Álgebras de Grupo Cujas Unidades Satisfazem uma Identidade de Grupo

Raul Antonio Ferraz

DISSERTAÇÃO APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA
OBTENÇÃO DO GRAU
DE
MESTRE EM MATEMÁTICA

Área de Concentração: **Álgebra**
Orientador: **Prof. Dr. Jairo Zacarias Gonçalves**

Durante este trabalho, o autor teve o apoio financeiro do CNPq

26 de Setembro de 1997

Álgebras de Grupo Cujas Unidades Satisfazem uma Identidade de Grupo

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Raul Antonio Ferraz e aprovada pela comissão julgadora.

São Paulo, 26 de setembro de 1997.

Banca examinadora:

- Prof. Dr. Jairo Zacarias Gonçalves (Orientador) - IME - USP
- Prof. Dr. Francisco César Polcino Milies - IME - USP
- Prof. Dr. Guilherme Augusto de La Rocque Leal - UFRJ.

Dedicada à memória de *Mariana Issa Steiner*
(19/08/13-17/11/94)

There is no permanent place in the world for ugly mathematics.

G. H. Hardy

Agradecimentos

A Deus por me dar saúde, e me reconfortar nos momentos mais díficeis.

Ao meu orientador Prof. Dr. Jairo Zacarias Gonçalves pelo excelente trabalho de orientação e pelo apoio, incentivo, paciência e atenção constantes durante o trabalho.

Aos meus pais Thelmo e Neuza pelo carinho, amor, afeto, dedicação, atenção, ...enfim, por tudo que sempre fizeram por mim.

Aos meus familiares pelo apoio incentivo amor e carinho que sempre me dedicaram.

Ao Carlos Juiti Watanabe pela inestimável ajuda com os computadores das ET's., sem a qual esta tese não existiria. Gostaria de agradecer também ao Claus pelos vários conselhos sobre o Latex.

Aos meus colegas de graduação, mestrado, e doutorado pelo companheirismo.

A Luis Renato e Pedro pelas listas que tivemos a oportunidade de discutir juntos.

A Patrícia pela colaboração durante os exames de Cálculo e Funções Analíticas, sem a qual não conseguiria aprovação.

Ao Samuel pelas encomendas de livro que tive a oportunidade de fazer através de sua conta na Amazon.com.

A Daniel, Fernando e Walquíria pela companhia nos intermináveis lanches vespertinos.

Às professoras Profa. Dra. Iracema Bund, e Profa. Dra. Carmen Sílvia Cardassi pela oportunidade da Iniciação Científica que me despertou o gosto pela pesquisa em Matemática. Em particular à Profa. Dra. Carmen Sílvia Cardassi pelo carinho e atenção que sempre teve comigo durante o período em que me orientou.

A todos professores com os quais tive o prazer de ter assistido aulas e através delas enriquecer o meu conhecimento em Matemática.

Aos professores da área de de Álgebra não comutativa, em especial as professoras Profa. Dra. Marly Mandia e Profa. Dra. Leilá Maria Vasconcelos Figueiredo.

Aos Professores Prof. Dr. Daniel Levcovitz e Prof. Dr. Paulo Agozzini Martins, pela atenção especial que tiveram por mim durante o mestrado.

Ao CNPq pelo apoio financeiro durante a elaboração desta dissertação.

Resumo:

Seja $F[G]$ a álgebra de grupo do grupo G sobre o corpo F, e seja $U(F[G])$ o seu grupo de unidades. O principal objetivo deste trabalho é investigar a validade da seguinte conjectura, devida a Brian Hartley.(problema 52, pag 307 de [Seh93]):

Conjectura: Se G é um grupo de torção e $U(F[G])$ satisfaz uma identidade de grupo, então $F[G]$ satisfaz uma identidade polinomial.

Como suporte da afirmação acima provaremos:

Teorema 1:[GJV94],[GSV97]. A conjectura é verdadeira se F é infinito.

Teorema 2:[Pas97]. Se F é infinito, char $F = p > 0$ e G é um grupo de torção, então $U(F[G])$ satisfaz uma identidade de grupo se, e somente se, G possui um subgrupo abeliano normal de índice finito, e G' é um p-grupo de expoente limitado.

Abstract:

Let $F[G]$ be the group ring of the group G over the field F, and let $U(F[G])$ be its group of units. The main objective of this work is to investigate the following conjecture, due to Brian Hartley

Conjecture: If G is a torsion group, and $U(F[G])$ satisfies a group identity, then $F[G]$ satisfy a polynomial identity.

In support of the statement above we prove:

Theorem 1: **[GJV94],[GSV97]** The conjecture is true when F is infinite.

Theorem 2: **[Pas97]** If F is infinite, char$F = p > 0$ and G is a torsin group, then $U(F[G])$ satisfies a group identity if and only if, the group G owns a p-abelian normal subgroup of finite index, and G' is a p-group of bounded expoent.

Índice de notações:

(m, n)	mdc entre m, e n.
$\mathbb{Z}$	Anel dos números inteiros.
$\mathbb{Q}$	Corpo dos números racionais.
G,H	Grupos.
$\|G\|$	Ordem do grupo.
$o(g)$	ordem do elemento g de um grupo.
$per(G)$	Expoente (período) do grupo G.
$cl_G(g)$	Classe de conjugação do elemento g no grupo G.
$Z(G)$	Centro do grupo G.
$\langle g \rangle$	Grupo cíclico gerado por g.
$\langle A_1, \ldots A_n \rangle$	Grupo gerado pelos conjuntos $A_1, \ldots A_n$.
$[G : H]$	Índice do subgrupo H em G.
G'	Comutador do grupo G.
$\cong$	É isomorfo a.
Q_8	Grupo dos Quatérnios.
P	Conjunto dos p-elementos.
Q	Conjunto dos p'-elementos.
(g, h)	Comutador multiplicativo.$(g^{-1}h^{-1}gh)$
$[g, h]$	Comutador aditivo.$(xy - yx)$
R	Anel,ou álgebra.
$tr(x)$	Traço do elemento x. (ver cap 4, seç 2.)
F	Corpo.
$\mathcal{J}(R)$	Radical de Jacobson do anel R.
$GF(n)$	Corpo finito com n elementos.

$M_n(R)$	Anel de matrizes $n \times n$, com entradas no anel R.
$[\alpha_{i,j}]$	Matriz pertencente a $M_n(R)$.ver proposição 4.14.
$Z(R)$	Centro do anel R.
$U(R)$	Grupo de unidades do anel R.
$char(R)$	Característica do anel.
$F[G]$	Anel de grupo do grupo G, sobre o corpo F.
$\Delta(G)$	Ideal de aumento do anel $F[G]$.
$\Delta(G,N)$	Kernel do epimorfismo canônico de $F[G]$ em $F[G/\Lambda$
$\mathcal{F}$	Grupo livre.
$F\langle x_1,\ldots,x_n\rangle$	Álgebra livre sobre o corpo F, a n variáveis.
$\mathcal{A}, F\langle x_1,\ldots x_n\rangle[[t]]$	Série de potências de t em $F\langle x_1,\ldots x_n\rangle[[t]]$.
$\omega(x_1,\ldots x_n)=1$	Identidade de grupo.
$p(x_1,\ldots x_n)=0$	Identidade Polinomial.
$\Gamma_n(x_1,\ldots,x_n)=0$	Identidade Polinomial Standard.
S_n	Grupo de permutações a n variáveis.
$\mathcal{S}(\sigma)$	Sinal da permutação sigma.
$\mathcal{H}(R)$	Conjunto dos elementos $a \in R$, tal que aR é nil de expoente limitado.
$\Phi(G)$	Grupo dos elementos de conjugação finita de G.
$\Phi_p(G)$	$\langle \Phi(G) \cap P\rangle$
$N(R)$	Soma dos ideais nilpotentes de R.
$\mathcal{N}(R)$	Conjunto dos elementos nilpotentes de R.
$H \leq G$	H é subgrupo de G.
$A \leq R$	A é subanel de R.
$A \rtimes H$	Produto semidireto de A por H.
$supp(h)$	Suporte do elemento h.

Conteúdo

Capítulo 1

Introdução

Seja $F[G]$ o anel de grupo do grupo G sobre o corpo F, e seja $U(F[G])$ o seu grupo de unidades.

Investigando a estrutura de $U(F[G])$, Brian Hartley propôs:

Conjectura: Se a característica de F é $p > 0$ G é um p-grupo localmente finito e $U(F[G])$ satisfaz uma identidade de grupo, então $F[G]$ satisfaz uma identidade polinomial. [War81]

Os primeiros resultados confirmando esta conjectura foram obtidos por Gonçalves e Mandel, [GM91], assumindo que o cardinal de F é infinito e que a identidade satisfeita por $U(F[G])$ é uma identidade de semigrupo.

A seguir, em [GJV94], Giambruno, Jespers, e Valenti estudam o caso semiprimo para identidades de grupo. Posteriormente, em [GSV97], Giambruno, Sehgal, e Valenti conseguem remover esta restrição, e em [Pas97], Passman dá uma condição necessária e suficiente para que $U(F[G])$ satisfaça uma identidade de grupo quando $p > 0$.

Muito recentemente, Chia Hsin Liu [Liu] demonstrou que se G é um grupo de torção F é um corpo qualquer (não necessariamente infinito), e $U(F[G])$ satisfaz uma identidade de grupo, então $F[G]$ satisfaz uma identidade polinomial, confirmando a Conjectura de Hartley.

Neste trabalho trataremos apenas do caso em que F é infinito. Detalharemos a caracterização dos grupos, conforme Passman no caso em que F tem característica $p > 0$.

Inicialmente vamos enunciar alguns teoremas que nos serão úteis na compreensão desta dissertação. Demonstraremos alguns e indicaremos demonstrações detalhadas

de outros.

No capítulo 2, estudaremos álgebras semiprimas, cujo o grupo de unidades satisfaz uma identidade de grupo. Concluindo, entre outros resultados, que nesta álgebra todo idempotente é central.

No capítulo 3, demonstraremos que $F[G]$ satisfaz uma identidade polinomial, sempre que F é um corpo infinito, G é um grupo de torção, e $U(F[G])$ satisfaz uma identidade de grupo.

Por fim, no capítulo 4, mostraremos que no caso em que F tem característica $p > 0$, $U(F[G])$ irá satisfazer uma identidade de grupo, se e somente se G' for p-grupo de período limitado, e G possuir um subgrupo A normal p-abeliano de índice finito.

1.1 Alguns Teoremas da Teoria de Grupos

Nesta seção enunciaremos alguns teoremas sobre teoria de grupos, muitos dos quais consagrados pelo constante uso em trabalhos nesta área.

Definição 1.1. *Dizemos que um grupo G é* **hamiltoniano** *se ele é da forma*

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

onde Q_8 é grupo dos Quatérnios, E é um 2-grupo abeliano elementar e A é um grupo abeliano de torção, no qual todo elemento tem ordem ímpar.

Teorema 1.2 (Dedekind-Baer). *Seja G um grupo. São equivalentes:*

1. *Todo subgrupo de G é normal em G*
2. *Todo subgrupo cíclico de G é normal em G*
3. *G é ou abeliano ou hamiltoniano.*

DEMONSTRAÇÃO: pag 143, teorema 5.3.7 de [Rob95]. ■

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

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

Proposição 1.3. *Seja G um grupo com um subgrupo H central de índice finito $[G : H] = n$. Então G' é finito, com ordem menor ou igual a $(n^2)^{n^3}$.*

DEMONSTRAÇÃO: pag 115, teorema 1.4 do capítulo 4 de [Pas77]. ■

Definição 1.4. *Seja G um grupo. Dizemos que G é* **localmente finito** *se todo subgrupo finitamente gerado de G é finito.*

Teorema 1.5 (Teorema de Schmidt). *Seja G um grupo e H um subgrupo normal de G. Se H e $\frac{G}{H}$ são localmente finitos, então G é localmente finito.*

DEMONSTRAÇÃO: pag 429, teorema 14.3.1 de [Rob95].■

Nem sempre é verdade que um subgrupo H de um grupo G finitamente gerado, é finitamente gerado. Se tomarmos G o grupo livre de posto 2, e H o seu comutador teremos que G é finitamente gerado mas H não. Porém, em um caso particular podemos concluir que H é finitamente gerado.

Proposição 1.6. *Seja G um grupo finitamente gerado e H um subgrupo de índice finito. Então H é finitamente gerado.*

DEMONSTRAÇÃO: pag 36, teorema 1.6.11 de [Rob95]. ■

1.2 Noções de Teoria de Anéis.

Nesta seção vamos recordar alguns fatos básicos da teoria de anéis.

Definição 1.7. *Seja R um anel. Dizemos que R é* **artiniano a esquerda** *se toda cadeia descendente de ideais a esquerda de R é estacionária. Ou seja, se I_1, I_2, ... , são ideais de R, com*

$$I_1 \geq I_2 \geq I_3 \geq ....$$

então existe um $k \in \mathbb{N}$ tal que para todo $n \geq k$

$$I_n = I_k.$$

Seja R um anel unitário. Sabe-se que a intersecção dos ideais maximais a esquerda de R, coincide com a intersecção dos ideais maximais a direita. Usando tal fato definimos:

Definição 1.8. *Seja R um anel unitário. O* **radical de Jacobson de R,** *como sendo a intersecção de todos ideais maximais a esquerda de R. E o denotamos por $\mathcal{J}(R)$, ou não havendo risco de dubiedade apenas por $\mathcal{J}$.*

Proposição 1.9. *Se R é um anel artiniano e unitário, então $\mathcal{J}(R)$ é nilpotente.*

DEMONSTRAÇÃO: ver pag 56 teorema 4.12 de [Lam91].■

Definição 1.10. *Dizemos que um anel R é* **semiprimitivo** *se $\mathcal{J}(R)$ é o ideal nulo.*

Definição 1.11. *Dizemos que um anel R é* **semiprimo** *se R não tem ideais nilpotentes não triviais.*

Sempre podemos encarar R como sendo um módulo sobre si mesmo. Assim podemos definir anel semi-simples:

Definição 1.12. *Seja R um anel. Dizemos que R é* **semi-simples a esquerda** *, se todo submódulo a esquerda I de R é somando direto de R. Isto é, para todo submódulo a esquerda de I, existe um submódulo a esquerda J, tal que $I \cap J = (0)$, e $I + J = R$. Denotamos a soma direta de I e J por,*

$$I \oplus J$$

É fato conhecido que um anel unitário é semi-simples a esquerda se e somente se é semi simples a direita. Portanto usaremos o termo **semi-simples**.

Teorema 1.13. *Seja R um anel unitário artiniano a esquerda. São equivalentes:*

1. *R é semiprimitivo;*
2. *R é semiprimo;*
3. *R é semi-simples.*

DEMONSTRAÇÃO: pag 184 teorema 11.7 de [Lam91] ■

Teorema 1.14 (Wedderburn-Artin). *Seja R um anel unitário semisimples . Então $R \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i)$, onde cada D_i é um anel com divisão, r é único, e os pares (D_i, n_i), são únicos a menos de permutação.*

DEMONSTRAÇÃO: pag 35 teorema 3.5 [Lam91] ■

Teorema 1.15 (Cayley-Hamilton). *Seja C um anel comutativo, não necessariamente unitário. Seja A uma matriz pertencente a $M_n(C)$. Se p_A é o polinômio característico de A (isto é $p_A(\lambda) = det(\lambda I - A)$), então $p_A(A) = 0$.*

Demonstração: pag 18 teo 1.3.18 de [Row80]. ■

Para encerrar esta seção um teorema que não é básico, mas nos será muito útil futuramente.

Teorema 1.16 (Gonçalves). *Seja D um anel com divisão não comutativo, que tenha dimensão finita sobre seu centro Z. Então $D^* = D - 0$ contém um grupo livre de posto 2.*

DEMONSTRAÇÃO: ver [JZG84]. ■

1.3 Anéis de grupo

Vamos nesta seção introduzir a noção de **Anel de Grupo,** e estudar algumas de suas propriedades.

Definição 1.17. *Seja A um anel e G um grupo. O* **anel de grupo** *do grupo G sobre o anel A notado por $R = A[G]$, é o conjunto de todas somas finitas formais:*

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

com $g \in G$ e $a_g \in A$, e com a seguinte estrutura de anel. A soma é definida como

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

e o produto

$$\sum_{g \in G} a_g g \cdot \sum_{h \in G} b_h h = \sum_{g,h \in G} (a_g b_h) gh.$$

Também tem a estrutura de A-módulo:

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

Podemos notar que se o anel A é unitário, o anel $A[G]$ também o será, tendo como unidade o elemento $1_A 1_G$.

Vamos centrar nossas atenções para o caso específico em o anel A é um corpo. Usaremos a letra F para denotar tal corpo.

Vamos estudar alguns ideais de $F[G]$.

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

$$\begin{array}{rcl} \pi_H : F[G] & \longrightarrow & F[H] \\ \sum_{g \in G} \alpha_g g & \longrightarrow & \sum_{g \in H} \alpha_g g \end{array}$$

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

Lema 1.18. *Sejam F um corpo, G um grupo, H um subgrupo de G, e Y uma transversal a direita de H em G. Então para todo elemento $\alpha \in F[G]$, existem e são únicos $\alpha_y \in F[H]$ tal que:*

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

Além disso temos $\alpha_y = \pi_H(\alpha y^{-1}) \in K[G]$

DEMONSTRAÇÃO: ver pagina 6, lema 1.3 do capítulo 1 de [Pas77]. ■

Definição 1.19. *Dizemos que um ideal I de $F[H]$, é G-**invariante** , se para todo g pertencente a G temos $g^{-1}Ig \leq I$.*

Lema 1.20. *Seja G um grupo e F um corpo, $H \lhd G$, e seja $\mathcal{I}$ um ideal de $F[G]$. São equivalentes:*

1. *$\mathcal{I} = I \cdot F[G]$, para algum I ideal G-invariante de $F[H]$;*
2. *$\mathcal{I} = (\mathcal{I} \cap F[H]) \cdot F[G]$;*
3. *$\mathcal{I} = \pi_H(\mathcal{I}) \cdot F[G]$.*

Nestas condições temos:

$$I = \mathcal{I} \cap F[H] = \pi_H(\mathcal{I}).$$

DEMONSTRAÇÃO: ver pag 8, lema 1.6 do capítulo 1 de [Pas77]. ■

Vamos introduzir, agora, a noção de **Ideal de Aumento** , que nos será muito útil posteriormente.

