Universidade Federal do Amazonas
Instituto de Ciências Exatas
Programa de Pós–Graduação em Matemática
Mestrado em Matemática

Identidades de Grupo em Unidades de Anel de Grupo

Joerlen Alves de Souza

Manaus – AM
Novembro de 2018

Universidade Federal do Amazonas
Instituto de Ciências Exatas
Programa de Pós–Graduação em Matemática
Mestrado em Matemática

Identidades de Grupo em Unidades de Anel de Grupo

por

Joerlen Alves de Souza

sob a orientação do

Prof. Dr. Claudenir Freire Rodrigues
Orientador

Manaus – AM
Novembro de 2018

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Souza, Joerlen Alves de

S729i Identidades de grupo em unidades de anel de grupo / Joerlen Alves de Souza . 2018

43 f.: 31 cm.

Orientador: Claudenir Freire Rodrigues

Dissertação (Mestrado em Matemática) - Universidade Federal do Amazonas.

1. Anel de grupo. 2. Identidade de grupo. 3. Identidade polinomial. 4. Conjectura de Brian Hartley. I. Rodrigues, Claudenir Freire. II. Universidade Federal do Amazonas III. Título

Identidades de Grupo em Unidades de Anel de Grupo

por

Joerlen Alves de Souza

Dissertação apresentada ao Corpo Docente do Programa de Pós–Graduação em Matemática da Universidade Federal do Amazonas como requisitos necessários para a obtenção do título de Mestre em Matemática.

Área de Concentração: Matemática

Aprovada em 06 de Novembro de 2018.

Banca Examinadora:

Claudenir F. Rodrigues

Prof. Dr. Claudenir Freire Rodrigues – (Orientador)
Universidade Federal do Amazonas - UFAM

Prof. Dr. Stefan Josef Ehbauer – (Membro Interno)
Universidade Federal do Amazonas - UFAM

Prof. Dr. Vitor de Oliveira Ferreira – (Membro Externo)
Universidade de São Paulo - USP

Dedico este trabalho ao meu esposo Nilfran Alves da Costa e aos meus filhos, Hugo Alves de Souza, Nicolly Alves de Souza, João Vitor Alves de Souza e Yasmin Alves de Souza, os quais são minha razão para eu seguir cada dia mais adiante.

Agradecimentos

A Deus pelo dom da vida, pela saúde e por me ajudar a levantar nas tantas vezes que caí.

Ao meu orientador, Dr. Claudenir Freire Rodrigues, pela paciência, dedicação e pela imensa contribuição para que este sonho se concretizasse.

A minha mãe Erlita de Souza e Souza e ao meu pai José Roberto Andrade de Souza (In Memoriam), pelo amor, afeto, dedicação e incentivo nos estudos.

Ao meu esposo, Nilfran Alves da Costa, que sempre me apoiou e nunca deixou de acreditar em mim. Seus incentivos foram essenciais para que eu pudesse concluir essa caminhada. Obrigada principalmente pelo seu amor e pela sempre dedicação aos nossos filhos.

Aos meus filhos, Hugo Alves de Souza, Nicolly Alves de Souza, João Vitor Alves de Souza e Yasmin Alves de Souza, pela compreensão, amor e carinho.

Ao meu irmão, Lauriano de Souza e Souza, pelo incentivo e pela ajuda com os livros e as notas de aula que muito contribuíram nessa minha jornada.

Às amigas, Ionay Batalha, Josinara Muniz, Lene Michiles, Vanessa Bentes e Eliane Alves, por terem me ajudado com meus pequenos durante essa trajetória.

Aos professores do Departamento de Matemática da UFAM: Dra. Juliana Ferreira Ribeiro de Miranda, a qual também agradeço pelos seus trabalhos como coordenadora do PPGM, Dr. Stefan Josef Ehbauer, Dr. Claudenir Freire Rodrigues, Dra. Maria Rosilene Barroso dos Santos, Dr. Dmitry Logachev, Dr. Germán Alonso Benitez Monsalve, Dr. Michel Pinho Rebouças, Dr. Valtemir Martins Cabral, pelas valiosíssimas aulas que muito contribuíram para a minha formação acadêmica e profissional.

Aos amigos de mestrado, pela imensa contribuição nos estudos. Em especial a(o):
Sabrina Rodrigues, companheira de estudos, que muitas vezes me recebeu em sua casa para passarmos horas e horas estudando.
Wanessa Ferreira, pelos incentivos e por ser fonte de inspiração por nunca desistir.
Cristiano, Leonardo, João Batista, Claudeilsio, Edfram Rodrigues, Lemuel, Kleberson, Alberth, companheiros de zuação da Wanessa e de resolução das listas de exercício, é claro.
Todos vocês foram essenciais para que eu chegasse até aqui.

Às amigas mestrandas, Maristela e Flávia, pela torcida e apoio.

Aos meus colegas de trabalho: Júlio Cézar Marinho da Fonseca, Márcia Sarraff

Nascimento, Pedro Sílvio Coimbra Rodrigues, Paulo Sérgio Ribeiro da Silva, Maildson Araújo Fonseca, Lucélida de Fátima Maia da Costa, Clodoaldo Pires Araújo, Isabel do Socorro Lobato Beltrão, Manoel Fernandes Braz Rendeiro, David Xavier da Silva e Marceliano Eduardo, pelo imenso apoio e incentivo.

Aos professores de graduação: Aurélia Nogueira, Elizabeth Blanco, Isabel Lobato, Domingos Furtado, Francisco Miranda, Carlos Lima, João Raimundo, pela imensa contribuição na minha formação. Em especial aos professores, Ana Acácia Valente e Francisco Eteval Feitosa, minhas inspirações para seguir o magistério, e cujos ensinamentos foram valiosíssimos.

Aos secretários do PPGM, Aristocles Rannyeri Nascimento de Lima e ao Elclimar Alves Saraiva, pela paciência e pelo ótimo trabalho junto à coordenação do PPGM.

Resumo

Neste trabalho abordamos a confirmação da conjectura de Brian Hartley, a saber: "Seja K um corpo e G um grupo de torção. Se $U(KG)$, o grupo das unidades da álgebra de grupo KG, satisfaz uma identidade de grupo, então KG satisfaz uma identidade polinomial. Estudamos o caso particular desta conjectura, seguindo de perto o trabalho intitulado "Group identities on units of rings, de Antônio Giambruno, Eric Jespers e Ângela Valenti, os quais provaram a conjectura de Hartley para anéis de grupo RG sobre um domínio comutativo infinito R de característica $p \geq 0$ e G um p'-grupo de torção.

Palavras-chave: Anel de Grupo; Identidade de Grupo; Identidade Polinomial; Conjectura de Brian Hartley.

Abstract

In this work, we address the confirmation of Brian Hartley's conjecture, namely: "Let K be a body and G a torsion group. If $U(KG)$, the group of units of group algebra KG, satisfies a group identity, then KG satisfies a polynomial identity. We study the particular case of this conjecture, closely following the work entitled "Group identities on units of rings", by Antônio Giambruno, Eric Jespers and Ângela Valenti, who proved the Hartley conjecture for group rings RG over an infinite commutative domain R of characteristic $p \geq 0$ and G a p'-torsion group.

Keywords: Group Ring; Group Identity; Polynomial identity; Brian Hartley's conjecture.

Sumário

Introdução **11**

1 Conceitos Preliminares **13**
1.1 Algumas noções da teoria de Grupo 13
1.1.1 Grupo Hamiltoniano 14
1.2 Grupo Livre 15
1.3 Anéis e Ideais Nilpotentes 16
1.4 Localização 17
1.4.1 Construção do Anel de Localização 17
1.4.2 O Anel local $R_{(p)}$ 19
1.5 Álgebras 20

2 Anéis de Grupo, Identidades de Grupo e Identidades Polinomiais **22**
2.1 Anéis de Grupo 22
2.1.1 Unidades de Anéis de Grupo 24
2.2 Identidades de Grupo e Identidades Polinomiais. 24
2.2.1 Processo de Linearização 30
2.2.2 Identidade Polinomial Generalizada 32

3 Conjectura de Brian Hartley **34**

Referências Bibliográficas **42**

Introdução

Seja K um corpo e G um grupo. KG é denotado o anel de grupo do grupo G sobre o corpo K e $U(KG)$ o seu grupo de unidades.

Estudando sobre a estrutura de $U(KG)$, Brian Hartley propôs a seguinte Conjectura:

"Seja K um corpo e G um grupo de torção. Se $U(KG)$, satisfaz uma identidade de grupo, então KG satisfaz uma identidade polinomial".

Em 1999, C. H. Liu [9] deu uma demonstração para esta conjectura, sendo K um corpo qualquer (não necessariamente infinito). Antes dele, alguns casos particulares da conjectura foram estudados, a saber:

Primeiramente, a conjectura foi estudada por Warhurst [20] em 1981 em sua tese de doutorado, o qual investigou algumas palavras especiais satisfeitas por $U(KG)$. Nesse mesmo ano, Pere Menal [12] sugeriu uma possível solução para alguns p-grupos.

Em 1991 e assumindo que o corpo é infinito, Gonçalves e Mandel [6], verificaram a conjectura de Hartley no caso em que $U(RG)$ satisfaz uma identidade de semigrupo. E em 1994, Dokuchaev e Goncalves [3] estenderam este último resultado para $R = \mathbb{Z}$.

Ainda, em 1994, A. Giambruno, E. Jespers e A. Valenti [4] provaram a conjectura de Hartley para anéis de grupo RG sobre um domínio comutativo infinito R de característica $p \geq 0$ e G um grupo de torção que não tem p-elementos.

Em 1997, A. Giambruno, S. Sehgal e A. Valenti [5] provaram a conjectura para o caso em que o corpo é infinito.

Em seguida Passman [14], encontrou condições necessárias e suficientes para que $U(KG)$ satisfaça uma identidade de grupo, para o caso em que o corpo K é infinito . E para o caso geral a prova foi feita em 1999, por C. H. Liu e D. Passman [10].

Nosso interesse neste trabalho é expor a solução apresentada por A. Giambruno, E. Jespers e A. Valenti [4] no artigo intitulado "Group identities on units of rings", onde tratam um caso particular da conjectura de Brian Hartley.

A dissertação está dividida em três capítulos, como segue:

No primeiro capítulo, apresentamos algumas noções preliminares necessárias à compreensão deste trabalho, como a teoria de Grupo, especialmente Grupo de torção, Grupo Hamiltoniano, Grupos Livres. Discorremos também sobre alguns conceitos básicos de Anéis, Ideais nilpotentes, Localização e Álgebras.

No segundo capítulo, estudamos sobre os Anéis de grupo e apresentamos alguns resultados importantes sobre esta estrutura algébrica. Em seguida, definimos Identidades de Grupo e Identidades Polinomiais, como a identidade polinomial Standard, Identidade Polinomial Generalizada e Identidade Polinomial Multilinear generalizada não-degenerada. Demonstramos alguns teoremas, conforme D. S. Passman [13], que caracterizam álgebras de grupo satisfazendo identidades polinomiais. E ainda, damos a demonstração do Teorema devido a Kaplansky, que trata do Processo de Linearização sobre identidades Polinomiais.

No terceiro capítulo, estudamos o artigo Group identities on units of rings de Giambruno, Jespers e Valenti.

Capítulo 1

Conceitos Preliminares

Neste capítulo apresentamos fundamentos teóricos utilizados ao longo do texto e necessários para uma melhor compreensão deste trabalho.

1.1 Algumas noções da teoria de Grupo

Definição 1.1.1. *Sejam G um grupo e $g \in G$. Dizemos que g tem ordem finita se existe $n \in \mathbb{Z}$ não nulo tal que $g^n = e$. Neste caso, definimos a ordem de g, denotada por $|g|$, como sendo:*

$$|g| = min\{n \in \mathbb{N} \mid g^n = e\}.$$

Se $g^n = e$ vale somente para $n = 0$, dizemos que a ordem de G é infinita, e denotamos por $|g| = \infty$.

