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

Identidades Polinomiais via Identidades de Grupo: A Conjectura de Brian Hartley

Dalton Couto Silva

Orientador: Humberto Luiz Talpo

São Carlos
Fevereiro de 2017

Identidades Polinomiais via Identidades de Grupo: A Conjectura de Brian Hartley

Dalton Couto Silva

Orientador: Humberto Luiz Talpo

Dissertação apresentada ao Departamento de Matemática - UFSCar, como parte dos requisitos para a obtenção do título de Mestre em Matemática.

São Carlos
Fevereiro de 2017

Agradecimentos

Resumo

Neste trabalho, apresentamos a Conjectura de Brian Hartley e estudamos sua validade, ou seja, verificamos se identidades de grupo no grupo das unidades $U(\mathbb{F}G)$ levam $\mathbb{F}G$ a satisfazer identidades polinomiais, onde G é um grupo de torção e $\mathbb{F}$ corpo qualquer. Tal estudo será realizado primeiramente para corpos infinitos, e em seguida para corpos quaisquer. A partir deste resultado, serão deduzidas condições necessárias e suficientes em um grupo G, para que o grupo das unidades $U(\mathbb{F}G)$ satisfaça identidades de grupo.

Abstract

In this work, we present the Conjecture of Brian Hartley and study its validity, i.e, we verify if group identities in the unity group $U(\mathbb{F}G)$ make $\mathbb{F}G$ satisfy a polynomial identity, where G is a torsion group and $\mathbb{F}$ any field. This study will be made first for infinite fields, and next for any field. From this result, will be deduced necessary and suficient conditions in a group G, for the unity group $U(\mathbb{F}G)$ satisfy group identities.

Conteúdo

Introdução

Em uma tentativa de conectar as estruturas aditiva e multiplicativa de uma álgebra de grupo $\mathbb{F}G$ de um grupo G sobre um corpo $\mathbb{F}$, Brian Hartley, no final dos anos 70, propôs a seguinte conjectura:

Conjectura. *Sejam G um grupo de torção e $\mathbb{F}$ um corpo. Se o grupo das unidades $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, então $\mathbb{F}G$ satisfaz uma identidade polinomial.*

Uma demonstração para esta conjectura foi dada por C. H. Liu, em 1999, [12]. Antes dele, casos particulares da conjectura foram estudados, como segue:

- Primeiramente, em 1981, D. S. Warhust estudou a conjectura em sua tese de doutorado, investigando determinadas palavras satisfeitas por $U(\mathbb{F}G)$.
- No mesmo ano, P. Menal sugeriu uma possível solução para alguns p-grupos.
- Com a hipótese do corpo ser infinito, em 1991, J. Gonçalves e A. Mandel verificaram a conjectura para o caso em que a identidade de grupo é uma identidade de semigrupo.
- Três anos depois, A. Giambruno, E. Jespers e A. Valenti verificaram dois casos da conjectura: a característica do corpo sendo zero e a característica do corpo sendo p, com o grupo G não contendo p-elementos.
- Em 1997, A. Giambruno, S. Sehgal e A. Valenti provaram a conjectura para o caso em que o corpo é infinito.

Tendo encontrado respostas positivas para a conjectura de Brian Hartley, o próximo passo passou a ser encontrar condições necessárias e suficientes em um grupo G para que $U(\mathbb{F}G)$ satisfaça identidades de grupo. Tal resultado foi feito por D. Passman no caso infinito em 1997 e por D. Passman e C. H. Liu em 1999 para o caso geral.

Dividiremos esta dissertação em três capítulos. O primeiro apresenta fundamentos teóricos básicos da teoria de anéis, grupos e polinômios não comutativos, os quais serão importantes no decorrer deste trabalho. As duas primeiras seções deste capítulo serão dedicadas ao estudo dos Grupos, nomeadamente os Grupos de Torção e os Grupos Livres. Na sequência, trataremos de algumas classes importantes de anéis, e faremos uma breve introdução ao conceito de álgebra, com alguns exemplos. Passaremos então a dois conceitos específicos: o estudo do Radical de Jacobson de uma álgebra e o estudo das Álgebras de Grupo, esta última sendo um dos temas centrais de nosso trabalho. A última seção será dedicada ao estudo dos polinômios não comutativos, em particular, identidades polinomiais e suas relações com grupos, anéis e álgebras.

No segundo capítulo, começamos apresentando alguns resultados clássicos das Álgebras de Grupo relacionados às identidades polinomiais. A partir da seção 2, utilizamos tais resultados para demonstrar o caso particular da conjectura de Brian Hartley, em que o corpo $\mathbb{F}$ é infinito. Com a validade do caso particular, buscamos, na seção 3, condições necessárias e suficientes em um grupo G para que $U(\mathbb{F}G)$ satisfaça uma identidade de grupo. Este estudo surgiu do problema de verificar se a recíproca da conjectura de Brian Hartley era verdadeira.

No terceiro capítulo, estudamos o caso geral, em que o corpo $\mathbb{F}$ não é necessariamente infinito. Para isso , a primeira seção é dedicada a encontrar resultados que substituam os argumentos utilizados no caso infinito. Com tais resultados, provamos a conjectura de uma forma geral, seguindo de perto o trabalho feito no capítulo 2. Finalizamos este capítulo e a dissertação com a generalização dos resultados encontrados na seção 3 do capítulo 2.

CAPÍTULO 1

Conceitos Preliminares

Este capítulo tem como objetivo apresentar os fundamentos teóricos necessários para o entendimento do texto.

Dessa forma, optamos por definir conceitos e enunciar resultados que sejam menos usuais nas disciplinas básicas de álgebra, e deixamos referências suficientes em cada seção. Vale mencionar aqui algumas referências gerais, que nos guiaram na escrita deste capítulo: [1], [2], [3], [7], [8], [15] e [16].

1.1 Grupos de Torção

Vamos assumir nesta seção que o leitor conheça as definições iniciais da Teoria de Grupos (grupos, subgrupos, homomorfismos, quocientes, produtos diretos), e enunciar as definições e resultados necessários para o seguimento do texto. Para uma exposição mais completa a respeito do assunto, recomendamos [8].

Dado um grupo G, chamamos de *ordem* de G ao seu número de elementos, e denotamos por $|G|$. Para um elemento $g \in G$, definimos sua *ordem*, ou *período*, como sendo o número de elementos do subgrupo gerado por g, ou seja, $|g| = |\langle g \rangle|$. Uma classe importante de grupos, e amplamente utilizada neste trabalho, é a classe dos *Grupos de Torção*, isto é, grupos em que todos os elementos possuem ordem finita. É importante observar que os grupos de torção não são necessariamente finitos, como mostra o seguinte exemplo:

Exemplo 1.1.1. Sejam $\mathbb{Q}$ o grupo abeliano dos números racionais e $\mathbb{Z} \lhd \mathbb{Q}$ o subgrupo normal dos inteiros. Assim,

$$\frac{\mathbb{Q}}{\mathbb{Z}} = \left\{ \frac{p}{q} + \mathbb{Z} : p, q \in \mathbb{Z}, q \neq 0 \right\}$$

é infinito, e de torção pois, dado $p/q + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$,

$$q(p/q + \mathbb{Z}) = p + \mathbb{Z} = \mathbb{Z}.$$

O exemplo acima ilustra um grupo de ordem infinita em que todos os seus elementos possuem ordem finita. Ainda, vemos que, sendo um grupo abeliano, todos os seus subgrupos são normais. Mas a recíproca dessa afirmação não é válida, uma vez que existem grupos não abelianos em que todos os seus subgrupos são normais. A classe de grupos de torção que possuem esta propriedade nos será interessante.

Definição 1.1.2. Dizemos que um grupo G é *hamiltoniano* se todos os seus subgrupos são normais e G não é abeliano.

Exemplo 1.1.3. O principal exemplo de grupo hamiltoniano é o grupo dos quatérnios

$$K_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Este grupo não é abeliano, uma vez que $i \cdot j = k$ e $j \cdot i = -k$, mas todos os seus subgrupos são normais.

Os grupos hamiltonianos foram estudados primeiramente por Richard Dedekind no final do século XIX, e receberam este nome em homenagem a Willian Rowan Hamilton, em virtude de sua descoberta dos números quatérnios. Anos depois, Dedekind e Reinhold Baer demonstraram o seguinte teorema, classificando os grupos hamiltonianos.

Teorema 1.1.4. *Um grupo hamiltoniano G pode ser escrito da forma:*

$$G = K_8 \times A \times B$$

onde A é um grupo abeliano em que todos os elementos não triviais tem ordem 2 e B é um grupo abeliano em que todo elemento tem ordem ímpar.

Demonstração. [7], Teorema 12.5.4. □

Em um grupo não abeliano G, dois subconjuntos de grande interesse são o seu centro, denotado $Z(G)$, e o comutador, denotado G'. A fim de definí-los, denotemos o *comutador* entre dois elementos $x, y \in G$ por $(x, y) = x^{-1}y^{-1}xy$.

Definição 1.1.5. Dado um grupo G, definimos o *centro* $Z(G)$ como sendo o conjunto dos elementos $x \in G$ tal que $xy = yx$, $\forall y \in G$. Ainda, definimos o seu *subgrupo comutador* G', como sendo o subgrupo gerado por todos os comutadores de elementos de G.

Assim, um elemento qualquer do subgrupo comutador, $x \in G'$, pode ser escrito da forma:

$$x = (x_1, y_1)^{r_1}(x_2, y_2)^{r_2} \dots (x_n, r_n)^{r_n}$$

onde $x_i, y_i \in G$, $r_i \in \mathbb{Z}$ $\forall i = 1, \ldots, n$.

O próximo resultado relaciona o índice do centro $Z(G)$ com a ordem do comutador G'. Esta relação será importante mais a frente, e sua demonstração pode ser encontrada em [19, Teorema I.4.2].

Proposição 1.1.6. *Sejam G um grupo qualquer e $Z(G)$ seu centro. Se $[G : Z(G)] = n < \infty$, então G' é finito e sua ordem divide n.*

Outra relação importante é:

Proposição 1.1.7. *Sejam G um grupo e $Z(G)$ seu centro. Se $G/Z(G)$ é cíclico, então G é grupo abeliano.*

Demonstração. Sabemos que $G/Z(G) = \langle gZ(G)\rangle$ para algum $g \in G$. Logo, dados $a, b \in G$, $aZ(G) = g^iZ(G)$ e $bZ(G) = g^kZ(G)$, para alguns $i, k \in \mathbb{N}$. Assim, $a = g^ih_1$ e $b = g^kh_2$, onde $h_1, h_2 \in Z(G)$. Dessa forma,

$$\begin{aligned} ab &= g^ih_1g^kh_2 \\ &= g^ig^kh_1h_2 \quad (\text{pois } h_1 \in Z(G)) \\ &= g^kg^ih_2h_1 \\ &= g^kh_2g^ih_1 \quad (\text{pois } h_2 \in Z(G)) \\ &= ba. \end{aligned}$$

□

Dados um grupo G e dois elementos $x, y \in G$, dizemos que xyx^{-1} é um *conjugado* de y. Se $y \in Z(G)$, então claramente $xyx^{-1} = y$ para todo $x \in G$, ou seja, o conjunto de conjugados de y é unitário, $\{y\}$. Se $y \notin Z(G)$, então o conjunto de conjugados de y possui mais elementos, e estaremos interessados no caso em que este conjunto é finito. Os elementos que possuem um número finito de conjugados formam um subgrupo, chamado FC-subgrupo (Finite Conjugate Subgroup):

Definição 1.1.8. Dado um grupo G, definimos o *FC-subgrupo* ϕ como sendo

$$\phi = \phi(G) = \{g \in G : g \text{ possui um número finito de conjugados}\}.$$

Além dos elementos que possuem uma quantidade finita de conjugados, outra classe de elementos que possui grande importância em nosso contexto são os p-elementos e os p'-elementos:

Definição 1.1.9. Seja p um número natural primo. Um elemento $x \in G$ é dito *p-elemento* se $|x| = p^k$ para algum $k \in \mathbb{N}$, e $y \in G$ é dito um *p'-elemento* se $p \nmid |y|$. Um grupo G é dito um *p-grupo* (respectivamente *p'-grupo*) quando todos os seus elementos são p-elementos (resp.

p'-elementos). Denotaremos por P o conjunto dos p-elementos de um grupo G, e Q aos p'-elementos de G, para um dado primo p. Em geral, tais subconjuntos não são subgrupos de G.

Definição 1.1.10. Um grupo G é dito *p-abeliano* se o seu subgrupo comutador G' é finito e p-grupo.

Exemplo 1.1.11. Seja A_4 o subgrupo das permutações pares de S_4, ou seja,

$$A_4 = \{1, (123), (124), (134), (132), (142), (143),$$
$$(234), (243), (12)(34), (13)(24), (14)(23)\}.$$

Assim, A_4 não é um 2-grupo, mas é 2-abeliano, uma vez que

$$A_4' = \{1, (12)(34), (13)(24), (14)(23)\}.$$

Com as construções acima, definimos ainda o seguinte subgrupo de um grupo G:

$$\phi_p(G) = \langle \phi \cap P \rangle.$$

Passemos agora a outra característica notável para os grupos. Em um grupo G, um subgrupo H finitamente gerado em geral não é finito. Por exemplo, $\langle 1 \rangle \leq \mathbb{Q}$ é infinito, enquanto $\langle \frac{1}{3}\mathbb{Z} \rangle \leq \frac{\mathbb{Q}}{\mathbb{Z}}$ é finito. Em nosso estudo, por vezes será importante que subgrupos finitamente gerados sejam finitos. Isto nos motiva à seguinte definição.

Definição 1.1.12. Um grupo G é dito *localmente finito* se todo subgrupo finitamente gerado de G é finito.

Lema 1.1.13. *Sejam G grupo de torção, ϕ o FC-subgrupo de G. Se $[G : \phi] < \infty$ e $|\phi'| < \infty$, então G é localmente finito.*

Demonstração. Tomemos H subgrupo de G finitamente gerado. Como $[G : \phi] < \infty$, então $[\phi H : \phi] < \infty$. Mas $\frac{\phi H}{\phi} \cong \frac{H}{\phi \cap H}$, ou seja, $[H : \phi \cap H] < \infty$.

Observemos que:

$$\frac{\phi \cap H}{\phi' \cap H} = \frac{\phi \cap H}{\phi' \cap (\phi \cap H)} \cong \frac{\phi'(\phi \cap H)}{\phi'} = \frac{\phi \cap \phi' H}{\phi'} < \frac{\phi}{\phi'}$$

que é um grupo abeliano. Logo, $\frac{\phi \cap H}{\phi' \cap H}$ é um grupo finitamente gerado, abeliano e de torção, e portanto finito, ou seja, $[\phi \cap H : \phi' \cap H] < \infty$.

Por último, observemos que, como $|\phi'| < \infty$, então $|\phi' \cap H| < \infty$. Utilizando o Teorema de

Lagrange, e juntando as informações acima, temos que

$$|H| = \underbrace{[H : \phi \cap H]}_{<\infty}\underbrace{[\phi \cap H : \phi' \cap H]}_{<\infty}\underbrace{|\phi' \cap H|}_{<\infty} < \infty.$$

□

Por fim, ao lidarmos com grupos quocientes, um subconjunto será de grande utilidade. Dado um grupo G e $H \lhd G$, definimos a *transversal* de H em G como sendo um subconjunto S tal que cada classe lateral à esquerda de H contém exatamente um elemento de S. Dessa forma, S possui $[G : H]$ elementos.

1.2 Grupos Livres e o Argumento de Magnus

Dado um conjunto de símbolos X, vamos construir um grupo F que seja "livre" em um certo sentido no conjunto X. Se $X = \varnothing$, então F é o grupo trivial $F = \{e\}$. Se $X \neq \varnothing$, seja X^{-1} um conjunto disjunto de X tal que $|X| = |X^{-1}|$. Escolha uma bijeção $X \to X^{-1}$ e denote a imagem de $x \in X$ por x^{-1}. Escolha também um conjunto disjunto de $X \cup X^{-1}$ que tenha exatamente um elemento, e denote-o por 1. Uma *palavra* é uma sequência finita $a_1 a_2 \dots a_n$ tal que $a_i \in X \cup X^{-1} \cup \{1\}$. A palavra 1 é chamada palavra vazia. Informalmente, o grupo que definiremos será livre no conjunto X pois não haverá relação existente entre as palavras, além das relações triviais entre os símbolos.

Uma palavra $a_1 a_2 \dots a_n$, diferente da palavra vazia, é dita reduzida quando:

- Se $a_i = x$ então $a_{i+1} \neq x^{-1}$ e se $a_i = x^{-1}$, então $a_{i+1} \neq x$ para todo $i = 1, 2, \dots, n-1$.
- $a_i \neq 1$ para todo $i = 1, 2, \dots, n$.

A palavra vazia é considerada reduzida. Assim, podemos escrever uma palavra reduzida não vazia em geral como $a_1^{\lambda_1} \dots a_m^{\lambda_m}$, onde $a_i \in X$ e $\lambda_i \in \{\pm 1\}$.

Chamamos de $F = F(X)$ ao conjunto de todas as palavras reduzidas construídas acima.

Definimos agora uma operação binária de justaposição no conjunto F. A palavra vazia 1 agirá como elemento neutro, ou seja, $1 \cdot w = w \cdot 1 = w$ para toda palavra $w \in F$, e dadas duas palavras reduzidas não vazias $a_1^{\lambda_1} \dots a_m^{\lambda_m}$, $b_1^{\gamma_1} \dots b_s^{\gamma_s}$, seu produto será a justaposição reduzida das duas palavras, ou seja,

$$(a_1^{\lambda_1} \dots a_m^{\lambda_m}) \cdot (b_1^{\gamma_1} \dots b_s^{\gamma_s}) = a_1^{\lambda_1} \dots a_m^{\lambda_m} b_1^{\gamma_1} \dots b_s^{\gamma_s}$$

com os possíveis cancelamentos de termos adjacentes, até obtermos uma palavra reduzida.

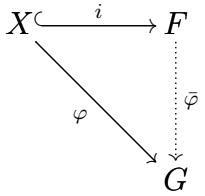
Por exemplo, $(a_3 a_5^{-1} a_6 a_2^{-1})(a_2 a_6^{-1} a_7) = a_3 a_5^{-1} a_7$.

Definição 1.2.1. Com a operação de justaposição definida acima, F é um grupo, chamado *grupo livre* em X.

O conjunto X é chamado *base* de F, e a cardinalidade de X, $|X|$, o *posto* de F.

Exemplo 1.2.2. O grupo abeliano $\mathbb{Z}$ é grupo livre com base $\{1\}$. Observemos que a palavra vazia neste caso é denotada por 0.

Formalmente, F ser um grupo *livre* sobre X significa que F satisfaz a seguinte propriedade: Dados um grupo G e uma função $\varphi : X \to G$, existe um único homomorfismo de grupos $\bar{\varphi} : F \to G$ tal que o seguinte diagrama é comutativo.



onde $i : X \to F$ é a inclusão natural.

A propriedade enunciada acima é chamada de Propriedade Universal do grupo F sobre X.

Agora, definidos o grupo livre e sua propriedade universal, nosso interesse passa a ser descobrir se, dado um subconjunto X de um grupo G qualquer, o subgrupo gerado por X é livre em G. Neste sentido, existe o Argumento de Magnus, devido a Wilhelm Magnus, proveniente da Teoria Combinatória de Grupos:

Teorema 1.2.3 (Argumento de Magnus)**.** *Seja X um subconjunto de um grupo G tal que $X \cap X^{-1} = \varnothing$. Então X é uma base de um subgrupo livre de G se e só se nenhum produto $w = x_1 \dots x_n$ é trivial, onde $n \geq 1$, $x_i \in X^{\pm 1}$ para todo $i = 1, \dots, n$ e $x_i x_{i+1} \neq 1$ para todo $i = 1, \dots, n-1$.*

Demonstração. [15, Proposição I.1.9]. □

1.3 Anéis e Ideais Nilpotentes

Os anéis são uma estrutura fundamental no estudo de álgebra. A presente seção se concentra em enunciar algumas classes particulares de anéis, assim como algumas de suas propriedades. Tal como anteriormente, assumimos que o leitor conheça os princípios básicos da Teoria de Anéis, e recomendamos [8] para possíveis esclarecimentos.

Observemos que, a menos que seja mencionado antecipadamente, todos os anéis considerados neste trabalho possuem identidade 1. Assim, podemos estudar os elementos do anel que são invertíveis em relação à multiplicação. Vamos chamar tais elementos de *unidades*. Ainda, em um anel R, o conjunto das unidades, $U(R)$ forma um grupo com relação à multiplicação.

Definição 1.3.1. A *característica* de um anel R é o menor inteiro n tal que $nx = 0$ para todo $x \in R$. Se tal inteiro n não existe, dizemos que a característica do anel é 0. Denotamos a característica de R por $char(R)$

Exemplo 1.3.2. $char(\mathbb{Z}_5) = 5$ e $char(\mathbb{Z}) = char(\mathbb{Q}) = char(\mathbb{R}) = 0$.

Exemplo 1.3.3. Para $n \in \mathbb{N}$, o anel de polinômios $\mathbb{Z}_n[x]$, ou seja, os polinômios na variável x com coeficientes em $\mathbb{Z}_n$ é um exemplo de anel infinito com característica não nula, pois $char(\mathbb{Z}_n[x]) = n$.

Com o exemplo anterior, vemos que dado $n \in \mathbb{N}$ qualquer, existe um anel com tal característica. Isto não acontece nos corpos, e esta é uma observação que utilizaremos muitas vezes durante o texto sem citá-la.

Proposição 1.3.4. *Dado um corpo $\mathbb{F}$, se $char(\mathbb{F}) \neq 0$, então $char(\mathbb{F})$ é um número primo.*

Demonstração. Suponhamos, por absurdo, que $char(\mathbb{F}) = p$ não é primo, ou seja, é um número composto, e tomemos q um divisor de p, com $q < p$ primo. Dessa forma, $p = qk$, para algum $k \in \mathbb{N}$, $k < p$, e assim

$$0 = \underbrace{1 + 1 + \cdots + 1}_{p \text{ vezes}} = (\underbrace{1 + 1 + \cdots + 1}_{q \text{ vezes}})(\underbrace{1 + 1 + \cdots + 1}_{k \text{ vezes}}).$$

Mas como $\mathbb{F}$ é corpo, temos de ter $(\underbrace{1 + 1 + \cdots + 1}_{q \text{ vezes}}) = 0$ ou $(\underbrace{1 + 1 + \cdots + 1}_{k \text{ vezes}}) = 0$, e assim, supondo sem perda de generalidade que $(\underbrace{1 + 1 + \cdots + 1}_{q \text{ vezes}}) = 0$, se $x \in \mathbb{F}$, então $(\underbrace{x + x + \cdots + x}_{q \text{ vezes}}) = x(\underbrace{1 + 1 + \cdots + 1}_{q \text{ vezes}}) = x.0 = 0$. Logo, $char(\mathbb{F}) = q$, absurdo. □

Neste trabalho, um ideal, a menos que seja dito antecipadamente, será sempre bilateral. Relembremos agora que, dados dois ideais I e J de R, o seu produto, IJ, é o subgrupo aditivo gerado pelo conjunto $\{uv : u \in I, v \in J\}$ e é ideal. Vamos enunciar agora duas classes de ideais com "más" propriedades:

Definição 1.3.5. Um ideal I de um anel R é dito *nilpotente* se existe $n \in \mathbb{N}$ tal que $I^n = 0$, em particular, $u_1u_2 \ldots u_n = 0$ para todo $u_i \in I$.

Definição 1.3.6. Um elemento $a \in R$ é dito *nilpotente* se existe $n \in \mathbb{N}$ tal que $a^n = 0$.

Definição 1.3.7. Um ideal I de um anel R é dito *nil* se todo elemento de I é nilpotente.

Dizemos que um ideal I de R é nil de *expoente limitado* se existe $k \in \mathbb{N}$ tal que $a^k = 0$ $\forall a \in I$.

Vale observar que todo ideal nilpotente em particular é nil. Para ilustrar as definições acima, vejamos alguns exemplos:

Exemplo 1.3.8. No anel $\mathbb{Z}_{p^m}$, p primo, o ideal $p\mathbb{Z}_{p^m}$ é nilpotente, pois $(p\mathbb{Z}_{p^m})^m = 0$.