Definição 1.21. *Seja $F[G]$ um anel de grupo, e seja a aplicação π:*

$$\begin{array}{ccc} \pi : F[G] & \longrightarrow & F \\ \sum\limits_{g \in G} \alpha_g g & \longrightarrow & \sum\limits_{g \in G} \alpha_g \end{array}$$

π assim definido é homomorfismo de anéis. Tal homomorfismo é denominado a **aplicação de aumento de $F[G]$.** *O* **ideal de aumento de $F[G]$, é** *o kernel desta aplicação, e o notamos por $\Delta(G)$*

Definição 1.22. *Seja $N \lhd G$ e seja π' o homomorfismo:*

$$\begin{aligned} \pi' : F[G] &\longrightarrow F[\frac{G}{N}] \\ \sum_{g\in G} \alpha_g g &\longrightarrow \sum_{g\in G} \alpha_g gN \end{aligned}$$

Notamos por $\Delta(G,N)$, o kernel de π'. O epimorfismo π' será denominado **epimorfismo canônico de $F[G]$ em $F\left[\frac{G}{N}\right]$.**

Nas condições acima, vale a igualdade:

$$F[G](\Delta(N))^n = (\Delta(G,N))^n = (\Delta(N))^n F[G]$$

Para maiores detalhes ver o lema 1.8 do capítulo 1 de [Pas77].

Proposição 1.23. *Sejam G um grupo não trivial e F um corpo. Então $\Delta(G)$ é nilpotente se e somente se car(F)=p > 0 e G for um p-grupo finito. Se a característica de F for 0, então $\Delta(G)$ é não nilpotente.*

DEMONSTRAÇÃO: ver pag 70 teorema 1.6 do capítulo 3 do [Pas77]. ■

Da proposição acima e da observação anterior segue o corolário:

Corolário 1.24. *Sejam G um grupo, N um p-subgrupo finito, normal em G e F um corpo de característica $p > 0$. Então $\Delta(G,N)$ é nilpotente.*

1.4 Identidades polinomiais e identidades de grupo.

Definição 1.25. *Seja $\omega(x_1, \ldots x_n) \neq 1$ um elemento do grupo livre de posto n. Dizemos que $\omega = 1$ é uma* **identidade de grupo para G,** *se para todos $g_1, g_2, \ldots g_n \in G$ temos*

$$\omega(g_1, \ldots, g_n) = 1.$$

Sejam R e S dois anéis unitários, consideraremos como homomorfismos de R em S, apenas os homomorfismos que levem 1_R em 1_S. Com esta consideração vamos enunciar

Proposição 1.26. *Sejam R e S anéis unitários, e seja f um epimorfismo de R em S. Se o kernel de f é nilpotente, e $U(R)$ satisfaz a identidade de grupo $\omega(x_1, \ldots, x_n) = 1$, então $U(S)$ também satisfaz $\omega = 1$.*

DEMONSTRAÇÃO:

Como f é epimorfismo temos que para todo $a \in S$, existe um $a_1 \in R$, tal que $f(a_1) = a$. Inicialmente demonstraremos que se $a = f(a_1) \in U(S)$, então $a_1 \in U(R)$:

Seja $a \in U(S)$, existe $b = f(b_1) \in U(S)$ tal que

$$ab = ba = 1_S$$

Assim,

$$f(a_1b_1) = f(a_1)f(b_1) = ab = 1_S = f(1_R),$$

logo $1_R - a_1b_1$ pertence ao kernel de f.

Seja $j = 1_R - a_1b_1$, como kernel de f é nilpotente, temos que existe n, tal que $j^n = 0$.

Sendo assim temos:

$$(1_R - j)(1_R + j + \cdots + j^{n-1}) = 1_R - j^n = 1_R,$$

e portanto

$$(a_1b_1)(1_R + j + \cdots + j^{n-1}) = 1_R.$$

Concluimos, portanto, que a_1 é inversível a direita.

De forma análoga podemos concluir que a_1 é inversível a esquerda, e que portanto $a_1 \in U(R)$. Vamos agora demonstrar que $U(S)$ satisfaz $\omega = 1_S$:

Sejam $s_1, \ldots, s_n \in U(S)$, e digamos $s_i = f(r_i)$ com $r_i \in U(R)$.

Como $U(R)$ satisfaz $\omega = 1_R$, teremos:

$$\omega(s_1, \ldots s_n) = \omega(f(r_1), \ldots, f(r_n)) = f(\omega(r_1, \ldots, r_n)) = f(1_R) = 1_S.$$

Para todos $s_1, \ldots s_n \in S$. ■

Um caso especial da proposição acima, que utilizaremos a posteriori é:

Proposição 1.27. *Sejam F um corpo de característica $p > 0$, G um grupo, e N um p-subgrupo finito normal em G. Se $U(F[G])$ satisfaz a identidade de grupo $\omega = 1$ então $U(F[\frac{G}{N}])$ também irá satisfazer $\omega = 1$.*

DEMONSTRAÇÃO:

Seja π o epimorfismo canônico de $F[G]$ em $F\left[\frac{G}{N}\right]$.

Pelo corolário 1.24, o kernel de π é nilpotente.

Segue da proposição anterior que $U\left(F\left[\frac{G}{N}\right]\right)$ satisfaz $\omega = 1$. ■

Definição 1.28. *Seja $F\langle x_1, x_2, \ldots\rangle$ a àlgebra livre de posto enumerável sobre o corpo F. Dizemos que uma F-álgebra R* **satisfaz uma identidade polinomial de grau** *s* se existe $p(x_1, x_2, \ldots, x_n) \in F\langle x_1, x_2, \ldots\rangle$, $p \neq 0$ com grau de p igual a s tal que

$$p(r_1, r_2, \ldots, r_n) = 0,$$

para todos $r_1, r_2, \ldots r_n \in R$.

Teorema 1.29 (Kaplansky). *Seja R uma álgebra sobre um corpo F. Se R satisfaz uma identidade polinomial de grau n, então R satisfaz uma identidade polinomial da forma*

$$f(x_1, x_2, \ldots x_n) = \sum_{\sigma \in S_n} a_\sigma x_{\sigma(1)} \cdots x_{\sigma(n)} = 0,$$

com os a_σ pertencentes a F, não todos nulos.

DEMONSTRAÇÃO: ver pag 170, Lema 1.1 do capítulo 5 de [Pas77]. ■

Definição 1.30. *Dizemos que um anel R satisfaz a* **identidade polinomial standard de grau** *n*, se para todos $r_1, \ldots, r_n$ vale:

$$\Gamma_n(r_1, \ldots, r_n) = \sum_{\sigma \in S_n} \mathcal{S}(\sigma) r_{\sigma(1)} \cdots r_{\sigma(n)} = 0,$$

onde $\mathcal{S}(\sigma)$ é a assinatura (ou o sinal) da permutação σ.

Teorema 1.31 (Amitsur-Levitsky). *Seja R um anel unitário comutativo. Então $M_n(R)$ satisfaz a identidade polinomial standard de grau $2n$*

DEMONSTRAÇÃO: ver pag 175, teorema 1.9 do capítulo 5 de [Pas77]. ■

Definição 1.32. *Seja R uma álgebra sobre F. Dizemos que f é um* **polinômio multilinear generalizado** *se f é da forma:*

$$f(\zeta_1, \ldots \zeta_n) = \sum_{\sigma \in S_n} f^\sigma(\zeta_1 \ldots \zeta_n),$$

onde f^σ é um polinômio da forma,

$$f^\sigma(\zeta_1, \ldots \zeta_n) = \sum_{j=1}^{a_\sigma} \alpha_{0,\sigma,j} \zeta_1 \cdots \alpha_{n-1,\sigma,j} \zeta_n \alpha_{n,\sigma,j},$$

onde cada $\alpha_{i,\sigma,j}$ é um elemento de R.

Definição 1.33. *Dizemos que f é um* **polinômio multilinear generalizado não degenerado,** *se para algum σ, $f^\sigma(\zeta_1, \ldots \zeta_n)$, não é identidade polinomial generalizada para a álgebra R, ou seja existem $r_1, \ldots r_n \in R$, tal que $f^\sigma(r_1, \ldots r_n) \neq 0$.*

Capítulo 2

Identidades no caso semiprimo

Neste capítulo estudaremos a estrutura de um anel semiprimo A cujo grupo de unidades $U(A)$ satisfaz uma identidade de grupo. Concluiremos, dentre outros resultados, que se A é uma álgebra semiprima sobre um domínio de integridade e o grupo de unidades de A satisfaz uma identidade de grupo, todos os idempotentes de $R^{-1}A$ são centrais.

Vamos começar com uma proposição típica da teoria combinatória de grupos:

Proposição 2.1. *Seja G um grupo. Se G satisfaz uma identidade de grupo*

$$\omega(x_1, \ldots, x_n) = 1,$$

então G satisfaz uma identidade em duas variaveis $\nu(y_1, y_2) = 1$.

DEMONSTRAÇÃO:

Seja

$$\omega(x_1, \ldots, x_n) = x_{i_1}^{r_1} \cdots x_{i_k}^{r_k}$$

com $i_j \neq i_{j+1}, i_j \in \{1, \ldots, n\}$ Tomemos a identidade de grupo ν:

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

Como $i_j - i_{j+1} \neq 0$ para todo j, temos que ν é não trivial.

Vamos mostrar que G satisfaz $\nu = 1$.

Sejam $g_1, g_2 \in G$ Vamos definir n h_i's 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:

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

E por outro lado:

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

Portanto concluimos que $\nu(g_1, g_2) = 1$ para todos $g_1, g_2 \in G$. Logo G satisfaz $\nu = 1$. ■

O próximo teorema tomará parte central, na demonstração do principal teorema deste capítulo, e na demonstração de um dos lados do teorema do último capítulo. Vamos a ele:

Teorema 2.2 (Giambruno, Jespers e, Valenti). *Seja A uma álgebra unitária sobre um domínio comutativo infinito R, cujo grupo de unidades $U(A)$ satisfaz uma identidade de grupo. Então existe um inteiro positivo k tal que, se $a, b, c \in A$ e $a^2 = bc = 0$ então $bacA$ é um ideal nil a direita de expoente limitado menor ou igual a k.*

DEMONSTRAÇÃO:

Inicialmente vamos provar o caso em que $b = c$:

Para tanto vamos mostrar que se existem $c, d \in A$ tal que $c^2 = d^2 = 0$, então dc é nilpotente, sendo que o grau de nilpotência de dc só depende da natureza da identidade de grupo satisfeita por $U(A)$, e não da escolha de c e d.

Usando a Proposição 2.1, podemos supor que $U(A)$ satisfaz uma identidade de grupo em duas variaveis do tipo:

$$\omega(y_1, y_2) = y_1^{r_1} y_2^{r_2} y_1^{r_3} \cdots y_1^{r_{2k+1}} = 1.$$

Além disso, se a identidade vale para todo $x \in G$, vale também para x^{-1}, e portanto podemos supor $r_1 > 0$.

Sejam $c, d \in A$ tal que $c^2 = d^2 = 0$, e seja $\lambda \in R$. Façamos:

$$x_1 = 1 + \lambda dcd$$

$$x_2 = 1 + \lambda c$$

$$x_3 = 1 + \lambda(1-d)(cdc)(1+d).$$

Vale observar que $x_1, x_2, x_3 \in U(A)$

$$x_1 \cdot (1 - \lambda dcd) = 1 - \lambda^2 dc \underbrace{d^2}_{=0} c = 1$$

$$x_2 \cdot (1 - \lambda c) = 1 - \lambda^2 \underbrace{c^2}_{=0} = 1$$

$$x_3 \cdot (1 - \lambda(1-d)(cdc)(1+d)) = 1 - \lambda^2(1-d)(cdc)\underbrace{(1+d)(1-d)}_{=1}(cdc)(1+d) =$$

$$1 - \lambda^2(1-d)cd\underbrace{c^2}_{=0}dc(1+d) = 1$$

E portanto x_1x_2 e x_1x_3 também são unidades de A. Assim:

$$(x_1x_2)^{r_1}(x_1x_3)^{r_2}\cdots(x_1x_2)^{r_{2k+1}} = 1$$

Podemos notar que $(x_1x_2)^{r_1}(x_1x_3)^{r_2}\cdots(x_1x_2)^{r_{2k+1}}$ pode ser escrito na forma $\prod_{i=1}^{\epsilon} {x_{j_i}}^{\delta_i}$, onde $\epsilon \leq 2(|r_1| + \cdots + |r_{2k+1}|)$, δ_i é 1 ou -1, e $x_{j_i} \neq x_{j_{i+1}}$ ($j_i \in \{1,2,3\}$ para todo i). Além disso $\epsilon \geq 2(|r_1| + \cdots + |r_{2k+1}|) - 4k$, visto que existem no máximo $2k$ encontros de ${x_1}^{-1}$ com x_1 e que em cada encontro temos 2 elementos a menos. Em particular temos $\epsilon \geq 2$.

Vamos analisar agora $\omega(x_1x_2, x_1x_3)$ como função de c e d e λ:

- **Afirmação:**

Para todo $\lambda \in R$, podemos escrever $\omega(x_1x_2, x_1x_3)$ como

$$\prod_{i=1}^{\epsilon} {x_{j_i}}^{\delta_i} = 1 + \sum_{i=1}^{\epsilon} \lambda^i p_i(c,d)$$

onde os p_i's são polinômios na álgebra livre em duas variáveis sobre o anel R, $R\langle x, y\rangle$, que não dependem da escolha de λ, e $p_\epsilon(c,d) = \pm l_\epsilon$, com l_ϵ da forma:

$$l_\epsilon = \begin{cases} (dc)^\alpha d & se \quad j_\epsilon = 1 \\ (dc)^\alpha & se \quad j_\epsilon = 2 \\ (dc)^\alpha(1+d) & se \quad j_\epsilon = 3 \end{cases}$$

Onde α é um inteiro positivo menor ou igual a 2ϵ.

DEMONSTRAÇÃO:

Seja

$$\omega(x_1x_2, x_1x_3) = \prod_{i=1}^{\epsilon} {x_{j_i}}^{\delta_i}$$

Vamos mostrar que a afirmação é verdadeira por indução em ϵ.

Começaremos a indução com $\epsilon = 2$, visto que $\epsilon \geq 2$ independente de ω.

• $\epsilon = 2$:

Como supomos $r_1 > 0$, temos

$$\omega = x_1x_2 = (1 + \lambda dcd)(1 + \lambda c) =$$

$$1 + \lambda dcd + \lambda c + \lambda^2 dcdc = 1 + \lambda(dcd + c) + \lambda^2 (dc)^2$$

Logo $p_\epsilon(c, d) = p_2(c, d) = (dc)^2$, e portanto a afirmação vale se $\epsilon = 2$.

• $\epsilon > 2$: Vamos supor que a afirmação valha para $\epsilon - 1$ e vamos provar que vale para ϵ:

Usaremos α' e p'_i para descrevermos o caso $\epsilon - 1$. Por convenção $p_0(c, d) = 1$. Consideraremos várias possibilidades, utilizando a hipótese que $x_{j-1} \neq x_j$.

(1)$j_{\epsilon-1} = 1, \quad j_\epsilon = 2$

$$\prod_{i=1}^{\epsilon} x_{j_i}^{\delta_i} = \underbrace{(1 + \sum_{i=1}^{\epsilon-2} \lambda^i {p'}_i(c, d) \pm \lambda^{\epsilon-1} \cdot (dc)^{\alpha'} d)}_{\prod_{i=1}^{\epsilon-1} x_{j_i}^{\delta_i}} \underbrace{(1 + \delta_\epsilon \lambda c)}_{x_{j_\epsilon}^{\delta_\epsilon}} =$$

$$1 + \lambda\delta_\epsilon c + \sum_{i=1}^{\epsilon-2} \lambda^i p'_i(c, d) + \sum_{i=1}^{\epsilon-2} \delta_\epsilon \lambda^{i+1} p'_i(c, d)c +$$

$$\pm\lambda^{\epsilon-1}(dc)^{\alpha'} d \pm \delta_\epsilon \lambda^\epsilon (dc)^{\alpha'} dc =$$

$$1 + \sum_{i=1}^{\epsilon-1} \lambda^i \underbrace{(\delta_\epsilon p'_{i-1}(c, d)c + p'_i(c, d))}_{p_i(c,d)} \pm\lambda^\epsilon (dc)^{\alpha'+1}$$

Como $\alpha' \leq 2(\epsilon - 1)$, então $\alpha = \alpha' + 1 \leq 2\epsilon$ e portanto a afirmação é verdadeira.

(2) $j_{\epsilon-1}=1, \quad j_\epsilon=3$

$$\prod_{i=1}^{\epsilon} x_{j_i}^{\delta_i} = \underbrace{(1+\cdots\pm\lambda^{\epsilon-1}\cdot(dc)^{\alpha'}d)}_{\prod_{i=1}^{\epsilon-1} x_{j_i}^{\delta_i}} \underbrace{(1+\delta_\epsilon\lambda(1-d)(cdc)(1+d))}_{x_{j_\epsilon}^{\delta_\epsilon}} =$$

$$1+\cdots\pm\lambda^{\epsilon}(dc)^{\alpha'}d(1-d)(cdc)(1+d) =$$
$$1+\cdots\pm\lambda^{\epsilon}(dc)^{\alpha'+2}(1+d)$$

Como $\alpha'\leq 2(\epsilon-1)$, então $\alpha=\alpha'+2\leq 2\epsilon$ e portanto a afirmação é verdadeira.