Observação 1.1.1. *Denotamos por $T(G)$ o conjunto dos elementos de ordem finita de G. Dizemos que G é um grupo de torção se $T(G) = G$. Dizemos que G é um grupo livre de torção se $T(G) = e$.*

Notaremos por G' o subgrupo comutador de G, isto é:

$$G' = \langle\{(g, h) = g^{-1}h^{-1}gh \mid g, h \in G\}\rangle.$$

Definição 1.1.2. Seja G um grupo. Dizemos que G é localmente finito se todo subgrupo finitamente gerado de G é finito.

Teorema 1.1.1 (Teorema de Schmidt). [**Ver [8], Teorema 14.3.1**]. Seja G um grupo e H um subgrupo normal de G. Se H e G/H são localmente finitos, então G é localmente finito.

Definição 1.1.3. Dado um grupo G, definimos o centro $Z(G)$ como sendo o conjunto dos elementos $x \in G$ tal que $xy = yx$, $\forall\ y \in G$.

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 1.1.4. Dado um grupo G, definimos o FC-subgrupo ϕ como sendo:

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

.

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 1.1.5. 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. $p' - elementos$).

Observação 1.1.2. Denotaremos por G_p o conjunto dos $p - elementos$ de um grupo G, e $G_{p'}$ aos $p' - elementos$ de G, para um dado primo p.

Definição 1.1.6. Um grupo G é dito $p - abeliano$ se o seu subgrupo comutador G' é finito e $p - grupo$.

Exemplo 1.1.1. Seja A_4 o conjunto 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:

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

.

1.1.1 Grupo Hamiltoniano

O grupo Hamiltoniano terá grande relevância na demonstração da Conjectura de Brian Hartley. Para tanto, faz-se necessário conhecermos um pouco desse Grupo. Para um melhor aprofundamento, consultar [15].

Definição 1.1.7. Dizemos que G é um grupo hamiltoniano se todos os seus subgrupos são normais e G não é abeliano.

Observação 1.1.3. O Grupo que definimos abaixo através de sua apresentação é chamado de grupo dos Quatérnios de ordem 8:

$$Q_8 = \langle a, b : a^4 = 1,\ a^2 = b^2,\ bab^{-1} = a^{-1} \rangle.$$

Seus elementos podem ser facilmente enumerados:

$$Q_8 = \{1,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b\}.$$

Um cálculo direto mostra que $Q_8' = Z(Q_8) = \{a^2\}$. Além disso, a^2 é o único elemento de Q_8 de ordem 2, portanto, se H é qualquer subgrupo próprio de Q_8, temos que $Q_8' = \{a^2\} \subset H$. Segue imediatamente que todo subgrupo de Q_8 é normal.

Teorema 1.1.2. [**Ver [15], Teorema 1.8.5**]. Um grupo G é hamiltoniano se ele é escrito da forma:

$$G = Q_8 \times E \times A,$$

onde Q_8 é o grupo dos quatérnios de ordem 8, E é um $2-$grupo abeliano elementar e A é um grupo abeliano no qual todo elemento tem ordem ímpar.

1.2 Grupo Livre

Dado um conjunto de símbolos X, vamos construir um grupo F que seja "livre" em um certo sentido no conjunto X. Para um melhor aprofundamento do assunto, consultar [8].

Se $X = \emptyset$, então F é o grupo trivial $\{e\}$. Se $X \neq \emptyset$, seja X^{-1} um conjunto disjunto de X tal que $|X| = |X^{-1}|$. Escolha uma bijeção $X \longrightarrow X^{-1}$ definida por $x \mapsto x^{-1}$. Finalmente escolha um conjunto disjunto de $X \cup X^{-1}$ que tenha exatamente um elemento; denote esse elemento por 1. Uma palavra sobre X é uma sequência finita $a_1 a_2 ... a_n$ tal que $a_i \in X \cup X^{-1} \cup \{1\}$ tal que para algum $n \in \mathbb{N}^*$, $a_k = 1$ para todo $k \geq n$. 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.

Definição 1.2.1. Uma palavra $a_1 a_2 ... a_n$, diferente da palavra vazia, é dita reduzida quando:

(i) Se $a_i = x^i$ então $a_{i+1} \neq x^{-i}$ para todo $i = 1, 2, ..., n-1$.
(ii) $a_i \neq 1$ para todo $i = 1, 2, ..., n$.

A palavra vazia é considerada reduzida. Assim, podemos escrever uma palavra reduzida não vazia em geral como $a_1^{\lambda_1} ... a_m^{\lambda_m}$, 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, $1 \cdot w = w \cdot 1$ para toda palavra $w \in F$, e dadas duas palavras reduzidas não vazias $a_1^{\lambda_1}...a_m^{\lambda_m}$, $b_1^{\lambda_1}...b_s^{\lambda_s}$, seu produto será a justaposição reduzida das duas palavras, ou seja,

$$(a_1^{\lambda_1}...a_m^{\lambda_m}) \cdot (b_1^{\lambda_1}...b_s^{\lambda_s}) = a_1^{\lambda_1}...a_m^{\lambda_m} b_1^{\lambda_1}...b_s^{\lambda_s}$$

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

Exemplo 1.2.1. $(a_3a_2^{-1}a_5a_6^{-1})(a_6a_5^{-1}a_2a_4) = a_3a_4$

Definição 1.2.2. 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.

Teorema 1.2.1. [**Ver [11], Proposição I.1.9**] Seja X um subconjunto de um grupo G tal que $X \cap X^{-1} = \emptyset$. Então X é uma base de um subgrupo livre 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 $x_ix_{i+1} \neq 1$ para todo $i = 1, \dots, n-1$.

1.3 Anéis e Ideais Nilpotentes

Nesta seção iremos recordar alguns fatos básicos da teoria de anéis e Ideais Nilpotentes.

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 1.3.1. $char(\mathbb{Z}_3) = 3$ e $char(\mathbb{Z}) = char(\mathbb{Q}) = char(\mathbb{R}) = 0$.

Definição 1.3.2. Um ideal I de um anel R é dito nilpotente se existe $n \in \mathbb{N}$ tal que $I^n = 0$, em particular, $u_1u_2...u_n = 0$ para todo $u_i \in I$.

Definição 1.3.3. Um elemento $a \in R$ é dito nilpotente se existe $n \in \mathbb{N}$ tal que $a^n = 0$.

Definição 1.3.4. 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.

Definição 1.3.5. Dizemos que um anel R é semiprimo se R não tem ideais nilpotentes não triviais.

1.4 Localização

Nessa seção apresentamos a construção do Anel de Localização, bem como alguns resultados importante que envolvem esta estrutura. Os resultados aqui expostos podem ser encontrados em [1].

Definição 1.4.1. Seja R um anel. Um **conjunto multiplicativo** $S \subset R$ é um subconjunto tal que $0 \notin S$, $1 \in S$ e que é fechado com relação ao produto: $a, b \in S \Rightarrow ab \in S$.

Um caso particular de grande interesse para nós, é quando S é denotado por $S = R \setminus (p)$, o complemento de um ideal primo (p). Que será visto mais adiante.

Dado um conjunto multiplicativo $S \subset R$, vamos construir um novo anel $S^{-1}R$, o anel de Localização, também chamado anel de frações de R por S, onde todos os elementos de S se tornem unidades. Fazemos isto invertendo formalmente os elementos de S, tomando alguns cuidados para evitar problemas com os divisores de zero em R:

1.4.1 Construção do Anel de Localização

Se S é um subconjunto multiplicativo do anel R, definimos uma relação de equivalência em $R \times S$ por $(r_1, s_1) \sim (r_2, s_2)$ se para algum $t \in S$ temos $t(r_1s_2 - r_2s_1) = 0$. Se $r \in R$ e $s \in S$, definimos a fração r/s como a classe de equivalência de (r, s). Fazemos o conjunto de frações em um anel de maneira natural. Onde a soma e o produto são definidos da seguinte forma:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2 + r_2s_1}{s_1s_2} \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}$$

a identidade aditiva é $\frac{0}{1}$, que coincide com $\frac{0}{s}$ para todo $s \in S$. O inverso aditivo de r_1/s_1 é $-(r_1/s_1) = -(r_1)/s_1$. A identidade multiplicativa é $1/1$, que coincide com s/s para todo $s \in S$. Para resumir:
$S^{-1}R$ é um anel. Se R é um domínio integral, também o é $S^{-1}R$. Se R é um domínio integral e $S = R \setminus \{0\}$, então $S^{-1}R$ é um corpo, o corpo de frações de R.

Observação 1.4.1.

- Existe um homomorfismo natural $h : R \longrightarrow S^{-1}R$ dado por $r \mapsto r/1$ chamado de Localização.
- Se S não tem divisores de zero, então h é um monomorfismo, e neste caso é denotado pela inclusão $R \subseteq S^{-1}R$.
- Em particular, um anel R pode ser mergulhado em seu anel de frações $S^{-1}R$, onde S consiste em todos os não-divisores de 0 em R.
Um domínio integral pode ser mergulhado em seu corpo de fração. .

Nosso objetivo nessa seção é abordar a relação entre ideais primos de R e ideais primos de $S^{-1}R$.

Lema 1.4.1. Se X é um subconjunto qualquer de R, defina $S^{-1}X = \{x/s \mid x \in X, s \in S\}$. Se I é um ideal de R, então $S^{-1}I$ é um ideal de $S^{-1}R$. Se J é outro ideal de R, então:

(1) $S^{-1}(I+J) = S^{-1}I + S^{-1}J$;

(2) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$;

(3) $S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$;

(4) $S^{-1}I$ é um ideal próprio sse $S \cap I = \emptyset$.

Demonstração: As definições de adição e multiplicação em $S^{-1}R$ implicam que $S^{-1}R$ é um ideal, e que em (i), (ii) e (iii), o lado esquerdo está contido no lado direito. As inclusões contrárias em (i) e (ii) seguem de

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \qquad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

Para provar (iii), temos que $\frac{a}{s} = \frac{b}{t}$, onde $a \in I,\ b \in J,\ s,\ t \in S$, logo existe $u \in S$ tal que $u(at - bs) = 0$. Logo $\frac{a}{s} = \frac{uat}{ust} = \frac{ubs}{ust} \in S^{-1}(I \cap J)$.

Finalmente, se $s \in S \cap I$, então $\frac{1}{1} = \frac{s}{s} \in S^{-1}I$, então $S^{-1}I = S^{-1}R$. Por outro lado, se $S^{-1}I = S^{-1}R$, então $\frac{1}{1} = \frac{a}{s}$ para algum $a \in I,\ s \in S$. Temos que existe $t \in S$ tal que $t(s-a) = 0$, então $at = st \in S \cap I$.

□

Lema 1.4.2. Seja h o homomorfismo natural de R para $S^{-1}R$ [veja **Observação 1.4.1**]. Se J é um ideal de $S^{-1}R$ e $I = h^{-1}(J)$, então I é um ideal de R e $S^{-1}I = J$.

Demonstração: Temos que I é um ideal pelas propriedades básicas de pré-imagem de conjuntos. Seja $a/s \in S^{-1}I$, com $a \in I$ e $s \in S$, então $a/1 = h(a) \in J$, logo $a/s = (a/1)(1/s) \in J$. Por outro lado, seja $a/s \in J$, com $a \in R,\ s \in S$, então $h(a) = a/1 = (a/s)(s/1) \in J$, consequentemente $a \in I$ e $a/s \in S^{-1}I$.

□

Lema 1.4.3. Se I é qualquer ideal de R, então $I \subseteq h^{-1}(S^{-1}I)$. Haverá igualdade se I é primo e disjunto de S.

Demonstração: Se $a \in I$, então $h(a) = a/1 \in S^{-1}I$. Assim, assuma que I é primo e disjunto de S, e seja $a \in h^{-1}(S^{-1}I)$, então $h(a) = a/1 \in S^{-1}I$, logo $a/1 = b/s$ para algum $b \in I,\ s \in S$. Consequentemente, existe $t \in S$ tal que $t(as - b) = 0$. Portanto $ast = bt \in I$, com $st \notin I$, pois $S \cap I = \emptyset$. Como I é primo, temos que $a \in I$.