Exemplo 1.3.9. Seja $R = T_n(\mathbb{F})$ o anel das matrizes $n \times n$ triangulares superiores sobre um corpo $\mathbb{F}$. Tomemos N o ideal das matrizes $n \times n$ estritamente triangulares superiores, ou seja, cuja diagonal principal também é nula. Assim, N é ideal nilpotente de R, com $N^n = 0$.

O próximo exemplo mostra que nem todo ideal nil é nilpotente.

Exemplo 1.3.10. Seja R o anel das matrizes de ordem infinita $\mathbb{N} \times \mathbb{N}$ sobre um corpo $\mathbb{F}$ que são triangulares superiores e com apenas uma quantidade finita de entradas não nulas. Como no caso acima, tomemos N o ideal das matrizes estritamente triangulares superiores. Então N é nil, pois, dada uma matriz $M \in N$, como M possui uma quantidade finita de entradas não nulas,

$$M = \begin{bmatrix} M^*_{k\times k} & 0 & \dots \\ 0 & 0 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix}_{\mathbb{N}\times\mathbb{N}}$$

onde $M^*_{k\times k}$ é uma matriz estritamente triangular superior, para algum $k \in \mathbb{N}$. Logo, pelo exemplo anterior, sabemos que $(M^*)^k = 0$, assim, $M^k = 0$. Portanto, N é nil. Mas N não é nilpotente, pois, dado $n \in \mathbb{N}$, existe uma matriz $S \in N$,

$$S = \begin{bmatrix} S^* & 0 & \dots \\ 0 & 0 & \dots \\ \vdots & \vdots & \ddots \end{bmatrix}_{\mathbb{N}\times\mathbb{N}}, \qquad S^* = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix}_{n+1\times n+1}.$$

e $S^n \neq 0$, pois $(S^*)^n \neq 0$.

Com as definições acima, podemos mostrar que a classe dos ideais nilpotentes é fechada para a soma finita.

Lema 1.3.11. *A soma de dois ideais nilpotentes é um ideal nilpotente.*

Demonstração. Sejam I, J ideais de R tal que $I^n = J^m = 0$. Afirmamos que $(I + J)^{n+m-1} = 0$. Para mostrar esta afirmação, basta-nos mostrar que o produto de $n + m - 1$ elementos da forma $u + v$, com $u \in I$, $v \in J$ é 0. Tal produto pode ser escrito como uma soma de produtos $w = w_1 w_2 \dots w_{n+m-1}$ onde cada $w_i \in I \cup J$. Se ao menos n desses w_i's estão em I, como I é ideal e $I^n = 0$, temos $w = 0$. Se o número de w_i's em I é menor do que n, existem ao menos m w_i's em J, e como $J^m = 0$, $w = 0$. Portanto, o produto será 0, e $I + J$ é nilpotente. □

Dessa forma, vemos que a soma finita de ideais nilpotentes é também um ideal nilpotente. O mesmo não pode ser dito para uma soma qualquer de ideais nilpotentes.

A fim de relacionar ideais nilpotentes e ideais nil de expoente limitado, temos o seguinte resultado, devido a Israel Nathan Herstein e Jacob Levitzki.

Lema 1.3.12. *Seja R um anel. Se R possui um ideal à esquerda (ou direita) nil de expoente limitado, então R possui um ideal nilpotente não nulo.*

Demonstração. Seja I um ideal nil à esquerda (o caso à direita é análogo), de expoente limitado $n \geq 2$. Escolha $a \in I$ com $a^{n-1} \neq 0$. Fixemos qualquer $r \in R$, e seja $s = ra^{n-1}$. Então $sa = ra^n = 0$. Ainda, como I é ideal, $s \in I$, logo $s^n = 0$. Agora, como $s + a \in I$, temos que $(s + a)^n = 0$. Expandindo esta expressão e excluindo os termos envolvendo sa, assim como os termos s^n e a^n, teremos

$$\sum_{i=1}^{n-1} a^{n-i}s^i = 0.$$

Mas observemos que, para todo $i \in \{2, 3, \ldots, n-1\}$, temos que $a^{n-i}s^i = (a^{n-i}s^{i-2}r)a^{n-1}s \in aRa^{n-1}s$. Logo,

$$0 = \sum_{i=1}^{n-1} a^{n-i}s^i = a^{n-1}s + ar'a^{n-1}s = (1 + ar')a^{n-1}s$$

para algum $r' \in R$. Mas $(ar')^{n+1} = a(r'a)^n r' = 0$, pois $r'a \in I$. Assim, ar' é nilpotente, e $1 + ar'$ é uma unidade. Logo, $0 = a^{n-1}s = a^{n-1}ra^{n-1}$ para todo $r \in R$. Segue então que o ideal $(Ra^{n-1}R)$ é não nulo e nilpotente de grau 2. □

1.4 Anéis Primos, Semiprimos e Artinianos

Nesta seção, definimos outras classes importantes de anéis, nomeadamente os anéis primos, semiprimos e artinianos. Tais conceitos foram fundamentais, por exemplo, para a Teoria de Wedderburn, desenvolvida no início do século XX, por Joseph Wedderburn.

Lema 1.4.1. *Seja R um anel, não necessariamente com unidade 1. As condições seguintes são equivalentes:*

a) Para todos $a, b \in R$, se $aRb = 0$, então $a = 0$ ou $b = 0$.

b) Para todos os ideais à esquerda I e J de R, se $IJ = 0$, então $I = 0$ ou $J = 0$.

c) Para todos os ideais à direita I e J de R, se $IJ = 0$, então $I = 0$ ou $J = 0$.

d) Para todos os ideais I e J de R, se $IJ = 0$, então $I = 0$ ou $J = 0$.

Demonstração. $a) \Rightarrow b)$ Se I e J são ideais à esquerda de R satisfazendo $IJ = 0$, então $IRJ = 0$, pois $RJ \subset J$. Logo, por (a), vemos que $I = 0$ ou $J = 0$.

$a) \Rightarrow c)$ Análogo ao anterior.

$b) \Rightarrow d)$ e $c) \Rightarrow d)$ são claros.

$d) \Rightarrow a)$ Sejam $a, b \in R$ tal que $aRb = 0$. Assim, o produto dos ideais RaR e RbR é 0. Assim, um dos dois tem de ser 0, suponhamos que seja $RaR = 0$. Com isso, temos que aR e Ra se tornam ideais bilaterais tais que $R \cdot aR = Ra \cdot R = 0$. Por (d), devemos ter $Ra = aR = 0$. Mas assim $\mathbb{Z}a$ é um ideal de R satisfazendo $\mathbb{Z}a \cdot R = 0$, ou seja, $\mathbb{Z}a = 0$, e assim, $a = 0$. □

Definição 1.4.2. Um anel R é dito *primo* se satisfaz alguma das condições do Lema 1.4.1.

Definimos agora uma classe de anéis um pouco mais geral:

Lema 1.4.3. *Seja R um anel. As condições seguintes são equivalentes:*

a) Para todo $a \in R$, $aRa = 0$ implica $a = 0$.

b) Para todos os ideais à esquerda I de R, $I^2 = 0$ implica $I = 0$.

c) Para todos os ideais à direita I de R, $I^2 = 0$ implica $I = 0$.

d) Para todos os ideais I de R, $I^2 = 0$ implica $I = 0$.

e) R não possui ideais não nulos nilpotentes.

Demonstração. $a) \Rightarrow b)$ Seja I ideal à esquerda de R tal que $I^2 = 0$. Tomemos $a \in I$. Como I é ideal à esquerda, $Ra \subset I$. Logo, $a(Ra) \subset I(I) = I^2 = 0$. Logo, $aRa = 0$, e assim, $a = 0$, ou seja, $I = 0$.

$a) \Rightarrow c)$ e $a) \Rightarrow d)$ são análogos ao caso anterior.

$d) \Rightarrow a)$ Seja $a \in R$ tal que $aRa = 0$. Assim, tomando o ideal RaR de R, vemos que $RaRRaR = 0$, mas assim, por $d)$, $RaR = 0$. Logo, Ra e aR se tornam ideais bilaterais, e em particular, $RaRa = 0$, ou seja, $Ra = 0$. Como $\mathbb{Z}a$ é um ideal de Ra satisfazendo $\mathbb{Z}a\mathbb{Z}a = 0$, vemos que $a = 0$.

$b) \Rightarrow d)$ e $c) \Rightarrow d)$ são claros.

Dessa forma, $a) - d)$ são equivalentes.

$d) \Rightarrow e)$ Seja I um ideal de R tal que $I^n = 0$. Assim, $(I^{n-1})^2 = 0$, e por $d)$, $I^{n-1} = 0$. Repetindo este processo um número finito de vezes, temos que $I = 0$.

$e) \Rightarrow d)$ Claro. □

Definição 1.4.4. Um anel R é dito *semiprimo* se satisfaz alguma das condições do Lema 1.4.3.

Vejamos dois exemplos das estruturas definidas acima.

Exemplo 1.4.5. O anel $\mathbb{M}_n(\mathbb{Z})$, com $n \geq 1$ é primo.

Exemplo 1.4.6. Todo anel comutativo que possui divisores de zero mas não possui elementos nilpotentes não nulos, é semiprimo e não primo. Um exemplo concreto é o anel das funções contínuas $C[a, b]$.

Estudaremos agora as condições de cadeia ascendentes e descendentes em anéis, tópico que possui papel central na teoria de anéis comutativos. Os anéis que satisfazem tais cadeias são chamados de anéis artinianos (para a cadeia descendente) e anéis noetherinos (para a cadeia ascendente), devidos a Emil Artin e Emmy Noether. Em nosso trabalho, utilizaremos apenas o conceito de anel artiniano, e assim, o leitor interessado em uma referência completa pode consultar [8].

Definição 1.4.7. Um anel R é dito *artiniano à esquerda* [respec. à direita], se satisfaz a condição de cadeia descendente em ideais à esquerda [respec. à direita], ou seja, para toda cadeia descendente de ideais à esquerda $B_1 \supset B_2 \supset B_3 \supset \ldots$, existe $m \in \mathbb{N}$ tal que $B_i = B_m$ para todo $i \geq m$. Um anel R é dito *artiniano* se for artiniano à esquerda e à direita.

Quando existe $m \in \mathbb{N}$ tal que $B_i = B_m$ para todo $i \geq m$ em uma cadeia descendente $B_1 \supset B_2 \supset B_3 \supset \ldots$, dizemos que a cadeia estabiliza.

Exemplo 1.4.8. Todo anel de divisão D é artiniano, uma vez que seus únicos ideais são 0 e D.

Exemplo 1.4.9. O anel $\mathbb{Z}$ não é artiniano, pois a cadeia descendente $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \ldots$ não estabiliza.

1.5 Álgebras

Nesta seção, faremos uma breve introdução às álgebras, fixando algumas notações e ilustrando alguns exemplos. A principal classe de álgebras a ser estudada neste trabalho serão as álgebras de grupo, objeto de estudo de uma seção posterior.

Definição 1.5.1. Um espaço vetorial A sobre um corpo $\mathbb{F}$ é uma *álgebra* sobre $\mathbb{F}$, ou uma $\mathbb{F}$-álgebra, se é munido de uma multiplicação associativa $A \times A \to A$, $(x, y) \mapsto xy$ tal que

1. $(\lambda x + \gamma y)z = \lambda(xz) + \gamma(yz)$.
2. $x(\lambda y + \gamma z) = \lambda(xy) + \gamma(xz)$.

para todo $\lambda, \gamma \in \mathbb{F}$, $x, y, z \in A$.

Dessa forma, vemos que as álgebras são espaços vetoriais que também possuem estrutura de anel. Assim, podemos utilizar aqui as teorias desenvolvidas para ambas as estruturas.

Se, para todo $a, b \in A$, $ab = ba$, dizemos que A é uma álgebra comutativa. Se A possui o elemento neutro para a multiplicação, 1, dizemos que A é álgebra unitária. A menos que se diga antecipadamente, todas as álgebras consideradas daqui em diante serão unitárias. Vejamos alguns exemplos:

Exemplo 1.5.2. O espaço das matrizes $\mathbb{M}_n(\mathbb{F})$ com a soma e multiplicação usuais é uma $\mathbb{F}$-álgebra unitária, mas não comutativa. Uma base para esta álgebra é o conjunto $B = \{e_{ij} : 1 \leq i, j \leq n\}$, onde e_{ij} possui 1 na entrada (i, j) e 0 nas restantes.

Exemplo 1.5.3. Seja V um $\mathbb{F}$-espaço vetorial e $End_{\mathbb{F}}(V) = \{T : V \to V : T \text{ é } \mathbb{F}\text{-linear}\}$. Defina

$$\begin{array}{rccc} \varphi: & End_{\mathbb{F}}(V) \times End_{\mathbb{F}}(V) & \to & End_{\mathbb{F}}(V) \\ & (S, T) & \mapsto & S \circ T \end{array}$$

composição de funções. Assim, $End_{\mathbb{F}}(V)$ é uma $\mathbb{F}$-álgebra, unitária e não comutativa.

Exemplo 1.5.4. O conjunto $\mathbb{F}[x]$ dos polinômios na variável x com coeficientes em $\mathbb{F}$ é uma $\mathbb{F}$-álgebra com a multiplicação usual. Uma base para $\mathbb{F}[x]$ é

$$B = \{1, x, x^2, x^3, \dots\}.$$

Mais geralmente, se $X = \{x_1, \dots, x_n\}$, o conjunto $\mathbb{F}[X]$ dos polinômios em várias variáveis é uma $\mathbb{F}$-álgebra.

O próximo exemplo é um pouco mais exótico, e com ele, temos o objetivo de ilustrar o quão rica é a classe das álgebras.

Exemplo 1.5.5. Seja P um conjunto finito parcialmente ordenado por $\leq$. Tomemos $I(P,\mathbb{F}) = \{f : P \times P \to \mathbb{F} : f(x,y) = 0 \text{ sempre que } x \not\leq y\}$. Este conjunto tem estrutura de espaço vetorial sobre $\mathbb{F}$. Defina agora $\varphi : I(P,\mathbb{F}) \times I(P,\mathbb{F}) \to I(P,\mathbb{F})$, $(f,g) \mapsto fg$, onde

$$fg(x,y) = \sum_{x \leq z \leq y} f(x,z)g(z,y).$$

Com a multiplicação definida acima, $I(P,\mathbb{F})$ se torna uma $\mathbb{F}$-álgebra unitária.

Como as álgebras são, em particular, anéis, podemos definir os ideais de uma álgebra, mas precisamos fazer um pequeno ajuste. Dizemos que I é um ideal de uma álgebra A se I é ideal no sentido da teoria de anéis, e ainda é um subespaço vetorial de A.

Um homomorfismo entre álgebras é uma transformação linear que também é um homomorfismo de anéis.

Neste trabalho, em geral serão consideradas álgebras não comutativas, e por isso, o comutador aditivo entre dois elementos quaisquer será uma ferramenta notável. Denotaremos o comutador entre dois elementos $a, b \in A$ por $[a,b] = ab - ba$.

Definição 1.5.6. Uma álgebra A é dita *semiprima* quando, olhada como anel, A é um anel semiprimo.

Um elemento α de uma $\mathbb{F}$-álgebra A é dito *algébrico* se existe um polinômio não nulo $f(x) \in \mathbb{F}[x]$ tal que $f(\alpha) = 0$. Para cada elemento algébrico α, seja I_α o conjunto dos polinômios em $\mathbb{F}[x]$ que anulam α. Afirmamos que este conjunto possui um único polinômio mônico de menor grau.

De fato, se houvessem dois polinômios mônicos f_1, f_2 de grau n minimais em I_α, como α é raiz de ambos, então $f_1 - f_2 \in I_\alpha$, e o grau de $f_1 - f_2$ é estritamente menor do que n, por ambos serem mônicos. Logo, temos de ter $f_1 - f_2 = 0$, ou seja, $f_1 = f_2$.

1.6 Radical de Jacobson

Nesta seção, temos o objetivo de enunciar uma ferramenta capaz de traduzir a complexidade da estrutura de uma álgebra dada. Em especial, com esta ferramenta em mãos, teremos

informações precisas a respeito das álgebras de dimensão finita.

Começaremos no contexto de anéis, definindo um ideal que contenha todos os elementos indesejáveis, no sentido de que estes elementos criam um obstáculo para entender a estrutura do anel. Quocientando o anel por este ideal, teremos um anel com boas propriedades. Para as álgebras de dimensão finita, este quociente se tornará um produto direto de álgebras de matrizes, estruturas que nos são mais familiares.

Boa parte desta teoria foi desenvolvida por Nathan Jacobson em torno de 1945. Para não carregar o texto, faremos uma breve exposição do assunto, não cobrindo a teoria de módulos necessária. Boas referências sobre o tema são [10] e [1].

Definição 1.6.1. Um ideal à esquerda M de um anel A, $M \neq A$, é dito *ideal maximal à esquerda* se, dado I ideal à esquerda de A e $M \subset I$, então $I = M$ ou $I = A$.

Analogamente, define-se ideal maximal à direita, e dizemos que M é *ideal maximal* se é ideal maximal à esquerda e à direita.

Exemplo 1.6.2. No anel dos inteiros $\mathbb{Z}$, os ideais $4\mathbb{Z}$ e $9\mathbb{Z}$ não são maximais, pois $4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$ e $9\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}$. Por outro lado, $2\mathbb{Z}$ e $3\mathbb{Z}$ são ideais maximais.

Se A é um anel não nulo, sempre existem ideais maximais à esquerda pelo Lema de Zorn. Assim, podemos definir:

Definição 1.6.3. Em um anel A, definimos o *radical de Jacobson*, denotado por $J(A)$ como sendo a interseção dos ideais maximais à esquerda de A.

Lema 1.6.4. *Dado um elemento a em um anel A, são equivalentes:*

a) $a \in J(A)$.

b) $1 - ba$ *é invertível à esquerda para todo* $b \in A$.

c) $aV = 0$ *para todo* A*-módulo simples à esquerda* V.

Demonstração. $a) \Rightarrow b)$ Seja $a \in J(A)$ e suponhamos que existe $b \in A$ tal que $1 - ba$ não é invertível à esquerda. Logo, o ideal à esquerda $I = A(1 - ba)$ satisfaz: $I \neq A$, pois $1 \notin I$ e I está contido em algum ideal maximal à esquerda M. Dessa forma, $(1 - ba) \in M$ e $a \in M$, logo, $1 \in M$, absurdo.

$b) \Rightarrow c)$ Suponhamos que exista $v \in V$ tal que $av \neq 0$. Como V é simples, $Aav = V$, e assim, $v = bav$ para algum $b \in A$. Dessa forma, $(1 - ba)v = 0$, mas por hipótese, $(1 - ba)$ é invertível à esquerda, logo, $v = 0$, absurdo.

$c) \Rightarrow a)$ Seja M um ideal maximal à esquerda de A. Assim, A/M é um A-módulo simples à esquerda, e portanto, por hipótese, $y(A/M) = 0$, ou seja, $y \in M$. Logo, $y \in J(A)$. □

Com a caracterização acima dos elementos de $J(A)$, temos o seguinte resultado:

Lema 1.6.5. *Todo ideal nil à direita ou à esquerda de A está contido em $J(A)$.*

Demonstração. Seja I ideal nil à esquerda de A (o caso à direita é análogo). Tomemos $a \in I$, e dado $b \in A$, $ba \in I$ é um elemento nilpotente. Dessa forma, $1 - ba$ é elemento invertível à esquerda. Portanto, pelo Lema 1.6.4, $a \in J(A)$. □

O Radical de Jacobson de um álgebra A é definido analogamente, como sendo a interseção de todos os ideais (de álgebra) maximais à esquerda de A.

Para as álgebras de dimensão finita, temos um único ideal nilpotente maximal, e assim, este é o radical de Jacobson $J(A)$.

A seguir compilamos algumas das principais propriedades satisfeitas pelo Radical de Jacobson.

Proposição 1.6.6. *Sejam $\mathbb{F}$ um corpo e G um grupo. Então, $J(\mathbb{F}G)$ possui as seguintes propriedades:*

1. *Se G é finito, então $J(\mathbb{F}G)$ é nilpotente, e $\mathbb{F}G/J(\mathbb{F}G)$ é uma soma direta de álgebras de matrizes sobre $\mathbb{F}$-álgebras de divisão.*

2. *Se G é finito e $\mathbb{F}$ é um corpo perfeito, então $\mathbb{F}G$ possui uma subálgebra isomorfa a*

$$\mathbb{F}G/J(\mathbb{F}G).$$

3. *Se $\mathbb{F}'$ é uma extensão de corpo de $\mathbb{F}$, então $J(\mathbb{F}'G) \cap \mathbb{F}G \subset J(\mathbb{F}G)$.*

4. *Se $\mathbb{F}'$ é uma extensão algébrica de corpo de $\mathbb{F}$, então $J(\mathbb{F}G) \subset J(\mathbb{F}'G)$.*

5. *Se H é um subgrupo de G, então $J(\mathbb{F}G) \cap \mathbb{F}H \subset J(\mathbb{F}H)$.*

6. *Se H é subgrupo normal de G de índice finito, então $J(\mathbb{F}H) \subset J(\mathbb{F}G)$.*

Demonstração. [11, Proposição 1.3.3].

□

A demonstração do próximo resultado pode ser encontrado em [9, pág. 43].

Lema 1.6.7. *Seja R um anel e suponha $R/J(R)$ artiniano, onde $J(R)$ é o radical de Jacobson de R. Se I é qualquer ideal de R, então a aplicação natural $U(R) \to U(R/I)$ é sobrejetora.*

1.7 Álgebras de Grupo

Os anéis e as álgebras de grupos são estruturas de grande interesse na matemática. Além das relações claras com as Teorias de Grupos e Anéis, elas também se relacionam fortemente

com a Teoria de Representações de Grupos, como foi estabelecido por Emmy Noether e Richard Brauer no início do século XX. Aqui, faremos uma exposição dos principais conceitos e resultados iniciais da teoria, e para uma exposição mais completa, o leitor pode consultar [16].

Dado um grupo G e um anel R, definimos o conjunto RG das somas formais da forma

$$\alpha = \sum_{g \in G} \alpha_g g$$

onde $\alpha_g \in R$, $\alpha_g = 0$ quase sempre, ou seja, apenas um número finito de coeficientes são diferentes de 0. Neste conjunto, podemos definir a soma e o produto dos elementos da seguinte forma:

$$(\sum_{g \in G} \alpha_g g) + (\sum_{g \in G} \beta_g g) = \sum_{g \in G} (\alpha_g + \beta_g) g$$

e, se $\alpha = \sum_{g \in G} \alpha_g g$, $\beta = \sum_{g \in G} \beta_g g$,

$$\alpha\beta = \sum_{g,h \in G} \alpha_g \beta_h gh.$$

Ainda, é possível definir um produto por elementos de R, nomeadamente

$$\lambda(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} (\lambda \alpha_g) g.$$

Definição 1.7.1. O conjunto RG, com as operações acima de soma e produto possui estrutura de anel, e é chamado *anel de grupo*. Caso R seja um corpo e com a operação de produto por elementos de R, RG possui estrutura de álgebra, e é chamada *álgebra de grupo*.

A construção acima não se restringe a grupos. De fato, construções análogas podem ser feitas para os casos em que G é um semigrupo ou um monóide. Em tais casos, dizemos que RG é um anel (álgebra) de semigrupo ou anel (álgebra) de monóide, respectivamente.

Para um elemento $\alpha \in RG$, definimos o suporte de α, denotado $supp(\alpha)$, como sendo o conjunto $supp(\alpha) = \{g \in G : \alpha_g \neq 0\}$. Pela definição de anel de grupo, temos que $supp(\alpha)$ é sempre finito.

Daqui em diante, o anel R será sempre um corpo, e denotaremos a álgebra de grupo por $\mathbb{F}G$. A fim de estudar a estrutura das álgebras de grupo, um ideal se sobrepõe por sua utilidade:

Definição 1.7.2. A aplicação $\phi : \mathbb{F}G \to \mathbb{F}$ dada por

$$\sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g$$

é um homomorfismo de anéis, chamado *homomorfismo de aumento* de $\mathbb{F}G$. Seu núcleo, denotado por $\Delta(G)$ é chamado *ideal de aumento* de $\mathbb{F}G$.