(3) $j_{\epsilon-1}=2, \quad j_\epsilon=1$

$$\prod_{i=1}^{\epsilon} x_{j_i}^{\delta_i} = \underbrace{(1+\cdots\pm\lambda^{\epsilon-1}\cdot(dc)^{\alpha'})}_{\prod_{i=1}^{\epsilon-1} x_{j_i}^{\delta_i}} \underbrace{(1+\delta_\epsilon\lambda dcd)}_{x_{j_\epsilon}^{\delta_\epsilon}} =$$

$$1+\cdots\pm\lambda^{\epsilon}(dc)^{\alpha'+1}d$$

Como $\alpha'\leq 2(\epsilon-1)$, então $\alpha=\alpha'+1\leq 2\epsilon$ e portanto a afirmação é verdadeira.

(4) $j_{\epsilon-1}=2, \quad j_\epsilon=3$

$$\prod_{i=1}^{\epsilon} x_{j_\epsilon}^{\delta_\epsilon} = \underbrace{(1+\cdots\pm\lambda^{\epsilon-1}\cdot(dc)^{\alpha'})}_{\prod_{i=1}^{\epsilon} x_{j_i}^{\delta_i}} \underbrace{(1+\delta_\epsilon\lambda(1-d)cdc(1+d))}_{x_{j_\epsilon}^{\delta_\epsilon}} =$$

$$1+\cdots\pm\lambda^{\epsilon}(dc)^{\alpha'+2}(1+d)$$

Como $\alpha'\leq 2(\epsilon-1)$, então $\alpha=\alpha'+2\leq 2\epsilon$ e portanto a afirmação é verdadeira.

(5) $j_{\epsilon-1}=3, \quad j_\epsilon=1$

$$\prod_{i=1}^{\epsilon} x_{j_\epsilon}^{\delta_\epsilon} = (1+\cdots\pm\lambda^{\epsilon-1}\cdot(dc)^{\alpha'}(1+d))(1+\delta_\epsilon\lambda dcd) =$$

$$1+\cdots\pm\lambda^{\epsilon}(dc)^{\alpha'+1}d$$

Como $\alpha'\leq 2\cdot(\epsilon-1)$, então $\alpha=\alpha'+1\leq 2\cdot\epsilon$ e portanto a afirmação é verdadeira.

(6) $j_{\epsilon-1} = 3, \quad j_\epsilon = 2$

$$\prod_{i=1}^{\epsilon} x_{j_\epsilon}^{\delta_\epsilon} = (1 + \cdots \pm \lambda^{\epsilon-1} \cdot (dc)^{\alpha'}(1+d))(1+\delta_\epsilon \lambda c) =$$

$$1 + \cdots \pm \lambda^{\epsilon}(dc)^{\alpha'+1}$$

Como $\alpha' \leq 2(\epsilon - 1)$, então $\alpha = \alpha' + 1 \leq 2\epsilon$ e portanto a afirmação é verdadeira.

Além disso o fato de $p_i'(c,d)$ não depender de λ nos garante que $p_i(c,d)$ também não depende. Logo concluimos nossa demonstração.

Assim, por esta afirmação, e do fato que $\omega(x_1x_2, x_1x_3) = 1$ temos:

$$\sum_{i=1}^{\epsilon} \lambda^i p_i(c,d) = 0.$$

Como o anel R é infinito, se tomarmos $\epsilon + 1$ elementos distintos de R, $\lambda_1, \ldots \lambda_{\epsilon+1}$, teremos

$$\begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^\epsilon \\ 1 & \lambda_2 & \cdots & \lambda_2^\epsilon \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_{\epsilon+1} & \cdots & \lambda_{\epsilon+1}^\epsilon \end{pmatrix} \begin{pmatrix} 0 \\ p_1(c,d) \\ \vdots \\ p_\epsilon(c,d) \end{pmatrix} = 0$$

Como R é domínio de integridade, usando o determinante de Vandermonde teremos :

$$p_i(c,d) = 0,$$

para todo i. Em particular:

$$p_\epsilon(c,d) = 0$$

Assim:

ou

$$(dc)^\alpha = 0,$$

e dc é nilpotente de expoente α

ou

$$(dc)^\alpha d = 0 \Longrightarrow (dc)^{\alpha+1} = 0$$

e dc é nilpotente de expoente $\alpha + 1$,

ou

$$(dc)^\alpha(1+d) = 0 \Longrightarrow (dc)^\alpha(1+d)c = 0 \Longrightarrow (dc)^{\alpha+1} = 0$$

e dc é nilpotente de expoente $\alpha + 1$

Portanto concluimos que dc é nilpotente com expoente menor ou igual a $\alpha + 1$, e além do mais

$$\alpha + 1 \leq 2\epsilon + 1 \leq 4(|r_1| + \cdots + |r_{2k+1}|) + 1$$

Ou seja, o grau de nilpotência não depende da escolha de c e d. Depende somente da natureza de ω.

Vamos notar por l o número $|r_1| + \cdots + |r_{2k+1}|$

Vamos mostrar agora que se $a^2 = b^2 = 0$ então $babA$ é nil de expoente limitado

Seja $x \in A$. Fazendo $d = bxb$ e $c = abxba$, pelo raciocínio anterior teremos

$$(dc)^m = 0 \Longrightarrow (bxbabxba)^m = 0,$$

onde $m = 4l + 1$.(vale notar que $c^2 = d^2 = 0$)

Assim $(babx)^{2m+1} = ba(bxbabxba)^m bx = 0$, e portanto $babA$ é nil de expoente limitado $8l + 3$.

Finalmente vamos mostrar que se $bc = a^2 = 0$, então $bacA$ é nil de grau limitado.

Se $bc = 0$ temos para todo $x \in A$ que $(cxb)^2 = 0$. Assim, como $a^2 = 0$, temos pelo passo anterior que $cxbacxbA$ é nil de grau limitado $n = 8l + 3$. Desse modo

$$(bacx)^{2n+1} = ba(cxbacxba)^n cx = 0$$

Logo concluimos que $bacA$ é nil de expoente limitado, sendo que tal expoente não depende de a, b ou c, mas apenas da natureza da identidade polinomial. (é menor ou igual a $k = 16l + 7$, onde l é a soma dos módulos dos r_i's)

Logo existe k, tal que para todo a, b, c, com $bc = a^2 = 0$, o ideal a direita $bacA$ é nil de expoente limitado menor igual a k. ■

O próximo lema nos dará condições, sobre as quais podemos garantir que todos idempotentes de uma álgebra são centrais.

Lema 2.3. *Seja A uma álgebra sobre um domínio comutativo R. Suponha que para todo $a, b, c \in A$ tais que $a^2 = bc = 0$ tenhamos $bac = 0$. Então todo idempotente de $R^{-1}A$ é central.*

DEMONSTRAÇÃO:

Seja e um idempotente em $R^{-1}A$. Então para algum $r \neq 0, r \in R$, $f = re \in A$

$$(re)^2 = rere = r^2e^2 = r^2e$$

Logo

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

Se $u \in R^{-1}A$ temos:

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

pois

$$(reu(r-re))^2 = (reur - reure)^2 = (r^2eu - r^2eue)^2 =$$
$$r^2eur^2eu - r^2eur^2eue - r^2euer^2eu + r^4eueeue =$$
$$r^4eueu - r^4eueue - r^4eueu + r^4eueue = 0$$

Assim, por hipótese

$$\underbrace{f}_{=b} \cdot \underbrace{(fu(r-f))}_{=a} \cdot \underbrace{(r-f)}_{=c} = 0$$

Portanto temos

$$f(fu(r-f))r - f(fu\underbrace{(r-f))f}_{=f(r-f)=0} = 0$$

e consequentemente

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

Por outro lado

$$f(fu(r-f))r = rf^2u(r-f) = r^3e^2u(r-f) =$$
$$r^3eur - r^3euf = r^4eu - r^4eue.$$

Do fato que r não é divisor de 0 vem que:

$$eu = eue$$

De forma análoga concluimos:

$$eue = ue,$$

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. ■

Pelo lema acima, podemos concluir, que para que uma álgebra tenha todos os seus idempotentes centrais basta que, para todo $a, b, c \in A$, com $a^2 = bc = 0$, tenhamos $bac = 0$. Vamos mostrar com o auxílio do teorema 2.2, e do teorema de Levitski, que se a álgebra A é semiprima e $U(A)$ satisfaz uma identidade de grupo, então temos esta condição satisfeita.

Antes porém vamos enunciar uma proposição que amplia o conjunto dos a's, que fazem $bac = 0$, sempre que $bc = 0$.

Proposição 2.4. *Seja R um anel unitário semiprimo. Suponha que para todos $b,c,x \in R$ tais que $x^2 = bc = 0$ tenhamos $bxc = 0$. Então para todo elemento nilpotente $a \in R$, tal que $bc = 0$, temos $bac = 0$.*

DEMONSTRAÇÃO:

Vamos provar usando indução no índice de nilpotência de a.

Seja $a \in R$ tal que $a^n = 0$, $a^{n-1} \neq 0$.

Se $x^2 = 0$, por hipótese $bxc = 0$.

Hipótese de indução: Se $x \in R$ com $x^m = 0$ e $m < n$, então $b'xc' = 0$ sempre que $b'c' = 0$, e b' e c' estão em R.

Se $a^n = 0$ para algum n, então:

$$(1-a)\cdot(1+a+\cdots a^{n-1}) = (1+a+\cdots a^{n-1})(1-a) = 1-a^n = 1.$$

Logo $1-a$ é inversível.

Sejam $b, c \in R$ tal que $bc = 0$ e seja $r \in R$.

Tomando $b_1 = b(1-a)^{-1}$ e $c_1 = (1-a)c$ temos

$$b_1c_1 = b(1-a)^{-1}(1-a)c = bc = 0$$

Assim, do fato que $(crb)^2 = crbcrb = 0$, teremos, por um lado:

$$b_1crbc_1 = 0.$$

Por outro lado, se $m \geq 2$ e $n \geq 2$ temos $m(n-1) \geq n$ e portanto:

$$(a^m)^{n-1} = a^{m(n-1)} = 0$$

Assim, pela hipótese de indução $ba^mc = 0$ para todo m, maior ou igual a 2.

Donde concluimos que,

$$b_1c = b(1+a+a^2+\cdots a^{n-1})c = bc + bac + \underbrace{ba^2c + \cdots ba^{(n-1)}c}_{=0} = bac$$

e

$$bc_1 = b(1-a)c = bc - bac = -bac$$

e assim:

$$b_1crbc_1 = (bacr(-bac)) = -bacrbac.$$

Portanto:

$$bacrbac = 0,$$

para todo $r \in R$.

Se supormos que $bac \neq 0$, o ideal bilateral $RbacR = \{\sum r_i bacs_i | r_i, s_i \in R\}$, será não nulo, pois $bac \in RbacR$

E além disto será nilpotente:

Sejam $x_1 = \sum_{i=1}^{n} r_i bacs_i$,e $x_2 = \sum_{j=1}^{m} t_j bacw_j$, com $s_i, r_i, t_j, w_j \in R$. Teremos:

$$x_1 x_2 = \sum_{i,j} r_i bac \underbrace{s_i t_j}_{=l_{i,j} \in R} bacw_j =$$

$$\sum_{i,j} r_i \underbrace{bacl_{i,j}bac}_{=0} w_j = 0,$$

Logo $RbacR$ é não nulo, e nilpotente de expoente 2, o que contraria o fato de R ser semiprimo.

Portanto $bac = 0$, para todo elemento nilpotente a pertencente a R, e todo b, e c tal que $bc = 0$. ■

Teorema 2.5 (Levitzky). *Seja R um anel. E seja $\mathcal{H}(R)$, o conjunto:*

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

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

DEMONSTRAÇÃO: ver pag 46, corolário 1.6.26 de [Row80]. ■

Enfim enunciaremos, e demonstraremos, o teorema principal do capítulo.

Teorema 2.6. *Seja A uma álgebra semiprima unitária sobre um domínio comutativo infinito R. Se $U(A)$ satisfaz uma identidade de grupo, então para todos $b, c \in A$ tais que $bc = 0$ e todo elemento nilpotente $a \in A$ tem-se $bac = 0$. Além disso todo idempotente de $R^{-1}A$ é central.*

DEMONSTRAÇÃO:

Sejam $a, b, c \in A$,tal que $a^n = bc = 0$, para algum $n \in \mathbb{N}$. Vamos primeiramente mostrar que:

$$a^2 = bc = 0 \Longrightarrow bac = 0 :$$

Pelo teorema 2.2 temos que $bacA$ é um ideal nil a direita de expoente limitado.

Se $bac \neq 0$,temos $\mathcal{H}(A) \neq (0)$. Pelo teorema de Levitzki, A não seria semiprimo. Assim temos $bac = 0$.

Pela proposição 2.4 temos que para todo elemento nilpotente $a \in A$ $bac = 0$.

Além disso pelo lema 2.3 temos que todos idempotentes de $R^{-1}A$ são centrais, concluindo nossa demonstração. ■

Este resultado será fundamental na demonstração do principal teorema do próximo capítulo, no caso em que $F[G]$ for um anel semiprimo. Indiretamente também terá importância na demonstração do caso em que $N(F[G])$, (que será definido posteriormente), é nilpotente.

Capítulo 3

Caso Geral.

3.1 Introdução

Nosso objetivo neste capítulo será demonstrar o seguinte teorema:

Teorema 3.1 (Giambruno, Sehgal, Valenti). *Sejam F um corpo infinito e G um grupo de torção. Se $U(F[G])$ satisfaz uma identidade de grupo então $F[G]$ satisfaz uma identidade polinomial.*

Vamos antes fixar algumas notações.

Usaremos a letra p para designar a característica do corpo F. Usaremos (u, v) para denotar o comutador multiplicativo $u^{-1}v^{-1}uv$, e $[x, y]$ para denotar o comutador aditivo $xy - yx$.

Como no capítulo 1, se N é um subgrupo normal de G, denotaremos por $\Delta(G, N)$, o kernel da projeção canônica π,

$$\pi : F[G] \longrightarrow F\left[\frac{G}{N}\right],$$

e por $\Delta(G, G)$, o ideal de aumento que corresponde ao kernel da projeção canônica π',

$$\pi' : F[G] \longrightarrow F.$$

Vamos definir também

$$P = \{g \in G | o(g) = p^k \text{ para algum } k \in \mathbb{N}\}.$$

$$Q = \{g \in G \mid p \nmid o(g)\}.$$

Os elementos de P e Q serão chamados de p-elementos, e p'-elementos respectivamente.

Proposição 3.2. *Seja p um inteiro primo, G um grupo de torção e P e Q como acima. Então $G = PQ$*

DEMONSTRAÇÃO:

Seja $g \in G$, e seja m a ordem de g. Claramente m pode ser escrito na forma $m = p^k a$ com $(a, p) = 1$.

Usando o teorema de Bezout temos que existem r e s inteiros tais que

$$1 = rp^k + sa$$

Assim

$$g = g^{rp^k + sa} = g^{sa} g^{rp^k}$$

Se observarmos que

$$(g^{sa})^{p^k} = g^{s \cdot a p^k} = g^{sm} = 1$$

e que

$$(g^{rp^k})^a = g^{r \cdot a p^k} = g^{rm} = 1$$

Temos que $o(g^{sa})$ divide p^k, e portanto $g^{sa} \in P$. Também concluimos que p não divide a ordem de g^{rp^k} pois senão dividiria $o(a)$. Logo $g^{rp^k} \in Q$.

Portanto concluimos que $G = PQ$ ■

Vamos introduzir a noção de grupo **p-abeliano.**

Definição 3.3. *Seja G um grupo. Dizemos G é* **p-abeliano** *se o seu comutador é um p-grupo finito.*

Proposição 3.4. *Sejam G e P como no teorema anterior. Se G' é um p-grupo, então P é subgrupo de G.*

DEMONSTRAÇÃO:

Claramente $1 \in P$, (basta tomar $k = 0$), e se $o(g) = p^k$, temos $o(g^{-1}) = p^k$. Logo basta mostrar que se $o(g_1) = p^{k_1}$, e $o(g_2) = p^{k_2}$ então existe k_3 tal que $o(g_1 g_2) = p^{k_3}$.

Vamos notar por $\bar{g}$, o elemento $g \cdot G' \in G/G'$, e seja $k = k_1 + k_2$.

Como G/G' é abeliano teremos:

$$\overline{(g_1 g_2)^{p^k}} = (\overline{g_1 g_2})^{p^k} = (\bar{g_1}\bar{g_2})^{p^{k_1+k_2}} = \bar{g_1}^{p^{k_1+k_2}} \bar{g_2}^{p^{k_1+k_2}} = \bar{1}$$

Logo $(g_1g_2)^{p^{k_1+k_2}} \in G'$.

Como G' é p-grupo, para todo $a \in G'$, existe k_4 tal que $a^{p^{k_4}} = 1$.

Logo se tomarmos $k_3 = k_1 + k_2 + k_4$, teremos $(g_1g_2)^{p^{k_3}} = 1$. ■

Vamos agora introduzir alguns conceitos referentes a álgebras livres.

Seja F um corpo de característica p. Notaremos por $F\langle x_1, x_2, \ldots, x_n\rangle$ a F-álgebra livre em n variáveis, por $\mathcal{A} = F\langle x_1, x_2, \ldots, x_n\rangle [[t]]$, o anel das séries de potências na variável comutativa t sobre o álgebra livre $F\langle x_1, x_2, \ldots, x_n\rangle$.

