $\zeta_{l,y}$. Como $\xi_l^{p_l}(x, y) = (\zeta_{l,y}^{p_l}(x), y) = (x, y)$, o período p_l de $\zeta_{l,y}$ divide o período k_l de ξ_l. Logo, para todo o $x \in P$, $\zeta_{l,y}^{k_l}(x) = x$, ou seja, $[x, {}_{k_l}y]_l = x$. □

O próximo teorema diz-nos que os grupos nilpotentes finitos são precisamente os grupos finitos onde o operador ξ_t é aperiódico [25].

Teorema 4.10. $\mathsf{G_{nil}} = [\![[x, {}_{\omega}y]_t = [x, {}_{\omega+1}y]_t]\!]$.

Demonstração. Como $\mathsf{G_{nil}} \models [x, {}_{\omega}y]_t = 1$, a inclusão $\mathsf{G_{nil}} \subseteq [\![[x, {}_{\omega}y]_t = [x, {}_{\omega+1}y]_t]\!]$ é imediata.

Suponhamos, por redução ao absurdo, que $\mathsf{G}_{\mathsf{nil}} \subsetneq [\![[x, {}_{\omega}y]_t = [x, {}_{\omega+1}y]_t]\!]$. Então a classe $\mathscr{C} = [\![[x, {}_{\omega}y]_t = [x, {}_{\omega+1}y]_t]\!] \setminus \mathsf{G}_{\mathsf{nil}}$ é não vazia e possui um elemento G de ordem mínima. Todos os divisores de G estão em $[\![[x, {}_{\omega}y]_t = [x, {}_{\omega+1}y]_t]\!]$, e portanto, pela minimalidade da ordem de G, aqueles que são próprios também estão em $\mathsf{G}_{\mathsf{nil}}$. Pelas proposições 3.6 e 3.7, existem primos distintos p e q tais que P é um p-subgrupo de Sylow normal e Abeliano, Q é um q-subgrupo de Sylow cíclico e $G = PQ$. Ainda pela proposição 3.7, $Z(G) = 1$.

Podemos agora aplicar o lema 4.9. Como por hipótese o período de ξ_t em G é 1, concluímos que se y é um gerador de Q então

$$\forall x \in P,\ [x, y]_t = x.$$

Ora

$$[x, y]_t = x \Leftrightarrow xyx^{-1}y^{-1} = x \Leftrightarrow yx^{-1}y = 1 \Leftrightarrow x = 1.$$

pelo que $P = 1$ e $G = Q$, um grupo nilpotente, o que é uma contradição. □

Exemplo 4.11. *Pela proposição 4.7, num grupo diedral D_{2m} o operador ξ_t é aperiódico se e só se m for uma potência de 2. Aplicando o teorema 4.10, concluímos que um grupo diedral finito é nilpotente se e só se a sua ordem for uma potência de 2.*

Como um grupo finito satisfaz uma pseudoidentidade com n variáveis (no máximo) se e só se todo o subgrupo gerado por n elementos satisfaz essa pseudoidentidade, o teorema 4.10 tem o seguinte corolário:

Corolário 4.12. *Um grupo finito é nilpotente se e só se todo o subgrupo gerado por dois elementos é nilpotente.*

Proposição 4.13. $\left[[x, {}_{n}y]_t = [x, {}_{n+1}y]_t\right] = \left[[x, {}_{n}y]_t = 1\right]$.

Demonstração.

$$\begin{aligned}
[x, {}_{n}y]_t = [x, {}_{n+1}y]_t &\Leftrightarrow [x, {}_{n}y]_t = [[x, {}_{n}y]_t, y]_t \\
&\Leftrightarrow 1 = y[x, {}_{n}y]_t{}^{-1}y^{-1} \\
&\Leftrightarrow [x, {}_{n}y]_t = 1.
\end{aligned}$$

□

Corolário 4.14 (Teorema de Zorn).

$$\mathsf{G}_{\mathsf{nil}} = [\![[x, {}_{\omega}y]_c = 1]\!] = [\![[x, {}_{\omega}y]_t = 1]\!] = [\![[{}_{\omega}x, y]_c = 1]\!] = [\![[{}_{\omega}x, y]_t = 1]\!].$$

Demonstração. As igualdades $[\![[x, {}_{\omega}y]_c = 1]\!] = [\![[x, {}_{\omega}y]_t = 1]\!] = [\![[{}_{\omega}x, y]_c = 1]\!] = [\![[{}_{\omega}x, y]_t = 1]\!]$ decorrem da proposição 4.3. A igualdade $\mathsf{G}_{\mathsf{nil}} = [\![[x, {}_{\omega}y]_c = 1]\!]$ resulta do teorema 4.10 e da proposição 4.13. □

Para sermos um pouco mais precisos, a proposição 4.13 permite-nos concluir que o teorema 4.10 e o Teorema de Zorn podem ser deduzidos um a partir do outro.

O Teorema de Zorn não pode ser generalizado para grupos infinitos: para $n > 2$, existem grupos infinitos que satisfazem a identidade $[x, {}_n y]_c = 1$ mas que não são nilpotentes [30]. Contudo, qualquer grupo que satisfaça a identidade $[x, {}_2 y]_c = 1$ é nilpotente de classe menor ou igual a 3 [30].

Para cada grupo G, seja $L(G)$ o conjunto $\{y \in G : \forall x \in G, \exists n \in \mathbb{N} : [x, {}_n y]_c = 1\}$. A demonstração da próxima proposição pode ser encontrada em [30].

Proposição 4.15. *Se G é um grupo finito e $y \in L(G)$, então o fecho normal $\langle y \rangle^G$ é nilpotente.*

O resultado seguinte deduz-se facilmente a partir do anterior:

Proposição 4.16. *Seja G um grupo finito. Então* $\mathrm{Fit}(G) = L(G)$.

Demonstração. Sejam $y \in \mathrm{Fit}(G)$ e $x \in G$. Como $\mathrm{Fit}(G)$ é um subgrupo normal, $[x, y]_c \in \mathrm{Fit}(G)$. Então, como $\mathrm{Fit}(G)$ é nilpotente, existe $n \in \mathbb{N}$ tal que $[[x, y]_c, {}_n y]_c = 1$, ou seja, $[x, {}_{n+1} y]_c = 1$. Logo $y \in L(G)$. Reciprocamente, suponhamos que $y \in L(G)$. Pela proposição 4.15, o subgrupo $\langle y \rangle^G$ está contido em $\mathrm{Fit}(G)$. □

A demonstração dada em [30] da proposição 4.15 é independente do Teorema de Zorn. Deste modo temos uma demonstração alternativa do Teorema de Zorn: dado um grupo finito G, por um lado G é nilpotente se e só se $\mathrm{Fit}(G) = G$, e por outro lado G satisfaz a pseudoidentidade $[x, {}_\omega y]_c = 1$ se e só se $L(G) = G$.

Não se sabe ainda se para qualquer grupo G o conjunto $L(G)$ é um subgrupo de G. Um grupo G tal que $L(G) = G$ diz-se um *grupo de Engel*. Em [30, 29] podemos encontrar uma síntese do que se sabe (e do que não se sabe) sobre os grupos de Engel, o conjunto $L(G)$ e outros conjuntos aparentados.