□

Lema 1.4.4. Se I é um ideal primo de R disjunto de S, então $S^{-1}I$ é um ideal primo de $S^{-1}R$.

Demonstração: Pelo item (4) do **Lema 1.4.1**, $S^{-1}I$ é um ideal próprio. Seja $(a/s)(b/t) = ab/st \in S^{-1}I$, com $a,\ b \in R$ e $s,\ t \in S$. Então $ab/st = c/u$ para algum $c \in I,\ u \in S$. Temos que existe $v \in S$ tal que $v(abu - cst) = 0$. Portanto, $abuv = cstv \in I$, e $uv \notin I$, pois $S \cap I = \emptyset$. Como I é primo, $ab \in I$, consequentemente $a \in I$ ou $b \in I$. Logo ou a/s ou b/t pertence a $S^{-1}I$.

□

Teorema 1.4.1. Existe uma correspondência um-a-um entre os ideais primos P de R que são disjuntos de S e os ideais Primos Q de $S^{-1}R$, dados por

$$P \to S^{-1}P \qquad \text{e} \qquad Q \to h^{-1}(Q)$$

Demonstração: Pelo **Lema 1.4.2** e **Lema 1.4.3**, temos respectivamente que $S^{-1}(h^{-1}(Q)) = Q$ e $h^{-1}(S^{-1}P) = P$. Pelo **Lema 1.4.4**, $S^{-1}P$ é um ideal primo, e $h^{-1}(Q)$ é um ideal primo pelas propriedades básicas de pré-imagens de conjuntos. Se $h^{-1}(Q)$ satisfaz S, então pelo item (4) do **Lema 1.4.1**, $Q = S^{-1}(h^{-1}(Q)) = S^{-1}R$, uma contradição. Portanto, as aplicações $P \to S^{-1}P$ e $Q \to h^{-1}(Q)$ são inversas uma da outra, e o resultado segue.

□

1.4.2 O Anel local $R_{(p)}$

Nesta subseção discorremos sobre o Anel $R_{(p)}$, o qual terá grande importância na demonstração do último corolário do capítulo 3.

Definição 1.4.2. Se (p) é um ideal primo de R, então $S = R \setminus (p)$ é um conjunto multiplicativo. Neste caso, nós escrevemos $R_{(p)}$ para $S^{-1}R$, e chamamos de localização de R em (p).

Mostraremos que $R_{(p)}$ é um anel Local, isto é, um anel com um único ideal maximal. Mas primeiramente, daremos algumas condições equivalentes à definição de um anel local.

Proposição 1.4.1. Para um anel R, as seguintes condições são equivalentes:

(1) R é um anel local;

(2) Existe um ideal próprio I de R que contém todas as não-unidades de R;

(3) O conjunto das não-unidades de R é um ideal.

Demonstração: (i) implica (ii): Se a é não-unidade, então (a) é um ideal próprio, portanto está contido no único ideal maximal I.
(ii) implica (iii): Se a e b são não-unidades, também o são $a + b$ e ra. Se não, então I contém uma unidade, logo $I = R$, contradizendo a hipótese.
(iii) implica (i): Se I é ideal de não-unidades, então I é maximal, pois qualquer ideal J maior teria que conter uma unidade, logo $J = R$. Se H é qualquer ideal próprio, então H pode conter uma unidade, portanto $H \subseteq I$. Consequentemente I é o único ideal maximal.

□

Teorema 1.4.2. $R_{(p)}$ é um Anel local.

Demonstração: Seja Q um ideal maximal de $R_{(p)}$, então Q é primo, e pelo **Teorema 1.4.1**, $Q = S^{-1}I$ para algum ideal primo I de R que é disjunto de $S = R \setminus (p)$. Em outras palavras, $I \subseteq (p)$. Consequentemente, $Q = S^{-1}I \subseteq S^{-1}(p)$. Se $S^{-1}(p) = R_{(p)} = S^{-1}R$, então pelo **Lema 1.4.1**, item (4), (p) não é disjunto de $S = R \setminus (p)$, o que é impossível. Portanto, $S^{-1}(p)$ é um ideal próprio contendo todos os ideais maximais, logo deve ser o único ideal maximal.

□

Observação 1.4.2. É conveniente escrever o ideal $S^{-1}I$ como $IR_{(p)}$. Não há ambiguidade, porque o produto de um elemento de I e um elemento arbitrário de R pertence a I.

1.5 Álgebras

Definimos nesta seção a estrutura algébrica denominada Álgebra, bem como apresentamos a definição de Álgebra Semiprima e Álgebra Livre. Para um melhor aprofundamento sobre álgebra livre indicamos [2].

Definição 1.5.1. Seja R um anel comutativo. Um R-módulo A é chamado de R-álgebra, se houver uma multiplicação definida em A, de forma que, com a mesma adição dada em A e esta multiplicação, A é um anel tal que a seguinte condição é válida:

$$r(ab) = (ra)b = a(rb),$$

para todo $r \in R$ e todo $a,\ b \in A$.

Se A, como um anel tem unidade 1, então a condição acima implica que $R \cdot 1$ (que é um anel isomorfo a R) está contido no centro de A. Note que se R é um anel comutativo, então o anel $R[X]$ de polinômios com coeficientes em R e o anel completo de matrizes $M_n(R)$ são exemplos de R-álgebras.

Observação 1.5.1.

(1) Quando o produto de A admite uma identidade, isto é, existe um elemento 1 ou 1_A em A tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in A$, dizemos que A é uma álgebra unitária.

(2) Se, para todo $ab \in A$, $ab = ba$, dizemos que A é uma álgebra comutativa.

(3) Se, para todo $a, b, c \in A$, a(bc) =(ab)c, dizemos que A é uma álgebra associativa.

.

Exemplo 1.5.1. O conjunto $M_2(\mathbb{R})$ com as operações de soma, produto e produto por escalar usuais é uma $\mathbb{R}$-álgebra não comutativa.

Definição 1.5.2. Uma álgebra A é dita semiprima quando, olhada como anel, A é um anel semiprimo.

Definição 1.5.3. (Álgebra livre) Uma K-álgebra A é dita livre sobre um subconjunto X (livremente gerada por X) se para qualquer álgebra R e qualquer aplicação $f : X \to R$ existe um único homomorfismo de álgebras $h : A \to R$ que estende f, ou seja, $h_{|X} = f$. A cardinalidade de X é dita o posto de A.

Considerando um conjunto infinito e enumerável $X = \{x_1, x_2, \ldots\}$ de elementos não comutativos, ditos indeterminadas, a álgebra $K\langle X\rangle$ é o espaço vetorial que tem uma base formada por todas as sequências $x_{i_1}x_{i_2}\ldots x_{i_n}$ em X, com $n \geq 0$, munido com a multiplicação natural por justaposição, onde a sequência com $n = 0$ denota a unidade $1 \in K$.

Definição 1.5.4. A álgebra $K\langle X\rangle$ é livremente gerada por X e é chamada a álgebra livre dos polinômios sobre X.

Capítulo 2

Anéis de Grupo, Identidades de Grupo e Identidades Polinomiais

2.1 Anéis de Grupo

Os anéis de grupos são estruturas bastante estudadas por pesquisadores da área de teoria abstrata de grupo. Dentre os principais algebristas que contribuíram e contribuem com as pesquisas relacionadas aos Anéis de Grupo, podemos destacar D.S. Passman, S.K. Sehgal e C. Polcino. Aqui, faremos uma exposição dos principais conceitos e resultados iniciais da teoria e para um melhor aprofundamento sobre o assunto, o leitor poderá consultar [13], [15], [18] e [19].

Definição 2.1.1. Seja R um anel e G um grupo. O **anel de grupo** do grupo G sobre o anel R notado por RG, é o conjunto de todas somas finitas formais:

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

com $g \in G$ e $\alpha_g \in R$, e com a seguinte estrutura de anel:

A soma é definida como

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

e o produto

$$\cdot \ : \sum_{g \in G} \alpha_g g \cdot \sum_{h \in G} \beta_h h = \sum_{g,h \in G} (\alpha_g \beta_h) gh$$

Também tem estrutura de R-módulo:

$$a \cdot \sum_{g \in G} \alpha_g g = \sum_{g \in G} a \cdot \alpha_g g.$$

Podemos notar que se o anel R é unitário, o anel RG também o será, tendo como elemento unidade o elemento $1_A 1_R$.

Observação 2.1.1. No caso em que R é comutativo, RG também é chamado de álgebra de grupo de G sobre R.

Vamos centrar nossas atenções para o caso específico que o anel R é um corpo. Usaremos a letra K para denotar tal corpo.
Notemos que a dimensão da álgebra KG é $|G|$.

Observação 2.1.2. Seja H subgrupo de G. Notaremos por π_H a função:

$$\begin{aligned} \pi_H : KG &\longrightarrow KH \\ \sum_{g\in G} \alpha_g g &\longmapsto \sum_{g\in H} \alpha_g g \end{aligned}$$

Ou seja, tiramos da soma os elementos que não estão em H.

Definição 2.1.2. Para um elemento $\alpha \in KG$, definimos o suporte de α, denotado por $Supp\alpha$, como sendo o conjunto $Supp\alpha = \{g \in G \mid \alpha_g \neq 0\}$. Pela definição de anel de grupo, temos que $Supp\alpha$ é sempre finito.

Definição 2.1.3. Seja KG um anel de grupo. O homomorfismo $\psi : KG \to K$ dado por

$$\psi\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \alpha_g$$

é chamado aplicação de aumento de KG. E o kernel desta aplicação, é o ideal de aumento de KG e o denominamos de $\Delta(G)$.

Lema 2.1.1. Sejam K um corpo, G um grupo, H um subgrupo de G, e Y uma transversal a esquerda de H em G. Então para todo elemento $\alpha \in KG$, existem e são únicos $\alpha_y \in KH$ tal que:

$$\alpha = \sum_{y\in Y} y\alpha_y$$

com $\alpha_y = \pi_H(y^{-1}\alpha) \in KH$.

Demonstração: Seja $\alpha = \sum a_x x \in KG$. Como o suporte de α é finito, existe uma quantidade finita de classes laterais à esquerda de H, digamos, $y_1H, y_2H, ..., y_nH$ com $y_i \in Y$, cuja união contém $Supp\alpha$. Podemos então escrever $\alpha = \alpha_1 + \alpha_2 + ... + \alpha_n$, onde α_i é a soma parcial formada pelos elementos $a_x x$ com $x \in y_iH$. Uma vez que $x \in y_iH$ implica em $y_i^{-1}x \in H$, então

$$\alpha = \sum_{1}^{n} y_i(y_i^{-1}\alpha_i).$$

com $y_i^{-1}\alpha_i \in KH$. Assim α pode ser escrito como uma soma da forma $\sum y\alpha_y$ com $\alpha_y \in KH$. Para provar a unicidade seja $\alpha = \sum y\alpha_y$ e $y_0 \in Y$, então $y_0^{-1}\alpha = \sum y_0^{-1}y\alpha_y$ e $y_0^{-1}y \in H$ se, e somente se, $y = y_0$, pois Y é uma transversal de H em G. Logo,

$$\pi_H(y_0^{-1}\alpha) = y_0y_0^{-1}\alpha_{y_0} = \alpha_{y_0}$$

em particular se $\alpha = 0$ então $\alpha_y = 0$, $\forall\ y \in Y$.

$\square$

2.1.1 Unidades de Anéis de Grupo

Dado um anel A, denotamos por $U(A)$ o grupo multiplicativo das unidades de A. Isto é,

$$U(A) = \{x \in A \mid (\exists y \in A)\ xy = yx = 1\}$$

Definição 2.1.4. (Grupo das unidades de RG). Dado um grupo G e um anel R, $U(RG)$ indica o grupo de unidades do anel de grupo RG assim definido:

$$U(RG) = \{\alpha \in RG \mid \exists\ \beta \in RG \text{ tal que } \alpha\beta = \beta\alpha = 1\}$$

Observação 2.1.3. Como a aplicação $\psi : KG \to K$, dada por $\psi\left(\sum_{g\in G}\alpha_g g\right) = \sum_{g\in G}\alpha_g$ é um homomorfismo de anéis, segue que se $u \in U(KG)$, então $\psi(u) \in U(K)$. De fato, basta observar que $1 = \psi(1) = \psi(uu^{-1}) = \psi(u)\psi(u^{-1})$.