Exemplo 1.7.3. Sejam $G = \mathbb{Z}_2$ com notação multiplicativa, ou seja, $\mathbb{Z}_2 = \{1, g\}$ e $R = \mathbb{R}$ o corpo dos números reais. Assim, construímos a álgebra de grupo $\mathbb{R}\mathbb{Z}_2$ formada pelos seguintes elementos

$$\alpha = \lambda_1 1 + \lambda_2 g$$

onde $\lambda_1, \lambda_2 \in \mathbb{R}$. Seu ideal de aumento é:

$$\Delta(\mathbb{Z}_2) = \{\lambda 1 - \lambda g : \lambda \in \mathbb{R}\}.$$

O próximo resultado, demonstrado por Heinrich Maschke no início do século XX, originalmente da Teoria de Representações de Grupos e posteriormente traduzido para as Álgebras de Grupo, caracteriza as álgebras de grupos semiprimas para grupos finitos.

Teorema 1.7.4 (Maschke)**.** *Seja G um grupo finito. Então a álgebra de grupo $\mathbb{F}G$ é semiprima se, e somente se, $char(\mathbb{F}) = 0$ ou $char(\mathbb{F}) = p$ primo que não divide $|G|$.*

Demonstração. Como $\mathbb{F}G$ é um espaço vetorial de dimensão finita sobre $\mathbb{F}$, podemos definir um funcional linear

$$\begin{array}{rccc} \varphi: & \mathbb{F}G & \to & \mathbb{F} \\ & a & \mapsto & tr(\varphi_a) \end{array}$$

onde $\varphi_a : \mathbb{F}G \to \mathbb{F}G$, com $\varphi_a(b) = ab$, e $tr(\varphi_a)$ denotando o traço da transformação linear.

Seja $n = |G|$ e denote seus elementos por $g_1, g_2, \ldots, g_n$ onde $g_1 = 1$. Assim, $\varphi(1) = n$. Se $i \geq 2$, então

$$\varphi_{g_i}(g_j) = g_i g_j \in G \backslash \{g_j\}$$

para todo j. Assim a matriz representante de φ_{g_i} com respeito a base $\{g_1, \ldots, g_n\}$ terá diagonal nula, consequentemente, $\varphi(g_i) = 0$.

Agora, suponhamos por absurdo que I seja um ideal nilpotente não nulo de $\mathbb{F}G$. Queremos mostrar que $\mathbb{F}$ tem característica p que divide $n = |G|$. Tome um elemento não nulo $a \in I$, e escreva $a = \sum_{i=1}^{n} \lambda_i g_i$. Sem perda de generalidade, podemos supor que $\lambda_1 \neq 0$. Então, temos

$$\varphi(a) = \lambda_1 \varphi(g_1) + \lambda_2 \varphi(g_2) + \cdots + \lambda_n \varphi(g_n) = n\lambda_1.$$

Como $a \in I$ e I é nilpotente, a é nilpotente. Dessa forma, φ_a é uma transformação linear nilpotente, e seu traço é 0, ou seja, $\varphi(a) = 0$. Logo, da equação acima, temos que $n\lambda_1 = 0$. Como $\lambda_1 \neq 0$, isso só é possível quando $p = char(\mathbb{F})$ divide n, absurdo.

Reciprocamente, vamos assumir, por absurdo, que $p = char(\mathbb{F})$ divide $|G|$. Seja $r = \sum_{i=1}^{n} g_i$. Como $rg_j = g_j r = r$ para todo j, vemos que o espaço unidimensional $\mathbb{F}r$ é um ideal de $\mathbb{F}G$. Porém, $r^2 = |G|r = 0$, e assim, $\mathbb{F}r$ é um ideal nilpotente, absurdo. □

Veremos agora uma generalização do conceito de ideal de aumento:

Definição 1.7.5. Dado um subgrupo normal $N \lhd G$, denotaremos por $\Delta(G,N)$ ao núcleo da aplicação natural $\varphi : \mathbb{F}G \to \mathbb{F}(G/N)$.

Com a definição acima, o próximo resultado é uma constatação técnica que utilizaremos mais a frente. Sendo $N = \{x_1, \ldots, x_k\}$ subgrupo finito de G, denotemos por $\bar{N} \in \mathbb{F}G$ à soma de seus elementos, ou seja, $\bar{N} = x_1 + \cdots + x_k$.

Lema 1.7.6. *Sejam $\mathbb{F}$ um corpo e G um grupo. Seja ainda $N \lhd G$ finito. Então, para $\alpha \in \mathbb{F}G$, $\alpha\bar{N} = 0 \Leftrightarrow \alpha \in \Delta(G,N)$.*

Demonstração. Seja X uma transversal de N em G. Podemos escrever

$$\alpha = \alpha_1 g_1 + \cdots + \alpha_n g_n$$

onde $\alpha_i \in \mathbb{F}N$ e $g_i \in X$. Não é difícil ver que $\bar{N}$ é central em $\mathbb{F}G$, logo,

$$\alpha\bar{N} = \alpha_1\bar{N}g_1 + \cdots + \alpha_n\bar{N}g_n.$$

Segue que $\alpha\bar{N} = 0 \Leftrightarrow \alpha_i\bar{N} = 0$ para cada i.

Sendo $\alpha_i = a_{i1}x_1 + \cdots + a_{ik}x_k$, com $a_{ij} \in \mathbb{F}$ e $x_j \in N$ então, $\alpha_i\bar{N} = (a_{i1} + \cdots + a_{ik})\bar{N}$, logo, $\alpha_i\bar{N} = 0 \Leftrightarrow \alpha_i \in \Delta(N)$.

Agora, sendo a aplicação natural $\varphi : \mathbb{F}G \to \mathbb{F}(G/N)$, então

$$\begin{aligned} \varphi(\alpha) &= (a_{11}x_1 + \cdots + a_{1k}x_k)g_1N + \cdots + (a_{n1}x_1 + \cdots + a_{nk}x_k)g_nN \\ &= (a_{11} + \cdots + a_{1k})g_1N + \cdots + (a_{n1} + \cdots + a_{nk})g_nN \end{aligned}$$

e assim, vemos que $\alpha_i \in \Delta(N) \Leftrightarrow \alpha \in \Delta(G,N)$. □

A demonstração do próximo resultado pode ser encontrada em [11, Lema 1.1.1].

Lema 1.7.7. *Sejam G um grupo e R um anel comutativo de característica p^m para algum p primo. Se N é subgrupo normal finito de G, então $\Delta(G,N)$ é um ideal nilpotente se e somente se N é um p-grupo.*

1.8 Polinômios Não Comutativos

Nesta seção, serão definidos os primeiros conceitos da Teoria das Álgebras com Identidades Polinomiais (PI-álgebras). Utilizamos como principal referência, o livro [1], que possui uma abordagem simples e atual da teoria, mas suficiente para o propósito deste texto. Começamos construindo a álgebra livre em um conjunto X, e destacamos que sua construção se assemelha à dos grupos livres.

Seja X um conjunto não vazio, $X = \{\xi_i | i \in I\}$. Uma sequência finita de elementos de X será denotada por $\xi_{i_1}\xi_{i_2}\dots\xi_{i_m}$ e chamada de *palavra*. A sequência vazia será denotada por 1 e chamada *palavra vazia*. Definimos uma multiplicação entre essas palavras por justaposição, ou seja,

$$(\xi_{i_1}\xi_{i_2}\dots\xi_{i_m})\cdot(\xi_{j_1}\xi_{j_2}\dots\xi_{j_n}) = \xi_{i_1}\xi_{i_2}\dots\xi_{i_m}\xi_{j_1}\xi_{j_2}\dots\xi_{j_n}.$$

Assim, o conjunto de todas as palavras se torna um monóide (com elemento neutro sendo a palavra vazia), que denotamos por X^*

Definição 1.8.1. Sejam $\mathbb{F}$ um corpo e X um conjunto. Definimos a *álgebra livre* em X sobre $\mathbb{F}$ como sendo a álgebra de monóide $\mathbb{F}X^*$, que denotaremos por $\mathbb{F}\langle X\rangle$.

Observação 1.8.2. Quando X for um conjunto finito, $X = \{\xi_1, \xi_2, \dots, \xi_n\}$, denotaremos $\mathbb{F}\langle X\rangle$ por $\mathbb{F}\langle\xi_1, \xi_2, \dots, \xi_n\rangle$. Os elementos de X são chamados de indeterminadas, e os de $\mathbb{F}\langle X\rangle$ são chamados polinômios não comutativos.

Um polinômio é dito um *monômio* se for um múltiplo escalar de uma palavra. Assim, todo polinômio não nulo $f \in \mathbb{F}\langle X\rangle$ é uma soma de monômios, mais precisamente, f pode ser escrita de forma única como $f = \lambda_1 w_1 + \cdots + \lambda_m w_m$, onde $w_1, \dots, w_m$ são duas a duas palavras distintas com coeficientes $\lambda_1, \dots, \lambda_m$ não nulos.

Definimos o comprimento de uma palavra não nula $w = \xi_{i_1}\xi_{i_2}\dots\xi_{i_m}$ por $l(w) = m$, e o comprimento da palavra vazia $l(1) = 0$. O *grau* de um polinômio não nulo $f = \lambda_1 w_1 + \cdots + \lambda_m w_m$ é definido como

$$deg(f) = max\{l(w_1), \dots, l(w_m)\}.$$

Alguns polinômios com propriedades especiais terão papel fundamental durante nosso estudo.

Definição 1.8.3. Um polinômio não nulo $f = \lambda_1 w_1 + \cdots + \lambda_m w_m$ é dito *homogêneo* se $l(w_1) = \cdots = l(w_m)$. Ainda, se além de ser homogêneo, cada indeterminada ξ_i aparece em cada monômio de f exatamente uma vez, dizemos que o polinômio é *multilinear*.

Exemplo 1.8.4. Em $\mathbb{F}\langle\xi_1, \xi_2\rangle$, $f = \xi_1^2\xi_2 - \xi_1\xi_2\xi_1 + \xi_2^3$ é um polinômio homogêneo de grau 3, mas não multilinear. Exemplos de polinômios multilineares serão vistos adiante.

Dentro dos polinômios multilineares, destacaremos uma classe especial de polinômios.

Definição 1.8.5. Um polinômio multilinear $f = f(\xi_1, \dots, \xi_n, \eta_1, \dots, \eta_r) \in \mathbb{F}\langle X\rangle$ é dito *alternante* em $\xi_1, \dots, \xi_n$ se f se anula ao substituir ξ_j por ξ_i, com $1 \leq i < j \leq n$.

Antes de passarmos a um exemplo de polinômio multilinear e alternante, façamos um resultado, que à primeira vista, parece simples, mas possui como uma de suas consequências o fato de que toda álgebra de dimensão finita é PI-álgebra.

Lema 1.8.6. *Sejam A uma $\mathbb{F}$-álgebra e $a_1, \ldots, a_n \in A$ elementos linearmente dependentes. Se um polinômio multilinear $f = f(\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_r) \in \mathbb{F}\langle X \rangle$ é alternante em $\xi_1, \ldots, \xi_n$, então $f(a_1, \ldots, a_n, x_1, \ldots, x_r) = 0$ para todo $x_1, \ldots, x_r \in A$.*

Demonstração. Podemos assumir que $a_n = \sum_{i=1}^{n-1} \lambda_i a_i$ com $\lambda_i \in \mathbb{F}$. Consequentemente,

$$f(a_1, \ldots, a_n, x_1, \ldots, x_r) = \sum_{i=1}^{n-1} f(a_1, \ldots, a_{n-1}, a_i, x_1, \ldots, x_r) = 0$$

pois f é alternante nas primeiras n coordenadas. □

Definição 1.8.7. Seja $n \geq 2$. O polinômio

$$s_n = s_n(\xi_1, \ldots, \xi_n) = \sum_{\sigma \in S_n} sgn(\sigma) \xi_{\sigma(1)} \ldots \xi_{\sigma(n)}$$

é chamado *polinômio standard* de grau n. Este é um polinômio multilinear e alternante.

Exemplo 1.8.8. $s_2 = \xi_1\xi_2 - \xi_2\xi_1$ é o polinômio standard de grau 2 e

$$s_3 = \xi_1\xi_2\xi_3 - \xi_2\xi_1\xi_3 - \xi_3\xi_2\xi_1 - \xi_1\xi_3\xi_2 + \xi_2\xi_3\xi_1 + \xi_3\xi_1\xi_2$$

o polinômio standard de grau 3.

Definição 1.8.9. Um polinômio $f = f(\xi_1, \ldots, \xi_n) \in \mathbb{F}\langle \xi_1, \xi_2, \ldots \rangle$ é dito uma *identidade polinomial* de uma $\mathbb{F}$-álgebra A se $f(x_1, \ldots, x_n) = 0$ para todo $x_1, \ldots, x_n \in A$. Se um polinômio não nulo f é uma identidade polinomial de A, então A é chamada *PI-álgebra*, e dizemos que A satisfaz f.

Exemplo 1.8.10. Toda álgebra A comutativa é uma PI-álgebra. De fato, A satisfaz o polinômio $f(\xi_1, \xi_2) = \xi_1\xi_2 - \xi_2\xi_1$.

Exemplo 1.8.11. Toda álgebra de dimensão finita A é PI-álgebra. De fato, sendo $n = dim(A)$, pelo Lema 1.8.6, A satisfaz qualquer polinômio alternante em $n+1$ variáveis. Em particular, A satisfaz s_{n+1}.

Veremos agora duas propriedades importantes das PI-álgebras. A primeira delas nos garante que homomorfismos de álgebras preservam identidades polinomiais, e será amplamente utilizada em nosso trabalho. A segunda nos diz que se A é uma PI-álgebra, é possível encontrar um polinômio multilinear que seja identidade polinomial de A.

Lema 1.8.12. *Seja $\phi : A \to B$ homomorfismo de álgebras. Se A satisfaz uma identidade polinomial, então $\phi(A)$ também satisfaz a mesma identidade.*

Demonstração. Seja $f(\xi_1, \ldots, \xi_n)$ a identidade satisfeita por A. Tomemos $\phi(x_1), \ldots, \phi(x_n) \in \phi(A)$ quaisquer. Então, como ϕ é homomorfismo,

$$f(\phi(x_1), \ldots, \phi(x_n)) = \phi(f(x_1, \ldots, x_n)) = \phi(0) = 0,$$

ou seja, $\phi(A)$ é uma PI-álgebra. □

Para o próximo resultado, definimos uma noção auxiliar. O *grau do polinômio f em ξ_i* é o número máximo de ocorrências de ξ_i nos monômios de f. Por exemplo, $f = \xi_2^3\xi_1\xi_2\xi_1^4 - \xi_2\xi_1 + \xi_1^2\xi_3\xi_2^2$ tem grau 5 em ξ_1, grau 4 em ξ_2 e grau 1 em ξ_3.

Teorema 1.8.13. *Se uma álgebra A satisfaz uma identidade polinomial não nula, então A também satisfaz uma identidade polinomial multilinear não nula de mesmo grau ou menor.*

Demonstração. Seja $f = f(\xi_1, \ldots, \xi_n)$ identidade polinomial não nula de A. Denotando por d_i o grau de f em ξ_i, a prova será por indução em $d = max\{d_1, \ldots, d_n\} > 0$.

Se $d = 1$, então cada variável aparece em cada monômio de f no máximo uma vez, mas não exatamente uma vez. Seja $\lambda\xi_1 \ldots \xi_m$ o monômio de menor grau. Assim, $g(\xi_1, \ldots, \xi_m) = f(\xi_1, \ldots, \xi_m, 0, \ldots, 0) = \lambda\xi_1 \ldots \xi_m$ é identidade polinomial multilinear de A, de grau menor ou igual ao grau de f.

Seja $d > 1$. Sem perda de generalidade, podemos supor que existe $k \leq n$ tal que $d_k = \cdots = d_n = d$ e $d_i < d$ para $i < k$. Vamos definir um polinômio $g = g(\xi_1, \ldots, \xi_n, \xi_{n+1})$ por

$$g = f(\xi_1, \ldots, \xi_{n-1}, \xi_n + \xi_{n+1}) - f(\xi_1, \ldots, \xi_n) - f(\xi_1, \ldots, \xi_{n-1}, \xi_{n+1}).$$

Notemos que g é identidade polinomial de A. Escrevendo $f = \sum \lambda_1 w_i$, então $g = \sum \lambda_i g_i$, onde os polinômios g_i são obtidos a partir das palavras w_i da mesma forma que g é obtida de f.

Se ξ_n não aparece em w_i, então $g_i = -w_i$. Se ξ_n aparece apenas uma vez em w_i, então $g_i = 0$. Se ξ_n ocorre mais de uma vez em w_i, então g_i é a soma de todas as possíveis palavras obtidas por trocar pelo menos uma, mas não todas as letras ξ_n por ξ_{n+1}. Como $d > 1$, os índices i em que ξ_n ocorre ao menos duas vezes em w_i existem. Logo, $g \neq 0$.

Portanto:

- g é identidade não nula de A.
- $deg(g) \leq deg(f)$.
- Para $j = 1, \ldots, n-1$, o grau de g em ξ_j é menor ou igual a d_j.
- O grau de g em ξ_n e ξ_{n+1} é $d - 1$.

Agora, repetimos esse processo, com g no lugar da f e ξ_{n-1} no lugar de ξ_n e continuamos até ξ_k. Assim, teremos uma identidade polinomial não nula em que o grau máximo é menor do que d, e por hipótese de indução, existe uma identidade polinomial multilinear. □

Antes de passarmos ao estudo das identidades de grupo, façamos uma breve introdução às identidades polinomiais generalizadas. Definimos um polinômio generalizado f sobre uma $\mathbb{F}$-álgebra A como sendo um polinômio onde elementos da álgebra são permitidos aparecerem como coeficientes dos monômios e entre as letras.

Por exemplo, sendo $a, b, c \in A$ elementos quaisquer, $f(\xi_1, \xi_2) = a\xi_2 c\xi_1 - 3\xi_1 b\xi_2$ é um polinômio generalizado sobre A.

Dizemos que A satisfaz uma identidade polinomial generalizada se existe $f(\xi_1, \ldots, \xi_n)$ polinômio generalizado *não degenerado* sobre A tal que $f(a_1, \ldots, a_n) = 0$ para todo $a_1, \ldots, a_n \in A$. Temos agora de definir o que significa um polinômio generalizado ser não degenerado. Por conveniência, definiremos apenas os polinômios multilineares.

Definição 1.8.14. Dizemos que f é um *polinômio generalizado multilinear não degenerado de grau* n se

$$f(\xi_1, \ldots, \xi_n) = \sum_{\sigma \in S_n} f^\sigma(\xi_1, \ldots, \xi_n)$$

onde

$$f^\sigma(\xi_1, \ldots, \xi_n) = \sum_{j=1}^{a_\sigma} \alpha_{0,\sigma,j} \xi_{\sigma(1)} \alpha_{1,\sigma,j} \xi_{\sigma(2)} \cdots \alpha_{n-1,\sigma,j} \xi_{\sigma(n)} \alpha_{n,\sigma,j}$$

com $\alpha_{i,\sigma,j} \in A$, a_σ inteiros positivos e para algum $\sigma \in S_n$, f^σ não é uma identidade polinomial generalizada para A. Denotaremos tais polinômios por GPI.

Passemos agora ao estudo das identidades de grupo de um grupo G. Sendo F o grupo livre das palavras com letras em $\{x_1, x_2, x_3, \ldots\}$, definimos:

Definição 1.8.15. Uma palavra não nula $w = x_{i_1}^{r_1} x_{i_2}^{r_2} \ldots x_{i_k}^{r_k} \in F$ é dita *identidade de grupo* do grupo G se $g_{i_1}^{r_1} g_{i_2}^{r_2} \ldots g_{i_k}^{r_k} = 1$ para todo $g_{i_j} \in G$. Neste caso, dizemos que G satisfaz $w = 1$.

Exemplo 1.8.16. Se G é um grupo abeliano, então G satisfaz $(x_1, x_2) = 1$.

Exemplo 1.8.17. Todo grupo G finito de ordem n satisfaz $x^n = 1$.

Assim como no caso das identidades polinomiais, as identidades de grupos também são preservadas por homomorfismos.

Lema 1.8.18. *Seja $\varphi : G \to H$ homomorfismo de grupos. Se G satisfaz $w = 1$, então $\varphi(G)$ também satisfaz.*

Demonstração. Análogo ao Lema 1.8.12. □

Lema 1.8.19. *Seja R anel. Se $U(R)$ satisfaz uma identidade de grupo $w = 1$, então $U(R)$ satisfaz uma identidade de grupo da seguinte forma:*

$$w_0(x, y) = x^{\alpha_1} y^{\beta_1} \ldots x^{\alpha_s} y^{\beta_s} = 1$$

onde α_i, β_j são inteiros não nulos determinados por w e $\alpha_1 < 0$, $\beta_s > 0$.

Demonstração. Se $w = w(x_1, \ldots, x_r)$, então trocando x_i por $x^{-i}yx^i$, temos uma identidade de grupo não trivial em duas variáveis x e y satisfeita por $U(R)$, nomeadamente

$$x^{\alpha_1}y^{\beta_1}\ldots x^{\alpha_s}y^{\beta_s}x^{\alpha_{s+1}} = 1$$

onde α_i e β_j são inteiros não nulos. Então, $U(R)$ satisfaz

$$x^{\alpha_1+\alpha_{s+1}}y^{\beta_1}\ldots x^{\alpha_s}y^{\beta_s} = 1.$$

Se $\alpha_1 + \alpha_{s+1} \neq 0$, então:

- Se $\alpha_1 + \alpha_{s+1} > 0$ e $\beta_s > 0$, trocamos x por x^{-1} e obtemos a identidade desejada.
- Se $\alpha_1 + \alpha_{s+1} > 0$ e $\beta_s < 0$, trocamos x por x^{-1} e y por y^{-1}, e assim obtemos a identidade desejada.
- Se $\alpha_1 + \alpha_{s+1} < 0$ e $\beta_s > 0$, já temos a identidade desejada.
- Se $\alpha_1 + \alpha_{s+1} < 0$ e $\beta_s < 0$, trocamos y por y^{-1} e obtemos a identidade desejada.

Se $\alpha_1 + \alpha_{s+1} = 0$, então temos

$$y^{\beta_1}x^{\alpha_2}\ldots x^{\alpha_s}y^{\beta_s} = 1.$$

Trocando o papel de x e y e repetindo o processo acima, teremos a identidade desejada ou uma simplificada da forma:

$$x^{\alpha_2}y^{\beta_2}\ldots y^{\beta_{s-1}}x^{\alpha_s} = 1.$$

Repetindo o processo finitas vezes, teremos o resultado, ou então chegaremos a uma identidade da forma $x^\alpha = 1$, com $\alpha \neq 0$. Se $\alpha > 0$, trocamos x por $x^{-1}y$, e assim $U(R)$ satisfaz $(x^{-1}y)^\alpha = 1$, que está na forma desejada. Se $\alpha < 0$, trocamos x por $y^{-1}x$, e assim $U(R)$ satisfaz $1 = (y^{-1}x)^\alpha = (x^{-1}y)^{-\alpha}$. □

CAPÍTULO 2

A Conjectura de Brian Hartley: Caso Infinito

Neste capítulo, temos o objetivo de estudar dois problemas. Sendo G um grupo de torção:

1. Conjectura de Brian Hartley Particular: Se $\mathbb{F}$ é corpo infinito e $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, então $\mathbb{F}G$ satisfaz uma identidade polinomial.

2. Se $\mathbb{F}$ é corpo infinito, quais são as condições necessárias e suficientes em um grupo G para que o grupo $U(\mathbb{F}G)$ satisfaça uma identidade de grupo?

A primeira seção será dedicada a estudar alguns resultados clássicos da teoria de álgebras de grupo. Na segunda seção, demonstraremos a Conjectura de Brian Hartley Particular, seguindo de perto [5], e a terceira seção se concentra no segundo problema aqui proposto.