Passemos agora ao estudo da pseudovariedade $[\![[x, {}_\omega y]_c = [x, {}_{\omega+1} y]_c]\!]$. Tenhamos bem presente que esta pseudovariedade é distinta da pseudovariedade $[\![[x, {}_\omega y]_t = [x, {}_{\omega+1} y]_t]\!]$, ou seja, de $\mathsf{G}_{\mathsf{nil}}$. Com efeito, como já assinalámos, $S_3 \models [x, {}_\omega y]_c = [x, {}_{\omega+1} y]_c$. Mais precisamente, $S_3 \models [x, {}_2 y]_c = [x, {}_3 y]_c$.

Para os nossos propósitos ser-nos-á útil o seguinte resultado auxiliar:

Lema 4.17. *Seja G um grupo finito que não é nilpotente mas cujos divisores próprios são nilpotentes. Sejam P um p-subgrupo de Sylow normal e Abeliano e Q um q-subgrupo de Sylow cíclico Q tais que $G = PQ$. Se para qualquer gerador y de Q e para qualquer elemento x de P se verificar a igualdade $[x, y]_c = x$, então G é isomorfo a S_3.*

Observemos que, pelas proposições 3.6 e 3.7, os grupos P e Q nas condições do enunciado existem. Notemos também que o grupo S_3 efectivamente verifica as condições do lema 4.17 (com $p = 3$ e $q = 2$).

Demonstração do lema 4.17. Comecemos por observar que

$$[x, y]_c = x \Leftrightarrow x^2 = y^{-1}xy. \tag{4.20}$$

Notemos também que qualquer gerador de um q-subgrupo de Sylow é conjugado de algum gerador y de Q. Sejam $z \in G$ e $x \in P$. Então

$$\begin{aligned} y^{-z}xy^z &= (z^{-1}y^{-1}z)x(z^{-1}yz) \\ &= z^{-1}y^{-1}(zxz^{-1})yz \\ &= z^{-1}(zxz^{-1})^2z \qquad \text{por (4.20) e porque } zxz^{-1} \in P, \text{ uma vez que } P \lhd G \\ &= z^{-1}(zx^2z^{-1})z \\ &= x^2. \end{aligned}$$

Logo, para qualquer gerador y de um qualquer q-subgrupo de Sylow continua a ser válida para todo $x \in P$ a igualdade $x^2 = y^{-1}xy$.

Sejam $a \in P \setminus \{1\}$ e y um gerador de Q. Mostremos por indução que

$$a^{2^n} = y^{-n}ay^n, \quad \forall n \in \mathbb{N}. \tag{4.21}$$

O passo inicial é válido por (4.20). Eis o passo indutivo:

$$a^{2^{n+1}} = (a^2)^{2^n} = (y^{-1}ay)^{2^n} = y^{-1}a^{2^n}y = y^{-1}(y^{-n}ay^n)y = y^{-(n+1)}ay^{n+1}.$$

Se r é um primo distinto de q então y^r tem a mesma ordem de y, ou seja, y^r é um gerador de um q-subgrupo de Sylow de G. Logo também $a^2 = y^{-r}ay^r$. Mas por (4.21), $a^{2^r} = y^{-r}ay^r$, pelo que $a^{2^r} = a^2$ e $a^{2^r-2} = 1$. Então, como $a^{2^{r-1}-1} \in P$, temos $1 = a^{2^r-2} = (a^{2^{r-1}-1})^2 = y^{-1}a^{2^{r-1}-1}y$, pelo que $a^{2^{r-1}-1} = 1$. Uma vez que a ordem de a é uma potência positiva de p, concluímos que p divide $2^{r-1} - 1$, para todo o primo r distinto de q. Se $q \neq 2$, então podemos tomar $r = 2$, o que conduz ao absurdo de p dividir 1. Logo $q = 2$. Podemos pois tomar $r = 3$, pelo que p divide $2^2 - 1 = 3$, e portanto $p = 3$.

Como para todo o $x \in P$, $x = [x, y]_c$, temos $P \leq [P, G]$. Por outro lado, $G/P \simeq Q$ é um grupo Abeliano, pelo que $G' \leq P$. Em resumo: $[P, G] \leq G' \leq P \leq [P, G]$, e portanto $P = [P, G] = G'$. Mostremos agora por indução que $\gamma_n(G) = P$ se $n \geq 2$. Para tal, falta-nos apenas o passo indutivo: $\gamma_{n+1}(G) = [\gamma_n(G), G] = [P, G] = P$. Portanto $\gamma_\omega(G) = P$.

Seja agora g um elemento arbitrário de G. Como $G = P\langle y\rangle$, existem $z \in P$ e $k \in \mathbb{N}$ tais que $g = zy^k$. Então

$$\begin{aligned} g^{-1}ag &= y^{-k}z^{-1}azy^k \\ &= y^{-k}ay^k \qquad \text{uma vez que } P \text{ é Abeliano} \\ &= a^{2^k} \qquad \text{por (4.21).} \end{aligned}$$

Logo $\langle a\rangle \lhd G$. O grupo $G/\langle a\rangle$ é um divisor próprio de G, donde, por hipótese, é nilpotente. Então

$$1 = \gamma_\omega(G/\langle a\rangle) = \gamma_\omega(G)\langle a\rangle/\langle a\rangle$$

e portanto $\gamma_\omega(G) \leq \langle a\rangle$. Mas vimos que $\gamma_\omega(G) = P$, pelo que $P = \langle a\rangle$. Ora a é um elemento arbitrário de $P \setminus \{1\}$, e P é um 3-grupo. Pelo Teorema de Cauchy, ou simplesmente por P ser um 3-grupo cíclico, podemos escolher a de ordem 3. Logo $|P| = 3$.

Seja $n \in \mathbb{N}$ tal que $|Q| = 2^n$. Seja X o conjunto dos conjugados de Q, e consideremos o homomorfismo

$$\begin{aligned} \psi : G &\longrightarrow S_X \\ g &\longmapsto \psi_g : R \mapsto R^g \end{aligned}$$

entre G e o grupo das permutações de X.[5] Sabemos desde já que $\operatorname{Ker}\psi \leq N_G(Q)$. Se $Q < N_G(Q)$ então, como $|G| = 3 \cdot |Q|$, temos $N_G(Q) = G$, ou seja, $Q \lhd G$. Mas tal implica que G seja o produto directo de P e Q, dois grupos Abelianos, e que por isso G seja ele próprio Abeliano. Como G nem sequer é nilpotente, $Q = N_G(Q)$ e portanto $\ker\psi$ é um 2-grupo. Seja $m \in \mathbb{N}_0$ tal que $|\ker\psi| = 2^m$. Como Q não é um subgrupo normal de G, temos $\operatorname{Ker}\psi < Q$, ou seja, $n - m > 0$. Pelo Teorema do Homomorfismo, a ordem de $G/\operatorname{Ker}\psi$, que é $3 \times 2^{n-m}$, divide a ordem de S_X, que é $|X|!$. Ora $|X| = [G : N_G(Q)] = [G : Q] = 3$, pelo que $3 \times 2^{n-m}$ divide 6. Como $n - m > 0$, só podemos ter $n - m = 1$, e portanto a ordem de $G/\operatorname{Ker}\psi$ é 6. A menos de isomorfismo, os únicos grupos de ordem 6 são $\mathbb{Z}_6$ e S_3. Se $G/\operatorname{Ker}\psi$ for Abeliano, então $P = G' \leq \operatorname{Ker}\psi < Q$, o que é absurdo. Logo $G/\operatorname{Ker}\psi \simeq S_3$, e portanto S_3 é um divisor de G. Mas como S_3 não é nilpotente, não é um divisor próprio, pelo que G é isomorfo a S_3. □