Proposição 3.5. *Sejam F um corpo de característica $p > 0$, e $\mathcal{A} = F\langle x_1, x_2 \ldots x_n\rangle [[t]]$. Então:*

1. $(1 + x_it)^{p^{\alpha_i}} = 1 + (x_it)^{p^{\alpha_i}}$;
2. $(1 + (x_it)^{\beta})$ *é inversível para todo β em $\mathbb{N}$, com inverso,*

$$1 + \sum_{k=1}^{\infty} (-1)^k {x_i}^{\beta k} t^{\beta k};$$

3. $(1 + (x_it)^{\beta})^n = 1 + n(x_it)^{\beta} + (x_it)^{2\beta} q_n((x_it)^{\beta})$, *onde q_n é um polinômio (se $n \geq 0$), ou uma série de potências (se $n < 0$) com coeficientes em F.*

DEMONSTRAÇÃO:

(1)-Usando o teorema do binômio , mais o fato que se p é primo p divide $\binom{p^{\alpha_i}}{k}$, para $1 \leq k \leq p^{\alpha_i} - 1$, concluimos que:

$$(1 + x_it)^{p^{\alpha_i}} = 1 + (x_it)^{p^{\alpha_i}}.$$

(2)

$$(1 + (x_it)^{\beta})(1 + \sum_{k=1}^{\infty} (-1)^k {x_i}^{\beta k} t^{\beta k}) =$$

$$1 + \sum_{k=1}^{\infty} ({x_i}^{\beta k} - {x_i}^{\beta k}) t^{\beta k} = 1.$$

Analogamente:

$$(1 + \sum_{k=1}^{\infty} (-1)^k {x_i}^{\beta k} t^{\beta k})(1 + (x_it)^{\beta}) = 1$$

(3)

Se $n \geq 0$, a conclusão segue pelo teorema do binômio.

Vamos ao caso $n < 0$:

Seja $m = -n$.

Provaremos por indução em m.

Se $m = 1$ a afirmação segue do item 2 isto é

$$q_{-1}((x_i t)^\beta) = \sum_{k=0}^{\infty} (-1)^k \cdot (x_i t)^{\beta k}$$

Pela hipótese de indução temos

$$(1 + (x_i t)^\beta)^{-(m-1)} = (1 - (m-1)(x_i t)^\beta + (x_i t)^{2\beta} q_{n+1}((x_i t)^\beta),$$

onde $q_{n+1}((x_i t)^\beta)$ é uma série de potências. Assim temos:

$$(1 + (x_i t)^\beta)^{-m} = [1-(x_i t)^\beta+(x_i t)^{2\beta} q_{-1}((x_i t)^\beta)][1-(m-1)(x_i t)^\beta+(x_i t)^{2\beta} q_{n+1}((x_i t)^\beta)] =$$
$$1 - (x_i t)^\beta - (m-1)(x_i t)^\beta + (x_i t)^{2\beta} q_n((x_i t)^\beta) =$$
$$1 - m(x_i t)^\beta + (x_i t)^{2\beta} q_n((x_i t)^\beta)$$

onde

$$q_n((x_i t)^\beta) = m - 1 + [1 - (x_i t)^\beta] q_{n+1}((x_i t)^\beta) + q_{-1}((x_i t)^\beta) \cdot (1 + (x_i t))^{n+1}$$

E assim concluimos a demonstração. ■

Definição 3.6. *Seja $h(x_1, \ldots, x_n, t) = \alpha {x_{i_1}}^{r_1} \cdots {x_{i_k}}^{r_k} t^\beta$ um monômio não constante do anel das séries de potências de t sobre a álgebra livre , $F\langle x_1, \ldots x_n\rangle [[t]]$, ($\alpha \in F$), tal que $i_j \neq i_{j+1}$, para todo $j \leq k-1$. Nesta situação diremos que k é o* **comprimento silábico** *de h. (Se h for do tipo αt^r, diremos que h tem comprimento silábico igual a 0)*

Vale notar que sempre podemos escrever um monômio h não constante de $F\langle x_1, \ldots x_n\rangle$ na forma acima de maneira única, garantindo assim que **comprimento silábico** está bem definido.

Vamos demonstrar agora uma proposição, devida a Wilhelm Magnus. (ver [MKS76].)

Proposição 3.7 (Magnus). *Seja F um corpo de característica $p > 0$, e $\mathcal{A} = F\langle x_1, \ldots x_n\rangle [[t]]$. Os elementos $1 + x_1 t, \ldots, 1 + x_n t$, geram um grupo livre no grupo das unidades de $\mathcal{A}$.*

DEMONSTRAÇÃO:

Vimos no item 2 da proposição 3.5, que $1+x_1t, \ldots, 1+x_nt$ são elementos inversíveis de $\mathcal{A}$. Basta mostrar que qualquer produto ω da forma,

$$\omega = (1 + x_{i_1}t)^{r_1} \cdots (1 + x_{i_k}t)^{r_k},$$

com $i_j \neq i_{j+1}$, para $j \leq k-1$, e $r_j \neq 0$, para todo j, é diferente de 1.

Vamos escrever $r_j = \alpha_j \cdot \beta_j$, onde α_j é uma potência de p, e $(p, \beta_j) = 1$.

Pelo item 1 da proposição 3.5, temos:

$$\omega = (1 + (x_{i_1}t)^{\alpha_1})^{\beta_1} \cdots (1 + (x_{i_1}t)^{\alpha_k})^{\beta_k}.$$

E pela parte 3 da mesma proposição temos,

$$\omega = (1 + \beta_1(x_{i_1}t)^{\alpha_1} + Q_1) \cdots (1 + \beta_k(x_{i_1}t)^{\alpha_k} + Q_k)$$

onde os Q_j's são somas de monômios onde t tem grau maior ou igual a $2\alpha_j$.

Segue daí que o único monômio resultante do produto que tem comprimento silábico k, e cujo grau de t é igual a $s = \sum_{i=1}^{k} \alpha_k$ será

$$\beta_1 \cdots \beta_k {x_{i_1}}^{\alpha_1} \cdots {x_{i_k}}^{\alpha_k} t^s$$

Como $(\beta_j, p) = 1$, para todo j, temos,

$$\omega = 1 + \cdots + \beta_1 \cdots \beta_k {x_{i_1}}^{\alpha_1} \cdots {x_{i_k}}^{\alpha_k} t^s + \cdots \neq 1.$$

E portanto concluimos, que $1 + x_1t, \ldots, 1 + x_nt$ geram um grupo livre de posto n no grupo de unidades de $\mathcal{A}$. ■

Lema 3.8 (Giambruno,Sehgal,Valenti). *Seja G um grupo finito e F um corpo infinito tal que $U(F[G])$ satisfaz uma identidade de grupo. Se a característica de F é $p > 0$ então G é p-abeliano. Se F é um corpo de característica 0 G será abeliano.*

DEMONSTRAÇÃO:

O fato de G ser finito implica que $F[G]$ é artiniano a esquerda, pois todo ideal a esquerda de $F[G]$, pode ser visto como um espaço vetorial de dimensão finita sobre F. Portanto, se um ideal está contido propriamente em outro, então sua dimensão

será menor que a daquele que o contém. Como $F[G]$ tem dimensão finita sobre F, em algum momento a cadeia para de decrescer.

Seja $\mathcal{J}$ o radical de Jacobson de $F[G]$. Então, $\mathcal{J}$ é nilpotente e temos o epimorfismo canônico:

$$\pi : F[G] \longrightarrow \frac{F[G]}{\mathcal{J}}$$

Como o radical de Jacobson é nilpotente, segue pela proposição 1.26 que $U\left(\frac{F[G]}{\mathcal{J}}\right)$ satisfaz a uma identidade de grupo.

Do fato de $F[G]$ ser artiniano a esquerda temos que $\frac{F[G]}{\mathcal{J}}$ também será.

Como $\frac{F[G]}{\mathcal{J}}$ é semiprimitivo e artiniano a esquerda pelo teorema 1.13, será semisimples.

Usando o teorema de Artin-Wedderburn (ver teorema 1.14):

$$\frac{F[G]}{\mathcal{J}} = \bigoplus_{i \in I} M_{n_i}(D_i)$$

Como $\frac{F[G]}{\mathcal{J}}$ é semiprimitivo, pela proposição 1.13, será semiprimo e usando o teorema 2.6 temos que todo idempotente de $\frac{F[G]}{\mathcal{J}}$ é central. E portanto concluimos que $n_i = 1$ para todo i. Assim,

$$\frac{F[G]}{\mathcal{J}} = \bigoplus_{i \in I} D_i.$$

onde cada D_i é um anel com divisão, com F contido em seu centro.

Além disso, do fato de G ser finito temos que $[D_i : F] < \infty$.

Pelo lema 1.16 cada D_i deve ser comutativo. Caso contrário irá conter um grupo livre de posto 2, e portanto seu grupo de unidades não irá satisfazer nenhuma identidade de grupo.

Assim $\frac{F[G]}{\mathcal{J}}$ é soma direta de corpos, logo é comutativo. Logo, para todo x, y pertencentes a $U(F[G])$

$$\pi(x, y) = (\pi(x), \pi(y)) = 1 = \pi(1),$$

e portanto,

$$(x, y) = 1 \ (\mathrm{mod}\mathcal{J}),$$

Assim concluimos que $G' \subseteq 1 + \mathcal{J}$, logo

$$\Delta(G') \subseteq \mathcal{J}.$$

Assim, $\Delta(G')$ será nilpotente.

Se $p > 0$, pela proposição 1.23 temos que G' é um p-grupo finito. Se $p = 0$, temos pela mesma proposição que $G' = (1)$, e portanto G é abeliano. ■

Podemos remover a hipótese de G ser finito, e enunciar uma espécie de recíproca:

Lema 3.9 (Giambruno, Sehgal, Valenti). *Seja G um grupo, e seja F um corpo de característica $p > 0$. Se G é p-abeliano então U satisfaz uma identidade de grupo, e $F[G]$ satisfaz a identidade polinomial $[x, y]^{p^m} = 0$ para algum $m \in \mathbb{N}$.*

DEMONSTRAÇÃO:

Seja π,

$$\pi : F[G] \longrightarrow F\left[\frac{G}{G'}\right]$$

o epimorfismo canônico. Sejam u e v elementos de $U(F[G])$.

Como $\frac{G}{G'}$ é abeliano, temos:

$$\pi(uvu^{-1}v^{-1}) = (\pi(u), \pi(v)) = 1$$

e portanto concluimos que $1 - (u, v)$ pertence ao kernel de π.

Pelo corolário 1.24 temos que o kernel de π é nilpotente. Assim existe k, tal que

$$(1 - (u, v))^{p^k} = 0.$$

Por outro lado,

$$(1 - (u, v))^{p^k} = 1 - (u, v)^{p^k},$$

Donde concluimos que $(u, v)^{p^k} = 1$, e portanto $U(F[G])$ satisfaz a identidade de grupo

$$\omega(x, y) = (x, y)^{p^k} = 1$$

Além disso se $x, y \in F[G]$:

$$[x, y] = \sum c[g, h],$$

onde $c \in F$ e $g, h \in G$

$$= \sum cgh - chg = \sum cgh(1 - h^{-1}g^{-1}hg) = \sum \underbrace{cgh}_{\in F[G]} \underbrace{(1 - (g, h))}_{\in \Delta(G')}$$

Logo $[x,y] \in F[G] \cdot (\Delta(G'))$. Da proposição 1.23, e do fato que G' é p grupo segue que existe k, tal que $[x,y]^{p^k} = 0$

Assim demonstramos que $F[G]$ satisfaz uma identidade polinomial. ■

3.2 O grupo $\Phi(G)$

Nesta seção estudaremos o subgrupo de conjugação finita de G, que iremos notar o grupo $\Phi(G)$. Ele irá ocupar um lugar importante na demonstração do principal teorema deste capítulo.

Definição 3.10. *Seja G um grupo e g, um elemento de G. A* **classe de conjugação de g em G,** *que notamos por* $\mathbf{cl}_G(g)$ *é o conjunto*

$$cl_G(g) = \{h^{-1}gh | h \in G\}.$$

Um elemento g de G é dito de conjugação finita em G se $|cl_G(g)| < \infty$. Representaremos por $\Phi(G)$ o conjunto dos elementos de conjugação finita em G.

Teorema 3.11. *$\Phi(G)$ é subgrupo normal de G*

DEMONSTRAÇÃO:

Inicialmente vamos demonstrar que $\Phi(G)$ é subgrupo de G:

Certamente $1 \in \Phi(G)$ e $|\mathrm{cl}(g)| = |\mathrm{cl}(g^{-1})|$. Vamos mostrar que se $g, h \in \Phi(G)$ então $gh \in \Phi(G)$. De fato

$$\mathrm{cl}(gh) = \{k^{-1}ghk | k \in G\} = \{k^{-1}gkk^{-1}hk | k \in G\},$$

e

$$|\mathrm{cl}(gh)| \leq |\mathrm{cl}(g)| \cdot |\mathrm{cl}(h)| < \infty.$$

Portanto $gh \in \Phi(G)$, e $\Phi(G)$ é subgrupo de G.

A normalidade de $\Phi(G)$, segue do fato que $\mathrm{cl}(h^{-1}gh) = \mathrm{cl}(g)$, para todo $g \in \Phi(G)$, e todo $h \in G$. ■

Se $G = \Phi(G)$, ou equivalentemente, todo elemento de G tem conjugação finita, dizemos que G é um grupo de **conjugação finita.**

Seja G um grupo, g um elemento de G e seja $C_G(g) = \{h \in G | hg = gh\}$, o centralizador de g em G. Então:

$$|\mathrm{cl}_G(g)| = [G : C_G(g)]$$

Este resultado nos diz que $g \in \Phi(G)$ se e somente se $[G : C_G(g)] < \infty$. Usaremos esta equivalência para demonstrar o seguinte resultado:

Proposição 3.12. *Seja G um grupo de torção. Então $\Phi(G)$ é localmente finito.*

DEMONSTRAÇÃO:

Seja G_0 um subgrupo de Φ com um número finito de geradores, $G_0 = \langle h_1, \ldots h_n \rangle$. Comò G_0 é um grupo de conjugação finita, temos,

$$[G_0 : C_{G_0}(h_i)] < \infty,$$

para todo h_i e portanto,

$$[G_0 : \bigcap C_{G_0}(h_i)] < \infty.$$

Mas $\bigcap C_{G_0}(h_i) = Z(G_0)$, logo

$$[G_0 : Z(G_0)] < \infty.$$

Da desigualdade acima, e da proposição 1.6, podemos concluir que $Z(G_0)$ é finitamente gerado.

Ora, $Z(G_0)$ é finitamente gerado, abeliano e de torção, logo $Z(G_0)$ é finito. Portanto G_0 é finito. Logo $\Phi(G)$ será localmente finito. ■

Quando não houver o risco de interpretações dúbias, notaremos por Φ o conjunto $\Phi(G)$.

Notaremos por $\Phi_p(G)$, o subgrupo de G, gerado pela intersecção dos conjuntos $\Phi(G)$, e $P = \{g \in G | o(g) = p^k$ para algum $k \in \mathbb{N}\}$, isto é,

$$\Phi_p = \langle P \cap \Phi \rangle .$$

Proposição 3.13. *Seja G um grupo de torção. Se $\Phi_p(G)$ é finito então $\Phi(\frac{G}{\Phi_p(G)})$, não contém p-elementos.*

DEMONSTRAÇÃO:

Vamos notar por N o grupo $\Phi_p(G)$.

Seja $\bar{h} = hN \in \Phi(\frac{G}{\Phi_p(G)})$, vamos mostrar que p não divide $o(hN)$.

Vamos primeiramente mostrar que $h \in \Phi(G)$ sempre que $hN \in \Phi(\frac{G}{\Phi_p(G)})$: De fato, se $hN \in \Phi(\frac{G}{\Phi_p(G)})$ então o conjunto

$$\mathrm{cl}(hN) = \{g^{-1}hgN | gN \in \frac{G}{N}\}$$

é finito. Como N é um conjunto finito, o conjunto união de $\mathrm{cl}(hN)$, que notaremos por S

$$S = \{x | x \in g^{-1}hgN, g \in G\},$$

também será finito. Logo se $q \in G$ é tal que existe g com $q = g^{-1}hg$, claramente $q \in S$, e assim

$$cl(h) = \{g^{-1}hg | g \in G\}$$

é finito. Assim temos que $h \in \Phi(G)$.

Vamos mostrar agora que p não divide $o(hN)$:

Seja $o(h) = p^k m$, onde k é um número natural e $(m, p) = 1$.

Pela proposição 3.2 existem h_1 e h_2, tais que

$$h = h_1 h_2 = h_2 h_1$$

e

$$h_1{}^m = h_2{}^{p^k} = 1$$

em particular temos que $h_2 \in N$,e assim:

$$(hN)^m = (h_1 N h_2 N)^m = (h_1 N)^m \underbrace{(h_2 N)^m}_{h_2 \in N} = h_1{}^m N = N$$

Logo $o(hN)$ divide m, e portanto p não irá dividir a ordem de hN.

Logo $\Phi(\frac{G}{\Phi_p(G)})$ não tem p-elementos. ■

Lema 3.14 (Passman). *Suponha que F é um corpo de característica $p > 0$. Então $F[G]$ é semiprimo se e somente se $\Phi(G)$ é um p'-grupo.*

DEMONSTRAÇÃO: ver pag 131, teorema 2.13 do capítulo 4 de [Pas77]. ■

Vamos notar por $N = N(F[G])$ a soma de todos ideais nilpotentes de $F[G]$. Claramente N será um ideal nil de $F[G]$.