Apesar dos artigos [12] e [13], publicados em 1999, cobrirem o caso particular em que o corpo $\mathbb{F}$ é infinito, optamos por trazer também as demonstrações feitas apenas para este caso, uma vez que o método utilizado envolve conceitos simples e elegantes, como a matriz de Vandermonde.

2.1 Resultados Clássicos sobre Álgebras de Grupo

Para estudar a Conjectura de Brian Hartley Particular, serão necessários alguns resultados auxiliares, assim como resultados clássicos da teoria de Álgebras de Grupo e Identidades Polinomiais. Dentre os resultados auxiliares necessários, dois se destacam. Mostraremos que em uma álgebra semiprima cujas unidades satisfazem uma identidade de grupo, seus idempotentes são centrais, e veremos condições na álgebra de grupo $\mathbb{F}G$ para que o grupo G seja p-abeliano.

Lema 2.1.1. *Sejam R um anel semiprimo e $S = \{a \in R : \forall b, c \in R, bc = 0 \Rightarrow bac = 0\}$. Se S contém todos os elementos nilpotentes de grau 2, então S contém todos os elementos nilpotentes de R.*

Demonstração. Faremos indução sobre o grau de nilpotência. Se $a \in R$ é nilpotente de grau 1, $a = 0$ está em S. Seja agora $a \in R$, $a^n = 0$, $a^{n-1} \neq 0$ e suponhamos por hipótese de indução que se $x \in R$, $x^m = 0$, $m < n$, então $x \in S$. Tomemos $b, c \in R$ tais que $bc = 0$ e $r \in R$. Então, como $(1 - a)$ é elemento invertível com inversa $(1 + a + \cdots + a^{n-1})$,

$$b(1-a)^{-1}(1-a)c = 0 \qquad \text{e} \qquad (crb)^2 = 0,$$

e assim, por hipótese,

$$\begin{aligned} 0 &= b(1-a)^{-1}crb(1-a)c \\ &= b(1+a+\cdots+a^{n-1})crb(1-a)c. \end{aligned}$$

Como $a^n = 0$, então $\exists m < n$ tal que $(a^2)^m = 0$, e assim, por hipótese de indução, $a^2 \in S$. Analogamente, $a^i \in S$, $i = 3, 4, \ldots, n-1$. Logo,

$$b(1+a+\cdots+a^{n-1})c = bac \qquad \text{e} \qquad b(1-a)c = -bac.$$

Assim,

$$\begin{aligned} 0 &= b(1+a+\cdots+a^{n-1})crb(1-a)c \\ &= -bacrbac \\ &= bacrbac \end{aligned}$$

para todo $r \in R$.

Como R é semiprimo, $bac = 0$ e portanto, $a \in S$. □

Lema 2.1.2. *Seja R um anel, e suponhamos que para todos $a, b, c \in R$, se $a^2 = bc = 0$, então $bac = 0$. Assim, todo idempotente de R é central.*

Demonstração. Sejam e um idempotente e $r \in R$ elemento qualquer. Façamos $a = er(1-e)$, $b = e$, e $c = 1 - e$, assim, $a^2 = bc = 0$. Logo,

$$0 = bac = e^2r(1-e)^2 = er(1-e),$$

ou seja, $er = ere$. Agora, tomando $a = (1-e)re$, $b = 1 - e$ e $c = e$, fazendo as mesmas contas acima, temos que $re = ere$. Portanto, $re = er$. □

Com os lemas acima, conseguimos o seguinte resultado, de grande utilidade em nosso trabalho.

Lema 2.1.3. *Seja A uma $\mathbb{F}$-álgebra semiprima. Se $U(A)$ satisfaz uma identidade de grupo, então todo idempotente de A é central.*

Demonstração. Tomemos $a, b, c \in A$ tal que $a^2 = bc = 0$. Pelo Lema 2.1.2, basta-nos mostrar que $bac = 0$. Suponhamos que $bac \neq 0$, então, por [4, Proposição 1], $bacA$ é ideal nil à direita de expoente limitado. Mas então, pelo Lema 1.3.12, A possui um ideal nilpotente não nulo, contradição, pois A é semiprima. Logo, $bac = 0$, e pelo Lema 2.1.2, segue o resultado. □

A demonstração do próximo resultado pode ser encontrada em [6, Lema 2.0]:

Lema 2.1.4. *Seja D um anel de divisão não comutativo de dimensão finita sobre seu centro. Então $U(D)$ contem um subgrupo livre de posto dois.*

Lema 2.1.5. *Sejam G um grupo finito não abeliano e $\mathbb{F}$ corpo infinito de característica $p > 0$. Se $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, então G é p-abeliano.*

Demonstração. Seja J o radical de Jacobson de $\mathbb{F}G$. Como G é finito, sabemos que J é nilpotente de grau k, para algum $k \in \mathbb{N}$, e o epimorfismo natural $\mathbb{F}G \to \mathbb{F}G/J$ induz um homomorfismo

$$U(\mathbb{F}G) \to U(\mathbb{F}G/J).$$

A aplicação acima é sobrejetora, pois, dado $\bar{u} \in U(\mathbb{F}G/J)$, existe $\bar{v} \in U(\mathbb{F}G/J)$ tal que $\bar{u}\bar{v} = \bar{v}\bar{u} = \bar{1} = 1 + J$, ou seja, $uv + J = vu + J = 1 + J$. Logo, existem $j_1, j_2 \in J$ tal que $uv = vu + j_1$ e $uv = 1 + j_2$ com $j_1^k = j_2^k = 0$.

Dessa forma, $vu = 1 + (j_2 - j_1)$, e sendo j_2 e $(j_2 - j_1)$ elementos nilpotentes, $(1 + j_2)$ e $(1 + (j_2 - j_1))$ são unidades, ou seja, uv e vu são unidades. Logo, u é unidade, e portanto, a aplicação é sobrejetora.

Agora, por hipótese, $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, e assim, pelo Lema 1.8.18, $U(\mathbb{F}G/J)$ também satisfaz. Pela Proposição 1.6.6, podemos escrever:

$$\frac{\mathbb{F}G}{J} = \oplus_i \mathbb{M}_{n_i}(D_i)$$

onde D_i são $\mathbb{F}$-álgebras de divisão e n_i são inteiros positivos.

Porém, sabemos que $\mathbb{F}G/J$ é álgebra semiprima, e assim, utilizando o Lema 2.1.3, todo idempotente é central, isso implica que $n_i = 1$ para todo i. Mais ainda, cada D_i tem de ser comutativo, pois, caso contrário, pelo Lema 2.1.4, $U(D_i)$ teria um subgrupo livre, contradizendo o fato de que $U(\mathbb{F}G/J)$ satisfaz uma identidade de grupo.

Logo, $\mathbb{F}G/J$ é comutativo. Segue que $(x, y) + J = 1 + J$ para todo $x, y \in G$, e assim, $G' \subset 1 + J$. Tomemos $l \in \mathbb{N}$ tal que $p^l > k$ e $x \in G'$. Escrevemos $x = 1 + j$, e

$$\begin{aligned} x^{p^l} &= (1 + j)^{p^l} \\ &= 1 + j^{p^l} \\ &= 1 \end{aligned}$$

Portanto, G' é p-grupo. □

Vamos agora enunciar alguns resultados clássicos que caracterizam as álgebras de grupo $\mathbb{F}G$ que satisfazem identidades polinomiais. Tais resultados foram demonstrados em sua maioria por Donald Passman e I. Martin Isaacs, e posteriormente foram compilados em [18].

Proposição 2.1.6. *Seja $\mathbb{F}G$ álgebra de grupo e $char(\mathbb{F}) = 0$. Então, $\mathbb{F}G$ é álgebra semiprima.*

Demonstração. [18, Teorema 2.12, p. 130]. □

Teorema 2.1.7. *Se $char(\mathbb{F}) = p > 0$, são equivalentes:*

a) $\mathbb{F}G$ é semiprimo.

b) $\phi(G)$ é um p'-grupo.

c) G não possui subgrupo finito normal com ordem divisível por p.

Demonstração. [18, Teorema 2.13, p. 131]. □

Teorema 2.1.8. *Sendo $\mathbb{F}$ um corpo e G grupo qualquer, temos:*

a) Se $char(\mathbb{F}) = 0$, então $\mathbb{F}G$ satisfaz uma identidade polinomial se e só se G contém um subgrupo normal abeliano de índice finito.

b) Se $char(\mathbb{F}) = p > 0$, então $\mathbb{F}G$ satisfaz uma identidade polinomial se e só se G contém um subgrupo normal p-abeliano de índice finito.

Demonstração. [18, Corolários 3.8 e 3.10, p. 196]. □

Proposição 2.1.9. *Seja $\mathbb{F}G$ álgebra de grupo. Então $\mathbb{F}G$ satisfaz uma identidade polinomial generalizada não degenerada se e somente se $[G : \phi] < \infty$ e $|\phi'| < \infty$.*

Demonstração. [18, Teorema 3.15, p. 202]. □

Proposição 2.1.10. *Se $char\mathbb{F} = p > 0$, então $N(\mathbb{F}G)$ é nilpotente se e só se $\phi_p(G)$ é finito, onde $N(\mathbb{F}G)$ é o ideal soma de todos os ideais nilpotentes de $\mathbb{F}G$.*

Demonstração. [18, Teorema 1.12, p. 311]. □

Proposição 2.1.11. *Sejam $\mathbb{F}$ um corpo de característica $p > 0$ e G um grupo. Se $N(\mathbb{F}G)$ é ideal nilpotente de $\mathbb{F}G$, então G possui subgrupos S e H tal que S é p-grupo finito, $[G : H] < \infty$ e $S = \phi_p(H)$.*

Demonstração. [18, Demonstração do Corolário 1.14, p. 312-313]. □

2.2 Resultado Principal

Agora, estamos em condições de demonstrar o primeiro problema deste capítulo, a Conjectura de Brian Hartley Particular. Para isto, vamos dividir a demonstração em três casos, exaustivos e mutuamente excludentes. Sendo N o ideal que é a soma de todos os ideais nilpotentes de $\mathbb{F}G$, temos três possibilidades:

i) $N = 0$, ou seja, $\mathbb{F}G$ é semiprima.

ii) $N \neq 0$, N nilpotente.

iii) $N \neq 0$, N nil, mas não nilpotente.

Os casos acima esgotam as possibilidades, pois, sendo N a soma de todos os ideais nilpotentes de $\mathbb{F}G$, N é nil. Se $N = 0$, estamos no primeiro caso. Se $N \neq 0$, podemos ter N nilpotente (Caso (ii)), ou não nilpotente (Caso (iii)).

Teorema 2.2.1. *Sejam $\mathbb{F}$ um corpo infinito e G um grupo de torção. Se $U(\mathbb{F}G)$ satisfaz uma identidade de grupo e $\mathbb{F}G$ é álgebra semiprima, ou seja, $N = 0$, então $\mathbb{F}G$ satisfaz uma identidade polinomial.*

Demonstração. Vamos mostrar que, nestas condições, G tem de ser um grupo abeliano. Sendo P o subconjunto dos p-elementos de G e Q o subconjunto dos p'-elementos de G como na Definição 1.1.9, tomemos $y \in Q$ de ordem m, com $p \nmid m$. Tome

$$\hat{y} = 1 + y + \cdots + y^{m-1} \in \mathbb{F}G.$$

Assim, como $\mathbb{F}G$ é semiprima e $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, $\hat{y}/m = e = e^2$ é central pelo Lema 2.1.3.

Logo, $\hat{y}$ é central em $\mathbb{F}G$, ou seja, dado $g \in G$, $\hat{y}g = g\hat{y}$, e assim,

$$g + yg + \cdots + y^{m-1}g = g + gy + \ldots gy^{m-1}.$$

Como $\mathbb{F}G$ é, em particular, espaço vetorial e os elementos de G são básicos, da igualdade acima podemos concluir que dado $k \in \{0, 1, \ldots, m-1\}$, existe $l \in \{0, 1, \ldots, m-1\}$ tal que $y^k g = gy^l$. Dessa forma, $\langle y \rangle \lhd G$, e com isso, mostra-se que Q é um subgrupo de G:

De fato, dados dois elementos $x, y \in Q$, com $x \neq e$ e $y \neq e$, sabemos que $y^{-1} \in Q$ pois também é um p'-elemento. Para mostrar que Q é subgrupo, basta-nos então mostrar que $xy \in Q$. Agora, como $\langle y \rangle \lhd G$,

$$(xy)^{|x||y|} = (x^{|x|})^{|y|}y^s = y^s \in Q$$

onde $s \geq |x||y|$. Dessa forma, $|xy|$ divide $|x||y|^2$, mas como $p \nmid |x||y|^2$, então $p \nmid |xy|$, ou seja, xy é um p'-elemento.

Logo, todo subgrupo de Q é normal em G, e em particular, é normal em Q, ou seja, Q é um subgrupo abeliano ou hamiltoniano.

Suponhamos que Q seja hamiltoniano. Pelo Teorema 1.1.4, $Q = K_8 \times A$, onde K_8 é o grupo do quatérnios de ordem 8 e A é um grupo abeliano. Sabemos que Q é um p'-grupo, logo K_8 também tem de ser. Mas como K_8 é um grupo finito não abeliano tal que $U(\mathbb{F}K_8) \subset U(\mathbb{F}G)$ satisfaz uma identidade de grupo, podemos aplicar o Lema 2.1.5, e assim K_8 é p-abeliano, ou seja, $K_8' \subset K_8$ é um p-grupo, absurdo. Portanto, Q é um grupo abeliano.

Se $char(\mathbb{F}) = 0$. então $P = 1$ e $G = Q$, logo G é abeliano, e $\mathbb{F}G$ é uma álgebra de grupo comutativa, satisfazendo, em particular, o polinômio $s_2 = [x_1, x_2]$.

Seja agora $char(\mathbb{F}) = p > 0$. Tomemos $g, h \in P$. Então $|g| = p^k$ para algum $k \in \mathbb{N}$, $|h| = p^m$ para algum $m \in \mathbb{N}$, e $(1-g)$ é nilpotente:

$$\begin{aligned}(1-g)^{p^k} &= \sum_{j=0}^{p^k} \binom{p^k}{j} (-g)^j \\ &= 1 + (-g)^{p^k}.\end{aligned}$$

A segunda igualdade segue do fato de que na soma, todos os coeficientes (à exceção de $j = 0$ e $j = p^k$) serão potências de p maiores do que 1, e como a característica do corpo é p, todos esses coeficientes se tornam 0. Se $p = 2$, teremos $(1-g)^{p^k} = 1 + 1 = 0$ e se $p > 2$, teremos $(1-g)^{p^k} = 1 - 1 = 0$.

Ainda, sendo $\hat{h} = 1 + h + \cdots + h^{p^m-1}$, temos

$$\begin{aligned}\hat{h}(1-h) &= (1 + h + \cdots + h^{p^m-1})(1-h) \\ &= 1 - h^{p^m} \\ &= 0.\end{aligned}$$

Logo, pela demonstração do Lema 2.1.3,

$$0 = \hat{h}(1-g)(1-h) = \hat{h}g(1-h),$$

e dessa forma, $\hat{h}g = \hat{h}gh$, ou seja

$$g + hg + \cdots + h^{p^m-1}g = gh + hgh + \cdots + h^{p^m-1}gh.$$

Novamente, como $\mathbb{F}G$ é, em particular, espaço vetorial e os elementos acima são básicos, podemos afirmar que $g = h^i gh$ para algum $i \in \{0, 1, \ldots, p^m - 1\}$. Assim, $ghg^{-1} = h^{-i}$. Como $g, h \in P$ são elementos quaisquer, repetindo o processo utilizado para mostrar que Q é subgrupo, mostra-se que P é subgrupo de G, e ainda, $\langle h \rangle \lhd P$. Assim, P é abeliano ou hamiltoniano. Veremos que P é trivial.

Tomemos $x \in P$ e seja $g \in Q$. Como $\langle g \rangle \lhd G$, temos que $H = \langle g, x \rangle$ é finito. De fato, dado

$h \in H$,

$$\begin{aligned} h &= g^{r_1}x^{s_1}\dots g^{r_k}x^{s_k} \\ &= g^r x^s, \end{aligned}$$

onde $r, s \in \mathbb{N}$ e, como G é grupo de torção, $|g|$ e $|x|$ são finitos, logo H é grupo finito.

Se H for abeliano, $(g, x) = 1$. Se H não for abeliano, podemos aplicar o Lema 2.1.5, e assim, H é subgrupo p-abeliano. Dessa forma, (g, x) é um p-elemento, porém, observemos que

$$(g, x) = g^{-1}x^{-1}gx = g^{-1}g^j = g^{j-1} \in \langle g \rangle$$

para algum $j \in \mathbb{N}$. O único p-elemento em $\langle g \rangle$ é 1, logo $(g, x) = 1$. Agora, todo elemento de G pode ser escrito como produto de um elemento de P e um de Q. De fato, dado $y \in G$, $|y| = n = p^{r_1}q^{r_2}$, com $p \nmid q$, então $n_1 = \frac{n}{p^{r_1}}$ e $n_2 = \frac{n}{q^{r_2}}$ são inteiros primos entre si. Assim, existem $a, b \in \mathbb{Z}$ tal que $an_1 + bn_2 = 1$. Logo,

$$y = y_1 y_2$$

onde $y_1 = y^{an_1} \in P$ pois $(y^{an_1})^{p^{r_1}} = (y^n)^a = 1$ e $y_2 = y^{bn_2} \in Q$ pois $(y^{bn_2})^{q^{r_2}} = (y^n)^b = 1$.

Portanto, como $\langle x \rangle \lhd P$, temos que, dados $y \in G$ e $x^i \in \langle x \rangle$,

$$yx^iy^{-1} = y_1y_2x^i(y_2)^{-1}(y_1)^{-1} = y_1x^i(y_1)^{-1} \in \langle x \rangle,$$

ou seja, $\langle x \rangle \lhd G$. Como $\mathbb{F}G$ é semiprima, pelo Teorema 2.1.7, $x = 1$, ou seja, $G = Q$ é grupo abeliano.

Portanto, $\mathbb{F}G$ satisfaz $s_2 = [x_1, x_2]$. □

Teorema 2.2.2. *Sejam $\mathbb{F}$ um corpo infinito e G um grupo de torção. Se $U(\mathbb{F}G)$ satisfaz uma identidade de grupo e N é ideal nilpotente, então $\mathbb{F}G$ satisfaz uma identidade polinomial.*

Demonstração. Observemos que, pela Proposição 2.1.6, basta considerarmos $char(\mathbb{F}) = p > 0$.

Como N é nilpotente, pela Proposição 2.1.10, $\phi_p(G)$ é um grupo finito. Ainda, como $\phi_p(G) = \langle \phi \cap P \rangle$, então temos que $\phi_p(G) \lhd G$, e assim,

$$\phi(G/\phi_p(G)) = \{g\phi_p(G) : g\phi_p(G) \text{ tem finitos conjugados}\}$$

não possui p-elementos. De fato, se $|g\phi_p(G)| = p^k$ para algum k, então

$$\phi_p(G) = (g\phi_p(G))^{p^k} = (g^{p^k})\phi_p(G)$$

e assim $g^{p^k} \in \phi_p(G)$ e $g \in P \cap \phi(G)$.

Pelo Teorema 2.1.7, $\mathbb{F}(G/\phi_p(G))$ é semiprima. Olhemos agora para o grupo finito $\phi_p(G)$. Se ele for abeliano, será um p-grupo, pois é gerado por p-elementos. Se ele não for abeliano,

aplicamos o Lema 2.1.5, e concluímos que seu subgrupo comutador é um p-grupo. Logo, os p-elementos de $\phi_p(G)$ formam um grupo. Como $\phi_p(G)$ é gerado por p-elementos, $\phi_p(G)$ é um p-grupo.

Sendo $\phi_p(G)$ um p-subgrupo normal finito, pelo Lema 1.7.7, $\Delta(G, \phi_p(G))$ é nilpotente, logo $U(\mathbb{F}(G/\phi_p(G)))$ satisfaz a identidade de grupo. Pelo Caso (i), $G/\phi_p(G)$ é abeliano, ou seja, $G' \subset \phi_p(G)$ é p-subgrupo finito.

Portanto, G é um subgrupo p-abeliano de índice finito de G, e assim, $\mathbb{F}G$ satisfaz uma identidade polinomial pelo Teorema 2.1.8. □

Teorema 2.2.3. *Sejam $\mathbb{F}$ um corpo infinito e G um grupo de torção. Se $U(\mathbb{F}G)$ satisfaz uma identidade de grupo e N é ideal nil, mas não nilpotente, então $\mathbb{F}G$ satisfaz uma identidade polinomial.*

Demonstração. Novamente, só precisamos analisar o caso em que $char(\mathbb{F}) > 0$. Tendo observado isso, vamos mostrar agora que N é uma PI-álgebra. Para isso, construiremos um candidato à identidade polinomial.

Sejam $R = \mathbb{F}\langle X\rangle$ a álgebra livre no conjunto enumerável $X = \{x_1, x_2, \dots\}$, t outra variável e $R[[t]]$ o anel das séries de potência sobre R, ou seja

$$R[[t]] = \left\{ \sum_{i=0}^{\infty} p_i t^i : p_i \in R \right\}.$$

Ainda, seja $w = w(y_1, y_2, \dots, y_n)$ a identidade de grupo não trivial satisfeita por $U(\mathbb{F}G)$.

Os elementos $1 + x_1 t, \dots, 1 + x_n t$ são unidades em $R[[t]]$. De fato, para cada $i = 1, \dots, n$, existe

$$g_i = 1 - x_i t + x_i^2 t^2 - x_i^3 t^3 + \cdots = \sum_{j=0}^{\infty} (-1)^j x_i^j t^j$$

tal que $(1 + x_i t) g_i = g_i (1 + x_i t) = 1$.

Os elementos $(1 + x_i t)$ geram um grupo livre pelo Argumento de Magnus. De fato, se

$$(1 + x_{i_1} t)^{\alpha_1} (1 + x_{i_2} t)^{\alpha_2} \dots (1 + x_{i_c} t)^{\alpha_c} = 1$$

com $\alpha_i \neq 0$ para todo i, escrevendo $\alpha_i = p^{s_i} \beta_i$, com $p \nmid \beta_i$, temos

$$[(1 + x_{i_1} t)^{p^{s_1}}]^{\beta_1} \dots [(1 + x_{i_c} t)^{p^{s_c}}]^{\beta_c} = 1.$$

Observemos que:

$$(1 + x_{i_j} t)^{p^{s_j}} = \sum_{k=0}^{p^{s_j}} \binom{p^{s_j}}{k} (x_{i_j} t)^k = 1 + x_{i_j}^{p^{s_j}} t^{p^{s_j}}$$

pois os outros coeficientes da soma são múltiplos de p maiores do que 1.

Tomando $y_{i_j} = x_{i_j}^{p^{s_j}}$, temos

$$(1 + y_{i_1} t^{p^{s_1}})^{\beta_1} \dots (1 + y_{i_c} t^{p^{s_c}})^{\beta_c} = 1$$

e o coeficiente de $y_{i_1} y_{i_2} \dots y_{i_c} t^{\sum_j p^{s_j}}$ é $\beta_1 \beta_2 \dots \beta_c$ que é não nulo, pois cada $\beta_i \neq 0$, contradição.

Dessa forma, como os elementos $(1 + x_i t)$ geram um grupo livre, substituindo-os em

$$w(y_1, y_2, \dots, y_n),$$

obtemos a expressão

$$1 \neq (1 + x_{i_1} t)^{l_1} (1 + x_{i_2} t)^{l_2} \dots (1 + x_{i_s} t)^{l_s} \in R[[t]],$$

e colocando cada t^i em evidência, podemos reescrever a desigualdade acima da seguinte forma:

$$\sum_{i \geq 1} p_i(x_1, \dots, x_n) t^i \neq 0,$$

onde $p_i(x_1, \dots, x_n)$ são polinômios homogêneos de grau i.

Observemos que a soma é possivelmente infinita, uma vez que algum l_i pode ser negativo. Como a soma é não nula, existe $l \geq 1$ tal que $p_l(x_1, \dots, x_n) \neq 0$ e $p_l(x_1, \dots, x_n) \in \mathbb{F}\langle X \rangle$ é um polinômio homogêneo de grau l. Este polinômio é nosso candidato a identidade de N.