Os resultados auxiliares de que dispomos permitem-nos uma demonstração expedita da seguinte caracterização parcial da pseudovariedade $[\![[x, {}_\omega y]_c = [x, {}_{\omega+1} y]_c]\!]$:

Teorema 4.18. *Seja G um grupo finito. Se $G \models [x, {}_\omega y]_c = [x, {}_{\omega+1} y]_c$, então G é nilpotente ou é divisível por S_3.*

Demonstração. Seja $\mathscr{D}$ a classe dos grupos que são divisíveis por S_3. Reparemos que, não sendo S_3 nilpotente, $\mathscr{D}$ e $\mathsf{G}_{\mathsf{nil}}$ são classes disjuntas. Consideremos a classe $\mathscr{C} = [\![[x, {}_\omega y]_c = [x, {}_{\omega+1} y]_c]\!] \setminus (\mathsf{G}_{\mathsf{nil}} \mathbin{\mathring{\cup}} \mathscr{D})$. Pretendemos mostrar que se trata de uma classe vazia. Suponhamos que $\mathscr{C}$ não é vazia. Então existe um elemento G de $\mathscr{C}$ de ordem mínima. Pela minimalidade de G, se K é um divisor próprio de G, então $K \in \mathsf{G}_{\mathsf{nil}} \mathbin{\mathring{\cup}} \mathscr{D}$. Como a relação de divisão entre álgebras é transitiva, se K pertencesse a $\mathscr{D}$ então S_3 seria um divisor de G. Logo $K \in \mathsf{G}_{\mathsf{nil}}$. Pelas proposições 3.6 e 3.7, existem primos distintos p e q e subgrupos P e Q tais que P é p-subgrupo de Sylow normal e Abeliano de G, Q é q-subgrupo de Sylow cíclico e $G = PQ$. Ainda pela

[5] Este homomorfismo é habitualmente designado como *representação de G nos conjugados de Q*.

proposição 3.7, $Z(G) = 1$. Se y for um gerador de Q então, pelo lema 4.9, para todo o $x \in P$ temos $[x, y]_c = x$. Logo, pelo lema 4.17, G é isomorfo a S_3: absurdo! □

Baseando-nos na pesquisa efectuada, julgamos que este teorema (juntamente com o lema que o precedeu) é um resultado original.

Exemplo 4.19. *O grupo D_{12} não é nilpotente e é um elemento da pseudovariedade $[\![[x, {}_n y]_c = [x, {}_{n+1} y]_c]\!]$. Este grupo é isomorfo a $S_3 \times \mathbb{Z}_2$.*

Exemplo 4.20. *O grupo T de ordem 12 gerado por dois elementos a e b tais que $a^6 = 1$ e $b^2 = a^3 = (ab)^2$ é um elemento da pseudovariedade $[\![[x, {}_n y]_c = [x, {}_{n+1} y]_c]\!]$. Este grupo não é nilpotente. Tem S_3 como divisor, mas não tem subgrupos isomorfos a S_3.*

Exemplo 4.21. *Os grupos $S_3 \times D_{10}$ e S_4 são divisíveis por S_3 mas não são elementos da pseudovariedade $[\![[x, {}_n y]_c = [x, {}_{n+1} y]_c]\!]$ (ver tabela 4.1).*

Recordemos mais uma vez que o problema da caracterização completa da pseudovariedade $[\![[x, {}_n y]_c = [x, {}_{n+1} y]_c]\!]$ continua em aberto. A variedade $[[x, {}_n y]_c = [x, {}_{n+1} y]_c]$ foi estudada em [17], onde se começa pela demonstração da seguinte proposição:

Proposição 4.22. *Se um grupo satisfaz a identidade $[x, {}_n y]_c = [x, {}_{n+1} y]_c$, para algum $n \in \mathbb{N}$, então também satisfaz as identidades $[x, {}_n y]^3 = 1$ e $[[x, {}_{n-1} y]_c, y^{2k}]_c = 1$, para qualquer $k \in \mathbb{N}$.*

Demonstração. Seja G um grupo onde a identidade $[x, {}_n y]_c = [x, {}_{n+1} y]_c$ é válida. A hipótese sobre G é equivalente a

$$G \models [x, {}_n y]_c^2 = [x, {}_n y]_c^y. \tag{4.22}$$

Por sua vez, a validade em G da identidade $[x, {}_n y]_c^2 = [x, {}_n y]_c^y$ é equivalente à validade da identidade $[x, {}_n y^{-1}]_c^2 = [x, {}_n y^{-1}]_c^{y^{-1}}$. Substituindo nesta última x por $[x, {}_n y]_c$, concluímos que

$$G \models [[x, {}_n y]_c, {}_n y^{-1}]^2 = [[x, {}_n y]_c, {}_n y^{-1}]^{y^{-1}}. \tag{4.23}$$

Vamos agora mostrar, por indução sobre i, que

$$G \models [[x, {}_n y]_c, {}_n y^{-1}]_c = [[x, {}_n y]_c^{(-1)^i}, {}_{n-i} y^{-1}]_c^{y^{-i}},\ i \in \{1, \ldots, n\}. \tag{4.24}$$

A validade de (4.24) para $i = 0$ é óbvia. Suponhamos que (4.24) é válida para $i \in \{0, \ldots, n-1\}$. Então, para quaisquer $x, y \in G$,

$$\begin{aligned}
[[x, {}_n y]_c, {}_n y^{-1}]_c &= [[x, {}_n y]_c^{(-1)^i}, {}_{n-i} y^{-1}]_c^{y^{-i}} \\
&= [[[x, {}_n y]_c^{(-1)^i}, y^{-1}]_c, {}_{n-i-1} y^{-1}]_c^{y^{-i}} \\
&= [[[x, {}_n y]_c^{(-1)^i}, y]_c^{-y^{-1}}, {}_{n-i-1} y^{-1}]_c^{y^{-i}} \qquad \text{pela alínea 2 do lema 3.1} \\
&= [[[x, {}_n y]_c^{(-1)^i}, y]_c^{-1}, {}_{n-i-1} y^{-1}]_c^{y^{-i-1}}.
\end{aligned} \tag{4.25}$$

Suponhamos que i é par. Então o comutador de (4.25) é igual a

$$[[[x, {}_n y]_c, y]_c^{-1}, {}_{n-i-1}y^{-1}]_c^{y^{-i-1}}. \tag{4.26}$$

Por hipótese, $[x, {}_{n+1}y]_c = [x, {}_n y]_c$. Logo (4.26) é igual a

$$[[x, {}_n y]_c^{(-1)^{i+1}}, {}_{n-(i+1)}y^{-1}]_c^{y^{-(i+1)}}.$$

Vamos supor agora que i é ímpar. Então, voltando ao ponto em que ficamos em (4.25), temos:

$$[[[x, {}_n y]_c^{-1}, y]_c^{-1}, {}_{n-i-1}y^{-1}]_c^{y^{-i-1}}.$$

Aplicando a alínea 2 do lema 3.1 vem

$$[[[x, {}_n y]_c, y]_c^{[x,{}_n y]_c{}^{-1}}, {}_{n-i-1}y^{-1}]_c^{y^{-i-1}},$$

Pela hipótese $[x, {}_{n+1}y]_c = [x, {}_n y]_c$,

$$[[x, {}_n y]_c^{[x,{}_n y]_c{}^{-1}}, {}_{n-(i+1)}y^{-1}]_c^{y^{-(i+1)}},$$

ou seja,

$$[[x, {}_n y]_c^{(-1)^{i+1}}, {}_{n-(i+1)}y^{-1}]_c^{y^{-(i+1)}}.$$

Fica assim provada a validade de (4.24), independentemente da paridade de i. Em particular, para $i = n$,