Definição 2.1.5. (Grupo das unidades de aumento 1). O Subgrupo das unidades de aumento 1 em $U(KG)$ é o conjunto

$$U_1(KG) = \{u \in U(KG) \mid \psi(u) = 1\}$$

Para uma unidade u do anel de grupo integral $\mathbb{Z}G$, temos que $\psi(u) = \pm 1$.

Definição 2.1.6. (Unidades Triviais) Um elemento da forma rg, onde $r \in U(R)$ e $g \in G$, possui um inverso $r^{-1}g^{-1}$. Os elementos desta forma são chamados unidades triviais de RG. Se K é um corpo, então as unidades triviais de KG são elementos da forma kg, onde $k \in K$, $k \neq 0$, $g \in G$.

2.2 Identidades de Grupo e Identidades Polinomiais.

Definição 2.2.1. Seja $w(x_1, ..., x_n) \neq 1$ um elemento do grupo livre de posto n. Dizemos que $w = 1$ é uma **identidade de grupo para** G, se para todos $g_1, g_2, ...g_n \in G$ temos $w(g_1, ..., g_n) = 1$. Escrevemos G é **GI**.

Exemplo 2.2.1.

(i) Se G é abeliano, então G satisfaz a identidade $w(x_1, x_2) = x_1^{-1}x_2^{-1}x_1x_2$

(ii) Se G é um grupo nilpotente, então G satisfaz a identidade $w(x_1, \ldots, x_l) = [x_1, \ldots, x_l]$ para algum $l \geq 2$, onde $[x_1, \ldots, x_l]$ denota o comutador de peso l no grupo G.

Definição 2.2.2. Seja $K\langle x_1, x_2, ...\rangle$ a álgebra livre de posto enumerável sobre o corpo K. Dizemos que uma K-álgebra R **satisfaz uma identidade polinomial de grau s** ou é uma **PI- álgebra** se existe $f(x_1, x_2, .., x_n) \in K\langle x_1, x_2, ...\rangle$, $f \neq 0$ com grau de f igual a s tal que

$$f(r_1, r_2, .., r_n) = 0$$

para todos $r_1, r_2, .., r_n \in R$.
Este polinômio $f(x_1, ..., x_n)$ que satisfaz esta propriedade é dito uma **identidade polinomial** em R.

- **Grau de um polinômio**

O grau de um polinômio não nulo $f(x_1, \ldots, x_n) \in K\langle x_1, x_2, \ldots\rangle$ é o maior grau dentre os graus de todos os monômios, com coeficientes não nulos, de$f$.

- PI **álgebra de grau** n

Dizemos que uma álgebra A é uma **PI**-álgebra de grau n quando satisfaz um polinômio de grau n, ou seja, quando A satisfaz uma identidade polinomial de grau n.

Exemplo 2.2.2.

i) Uma álgebra comutativa satisfaz $f(x_1, x_2) = x_1x_2 - x_2x_1$.

ii) Uma álgebra nilpotente de grau m satisfaz $f(x_1, \ldots, x_m) = x_1 \ldots x_m$.

- **Monômio multilinear**

Um monômio $x_{i_1}x_{i_2} \ldots x_{i_j}$ é dito multilinear se cada uma de suas variáveis ocorre uma única vez.

Exemplo 2.2.3.

(i) $x_1x_3x_4x_2$ é multilinear.

(ii) $x_1x_3x_2^2$ não é multilinear.

- **Polinômio multilinear**

Um polinômio $f \in K\langle x_1, x_2, ...\rangle$ é dito multilinear se suas parcelas são monômios multilineares que envolvem as mesmas variáveis. Ou seja, f é multilinear se, e somente se, for da forma $f(x_1, x_2, ...x_n) = \sum_{\sigma \in S_n} a_\sigma x_{\sigma(1)} ... x_{\sigma(n)}$ com $a_\sigma \in K$.

Exemplo 2.2.4.

(i) $f(x_1, x_2, x_3) = x_1x_2x_3 + 4x_3x_2x_1 - 2x_2x_1x_3$ é um polinômio multilinear.

(ii) $f(x_1, x_2, x_3) = x_3x_2 + 5x_2x_1x_3$ não é um polinômio multilinear.

(iii) $f(x_1, x_2) = x_1x_2^2 - 3x_1x_2^2$ não é um polinômio multilinear.

Definição 2.2.3. (Identidade Polinomial Standard). Dizemos que um anel R satisfaz a identidade polinomial standard de grau n, se para todos $x_1, x_2, ...x_n$ vale:

$$s_n(x_1, ..., x_n) = \sum_{\sigma \in S_n} (-1)^\sigma x_{\sigma(1)}...x_{\sigma(n)} = 0$$

onde σ varia em S_n (grupo das permutações de n elementos) e $(-1)^\sigma = \pm 1$ dependendo se σ é uma permutação par ou ímpar.

Exemplo 2.2.5.

(1) $s_2(x_1, x_2) = x_1x_2 - x_2x_1$ é a identidade standard de grau dois.

(2) $s_3(x_1, x_2, x_3) = x_1x_2x_3 + x_2x_3x_1 - x_3x_2x_1 + x_3x_1x_2 - x_1x_3x_2 - x_2x_1x_3$ é a identidade standard de grau três.

Lema 2.2.1. Seja $s_n(x_1, ..., x_n)$ o polinômio standard de grau n. Temos:

(i) s_n é linear em cada variável;

(ii) $s_n(\ldots, x_i, \ldots, x_j, \ldots) = -s_n(\ldots, x_j, \ldots, x_i, \ldots)$;

(iii) $s_n(\ldots, x_i, \ldots, x_i, \ldots) = 0$;

(iv) $s_{n+1}(x_1, x_2, \ldots, x_{n+1}) = \sum \pm x_i s_n(x_1, \ldots, \hat{x_i}, \ldots, x_{n+1})$. Em particular, se V é uma álgebra que satisfaz s_n, então V satisfaz s_{n+1};

(v) $s_{2n}(1, x_2, x_3, \ldots, x_{2n}) = 0$

(vi) $s_n(x_1, x_2, \ldots, x_n) = 0$ se $x_1, x_2, \ldots, x_n$ são linearmente dependentes sobre K.

Demonstração: (i) segue da definição.
(ii) Note que se $\tau = (i, j)$ é uma transposição e $\sigma \in s_n$, então $(-1)^{\sigma\tau} = -(-1)^\sigma$ e que os monômios de $s_n(\ldots, x_i, \ldots, x_j, \ldots)$ são exatamente os mesmos de $s_n(\ldots, x_j, \ldots, x_i, \ldots)$, logo $s_n(\ldots, x_i, \ldots, x_j, \ldots) = -s_n(\ldots, x_j, \ldots, x_i, \ldots)$.
(iii) Basta observar que os monômios de $s_n(\ldots, x_i, \ldots, x_i, \ldots)$ aparecem aos pares, com sinais trocados, portanto cancelam-se dois a dois, assim $s_n(\ldots, x_i, \ldots, x_i, \ldots) = 0$.
(iv) Isto é verdade, pois $\pm x_i s_n(x_1, \ldots, \hat{x_i}, \ldots, x_{n+1})$ é apenas a soma de todos os termos de s_{n+1} que começam com x_i.
(v) Para cada ordenação de $x_2, x_3, \ldots, x_{2n}$ existem exatamente $2n$ monômios

$$1x_{i_2}x_{i_3}\ldots x_{i_{2n}}$$

$$x_{i_2}1x_{i_3}\ldots x_{i_{2n}}$$

$$\vdots$$

$$x_{i_2}x_{i_3}\dots x_{i_{2n}}1$$

na escrita de $s_{2n}(1, x_2, \dots, x_{2n})$ e o coeficiente destes são, respectivamente, $1, -1, 1, \dots$, logo $s_{2n}(1, x_2, \dots, x_{2n}) = 0$.
(vi) Segue de (i) e (ii) ao substituir umas das variáveis por uma combinação linear das demais.

□

O próximo resultado nos garante que uma álgebra de dimensão finita sobre um corpo sempre satisfaz uma identidade polinomial.

Teorema 2.2.1. Seja R uma K-álgebra. Se $dim_K R = n < \infty$, então R satisfaz s_{n+1}. Por outro lado, se R é algébrica de grau limitado n, então R satisfaz a identidade

$$f(x_1, x_2) = s_{n+1}(x_1, x_1x_2, x_1x_2^2, \dots, x_1x_2^n)$$

Demonstração: Se $dim_K R = n$, então qualquer $n+1$ elementos são linearmente dependentes, então R satisfaz s_{n+1} pelo item (vi) do **Lema 2.2.1**. Suponhamos agora que R seja algébrica de grau limitado n e sejam $\alpha, \beta \in R$. Então $1, \beta, \dots \beta^n$ são linearmente dependentes e, consequentemente, o mesmo vale para $\alpha, \alpha\beta, \dots, \alpha\beta^n$. Assim, novamente pelo item (vi) do **Lema 2.2.1**, temos $f(\alpha, \beta) = 0$ e como $f(x_1, x_2) \neq 0$, pois os monômios de f são dois a dois distintos, com isso segue o resultado.

□

Note que em particular o **Teorema 2.2.1** nos diz que $M_m(K)$ satisfaz s_{m^2+1}. De fato, como $M_m(K)$ tem dimensão m^2, pelo teorema anterior, temos que $M_m(K)$ satisfaz a identidade standard de grau m^2+1.

Partindo desse teorema podemos observar que se G é um grupo finito então a álgebra de grupo KG satisfaz uma identidade polinomial, visto que $dimKG = |G|$.

Proposição 2.2.1. [**Ver [13], Lema V.1.7**] Se s''' é a soma de todos os termos em $s_n(x_1, x_2, \dots, x_n)$ onde aparece o produto $x_1x_2x_3$ e s'' é a soma de todos os termos em $s_n(x_1, x_2, \dots, x_n)$ onde aparece o produto x_1x_2. Então:

(i) $s''' = s_{n-2}(x_1x_2x_3, x_4, \dots, x_n)$;

(ii) $s'' = s_{n-2}(x_3, x_4, \dots, x_n)x_1x_2 + \Sigma_{i=3}^{n}(\pm)s_{n-2}(x_1x_2x_i, x_3, \dots, \hat{x_i}, \dots, x_n)$.