Lema 3.15 (Passman). *Seja F um corpo de característica $p > 0$. Então $N(F[G])$ é nilpotente se e somente se Φ_p é finito.*

DEMONSTRAÇÃO: ver pag 311, teorema 1.12 do capítulo 8 de [Pas77]. ■

3.3 Relações entre o grupo G e as identidades polinomiais satisfeitas por $F[G]$

Nesta seção analisaremos algumas relações entre o grupo G e o fato de $F[G]$ satisfazer uma identidade polinomial. (Ou uma identidade polinomial generalizada.). Enunciaremos alguns teoremas, que por terem demonstrações trabalhosas não serão demonstrados. Indicaremos ao leitor, porém, onde encontrar tais demonstrações.

Lema 3.16 (Isaacs-Passman). *1. Sejam G um grupo, e F um corpo de característica 0. São equivalentes:*

(i) *$F[G]$ satisfaz uma identidade polinomial;*

(ii) *G contém um subgrupo A abeliano de índice finito;*

(iii) *G contém um subgrupo normal N, abeliano de índice finito.*

2. Sejam G um grupo e F um corpo de característica $p > 0$. São equivalentes:

(i) *$F[G]$ satisfaz uma identidade polinomial;*

(ii) *G contém um subgrupo A p-abeliano de índice finito;*

(iii) *G contém um subgrupo normal N, p- abeliano de índice finito.*

DEMONSTRAÇÃO: ver pp 196 e 197, corolários 3.8 e 3.9 do capítulo 5 de [Pas77]. ■

Teorema 3.17 (Passman). *Seja G um grupo,e F um corpo de característica 0. Então $F[G]$ é semiprimo.*

DEMONSTRAÇÃO: ver teorema 2.12 do capítulo 4 de [Pas77]. ■

Vamos enunciar dois resultados que relacionam mais estreitamente identidades polinomiais e o grupo $\Phi(G)$.

Proposição 3.18 (Passman). *Se $F[G]$ satisfaz uma identidade polinomial de grau n, então $[G : \Phi(G)] \leq n/2$, e $|(\Phi(G))'| < \infty$.*

DEMONSTRAÇÃO: ver pag 189, do teorema 2.14, do capítulo 5 de [Pas77]

Teorema 3.19. *Seja $F[G]$ um anel de grupo. São equivalentes:*

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

2. *$F[G]$ possui um idempotente e diferente de 0, tal que $eF[G]e$ satisfaz uma identidade polinomial;*

3. *$F[G]$ satisfaz uma identidade polinomial generalizada não degenerada.*

DEMONSTRAÇÃO: ver [Pas71]. ■

3.4 Demonstração do Teorema Principal

Dedicaremos esta seção a demonstração do teorema enunciado no começo do capítulo:

Teorema (Giambruno, Sehgal, Valenti). *Sejam F um corpo infinito e G um grupo de torção. Se $U(F[G])$ satisfaz uma identidade de grupo então $F[G]$ satisfaz uma identidade polinomial.*

DEMONSTRAÇÃO: Dividiremos a demonstração em 3 casos:

- **1-$F[G]$ é semiprimo:(isto é, $N = 0$)**

  Seja $p = 0$

  Seja $y \in G$, com $o(y) = m$. Tomando $e = \dfrac{\hat{y}}{m} = \dfrac{1 + y + \cdots + y^{m-1}}{m}$, e será idempotente. Pelo lema 2.3, e é central.Logo

$$g\hat{y} = \hat{y}g, \quad \forall g \in G$$

e portanto

$$g\hat{y}g^{-1} = \hat{y} \Longrightarrow$$
$$1 + gyg^{-1} + \cdots + gy^{m-1}g^{-1} = 1 + y + \cdots + y^{m-1}$$

Daqui concluimos que existe um j tal que $gyg^{-1} = y^j$ e portanto $\langle y \rangle \lhd G$ para todo $y \in G$.

Como todo subgrupo cíclico de G é normal podemos concluir pelo teorema de Dedekind-Baer que ou G é abeliano ou é hamiltoniano. Se G for Hamiltoniano $Q_8 \leq G$, e portanto $U(F[Q_8])$ satisfará uma identidade de grupo. Pelo lema 3.8 Q_8 será abeliano, absurdo.

Logo concluimos que G é abeliano e portanto $F[G]$ satisfaz a identidade polinomial

$$g(x, y) = xy - yx = 0.$$

Seja $p > 0$:

Sejam P e Q os conjuntos:

$$Q = \{g \in G | p \not| o(g)\}$$

e

$$P = \{g \in G | o(g) = p^k \text{ para algum } k\}.$$

Usando raciocínio análogo ao caso anterior concluimos que para todo y pertencente a Q, $\langle y \rangle \lhd G$. Vamos mostrar agora que $P = (1)$, e portanto $G = Q$.

Vamos inicialmente demonstrar que para todo $h \in P$, $\langle h \rangle \lhd P$.

Seja $g \in P$, com $o(g) = p^k$. Temos $(1-g)^{p^k} = 1 - g^{p^k} = 0$. Além disso

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

Usando a proposição 2.4 temos:

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

$$(\hat{h} - \hat{h}g)(1-h) = \underbrace{\hat{h}(1-h)}_{=0} - \hat{h}g + \hat{h}gh = 0$$

Donde concluimos

$$g + hg + \cdots + h^{n-1}g = gh + \cdots + h^{n-1}gh,$$

e portanto existirá um k tal que,

$$h^k = ghg^{-1}.$$

Afirmamos que para todo q em Q, e todo h em P, temos $qhq^{-1} = h$.

Como $\langle q \rangle \lhd G$ o subgrupo $H = \langle q, h \rangle$ é finito pois $\langle q \rangle$ e $\langle h \rangle$ são finitos, e para todo r existe s tal que $hq^r = q^s h$ e Portanto $| \langle q, h \rangle | \leq o(q) \cdot o(h)$.

Do fato de $U(F[G])$ satisfazer uma identidade de grupo, concluimos que $U(F[H])$ também satisfaz, Pelo lema 3.8, H é p-abeliano.

Assim

$$(q, h) = q^{-1} \underbrace{h^{-1}qh}_{\in \langle q \rangle} = q^{-1}q^r$$

para algum r e daqui segue que $(q, h) \in \langle q \rangle$.

Desse modo conseguimos um elemento em $\langle q \rangle$ de ordem p^s, para algum s. Logo este elemento é a identidade do grupo.

Portanto $(q, h) = 1$ e $qhq^{-1} = h$, para todo $h \in P$, e para todo $q \in Q$.

Da proposição 3.2 temos que $G = PQ$, e portanto temos $\langle h \rangle \lhd G$.

Desse modo podemos concluir que $|cl(h)| < o(h) < \infty$. Logo $h \in \Phi(G)$ e como $F[G]$ é semiprimo, por 3.14, Φ é um p'-grupo. Logo $P = (1)$, e portanto $G = Q$.

Pelo teorema de Dedekind-Baer, $G = Q$ será abeliano ou hamiltoniano.

Se $p = 2$ Q não pode ter elementos de ordem 2. Logo $Q \neq Q_8 \times A \times E$ (Q_8 é 2-grupo). Assim Q é abeliano.

Como $U(F[G])$ satisfaz uma identidade de grupo, $U(F[Q_8])$ também a satisfaz.

Por outro lado, se $p \neq 2$, pelo lema 3.8 Q_8 deverá ser um grupo p-abeliano, ou seja seu derivado deve ser p-grupo. Mas $Q_8' = \{1, -1\}$ é um 2-grupo. Logo $Q_8 \not\leq Q$, donde concluimos que Q é abeliano.

Como G é abeliano $F[G]$ satisfaz a identidade polinomial

$$g(x, y) = xy - yx,$$

E assim concluimos o caso semi-primo.

Pelo teorema 3.17, podemos supor $p > 0$, daqui em diante.

• **2-N é nilpotente e diferente de 0:**

Afirmamos que $\Phi_p(G) = \langle P \cap \Phi \rangle$ é normal em G.

De fato, se $h \in \Phi_p$, $h = h_1 \cdot h_2 \cdots h_k$, com $h_1, \ldots, h_k \in P \cap \Phi$.

Portanto

$$g^{-1}hg = g^{-1}h_1g \cdot g^{-1}h_2g \cdots g^{-1}h_kg$$

Mas $o(g^{-1}h_ig) = o(h_i)$ e $cl(g^{-1}h_ig) = cl(h_i)$. Assim, para cada i, temos $g^{-1}h_ig \in P \cap \Phi$, e portanto $g^{-1}hg \in \Phi_p(G)$, o que prova a afirmação.

Agora, como N é nilpotente, pelo lema 3.15 $\Phi_p(G)$ é grupo finito. Além disso, segue do lema 3.8, que $(\Phi_p(G))'$, é p-grupo e portanto da proposição 3.4, $\Phi_p(G)$ é p-grupo. Pela proposição 1.27, temos que $U(F[\frac{G}{\Phi_p(G)}])$ satisfaz uma identidade de grupo

Por outro lado, pela proposição 3.13, temos que $\Phi(G/\Phi_p(G))$ não tem p-elementos, e portanto pelo lema 3.14 $F[\frac{G}{\Phi_p(g)}]$ é semiprimo.

Assim, pelo caso anterior temos que $F[\frac{G}{\Phi_p(G)}]$ é comutativo, e portanto $G/\Phi_p(G)$ é abeliano. Logo como $G' \subset \Phi_p(G)$, G' é um p-grupo finito.

Pelo lema 3.9 $F[G]$ satisfaz uma identidade polinomial da forma $[x,y]^{p^m} = 0$.

• **3-N é nil mas não é nilpotente:** Pela proposição 2.1 podemos supor que $U(F[G])$ satisfaz a identidade $\omega(x_1, x_2) = 1$ em duas variáveis.

Seja $\mathcal{A} = F\langle x_1, x_2\rangle [[t]]$ e seja $\mathcal{F}$ o grupo livre de posto 2.

Pela proposição 3.7 sabemos que $1+x_1t$ e $1+x_2t$, geram um grupo livre em $U(\mathcal{A})$. Temos assim:

$$1 \neq \omega(1+x_1, 1+x_2) = 1 + \sum_{i=1}^{\infty} t^i p_i(x_1, x_2)$$

onde os p_i's são polinômios homogêneos de grau i em $F\langle x_1, x_2\rangle$. Assim podemos concluir que

$$\sum_{i=1}^{\infty} t^i p_i(x_1, x_2) \neq 0$$

Logo existe p_{i_0} tal que $p_{i_0}(x_1, x_2) \neq 0$, e portanto p_{i_0} é não trivial.

Afirmamos que $N(F[G])$ satisfaz $p_{i_0} = 0$.

Sejam $r_1, r_2 \in N(F[G])$. Sabemos que os elementos $1 + r_i\lambda$ são inversíveis em $F[G]$ para todo $\lambda \in F$ com inverso

$$1 - r_i\lambda + {r_i}^2\lambda^2 - \cdots + (-1)^{d_i-1}{r_i}^{d_i-1}\lambda^{d_i-1},$$

onde d_i é o menor inteiro tal que ${r_i}^{d_i} = 0$.

Logo $(1 + r_1\lambda), (1 + r_2\lambda)$ satisfazem a identidade $\omega = 1$ Assim

$$\omega(1 + \lambda r_1, 1 + \lambda r_2) = 1,$$

isto é,

$$\sum_{i=1}^{\infty} \lambda^i p_i(r_1, r_2) = 0$$

Vale notar que se $\omega(x_1, x_2)$ é da forma ${x_1}^{s_1} \cdots {x_{i_k}}^{s_k}$, então o polinômio homogêneo de grau maior que k tem em todos seus monômios um ${x_1}^2$ ou um ${x_2}^2$, (ou seja em alguns monômios ${x_1}^2$, e em outros ${x_2}^2$). Da mesma forma o polinômio homogêneo de grau

maior que kd_3 onde d_3 é o máximo entre d_1 e d_2 tem em todos os monômios ou um $x_1^{d_3+1}$ ou um $x_2^{d_3+1}$. Usando o fato que ${r_1}^{d_3} = {r_2}^{d_3} = 0$ e tomando $d = kd_3$ temos:

$$\sum_{i=1}^{\infty} \lambda^i p_i(r_1, r_2) = \sum_{i=1}^{d} \lambda^i p_i(r_1, r_2)$$

Em outras palavras se o nosso $i_0 > d$ então $p_{i_0}(r_1, r_2) = 0$. Vamos mostrar agora que $p_{i_0}(r_1, r_2) = 0$ se $i_0 \leq d$:

Como F é infinito tomemos $d+1$ elementos distintos em F, $\lambda_1, \ldots \lambda_{d+1}$ e observemos que vale a igualdade:

$$\begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^d \\ 1 & \lambda_2 & \cdots & \lambda_2^d \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_{d+1} & \cdots & \lambda_{d+1}^d \end{pmatrix} \begin{pmatrix} 0 \\ p_1(r_1, r_2) \\ \vdots \\ p_d(r_1, r_2) \end{pmatrix} = 0$$

Pelo determinante de Vandermonde a matriz

$$\begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^d \\ 1 & \lambda_2 & \cdots & \lambda_2^d \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_{d+1} & \cdots & \lambda_{d+1}^d \end{pmatrix}$$

é inversível e portanto:

$$p_i(r_1, r_2) = 0,$$

para todo $i \leq d$.

Logo, para todos $r_1, r_2 \in N(F[G])$, $p_{i_0}(r_1, r_2) = 0$. Assim concluimos que $N(F[G])$ satisfaz uma identidade polinomial.

Usando o teorema 1.29 temos que $N(F[G])$ satisfaz uma identidade multilinear

$$\sum_{\sigma \in S_{i_0}} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(i_0)} = 0$$

Com $\alpha_\sigma \in F$, para todo σ e pelo menos um $\alpha_{\sigma'}$ diferente de 0.

Como $N(F[G])$ é ideal temos que $F[G]$ satisfaz a identidade polinomial multilinear generalizada:

$$\sum_{\sigma \in S_{i_0}} \alpha_\sigma a_1 x_{\sigma(1)} \cdots a_{i_0} x_{\sigma(i_0)}$$

Com,

$$a_1 a_2 \cdots a_{i_0} \neq 0,$$

(tais a_i's existem devido ao fato de $N(F[G])$ ser não nilpotente.) Segue daí que se tomarmos $x_1 = x_2 = \cdots x_{i_0} = 1$,

$$\alpha_{\sigma'} a_1 x_{\sigma'(1)} \cdots a_{i_0} x_{\sigma'(i_0)} = \alpha_{\sigma'} a_1 \cdots a_{i_0} \neq 0$$

Logo, temos que $F[G]$ satisfaz uma identidade polinomial não degenerada.

Usando o lema 3.19 temos que $[G : \Phi] < \infty$ e $|\Phi'| < \infty$. Vamos mostrar agora que Φ' é p-grupo.

Pela proposição 3.12 Φ é localmente finito.

Logo pelo teorema 1.5, podemos concluir que G é localmente finito. Afirmamos que Φ' é p-grupo:

Seja $\alpha \in \Phi'$. O elemento α será da forma $(h_1, h_2) \cdots (h_{2n-1}, h_{2n})$, com $h_i \in \Phi$. Seja $H = \langle h_1, \ldots h_{2n} \rangle$. Como Φ é localmente finito H será um subgrupo finito de Φ. Sabemos que $U(F[H])$ satisfaz uma identidade de grupo. Assim pelo lema 3.8 H' é p-grupo finito, e como $\alpha \in H'$ temos que $o(\alpha)$ é uma potência de p. Portanto podemos concluir que Φ' é p-grupo.

Agora pelo lema 3.16 concluimos que $F[G]$ satisfaz uma identidade polinomial.

Isto termina a demonstração do teorema. ■

Deste teorema segue

Corolário 3.20. *Sejam F um corpo infinito, e G um grupo de torção tal que $U(F[G])$ satisfaz uma identidade de grupo. Então G é localmente finito.*

DEMONSTRAÇÃO:

Pela proposição 3.12 temos que $\Phi(G)$ é localmente finito.

Pelo Teorema que acabamos de demonstrar temos que $F[G]$ satisfaz uma identidade polinomial. Usando o lema 3.18 temos que $[G : \Phi(G)] < \infty$.

Assim pelo teorema 1.5, teremos que G é localmente finito. ■

Com o corolário acima poderemos remover a hipótese de G ser finito e supor apenas G de torção no lema 3.8. Enunciamos:

Lema 3.21. *Sejam G um grupo de torção e F um corpo infinito de característica $p > 0$. Se $U(F[G])$ satisfaz uma identidade de grupo, então G' é p-grupo. Se F é um corpo de característica 0, então G será um grupo abeliano.*

DEMONSTRAÇÃO: Caso $p > 0$

Queremos mostrar que todo elemento de G' é um p-elemento de G.

Seja $h \in G'$, $h = (h_1, h_2) \cdots (h_{2n-1}, h_{2n})$ e seja H o subgrupo, gerado pelos h_i's:

$$H = \langle h_1, \ldots h_{2n} \rangle$$

Usando a proposição acima G será localmente finito, e portanto H será finito. Pelo lema 3.8, temos que H' é p-grupo.

Como $h \in H'$ temos que h é um p-elemento, e portanto G' será p-grupo.

Caso $p = 0$

Queremos mostrar que para todos x e y em G, $xy = yx$. Tomando $H = \langle x, y \rangle$, temos que H é finito, e portanto pelo lema 3.8, H será abeliano. Logo temos $xy = yx$. ■

Existem álgebras de grupo onde o corpo F é infinito, o grupo G é de torção, $F[G]$ satisfaz uma identidade polinomial mas $U(F[G])$ não satisfaz nenhuma identidade de grupo. *Ou seja não vale a recíproca do nosso teorema.*

Por exemplo:

Seja $F = \mathbb{Q}$, o corpo dos números racionais. $G = S_3$. O anel de grupo $\mathbb{Q}[S_3]$ é semiprimo visto que $\mathbb{Q}$ tem característica 0. Como vimos se $U(\mathbb{Q}[S_3])$ satisfazesse uma identidade de grupo $\mathbb{Q}[S_3]$ seria comutativo. Logo $U(\mathbb{Q}[S_3])$ não satisfaz nenhuma identidade de grupo.