$$G \models [[x, {}_n y]_c, {}_n y^{-1}]_c = [x, {}_n y]_c^{(-1)^n y^{-n}}.$$

Substituindo em ambos os membros da identidade que surge em (4.23) o termo $[[x, {}_n y]_c, {}_n y^{-1}]_c$ pelo termo $[x, {}_n y]_c^{(-1)^n y^{-n}}$, concluímos que

$$G \models [x, {}_n y]_c^{(-1)^n 2y^{-n}} = [x, {}_n y]_c^{(-1)^n y^{-n-1}}.$$

Simplificando, fica

$$G \models [x, {}_n y]_c^{2y} = [x, {}_n y]_c. \tag{4.27}$$

Ora, elevando ao quadrado ambos os membros da identidade de (4.22), obtemos

$$G \models [x, {}_n y]_c^4 = [x, {}_n y]_c^{2y},$$

donde, por (4.27),

$$G \models [x, {}_n y]_c^3 = 1.$$

Finalmente, vamos provar por indução que se $k \in \mathbb{N}$ então, para quaisquer $x, y \in G$,

$$[[x, {}_{n-1}y]_c, y^{2k}]_c = 1.$$

Primeiro o passo inicial:

$$\begin{aligned}
[[x, {}_{n-1}y]_c, y^2]_c &= [[x, {}_{n-1}y]_c, y \cdot y]_c \\
&= [[x, {}_{n-1}y]_c, y]_c[[x, {}_{n-1}y]_c, y]_c^y \qquad \text{pela alínea 4 do lema 3.1} \\
&= [x, {}_{n}y]_c[x, {}_{n}y]_c^y \\
&= [x, {}_{n}y]_c^3 \qquad \text{por (4.22)} \\
&= 1.
\end{aligned}$$

Agora o passo indutivo:

$$\begin{aligned}
[[x, {}_{n-1}y]_c, y^{2(k+1)}]_c &= [[x, {}_{n-1}y]_c, y^{2k} \cdot y^2] \\
&= [[x, {}_{n-1}y]_c, y^2]_c[[x, {}_{n-1}y]_c, y^{2k}]_c^{y^2} \qquad \text{pela alínea 4 do lema 3.1} \\
&= 1.
\end{aligned}$$

Isto completa a demonstração. □

O mesmo artigo [17] termina com uma demonstração simples da solubilidade dos elementos da pseudovariedade $[\![[x, {}_{\omega}y]_c = [x, {}_{\omega+1}y]_c]\!]$, possível graças à proposição que acabamos de demonstrar.

Teorema 4.23. *A pseudovariedade* $[\![[x, {}_{\omega}y]_c = [x, {}_{\omega+1}y]_c]\!]$ *está contida na pseudovariedade dos grupos solúveis finitos.*

Demonstração. Seja G um grupo da pseudovariedade $[\![[x, {}_{\omega}y]_c = [x, {}_{\omega+1}y]_c]\!]$. Seja y um elemento de ordem ímpar de G. Então existe $k \in \mathbb{N}$ tal que $y^{2k} = y$. Pela proposição 4.22, $[x, {}_{\omega}y]_c = 1$, para todo $x \in G$. Logo, pela proposição 4.16, o conjunto dos elementos de ordem ímpar de G está contido em $\mathrm{Fit}(G)$. Dado qualquer elemento x de G, sejam $n \in \mathbb{N}_0$ e m um inteiro positivo ímpar tais que a ordem de x é $2^n m$. Como x^{2^n} tem ordem ímpar, igual a m, x^{2^n} é um elemento de $\mathrm{Fit}(G)$. Logo $G/\mathrm{Fit}(G)$ é um 2-grupo, e portanto é solúvel. Pela proposição 3.4, o grupo G é solúvel. □

Em [8] foi provado que um grupo da pseudovariedade $[\![[x, {}_{\omega}y]_c = [x, {}_{\omega+1}y]_c]\!]$ é supersolúvel[6] e que é o produto directo de um grupo nilpotente de ordem que é prima com 6 por um grupo H com um 3-subgrupo de Sylow normal N tal que H/N é um 2-grupo. Este subgrupo H pode então ser descrito de forma mais abreviada como sendo um produto semidirecto[7] de um 3-grupo por um 2-grupo. Pelo teorema 4.18, se H não for nilpotente então é divisível por S_3.

[6] Um grupo *supersolúvel* é um grupo que possui uma *série normal cíclica*, que é uma série normal cujos factores são cíclicos [30]. O grupo diedral D_{2n} é supersolúvel: ele possui um subgrupo cíclico H de índice 2 (razão pela qual se conclui que é normal), pelo que $D_{2n} \geq H \geq 1$ é uma série normal cíclica. Os grupos nilpotentes finitamente gerados são supersolúveis, e os grupos supersolúveis são solúveis. Encontramos entre os grupos diedrais exemplos de grupos supersolúveis que não são nilpotentes nem pertencem à pseudovariedade $[\![[x, {}_{\omega}y]_c = [x, {}_{\omega+1}y]_c]\!]$; o grupo A_4 é um exemplo de um grupo solúvel que não é supersolúvel.

[7] Um grupo G é um produto semidirecto de K por Q, denotado por $G = K \rtimes Q$, se $K \lhd G$ e se existir um subgrupo Q_0 de G tal que $K \cap Q_0 = 1$, $KQ_0 = G$ e $Q_0 \simeq Q$. Consequentemente, $G/K \simeq Q$.

4.6 Outros valores do período de um operador de Engel

Pouco depois de ter demonstrado em [17] o teorema 4.23, N. D. Gupta participou, em conjunto com H. Heineken, na elaboração do artigo [19], onde se fez um estudo mais sistemático da influência do período de Engel na estrutura de um grupo. Nesse artigo, os seus autores demonstraram um resultado que generaliza de modo muito abrangente o teorema 4.23: se k for um inteiro positivo ímpar, então os elementos das pseudovariedades $[\![[x,_\omega y]_c = [x,_{\omega+k} y]_c]\!]$ e $[\![[x,_\omega y]_t = [x,_{\omega+k} y]_t]\!]$ são solúveis. A proposição 4.8 garante-nos que existe uma infinidade de cada um destes dois tipos de pseudovariedades. A demonstração de que elas estão contidas na pseudovariedade dos grupos solúveis finitos é elaborada e depende da classificação dos grupos simples minimais, cuja extraordinária dificuldade já assinalámos. A primeira parte da demonstração de Gupta e Heineken consistiu em provar que qualquer grupo de ordem ímpar das pseudovariedades $[\![[x,_\omega y]_c = [x,_{\omega+k} y]_c]\!]$ e $[\![[x,_\omega y]_t = [x,_{\omega+k} y]_t]\!]$ é nilpotente.[8] No caso em que $k = 1$, este facto é uma consequência imediata dos teoremas 4.10 e 4.18. O grupo D_{10} é um exemplo de um grupo solúvel onde tanto ξ_c como ξ_t têm período par, e que portanto não está em nenhuma das pseudovariedades anteriores. O artigo de Gupta e Heineken contém mais alguns resultados sobre as variedades que têm vindo a ser o objecto de estudo deste capítulo (recordemos que $\mathfrak{S}_2$ designa a variedade dos grupos metabelianos):