Agora, tomemos $r_1, \dots, r_n \in N(\mathbb{F}G)$. Os elementos $1 + r_i \lambda$, $i = 1, \dots, n$, $\lambda \in \mathbb{F}$ são invertíveis em $\mathbb{F}G$, com inversa

$$(1 + r_i \lambda)^{-1} = 1 - r_i \lambda + r_i^2 \lambda^2 - \dots$$

que está bem definida, uma vez que r_i é elemento nilpotente, para todo $i = 1, \dots, n$.

Assim, tomando os valores de $1 + r_1 \lambda, \dots, 1 + r_n \lambda$ na identidade de grupo, temos que

$$\sum_{i=1}^{k} p_i(r_1, \dots, r_n) \lambda^i = 0.$$

Observemos que a soma é finita, pois $\exists I_1, I_2, \dots, I_m$ ideais nilpotentes tal que $\{r_1, \dots, r_n\} \subset I = I_1 + I_2 + \dots + I_m$, que é um ideal nilpotente, uma vez que é soma finita de ideais nilpotentes. Logo, se o grau de nilpotência de I é $k + 1$, $p_t(r_1, \dots, r_n) = 0$, para todo $t > k$.

Pela observação acima, se $l > k$, então $p_l(r_1, \dots, r_n) = 0$. Por outro lado, se $l \leq k$, como $\mathbb{F}$ é infinito, existem elementos não nulos distintos $\lambda_1, \dots, \lambda_{k+1} \in \mathbb{F}$ tal que

$$\sum_{i=1}^{k} p_i(r_1, \dots, r_n) \lambda_j^i = 0 \qquad \forall j = 1, \dots, k + 1.$$

Podemos escrever as igualdades acima de forma matricial:

$$\begin{bmatrix} 1 & \lambda_1 & \dots & \lambda_1^k \\ 1 & \lambda_2 & \dots & \lambda_2^k \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_{k+1} & \dots & \lambda_{k+1}^k \end{bmatrix} \begin{bmatrix} 0 \\ p_1(r_1,\dots,r_n) \\ \vdots \\ p_k(r_1,\dots,r_n) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

e, como o determinante da matriz de Vandermonde acima é não nula, temos:

$$p_1(r_1,\dots,r_n) = \cdots = p_k(r_1,\dots,r_n) = 0.$$

Logo, $p_l(r_1,\dots,r_n) = 0$ também nesse caso, ou seja, $p_l(x_1,\dots,x_n)$ é uma identidade polinomial para para $N(\mathbb{F}G)$.

Pelo Teorema 1.8.13, segue que N satisfaz uma identidade polinomial multilinear

$$f(x_1,\dots,x_d) = \sum_{\sigma\in S_d} \alpha_\sigma x_{\sigma(1)}\dots x_{\sigma(d)}$$

onde $\alpha_\sigma \in \mathbb{F}$ e S_d é o grupo simétrico de grau d. Como N não é nilpotente, podemos escolher $a_1,\dots,a_d \in N(\mathbb{F}G)$ tal que $a_1a_2\dots a_d \neq 0$. Logo

$$a_1\mathbb{F}Ga_2\mathbb{F}G\dots a_d\mathbb{F}G \neq 0$$

e

$$\sum_{\sigma\in S_d} \alpha_\sigma a_{\sigma(1)}x_{\sigma(1)}\dots a_{\sigma(d)}x_{\sigma(d)}$$

é uma identidade polinomial multilinear generalizada não degenerada de $\mathbb{F}G$.

Pela Proposição 2.1.9, concluímos que $[G;\phi] < \infty$ e $|\phi'| < \infty$. Assim, pelo Lema 1.1.13, G é localmente finito.

Agora, mostremos que ϕ' é p-grupo. De fato, se ϕ' não for um p-grupo, existe um elemento $x = (a_1,b_1)^{r_1}(a_2,b_2)^{r_2}\dots(a_s,b_s)^{r_s}$ que não é p-elemento. Em particular, $x \neq 1$. Então, tomando $H = \langle a_1,b_1,a_2,b_2,\dots,a_s,b_s\rangle$, H é finito e não abeliano. Logo, pelo Lema 2.1.5, H é p-abeliano, absurdo, pois $x \in H'$ e não é p-elemento.

Portanto, ϕ' é p-grupo, ou seja, ϕ é subgrupo p-abeliano de índice finito, logo, pelo Lema 2.1.8, $\mathbb{F}G$ satisfaz uma identidade polinomial. □

Observação 2.2.4. Nas demonstrações acima, é importante mencionar que em poucos momentos foi utilizada a hipótese do corpo $\mathbb{F}$ ser infinito. O uso mais claro dessa hipótese se deu ao construir a matriz de Vandermonde com determinante não nulo. No Capítulo 3, faremos o caso geral dos teoremas acima, e as demonstrações serão muito parecidas, contornando este argumento de Vandermonde utilizado e outras observações.

2.3 Caracterização dos Grupos G tais que $U(\mathbb{F}G)$ satisfaz uma Identidade de Grupo

Tendo demonstrado os Teoremas 2.2.1, 2.2.2 e 2.2.3, naturalmente surge a questão de verificar se a recíproca da Conjectura de Brian Hartley é verdadeira. Ou seja, sendo $\mathbb{F}$ corpo infinito e G grupo de torção, se $\mathbb{F}G$ satisfaz uma identidade polinomial, então $U(\mathbb{F}G)$ satisfaz uma identidade de grupo?

Sabemos que, se G é finito, então $\mathbb{F}G$ sempre satisfaz identidades polinomiais, pelo Exemplo 1.8.11. No Teorema 2.2.1, mostramos que, se $char(\mathbb{F}) = 0$ e $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, então G é um grupo abeliano. Portanto, se tomarmos G um grupo finito não abeliano e $char(\mathbb{F}) = 0$, então $\mathbb{F}G$ satisfaz identidades polinomiais, mas $U(\mathbb{F}G)$ não satisfaz identidades de grupo, ou seja, a recíproca da Conjectura de Brian Hartley é falsa.

Dessa forma, o próximo objetivo é encontrar condições adicionais para que a recíproca da Conjectura seja verdadeira. Porém, ao encontrar tais condições, veremos que elas são necessárias e suficientes, e assim, estaremos respondendo ao segundo problema colocado no início deste capítulo.

Observemos que, se a característica do corpo $\mathbb{F}$ é 0, então $\mathbb{F}G$ é álgebra semiprima e $U(\mathbb{F}G)$ satisfaz identidades de grupo se, e só se, $\mathbb{F}G$ satisfaz identidades polinomiais e G é abeliano.

Logo, basta-nos agora estudar o caso em que $char(\mathbb{F}) = p > 0$, e neste caso, um fenômeno parecido acontecerá.

Nomeadamente, em 1997, Passman [17], demonstrou o seguinte resultado:

Teorema 2.3.1. *Seja $\mathbb{F}G$ a álgebra de grupo de um grupo de torção G sobre um corpo infinito $\mathbb{F}$ de característica $p > 0$. Sendo U o grupo das unidades de $\mathbb{F}G$, são equivalentes:*

a) U satisfaz uma identidade de grupo.

b) G possui um subgrupo p-abeliano normal de índice finito, e G' é um p-grupo de período limitado.

c) U satisfaz $(x, y)^{p^k} = 1$ para algum $k \geq 0$.

A implicação $c) \Rightarrow a)$ é direta. Para maior clareza, vamos demonstrar cada uma das implicações como um teorema, a saber, os Teoremas 2.3.9 e 2.3.12. Para isso, precisamos compreender a forma dos elementos do subgrupo comutador G'. Começamos com uma classe especial de grupos.

Lema 2.3.2. *Seja G um grupo de torção que contém um subgrupo abeliano normal A, tal que $G/A = \langle Ag \rangle$, isto é, o quociente é cíclico gerado por Ag. Então $G' = \{(a, g) : a \in A\}$.*

Demonstração. Defina $\phi : A \to A$ por $\phi(a) = (a, g)$. ϕ está bem definida, pois como $A \lhd G$, dado $a \in A$, $g^{-1}ag \in A$, e assim $(a, g) = a^{-1}g^{-1}ag \in A$. Agora, como A também é abeliano, ϕ é

um homomorfismo. De fato:

$$\begin{aligned}\phi(ab) &= (ab, g)\\ &= (ab)^{-1}g^{-1}abg\\ &= b^{-1}a^{-1}\underbrace{(g^{-1}ag)}_{\in A}g^{-1}bg\\ &= a^{-1}(g^{-1}ag)b^{-1}g^{-1}bg\\ &= \phi(a)\phi(b).\end{aligned}$$

Seja $H = Im\phi$, então $H \leq G'$. Nosso objetivo é mostrar que $H = G'$. Primeiramente, mostremos que $H \lhd G$. Como $H \leq A$, e A é abeliano, H é central em A. Ainda,

$$\begin{aligned}g^{-1}(a, g)g &= g^{-1}a^{-1}g^{-1}agg\\ &= g^{-1}a^{-1}gg^{-1}g^{-1}agg\\ &= (\underbrace{g^{-1}ag}_{\in A}, g) \in H\end{aligned}$$

Como $G/A = \langle Ag\rangle$, um elemento qualquer de G é da forma ag^k, com $a \in A$ e para algum $k \in \mathbb{N}$. Assim, dado um elemento qualquer $x = ag^k \in G$, e $b \in A$,

$$\begin{aligned}(ag^k)^{-1}(b, g)ag^k &= g^{-k}a^{-1}(b, g)ag^k\\ &= g^{-k}(b, g)g^k\\ &= (c, g) \in H,\end{aligned}$$

onde $c \in A$ pela observação anterior aplicada k vezes. Portanto, $H \lhd G$.

Agora, para $a \in A$ e $i \in \mathbb{Z}$, temos

$$\begin{aligned}g^{-i}ag^i &= g^{-i+1}aa^{-1}g^{-1}agg^{i-1}\\ &= g^{-i+1}a(a, g)g^{i-1}\\ &= g^{-i+2}a\underbrace{\underbrace{(a^{-1}g^{-1}ag)}_{\in H}\underbrace{g^{-1}(a, g)g}_{\in H}}_{h_1 \in H}g^{i-2}\\ &= g^{-i+2}ah_1g^{i-2}\\ &= \vdots\\ &= ah\end{aligned}$$

onde $h \in H$. Com isso, podemos mostrar que A/H (observemos que este quociente faz sentido uma vez que A é abeliano, e assim, todo subgrupo é normal) é central em G/H. De fato, sendo

$x = bg^i \in G$, onde $b \in A$ e $a \in A$,

$$\begin{aligned} bg^iHaHg^{-i}b^{-1}H &= bg^iag^{-i}b^{-1}H \\ &= bahb^{-1}H \\ &= aH. \end{aligned}$$

Assim, podemos quocientar G/H por A/H, e,

$$\frac{G/H}{A/H} \cong \frac{G}{A}$$

que é um grupo cíclico por hipótese. Ainda, sendo $Z(G/H)$ o centro de G/H,

$$\frac{G/H}{Z(G/H)} \cong \frac{(G/H)/(A/H)}{Z(G/H)/(A/H)}$$

que também é cíclico pois é quociente de um grupo cíclico. Logo, pela Proposição 1.1.7, G/H é abeliano, ou seja, $G' \leq H$, e portanto, $G' = H$, como queríamos. □

A demonstração do próximo resultado pode ser encontrado em [11, Lema 1.2.5].

Lema 2.3.3. *Seja A uma $\mathbb{F}$-álgebra tal que $U(A)$ satisfaz $w = 1$. Existe um inteiro positivo n determinado por $w = 1$ e pela característica do corpo tal que se $a, b \in A$, $a^2 = b^2 = 0$ e $(ab)^n \neq 0$ então ab não é nilpotente.*

Conhecendo a forma dos elementos em G', é possível demonstrar parte da implicação $a) \Rightarrow b)$ do Teorema 2.3.1 para classes particulares de grupos. Vamos agora, supor que G é grupo contendo um p-subgrupo abeliano normal A, tal que G/A é cíclico e mostrar, nas hipóteses do Teorema 2.3.1, que G' possui período limitado.

Primeiramente, restringimos a ordem do elemento g aos primos, e depois concluímos o caso geral.

Lema 2.3.4. *Suponha que G é grupo de torção tal que $G/A = \langle Ag \rangle$, onde A é um p-grupo abeliano normal e g tem ordem prima $q \neq p$, $p = char(\mathbb{F})$. Se $\mathbb{F}$ é corpo infinito e $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, então G' tem período limitado.*

Demonstração. Definimos $\theta : \mathbb{F}A \to \mathbb{F}A$ por $\theta(\alpha) = \alpha + g^{-1}\alpha g + g^{-2}\alpha g^2 + \cdots + g^{-(q-1)}\alpha g^{q-1}$. θ está bem definida pois $A \lhd G$. Sabemos que $\mathbb{F}A$ é comutativa. Mostremos que g comuta com $\theta(\alpha)$:

$$\begin{aligned} g\theta(\alpha) &= g(\alpha + g^{-1}\alpha g + \cdots + g^{-(q-1)}\alpha g^{q-1}) \\ &= g\alpha + \alpha g + g^{-1}\alpha g^2 + \cdots + g^{-(q-2)}\alpha g^{q-1} \\ &= g\alpha + (\alpha + g^{-1}\alpha g + \cdots + g^{-(q-2)}\alpha g^{q-2})g \\ &= g\alpha + (\theta(\alpha) - g^{-(q-1)}\alpha g^{q-1})g \\ &= g\alpha + \theta(\alpha)g - g\alpha \\ &= \theta(\alpha)g. \end{aligned}$$

Assim, $\theta(\alpha)$ é central em $\mathbb{F}G$, para todo $\alpha \in \mathbb{F}A$.

Agora, lembrando que $\hat{g} = 1 + g + \cdots + g^{q-1}$, fixemos $a \in A$, e seja $\beta = \hat{g}a^{-1}(1 - g^{-1})$. Como $(1 - g^{-1})\hat{g} = 0$, então $\beta^2 = 0$. Seja ainda $\gamma = (qa - \theta(a))\hat{g}$. Observemos que $qa - \theta(a) \in \Delta(A)$. Vamos mostrar que $\Delta(A)$ é nil: De fato, se $\Delta(A)$ não fosse nil, existiria $\alpha \in \Delta(A)$, $\alpha = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n$ que não é nilpotente. Tomando $H = \langle a_1, a_2, \ldots, a_n \rangle$, como A é p-grupo abeliano, é localmente finito, e assim H é finito e p-grupo. Pelo Lema 1.7.7, $\Delta(A, H)$ é nilpotente, mas $\alpha \in \Delta(A, H)$, absurdo.

Portanto, $\Delta(A)$ é nil. Sabemos que todo ideal nil está contido no radical de Jacobson. Logo, $\gamma \in J(\mathbb{F}A)\mathbb{F}G \subset J(\mathbb{F}G)$ pela Proposição 1.6.6.

Agora, mostremos que $J(\mathbb{F}G)$ é nil. Tomemos $\delta \in J(\mathbb{F}G)$. Sabemos que G é localmente finito, logo, tomando H subgrupo gerado pelo suporte de δ como fizemos acima, $\delta \in \mathbb{F}H$, onde H é finito. Pela Proposição 1.6.6, $\delta \in J(\mathbb{F}H)$ e $J(\mathbb{F}H)$ é nilpotente, pois $\mathbb{F}H$ é de dimensão finita, ou seja, δ é nilpotente.

Dessa forma, $\beta\gamma \in J(\mathbb{F}G)$ é nilpotente.

Ainda, com alguns cálculos diretos, vê-se que para todo $\alpha \in \mathbb{F}A$,

$$\hat{g}\alpha\hat{g} = \theta(\alpha)\hat{g}.$$

Logo,

$$\begin{aligned} \gamma^2 &= (qa - \theta(a))\hat{g}(qa - \theta(a))\hat{g} \\ &= (qa - \theta(a))\theta(qa - \theta(a))\hat{g}. \end{aligned}$$

Mas,

$$\begin{aligned} \theta(qa - \theta(a)) &= (qa - \theta(a)) + g^{-1}(qa - \theta(a))g + \cdots + g^{-(q-1)}(qa - \theta(a))g^{q-1} \\ &= qa - \theta(a) + qg^{-1}ag - g^{-1}\theta(a)g + \cdots + qg^{-(q-1)}ag^{q-1} - g^{-(q-1)}\theta(a)g^{q-1} \\ &= q\theta(a) - q\theta(a) \\ &= 0. \end{aligned}$$

Ou seja, $\gamma^2 = 0$. Pelo Lema 2.3.3, existe um inteiro positivo n dependendo da identidade de grupo tal que $(\beta\gamma)^n = 0$. Escolha r tal que $p^r \geq n$. Logo, $(\beta\gamma)^{p^r} = 0$. Ainda,

$$\begin{aligned} \beta\gamma &= \hat{g}a^{-1}(1 - g^{-1})(qa - \theta(a))\hat{g} \\ &= \hat{g}a^{-1}(1 - g^{-1})qa\hat{g} - \hat{g}a^{-1}(1 - g^{-1})\theta(a)\hat{g} \\ &= \hat{g}a^{-1}(1 - g^{-1})qa\hat{g} \\ &= q\hat{g}(1 - a^{-1}g^{-1}ag)\hat{g} \\ &= q(q\hat{g} - \hat{g}(a, g)\hat{g}). \end{aligned}$$

Sabemos que $\hat{g}(a, g)\hat{g} = \theta((a, g))\hat{g}$, logo

$$\beta\gamma = q(q - \theta((a, g)))\hat{g}.$$

Agora, observando que $char(\mathbb{F}) = p$, para todo $\alpha \in \mathbb{F}A$,

$$\begin{aligned}(\theta(\alpha))^{p^r} &= \alpha^{p^r} + (g^{-1}\alpha g)^{p^r} + \cdots + (g^{-(q-1)}\alpha g^{q-1})^{p^r} \\ &= \alpha^{p^r} + g^{-1}\alpha^{p^r} g + \cdots + g^{-(q-1)}\alpha^{p^r} g^{q-1} \\ &= \theta(\alpha^{p^r}).\end{aligned}$$

Assim, como $\theta((a,g))$ é central e $\hat{g}^m = q^{m-1}\hat{g}\ \forall m > 0$, temos que

$$\begin{aligned}0 &= (\beta\gamma)^{p^r} \\ &= q^{p^r}(q - \theta((a,g)))^{p^r}\hat{g}^{p^r} \\ &= q^{p^r}(q^{p^r} - \theta((a,g))^{p^r})q^{p^r-1}\hat{g}.\end{aligned}$$

Dessa forma, pelo Pequeno Teorema de Fermat, sabemos que $q^{p^r} = q$, logo, da equação acima, temos:

$$(q - \theta((a,g)^{p^r}))\hat{g} = 0.$$

Observemos que $q - \theta((a,g)^{p^r}) \in \mathbb{F}A$, e elementos de $\mathbb{F}G$ são unicamente escritos como $\sum_{i=0}^{q-1} \alpha_i g^i$, com $\alpha_i \in \mathbb{F}A$. Logo, na equação acima, devemos ter $\theta((a,g)^{p^r}) = q$.

Mas $(a,g)^{p^r}$ é um elemento de A, e aplicando θ, temos uma soma de seus conjugados. A única forma disso somar q é se $(a,g)^{p^r} = 1$. Logo, pelo Lema 2.3.2, G' tem período limitado. □

Agora, analisemos o caso em que a ordem de g é exatamente p.

Lema 2.3.5. *Suponha que G é grupo tal que $G/A = \langle Ag \rangle$, onde A é um p-grupo abeliano e $|g| = p$. Se $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, então G' tem período limitado.*

Demonstração. Defina θ como no lema anterior, com $q = p$. Fixando $a \in A$, notemos que $(\hat{g})^2 = (a^{-1}\hat{g}a)^2 = 0$. Ainda, $\hat{g} \in \Delta(G)$, logo, $\beta = a^{-1}\hat{g}a\hat{g} \in \Delta(G)$, mas como G é um grupo localmente finito, β é nilpotente: De fato, se $\beta = \lambda_1 a_1 + \cdots + \lambda_k a_k$, tome $H = \langle a_1, \ldots, a_k \rangle$, como G é localmente finito, H é um p-grupo finito, ou seja, existe p^r tal que $a_i^{p^r} = 1$ para todo $i = 1, \ldots, k$. Assim, como $\beta \in \Delta(G)$ e pelo Pequeno Teorema de Fermat,

$$\beta^{p^r} = \lambda_1^{p^r} a_1^{p^r} + \cdots + \lambda_k^{p^r} a_k^{p^r} = \lambda_1 + \cdots + \lambda_k = 0.$$

Sabemos pelo lema anterior que $\forall \alpha \in \mathbb{F}A$, $\theta(\alpha)$ é um elemento central e $\hat{g}\alpha\hat{g} = \theta(\alpha)\hat{g}$. Logo,

$$\begin{aligned}\beta^2 &= a^{-1}\hat{g}a(\hat{g}a^{-1}\hat{g})a\hat{g} \\ &= a^{-1}\hat{g}a\theta(a^{-1})\hat{g}a\hat{g} \\ &= \theta(a^{-1})a^{-1}(\hat{g}a\hat{g})a\hat{g} \\ &= \theta(a^{-1})\theta(a)\beta.\end{aligned}$$

Assim, segue que

$$0 = \beta^{p^r} = (\theta(a^{-1})\theta(a))^{p^r-1}\beta$$

e analogamente,

$$\begin{aligned} 0 &= \hat{g}\beta^{p^r} \\ &= (\theta(a^{-1})\theta(a))^{p^r-1}\hat{g}a^{-1}\hat{g}a\hat{g} \\ &= \theta(a^{-1})^{p^r}\theta(a)^{p^r-1}\hat{g}a\hat{g} \\ &= \theta(a^{-1})^{p^r}\theta(a)^{p^r}\hat{g}. \end{aligned}$$

Assim, como $\theta(a)$ e $\theta(a^{-1})$ pertencem a $\mathbb{F}A$, a equação acima implica que

$$\theta(a^{-1})^{p^r}\theta(a)^{p^r} = 0.$$

Do lema anterior, sabemos que $\theta(a^{-1})^{p^r}\theta(a)^{p^r} = \theta(a^{-p^r})\theta(a^{p^r})$. Seja $b = a^{p^r}$, então, desenvolvendo a expressão acima, obtemos:

$$\begin{aligned} 0 &= \theta(b^{-1})\theta(b) \\ &= \textstyle\sum_{i=0}^{p-1}\theta(b^{-1}g^{-i}bg^i). \end{aligned}$$

Porém, para $i = 0$, temos $\theta(1) = p = 0$, logo, a soma é, de fato,

$$\sum_{i=1}^{p-1}\theta((b, g^i)) = 0.$$

Agora, observemos que, aplicando θ a um elemento do grupo, obtemos uma soma de p elementos do grupo, então o lado esquerdo da equação acima é a soma de $p(p-1)$ elementos do grupo. Como a soma é 0, a única forma possível é ocorrer grupos de tamanho p de elementos iguais. Assim, podem haver no máximo $p-1$ elementos distintos na soma acima. Mas os conjugados de um elemento do grupo por potências de um elemento de ordem prima são todos iguais ou todos distintos. Logo, se (b, g) não é central, produziria p elementos distintos, o que não pode ocorrer. Portanto, (b, g) é central.

Sendo central, $g^{-i}(b, g)g^i = (b, g)\forall i \in \mathbb{Z}$, e segue que:

$$\begin{aligned} (b, g)^p &= (b, g)[g^{-1}(b, g)g]\dots[g^{-(p-1)}(b, g)g^{p-1}] \\ &= \underbrace{[(b, g)g^{-1}][(b, g)g^{-1}]\dots[(b, g)g^{-1}]}_{p \text{ vezes}} \\ &= [b^{-1}g^{-1}b][b^{-1}g^{-1}b]\dots[b^{-1}g^{-1}b] \\ &= b^{-1}g^{-p}b \\ &= 1. \end{aligned}$$

Por fim, como a função $a \mapsto (a, g)$ é homomorfismo, temos que

$$1 = (b, g)^p = (a^{p^r}, g)^p = (a, g)^{p^{r+1}}$$

para todo $a \in A$. Logo, G' tem período limitado. □

A fim de analisar o caso geral, precisamos dos dois seguinte resultados.