Lema 2.2.2. Seja $m > 1$ e assuma que $M_{m-1}(K)$ satisfaz a identidade S_{2m-2}. Seja $\{e_{a_ib_i}\}$ um conjunto com $2m$ matrizes unidades em $M_m(K)$ e suponha que

$$S_{2m}(e_{a_1b_1}, e_{a_2b_2}, \dots, e_{a_{2m}b_{2m}}) \neq 0.$$

Para cada $u = 1, 2, \dots, m$, seja $n(u)$ o número de vezes que u aparece como um índice em $\{e_{a_ib_i}\}$. Então os possíveis valores para $n(u)$ são

$$3, 5, 4, 4, \dots, 4$$

$$3, 3, 6, 4, \dots, 4$$

ou

$$4, 4, 4, 4, \ldots, 4$$

Demonstração: Seja u tal que $n(u) = 0$, ou seja, nenhum dos elementos de $\{e_{a_i b_i}\}$ possui a i-ésima linha e i-ésima coluna, então $\{e_{a_i b_i}\} \subseteq M_m(K)^{(u)} \cong M_{m-1}(K)$ e como s_{2m-2} é uma identidade para $M_{m-1}(K)$ (por hipótese), o **Lema 2.2.1**, item (iv), nos diz que s_{2m} é uma identidade para $M_{m-1}(K)$ e assim $S_{2m}(e_{a_1b_1}, e_{a_2b_2}, \ldots, e_{a_{2m}b_{2m}}) = 0$, absurdo. Se $n(u) = 1$, então, digamos, $e_{ub_i} \in \{e_{a_i b_i}\}_{i=1}^{2m}$ e os únicos monômios de $S_{2m}(e_{a_1b_1}, e_{a_2b_2}, \ldots, e_{a_{2m}b_{2m}})$ não-nulos são aqueles onde e_{ub_i} aparece à esquerda, ou seja, $S_{2m}(e_{a_1b_1}, e_{a_2b_2}, \ldots, e_{a_{2m}b_{2m}}) = \pm\, e_{ubi} s_{2m-1}(\ldots)$, mas $s_{2m-1}(\ldots) = 0$ em $M_{m-1}(K) \cong M_m(K)^{(u)}$, pelo mesmo motivo anterior, logo $s_{2m}(\ldots) = 0$, absurdo. Notemos que de modo análogo poderíamos ter considerado $e_{a_i u}$ no lugar de e_{ub_i}. Se $n(u) = 2$, então existem as seguintes possibilidades (disjuntas) para u de modo que um monômio em s_{2m} se anule: $\{e_{uu}\}$, $\{e_{iu}, e_{ju}\}$ e $\{e_{ui}, e_{uj}\}$. Com isso, para que $s_{2m}(\ldots) \neq 0$, devemos ter e_{uj} e e_{iu} em algum monômio de s_{2m}. Neste caso, temos dois produtos possíveis envolvendo as matrizes e_{uj} e e_{iu} de modo que um monômio seja não-nulo, a saber, $e_{iu}e_{uj} = e_{ij}$ e $e_{uj} \ldots e_{iu}$, logo $s_{2m}(\ldots) = \pm e_{uj} s_{2m-2}(\ldots) e_{iu} + s'' = s'' = \pm s_{2m-2}(\ldots) e_{ij} + \Sigma \pm s_{2m-2}(\ldots) = 0$, pois $M_{m-1}(K)$ satisfaz s_{2m-2} e $e_{ij} \in M_m(K)^{(u)}$. Então podemos assumir que $n(u) \geq 3$. Como $s_{2m}(\ldots) \neq 0$, existe algum monômio M não-nulo. Temos duas possibilidades para a escrita de M, a saber,

$$M = Y e_{i_1 u} e_{u j_1} \ldots e_{i_n u} e_{u j_n} X$$

ou

$$M = Y e_{i_1 u} e_{u j_1} \ldots e_{i_n u}$$

onde X é um produto de matrizes unidades que possuem a u-ésima coluna e u-ésima linha nulas, Y é produto de matrizes unidades que possuem a u-ésima coluna nula (X e Y podem ser expressões vazias) e $\{e_{i_k u}\} \subseteq \{e_{a_i b_i}\}$ é o conjunto de "todas" as matrizes com u-ésima coluna não-nula. Com isso, se $n(u)$ é ímpar, independente de $e_{uu} \in \{e_{a_i b_i}\}$, temos duas possibilidades: $Y = e_{uj} Y'$ onde na escrita de Y' não aparece o índice u, ou $M = Y e_{i_1 u} e_{u j_1} \ldots e_{i_n u}$, em qualquer caso, temos uma matriz $e_{i_n u}$ à direita de M ou uma matriz do tipo e_{uj} à esquerda de M, consequentemente, existem no máximo dois $u_1, u_2 = 1, 2, \ldots, m$ tais que $n(u_i)$ é ímpar. No entanto, como $\Sigma_1^m n(u) = 4m$, concluímos que todos os $n(u)$ são pares ou dois são ímpares e os demais pares. Usando o fato de que $n(u) \geq 3$ e $\Sigma_1^m n(u) = 4m$, calcula-se os possíveis valores para $n(u)$. Por exemplo, $n(1) + n(2) + \ldots + n(m) = 4m$ nos diz, em particular, que algum $n(i)$, digamos $n(1)$, é menor ou igual a 4, ou seja $n(i) = 3$ ou 4. Suponhamos que nenhum dos $n(i)$ seja igual a 3. Logo $n(2) + \ldots + n(m) = 4(m-1)$ e novamente deve existir um $n(j) = 4$, continuando com esse procedimento chegamos a $4, 4, 4 \ldots$. Por outro lado se existir $n(u) = 3$, digamos $n(1)$, deve existir um único $n(u')$ ímpar, com $u \neq u'$, digamos $n(2)$, logo

$$4m = n(1) + n(2) + \ldots + n(m) \geq n(1) + n(2) + 4 + \ldots + 4,$$

consequentemente, $n(1) + n(2) \leq 8$. Com isso temos $3, 3$ ou $3, 5$, continuando com esse mesmo procedimento chega-se às possibilidades

$$3, 3, 6, 4, 4, \ldots,$$

e

$$3, 5, 4, 4, 4, \ldots.$$

□

Lema 2.2.3. Seja $e^2 = e \in M_n(D)$, onde D é um anel de divisão. Então existe $C \in M_n(D)$ invertível tal que $e = Ce_kC^{-1}$, onde $e_k = \Sigma_{i=1}^k e_{ii}$

Demonstração: Considere um espaço vetorial V sobre D de dimensão n com base B_1 e seja $\phi : M_n(D) \to End_D V$ um isomorfismo. Se $E = \phi(e)$, então $E^2 = E$, pois ϕ é um isomorfismo. Provaremos que $V = EV \oplus (I-E)V$. Já temos $EV \oplus (I-E)V \subseteq V$, além disso se $v \in V$, então $v = Ev + (v - Ev) \in EV + (I-E)V$. Logo $EV + (I-E)V = V$. Suponhamos agora que $v \in EV \cap (I-E)V$, então existe $w_1 \in V$ tal que $E_{w_1} = v$ e $w_2 \in (I-E)V$ tal que $v = (I-E)w_2$, logo $Ev = E(E_{w_1}) = E_{w_1} = v$, ou seja $v = Ev$, mas $Ev = E(I-E)w_2 = (E-E^2)w_2 = 0$, logo $v = 0$ e $V = EV \oplus (I-E)V$. Agora escolha uma base de V feita de uma base de EV e de $(I-E)V$, digamos que a base seja $B_2 = \{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$, onde $\{v_1, \ldots, v_k\}$ é a base de EV. Então a matriz de E nessa base tem a forma

$$\begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix} = e_k$$

onde I_k é a matriz identidade de ordem k e os zeros na matriz representam matrizes nulas. Então basta tomar C como sendo a matriz de mudança de base entre a base B_2 e B_1 e neste caso teremos $e = Ce_kC^{-1}$.

□

Teorema 2.2.2. (Amitsur-Levitzky) O polinômio standard s_{2m} é uma identidade de $M_m(K)$ para toda álgebra comutativa K.

Demonstração: Provaremos o Teorema por indução em m. Se $m = 1$, então $s_{2m}(x_1, x_2) = x_1x_2 - x_2x_1$ é uma identidade para $M_1(K)$, pois esta é uma álgebra comutativa. Sejam e, f dois elementos idempotentes ortogonais em $V = M_m(K)$. Mostraremos primeiro que $s_{2m}(e, f, V, V, \ldots, V) = 0$. Note que e e f são simultaneamente diagonalizáveis e possuem apenas 1 e 0 como autovalores. Se $s_{2m}(e, f, V, V, \ldots, V) \neq 0$, então, por linearidade, existe um conjunto de matrizes unidades $\{e_{a_ib_i}\}$ da forma e_{ii} e e_{jj} (por causa da forma diagonal de e e f) tal que $s_{2m}(e_{a_1b_1}, e_{a_2b_2}, \ldots, e_{a_{2m}b_{2m}}) \neq 0$. Sem perda de generalidade podemos tomar $e = e_{11}$ e $f = e_{22}$. Pelo **Lema 2.2.2** e pela hipótese de indução existe no máximo um $u = 1, 2, \ldots, m$ tal que $n(u) > 4$, logo $n(1) \leq 4$ ou $n(2) \leq 4$, digamos que $n(1) \leq 4$. Agora substituindo e_{11} por $1 - \Sigma_2^m e_{ii}$ em $s_{2m}(e_{a_1b_1}, e_{a_2b_2}, \ldots, e_{a_{2m}b_{2m}})$, e usando a multilinearidade de s_{2m}, obtemos uma expressão da forma

$$\begin{aligned} s_{2m}(e_{a_1b_1}, \ldots, e_{a_{2m}b_{2m}}) &= \pm s_{2m}(1, e_{a_{i_1}b_{i_1}}, \ldots, e_{a_{i_{2m-1}}b_{i_{2m-1}}}) \\ &\quad + \Sigma_{i=2}^n \pm s_{2m}(e_{ii}, e_{a_{i_1}b_{i_1}}, \ldots, e_{a_{i_{2m-1}}b_{i_{2m-1}}}) \end{aligned}$$

E o **Lema 2.2.1** nos diz que $s_{2m}(1, e_{a_{i_1}} b_{i_1}, \ldots, e_{a_{i_{2m-1}}} b_{i_{2m-1}}) = 0$. Note que neste caso, em cada um destes termos, tem-se $n(1) \leq 4 - 2 = 2$ e com isso, pelo **Lema 2.2.2**, todos estes são nulos, absurdo. Seja e um idempotente em V. Mostraremos que $s_{2m}(e, V, V, V, \ldots, V) = 0$. Pelo **Lema 2.2.3**, podemos supor, novamente sem perda de generalidade, que $e = e_{11}$ e considerar um conjunto de matrizes unidades $\{e_{a_i b_i}\}$ contendo e_{11}. Se todos os e_{aib_i} possuem um índice 1, então existem matrizes repetidas na escrita de

$$s_{2m}(e_{a_1 b_1}, \ldots, e_{a_{2m} b_{2m}}),$$

pois existem no máximo, $2m - 1$, matrizes unidades com índice 1, logo

$$s_{2m}(e_{a_1 b_1}, \ldots, e_{a_{2m} b_{2m}}) = 0,$$

pelo **Lema 2.2.1, (iii)**. Caso contrário algum e_{ij} aparece com $i, j \neq 1$. Mas pelo parágrafo anterior se $i = j$, temos $s_{2m}(e_{a_1 b_1}, \ldots, e_{a_{2m} b_{2m}}) = 0$, logo podemos supor que $i \neq j$ e ambos são diferentes de 1. Então $e_{ij} = (e_{ii} + e_{ij}) - e_{ii}$ é a diferença entre dois idempotentes, ambos ortogonais a e_{11}, então por linearidade e pelo parágrafo anterior, temos $s_{2m}(e_{a_1 b_1}, \ldots, e_{a_{2m} b_{2m}}) = 0$. Finalmente, mostraremos que $s_{2m}(V, V, \ldots, V) = 0$. Por linearidade, é suficiente provar que $s_{2m}(e_{a_1 b_1}, \ldots, e_{a_{2m} b_{2m}}) = 0$ quando $\{e_{a_i b_i}\}$ é um conjunto de matrizes unidades. Seja $e_{ab} \in \{e_{a_i b_i}\}$. Já vimos que no caso de termos $a = b, s_{2m}(\ldots) = 0$. Se $a \neq b$, então $e_{ab} = (e_{aa} + e_{ab}) - e_{aa}$ é a diferença entre dois idempotentes, então por linearidade temos novamente que $s_{2m}(\ldots) = 0$. Com isso V satisfaz s_{2m} e o resultado segue por indução.

□

Lema 2.2.4. [**Ver [13], Lema V.1.10**] Seja H um subgrupo de G de índice finito n. Então $KG \subseteq M_n(KH)$. Mais precisamente, a função $\eta_x : KG \to M_n(KH)$ dada por $\alpha \mapsto [\pi_H(x_i \alpha x_j^{-1})]$, onde $X = \{x_1, \ldots, x_n\}$ é uma transversal de H em G, é um monomorfismo.

2.2.1 Processo de Linearização

A seguir apresentamos o processo de linearização sobre identidades polinomiais, ou seja, se uma K-álgebra satisfaz uma identidade polinomial de grau n, então ela também satisfaz uma identidade polinomial multilinear de grau n. Ou seja, através do processo de linearização conseguimos obter, a partir do polinômio satisfeito pela álgebra, um novo polinômio, que será multilinear e de mesmo grau, e também satisfeito por essa álgebra.