Por outro lado, tomando a representação regular de $\mathbb{Q}[S_3]$, vemos que existe um isomorfismo entre $\mathbb{Q}[S_3]$ e um subgrupo H de $M_6(\mathbb{Q})$. Pelo Teorema de Amitsur-Levitzky, (ver teorema1.31), temos que H, e conseqüentemente $\mathbb{Q}[S_3]$, satisfazem a identidade polinomial standard de grau 12.

O próximo resultado, nos dá uma recíproca, no caso em que G é grupo nilpotente, e $F[G]$ satisfaz uma identidade polonomial muito particular, relacionada com a definição abaixo:

Definição 3.22. *Dizemos que um anel é Lie-n-Engel se para todo x,y no anel vale a identidade* $[x, \underbrace{y, \ldots, y}_{n \text{ vezes}}] = 0$.

Antes de enunciar, e demonstrar, o teorema, vamos enunciar um teorema devido a Sehgal:

Teorema 3.23. *Seja F um corpo de característica $p \geq 0$. Então, nestas condições $F[G]$ é Lie n-Engel, se e somente se:*

1. *G é nilpotente e contém um subgrupo normal p-abeliano A, com G/A, p-grupo finito se $p > 0$;*

2. *G é abeliano se $p = 0$.*

DEMONSTRAÇÃO: ver pag 155, teorema 6.1 do capítulo 5 de [Seh78]. ■

Teorema 3.24. *Seja F um corpo infinito de característica $p \geq 0$ e seja G um grupo nilpotente de torção. São equivalentes:*

1. *$U(F[G])$ satisfaz uma identidade de grupo;*

2. *$F[G]$ é Lie-n-Engel;*

3. *$U(F[G])$ satisfaz a identidade de grupo $(u^{p^m}, v) = 1$.*

DEMONSTRAÇÃO:

$(1 \Longrightarrow 2)$:

Como $U[F(G)]$ satisfaz uma identidade de grupo, com as hipóteses acima e com o teorema 3.1 podemos concluir que $F[G]$ satisfaz uma identidade polinomial.

Se F tem característica 0, pelo lema 3.21, teremos que $F[G]$ é comutativo e portanto será Lie n-Engel.

No caso $p > 0$ mostraremos que $\Phi = \Phi(G)$ é um subgrupo normal p-abeliano, e que $\frac{G}{\Phi(G)}$ é um p-grupo finito. E assim pelo teorema 3.23, poderemos concluir que G é Lie n-Engel.

Como $U(F[\Phi])$ satisfaz uma identidade de grupo, temos por 3.21 que Φ' é p-grupo. Da proposição 3.18 segue que Φ' é finito. Portanto Φ é p-abeliano.

De 3.18 também concluimos que $[G : \Phi] < \infty$, basta mostrar que $\frac{G}{\Phi}$ é p-grupo.

Sejam P o conjunto dos p-elementos, e Q o conjunto dos p'-elementos. Como G é nilpotente P e Q são subgrupos de G e $G = P \times Q$. Do lema 3.21 temos que G' é p-grupo e portanto $G' \leq P$. Donde concluimos que Q é central e portanto é subgrupo (normal) de Φ. Assim temos

$$\frac{G}{\Phi} \cong \frac{G/Q}{\Phi/Q} \cong \frac{P}{\Phi/Q}.$$

Logo $\frac{G}{\Phi}$ é p-grupo.

Assim pelo teorema 3.23, concluimos que $F[G]$ é Lie-n-Engel.

$(2 \Longrightarrow 3)$: O caso $p = 0$ segue diretamente de 3.23, portanto vamos supor $p > 0$.

Se $F[G]$ é Lie-n-Engel, então $[x, \underbrace{y, \ldots, y}_{n}] = 0$

Fazendo $[x, y, \ldots, y] = \sum_{i=0}^{n} \binom{n}{i}(-1)^i y^i x y^{n-i}$ e tomando m tal que $p^m > n$ teremos:

$$[x, \underbrace{y, \ldots, y}_{p^m}] = 0$$

e portanto

$$\sum_{i=0}^{p^m} \binom{p^m}{i}(-1)^i y^i x y^{p^m - i} = 0.$$

Como p divide $\binom{p^m}{i}$ para $1 \leq i \leq p^m - 1$, temos

$$xy^{p^m} - y^{p^m} x = 0.$$

Em particular para $u, v \in U(F[G])$ temos

$$vu^{p^m} - u^{p^m} v = 0 \Longrightarrow$$

$$vu^{p^m} = u^{p^m} v \Longrightarrow u^{-p^m} v^{-1} u^{p^m} v = 1$$

e portanto para todos $u, v \in U(F[G])$ vale $(u^{p^m}, v) = 1$.

Como $(3 \Longrightarrow 1)$ é trivial temos a tese. ■

Para encerrar o capítulo, vale citar o fato que, recentemente C.H.Liu, demonstrou o teorema 3.1, sem a hipótese de F ser infinito. Tal demonstração será parte integrante de sua tese de doutorado.

Capítulo 4

O caso modular-uma condição necessária e suficiente

4.1 Introdução:

No capítulo 2 vimos algumas propriedades do anel de grupo $F[G]$ quando $U(F[G])$ satisfaz uma identidade de grupo, e obtivemos resultados importantes no caso em que o anel é semi primo. No capítulo 3 vimos que se G é grupo de torção, F é um corpo infinito, e $U(F[G])$ satisfaz uma identidade de grupo, então $F[G]$ satisfaz uma identidade polinomial.

Neste capítulo vamos caracterizar os grupos de torção para os quais $U(F[G])$ satisfaz a uma identidade de grupo. Vamos provar:

Teorema 4.1 (Passman, [Pas97]). *Seja $U = U(F[G])$ o grupo de unidades da álgebra de grupo de um grupo de torção G sobre o corpo infinito F de característica $p > 0$. São equivalentes:*

i) *U satisfaz uma identidade de grupo.*

ii) *G tem um subgrupo normal p-abeliano de indice finito e G' é um p-grupo de período limitado.*

iii) *U satisfaz $(x, y)^{p^k} = 1$ para algum $k > 0$.*

Claramente (iii) $\Rightarrow$(i) é trivial.

Dedicaremos as próximas seções para demonstrar (i)$\Rightarrow$ (ii) e (ii)$\Rightarrow$(iii).

4.2 A implicação (i)⇒(ii)

Nesta seção, demonstraremos basicamente que se F é um corpo infinito de característica $p > 0$ e G é um grupo de torção que satisfaz uma identidade de grupo, então G' tem expoente limitado. As outras afirmações da tese seguem como corolário do fato que $F[G]$ satisfaz uma identidade polinomial.

Inicialmente vamos estender a proposição 1.27, com algumas restrições sobre o corpo F. Para isto, usaremos que com as hipóteses assumidas, o grupo G é localmente finito.

Lema 4.2. *Sejam F um corpo infinito com característica $p > 0$ e G um grupo de torção. Suponha que $U(F[G])$ satisfaça a identidade de grupo $\omega = 1$. Se H é qualquer subgrupo de G ou se $\frac{G}{N}$ é qualquer imagem homomórfica de G, então $U(F[H])$ e $U\left(F\left[\frac{G}{N}\right]\right)$ também satisfazem $\omega = 1$.*

DEMONSTRAÇÃO:

O resultado para $H \leq G$, é trivial visto que $U(F[H]) \subseteq U(F[G])$.

Para demonstrar a afirmação para $\frac{G}{N}$ consideraremos vários casos:

N é um p-grupo finito:

Feito na proposição 1.27.

N é um p'-grupo finito:

Seja $\hat{N} = \sum_{g \in N} g$, $n = |N|$. Tomando $e = \frac{\hat{N}}{n}$ temos que e é idempotente central, pois como N é normal,

$$g^{-1}\frac{\hat{N}}{n}g =$$

$$g^{-1}\frac{(g^{-1} + \cdots + g_n)}{n}g =$$

$$\frac{g^{-1}g_1g + g^{-1}g_2g + \cdots + g^{-1}g_ng}{n} = \frac{\hat{N}}{n},$$

para todo g em G.

Portanto

$$F[G] = e \cdot F[G] \oplus (1 - e) \cdot F[G].$$

Logo $U(eF[G])$ satisfaz $\omega = 1$. Além disso, como e é central temos,

$$\begin{aligned} \varphi : eF[G] &\longrightarrow F\left[\frac{G}{N}\right] \\ e \cdot \sum_{g \in G} \alpha_g g &\longrightarrow \sum_{g \in G} \alpha_g gN \end{aligned}$$

está bem definida e é isomorfismo.

Logo $U\Big(F\Big[\frac{G}{N}\Big]\Big)$ satisfaz $\omega = 1$.

N é finito:

Pelo lema 3.21, G' é p-grupo.

Se $N < G$, então $N' < G'$. Isto implica que se P é um p subgrupo de Sylow de N, então $N' < P$,e portanto $P \lhd N$. Como P é p subgrupo de Sylow normal de N e N é finito, pelo segundo teorema de Sylow, P é característico em N e portanto $P \lhd G$. Assim podemos escrever:

$$\frac{G}{N} \cong \frac{G/P}{N/P}.$$

Usando o primeiro caso concluimos que $U\Big(F\Big[\frac{G}{P}\Big]\Big)$ satisfaz uma identidade de grupo. (P é p–grupo) Como P é p-Sylow, temos que $\dfrac{N}{P}$ é p'–subgrupo de $\dfrac{G}{P}$.

Pelo caso 2, $U\Big(F\Big[\frac{G}{N}\Big]\Big) = U\Big(F\Big[\frac{G/P}{N/P}\Big]\Big)$ satisfaz $\omega = 1$.

N é um grupo qualquer:

Sejam $\bar{u_1}, \ldots, \bar{u_n} \in F\Big[\dfrac{G}{N}\Big]$. Queremos mostrar que:

$$\omega(\bar{u_1}, \ldots, \bar{u_n}) = 1,$$

para todos $\bar{u_1}, \ldots, \bar{u_n}$ pertencentes a $F[G/N]$.

Tomemos $u_1, \ldots, u_n$ e $v_1, \ldots, v_n$ tais que $\pi(u_i) = \bar{u_i}$, e $\pi(v_i) = \bar{u_i}^{-1}$, onde π é o epimorfismo canônico.

Denotaremos por $\text{supp}(u_i)$ o suporte de cada u_i em $F[G]$.

Seja $L = \langle \text{supp}(u_i), \text{supp}(v_i) | 1 \leq i \leq n \rangle$.

Como G é localmente finito, L é finito. Seja $M = L \cap N$. Podemos afirmar, com um pequeno abuso de linguagem, que os $\bar{u_i}$'s, e $\bar{u_i}^{-1}$'s, pertencem a $U(F[\frac{L}{M}])$. Como M é finito, segue do caso anterior que,

$$\omega(\bar{u_1}, \ldots, \bar{u_n}) = 1,$$

Para todos $\bar{u_1}, \ldots, \bar{u_n}$ em $U(F[\frac{G}{N}])$. E assim concluimos nossa demonstração. ■

Lema 4.3. *Seja G um grupo e seja A um subgrupo abeliano normal de G. Suponha que $\frac{G}{A}$ é cíclico de ordem finita q. Se $G = \langle A, t\rangle$, então $G' = (A, t) = \{(a, t) | a \in A\}$. Além disso $G \cap C_G(t)$ tem período dividindo q*

DEMONSTRAÇÃO:

Primeiramente vamos demonstrar que (A, t) *é subgrupo de* G.

(A, t) é fechado para inversos, isto é

$$(a^{-1}t^{-1}at)^{-1} \in (A, t).$$

Como A é abeliano e $A \lhd G$, temos

$$(a^{-1}t^{-1}at)^{-1} = t^{-1}a^{-1}ta = at^{-1}a^{-1}t = (a^{-1}, t) \in (A, t).$$

(A, t) é fechado para o produto, isto é

$$(a_1{}^{-1}t^{-1}a_1t)(a_2{}^{-1}t^{-1}a_2t) \in (A, t).$$

$$a_1{}^{-1}\underbrace{t^{-1}a_1t}_{\in A}a_2{}^{-1}t^{-1}a_2t = a_1{}^{-1}a_2{}^{-1}t^{-1}a_1tt^{-1}a_2t = (a_1a_2, t) \in (A, t)$$

Portanto (A, t) é grupo. Além disso, como $A \lhd G$ e A é abeliano, segue que $(A, t) \leq A$.

Vamos agora mostrar que $(A, t) \lhd G$.

Como A é abeliano e (A, t) é subgrupo de A segue que $(A, t) \lhd A$. Assim do fato que $G = \langle A, t\rangle$, basta mostrar que t normaliza (A, t), isto é

$$t^{-1}(A, t)t \leq (A, t).$$

$$t^{-1} \cdot a_1{}^{-1}t^{-1}a_1t \cdot t = t^{-1}a_1{}^{-1}tt^{-1}t^{-1}a_1t^2 =$$

$$\underbrace{t^{-1}a_1{}^{-1}t}_{a'^{-1}}t^{-1}\underbrace{t^{-1}a_1t}_{a'}t = a'^{-1}t^{-1}a't \in (A, t).$$

Assim concluimos que t normaliza (A,t), e portanto, $(A,t) \lhd G$.

Desta forma, podemos escrever:

$$\frac{G}{A} = \frac{G/(A,t)}{A/(A,t)}$$

Claramente temos que $(A,t) \leq G'$. Para conseguir $G' \leq (A,t)$ mostraremos que $\frac{G}{(A,t)}$ é abeliano. Usaremos para isso o fato que se o quociente de um grupo por um subgrupo central é cíclico, então este grupo é abeliano.

Basta provar então que $A/(A,t)$ é subgrupo central de $G/(A,t)$, ou equivalentemente, mostrar que para todo $g \in G$ e para todo $a \in A$ temos $g^{-1}a^{-1}ga \in (A,t)$.

Como $A \lhd G$ temos que $A \cdot \langle t \rangle$ será subgrupo de G. Como A e t estão em $A \cdot \langle t \rangle$, temos

$$G = A \cdot \langle t \rangle$$

Afirmamos que dado um $g = at^n \in G$ e um $b \in A$ temos:

$$g^{-1}b^{-1}gb \in (A,t).$$

Como A é abeliano, e normal em G, segue que:

$$g^{-1}b^{-1}gb = t^{-n} \underbrace{a^{-1}b^{-1}a}_{=b^{-1}} t^n b = bt^{-n}b^{-1}t^n$$

Logo basta provar que para todo $n \in \mathbb{Z}$ e para todo $a \in A$ temos

$$a^{-1}t^{-n}at^n \in (A,t) :$$

$n = 0$, Trivial.

$n > 0$. Usaremos indução em n.

Para $n = 1$ não há o que fazer. Vamos supor que valha para $n-1$, ou seja:

$a^{-1}t^{-(n-1)}at^{n-1} \in (A,t)$, para todo $a \in A$

Assim temos:

$$a^{-1}t^{-n}at^n = a^{-1}t^{-1} \underbrace{att^{-1}a^{-1}}_{=1} t^{-(n-1)}at^{n-1}t =$$

$$(a^{-1}t^{-1}at)\cdot t^{-1}\cdot(a^{-1}t^{-(n-1)}at^{n-1})\cdot t$$

Como $(A,t)\lhd G$ segue da hipótese de indução que $t^{-1}a^{-1}t^{-(n-1)}at^{n-1}t$ pertence a (A,t), e assim $a^{-1}t^{-n}at^n\in(A,t)$. Logo concluimos o caso em que $n>0$. Vamos agora considerar o caso $n<0$.

Para facilitar vamos fazer $m=-n>0$, e provar

$$a^{-1}t^mat^{-m}\in(A,t).$$

Temos

$$a^{-1}t^mat^{-m}=t^mat^{-m}a^{-1}=$$
$$t^mat^{-m}t^{-m}t^ma^{-1}t^{-m}t^m=(t^mat^{-m})t^{-m}(t^ma^{-1}t^{-m})t^m=$$
$$a'^{-1}t^{-m}a't^m,$$

onde $a'=t^ma^{-1}t^{-m}\in A$ devido ao fato de $A\lhd G$.

Assim concluimos que $A/(A,t)$ é subgrupo central de $G/(A,t)$, e por consequência que $(A,t)=G'$.

Mostraremos agora que o período de $(G'\cap C_G(t))$ divide q.

Seja $b\in G'\cap C_G(t)$. Usando o resultado anterior b será da forma $a^{-1}t^{-1}at$ para algum $a\in A$. Além disso $bt=tb$ o que implica $t(a^{-1}t^{-1}at)=a^{-1}t^{-1}at^2$.

Vamos provar que $b^n=a^{-1}t^{-n}at^n$ para todo n, positivo.

A afirmação é verdadeira para $n=1$.

Suponha $b^{n-1}=a^{-1}t^{-(n-1)}at^{n-1}$. Certamente t comuta com b^{n-1} e portanto

$$b^n=a^{-1}t^{-1}ata^{-1}t^{-(n-1)}at^{n-1}=a^{-1}t^{-1}t^{-(n-1)}at^{n-1}t=$$
$$a^{-1}t^{-n}at^n.$$

Assim, do fato que G/A é cíclico de período q, temos que $t^q\in A$. Logo, como A é abeliano.

$$b^q=a^{-1}t^{-q}at^q=a^{-1}at^{-q}t^q=1.$$

Portanto o período de $(G'\cap C_G(t))$ divide q. ■

Vamos agora construir uma função que exercerá um papel fundamental na demonstração dos próximos lemas desta seção.

Suponha G um grupo, A um subgrupo normal abeliano de G e t um elemento de G com ordem prima q, de tal forma que

$$G=A\rtimes\langle t\rangle.$$

Definição 4.4. *A função* **traço** é a aplicação de $F[A]$ em $F[A]$, dada por

$$Tr(\sigma) = \sigma + t^{-1}\sigma t + \cdots t^{-(q-1)}\sigma t^{q-1},$$

para todo σ pertencente a $F[A]$.