$$[[x,_2 y]_c = [x,_3 y]_c] = [[x,_2 y]_c = [x,_4 y]_c]; \tag{4.28}$$

$$[[x,_n y]_c = [x,_{n+1} y]_c] \cap \mathfrak{S}_2 = [[x,_n y]_c = [x,_{n+2} y]_c] \cap \mathfrak{S}_2; \tag{4.29}$$

$$[[x,_n y]_c = [x,_{n+1} y]_c] = [[x,_n y]_t = [x,_{n+2} y]_t]. \tag{4.30}$$

A demonstração de (4.28) que nos é dada em [19] é algo maçadora. A igualdade (4.29) foi largamente generalizada por R. Brandl, o qual mostrou em [8] a igualdade de pseudovariedades

$$[\![[x,_n y]_c = [x,_{n+1} y]_c]\!] = [\![[x,_n y]_c = [x,_{n+2} y]_c]\!]$$

e em [9], a igualdade

$$[[x,_n y]_c = [x,_{n+1} y]_c] \cap \mathfrak{S} = [[x,_n y]_c = [x,_{n+2} y]_c] \cap \mathfrak{S}$$

onde, recorde-se, $\mathfrak{S}$ designa a classe dos grupos solúveis. Dito de outro modo, não existem grupos finitos nem grupos solúveis onde o período de ξ_c seja 2. De seguida, e para terminar este périplo pelo artigo de Gupta e Heineken, faremos a demonstração da igualdade (4.30).

Teorema 4.24. $[[x,_n y]_c = [x,_{n+1} y]_c] = [[x,_n y]_t = [x,_{n+2} y]_t]$.

[8] A solubilidade de um qualquer grupo finito de ordem ímpar era já um celebrado resultado de Feit e Thompson [13].

Demonstração. Seja G um grupo.

$$\begin{aligned} G \models [x, {}_n y]_c [x, {}_{n+1} y]_c^2 = 1 &\Leftrightarrow G \models [x, {}_n y]_c [x, {}_{n+1} y]_c^2 [[x, {}_{n+1} y]_c, y]_c = [x, {}_{n+2} y]_c \\ &\Leftrightarrow G \models [x, {}_n y]_c [x, {}_{n+1} y]_c \, y^{-1} [x, {}_{n+1} y]_c \, y = [x, {}_{n+2} y]_c \\ &\Leftrightarrow G \models [x, {}_n y]_c [[x, {}_n y], y]_c \, y^{-1} [[x, {}_n y]_c, y]_c \, y = [x, {}_{n+2} y]_c \\ &\Leftrightarrow G \models [x, {}_n y]_c^{y^2} = [x, {}_{n+2} y]_c. \end{aligned}$$

Então, pelas alíneas 2 e 3 da proposição 4.4,

$$G \models [x, {}_n y]_c [x, {}_{n+1} y]_c^2 = 1 \Leftrightarrow G \models [x, {}_n y]_t = [x, {}_{n+2} y]_t.$$

Logo, o teorema fica demonstrado se provarmos a equivalência

$$G \models [x, {}_n y]_c [x, {}_{n+1} y]_c^2 = 1 \Leftrightarrow G \models [x, {}_n y]_c = [x, {}_{n+1} y]_c.$$

Comecemos por supor que

$$G \models [x, {}_n y]_c = [x, {}_{n+1} y]_c. \tag{4.31}$$

Então, pela proposição 4.22,

$$G \models [x, {}_n y]_c^3 = 1. \tag{4.32}$$

Combinando (4.31) e (4.32), obtemos $G \models [x, {}_n y]_c [x, {}_{n+1} y]_c^2 = 1$. Reciprocamente, suponhamos que

$$G \models [x, {}_n y]_c [x, {}_{n+1} y]_c^2 = 1.$$

Acontece o seguinte:

$$\begin{aligned} G \models [x, {}_n y]_c [x, {}_{n+1} y]_c^2 = 1 &\Leftrightarrow G \models y^{-1} [x, {}_n y]_c \, y [x, {}_{n+1} y]_c = 1 \\ &\Leftrightarrow G \models [x, {}_n y]_c \, y [x, {}_{n+1} y]_c \, y^{-1} = 1 \\ &\Leftrightarrow G \models [x, {}_n y]_c \, y [x, {}_n y]_c^{-1} y^{-1} [x, {}_n y]_c = 1 \\ &\Leftrightarrow G \models [x, {}_n y]_c [y^{-1}, [x, {}_n y]_c]_c = 1. \end{aligned}$$

A nossa hipótese é portanto equivalente a

$$G \models [x, {}_n y]_c = [[x, {}_n y]_c, y^{-1}]_c. \tag{4.33}$$

Substituindo em (4.33) a variável y por y^{-1}, obtemos

$$G \models [x, {}_n y^{-1}]_c = [[x, {}_n y^{-1}]_c, y]_c. \tag{4.34}$$

Substituindo agora em (4.34) a variável x por $[x, {}_n y]_c$, obtemos

$$G \models [[x, {}_n y]_c, {}_n y^{-1}]_c = [[[x, {}_n y]_c, {}_n y^{-1}]_c, y]_c. \tag{4.35}$$

Por (4.33), podemos substituir em (4.35) o termo $[[x, {}_n y]_c, {}_n y^{-1}]_c$ pelo termo $[x, {}_n y]_c$, concluindo-se assim que a identidade $[x, {}_n y]_c = [x, {}_{n+1} y]_c$ é válida em G. □

Esta demonstração deixa transparecer a sua proximidade com a da proposição 4.22.

4.7 Influência do pré-período

Os grupos cujo pré-período de Engel é igual a 1 são precisamente os grupos Abelianos não triviais. Este facto é um caso particular de um resultado mais geral de [18]. Iremos enunciar e demonstrar esse resultado. Necessitamos de uma definição prévia.

Dados elementos $x_1, \ldots, x_n$ de um grupo G, seja $[x_1, \ldots, x_n]_c$ o elemento de G definido por recorrência do seguinte modo: $[x_1]_c = x_1$ e $[x_1, \ldots, x_n]_c = [[x_1, \ldots, x_{n-1}]_c, x_n]_c$ se $n > 0$. Em particular, $[x, \underbrace{y, \ldots, y}_{n}]_c = [x, {}_n y]_c$.

Lema 4.25. *Se um grupo G satisfaz uma identidade $[x, y]_c = [x_1, \ldots, x_n]_c$ em que $n \geq 3$ e $x_1, x_2 \in \{x, y, x^{-1}, y^{-1}\}$, então para quaisquer $x, y \in G$ o comutador $[x, y]_c$ é um elemento de $\gamma_\omega(G)$.*

Demonstração. Seja G um grupo onde é válida a identidade

$$[x, y]_c = [x_1, \ldots, x_n]_c \tag{4.36}$$

onde $n \geq 3$ e $x_1, x_2 \in \{x, y, x^{-1}, y^{-1}\}$. Se (x_1, x_2) for um dos pares

$$(x, x), (x, x^{-1}), (x^{-1}, x), (x^{-1}, x^{-1}), (y, y), (y, y^{-1}), (y^{-1}, y), (y^{-1}, y^{-1})$$

então $[x_1, x_2]_c = 1$, donde $[x, y]_c = 1$, por (4.36). Vamos agora supor que se verifica alguma das restantes possibilidades para o par (x_1, x_2):

$$(x, y), (x, y^{-1}), (x^{-1}, y), (x^{-1}, y^{-1}), (y, x), (y, x^{-1}), (y^{-1}, x), (y^{-1}, x^{-1}). \tag{4.37}$$