Teorema 2.2.3. (Kaplansky) Seja R uma álgebra sobre um corpo K. Se R satisfaz uma identidade polinomial de grau n, então R satisfaz uma identidade polinomial da forma:

$$f(x_1, x_2, ...x_n) = \sum_{\sigma \in S_n} a_\sigma x_{\sigma(1)} ... x_{\sigma(n)},$$

com os a_σ pertencentes a K, não todos nulos.

Demonstração. Seja $g(x_1, x_2, ...)$ a identidade polinomial de grau n satisfeita por R. Em primeiro lugar, suponhamos que alguma variável x_i ocorra em algum dos monômios de g mas não em todos. Assim podemos escrever:

$$g = g' + g''$$

onde x_i ocorre em todos os monômios de g' e não ocorre nos monômios de g'' . Logo $g'' \neq 0$, grau $g'' \leq n$ e

$$g''(x_1, x_2, ..., x_i, ...) = g(x_1, x_2, ..., 0, ...)$$

Claramente R também satisfaz g''. Desta maneira substituindo g por g'' , temos uma identidade polinomial para R de grau menor ou igual a n, com menos variáveis. Repetimos este processo até obtermos uma identidade h de grau menor ou igual a n satisfeita por R, onde cada x_i aparece pelo menos uma vez em cada monômio. Como grau $h \leq n$, vemos que h é uma função com no máximo n variáveis. Reescrevendo, se necessário, podemos supor $h \in K\langle x_1, x_2, ..., x_n\rangle$.
Seja $\mathcal{H}$ o conjunto de todos $h \in K\langle x_1, x_2, ..., x_n\rangle$, $h \neq 0$ os quais são identidades polinomiais para R de grau menor ou igual a n e que todas as variáveis envolvidas em h apareça em cada monômio de h. Por construção $\mathcal{H}$ é não vazio.
Tomemos $f \in \mathcal{H}$ como sendo a função que possui um número máximo de variáveis, digamos t.
Agora, mostraremos que realmente f é a identidade polinomial procurada.
Sem perda de generalidade, suponhamos que algum monômio de h não é linear em x_1. Como grau $f \leq n$ e $f \in \mathcal{H}$, logo f não pode conter todos x_i, $1 \leq i \leq n$, portanto algum x_i não aparece em f. Suponhamos então que x_n não apareça em f. Seja

$$f' = f(x_1 + x_n, x_2, ...) - f(x_1, x_2, ...) - f(x_n, x_2, ...).$$

Considerando os monômios envolvidos que não são lineares em x_1, segue facilmente que $f' \neq 0$ e $f' \in \mathcal{H}$. Porém, f' é uma função de $t + 1$ variáveis, uma contradição. Consequentemente todos os monômios em f são lineares em cada variável x_i e desta forma todos possuem o mesmo grau $t \leq n$.
Suponhamos $t < n$ e digamos, x_n não aparece em f. Fazendo $f'' = x_n f$ obtemos uma contradição. Desta forma $t = n$ e f possui a forma desejada.

□

Agora, observaremos três exemplos que ilustram o processo de multilinearizar polinômios.

Exemplo 2.2.6. Se $f = x_1^2$, então

$$\begin{aligned} g &= f(x_1 + x_2) - f(x_1) - f(x_2) \\ &= (x_1 + x_2)^2 - x_1^2 - x_2^2 \\ &= (x_1 + x_2)(x_1 + x_2) - x_1^2 - x_2^2 \\ &= x_1x_2 + x_2x_1 \qquad \text{que é multilinear} \end{aligned}$$

Exemplo 2.2.7. Se $f(x_1, x_2) = x_1^2 x_2$, então

$$\begin{aligned} f_1(x_1, x_2, x_3) &= f(x_1 + x_3, x_2) - f(x_1, x_2) - f(x_3, x_2) \\ &= (x_1 + x_3)^2 x_2 - x_1^2 x_2 - x_3^2 x_2 \\ &= x_1 x_3 x_2 + x_3 x_1 x_2 \qquad \text{que é multilinear} \end{aligned}$$

Exemplo 2.2.8. Seja $f = x_1^3$. Linearizemos f passo a passo. Primeiro tome:

$$\begin{aligned} f_1(x_1, x_2) &= f(x_1 + x_2) - f(x_1) - f(x_2) \\ &= (x_1 + x_2)^3 - x_1^3 - x_2^3 \\ &= x_1 x_2 x_1 + x_2 x_1^2 + x_2^2 x_1 + x_1^2 x_2 + x_1 x_2^2 + x_2 x_1 x_2 \end{aligned}$$

Como o polinômio resultante não é multilinear, aplicaremos também o processo a $f_1(x_1, x_2)$.

Agora tome:

$$\begin{aligned} f_2(x_1, x_2, x_3) &= f_1(x_1 + x_3, x_2) - f_1(x_1, x_2) - f_1(x_3, x_2) \\ &= (x_1 + x_3) x_2 (x_1 + x_3) + x_2 (x_1 + x_3)^2 + x_2^2 (x_1 + x_3) + (x_1 + x_3)^2 x_2 + \end{aligned}$$

$+(x_1+x_3)x_2^2+x_2(x_1+x_3)x_2-(x_1x_2x_1+x_2x_1^2+x_2^2x_1+x_1^2x_2+x_1x_2^2+x_2x_1x_2)-(x_3x_2x_3+$
$+x_2x_3^2+x_2^2x_3+x_3^2x_2+x_3x_2^2+x_2x_3x_2)$

Portanto,

$$f_2(x_1, x_2, x_3) = x_3 x_2 x_1 + x_1 x_2 x_3 + x_2 x_1 x_3 + x_2 x_3 x_1 + x_1 x_3 x_2 + x_3 x_1 x_2$$

que é multilinear.

2.2.2 Identidade Polinomial Generalizada

Um polinômio generalizado f sobre uma K-álgebra R é informalmente falando, um polinômio onde elementos da álgebra são permitidos aparecerem como coeficientes dos monômios e entre as letras.

Dizemos que R satisfaz uma identidade polinomial generalizada se existe um polinômio generalizado não nulo $f(x_1, \ldots, x_n)$ tal que $f(a_1, \ldots, a_n) = 0 \ \ \forall\ a_i \in R$.
Por exemplo, sendo $a,\ b,\ c\ \in R$ elementos quaisquer, $f(x_1, x_2) = a x_2 c x_1 - 7 x_1 b x_2$ é um polinômio generalizado sobre R.

Na definição a seguir, caracterizamos os polinômios generalizados. Por conveniência, trataremos apenas dos polinômios multilineares.

Definição 2.2.4. (Polinômio Multilinear Generalizado de grau n). Seja R uma álgebra sobre K. Dizemos que f é um polinômio multilinear generalizado de grau n se tem a forma:

$$f(x_1, x_2, \ldots, x_n) = \sum_{\sigma \in S_n} f^\sigma(x_1, x_2, \ldots, x_n),$$

onde f^σ é um polinômio da forma,

$$f^\sigma(x_1, x_2, \ldots, x_n) = \sum_{j=1}^{a_\sigma} \alpha_{0,\sigma,j} x_{\sigma(1)} \alpha_{1,\sigma,j} x_{\sigma(2)} \ldots \alpha_{n-1,\sigma,j} x_{\sigma(n)} \alpha_{n,\sigma,j},$$

em que cada $\alpha_{i,\sigma,j} \in R$ e a_σ é algum inteiro positivo.

Definição 2.2.5. (Polinômio multilinear generalizado não - degenerado). Dizemos que f é um polinômio multilinear generalizado não degenerado, se para algum $\sigma \in S_n$, $f^\sigma(x_1, x_2, \ldots, x_n)$ não é identidade polinomial generalizada para a álgebra R, ou seja, existem $r_1, r_2, \ldots, r_n \in R$, tal que $f^\sigma(r_1, r_2, \ldots, r_n) \neq 0$.

Capítulo 3

Conjectura de Brian Hartley

Neste capítulo apresentaremos a demonstração da Conjectura de Brian Hartley fornecida por A. Giambruno, E. Jespers e A. Valenti [4], para o caso particular em que R é um domínio comutativo infinito com característica $p \geq 0$ e G um p'-grupo de torção.

Proposição 3.0.1. Seja G um grupo. Se G satisfaz uma identidade de grupo $w(x_1, \ldots, x_n) = 1$, então G satisfaz uma identidade em duas variáveis $v(y_1, y_2) = 1$.

Demonstração: Seja $w(x_1, \ldots, x_n) = x_{i_1}^{r_1} \ldots x_{i_k}^{r_k}$ com $i_j \neq i_{j+1}$, $i_j \in \{1, \ldots, n\}$. Tomemos a identidade de grupo v:

$$v(y_1, y_2) = y_1^{-i_1} y_2^{r_1} y_1^{i_1 - i_2} \ldots y_1^{i_{k-1} - i_k} y_2^{r_k} y_1^{i_k}.$$

Como $i_j - i_{j+1} \neq 0$ para todo j, temos que v é não trivial. Vamos mostrar que G satisfaz $v = 1$. Sejam $g_1, g_2 \in G$. Vamos definir h_i como abaixo:

$$h_i = g_1^{-i} g_2 g_1^{i}$$

Assim temos para todo r inteiro

$$(h_i)^r = g_1^{-i} g_2^{r} g_1^{i}.$$

Por um lado, usando nossa hipótese, temos:

$$w(h_1, \ldots, h_n) = 1$$

E por outro lado:

$$w(h_1, \ldots, h_n) = h_{i_1}^{r_1} \ldots h_{i_k}^{r_k} =$$
$$g_1^{-i_1} g_2^{r_1} g_1^{i_1} g_1^{-i_2} \ldots g_2^{r_k} g_1^{i_k} =$$
$$g_1^{-i_1} g_2^{r_1} g_1^{i_1 - i_2} \ldots g_2^{r_k} g_1^{i_k} = v(g_1, g_2)$$

Portanto concluímos que $v(g_1, g_2) = 1$ para todos $g_1, g_2 \in G$. Logo G satisfaz $v = 1$.

$\square$

Observação 3.0.1. Na verdade, a palavra v satisfeita por G pode ser escrita de uma maneira mais refinada, ou seja, G satisfaz:

$$v_1 = x_1^{\gamma_1} x_2^{\delta_1} \ldots x_1^{\gamma_k} x_2^{\delta_k}$$

onde $\gamma_i, \ \delta_j \ \in \ \{\pm 1, \pm 2\}$.

Teorema 3.0.1. Seja A uma álgebra sobre um domínio comutativo infinito R e suponha que $U(A)$ satisfaz uma identidade de grupo. Existe um inteiro positivo m tal que se $a, \ b, \ c \ \in A$ e $a^2 = bc = 0$, então $bacA$ é um ideal nil à direita de expoente limitado menor que ou igual a m.