Lema 2.3.6. *Sejam G um grupo e $\mathbb{F}$ corpo. Seja $N \lhd G$ de torção não contendo elementos de ordem divisível pela característica de $\mathbb{F}$. Se N é finito ou G é localmente finito e $U(\mathbb{F}G)$ satisfaz $w = 1$, então $U((G/N))$ satisfaz $w = 1$.*

Demonstração. Suponhamos que N é finito. Tomemos $\bar{N}$ como no Lema 1.7.6 e $e = \bar{N}/|N|$. Assim, e é um idempotente central, e $\mathbb{F}G = \mathbb{F}Ge \oplus \mathbb{F}G(1-e)$. Logo, $U(\mathbb{F}G) = U(\mathbb{F}Ge) \times U(\mathbb{F}G(1-e))$. Observemos que o núcleo de $\theta : \mathbb{F}G \to \mathbb{F}Ge$, tal que $\theta(\alpha) = \alpha e$ é $\Delta(G, N)$ pelo Lema 1.7.6. Logo,

$$\mathbb{F}(G/N) \cong \mathbb{F}G/\Delta(G, N) \cong \mathbb{F}Ge.$$

Portanto, $U(\mathbb{F}(G/N))$ é isomorfo a um subgrupo de $U(\mathbb{F}G)$, e assim satisfaz identidade polinomial.

Suponhamos agora que G é localmente finito, e sendo $w(x_1, \ldots, x_n) = 1$ a identidade de grupo, tomemos $\bar{\alpha_1}, \ldots, \bar{\alpha_n} \in U(\mathbb{F}(G/N))$, seus inversos, e os representantes $\alpha_1, \ldots, \alpha_n \in \mathbb{F}G$ assim como os representantes dos inversos. Então podemos tomar H subgrupo de G gerado pelos suportes dos representantes tomados acima. Como H é finitamente gerado e G é localmente finito, H é finito.

Assim, aplicando o primeiro caso, vemos que $U(\mathbb{F}(H/N \cap H))$ satisfaz $w = 1$. Mas como $\frac{H}{N \cap H} \cong \frac{NH}{N}$ e $\bar{\alpha_1}, \ldots, \bar{\alpha_n} \in U(\mathbb{F}(NH/N))$, então $w(\bar{\alpha_1}, \ldots, \bar{\alpha_n}) = 1$, e portanto $U(\mathbb{F}(G/N))$ satisfaz $w = 1$. □

Lema 2.3.7. *Seja $\mathbb{F}$ um corpo de característica $p > 0$ e G um grupo, tal que $U(\mathbb{F}G)$ satisfaz $w = 1$. Se N é um p-subgrupo normal de G, e N é finito ou G é localmente finito, então $U(\mathbb{F}(G/N))$ satisfaz $w = 1$.*

Demonstração. [11, Lema 1.2.18] □

Com os resultados demonstrados anteriormente, estamos próximos de concluir a implicação $a) \Rightarrow b)$ do Teorema 2.3.1. Antes, temos o seguinte resultado:

Lema 2.3.8. *Suponha que G contém um p-subgrupo abeliano normal A de índice finito. Se $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, então G' tem período limitado.*

Demonstração. Primeiro, consideramos o caso em que G/A é cíclico, digamos $G/A = \langle Ag \rangle$. Nossa prova é por indução em $|g|$. Se $|g| = 1$, $G = A$ é abeliano, e $G' = \{e\}$. Se $|g|$ é primo, os Lemas 2.3.4 e 2.3.5 nos dão o resultado.

Então seja $|g|$ um número composto, e q um primo dividindo $|g|$. Tomemos $H = \langle A, g^q \rangle$. Por hipótese de indução, H' tem período limitado. Pelo Lema 2.3.2, $H' = \{(a, g^q) : a \in A\}$. Logo, sendo k um limitante para o período de H', $N = \langle H', g^q \rangle$ tem período limitado $k|g^q|$. Agora, H'

é centralizado por A e normalizado por g. De fato,

$$\begin{aligned} g(a,g^q)g^{-1} &= ga^{-1}g^{-q}ag^qg^{-1} \\ &= \underbrace{ga^{-1}g^{-1}}_{b^{-1}}g^{-q}\underbrace{gag^{-1}}_{b}g^q \\ &= (b,g^q) \in H'. \end{aligned}$$

Logo, $H' \lhd G$.

Como $H' \leq N$, os conjugados de g^q estão em N. De fato, dado $x \in G$, $x = ag^i$, para algum $a \in A$ e algum $i \in \mathbb{N}$. Assim,

$$\begin{aligned} xg^qx^{-1} &= ag^ig^qg^{-i}a^{-1} \\ &= ag^qa^{-1} \\ &= g^q(g^{-q}ag^q)a^{-1} \\ &= g^q\underbrace{a(a^{-1}g^{-q}ag^q)a^{-1}}_{\in H'} \in N. \end{aligned}$$

Os elementos de N são produtos de elementos de H' com potências de g. Como cada elemento será normalizado, $N \lhd G$.

Observemos que G/N é gerado por AN/N e Ng. Ainda, como G quocientado por A é um p-grupo, mostremos que seus p-elementos formam um subgrupo: Seja $P = \{x \in G : |x| = p^k \text{ para algum } k \in \mathbb{N}\}$. Dados $x, y \in P$, sabemos que $y^{-1} \in P$ por ser p-elemento, assim basta-nos mostrar que $xy \in P$. Sabemos que $x = ag^i$, $y = bg^j$ com $a, b \in A$ e $i, j \in \mathbb{N}$ e existem $k, m \in \mathbb{N}$ tais que $x^{p^k} = y^{p^m} = e$.

Dessa forma, $e = x^{p^k} = (ag^i)^{p^k} = cg^{ip^k}$, onde $c \in A$. Logo, $g^{ip^k} \in A$. Analogamente, mostra-se que $g^{jp^m} \in A$. Assim,

$$(xy)^{p^{k+m}} = d(g^{ip^k})^{p^m}(g^{jp^m})^{p^k} \in A,$$

para algum $d \in A$. Portanto, $P \leq G$.

Em particular, os p-elementos de N formam um subgrupo $N_1 = N \cap P$. Sabemos que G é localmente finito, e logo, pelo Lema 2.3.7, $U(\mathbb{F}(G/N_1))$ satisfaz a identidade de grupo.

Observemos que N/N_1 não contém elementos de ordem divisível por p, G/N_1 é localmente finito e $U(\mathbb{F}(G/N_1))$ satisfaz $w = 1$. Logo, pelo Lema anterior,

$$U\left(\mathbb{F}\frac{(G/N_1)}{(N/N_1)}\right) \cong U(\mathbb{F}(G/N))$$

satisfaz $w = 1$.

Como $|Ng| \leq q < |g|$, por hipótese de indução, $(G/N)'$ tem período limitado. Mas, sabemos

que

$$\left(\frac{G}{N}\right)' = \frac{G'N}{N}$$

e N tem período limitado, logo G' também tem, pois, dado $x \in G'$, como $(G/N)'$ tem período limitado, existe k tal que $(xN)^k = N$, ou seja, $x^k \in N$. Mas como N tem período limitado, existe r tal que $(x^k)^r = e$, ou seja, $x^{kr} = e$, e G' tem período limitado.

Vamos agora ao caso geral. Sejam H_i os subgrupos de G contendo A tal que H_i/A é cíclico. Como G/A é finito, existem apenas um número finito de tais subgrupos, pois se existissem infinitos subgrupos H_i tal que H_i/A é cíclico, poderíamos encontrar uma quantidade infinita de classes laterais distintas h_iA, com $h_i \in H_i$, o que não pode ocorrer pois G/A é finito.

Pelo caso anterior, cada H_i' tem período limitado, e como cada $H_i' \subset A$, que é abeliano, o subgrupo K gerado por todos os H_i' tem período limitado.

Como a conjugação por um elemento é um isomorfismo, todo conjugado de um H_i é algum H_j, e análogo para H_i'. Logo, vemos que $K \lhd G$.

Ainda, A/K é central em G/K, pois, dado $a \in A$, $g \in G$, sendo $H_i = \langle A, g\rangle$, então $(a, g) \in H_i' \leq K$. Logo, $(a, g)K = K$. Assim, como $(G/K)/(A/K) \cong (G/A)$ é de índice finito, o centro de G/K também tem de ter índice finito. Logo, pela Proposição 1.1.6, $(G/K)'$ é finito. Mas $(G/K)' = G'K/K$, e como K possui período limitado, utilizando o mesmo raciocínio do caso anterior, vemos que G' também tem. □

Agora, estamos em condições de demonstrar a implicação $a) \Rightarrow b)$ do Teorema 2.3.1:

Teorema 2.3.9. *Sejam G grupo de torção, $\mathbb{F}$ corpo infinito com $char(\mathbb{F}) = p > 0$. Se $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, G possui um subgrupo p-abeliano de índice finito, G' é p-grupo e tem período limitado.*

Demonstração. Como $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, $\mathbb{F}G$ satisfaz uma identidade polinomial pelos Teoremas 2.2.1, 2.2.2 e 2.2.3, logo, pelo Lema 2.1.8, G possui um subgrupo A normal, p-abeliano de índice finito.

Observemos que G' é p-grupo, pois, se não fosse, existiria $x \in G'$ p'-elemento. Em particular, $x = (a_1, b_1)^{r_1} \dots (a_t, b_t)^{r_t} \neq e$. Tomando $H = \langle a_1, b_1, \dots, a_t, b_t\rangle$, H é finito pois G é localmente finito e não abeliano, assim, aplicando o Lema 2.1.5, H é p-abeliano, ou seja, x é um p-elemento, contradição. Portanto, G' é p-grupo.

Assim, falta-nos mostrar que G' tem período limitado. Temos dois casos a considerar: A é abeliano ou não.

Se A for abeliano, podemos escrever $A = P \times Q$, onde P é p-grupo normal e Q é p'-grupo normal. Pelo Lema 2.3.6, sabemos que $U(\mathbb{F}(G/Q))$ satisfaz identidade de grupo. Logo, A/Q é um p-subgrupo abeliano normal de G/Q, e pelo Lema 2.3.8, $(G/Q)'$ tem período limitado. Mas $(G/Q)' = G'Q/Q$, e tomando $x \in G'$, como $(G/Q)'$ tem período limitado, digamos k, $(xQ)^k = Q$, ou seja, $x^k \in Q$. Mas x^k é um p-elemento e Q é um p'-grupo, logo, $x^k = e$ e G' possui período limitado.

Se A não for abeliano, tomemos G/A' e A/A' subgrupo normal abeliano, e repetimos o processo anterior com estes grupos. Assim, teremos que $(G/A')'$ tem período limitado. Mas $(G/A')' = G'A'/A'$ e A' é finito. Logo, G' tem período limitado, pelo mesmo raciocínio da demonstração do Lema 2.3.8. □

O próximo resultado nos fornece uma condição para garantir que o grupo das unidades de uma álgebra satisfaz uma identidade de grupo.

Lema 2.3.10. *Sejam R uma $\mathbb{F}$-álgebra e I um ideal de R nil de expoente limitado $\leq p^k$. Se $U(R/I)$ satisfaz $(x,y)^{p^j} = 1$, então $U(R)$ satisfaz $(x,y)^{p^{k+j}} = 1$.*

Demonstração. A aplicação natural $R \to R/I$ induz um homomorfismo de grupos

$$U(R) \to U(R/I)$$

que é sobrejetor, pois dado $x+I \in U(R/I)$, existe $y+I \in U(R/I)$ tal que $xy+I = yx+I = 1+I$. Logo, $xy = 1 + j_1$ e $yx = 1 + j_2$, com $j_1, j_2 \in I$. Como I é nil de expoente limitado $\leq p^k$, $j_1^{p^k} = j_2^{p^k} = 0$, e portanto, $(xy)^{p^k} = 1 = (yx)^{p^k}$, ou seja, $x \in U(R)$, com $x^{-1} = (yx)^{p^k-1}y$.

Se $x, y \in U(R)$, então $\bar{x}, \bar{y} \in U(R/I)$ e $(\bar{x}, \bar{y})^{p^j} = 1$. Logo, $(x,y)^{p^j} - 1 \in I$, e assim, este elemento é nilpotente de grau $\leq p^k$. Logo,

$$\begin{aligned} 0 &= [(x,y)^{p^j} - 1]^{p^k} \\ &= \textstyle\sum_{m=0}^{p^k} \binom{p^k}{m} (-1)^m [(x,y)^{p^j}]^{m-p^k} \\ &= (x,y)^{p^{j+k}} + (-1)^{p^k} \\ &= (x,y)^{p^{j+k}} - 1. \end{aligned}$$

□

A demonstração do próximo resultado pode ser encontrada em [11, Lema 1.3.14].

Lema 2.3.11. *Sejam $\mathbb{F}$ um corpo de característica $p > 0$ e G um grupo tal que $\mathbb{F}G$ satisfaz uma identidade polinomial. Se N é um p-subgrupo normal de período limitado, então $\Delta(G,N)$ é nil de expoente limitado.*

Passemos agora para a implicação $b) \Rightarrow c)$ do Teorema 2.3.1.

Teorema 2.3.12. *Seja $\mathbb{F}G$ a álgebra de grupo de um grupo de torção G sobre um corpo infinito $\mathbb{F}$ de característica $p > 0$. Se G possui um subgrupo p-abeliano normal de índice finito e G' é um p-grupo de período limitado, então U satisfaz $(x,y)^{p^k} = 1$ para algum $k \geq 0$.*

Demonstração. Por hipótese, G possui um subgrupo normal p-abeliano A de índice finito e G' é um p-grupo de período limitado $\leq p^j$ para algum $j \in \mathbb{N}$.

Pelo Lema 2.1.8, sabemos que $\mathbb{F}G$ satisfaz uma identidade polinomial. Assim, pelo Lema 2.3.11, $\Delta(A, A')$ é nil de expoente limitado.

Agora, pelo Lema 2.3.10, basta-nos verificar que $U(\mathbb{F}G/\Delta(G, G'))$ satisfaz uma identidade de grupo. Mas, $\mathbb{F}G/\Delta(G, G') \cong \mathbb{F}(G/G')$, que é comutativo, logo, $U(\mathbb{F}G/\Delta(G, G'))$ satisfaz uma identidade de grupo. □

CAPÍTULO 3

A Conjectura de Brian Hartley: Caso Geral

No capítulo anterior, foram estudados dois problemas: A Conjectura de Brian Hartley Particular e a caracterização de grupos G tais que $U(\mathbb{F}G)$ satisfaz identidade de grupo. Uma questão que surge naturalmente no sentido de generalizar os resultados acima é saber se estes continuam válidos para corpos quaisquer, não apenas infinitos.

Neste capítulo, temos o objetivo de responder positivamente para esta questão. Para isso, seguiremos os artigos [12] e [13]. A estrutura deste capítulo é parecida com a anterior, a primeira seção será dedicada a introduzir resultados auxiliares para a Conjectura de Brian Hartley, enquanto a segunda seção será devotada à demonstração do mesmo. Na terceira seção, encontraremos condições necessárias e suficientes para um grupo G tal que $U(\mathbb{F}G)$ satisfaça uma identidade de grupo.

3.1 Identidades Polinomiais Generalizadas em Álgebras de Grupo

Um lema importante utilizado no capítulo anterior foi o Lema 2.1.5. Tal resultado não continua verdadeiro para corpos finitos, pois, dados G um grupo finito que não é p-abeliano e $\mathbb{F}$ corpo finito, $U(\mathbb{F}G)$ é grupo finito, logo, satisfaz identidade de grupo.

Assim, um dos objetivos desta seção é obter resultados que nos permitam contornar o uso de tal lema. Ainda, mostraremos que, se as unidades de uma álgebra de grupo satisfazem uma identidade de grupo e a álgebra satisfaz uma identidade polinomial generalizada, então a álgebra satisfaz identidades polinomiais.

Comecemos com a seguinte observação:

Um anel R é dito *localmente artiniano* se todo subconjunto finito $X \subset R$ está contido em um subanel artiniano de R.

Lema 3.1.1. *Sejam R um anel localmente artiniano e $U(R)$ satisfazendo $w = 1$. Se S é qualquer subanel de R ou $\bar{R}$ qualquer imagem homomorfa de R, então $U(S)$ e $U(\bar{R})$ também satisfazem $w = 1$.*

Demonstração. O resultado para $U(S)$ é claro pois $U(S) \subset U(R)$. Para $\bar{R}$, é suficiente mostrar que o homomorfismo induzido

$$U(R) \to U(\bar{R})$$

é sobrejetor. Para isso, seja $a \in R$ tal que $\bar{a} \in U(\bar{R})$. Seja ainda $b \in R$ tal que $\bar{b}$ é o inverso de $\bar{a}$. Então a e b estão em um subanel artiniano E de R, pois R é localmente artiniano. O subanel E está nas condições do Lema 1.6.7, logo, para todo ideal I de E, a aplicação natural $U(E) \to U(E/I)$ é sobrejetora. Observemos que $\bar{E} \cong E/I$ para algum I, logo, $U(\bar{E}) \cong U(E/I)$ e assim, $U(E) \to U(\bar{E})$ é sobrejetora. Mas $\bar{a} \in U(\bar{E})$, logo, existe $c \in U(E) \subset U(R)$ tal que $c \mapsto \bar{a}$. □

Lema 3.1.2. *Sejam R uma $\mathbb{F}$-álgebra e I um ideal à direita de R. Se I satisfaz uma identidade polinomial de grau k e $I^k \neq 0$, então R satisfaz uma identidade polinomial generalizada.*

Demonstração. Por um processo de linearização, I satisfaz uma identidade polinomial multilinear de grau $s \leq k$:

$$g(x_1, \ldots, x_s) = \sum_{\sigma \in S_s} \alpha_\sigma x_{\sigma(1)} \ldots x_{\sigma(s)}.$$

onde $\alpha_\sigma \in \mathbb{F}$ e $\alpha_1 \neq 0$. Como $I^s \neq 0$, existem $a_1, \ldots, a_s \in I$ tal que $a_1 \ldots a_s \neq 0$. Assim,

$$\sum_{\sigma \in S_s} \alpha_\sigma a_{\sigma(1)} x_{\sigma(1)} a_{\sigma(2)} x_{\sigma(2)} \ldots a_{\sigma(s)} x_{\sigma(s)}$$

é uma identidade polinomial multilinear generalizada para R. □

O próximo resultado, apesar do caráter técnico, tem grande utilidade para os próximos lemas. Seja $\mathbb{F}_0$ o subcorpo de $\mathbb{F}$ gerado pela unidade 1. Se $\mathbb{F}$ é infinito, não é difícil ver que $\mathbb{F}_0 \cong \mathbb{Q}$ e se $\mathbb{F}$ é finito, $\mathbb{F}_0 \cong \mathbb{Z}_p$ para algum p primo.

Lema 3.1.3. *Seja R uma $\mathbb{F}$-álgebra e suponha que $U(R)$ satisfaz $w = 1$. Então existe um polinômio $f(x)$ sobre $\mathbb{F}_0$ de grau d determinado por w tal que se $a, b \in R$ e $a^2 = b^2 = 0 \Rightarrow f(ab) = 0$.*

Demonstração. Pelo Lema 1.8.19, podemos assumir que $U(R)$ satisfaz uma identidade da forma

$$w_0(x_1, x_2) = x_1^{\alpha_1} x_2^{\beta_1} \ldots x_1^{\alpha_s} x_2^{\beta_s} = 1$$

onde α_i, β_j são inteiros não nulos e $\alpha_1 < 0$, $\beta_s > 0$. Trocando x_1 por $x_2x_1^{-1}$ e x_2 por $x_1^{-1}x_2$, a identidade de grupo $w_0 = 1$ se torna

$$w_1(x_1, x_2) = x_1^{\gamma_1}x_2^{\delta_1} \dots x_1^{\gamma_k}x_2^{\delta_k} = 1$$

onde $\gamma_i, \delta_j \in \{\pm 1, \pm 2\}$ e $\gamma_1 = \delta_k = 1$.

Se $char(\mathbb{F}) \neq 2$, seja h o seguinte polinômio em duas variáveis:

$$\begin{aligned} h(x_1, x_2) &= (1 + \gamma_1 x_1)(1 + \delta_1 x_2) \dots (1 + \gamma_k x_1)(1 + \delta_k x_2) - 1 \\ &= h_0(x_1, x_2) + g_{11}(x_1, x_2) + g_{12}(x_1, x_2) + g_{21}(x_1, x_2) + g_{22}(x_1, x_2) \end{aligned}$$

onde $h_0(x_1, x_2)$ é a soma dos monômios que contém x_1^2 ou x_2^2 e $g_{ij}(x_1, x_2)$ é a soma dos monômios que começam em x_i e terminam em x_j, com $i, j \in \{1, 2\}$. Note que todo monômio em $g_{12}(x_1, x_2)$ é da forma $x_1x_2 \dots x_1x_2 = (x_1x_2)^n$ para algum n e o coeficiente do termo de maior grau de $h(x_1, x_2)$ está em $g_{12}(x_1, x_2)$, sendo $\gamma_1\delta_1 \dots \gamma_k\delta_k \neq 0$ pois a característica do corpo não é 2.

Dessa forma, podemos escrever

$$x_2 g_{12}(x_1, x_2)x_1 = f(x_2x_1)$$

para algum polinômio $f(x)$ sobre $\mathbb{F}_0$ de grau $d = k + 1$. Observemos que f é determinada por $h(x_1, x_2)$ e logo por w.

Agora, se $a^2 = b^2 = 0$, então $(1 + a)$ e $(1 + b)$ são unidades de R. Ainda, $(1 + a)^n = 1 + na$ para todo $n \in \mathbb{Z}$. Logo, $w_1(1 + b, 1 + a) = 1$, e assim,

$$\begin{aligned} 0 &= a(w_1(1 + b, 1 + a) - 1)b \\ &= a((1 + b)^{\gamma_1}(1 + a)^{\delta_1} \dots (1 + b)^{\gamma_k}(1 + a)^{\delta_k} - 1)b \\ &= a((1 + \gamma_1 b)(1 + \delta_1 a) \dots (1 + \gamma_k b)(1 + \delta_k a) - 1)b \\ &= ah(b, a)b \\ &= a(h_0(b, a) + g_{11}(b, a) + g_{12}(b, a) + g_{21}(b, a) + g_{22}(b, a))b. \end{aligned}$$

Observemos que, $ah_0(b, a)b = 0$, pois cada termo de h_0 possui a^2 ou b^2 como fator. Ainda,

$$a(g_{21}(b, a) + g_{22}(b, a))b = 0$$

pois cada termo de g_{21} ou g_{22} começa com a, e $ag_{11}(b, a)b = 0$ pois cada termo de g_{11} termina em b.

Portanto, $f(ab) = ag_{12}(b, a)b = 0$.

Se $char(\mathbb{F}) = 2$, trocamos x_1 por x_1x_2 e x_2 por x_1x_3, e assim a identidade de grupo $w_1 = 1$ se torna

$$w_2(x_1, x_2, x_3) = (x_1x_2)^{\gamma_1}(x_1x_3)^{\delta_1} \dots (x_1x_2)^{\gamma_k}(x_1x_3)^{\delta_k} = 1$$

onde $\gamma_1 = \delta_k = 1$. Reduzindo, temos:

$$w_3(x_1, x_2, x_3) = z_1^{\eta_1} z_2^{\eta_2} \dots z_r^{\eta_r}$$

onde $z_i \in \{x_1, x_2, x_3\}$, $z_i \neq z_{i+1}$ e $\eta_i \in \{\pm 1\}$. Ainda, $z_1 = x_1$, $z_r = x_3$ e $\eta_1 = \eta_r = 1$.