O lema fica demonstrado se provarmos por indução sobre k que para qualquer $k \in \mathbb{N}_0$ existem $\varepsilon \in \{-1, 1\}$ e $g_i, g \in G$, com $i \in \{1, \ldots, (k+1)(n-2)\}$, tais que

$$[x, y]_c = [x_1, x_2, g_1, \ldots, g_{(k+1)(n-2)}]_c^{\varepsilon g}. \tag{4.38}$$

Designemos por t_k o número $(k+1)(n-2)$. O passo inicial é apenas a igualdade (4.36). Suponhamos que temos (4.38). Aplicando a cada um dos sete últimos casos de (4.37) a alínea 1 e/ou a alínea 2 do lema 3.1, concluímos que existem $\delta \in \{-1, 1\}$ e $h \in G$ tais que $[x_1, x_2]_c = [x, y]_c^{\delta h}$. Por (4.36), $[x_1, x_2]_c = [x_1, \ldots, x_n]_c^{\delta h}$. Substituindo em (4.38) o termo $[x_1, x_2]_c$ por $[x_1, \ldots, x_n]_c^{\delta h}$ obtemos

$$[x, y]_c = [[x_1, x_2, x_3, \ldots, x_n]_c^{\delta}, g_1^{h^{-1}}, \ldots, g_{t_k}^{h^{-1}}]_c^{\varepsilon h g}. \tag{4.39}$$

Se $\delta = 1$, isto conclui o passo indutivo sobre k, uma vez que a sequência

$$x_3, \ldots, x_n, g_1^{h^{-1}}, \ldots, g_{t_k}^{h^{-1}}$$

tem $t_k + (n-2) = t_{k+1}$ elementos. Suponhamos agora que $\delta = -1$. Seja $(z_m)_{-1 \leq m \leq t_k}$ a sequência definida recursivamente do seguinte modo:

$$\begin{cases} z_{-1} = 1 \\ z_0 = [x_1, x_2, x_3, \ldots, x_n]_c \\ z_{m+1} = [z_m, g_{m+1}^{h^{-1} z_{-1} \cdots z_{m-1}}]_c \quad \text{se } 0 \leq m \leq t_k - 1 \end{cases}$$

Pela alínea 2 do lema 3.1, para $0 \leq m \leq t_k - 1$,

$$[z_m^{-1}, g_{m+1}^{h^{-1}z_{-1}\cdots z_{m-1}}]_c = [z_m, g_{m+1}^{h^{-1}z_{-1}\cdots z_{m-1}}]_c^{-z_m^{-1}} = z_{m+1}^{-z_m^{-1}}. \tag{4.40}$$

Vamos mostrar por indução sobre m que, para $0 \leq m \leq t_k - 1$,

$$[x, y]_c = [z_m^{-1}, g_{m+1}^{h^{-1}z_{-1}\cdots z_{m-1}}, g_{m+2}^{h^{-1}z_{-1}\cdots z_{m-1}}, \ldots, g_{t_k}^{h^{-1}z_{-1}\cdots z_{m-1}}]_c^{\varepsilon z_{m-1}^{-1}\cdots z_{-1}^{-1}hg}. \tag{4.41}$$

O passo inicial é a igualdade (4.39). O passo indutivo justifica-se através de (4.40):

$$\begin{aligned}
[x, y]_c &= [[z_m^{-1}, g_{m+1}^{h^{-1}z_{-1}\cdots z_{m-1}}]_c, g_{m+2}^{h^{-1}z_{-1}\cdots z_{m-1}}, \ldots, g_{t_k}^{h^{-1}z_{-1}\cdots z_{m-1}}]_c^{\varepsilon z_{m-1}^{-1}\cdots z_{-1}^{-1}hg} \\
&= [z_{m+1}^{-z_m^{-1}}, g_{m+2}^{h^{-1}z_{-1}\cdots z_{m-1}}, \ldots, g_{t_k}^{h^{-1}z_{-1}\cdots z_{m-1}}]_c^{\varepsilon z_{m-1}^{-1}\cdots z_{-1}^{-1}hg} \\
&= [z_{m+1}^{-1}, g_{m+2}^{h^{-1}z_{-1}\cdots z_{m-1}z_m}, \ldots, g_{t_k}^{h^{-1}z_{-1}\cdots z_{m-1}z_m}]_c^{\varepsilon z_m^{-1} z_{m-1}^{-1}\cdots z_{-1}^{-1}hg}.
\end{aligned}$$

Tomando em (4.41) m igual a $t_k - 1$ e novamente por (4.40),

$$[x, y]_c = [z_{t_k-1}^{-1}, g_{t_k}^{h^{-1}z_{-1}z_0z_1\cdots z_{t_k-2}}]_c^{\varepsilon z_{t_k-2}^{-1}\cdots z_{-1}^{-1}hg} = z_{t_k}^{(-\varepsilon)z_{t_k-1}^{-1} z_{t_k-2}^{-1}\cdots z_{-1}^{-1}hg}. \tag{4.42}$$

Para cada $1 \leq m \leq t_k$ seja $f_m = g_m^{h^{-1}z_{-1}\cdots z_{m-2}}$. Então $z_m = [x_1, \ldots, x_n, f_1, \ldots, f_m]_c$. Logo, tomando m igual a t_k e por (4.42),

$$[x, y]_c = [x_1, \ldots, x_n, f_1, \ldots, f_{t_k}]_c^{(-\varepsilon)z_{t_k-1}^{-1}\cdots z_{-1}^{-1}hg}.$$

Isto conclui o passo indutivo sobre k, uma vez que a sequência

$$x_3, \ldots, x_n, f_1, \ldots, f_{t_k}$$

tem $t_k + (n-2) = t_{k+1}$ elementos. □

Corolário 4.26. *Um grupo nilpotente que satisfaz uma identidade* $[x, y]_c = [x_1, \ldots, x_n]_c$ *em que* $n \geq 3$ *e* $x_1, x_2 \in \{x, y, x^{-1}, y^{-1}\}$ *é um grupo Abeliano.*

Teorema 4.27. *Um grupo solúvel que satisfaz uma identidade* $[x, y]_c = [x_1, \ldots, x_n]_c$ *em que* $n \geq 3$, $x_1, x_2 \in \{x, y, x^{-1}, y^{-1}\}$ *e* $x_3 \in \{x^k, y^k : k \in \mathbb{Z}\}$ *é um grupo Abeliano.*

Demonstração. Seja G um grupo solúvel onde a identidade

$$[x, y]_c = [x_1, x_2, x_3, x_4, \ldots, x_n]_c \tag{4.43}$$

é válida e seja d o grau de solubilidade de G. Suponhamos que $d \geq 2$. Então podemos considerar o subgrupo $H = G^{(d-2)}$. Sejam $a \in H'$ e $b \in H$. Se $x_3 = x^k, k \in \mathbb{Z}$, substituindo em (4.43) a variável x por a e a variável y por b obtemos

$$[a, b]_c = [[[x_1, x_2]_c, a^k]_c, x_4 \ldots, x_n]_c \tag{4.44}$$

e se $x_3 = y^k, k \in \mathbb{Z}$, substituindo x por b e y por a obtemos

$$[b, a]_c = [[[x_1, x_2]_c, a^k]_c, x_4 \ldots, x_n]_c. \tag{4.45}$$

Ora $[[x_1, x_2]_c, a^k]_c \in [H', H'] = H''$. E como H'' é um subgrupo normal,

$$[[[x_1, x_2]_c, a^k]_c, x_4, \ldots, x_n]_c \in H''.$$

Assim, em qualquer dos dois casos (4.44) e (4.45), $[a, b]_c \in H''$. Mas

$$H'' = (G^{(d-2)})'' = G^{(d)} = 1$$

pelo que $[a, b]_c = 1$. Logo $\gamma_3(H) = 1$. Então, pelo corolário 4.26, o grupo H é Abeliano e portanto $G^{(d-1)} = H' = 1$. Mas isto contradiz a minimalidade de d. Logo $d \leq 1$. □