Demonstração: Usando a **Proposição 3.0.1**, podemos supor que U(A) satisfaz uma identidade de grupo nas variáveis x_1 e x_2 da forma:

(1) $x_1^{r_1} x_2^{s_1} x_1^{r_2} x_2^{s_2 \cdots} x_1^{r_k} x_2^{s_k} x_1^{r_{k+1}} = 1,$

onde $k \geq 1, \ r_i, \ s_i \ \in \mathbb{Z}$ e todos esses números inteiros são diferentes de zero, exceto possivelmente r_{k+1}. Se fizermos a substituição $x_1 = xy, \ x_2 = yx$ então temos uma identidade de grupo para $U(A)$ da forma:

(2) $(xy)^{r_1}(yx)^{s_1 \cdots}(xy)^{r_k}(yx)^{s_k}(xy)^{r_{k+1}} = 1.$

Seja $a, \ b \in A$ e $b = c$ tal que $a^2 = b^2 = 0$. Afirmamos que $abaA$ é um ideal nil à direita de expoente limitado. De fato, suponha primeiramente que $char R \neq 2$. Para $u \in A$ temos $(aua)^2 = (bauab)^2 = 0$ de modo que $1 + aua, \ 1 + bauab \in U(A)$ e seus inversos são respectivamente $(1 - aua)$ e $(1 - bauab)$. Agora avaliamos a identidade do grupo em $U(A)$ substituindo x e y por $1 + aua$ e $1 + bauab$ respectivamente; obtemos:

$((1 + aua)(1 + bauab))^{r_1}((1 + bauab)(1 + aua))^{s_1 \cdots}((1 + bauab)(1 + aua))^{s_k}((1 +$
$+ \ aua)(1 + bauab))^{r_{k+1}} = 1,$
para todo $a, \ b, \ u \in A, \ a^2 = b^2 = 0$.
Observamos que para $c \in A, \ n \in \mathbb{Z}, \ c^2 = 0$ implica que $(1 + c)^n = 1 + nc$, fato este que facilmente pode ser provado por indução sobre n; assim ao calcular todos os produtos na igualdade acima, obtemos uma expressão da forma $f(aua, bauab) = 0$, onde $f(x_1, x_2)$ é um polinômio não nulo com coeficientes integrais nas variáveis não comutadas $x_1, \ x_2$; além disso $f(x_1, \ x_2)$ tem termo constante zero. Segue-se que se $\lambda \in R$, então substituindo u por λu e expandindo, a identidade anterior pode ser escrita na forma:

(3) $\lambda p_1 + \lambda^2 p_2 + \ldots + \lambda^l p_l = 0,$

onde $p_1, \ldots, p_l$ são expressões polinomiais com coeficientes integrais em aua e $bauab$.

Podemos escrever a igualdade (3) acima de forma matricial:

$$\begin{bmatrix} 1 & \lambda_1 & \lambda_1^2 & \dots & \lambda_1^l \\ 1 & \lambda_2 & \lambda_2^2 & \dots & \lambda_2^l \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_{l+1} & \lambda_{l+1}^2 & \dots & \lambda_{l+1}^l \end{bmatrix} \begin{bmatrix} 0 \\ p_1 \\ \vdots \\ p_l \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

e usando o fato de que R é um domínio comutativo infinito de divisores diferentes de zero em A e como o determinante da matriz de Vandermonde acima é não nulo, podemos concluir que $p_1 = \ldots = p_l = 0$. Como cada variável em (2) pode aparecer com o expoente 1 ou -1, ou 2 ou -2, então $p_l = 0$ implica:

$$2^r(abau)^s = 0$$

para algum inteiro r e s, com $0 \leq r$ e $1 \leq s \leq m$, onde $m = 2+2|r_{k+1}|+2\sum_{i=1}^{k}|r_i|+|s_i|$.

Como $char R \neq 2$, $2^r(abau)^s = 0$ implica que $(abau)^s = 0$, para todos $a,\ b,\ u \in A$, $a^2 = b^2 = 0$. Portanto, $abaA$ é ideal nil de expoente limitado menor que ou igual m.
Suponha agora que $char R = 2$. Na identidade de grupo (1) substitua x_1 por x_1x_2 e x_2 por x_1x_3. Deste modo obtemos uma identidade para $U(A)$ da forma:

(4) $(x_1x_2)^{r_1}(x_1x_3)^{s_1\cdots}(x_1x_2)^{r_k}(x_1x_3)^{s_k}(x_1x_2)^{r_{k+1}} = 1,$

e cada variável em (4)(como uma palavra reduzida) pode aparecer com expoente 1 ou -1.
Seja $u \in A$, como $char R = 2$, temos que $((a+ba)u(a+ab))^2 = 0$, pois $((a+ba)u(a+$ $+ab))^2 = ((a+ba)u(a+ab))\cdot((a+ba)u(a+ab)) = (aua+auab+baua+bauab)(aua+$ $+auab+baua+bauab) = 2auabaua+2auabauab+2bauabaua+2bauabauab = 0$ de modo que $1+(a+ba)u(a+ab)$ é uma unidade de $U(A)$ com inversa $1-(a+ba)u(a+ab)$. Avaliemos agora a identidade de grupo (4) em $U(A)$, substituindo x_1 por $1+aua$, x_2 por $1+bauab$ e x_3 por $1+(a+ba)u(a+ab)$. Obtemos:

$$((1+aua)(1+bauab))^{r_1}((1+aua)(1+(a+ba)u(a+ab)))^{s_1\cdots} = 1.$$

Tome agora $\lambda \in R$ e troque u por λu, então obtemos uma igualdade da forma: $\lambda p_1 +$ $\lambda^2 p_2 + \ldots + \lambda^l p_l = 0$ e pelo argumento do determinante de Vandermonde concluímos que $p_l = 0$. Agora por um cálculo direto, é fácil verificar que $p_l = 0$ implica $(abau)^s = 0$ para algum inteiro s com $1 \leq s \leq m$. Assim, $abaA$ é um ideal nil à direita de expoente limitado menor que ou igual a m.
Seja agora, $a^2 = cd = 0$, temos que para todo $u \in A$, $(duc)^2 = 0$, pois $(duc)(duc) = 0$. Logo para $a^2 = (duc)^2 = 0$ obtemos que $(duc)a(duc)A$ é nil e assim $(duc)a(duc)a$ é nilpotente, digamos que $((duc)a(duc)a)^n = 0$ para algum n, é fácil ver que $cadA$ é um ideal nil de expoente limitado menor que ou igual a m.

□

Lema 3.0.1. Seja A uma álgebra sobre um domínio comutativo R. Suponha que para todo $a,\ b,\ c \in A$ tal que $a^2 = bc = 0$, temos $bac = 0$, então todo idempotente de $R^{-1}A$ (o anel de frações de A com respeito aos elementos não-nulos de R) é central.

Demonstração: Seja e um idempotente em $R^{-1}A = \{\frac{a}{r} \mid 0 \neq r \in R\ e\ a \in A\}$, e como e é idempotente temos $e^2 = e$. Seja $e = \frac{f}{r}$, multiplicando à esquerda por r, obtemos $f = re \in A$.

Temos que $(re)^2 = rere = r^2ee = r^2e^2 = r^2e$.
Consideremos $b = f$ e $c = (r - f)$, temos que:

$$f(r-f) = re(r-re) = r^2e - r^2e^2 = r^2e - r^2e = 0.$$

Se $u \in R^{-1}A$, afirmamos que:

$$(fu(r-f))^2 = 0$$

De fato, pois:

$$\begin{aligned}(reu(r-re))^2 &= (reur - reure)^2 \\ &= (r^2eu - r^2eue)^2 \\ &= (r^2eu - r^2eue)(r^2eu - r^2eue) \\ &= r^2eur^2eu - r^2eur^2eue - r^2euer^2eu + r^2euer^2eue \\ &= r^4eueu - r^4eueue - r^4eueu + r^4eueue \\ &= 0\end{aligned}$$

Assim, por hipótese temos:

$$f \cdot (fu(r-f)) \cdot (r-f) = 0$$

Logo,

$$\begin{aligned}f(fu(r-f)r) - f(fu(r-f))f &= 0 \\ re(reu(r-re)r) - re(reu(r-re))re &= 0 \\ re(r^3eu - r^3eue) - re(r^3eue - r^3euee) &= 0 \\ r^4eeu - r^4eeue - r^4eeue + r^4eeue &= 0 \\ r^4eu - r^4eue - r^4eue + r^4eue &= 0\end{aligned}$$

Consequentemente, $r^4eu - r^4eue = 0$
Como r não é divisor de zero, segue que

$$eu = eue.$$

De forma análoga, concluímos que $ue = eue$,
e portanto temos $ue = eu$ para todo idempotente de $R^{-1}A$ e para todo u de $R^{-1}A$. Logo todo idempotente de $R^{-1}A$ é central.

$\square$

Proposição 3.0.2 (Levitzky). [**Ver [17], Corolário 1.6.26**]. Seja R um anel. E seja $\mathcal{H}(R)$ o conjunto:

$$\mathcal{H}(R) = \{a \in R \mid aR \text{ é ideal nil de expoente limitado}\}$$

Se R é um anel semiprimo então $\mathcal{H}(R) = 0$.

Corolário 3.0.1. Seja A uma álgebra semiprima em um domínio comutativo infinito R. Se $U(A)$ satisfaz uma identidade de grupo, então todo idempotente de $R^{-1}A$ é central.

Demonstração: Tomemos $a, b, c \in A$ tal que $a^2 = bc = 0$. Pelo **Lema 3.0.1**, basta mostrarmos que $bac = 0$.
Pelo **Teorema 3.0.1** temos que $bacA$ é ideal nil à direita de expoente limitado. Suponhamos que $bac \neq 0$, então $\mathcal{H}(A) \neq 0$, pela **Proposição 3.0.2** A não seria semiprima. Assim temos $bac = 0$ e pelo **Lema 3.0.1** segue o resultado.

□

Proposição 3.0.3. [**Ver [13], Teorema IV.2.12**] . Seja KG álgebra de grupo e $char(K) = 0$. Então, KG é álgebra semiprima.

Proposição 3.0.4. [**Ver [13], Teorema IV.2.13**] . Seja KG a álgebra de grupo e $charK = p > 0$, são equivalentes:

(a) KG é semiprimo.

(b) $\phi(G)$ é um $p' - grupo$.

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

Lema 3.0.2. [**ver [7], Teorema 2**] . Seja G um grupo finito. Então exatamente uma das condições seguintes ocorre:

(i) G é abeliano(e $U(\mathbb{Z}G)$ também o é),

(ii) G é um $2-$grupo hamiltoniano, e $U(\mathbb{Z}G) = \{\pm g : g \in G\}$,

(iii) $U(\mathbb{Z}G)$ contém um subgrupo livre de posto 2.

Lema 3.0.3. [**ver [3], Lema 4.2**] .Seja $Q_8 = \langle a, b : a^4 = 1,\ a^2 = b^2,\ bab^{-1} = a^{-1}\rangle$, o grupo dos quatérnios de ordem 8. Então $U(\mathbb{Z}_{(p)}Q_8)$ contém um grupo livre não-cíclico.

Corolário 3.0.2. Seja G um grupo e R um domínio comutativo infinito. Suponhamos que $\phi(G)$ seja um $p' - grupo$ no caso $char(R) = p > 0$. Se $U(RG)$ satisfaz uma identidade de grupo, então qualquer $p' - subgrupo$ de torção de G é normal em G, e portanto, $G_{p'}$ é um grupo abeliano ou um grupo hamiltoniano.
Se além disso, $char(R) = 0$, então $G_{p'}$ é um grupo abeliano ou um $2 - grupo$ hamiltoniano; apenas ocorre o primeiro caso se R também for um domínio local.

Demonstração: Seja $charR = p > 0$ e $\phi(G)$ um p'-grupo, pela **Proposição 3.0.4**, RG é uma álgebra semiprima. E como $U(RG)$ satisfaz uma identidade de grupo, pelo **Corolário 3.0.1** para qualquer $g \in G_{p'}$ de ordem n, o idempotente

$\frac{\hat{g}}{n} = n^{-1}(1 + g + \ldots + g^{n-1}) = e = e^2$ é central em KG, onde K é o corpo de frações de R e $\hat{g} = 1 + g + \ldots + g^{n-1}$.

Afirmamos que $\langle g \rangle$ é normal em G.

De fato, temos que:

$$n^{-1}\hat{g}h = hn^{-1}\hat{g} \Rightarrow \hat{g}h = h\hat{g} \;\; \forall \;\; h \in G$$

Logo,

$$(1+g+g^2+\ldots+g^{n-1})h = h(1+g+g^2+\ldots+g^{n-1})$$
$$h+gh+g^2h+\ldots+g^{n-1}h = h+hg+hg^2+\ldots+hg^{n-1}$$

Em particular, pela unicidade da escrita temos $gh = hg^j \Rightarrow h^{-1}gh = g^j \in \langle g \rangle$, logo $\langle g \rangle \triangleleft G$, e mais, $G_{p'}$ é um subgrupo de G. De fato, dados $x, y \in G_{p'}$, como $o(x) = o(x^{-1})$ então $x^{-1} \in G_{p'}$, pois também é um $p' - elemento$. Para mostrar que $G_{p'}$ é subgrupo, basta-nos mostrar que $xy \in G_{p'}$. Como para cada $x, y \in G_{p'}$ temos $xy = yx^j$ e consequentemente $(xy)^n = y^n x^{k_n}$ para algum inteiro k_n. Tomando $n = o(y)$, obtemos $(xy)^n = x^{k_n}$ e elevando esta expressão a $m = o(x)$, obtemos $(xy)^{mn} = 1$, logo $o(xy) \setminus mn$, então $p \nmid o(xy)$ e assim $xy \in G_{p'}$. Logo $G_{p'}$ é um subgrupo de G.