Defina um polinômio h em duas variáveis por:

$$h(x_1, x_2) = (1 + t_1)(1 + t_2) \dots (1 + t_r) - 1$$

onde

$$t_i = \begin{cases} x_1 x_2 x_1, & \text{se } z_i = x_1 \\ x_2 x_1 x_2 x_1 x_2, & \text{se } z_i = x_2 \\ (x_1 + x_2 x_1) x_2 (x_1 + x_1 x_2), & \text{se } z_i = x_3 \end{cases}$$

Em particular, $t_1 = x_1 x_2 x_1$ e $t_r = (x_1 + x_2 x_1) x_2 (x_1 + x_1 x_2)$. Agora, escreva h da mesma forma que no caso anterior,

$$h = h_0 + g_{11} + g_{12} + g_{21} + g_{22}.$$

Olhando o monômio $t_1 t_2 \dots t_r$, vemos que $g_{12} \neq 0$, e assim, $x_2 g_{12}(x_1, x_2) x_1 = f(x_2 x_1)$ para algum polinômio não nulo $f(x) \in \mathbb{F}_0[x]$. Novamente, $f(x)$ é determinada por $h(x_1, x_2)$ e, logo, por w.

Agora, como $(bab)^2 = (ababa)^2 = ((b + ab)a(b + ba))^2 = 0$, segue que $1 + bab$, $1 + ababa$ e $1 + (b + ab)a(b + ba) \in U(R)$. Note que $(1 + c)^{-1} = 1 - c = 1 + c$ para todo $c \in R$ tal que $c^2 = 0$, pois a característica do corpo é 2. Logo,

$$w_3(1 + bab, 1 + ababa, 1 + (b + ab)a(b + ba)) = 1$$

e assim,

$$\begin{aligned} 0 &= a(w_3(1 + bab, 1 + ababa, 1 + (b + ab)a(b + ba)) - 1)b \\ &= a(z_1^{\eta_1} z_2^{\eta_2} \dots z_r^{\eta_r} - 1)b \\ &= a(h(b, a))b \\ &= a(h_0(b, a) + g_{11}(b, a) + g_{12}(b, a) + g_{21}(b, a) + g_{22}(b, a))b. \end{aligned}$$

Argumentando como no caso anterior, temos que $f(ab) = a g_{12}(b, a) b = 0$. □

Para o restante do trabalho, fixemos d como a constante encontrada no lema anterior. Temos então:

Lema 3.1.4. *Seja R uma $\mathbb{F}$-álgebra e suponha que $U(R)$ satisfaz $w = 1$. Sejam $a, b \in R$ tal que $a^2 = b^2 = 0$. Assim,*

a) Se $|\mathbb{F}| > d$, então $(ab)^d = 0$.

b) Se ab é nilpotente, então $(ab)^d = 0$.

Demonstração. a) Para todo $\lambda \in \mathbb{F}$, $(\lambda a)^2 = b^2 = 0$. Pelo Lema 3.1.3, existe $f(x) \in \mathbb{F}_0[x]$ de grau d tal que $f(\lambda ab) = 0$. Sendo

$$f(x) = \sum_{i=0}^{d} a_i x^i$$

onde $a_d \neq 0$, então

$$a_d(ab)^d\lambda^d + \cdots + a_1 ab\lambda + a_0 = 0 \quad \forall \lambda \in \mathbb{F}.$$

Se $|\mathbb{F}| > d$, existem $\lambda_1, \ldots, \lambda_{d+1} \in \mathbb{F}$ distintos dois a dois tal que

$$\begin{bmatrix} 1 & \lambda_1 & \ldots & \lambda_1^d \\ 1 & \lambda_2 & \ldots & \lambda_2^d \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_{d+1} & \ldots & \lambda_{d+1}^d \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 ab \\ \vdots \\ a_d(ab)^d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Como a matriz acima é uma matriz de Vandermonde de determinante não nulo, $a_0 = a_1 ab = \cdots = a_d(ab)^d = 0$, e assim, $(ab)^d = 0$.

b) Novamente pelo Lema 3.1.3, existe $f(x) \in \mathbb{F}[x]$ de grau d tal que $f(ab) = 0$. Como ab é elemento algébrico de R, seja $g(x)$ o polinômio minimal de ab sobre $\mathbb{F}$. Logo, $g(x) = x^k$ para algum k, pois ab é nilpotente. Ainda, $g(x)|f(x)$, e assim, $k \leq d$. Portanto, $(ab)^d = 0$ pois $0 = (ab)^k = g(ab)$. □

Considerando a álgebra de matrizes $\mathbb{M}_n(\mathbb{F})$, $n \geq 2$, se $U(\mathbb{M}_n(\mathbb{F}))$ satisfaz $w = 1$, com os resultados anteriores é possível obter limitantes superiores para o tamanho do corpo $\mathbb{F}$ e para a ordem das matrizes, baseada na constante d encontrada no Lema 3.1.3.

Lema 3.1.5. *Seja $\mathbb{F}$ um corpo. Se $U(\mathbb{M}_n(\mathbb{F}))$ satisfaz $w = 1$ e $n \geq 2$ então:*

a) $|\mathbb{F}| \leq d$*, ou seja, $\mathbb{F}$ é finito.*

b) $n < 2\log_{|\mathbb{F}|} d + 2 \leq 2\log_2 d + 2$.

Demonstração. a) Sejam $a = e_{12}$ e $b = e_{21}$, logo $a^2 = b^2 = 0$. Como $e_{11} = ab$ não é nilpotente, pelo Lema 3.1.4, $|\mathbb{F}| \leq d$.

b) Agora, seja s o menor inteiro positivo tal que $|\mathbb{F}|^s > d$. Então $|\mathbb{F}|^{s-1} \leq d < |\mathbb{F}|^s$.

Seja $\mathbb{E}$ um corpo finito tal que $[\mathbb{E} : \mathbb{F}] = s$, ou seja, $\mathbb{E}$ é um $\mathbb{F}$-espaço vetorial de dimensão s. Então $|\mathbb{E}| = |\mathbb{F}|^s > d$. Não é difícil ver que tal corpo existe, veja por exemplo, [14]. Como $\mathbb{E}$ age em si mesmo por multiplicação à direita, temos,

$$\mathbb{E} \hookrightarrow End_{\mathbb{F}}(\mathbb{E}) \cong \mathbb{M}_s(\mathbb{F})$$

Logo, $\mathbb{M}_{2s}(\mathbb{F}) = \mathbb{M}_2(\mathbb{M}_s(\mathbb{F})) \supset \mathbb{M}_2(\mathbb{E})$.

Se $n \geq 2s$, então $U(\mathbb{M}_{2s}(\mathbb{F}))$ satisfaz $w = 1$ por hipótese, e logo $U(\mathbb{M}_2(\mathbb{E}))$ também, mas $\mathbb{M}_2(\mathbb{E})$ é uma álgebra sobre $\mathbb{E}$ e $|\mathbb{E}| > d$, contradizendo (i). Assim, $n < 2s$ e, como $s-1 \leq \log_{|\mathbb{F}|} d$,

temos:

$$\begin{aligned} n &< 2(\log_{|\mathbb{F}|} d + 1) \\ &= 2\log_{|\mathbb{F}|} d + 2 \\ &\leq 2\log_2 d + 2 \end{aligned}$$

. □

Com o lema acima, temos o seguinte resultado, uma versão da Conjectura de Brian Hartley para p'-grupos localmente finitos.

Lema 3.1.6. *Sejam $\mathbb{F}$ um corpo de característica $p \geq 0$ e G um p'-grupo localmente finito. Se $U(\mathbb{F}G)$ satisfaz $w = 1$, então $\mathbb{F}G$ satisfaz o polinômio standard s_{2m} para algum inteiro m determinado por w.*

Demonstração. Seja m um inteiro maior do que $2\log_2 d + 2$. Tomemos $\alpha_1, \ldots, \alpha_{2m}$ elementos de $\mathbb{F}G$ e H o subgrupo de G gerado pelos seus suportes. Assim H é finito e $\mathbb{F}H$ é artiniano por ser álgebra de dimensão finita. Ainda, H não contém p-elementos, logo, pelo Teorema de Maschke, $\mathbb{F}H$ é semiprima, e sendo de dimensão finita, é semisimples. Assim, por Wedderburn-Artin,

$$\mathbb{F}H = \bigoplus_{i=1}^{r} \mathbb{M}_{n_i}(D_i)$$

onde D_i são $\mathbb{F}$-álgebras de divisão.

Certamente, cada $U(D_i)$ satisfaz $w = 1$ e $[D_i : Z_i] \leq [D_i : \mathbb{F}] < \infty$ onde Z_i denota o centro de D_i. Pelo Lema 2.1.4, D_i tem de ser comutativo, caso contrário $U(D_i)$ teria um subgrupo livre, não satisfazendo a identidade $w = 1$. Agora, cada $U(\mathbb{M}_{n_i}(D_i))$ satisfaz $w = 1$, logo, o Lema 3.1.5 nos diz que $n_i \leq m$. Assim, $\mathbb{F}H$ satisfaz $s_{2m} = 0$. Mas $\alpha_1, \ldots, \alpha_{2m} \in \mathbb{F}H$, ou seja, $s_{2m}(\alpha_1, \ldots, \alpha_{2m}) = 0$, e portanto, $\mathbb{F}G$ satisfaz $s_{2m} = 0$. □

O próximo resultado, além de ser de grande interesse, será fundamental na demonstração da Conjectura de Brian Hartley.

Lema 3.1.7. *Seja G um grupo de torção. Se $U(\mathbb{F}G)$ satisfaz $w = 1$ e $\mathbb{F}G$ satisfaz uma GPI, então $\mathbb{F}G$ satisfaz uma identidade polinomial.*

Demonstração. Seja ϕ o FC-subgrupo de G. Pelo Lema 2.1.9, $[G : \phi] < \infty$ e $|\phi'| < \infty$. Ainda, como G é de torção, segue do Lema 1.1.13 que G é localmente finito.

Seja

$$C = C_\phi(\phi') = \{g \in \phi : gh = hg \forall h \in \phi'\}.$$

Observemos que $\phi' \lhd \phi$, e podemos tomar o seguinte homomorfismo:

$$\begin{array}{rccccc} \varphi: & \phi & \to & Aut(\phi') & & \\ & g & \mapsto & \varphi_g: & \phi' & \to & \phi' \\ & & & & h & \mapsto & ghg^{-1} \end{array}$$

onde $Aut(\phi')$ indica o grupo dos automorfismos em ϕ'.

Assim, $Ker\varphi = C_\phi(\phi')$. Logo,

$$\frac{\phi}{C_\phi(\phi')} \cong S \subset Aut(\phi').$$

Como ϕ' é finito, $Aut(\phi')$ também é, e assim, $|\frac{\phi}{C_\phi(\phi')}| < \infty$, ou seja, $[\phi : C_\phi(\phi')] < \infty$.

Agora, $C' \subset Z(C)$, pois, como $C < \phi$, então $C' < \phi'$, e portanto, dados $(g,h) \in C'$, $k \in C$, em particular, $(g,h) \in \phi'$ e

$$(g,h)k = k(g,h)$$

por definição de C. Logo, $C' \subset Z(C)$.

Por [2, Teorema 8, p. 194], observamos que C é nilpotente, e tomando P o conjunto dos p-elementos em C, $P \lhd C$.

Então, temos que C é localmente finito (pois G é), $U(\mathbb{F}C)$ satisfaz $w = 1$ e P é p-subgrupo normal de C, logo, pelo Lema 2.3.7, $U(\mathbb{F}(C/P))$ satisfaz $w = 1$.

Agora, por [11, Lema 1.2.8], $\mathbb{F}(C/P)$ satisfaz uma identidade polinomial. Assim, o Lema 2.1.8 nos diz que C/P possui um subgrupo p-abeliano, A/P de índice finito.

Mas C/P é um p'-grupo, logo, $(A/P)'$ ser um p-grupo significa que $(A/P)' = P$, ou seja, A/P é abeliano. Agora,

$$[G : A] = \underbrace{[G : \phi]}_{<\infty}\underbrace{[\phi : C]}_{<\infty}\underbrace{[C : A]}_{<\infty} < \infty.$$

Por fim, $A' \subset P$ e $A' \subset \phi'$ (pois $A \subset \phi$). Logo, A é um subgrupo p-abeliano de índice finito, e dessa forma, $\mathbb{F}G$ satisfaz uma identidade polinomial. □

Lema 3.1.8. *Seja R uma álgebra sobre um corpo $\mathbb{F}$ e $U(R)$ satisfazendo $w = 1$. Se $a, b, c \in R$ tal que $a^2 = bc = 0$, então todos os elementos de $bacR$ satisfazem um polinômio $g(x) \in \mathbb{F}_0[x]$ de grau $d + 1$.*

Demonstração. Para qualquer $r \in R$, $a^2 = (crb)^2 = 0$. Pelo Lema 3.1.3, existe $f(x) \in \mathbb{F}_0[x]$ de grau d tal que $f(acrb) = 0$. Seja $g(x) = xf(x)$. Então

$$g(bacr) = bacrf(bacr) = bf(acrb)acr = 0.$$

□

3.2 Resultado Principal

Nesta seção, provamos a Conjectura de Brian Hartley, seguindo de perto a demonstração dada em [12]. Assim como na Seção 2.2, dividimos a prova em três casos: $N = 0$, $N \neq 0$

nilpotente e $N \neq 0$ nil, mas não nilpotente, onde N é o ideal soma de todos os ideais nilpotentes de $\mathbb{F}G$.

Teorema 3.2.1. *Sejam $\mathbb{F}$ um corpo de característica $p \geq 0$ e G um grupo de torção. Suponha que $\mathbb{F}G$ seja uma álgebra de grupo semiprima. Se $U(\mathbb{F}G)$ satisfaz $w = 1$, então $\mathbb{F}G$ satisfaz uma identidade polinomial.*

Demonstração. Fixemos $k = d+1$, onde d é a constante encontrada no Lema 3.1.3. Temos dois casos:

- Existem $a, b, c \in \mathbb{F}G$ tal que $a^2 = bc = 0$ e $(bac\mathbb{F}G)^k \neq 0$.
- Para todo $a, b, c \in \mathbb{F}G$ tal que $a^2 = bc = 0$, $(bac\mathbb{F}G)^k = 0$.

Para o primeiro caso, o Lema 3.1.8 nos diz que $bac\mathbb{F}G$ satisfaz uma identidade polinomial de grau k. Pelo Lema 3.1.2, $\mathbb{F}G$ satisfaz uma GPI, e agora o Lema 3.1.7 nos diz que $\mathbb{F}G$ satisfaz uma identidade polinomial.

Para o segundo caso, vamos seguir a demonstração do Teorema 2.2.1, fazendo pequenas alterações. Como $\mathbb{F}G$ é semiprima, $bac = 0$. Pelo Lema 2.1.3, todo idempotente de $\mathbb{F}G$ é central e se $a, b, c \in \mathbb{F}G$ tal que a é nilpotente e $bc = 0$, então $bac = 0$.

Sejam P o conjunto dos p-elementos e Q o conjunto dos p'-elementos de G. Se $p = 0$, $P = \{1\}$. Suponha que $p > 0$. Tome $h \in P$ e escreva $\hat{h} = 1 + h + h^2 + \ldots h^{|h|-1}$. Para qualquer $g \in P$, $g - 1$ é nilpotente, e $(h-1)\hat{h} = 0$. Logo, $0 = (h-1)(g-1)\hat{h} = (h-1)g\hat{h}$. Segue que $hg\hat{h} = g\hat{h}$ e $g = hgh^i$ para algum i. Logo, $g^{-1}hg = h^{-i}$, e assim, vemos que P é subgrupo e $\langle h \rangle \lhd P$.

Agora, para qualquer $h \in P$, $g \in Q$, $h - 1$ é nilpotente como vimos acima e $(g-1)\hat{g} = 0$. Logo $(g-1)(h-1)\hat{g} = 0$. Como anteriormente, $h = ghg^j$ para algum j e $h^{-1}gh = g^{-j}$.

Notemos que

$$(g,h) = \underbrace{g^{-1}h^{-1}g}_{\in P} h = g^{-j-1} \in P \cap Q = \{1\}$$

pois $P \lhd G$.

Assim como na demonstração do Teorema 2.2.1, $\langle h \rangle \lhd G$, mas pelo Lema 2.1.7, $h = 1$, logo, $P = \{1\}$.

Mostremos agora que Q é um subgrupo abeliano. Sendo $char(\mathbb{F}) = p \geq 0$, tome qualquer $x \in Q$ com ordem m. Como $m \neq 0$ em $\mathbb{F}$, $e = \hat{x}/m$ é um elemento idempotente. Como todo idempotente é central, $\forall g \in G$, $\hat{x}g = g\hat{x}$, e assim, $xg = gx^i$ para algum i. Com isso, mostra-se que Q é grupo e $\langle x \rangle \lhd G$. Assim, Q é abeliano ou hamiltoniano. Suponhamos que Q seja hamiltoniano. Logo, Q contém uma cópia de K_8. Notemos que Q é um p'-grupo e consequentemente K_8. Logo, $\mathbb{F}K_8$ é semiprimo pelo Teorema de Maschke e por Wedderburn-Artin, podemos decompô-lo como

$$\mathbb{F}K_8 = \bigoplus \mathbb{M}_{n_i}(D_i).$$

Sabemos que todo idempotente é central, logo cada $n_i = 1$. De fato, se algum $n_j \geq 2$, existiria uma matriz

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

tal que $A^2 = A$, porém A não é central. Ainda, pelo Lema 2.1.4, cada D_i é comutativo. Portanto, $\mathbb{F}K_8$ é comutativo, absurdo. Logo, $G = Q$ é abeliano, e $\mathbb{F}G$ satisfaz s_2. □

Teorema 3.2.2. *Sejam $\mathbb{F}$ um corpo de característica $p > 0$ e G grupo de torção. Se N é nilpotente e $U(\mathbb{F}G)$ satisfaz $w = 1$, então $\mathbb{F}G$ satisfaz uma identidade polinomial.*

Demonstração. Como N é nilpotente, podemos tomar subgrupos S e H de G, tal como na Proposição 2.1.11. Agora, como G é de torção e $\phi_p(H) = S$ é um p-grupo finito, logo

$$\phi(H/S) = \frac{\phi(H)}{\phi_p(H)}$$

é um p'-grupo e assim $\mathbb{F}(H/S)$ é semiprimo.

Como S é um p-grupo finito, pelo Lema 2.3.7, segue que $U(\mathbb{F}(H/S))$ satisfaz $w = 1$. Assim, o Teorema 3.2.1 garante que $\mathbb{F}(H/S)$ satisfaz uma identidade polinomial, ou seja, pelo Lema 2.1.8, H/S possui um subgrupo p-abeliano A/S de índice finito. Note que A' é um p-grupo finito e $[G : H] < \infty$. Logo, A é subgrupo p-abeliano de G de índice finito, ou seja, $\mathbb{F}G$ satisfaz uma identidade polinomial. □

Teorema 3.2.3. *Sejam $\mathbb{F}$ corpo de característica $p > 0$ e G um grupo de torção. Se N não é nilpotente e $U(\mathbb{F}G)$ satisfaz $w = 1$, então $\mathbb{F}G$ satisfaz uma identidade polinomial.*

Demonstração. Seguimos basicamente a mesma demonstração do Teorema 2.2.3.

Sejam t uma outra indeterminada e $\mathbb{F}\langle X\rangle[[t]]$ o anel das séries de potências sobre a álgebra livre $\mathbb{F}\langle X\rangle$, onde $X = \{x_1, x_2, \dots\}$.

Para qualquer n, os elementos $1 + x_1t, 1 + x_2t, \dots, 1 + x_nt$ são unidades em $\mathbb{F}\langle X\rangle[[t]]$, e geram um subgrupo livre no anel das séries de potências pelo Argumento de Magnus. Em particular, se a identidade de grupo w é uma palavra em n variáveis, então

$$w(1 + x_1t, 1 + x_2t, \dots, 1 + x_nt) \neq 1.$$

Segue que temos uma expressão da forma:

$$\sum_{i\geq 1} f_i(x_1, \dots, x_n)t^i \neq 0$$

onde $f_i \in \mathbb{F}\langle X\rangle$ é um polinômio homogêneo de grau i. Logo, existe um menor inteiro $s \geq 1$ tal

que $f_s(x_1, \ldots, x_n) \neq 0$, e podemos escrever

$$\sum_{i \geq s} f_i(x_1, \ldots, x_n) t^i \neq 0.$$

Suponhamos agora que $I^n = 0$ para todo ideal nilpotente I de $\mathbb{F}G$. Sejam $a_1, \ldots, a_n \in N$.

Então existem finitos ideais nilpotentes $I_1, \ldots, I_j$ tal que $\{a_1, \ldots, a_n\} \subset J = \sum I_i$. J é nilpotente por ser soma finita de ideais nilpotentes, logo, $J^n = 0$. Segue que $a_1 a_2 \ldots a_n = 0$ e $N(\mathbb{F}G)$ é nilpotente, contradição. Logo, podemos encontrar um ideal nilpotente I de $\mathbb{F}G$ tal que $I^r \neq 0$ e $I^{r+1} = 0$, para algum $r > s$.

Para quaisquer $a_1, \ldots, a_n, a_{n+1} \in I$, $1 + a_1, \ldots, 1 + a_n$ são unidades em $\mathbb{F}G$. Logo, temos

$$0 = w(1 + a_1, \ldots, 1 + a_n) - 1 = \sum_{i=s}^{r} f_i(a_1, \ldots, a_n)$$

pois $I^{r+1} = 0$.

Logo,

$$0 = \sum_{i=s}^{r} f_i(a_1, \ldots, a_n) a_{n+1}^{r-s}.$$

Para $i \geq s + 1$, $f_i(a_1, \ldots, a_n) a_{n+1}^{r-s} = 0$ pois $f_i(x_1, \ldots, x_n) x_{n+1}^{r-s}$ é polinômio homogêneo de grau $i + r - s \geq r + 1$ e $I^{r+1} = 0$. Logo,

$$f_s(a_1, \ldots, a_n) a_{n+1}^{r-s} = 0$$

ou seja, $f_s(x_1, \ldots, x_n) x_{n+1}^{r-s}$ é uma identidade polinomial de grau r para I. Ainda $I^r \neq 0$, logo, pelo Lema 3.1.2, $\mathbb{F}G$ satisfaz uma GPI e portanto uma identidade polinomial pelo Lema 3.1.7. □

3.3 Caracterização dos Grupos G tais que $U(\mathbb{F}G)$ satisfaz uma Identidade de Grupo

No capítulo 2, com a hipótese de $\mathbb{F}$ ser corpo infinito, U satisfazer identidades de grupo implicava, em particular, que G' era um p-grupo, onde p é a característica do corpo $\mathbb{F}$. Neste caso geral, isto não é necessariamente verdade, e para isso, temos de estudar os elementos de G' quando este não for um p-grupo.

Seja m o menor inteiro maior ou igual a $2\log_2 d + 2$, onde d é a constante encontrada no Lema 3.1.3, e defina

$$T = \prod_{|\mathbb{F}| \leq d} |U(\mathbb{M}_m(\mathbb{F}))|.$$

Certamente, T é finito, uma vez que os corpos são finitos.

Lema 3.3.1. *Seja x um p'-elemento em G', $x \neq 1$, e seja $y \neq 1$ um p'-elemento em um p'-subgrupo normal de G. Se $U(\mathbb{F}G)$ satisfaz $w = 1$, então $y^T = 1$.*

Demonstração. Suponhamos por absurdo que $y^T \neq 1$. Como $x \in G'$, podemos escrever

$$x = (x_1, y_1)(x_2, y_2)\dots(x_n, y_n) \neq 1.$$

Note que $x^{-1}y^T$ é um p'-elemento pois y está em um p'-subgrupo normal de G. De fato, sabemos que $p \nmid |x|$, $p \nmid |y|$ e

$$\begin{aligned}(x^{-1}y^T)^{|x||y|} &= x^{-1}y^T x^{-1}y^T \dots x^{-1}y^T \\ &= (x^{-1})^{|x||y|}y^l \qquad \text{onde } l \geq |x||y| \\ &= y^l\end{aligned}$$

Logo, $|x^{-1}y^T|$ divide $|x||y|^2$, e portanto, $p \nmid |x^{-1}y^T|$.

Se $x \neq y^T$, seja

$$\alpha = (1 - x^{-1})(1 - y^T)$$

então α não é nilpotente por [18, Lema 2.3.3]. Se $x = y^T$, seja $\alpha = 1 - x$, que também não é nilpotente por [18, Lema 2.3.3]. Observe que $H = \langle x_1, y_1, \dots, x_n, y_n, y\rangle$ é subgrupo finito de G, pois G é localmente finito.