Teorema 4.28. *Um grupo finito que satisfaz uma identidade* $[x, y]_c = [x_1, \ldots, x_n]_c$ *em que* $n \geq 3$, $x_1, x_2 \in \{x, y, x^{-1}, y^{-1}\}$ *e* $x_3 \in \{x^k, y^k : k \in \mathbb{Z}\}$ *é um grupo Abeliano.*

Demonstração. Suponhamos que o teorema é falso. Então existe um grupo G de ordem mínima na classe $[\![[x, y]_c = [x_1, \ldots, x_n]_c]\!] \setminus \mathsf{Ab}$. Como todo o seu subgrupo próprio é Abeliano, pela proposição 3.6 o grupo G é solúvel. Logo, pelo teorema 4.27, G é Abeliano: absurdo! □

Ainda em [18], entre outros resultados similares, N. D. Gupta demonstra que os grupos que satisfazem alguma das identidades $[x, y]_c = [x, {}_n y^{-1}]_c$, $n \geq 2$, ou $[x, y]_c = [x, {}_n y]_c$, $2 \leq n \leq 3$ são precisamente os Abelianos.

De modo independente, D. Nikolova e R. Brandl demonstraram que os grupos finitos cujo pré-período de Engel é 2 são solúveis [26, 10]. Em ambos os casos, a demonstração depende da classificação dos grupos simples minimais. Em [10] são descritas algumas características dos grupos finitos com pré-período de Engel igual a 2: se G é um desses grupos então $G/\mathrm{Fit}(G)$ é supersolúvel, metabeliano e os seus subgrupos de Sylow são Abelianos. Também são dadas condições suficientes para que um grupo tenha pré-período de Engel menor ou igual a 2: uma delas é a de que seja o produto semidirecto de dois grupos Abelianos finitos de ordens primas entre si.

Se subirmos mais um patamar na nossa pesquisa, encontramos grupos finitos não solúveis cujo pré-período de Engel é 3: por exemplo, A_5.

Epílogo

No decorrer do trabalho que apresentámos pudemos apreciar as vantagens da linguagem e da teoria da Álgebra Universal Finita, tanto sob o ponto de vista descritivo como sob o ponto de vista da obtenção de resultados. Um bom exemplo disto são as proposições acerca da invertibilidade dos operadores implícitos sobre grupos finitos: em primeiro lugar aquela que trata dos operadores que são invertíveis numa determinada pseudovariedade de p-grupos finitos (teorema 3.13), e em segundo lugar aquela que diz respeito aos operadores que são invertíveis na pseudovariedade dos grupos nilpotentes finitos (corolário 3.14). Do ponto de vista descritivo, estão lá as noções de operador implícito e de operação implícita. Mas mesmo que restringíssemos o enunciado destas proposições a operadores explícitos (e a noção de operador explícito, sinónima da noção de operador polinomial introduzida no primeiro capítulo, é uma noção da Álgebra Universal que extravasa a Álgebra Universal Finita), os métodos utilizados não deixariam de ser "implícitos", isto é, do domínio da Álgebra Universal Finita. É aliás natural que assim seja, pois a invertibilidade de um operador implícito está relacionada com a sua potência ómega na medida em que esse operador é invertível se e só se a sua potência ómega for o operador identidade, e a potência ómega de um operador explícito é um operador implícito que pode não ser explícito. Em geral, o comportamento dinâmico de um operador implícito está estreitamente relacionado com a sua potência ómega, como vimos na secção 4.1. Deste modo foi possível organizar o material do último capítulo, tornando a sua apresentação clara e escorreita (pelo menos esperamos ser este o julgamento do leitor).

Em [2], na sequência do estudo sobre operadores implícitos invertíveis, Almeida mostrou um interesse particular pelas pseudoidentidades entre as componentes da potência ómega de um operador binário. Dado um operador implícito binário $f = (w_1, w_2)$, seja π o conjunto dos primos de $\mathbb{N}$ que dividem o traço de $A(f)$, e seja $(v_1, v_2) = f^\omega$. Almeida mostrou que se Ab satisfaz a pseudoidentidade $w_1 = w_2$ e se o determinante de $A(f)$ for igual a zero (como o único grupo Abeliano onde f é invertível é o grupo trivial, esta segunda condição é redundante se f for um operador explícito, pelo teorema 3.13) então a pseudovariedade $\mathsf{G_{nil}} * \mathsf{G_{sol},\pi}$ gerada pelos produtos semidirectos de elementos de $\mathsf{G_{nil}}$ por elementos de $\mathsf{G_{sol},\pi}$ satisfaz a pseudoidentidade $v_1 = v_2$:

$$\mathsf{G_{nil}} * \mathsf{G_{sol},\pi} \subseteq [\![v_1 = v_2]\!] \qquad (*)$$

Logo, uma condição necessária para que tenhamos a igualdade

$$\mathsf{G}_{\mathsf{nil}} = [\![v_1 = v_2]\!] \qquad (**)$$

é que π seja o conjunto vazio. Pela proposição 2.45, esta condição é equivalente à invertibilidade do traço de $A(f)$. Trata-se de uma condição necessária, mas que evidentemente não é suficiente, como se conclui pelo operador (x, y). No entanto, a condição imposta sobre o traço de $A(f)$ para que a igualdade $(**)$ seja válida não é demasiado restritiva, pois no teorema 6.1 do mesmo artigo é-nos dito que se f for o operador $(b^{-1}ab, a)$ então $(**)$ verifica-se. Logo podemos deduzir a partir daqui que um grupo finito é nilpotente se e só se todo o subgrupo gerado por dois elementos é nilpotente. Este, recordemos, é precisamente o corolário 4.12 do teorema 4.10, teorema esse que nos diz que os grupos nilpotentes finitos são precisamente os grupos finitos onde o operador $\xi_t = (xyx^{-1}y^{-1}, y)$ é aperiódico. A demonstração da validade da igualdade $\mathsf{G}_{\mathsf{nil}} = [\![v_1 = v_2]\!]$ no caso do operador $(b^{-1}ab, a)$ foi comunicada pessoalmente por Almeida ao autor deste trabalho, e é independente dos resultados sobre os operadores de Engel. O operador $(b^{-1}ab, a)$ constitui portanto uma alternativa à demonstração do corolário 4.12.