Como A é subgrupo normal de G temos que a imagem da função traço está contida em $F[A]$. Além disso, podemos verificar facilmente que:

$$Tr(\sigma_1 + \sigma_2) = Tr(\sigma_1) + Tr(\sigma_2),$$

$$Tr(\lambda\sigma) = \lambda Tr(\sigma),$$

para todo λ pertencente a F, e $\sigma, \sigma_1, \sigma_2$ pertencentes a $F[A]$.

Vamos agora enumerar outras propriedades desta função:

Proposição 4.5. *Para todo σ pertencente a $F[A]$ temos $Tr(\sigma) \in Z(F[G])$*

Demonstração:

Basta demonstrar que $Tr(\sigma)$ comuta com os elementos de G.

Para todo $g \in G$, temos:

$$g^{-1}Tr(\sigma)g = g^{-1}\sigma g + \cdots + g^{-1}t^{-(q-1)}\sigma t^{(q-1)}g =$$

$$= t^{-l}a_1^{-1}\sigma a_1 t^l + \cdots + t^{-l}a_1^{-1}(t^{-(q-1)}\sigma t^{q-1})a_1 t^l,$$

pois como $G = A \rtimes \langle t \rangle$, para todo $g \in G$ existem $a_1 \in A$ e $l \in \mathbb{N}$, $0 \leq l \leq (q-1)$, tais que $g = a_1 \cdot t^l$.

Mas como A é abeliano e $t^n \mapsto t^n \cdot t^l$ é uma bijeção de $\langle t \rangle$ em $\langle t \rangle$, segue que:

$$g^{-1}Tr(\sigma)g =$$
$$t^{-l}\sigma t^l + \cdots + t^{-l}t^{-(q-1)}\sigma t^{q-1}t^l = Tr(\sigma).$$

E portanto $g \cdot Tr(\sigma) = Tr(\sigma) \cdot g$, logo $Tr(\sigma) \in Z(F[G])$. ■

Seja G um grupo e x e y elementos de G. Vamos notar por x^y o elemento $y^{-1}xy$.

Proposição 4.6. *Para todo σ pertencente a $F[A]$ temos*

$$Tr(\sigma)^p = Tr(\sigma^p).$$

DEMONSTRAÇÃO:

Como A é abeliano e normal em G $t^{-j}\sigma t^j$ comuta com $t^{-i}\sigma t^i$ para todo i e j. Assim:

$$Tr(\sigma)^p = (\sigma + \sigma^t + \ldots + \sigma^{t^{q-1}})^p =$$
$$\sigma^p + (\sigma^t)^p + \cdots (\sigma^{t^{q-1}})^p.$$

Como

$$(\sigma^{t^i})^p = (t^{-i}\sigma t^i)^p = t^{-1}\sigma^p t^i = (\sigma^p)^{t^i},$$

segue que $Tr(\sigma)^p = Tr(\sigma^p)$. ■

Proposição 4.7. *Para todo $\zeta \in F[A] \cap Z(F[G])$, e para todo $\sigma \in F[A]$ temos:*

$$Tr(\sigma\zeta) = \zeta Tr(\sigma)$$

Em particular, se tomarmos $\sigma = 1$ teremos

$$Tr(\zeta) = Tr(1)\zeta = q\zeta.$$

Ainda, $Tr(Tr(\sigma)) = q \cdot Tr(\sigma)$, para todo σ em $F[A]$.

DEMONSTRAÇÃO:

Se $\zeta \in F[A] \cap Z(F[G])$, então,

$$Tr(\sigma\zeta) = \sigma\zeta + t^{-1}\sigma t\zeta + \ldots + t^{-(q-1)}\sigma t^{q-1}\zeta = Tr(\sigma)\zeta$$

Em particular se $\sigma = 1$ temos, $Tr(\zeta) = Tr(\zeta \cdot 1) = \zeta Tr(1) = q\zeta$. ■

Notaremos por τ a soma:

$$\tau = 1 + t + \ldots + t^{q-1},$$

Vale observar que para todo i teremos $t^i\tau = \tau$ e portanto teremos $\tau^2 = q\tau$.

Proposição 4.8. *Seja τ definido como acima. Então $\tau\sigma\tau = Tr(\sigma)\tau$, para todo $\sigma \in F[A]$.*

DEMONSTRAÇÃO:

$$\tau\sigma\tau = \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} t^{-i}\sigma t^j = \sum_{i=0}^{q-1}(\sum_{j=0}^{q-1}(t^{-i}\sigma t^i)t^{j-i}) = \sum_{i=0}^{q-1} t^{-i}\sigma t^i \sum_{j=0}^{q-1} t^{j-i} =$$

Para cada i temos $\sum_{j=0}^{q-1} t^{j-i} = \tau$, logo

$$\tau\sigma\tau = \left(\sum_{i=0}^{q-1} t^{-i}\sigma t^{i}\right)\tau = Tr(\sigma)\tau \blacksquare$$

No próximo lema iremos demonstrar que G' tem período finito para uma classe muito restrita de grupos.

Lema 4.9. *Sejam F, um corpo infinito de característica $p > 0$ e $G = \langle A, t\rangle$, onde A é um subgrupo abeliano normal de G e t tem ordem q, q um número primo. Então se $U(F[G])$ satisfaz uma identidade de grupo G' tem período finito.*

DEMONSTRAÇÃO:

Dividiremos a demonstração em 2 casos:

Caso 1: $q \neq p$:

Seja $a \in A$, definiremos α e β, tais que $\alpha^2 = \beta^2 = 0$.

$$\alpha = \tau a^{-1}(1 - t^{-1}).$$

Temos

$$\alpha^2 = \tau a^{-1}(1 - t^{-1})\tau a^{-1}(1 - t^{-1}) = 0,$$

pois $(1 - t^{-1})\tau = 0$.

E seja β

$$\beta = (qa - Tr(a))\tau.$$

Como $Tr(a) \in F[A] \cap Z(F[G])$, pela proposição 4.7 segue que

$$Tr(qa - Tr(a)) = Tr(qa) - Tr(Tr(a)) = qTr(a) - qTr(a) = 0.$$

Assim teremos

$$\beta^2 = (qa - Tr(a))\underbrace{\tau(qa - Tr(a))\tau}_{Tr(q\cdot a - Tr(a))\tau = 0} = 0.$$

Como $U(F[G])$ satisfaz uma identidade de grupo, segue pelo teorema 2.2 que existe um n tal que se $x^2 = yz = 0$ então $yxz \cdot F[G]$ é ideal nil de expoente limitado n (n dependendo somente da identidade de grupo em questão.).

Tomando $x = \beta$ e $y = z = \alpha$ teremos que $(\alpha\beta\alpha\beta)^n = 0$ para tal n. Portanto tomando um k tal que $p^k \geq 2n$, teremos por um lado:

$$(\alpha\beta)^{p^k} = 0. \qquad (*)$$

Por outro lado temos:

$$\alpha\beta = \tau a^{-1}(1 - t^{-1})(qa - Tr(a))\tau =$$
$$= \tau a^{-1}(1 - t^{-1})qa\tau - \tau a^{-1}(1 - t^{-1})Tr(a)\tau = {}^{1}$$
$$= \tau a^{-1}(1 - t^{-1})qa\tau = q\tau(1 - a^{-1}t^{-1}a)\tau =$$
$$= q\tau(1 - a^{-1}a^t t^{-1})\tau = q\tau(\tau - a^{-1}a^t \underbrace{t^{-1}\tau}_{=\tau}) =$$
$$= q\tau(1 - a^{-1}a^t)\tau = q\tau^2 - q\tau(a^{-1}a^t)\tau =$$
$$= q^2\tau - qTr(a^{-1}a^t)\tau = q(q - Tr(a^{-1}a^t))\tau.$$

Seja $b = (a^{-1}a^t) = a^{-1}t^{-1}at \in A$. Então

$$\alpha\beta = q(q - Tr(b))\tau$$

e como $q(q - Tr(b))$ é central

$$(\alpha\beta)^{p^k} = q^{p^k}(q - Tr(b))^{p^k}\tau^{p^k} = q^{p^k}(q^{p^k} - Tr(b)^{p^k})\tau^{p^k}.$$

Mas $q^{p^k} = q$ e $q^{p^k - 1} = 1$ e portanto

$$(\alpha\beta)^{p^k} = q(q - Tr(b)^{p^k})\tau^{p^k}.$$

Levando em conta que $\tau^2 = q\tau$, podemos concluir que $\tau^n = q^{n-1}\tau$, sempre que $n \geq 2$, logo $\tau^{p^k} = q^{p^k - 1}\tau = \tau$, e assim

$$(\alpha\beta)^{p^k} = q(q - Tr(b)^{p^k})\tau$$

Por $(*)$ temos:

$$q(q - Tr(b)^{p^k})\tau = 0$$

o que implica

$$(q - Tr(b)^{p^k})\tau = 0.$$

[1] o segundo termo da soma se anula, pois $Tr(a)$ é central e $(1 - t^{-1}) \cdot \tau = 0$.

Afirmamos que $q - Tr(b)^{p^k} \in F[A]$, é igual a 0. De fato fazendo

$$(q - Tr(b)^{p^k}) = \alpha_1 a_1 + \cdots + \alpha_n a_n,$$

com $a_1, \ldots a_n \in A$ temos

$$(\alpha_1 a_1 + \cdots + \alpha_n a_n) \cdot (1 + t + \cdots + t^{q-1}) =$$

$$\alpha_1 a_1 + \cdots \alpha_n a_n + \alpha_1 a_1 t + \cdots + \alpha_1 a_1 t^{q-1} + \cdots \alpha_n a_n \ t^{q-1} = 0,$$

com $a_1, \ldots, a_n \in A$, e $\alpha_1, \ldots, \alpha_n \in F$.

Como $A \cap \langle t \rangle = (1)$, se $0 \leq \beta_1, \beta_2 \leq q-1$, a igualdade $a_{i_1} t^{\beta_1} = a_{i_2} t^{\beta_2}$ é equivalente a $a_{i_1} = a_{i_2}$ e $\beta_1 = \beta_2$.

Daqui concluimos que $\alpha_1 = \alpha_2 = \cdots \alpha_n = 0$, e portanto, $q - Tr(b)^{p^k} = 0$.

Agora pela proposição 4.6, obtemos $Tr(b^{p^k}) = q$.

Assim, $b^{p^k} + t^{-1} b^{p^k} t + \cdots t^{-(q-1)} b^{p^k} t^{q-1} = q$.

Segue daí que existe um i tal que

$$t^{-i} b^{p^k} t^i = 1,$$

e portanto,

$$b^{p^k} = 1.$$

Logo $(a,t)^{p^k} = 1$, Para todo $a \in A$.

Assim concluimos que (A,t) tem expoente limitado menor ou igual a p^k. Pelo lema 4.3 temos que $G' = (A,t)$, e portanto G' tem expoente limitado menor ou igual a p^k.

Caso 2: $q = p$

Seja $a \in A$. Como no caso anterior definiremos α e β tal que $\alpha^2 = \beta^2 = 0$.

Seja $\alpha = \tau$

$$\tau^2 = p\tau = 0,$$

e $\beta = a^{-1} \tau a$,

$$\beta^2 = (a^{-1} \tau a)^2 = a^{-1} \tau^2 a = 0$$

Usando raciocínio análogo ao caso anterior temos que $\beta\alpha\beta F[G]$ é ideal nil a direita de grau limitado menor ou igual a n, onde n é um número que não depende de a.

Portanto existe $k > 0$ tal que

$$(\beta\alpha)^{p^k} = 0.$$

Observando que

$$\beta\alpha = a^{-1}\tau a\tau = a^{-1}Tr(a)\tau$$

temos

$$(\beta\alpha)^2 = a^{-1}Tr(a)\tau a^{-1}Tr(a)\tau =$$
$$a^{-1}Tr(a)\tau a^{-1}\tau Tr(a) = a^{-1}Tr(a)Tr(a^{-1})\tau Tr(a) =$$
$$Tr(a)Tr(a^{-1})a^{-1}Tr(a)\tau = Tr(a)Tr(a^{-1})\beta\alpha.$$

Se $i \geq 2$ temos, por um argumento de indução:

$$(\beta\alpha)^i = [Tr(a^{-1}) \cdot Tr(a)]^{i-1} \cdot \beta\alpha.$$

Usando o fato que $Tr(F[A]) \subseteq Z(F[G])$ e desenvolvendo $\tau(\beta\alpha)^{p^k} = 0$ temos

$$\tau(\beta\alpha)^{p^k} = [Tr(a^{-1})Tr(a)]^{p^k-1}\tau\beta\alpha =$$
$$= [Tr(a^{-1})Tr(a)]^{p^k-1}Tr(a)\tau a^{-1}\tau =$$
$$= [Tr(a^{-1})Tr(a)]^{p^k-1}Tr(a)Tr(a^{-1})\tau =$$
$$= [Tr(a^{-1})Tr(a)]^{p^k}\tau = 0.$$

Como $\langle t\rangle \cap A = (1)$ e $[Tr(a^{-1}) \cdot Tr(a)]^{p^k} \in F[A]$, usando o mesmo raciocínio do primeiro caso, concluimos a partir de $[Tr(a^{-1}) \cdot Tr(a)]^{p^k} \cdot (1 + t + \cdots t^{p-1}) = 0$, que

$$[Tr(a^{-1}) \cdot Tr(a)]^{p^k} = 0.$$

Seja $b = a^{p^k}$. Por 4.6 temos

$$0 = [Tr(a^{-1})Tr(a)]^{p^k} = Tr(a^{-1})^{p^k}Tr(a)^{p^k} = Tr(a^{-p^k})Tr(a^{p^k}) = Tr(b^{-1})Tr(b).$$

E por 4.7

$$0 = Tr(b^{-1}) \cdot Tr(b) = Tr(b^{-1} \cdot Tr(b)) = Tr(b^{-1} + b^{-1} \cdot b^t + \cdots + b^{-1} \cdot b^{t^{p-1}}) =$$

$$= \sum_{i=0}^{p-1} Tr(b^{-1} \cdot b^{t^i}).$$

Como

$$Tr(b^{-1} \cdot b^{t^0}) = Tr(b^{-1} \cdot b) = Tr(1) = p = 0$$

segue que

$$0 = \sum_{i=1}^{p-1} Tr(b^{-1} \cdot b^{t^i}) =$$

$$\sum_{i=1}^{p-1} \sum_{j=0}^{p-1} (b^{-1} \cdot b^{t^i})^{t^j} =$$

$$\sum_{i=1,j=0}^{p-1} b^{-t^j} \cdot b^{t^{i+j}}.$$

Temos então a soma de $p(p-1)$ elementos de G, em $F[G]$.

Esta soma só será igual a 0 se para cada $b^{-t^j} b^{t^{i+j}}$ existir um número kp de elementos iguais a ele. Ou seja, para cada

$$i_0, j_0 \text{ com } i_0 \geq 1, j_0 \geq 0$$

devemos ter

$$|\{(i,j) | b^{-t^j} \cdot b^{t^{i+j}} = b^{-t^{j_0}} \cdot b^{t^{i_0+j_0}}\}| = kp,$$

para algum $k \in \mathbb{N}$, k diferente de 0.

Logo

$$|\{b^{-t^j} b^{t^{i+j}} | 0 \leq j \leq p-1, 1 \leq i \leq p-1\}| \leq \frac{p(p-1)}{p} = p-1,$$

em particular,

$$|\{b^{-t^j} \cdot b^{t^{1+j}} | 0 \leq j \leq p-1\}| \leq p-1.$$

Portanto existem j_1 e j_2 distintos tais que

$$b^{-t^{j_1}} b^{t^{1+j_1}} = b^{-t^{j_2}} b^{t^{1+j_2}}$$

ou

$$b^{(t-1)t^{j_1}} = b^{(t-1)t^{j_2}}.$$

Supondo $j_2 > j_1$, temos:

$$b^{(t-1)} = b^{(t-1) \cdot t^{j_2 - j_1}},$$

que implica

$$b^{t-1} = t^{j_1 - j_2} b^{(t-1)} t^{j_2 - j_1}$$

logo b^{t-1} comuta com $t^{j_2-j_1}$.

Como $|\langle t\rangle|$ é primo, e $j_2 - j_1$ não é múltiplo de p, o elemento $t^{j_2-j_1}$ gera $\langle t\rangle$. Portanto $b^{(t-1)}$ comuta com t. Assim $b^{-1}b^t \in C_G(t)$ o que implica que $b^{-1}b^t \in (A,t) \cap C_G(t)$.

Pelo lema 4.3 temos

$$(b^{-1}b^t)^p = 1 = (a^{-p^k}t^{-1}a^{p^k}t)^p = (a^{-1}t^{-1}at)^{p^{k+1}}.$$

Como tomamos a arbitrário em A e $G' = (A,t)$ temos que G' tem período menor ou igual a p^{k+1} e portanto G' tem período limitado. ■

Vamos remover agora a hipótese de q ser primo:

Lema 4.10. *Sejam $G = \langle A, t\rangle$ onde A é um subgrupo abeliano normal e t tem ordem q, e F um corpo infinito de característica $p > 0$. Então se $U(F[G])$ satisfaz uma identidade de grupo G' tem período finito.*

DEMONSTRAÇÃO:

Vamos fazer indução em q.

Se q é primo segue pelo lema 4.9 que se $U(F[G])$ satisfaz uma identidade de grupo, então G' tem período finito.

Se q não é primo, existe $\langle s\rangle$ subgrupo próprio de $\langle t\rangle$, com $\langle s\rangle \neq 1$

Seja $H = \langle A, s\rangle$. Como H satisfaz a hipótese de indução H' tem período finito, e pelo lema 4.3 $H' = (A,s)$.