Considere agora $H \leq G_{p'}$. Para todo $g \in H$ temos $\langle g \rangle \subset H \Rightarrow \langle g \rangle \subset G_{p'}$. Vimos que $\langle g \rangle \triangleleft G \Rightarrow \forall\ q \in G_{p'} \;\; q^{-1}gq \in \langle g \rangle \subset H$. Portanto, $H \triangleleft G_{p'}$.
Como todo subgrupo H de $G_{p'}$ é normal, segue que $G_{p'}$ é um grupo abeliano ou um grupo hamiltoniano. E assim provamos a primeira parte da afirmação.

Se $charR = 0$, pela **Proposição 3.0.3** RG é uma álgebra semiprima e analogamente ao caso anterior, concluímos que $G_{p'}$ é um grupo abeliano ou um grupo hamiltoniano. Considerando que $G_{p'}$ seja hamiltoniano. Como charR=p=0, temos que $G_p = 1$ e $G_{p'} = G_t$, o grupo de torção, e para qualquer subgrupo não abeliano finito H de G_t, temos $H = Q_8 \times E \times A$, onde Q_8, E e A são da forma como descritos no **Teorema 1.1.2**. Como $U(\mathbb{Z}H) \subset U(RG)$, temos que $U(\mathbb{Z}H)$ satisfaz uma identidade de grupo, consequentemente este grupo de unidades não contém um subgrupo livre não cíclico. Pelo **Lema 3.0.2** implica que A é trivial. Logo G_t é um $2-$grupo Hamiltoniano.
Mostraremos agora que G_t é na verdade Abeliano se R é local. De fato, suponha que G_t seja hamiltoniano, isto é, $G_t = Q_8 \times \hat{E} \times \hat{A}$. Consideremos $\mathbb{Z}_{(p)}$, o anel de localização de $\mathbb{Z}$ no ideal primo (p), temos que $\mathbb{Z}_{(p)} \subset \mathbb{Q} \subset R$. E como $Q_8 \leq G_t$, então $U(\mathbb{Z}_{(p)}Q_8) \subseteq U(RG)$ para algum inteiro primo p. Logo $U(\mathbb{Z}_{(p)}Q_8)$ também satisfaz uma identidade de grupo. No entanto, isso é impossível, pois pelo **Lema 3.0.3** $U(\mathbb{Z}_{(p)}Q_8)$ contém um subgrupo livre não-cíclico. Logo G_t é abeliano.

□

Lema 3.0.4. Seja A uma K-álgebra e suponha que $A = RS = \{\Sigma_i r_i s_i \mid r_i \in R, s_i \in S\}$, onde R é uma subálgebra central e S um subconjunto de A, se $f(x_1, \ldots, x_n) \in K\langle x_1, x_2, ..., x_n \rangle$ é um polinômio multilinear, então $f(A) \subseteq Rf(S)$. Em particular, f é uma identidade polinomial para A se, e somente se, $f(S) = 0$.

Demonstração: Sejam $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$. Por hipótese temos

$$\sum_{j=1}^{t_i} r_{i_j} s_j \qquad i = 1, 2, \ldots, n$$

com $r_{i_j} \in R$ e $s_j \in S$. Como f é multilinear e R é central obtemos

$$\begin{aligned} f(\alpha_1, \alpha_2, \ldots, \alpha_n) &= f(\Sigma_{j=1}^{t_1} r_{1_j} s_j, \Sigma_{j=1}^{t_2} r_{2_j} s_j, \ldots, \Sigma_{j=1}^{t_n} r_{n_j} s_j) \\ &= \sum_{j_1,\ldots,j_n} r_{1_{j_1}} r_{2_{j_2}} \ldots r_{n_{j_n}} f(s_{j_1}, s_{j_2}, \ldots, s_{j_n}) \in Rf(S) \end{aligned}$$

e o Lema está provado.

□

Lema 3.0.5. [**Ver [13], Teorema V.3.15**] . Seja KG um anel de grupo. São equivalentes:

1. $[G : \phi(G)] < \infty$ e $|(\phi(G))'| < \infty$;

2. KG possui um idempotente e diferente de zero, tal que $eKGe$ satisfaz uma identidade polinomial;

3. KG satisfaz uma identidade polinomial multilinear generalizada não degenerada.

Agora já temos tudo que precisamos para demonstrar a conjectura de Hartley, para o caso em que R é um domínio comutativo infinito com $charR = p \geq 0$ e G um grupo de torção que não contém $p - elementos$. Então:

Teorema 3.0.2. Seja G um grupo de torção e R um domínio comutativo infinito. Se $U(RG)$ satisfaz uma identidade de grupo, então:

1. Se $charR = 0$ ou $charR = p$ e G é um $p' - grupo$, então RG satisfaz s_4, a identidade standard de grau 4;
2. Se $charR = p > 0$ e G é qualquer grupo, então, ou $\phi(G)$ é de índice finito em G e $\phi(G)'$ é um grupo finito ou existe um inteiro fixo $m > 0$ tal que para todo $a,\ b,\ c \in RG$ com $a^2 = bc = 0$, temos que $bacRG$ é um ideal nilpotente de expoente menor que m.

Demonstração: Seja K o corpo de frações de R, ou seja, $K = R^{-1}R$. Se $charR = 0$ ou $charR = p$ e G é um p'-grupo, então pelo **Corolário 3.0.2**, G é um grupo abeliano ou um grupo hamiltoniano. Se G é abeliano, então RG satisfaz o polinômio $s_2(x_1, x_2) = x_1x_2 - x_2x_1$ e pelo **Lema 2.2.1** , item (iv), RG também satisfaz s_4. se G é hamiltoniano, isto é, $G = Q_8 \times E_1 \times A_1$, conforme descrito no **Teorema 1.1.2** e seja $A \leq G$ tal que:
$A = \langle a \rangle \times E_1 \times A_1$, em que $\langle a \rangle$ é subgrupo de $Q_8 = \langle a, b : a^4 = 1,\ a^2 = b^2,\ bab^{-1} = a^{-1} \rangle$ e $|\langle a \rangle| = 4$.
Temos que:
$\frac{G}{A} \cong \frac{Q_8}{\langle a \rangle} \Rightarrow (G : A) = 2$, com A abeliano, pois $\langle a \rangle$ é cíclico, E_1 e A_1 são ambos abelianos.
Como A tem índice finito 2, pelo **Lema 2.2.4** $KG \subseteq M_2(KA)$, e pelo **Teorema 2.2.2** $M_2(KA)$ satisfaz a identidade standard de grau 4, consequentemente KG satisfaz s_4 e

portanto, RG também satisfaz s_4.

Suponha agora que $charR = p > 0$. Como por hipótese $U(RG)$ satisfaz uma identidade de grupo, temos que, pelo **Teorema 3.0.1** existe um inteiro $m > 0$ tal que para todo $a, b, c \in RG$ com $a^2 = bc = 0$ temos que $bacRG$ é um ideal nil à direita de expoente limitado menor que ou igual a m. Suponha que para convenientes $a, b, c \in RG$ acontece que $(bacRG)^m \neq 0$. Como $bacRG$ é nil de expoente no máximo m, então claramente $bacRG$ satisfaz a identidade polinomial $x^m = 0$. Pelo **Teorema 2.2.3** temos que $bacRG$ satisfaz uma identidade multilinear

$$\tilde{f} = \sum_{\sigma \in S_m} x_{\sigma(1)} ... x_{\sigma(m)} = 0$$

$\Rightarrow \forall x_1, \ldots, x_m \in RG$, temos:

$$f(x_1, x_2, \ldots, x_m) = \tilde{f}(bacx_1, bacx_2, \ldots, bacx_m) = \sum_{\sigma \in S_m} bacx_{\sigma(1)} bacx_{\sigma(2)} \ldots bacx_{\sigma(m)}$$

Logo RG satisfaz a identidade polinomial multilinear generalizada,

$$f = \sum_{\sigma \in S_m} bacx_{\sigma(1)} bacx_{\sigma(2)} \ldots bacx_{\sigma(m)},$$

Como $(bacRG)^m \neq 0$, $\Rightarrow$ existe $bac\alpha_1 bac\alpha_2 \ldots bac\alpha_m \neq 0$, com $\alpha_i \in RG$, tal que

$$bac\alpha_{\sigma(1)} bac\alpha_{\sigma(2)} \ldots bac\alpha_{\sigma(m)} \neq 0,$$

onde $\sigma = id$.

Portanto f é identidade polinomial multilinear generalizada não-degenerada para RG. Logo KG satisfaz a mesma identidade polinomial multilinear generalizada não-degenerada. Portanto, pelo **Lema 3.0.5** $\phi(G)$ é de índice finito em G e $\phi(G)'$ é um grupo finito.

$\square$

Referências Bibliográficas

[1] Ash, R. B. *A Course in Algebraic Number Theory.* Dover Publications, 2010.

[2] Brešar, M. *Introduction to Noncommutative Algebra*, Universitext. Springer International Publishing, 2014. 1994.

[3] Dokuchaev, M. A. ; Gonçalves, J. Z. *Semigroup Identities on Units of Integral Group Rings*, 1994.

[4] Giambruno, A.; Jespers, E.; Valenti, A. *Group identities on units of rings*, Arch. Math 63(1994), pp. 291-296.

[5] Giambruno, A.; Sehgal, S.; Valenti, A. *Group algebras whose units satisfy a group identity*, Proc. Amer. Math. Soc. 125 (1997), pp. 629–634.

[6] Gonçalves, J. Z. ; Mandel, A. *Semigroup Identities on Units of Group Algebras*, Arch. Math. 57(1991), pp. 539-545.

[7] Hartley, B; Pickel, F. *Free subgroups in the unit groups of integral group rings*, Arch. Math. 32(1980), pp. 1342-1352.

[8] Hungerford, T. W. *Álgebra. Graduate Texts in Mathematics.* New York, Springer, 1993.

[9] Liu, C.H. *Group algebras with units satisfying a group identity*,Proc. Amer. Math. Soc. 127 (1999), pp. 327–336.

[10] Liu, C.H.; Passman, D. S. *Group algebras with units satisfying a group identity II*, Proc. Amer. Math. Soc. 127 (1999), pp. 337–341.

[11] Lyndon, R.C.; Schupp, P.E. *Combinatorial Group Theory. Classics in Mathematics*, Springer Berlin Heidelberg, 2001.

[12] Menal, P. *Private letter to B. Hartley*, April 6, 1981.

[13] Pasman, D. S. *The algebraic structure of groups rings.* New York, Wiley-interscience, 1977.

[14] Pasman, D. S. *Group Algebras Whose units satisfy a Group II.* Proc. Amer. Math. Soc. 125 (1997), pp. 657–662.

[15] Polcino, C.; Sehgal, S. K. *An Introduction to Group Rings.* Dordrecht, Kluwer Academic Publishers, 2002.

[16] Robinson, D. J. S. *A Course in the theory of Groups*, 2nd edition. Springer Verlag, New York, 1995.

[17] Rowen, L. *Polynomial Identities in Ring Theory*, london-New York-San Francisco, 1980.

[18] Sehgal, S. K. *Topics in Group Rings*. New York, 1978.

[19] Sehgal, S. K. *Units in Integral Group Rings*. New York, Essex, 1993.

[20] Warhurst, D. S. *Topics in Group Rings*. Tesis, Manchester, 1981.