Se $\mathbb{F}$ é infinito, então G' é p-grupo pelo Lema 2.3.1, o que é absurdo, logo $\mathbb{F}$ é finito. Seja $J = J(\mathbb{F}H)$ o radical de Jacobson de $\mathbb{F}H$. Assim, pela Proposição 1.6.6, $\mathbb{F}H/J = \oplus\mathbb{M}_{n_i}(D_i)$, mas como D_i é álgebra de divisão finita, é corpo pelo Teorema de Wedderburn, logo,

$$\frac{\mathbb{F}H}{J} = \oplus\mathbb{M}_{n_i}(\mathbb{F}_i).$$

Agora, como α não é nilpotente, $\alpha + J$ não é o elemento neutro em $\mathbb{F}H/J$. Logo, existe uma aplicação natural

$$\theta : \frac{\mathbb{F}H}{J} \to \mathbb{M}_{n_j}(\mathbb{F}_j)$$

tal que $\theta(\alpha + J) \neq 0$. Dessa forma, $\theta(1 - x^{-1} + J) \neq 0$ e assim $\theta(1 - x + J) \neq 0$, pois se $\theta(1 - x + J) = 0$, então $0 = \theta(1 - x + J)\theta(-x^{-1} + J) = \theta(1 - x^{-1} + J)$.

Se $n_j = 1$, então

$$\begin{aligned}\theta(x + J) &= \textstyle\prod_{i=1}^{n} \theta((x_i, y_i) + J) \\ &= \textstyle\prod_{i=1}^{n} (\theta(x_i + J), \theta(y_i + J)) \\ &= 1\end{aligned}$$

pois $\mathbb{F}_j$ é corpo. Mas assim, $\theta(1 - x + J) = \theta((1 + J) - (x + J)) = 1 - 1 = 0$, absurdo. Portanto, algum $n_j \geq 2$.

Pelo Lema 3.1.1, $U(\mathbb{F}H/J)$ satisfaz $w = 1$ e como a aplicação θ é sobrejetora, $U(\mathbb{M}_{n_j}(\mathbb{F}_j))$ satisfaz $w = 1$. Pelo Lema 3.1.5, $n_j \leq 2\log_2 d + 2 \leq m$ e $|\mathbb{F}_j| < d$.

Agora, observemos que

$$\theta(y+J)\theta(y^{-1}+J) = \theta(1+J) = 1$$

logo $\theta(y+J) \in U(\mathbb{M}_{n_j}(\mathbb{F}_j))$.

Mas, tomemos

$$\begin{array}{rccc} \varphi: & U(\mathbb{M}_{n_j}(\mathbb{F}_j)) & \hookrightarrow & U(\mathbb{M}_m(\mathbb{F}_j)) \\ & A & \mapsto & \begin{bmatrix} A & 0 \\ 0 & I_{m-n_j} \end{bmatrix} \end{array}$$

φ é um mergulho, e como o grupo $U(\mathbb{M}_m(\mathbb{F}_j))$ é finito,

$$\begin{aligned} 1 &= \theta(y+J)^{|U(\mathbb{M}_m(\mathbb{F}_j))|} \\ &= \theta(y+J)^T \\ &= \theta(y^T+J) \end{aligned}$$

e assim, $\theta(1-y^T+J) = 0$, ou seja, $\theta(\alpha+J) = 0$, absurdo. Nosso absurdo foi supor que $y^T \neq 1$. Logo, $y^T = 1$. □

Os próximos três resultados têm o propósito de mostrar que, se $U(\mathbb{F}G)$ satisfaz $w = 1$, então os p-elementos e os p'-elementos de G têm período limitado.

Lema 3.3.2. *Se $U(\mathbb{F}G)$ satisfaz $w = 1$ e G' não é um p-grupo, então os p'-elementos de G têm período limitado.*

Demonstração. Como $U(\mathbb{F}G)$ satisfaz $w = 1$, os Teoremas 3.2.1, 3.2.2 e 3.2.3 e o Corolário 2.1.8 implicam que G tem um subgrupo p-abeliano normal A de índice finito. Note que A' é um p-subgrupo finito normal de G. Ainda, (G/A') não é p-grupo, pois G' não é p-grupo e, pelo Lema 3.1.1, $U(\mathbb{F}(G/A'))$ satisfaz $w = 1$.

Agora, temos dois casos a considerar: Se A for abeliano ou não. Para demonstrar os dois casos é utilizado um mesmo processo, fazendo pequenas modificações em cada situação. Dessa forma, seria suficiente considerar o caso em que A é abeliano, para não carregar as notações. Neste resultado, vamos fazer os dois casos, a fim de deixar claro quais são as modificações necessárias, e nos próximos resultados, quando for necessário, consideraremos apenas um dos casos.

Se A for abeliano, podemos escrever $A = P \times Q$, onde P é o conjunto dos p-elementos e Q é o conjunto dos p'-elementos de A. Como A é subgrupo abeliano normal de G, P e Q são subgrupos normais de G. Agora, como A é subgrupo de índice finito de G, basta-nos limitar o período de Q. De fato, tomemos um elemento $x \in G$ p'-elemento. Como A é de índice finito, $G = A \cup g_1A \cup \cdots \cup g_kA$, ou seja, $x = g_ia$ com $i \in \{0, 1, \ldots k\}$ e $a \in A$. Logo, sendo

$r = |g_1||g_2|\dots|g_k|$,

$$\begin{aligned} x^r &= \underbrace{g_i a g_i a \dots g_i a}_{r \text{ vezes}} \\ &= g_i^r a^l \\ &= a^l \in A \end{aligned}$$

e como x é um p'-elemento, a^l também é p'-elemento, ou seja, $a^l \in Q$. Se Q tiver período limitado, digamos s, $x^{rs} = 1$ $\forall x \in G$ p'-elemento.

Portanto, nosso objetivo é mostrar que Q tem período limitado. Como G' não é p-grupo, existe um elemento $x \neq e$, p'-elemento em G'. Para qualquer $y \neq e$, $y \in Q$, pelo Lema 3.3.1, $y^T = 1$. Assim, Q possui período limitado e logo, os p'-elementos de G têm período limitado.

Se A não for abeliano, como $A' \lhd G$, tomemos o subgrupo A/A' de G/A', que é subgrupo abeliano normal de índice finito.

Escrevemos $A/A' = P \times Q$, onde P são os p-elementos de A/A' e Q os p'-elementos de A/A'. Como $A/A' \lhd G/A'$, P e Q também são subgrupos normais de G/A'. Da mesma forma como no caso anterior, basta-nos limitar o período de Q. Como $(G/A')'$ não é p-grupo, existe $xA' \neq A'$ p'-elemento em $(G/A')'$.

Para qualquer $yA' \neq A'$, $yA' \in Q$, $(yA')^T = A'$ pelo Lema 3.3.1. Assim, Q possui período limitado, e logo os p'-elementos de G/A' tem período limitado. Mas queremos mostrar que os p'-elementos de G têm período limitado. Assim, se $x \in G$ é p'-elemento, existe r tal que $(xA')^r = A'$, ou seja, $x^r \in A'$, mas como A' é p-grupo, então $x^r = 1$. □

Lema 3.3.3. *Se $U(\mathbb{F}G)$ satisfaz $w = 1$, então G' tem período limitado.*

Demonstração. Como na demonstração do Lema 3.3.2, podemos assumir que A é um subgrupo abeliano normal de índice finito de G. Assim, podemos escrever $A = P \times Q$, onde P é o conjunto dos p-elementos e Q o conjunto dos p'-elementos. Como A é subgrupo abeliano normal, P e Q são subgrupos normais de G.

Se G' for um p-grupo, façamos G/Q. Assim, A/Q é um p-subgrupo abeliano normal de índice finito de G/Q. Como $U(\mathbb{F}(G/Q))$ satisfaz $w = 1$, então pelo Lema 2.3.8, $(G/Q)'$ tem período limitado. Mas

$$\left(\frac{G}{Q}\right)' = \frac{G'Q}{Q}.$$

Assim, dado um gerador $x \in G'$, sendo r um limitante para o período de $(G/Q)'$, $(xQ)^r = Q$, ou seja, $x^r \in Q$, mas como Q é um p'-subgrupo, temos de ter $x^r = 1$.

Se G' não é um p-grupo, o Lema 3.3.1 nos diz que Q tem período limitado, logo, tomando novamente G/Q, A/Q é um p-subgrupo abeliano normal de índice finito. Como $U(\mathbb{F}(G/Q))$ satisfaz $w = 1$, pelo Lema 2.3.8, $(G/Q)'$ tem período limitado. Tomando $x \in G'$ como no caso anterior, e sendo r um limitante superior para o período de $(G/Q)'$, vemos que $x^r \in Q$. Mas como Q tem período limitado, existe s tal que $x^{rs} = 1$, logo G' tem período limitado. □

Lema 3.3.4. *Se $U(\mathbb{F}G)$ satisfaz $w = 1$ e G' não é um p-grupo, então os p-elementos de G tem período limitado.*

Demonstração. Como no Lema 3.3.2, podemos assumir que A é um subgrupo abeliano normal de índice finito de G e escrever $A = P \times Q$. Se $B = (P, G)$, então $B \lhd G$ e está contido em $P \cap G'$. Logo, pelo Lema 3.3.3, B é um p-grupo de período limitado. Assim, falta-nos analisar os outros p-elementos de G, e para isso podemos fazer o quociente G/B. Aqui podemos ter $B = \{1\}$ ou $B \neq \{1\}$. Como foi dito no Lema 3.3.2, vamos considerar apenas o caso $B = \{1\}$, ou seja, $P \subset Z(G)$. No Lema anterior, bastava-nos limitar o período de Q. De forma análoga, neste caso, basta-nos limitar o período de P.

Como G' não é um p-grupo, podemos encontrar um p'-elemento $x \in G'$, com

$$x = (x_1, y_1)(x_2, y_2)\dots(x_n, y_n) \neq 1.$$

Seja $H = \langle x_1, y_1, \dots, x_n, y_n \rangle$, então $x \in H'$ e H é finito pois G é localmente finito.

Se $C = H \cap P$, então C é p-subgrupo finito de G, e $C \lhd G$ pois P é central, logo de período limitado por ser finito. Assim, é suficiente agora considerarmos G/C, mas como observado anteriormente, podemos considerar $C = H \cap P = 1$.

Como G' não é p-grupo, pelo Teorema 2.3.1, $\mathbb{F}$ é corpo finito. Seja $J = J(\mathbb{F}H)$ e pela Proposição 1.6.6, escreva

$$\frac{\mathbb{F}H}{J} = \oplus \mathbb{M}_{n_i}(\mathbb{F}_i)$$

onde os $\mathbb{F}_i$'s são corpos, uma vez que $\mathbb{F}$ é finito.

Se todos os $n_i = 1$, então $\mathbb{F}H/J$ é comutativo, e como x é produto de comutadores, $x + J = 1 + J$. Agora, J é um ideal nil, então $x = 1 + j$, onde j é nilpotente com grau $k \in \mathbb{N}$. Seja l tal que $p^l > k$. Então

$$x^{p^l} = (1 + j)^{p^l} = 1$$

ou seja, x é um p-elemento, absurdo. Logo, existe algum $n_j \geq 2$.

Pela Proposição 1.6.6, $\mathbb{F}H$ contém uma cópia de $\mathbb{F}H/J$, e logo, uma cópia de $\mathbb{M}_{n_j}(\mathbb{F}_j)$, onde $n_j \geq 2$. Mas, observemos que é possível mergulhar $\mathbb{M}_2(\mathbb{F})$ em $\mathbb{M}_{n_j}(\mathbb{F}_j)$, uma vez que $\mathbb{F} \subset \mathbb{F}_j$. Assim, $\mathbb{F}H$ contém uma cópia de $\mathbb{M}_2(\mathbb{F})$.

Notemos que, como P é central e $P \cap H = \{1\}$, então $P \times H \cong PH$. Logo, por resultados básicos de Álgebra Tensorial, temos

$$\begin{aligned} \mathbb{M}_2(\mathbb{F}P) &\cong \mathbb{F}P \otimes_{\mathbb{F}} \mathbb{M}_2(\mathbb{F}) \\ &\hookrightarrow \mathbb{F}P \otimes_{\mathbb{F}} \mathbb{F}H \\ &\cong \mathbb{F}(P \times H) \\ &\cong \mathbb{F}PH \\ &\subset \mathbb{F}G. \end{aligned}$$

Como $U(\mathbb{F}G)$ satisfaz $w = 1$, $U(\mathbb{M}_2(\mathbb{F}P))$ também satisfaz $w = 1$. Se $y \in P$, então $(1-y)$ é nilpotente, pois P é p-grupo. Sejam

$$a = \begin{bmatrix} 0 & 1-y \\ 0 & 0 \end{bmatrix} \qquad \text{e} \qquad b = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Então, $a, b \in \mathbb{M}_2(\mathbb{F}P)$ e

$$ab = \begin{bmatrix} 1-y & 0 \\ 0 & 0 \end{bmatrix}$$

é nilpotente.

Pelo Lema 2.3.3, $(ab)^s = 0$ para algum inteiro positivo s. Fixe um inteiro k tal que $p^k \geq s$. Então $(ab)^{p^k} = 0$, ou seja, $(1-y)^{p^k} = 0$ e $y^{p^k} = 1$. Logo, P tem período limitado. □

Lema 3.3.5. *Sejam R um anel e I um ideal nil. Se $U(R)$ satisfaz a identidade de grupo $w = 1$, então $U(R/I)$ satisfaz a mesma identidade. Reciprocamente, se R tem característica prima p, I é nil de expoente limitado p^k, e $U(R/I)$ satisfaz a identidade $w = 1$, então $U(R)$ satisfaz $w^{p^k} = 1$.*

Demonstração. Suponha que $U(R)$ satisfaz $w(x_1, \ldots, x_n) = 1$ e tomemos $\bar{r_i} \in U(R/I)$, $1 \leq i \leq n$. Então, se $\bar{s_i} = (\bar{r_i})^{-1}$, tomemos seus representantes em R, r_i e s_i, respectivamente. Fazendo $u = r_i s_i - 1$, então $\bar{u} = 0$, ou seja, $u \in I$, e como I é nil, existe j inteiro positivo tal que $u^j = 0$. Logo,

$$r_i s_i (1 - u + u^2 - \cdots \pm u^{j-1}) = 1,$$

e similarmente r_i possui inverso à esquerda. Logo, cada $r_i \in U(R)$, e assim, $w(r_1, \ldots, r_n) = 1$, e portanto, $w(\bar{r_1}, \ldots, \bar{r_n}) = 1$.

Reciprocamente, se $r_1, \ldots, r_n \in U(R)$, então $w(\bar{r_1}, \ldots, \bar{r_n}) = 1$, ou seja, $w(r_1, \ldots, r_n) - 1 \in I$. Como I é nil, $(w(r_1, \ldots, r_n) - 1)^{p^k} = 0$, e o resultado segue. □

Lema 3.3.6. *Sejam G um grupo, e H um subgrupo de índice $n < \infty$. Sejam $g_1, \ldots, g_n$ uma transversal de H em G. Para qualquer corpo $\mathbb{F}$ e qualquer $\alpha \in \mathbb{F}G$, escreva $g_i\alpha = \sum_{j=1}^{n} \alpha_{ij} g_j$, com $\alpha_{ij} \in \mathbb{F}H$. Então a aplicação $\theta : \mathbb{F}G \to \mathbb{M}_n(\mathbb{F}H)$ dada por $\theta(\alpha) = (\alpha_{ij})$ é um mergulho de $\mathbb{F}$-álgebras.*

Demonstração. [11, Lema 1.3.12] □

Lema 3.3.7. *Sejam G um grupo e A um subgrupo abeliano normal de índice finito. Suponha que $char(\mathbb{F}) = p > 0$ e I é um ideal de $\mathbb{F}A$ tal que $g^{-1}\alpha g \in I$ para todo $\alpha \in I$ e todo $g \in G$. Se I é nil de expoente limitado no máximo p^k, então $I(\mathbb{F}G)$ é ideal nil de $\mathbb{F}G$ de expoente limitado no máximo np^k.*

Demonstração. [11, Lema 1.3.13] □

Com as observações acima, estamos em condições de demonstrar os resultados principais desta seção. Os dois teoremas seguintes caracterizam os grupos G tais que $U(\mathbb{F}G)$ satisfaz uma identidade de grupo. Esta caracterização foi dividida em dois casos, sendo G' p-grupo ou não. O primeiro teorema é análogo ao Teorema 2.3.1

Teorema 3.3.8. *Seja $\mathbb{F}G$ a álgebra de grupo de um grupo de torção G sobre um corpo $\mathbb{F}$ de característica $p > 0$ e seja $U(\mathbb{F}G)$ o grupo das unidades de $\mathbb{F}G$. Se G' é um p-grupo, então são equivalentes:*

a) $U(\mathbb{F}G)$ satisfaz uma identidade de grupo.

b) G possui um subgrupo normal p-abeliano de índice finito, e G' tem período limitado.

c) $U(\mathbb{F}G)$ satisfaz $(x, y)^{p^k} = 1$ para algum inteiro $k \geq 0$.

Demonstração. $a) \Rightarrow b)$ Como $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, pelos Teoremas 2.2.1, 2.2.2 e 2.2.3, $\mathbb{F}G$ satisfaz uma identidade polinomial, e assim, pelo Teorema 2.1.8, G possui um subgrupo normal p-abeliano de índice finito. Falta-nos mostrar que G' tem período limitado, mas isto segue do Lema 3.3.3.

$b) \Rightarrow c)$ Teorema 2.3.1.

$c) \Rightarrow a)$ Claro. □

Teorema 3.3.9. *Seja $\mathbb{F}G$ a álgebra de grupo de um grupo de torção G sobre um corpo $\mathbb{F}$ de característica $p > 0$ e seja $U(\mathbb{F}G)$ o grupo das unidades de $\mathbb{F}G$. Se G' não é um p-grupo, então são equivalentes:*

a) $U(\mathbb{F}G)$ satisfaz uma identidade de grupo.

b) G possui um subgrupo p-abeliano normal de índice finito, G tem período limitado e $\mathbb{F}$ é finito.

c) $U(\mathbb{F}G)$ satisfaz $x^n = 1$ para algum inteiro n.

Demonstração. $a) \Rightarrow b)$ Como $U(\mathbb{F}G)$ satisfaz uma identidade de grupo, pelos Teoremas 2.2.1, 2.2.2 e 2.2.3, $\mathbb{F}G$ satisfaz uma identidade polinomial, e assim, pelo Teorema 2.1.8, G possui um subgrupo normal p-abeliano de índice finito. Falta-nos mostrar que G tem período limitado e $\mathbb{F}$ é finito. Pelo Teorema 2.3.1, como G' não é p-grupo, temos que $\mathbb{F}$ tem de ser finito.

Agora, sendo A o subgrupo p-abeliano de índice finito de G, como foi observado no Lema 3.3.2, podemos supor que A é abeliano. Assim, escrevemos $A = P \times Q$, e sendo A normal e abeliano, P e Q são normais em G. Como A é de índice finito, $G = A \cup g_1A \cup \cdots \cup g_nA$, onde $g_i \in G$, $i = 1, \ldots, n$. Dado $g \in G$, $g = g_ja$, para algum $j = 1, \ldots, n$ e $a \in A$. Tomando $m = |g_1||g_2| \ldots |g_n|$, temos que $g^m \in A$, ou seja, $g^m = xy$, onde $x \in P$, $y \in Q$.

Pelos Lemas 3.3.2 e 3.3.4, sabemos que os p-elementos e os p'-elementos de G tem período limitado. Sejam k_P e k_Q limitantes para para os p-elementos e os p'-elementos respectivamente. Assim

$$(g^m)^{k_P k_Q} = (xy)^{k_P k_Q} = x^{k_P k_Q} y^{k_P k_Q} = 1.$$

Logo, G tem período limitado.

$b) \Rightarrow c)$ Seja A o subgrupo p-abeliano normal de índice finito. Pelos Lemas 1.7.7 e 3.3.5, é suficiente mostrar que $U(\mathbb{F}(G/A'))$ tem período limitado. A fim de evitar carregar a notação, podemos considerar A abeliano (Se A não for abeliano, tome G/A' e A/A' abeliano e repita o processo a seguir). Sendo A abeliano, escrevemos $A = P \times Q$, onde P é um p-subgrupo normal e Q é um p'-subgrupo normal. Como A é abeliano e P tem período limitado, temos que $\Delta(A, P)$ é nil de expoente limitado. Pelo Lema 3.3.7, temos então que $\Delta(G, P)$ é nil de expoente limitado. Novamente pelo Lema 3.3.5, é suficiente mostrar que $U(\mathbb{F}G/\Delta(G, P)) \cong U(\mathbb{F}(G/P))$ tem período limitado. Novamente, para não carregar a notação, podemos então considerar que A é um p'-grupo.

Pelo Lema 3.3.6, $\mathbb{F}G$ mergulha em $\mathbb{M}_n(\mathbb{F}A)$, onde $n = [G : A]$. Logo, é suficiente mostrar que $GL_n(\mathbb{F}A)$ tem período limitado. Tomando uma matriz $M \in GL_n(\mathbb{F}A)$, seja H o subgrupo gerado pelos suportes das entradas de M e M^{-1}. Como G é localmente finito, H é p'-grupo abeliano finito, e assim, pelo Teorema de Wedderburn-Artin, $\mathbb{F}H$ é soma direta de corpos. E ainda, se m é o período maximal de A, cada corpo (sendo finito), será da forma $\mathbb{F}(\xi^r)$, onde ξ é uma m-ésima raiz primitiva da unidade e r é um inteiro positivo.

Sendo $k = |GL_n(\mathbb{F}(\xi))|$, vemos que $M^k = 1$. Como k depende apenas do período maximal de A, então $U(\mathbb{F}G)$ satisfaz $x^k = 1$.

$c) \Rightarrow a)$ Claro. □

Bibliografia

[1] M. Brešar. *Introduction to Noncommutative Algebra*. Universitext. Springer International Publishing, 2014.

[2] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2004.

[3] Y. Garcia, A. e Lequain. *Elementos de Álgebra*. IMPA, 2015.

[4] A. Giambruno, E. Jespers, and A. Valenti. Group identities on units of rings. *Archiv der Mathematik*, 63(4):291–296, 1994.

[5] A. Giambruno, S. Sehgal, and A. Valenti. Group algebras whose units satisfy a group identity. *Proceedings of the American Mathematical Society*, 125(3):629–634, 1997.

[6] J.Z. Gonçalves. Free subgroups of units in group rings. *Canadian Mathematical Bulletin*, 27(3):309–312, 1984.

[7] M. Hall. *The Theory of Groups*. AMS Chelsea Pub., 1976.

[8] T.W. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2003.

[9] G. Karpilovsky. *Unit groups of group rings*. Pitman monographs and surveys in pure and applied mathematics. Longman Scientific & Technical, 1989.

[10] T.Y. Lam. *A First Course in Noncommutative Rings*. A First Course in Noncommutative Rings. Springer, 2001.

[11] G.T. Lee. *Group Identities on Units and Symmetric Units of Group Rings*. Algebra and Applications. Springer London, 2010.

[12] C.H. Liu. Group algebras with units satisfying a group identity. *Proceedings of the American Mathematical Society*, 127(2):327–336, 1999.

[13] C.H. Liu and D.S. Passman. Group algebras with units satisfying a group identity ii. *Proceedings of the American Mathematical Society*, 127(2):337–341, 1999.

[14] F. Lorenz and S. Levy. *Algebra: Volume I: Fields and Galois Theory*. Universitext. Springer New York, 2006.

[15] R.C. Lyndon and P.E. Schupp. *Combinatorial Group Theory*. Classics in Mathematics. Springer Berlin Heidelberg, 2001.

[16] C.P. Milies and S.K. Sehgal. *An Introduction to Group Rings*. Algebra and Applications. Springer Netherlands, 2002.

[17] D.S. Passman. Group algebras whose units satisfy a group identity ii. *Proceedings of the American Mathematical Society*, 125(3):657–662, 1997.

[18] D.S. Passman. *The Algebraic Structure of Group Rings*. Dover Books on Mathematics Series. Dover Publications, 2011.

[19] S.K. Sehgal. *Topics in group rings*. Pure and applied mathematics. M. Dekker, 1978.