Como dissemos na introdução desta monografia, um dos corolários da classificação de Thompson dos grupos simples minimais é o de que um grupo finito é solúvel se e só se todo o subgrupo gerado por dois elementos é solúvel [33]. A conjectura de B. Plotkin está relacionada com esta questão: usando agora a linguagem da Álgebra Universal Finita, recordemos que essa conjectura afirma que se π for a primeira componente da potência ómega do operador ternário $([[x, y]_c, [x, z]_c]_c, y, z)$ então $\mathsf{G}_{\mathsf{sol}} = [\![\pi([x, y]_c, x, y) = 1]\!]$. A conjectura de Plotkin propõe portanto uma pseudoidentidade em duas variáveis como forma de caracterização da pseudovariedade $\mathsf{G}_{\mathsf{sol}}$. Será que também poderemos encontrar entre os operadores binários estudados por Almeida um para o qual se verifica a igualdade $\mathsf{G}_{\mathsf{sol}} = [\![v_1 = v_2]\!]$? Por $(*)$, uma condição suficiente para que tenhamos a inclusão $\mathsf{G}_{\mathsf{sol}} \subseteq [\![v_1 = v_2]\!]$ é que π seja o conjunto de todos os primos de $\mathbb{N}$, além da pseudoidentidade $w_1 = w_2$ ser válida em Ab e do determinante de $A(f)$ ser nulo. O operador $([a, b]_c, [a, b]_t)$ está nestas condições (o traço da sua matriz de frequências é nulo). Para este operador Almeida conjecturou a igualdade $\mathsf{G}_{\mathsf{sol}} = [\![v_1 = v_2]\!]$; tal como é referido em [2], os cálculos com o GAP [32] até agora efectuados não detectaram qualquer contra-exemplo entre os grupos simples minimais. Constitui um problema interessante encontrar uma pseudoidentidade em duas variáveis que caracterize a pseudovariedade $\mathsf{G}_{\mathsf{sol}}$, demonstrando-o sem o recurso à classificação dos grupos simples minimais.

O problema de, fixado n, encontrar uma pseudoidentidade de operadores n-ários que caracterize uma pseudovariedade dada nem sempre tem solução. É o que acontece com a pseudovariedade dos grupos metabelianos finitos quando $n \leq 3$: em [22] é exibido um grupo finito de ordem 2^{14} que não é metabeliano mas cujos subgrupos gerados por 3 elementos (ou menos) são metabelianos.

Um problema que é de certo modo o inverso do anterior é o de caracterizar uma pseudovariedade definida por uma determinada pseudoidentidade. No capítulo 4

vimos diversos problemas em aberto deste tipo. Destacamos aquele que diz respeito à pseudovariedade $[\![[x, {}_{\omega}y]_c = [x, {}_{\omega+1}y]_c]\!]$, para o qual contribuímos mostrando que os seus elementos não nilpotentes são divisíveis por S_3.

Bibliografia

[1] J. Almeida, *Finite Semigroups and Universal Algebra*, World Scientific, Singapore, 1995. English translation.

[2] ———, *Dynamics of finite semigroups*, in Semigroups, Algorithms, Automata and Languages, G. M. S. Gomes, J.-E. Pin, and P. V. Silva, eds., Singapore, 2002, World Scientific, 269–292.

[3] ———, *Dynamics of implicit operations and tameness of pseudovarieties of groups*, Trans. Amer. Math. Soc. **354** (2002) 387–411.

[4] ———, *Finite semigroups: an introduction to a unified theory of pseudovarieties*, in Semigroups, Algorithms, Automata and Languages, G. M. S. Gomes, J.-E. Pin, and P. V. Silva, eds., Singapore, 2002, World Scientific, 3–64.

[5] J. Almeida and M. V. Volkov, *Profinite methods in finite semigroup theory*, in Proceedings of International Conference "Logic and applications" honoring Yu. L. Ershov on his 60-th birthday anniversary and of International Conference on mathematical logic, honoring A. I. Mal'tsev on his 90-th birthday anniversary and 275-th anniversary of the Russian Academy of Sciences, S. S. Goncharov, ed., Novosibirsk, Russia, 2002, 3–28.

[6] A. Almeida Costa, *Cours d'algèbre générale*, Fundação Calouste Gulbenkian, 2ª ed., 1969.

[7] G. Baumslag, *Residual nilpotence and relations in free groups*, J. Algebra **2** (1965) 271–282.

[8] R. Brandl, *Engel cycles in finite groups*, Arch. Math. (Basel) **41** (1983) 97–102.

[9] ———, *Infinite soluble groups with Engel cycles; a finiteness condition*, Math. Z. **182** (1983) 259–264.

[10] ———, *On groups with small Engel depth*, Bull. Austral. Math. Soc. **28** (1983) 101–110.

[11] R. Brandl and D. Nikolova, *Simple groups of small Engel depth*, Bull. Austral. Math. Soc. **33** (1986) 245–251.

[12] S. Burris and H. P. Sankappanavar, *A Course in Universal Algebra*, no. 78 in Grad. Texts in Math., Springer, Berlin, 1981.

[13] W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963) 775–1029.

[14] P. Flavell, *Finite groups in which every two elements generate a soluble group*, Invent. Math. **121** (1995) 279–285.

[15] D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968.

[16] F. Grunewald, B. Kuniavskii, D. Nikolova, and E. Plotkin, *Two-variable identities in groups and Lie algebras*, Zapiski Nauch. Seminarov POMI **272** (2000) 161–176. To appear also in J. Math. Sciences.

[17] N. D. Gupta, *Groups with Engel-like conditions*, Arch. Math. (Basel) **17** (1966) 193–199.

[18] ———, *Some group laws equivalent to the commutative law*, Arch. Math. (Basel) **17** (1966) 97–102.

[19] N. D. Gupta and H. Heineken, *Groups with two-variable commutator identity*, Math. Z. **95** (1967) 276–287.

[20] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, no. 84 in Grad. Texts in Math., Springer-Verlag, New York, 1982.

[21] S. MacLane, *Categories for the Working Mathematician*, no. 5 in Grad. Texts in Math., Springer-Verlag, New York, 2nd ed., 1998.

[22] B. H. Neumann, *On a conjecture of Hanna Neumann*, Proc. Glasgow Math. Assoc. **3** (1956) 13–17.

[23] H. Neumann, *Varieties of Groups*, Springer, Berlin, 1967.

[24] D. Nikolova, *Groups with a 2-variable commutator identity*, Ph.D. thesis, Sofia Univ., 1983.

[25] ———, *Groups with a two-variable commutator identity*, C. R. Acad. Bulgare Sci. **36** (1983) 721–724.

[26] ———, *Solubility of finite groups with a two-variable commutator identity*, Serdica **11** (1985) 59–63.

[27] J.-E. Pin, *Varieties of Formal Languages*, Plenum, London, 1986. English translation.

[28] L. Ribes and P. A. Zalesskiĭ, *Profinite Groups*, no. 40 in Ergeb. Math. Grenzgebiete 3, Springer, Berlin, 2000.

[29] D. J. S. Robinson, *Finiteness Conditions and Generalized Soluble Groups*, vol. 2 of Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, Berlin, 1972.

[30] ———, *A Course in Theory of Groups*, no. 80 in Grad. Texts in Math., Springer-Verlag, New York, 2 ed., 1996.

[31] J. J. Rotman, *An Introduction to the Theory of Groups*, no. 148 in Grad. Texts in Math., Springer, New York, 4th ed., 1995.

[32] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.1*, Aachen, St Andrews, 1999.
(`http://www-gap.dcs.st-and.ac.uk/~gap`).

[33] J. G. Thompson, *Non-solvable groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc. **74** (1968) 383–437.

[34] S. Willard, *General Topology*, Addison-Wesley, Reading, Mass., 1970.

[35] M. Zorn, *Nilpotency of finite groups (abstract)*, Bull. Amer. Math. Soc. **42** (1936) 485–486.

Índice remissivo

Índice de símbolos