Tomemos $B = \langle H', s\rangle$

Como $H' \lhd B$, temos que $B = H' \cdot \langle s\rangle$, e portanto, todo $b \in B$, é da forma

$$b = hk,$$

com $h \in H'$, e $k \in \langle s\rangle$. Vamos provar que B tem período finito e que $B \lhd G$.

B tem período finito:

Seja $b \in B$, $b = hk$, com $h \in H'$ e, $k \in \langle s\rangle$.

Seja $\bar{b} = b \cdot H'$, temos

$$\bar{b} = \bar{h}\bar{k} = \bar{k},$$

visto que $h \in H'$.

Logo, como

$$|\langle s\rangle| < |\langle t\rangle| = q < \infty,$$

notando por j a ordem de s temos $b^j \in H'$.

Como H' tem período finito, digamos n, temos

$$(b^j)^n = b^{jn} = 1$$

para todo $b \in B$.

Logo B tem período finito. (período de $B \leq jn$).

B é normal em G:

Basta mostrar que A e t normalizam B, pois $G = \langle A, t \rangle$.

A normaliza B:

Como $H' \leq B$, temos $B \lhd H$. Portanto, como $A \leq H$, temos que A normaliza B.

$\langle t \rangle$ normaliza B:

Seja $b \in B$, $b = hk$ com $h \in H'$ e $k \in \langle s \rangle$. Usando a proposição 4.3 temos que h é da forma (a_α, s_α), com $a_\alpha \in A$, e $s_\alpha \in \langle s \rangle$. De $\langle s \rangle < \langle t \rangle$ segue que t comuta com k e com s_α. Temos então

$$\begin{aligned} t^{-1}bt = t^{-1}hkt = t^{-1}htk = \\ = t^{-1}a_\alpha^{-1}s_\alpha^{-1}a_\alpha s_\alpha tk = \\ = t^{-1}a_\alpha^{-1}ts_\alpha^{-1}t^{-1}a_\alpha ts_\alpha k. \end{aligned}$$

Além disto, como $A \lhd G$ temos $t^{-1}a_\alpha t \in A$, e fazendo $a_\beta = t^{-1}a_\alpha t$ teremos,

$$t^{-1}bt = \underbrace{a_\beta{}^{-1}s_\alpha{}^{-1}a_\beta s_\alpha}_{\in H'} \underbrace{k}_{\langle s \rangle} \in B.$$

Logo $B \lhd G$.

Podemos portanto considerar $\bar{G} = \frac{G}{B} = \left\langle \bar{A}, \bar{t} \right\rangle$.

Claramente $\bar{A} \lhd \bar{G}$ e $\bar{A}$ é abeliano. Também vale que $o(\bar{t}) \leq \frac{o(t)}{o(s)}$ e como $\langle s \rangle \neq (1)$, $o(\bar{t}) < o(t)$. Pelo lema 4.2 temos que $U(F[\bar{G}])$ satisfaz a mesma identidade de grupo que $U(F[G])$. Assim podemos usar a hipótese de indução e, concluir que $\bar{G}'$ tem período finito.

Assim, como

$$\bar{G}' = \left(\frac{G}{B}\right)' = \frac{G' \cdot B}{B} \cong \frac{G'}{G' \cap B},$$

e $G' \cap B \leq B$ tem período finito, G' tem período finito.

(per$(G') \leq$ per$(B)\cdot$ per$(\bar{G}')$.) ■

Vamos agora supor apenas que G tem um subgrupo abeliano normal, de índice finito. Neste próximo caso G pode ter mais geradores fora do subgrupo A. Aqui usaremos que G é um grupo de torção.

Lema 4.11. *Sejam G grupo de torção e F um corpo infinito de característica $p > 0$. Se $U(F[G])$ satisfaz uma identidade de grupo e G tem um subgrupo normal A abeliano, de índice finito, então G' tem período limitado.*

Demonstração:

Nosso intuito nesta demonstração será construir um subgrupo B normal em G, de período limitado, tal que $\left(\frac{G}{B}\right)'$ tenha período finito.

Seja

$$B = \left\langle L' | A \leq L \leq G, \frac{L}{A} \text{ é cíclico} \right\rangle.$$

Vamos inicialmente mostrar que B tem período finito:

Como $[G : A] < \infty$, pelo teorema da correspondência, existirá uma relação biunívoca entre os conjuntos $\{L|A \leq L \leq G\}$, e $\{\frac{L}{A}|\frac{L}{A} \leq \frac{G}{A}\}$, e portanto $\{L|A \leq L \leq G\}$ será finito.

Como $\frac{L}{A}$ é cíclico, temos $L = \langle A, t\rangle$, com $t \in G$. Como $o(t)$ é finita, pelo lema 4.10, L' tem período finito, e pelo lema 4.3, $L' \leq A$, pois $L' = (A, t)$ e A é normal em G. Logo $B \leq A$, e portanto B é abeliano.

Ora B é um grupo gerado por um número finito de grupos de período finito que é abeliano. Logo B terá período finito.

Vamos mostrar agora que B é normal em G.

Se $A \leq L \leq G$, para todo $g \in G$, temos

$$g^{-1}Ag \leq g^{-1}Lg \leq G.$$

Como $A \lhd G$, para todo $g \in G$, $A = g^{-1}Ag$, e portanto,

$$\frac{g^{-1}Lg}{A} \cong \frac{L}{A}.$$

Logo $\frac{g^{-1}Lg}{A}$ será cíclico, e portanto $(g^{-1}Lg)'$ estará contido em B.

Seja $b \in B$, $b = h_1 \cdots h_n$, com $h_i \in L_i{}'$ com $\frac{L_i}{A}$ cíclico. Para todo $g \in G$ temos

$$g^{-1}bg = g^{-1}h_1 g \cdots g^{-1}h_n g$$

Como $g^{-1}h_i g \in (g^{-1}L_i g)'$ para todo i, e $(g^{-1}L_i g)' \leq B$ sempre que $L_i{}' \leq B$ temos que $g^{-1}h_i g \in B$ para todo i e portanto $g^{-1}bg \in B$, para todo $g \in G$.

Logo $B \lhd G$.

Vamos agora demonstrar que $\left(\frac{G}{B}\right)'$ é finito.

Se observarmos que para todo $g \in G$, o grupo $\dfrac{\langle A, g\rangle}{A}$ é cíclico e que pelo lema 4.3, $\langle A, g\rangle' = (A, g) \leq B$, temos que $a^{-1}g^{-1}ag \in B$ para todo $g \in G$, e para todo $a \in A$

Portanto temos

$$agB = gaB,$$

para todo $a \in A$ e para todo $g \in G$ donde concluimos que $\dfrac{A}{B}$ é central em $\dfrac{G}{B}$.

Usando o fato que $[\frac{G}{B} : \frac{A}{B}] = [G : A] < \infty$, do lema 1.3 temos que $\left(\frac{G}{B}\right)'$ é finito.

Como $L \leq G$, temos que $L' \leq G'$ e portanto $B \leq G'$ e assim

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

Como B tem período finito segue que G' tem período finito. ■

Vamos por fim retirar a hipótese A abeliano, e concluir a passagem (i)$\Longrightarrow$(ii). Mostraremos também que G' é p-grupo, e que G tem um subgrupo normal de índice finito p-abeliano.

Teorema 4.12. (i) $\Longrightarrow$ (ii).

DEMONSTRAÇÃO:

Assumindo que $U(F[G])$ satisfaz uma identidade de grupo, por 3.1 temos que $F[G]$ satisfaz uma identidade polinomial. Pelo lema 3.16 G tem um subgrupo A, p-abeliano, normal de índice finito.

Além disso, pelo lema 3.21 , segue que G' é um p-grupo. Resta mostrar, portanto, que G' tem período limitado.

Seja $G_1 = \frac{G}{A'}$ e $A_1 = \frac{A}{A'}$. ($A' \lhd G$ porque A' é subgrupo característico de A).

A_1 é subgrupo abeliano normal de G_1, e $[G_1 : A_1] = [G : A] < \infty$. Além disso pelo lema 4.2, se $U(F[G])$ satisfaz uma identidade de grupo, então $U(F[G_1])$ também irá satisfazer.

Agora usando o lema 4.11 segue que G_1' tem periodo finito. Assim, observando que

$$G_1' = \left(\frac{G}{A'}\right)' \cong \frac{G'}{A'}$$

e que A' é finito, concluimos que

$$\text{per}(G') \leq |A'| \cdot \text{per}(G_1') < \infty$$

Logo G' tem período finito, e assim concluimos a demonstração que (i)$\Longrightarrow$(ii) ■

4.3 A implicação (ii) $\Longrightarrow$ (iii).

Vamos inicialmente demonstrar o seguinte lema:

Lema 4.13. *Seja R uma F-álgebra e seja I um ideal de R que é nil de grau limitado ($\leq p^k$). Se $U(\frac{R}{I})$ satisfaz $(x,y)^{p^j} = 1$, então $U(R)$ satisfaz $(x,y)^{p^{j+k}} = 1$.*

DEMONSTRAÇÃO:

Seja

$$\begin{array}{rcl} \varphi : R & \longrightarrow & \frac{R}{I} \\ a & \longmapsto & a \cdot I \end{array}$$

φ induz um homomorfismo sobrejetor de grupos

$$\varphi : U(R) \longrightarrow U\left(\frac{R}{I}\right).$$

Se $x, y \in U(R)$, então,

$$(\bar{x}, \bar{y})^{p^j} = 1, (\bar{x} = \varphi(x), \bar{y} = \varphi(y)).$$

Logo $(x,y)^{p^j} - 1 \in I$. Como I é nil de expoente limitado existe p^k, tal que, para todo $i \in I$ $i^{p^k} = 0$. Assim

$$((x,y)^{p^j} - 1)^{p^k} = (x,y)^{p^{j+k}} - 1 = 0,$$

e portanto,

$$(x,y)^{p^{j+k}} = 1,$$

como queriamos demonstrar. ■

Seja $M_n(R)$ o anel de matrizes $n \times n$ sobre um anel R. Denotaremos por $[\alpha_{i,j}]$ a matriz pertencente a $M_n(R)$, que tem para cada i e j o elemento $\alpha_{i,j} \in R$ na i-ésima linha e j-ésima coluna.

Lema 4.14. *Seja A um subgrupo normal abeliano de G de índice finito n, e seja I um ideal de $F[A]$ nil de grau limitado menor ou igual a p^k G-invariante (ie $gIg^{-1} = I$ para todo $g \in G$). Então $I \cdot F[G]$ é um ideal de $F[G]$ que é nil de grau limitado menor ou igual a np^k.*

DEMONSTRAÇÃO:

Seja $\{g_1, \ldots, g_n\}$ um conjunto completo de representantes para A em G, e seja φ o homomorfismo:

$$\begin{array}{rcl} \varphi : F[G] & \longrightarrow & M_n(F[A]) \\ \alpha & \longrightarrow & [\alpha_{i,j}], \end{array}$$

onde $\alpha_{i,j}$ é definida pela fórmula :

$$g_i \cdot \alpha = \sum_{j=1}^{n} \alpha_{i,j} \cdot g_j$$

φ está bem definida, visto que a representação de $g_i\alpha$ através das classes laterais é única. Vamos mostrar que φ é homomorfismo:

É óbvio que vale $\varphi(x+y) = \varphi(x) + \varphi(y)$, vamos mostrar que

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

Sejam $\varphi(x) = [\alpha_{i,j}]$, e $\varphi(y) = [\beta_{i,j}]$.

Temos

$$g_i xy = (\sum_{k=1}^{n} \alpha_{i,k} g_k)y =$$

$$\sum_{k=1}^{n}\sum_{j=1}^{n} \alpha_{i,k}\beta_{k,j} g_j = \sum_{j=1}^{n}(\sum_{k=1}^{n} \alpha_{i,k}\beta_{k,j})g_j.$$

Pela definição de $\varphi(xy)$, concluimos que

$$\varphi(xy) = [\sum_{k=1}^{n} \alpha_{i,k} \cdot \beta_{k,j}] = [\alpha_{i,j}] \cdot [\beta_{i,j}] =$$

$$\varphi(x) \cdot \varphi(y).$$

Além disso se $\varphi(\alpha) = 0$, $\alpha_{i,j} = 0$ para cada i, e j. Logo para todo i

$$g_i \alpha = \sum_{j=1}^{n} \alpha_{i,j} g_j = 0$$

O que resulta em $\alpha = 0$ visto que g_i é inversível em $F[G]$. Logo φ é injetora.

Certamente $I \cdot F[G]$ é ideal de $F[G]$. Mostraremos agora que $I \cdot F[G]$ é nil de grau limitado menor ou igual a np^k. Para tanto demonstraremos que $\varphi(I \cdot F[G]) \leq M_n(I)$, e que $M_n(I)$ é nil de grau limitado. Do fato que φ é injetora segue que $I \cdot F[G]$ é nil de grau limitado.

Vamos mostrar que $\varphi(I \cdot F[G]) \leq M_n(I)$. Como I é G-invariante, para todo $\alpha \in I \cdot F[G]$, teremos $g_i \alpha g_j^{-1} \in I \cdot F[G]$.

Pelo lema 1.18 , temos que $\alpha_{i,j} = \pi_A(g_i \alpha g_j^{-1})$, onde π_A é a função :

$$\begin{array}{rcl} \pi_A : F[G] & \longrightarrow & F[A] \\ \alpha = \sum\limits_{g \in G} \alpha_g g & \longmapsto & \sum\limits_{a \in A} \alpha_a a \end{array}$$

Como I é G-invariante e $A \lhd G$ temos pelo lema 1.20 que

$$I = \pi_A(I \cdot F[G]),$$

e portanto $\alpha_{i,j} \in I$, para todo i, e para todo j, logo

$$\varphi(I \cdot F[G]) \subseteq M_n(I).$$

Vamos provar que $M_n(I)$ é nil de grau limitado menor ou igual a np^k.

Seja $\sigma \in M_n(I)$. Como $I \leq F[A]$ I é comutativo. Seja $p_\sigma(x)$ o polinômio característico da matriz σ

$$p_\sigma(x) = x^n - \gamma_{n-1} x^{n-1} - \cdots - \gamma_0.$$

com γ_i pertencentes a I. Usando o teorema de Cayley-Hamilton (ver teorema 1.15),temos :

$$\sigma^n = \gamma_0 + \gamma_1 \cdot \sigma + \cdots + \gamma_{n-1} \cdot \sigma^{n-1}.$$

Elevando os dois lados a p^k, observando que a característica de F é p e, que I é comutativo temos :

$$(\sigma^n)^{p^k} = \gamma_0^{p^k} + \gamma_1^{p^k} \cdot \sigma^{p^k} + \cdots + \gamma_{n-1}^{p^k} \cdot \sigma^{(n-1)p^k} = 0,$$

visto que I é nil de grau limitado, igual a p^k. Assim concluimos nossa demonstração. ■

Vamos provar agora (ii) $\Longrightarrow$ (iii):

Teorema 4.15. (ii) $\Longrightarrow$ (iii).

DEMONSTRAÇÃO:

Vamos dividir a demonstração em etapas:

1ª **etapa.** *Se existe A central em G tal que $[G : A] < \infty$, e G' é p-grupo então $U(F[G])$ satisfaz uma identidade de grupo do tipo $(u, v)^{p^k} = 1$.*

De fato: Se A é central e $[G : A] < \infty$ temos pelo lema 1.3 que G' é finito.

Seja

$$\pi : F[G] \longrightarrow F[\frac{G}{G'}]$$

o epimorfismo canônico, Pela proposição 1.23, do fato de G' ser um p-grupo finito, vem que $\ker(\pi)$ é nilpotente.

Mas

$$F\left[\frac{G}{G'}\right] = \frac{F[G]}{ker(\pi)}$$

e $U(F[\frac{G}{G'}])$ satisfaz $(u, v) = u^{-1}v^{-1}uv = 1$. Logo pelo lema 4.13, temos que $U(F[G])$ satisfaz $(u, v)^{p^k}$ para algum k.

2ª **etapa.** *Se G tem um subgrupo normal abeliano A de índice finito, e G' é p-grupo de período limitado, então $U(F[G])$ satisfaz uma identidade de grupo do tipo $(u, v)^{p^k} = 1$.*

De fato, seja $B = (A, G)$. Um elemento b pertencente a B será da forma:

$$b = (a_1, g_1) \cdots (a_n, g_n),$$

com $a_i \in A$ e $g_i \in G$. Para todo $h \in G$ temos

$$h^{-1}bh = h^{-1}a_1^{-1}h \cdots h^{-1}a_n h \cdot h^{-1}g_n h,$$

Como $A \lhd G$ $h^{-1}ah \in A$ para todo $a \in A$. Assim, $h^{-1}bh \in B$ e portanto $B \lhd G$.

Como $g_1^{-1}ag_1 \in A$, $B \leq A$ e $B \leq G'$. Portanto

$$B \leq A \cap G'.$$

Logo B é um p-grupo abeliano de período limitado.

Seja $\pi : F[A] \longrightarrow F[\frac{A}{B}]$, o epimorfismo canônico.

Vamos mostrar que $\ker(\pi)$ é nil de grau limitado. De fato

$$\ker(\pi) = \Delta(B) \cdot F[A],$$

Seja p^j o expoente de B, e seja $x \in \ker(\pi)$. Então

$$x = \sum(1 - b_i)\alpha_i$$

com $b_i \in B$ e $\alpha_i \in F[A]$. Portanto

$$x^{p^j} = [\sum(1 - b_i)\alpha_i]^{p^j} = \sum(1 - b_i)^{p^j}\alpha_i^{p^j} =$$

$$= \sum(1 - b_i^{p^j})\alpha^{p^j} = 0$$

pois

$$(1 - b_i^{p^j}) = 0,$$

para todo $b_i \in B$.

Além disso

$$g^{-1}\Delta(B) \cdot F[A]g = g^{-1}\Delta(B)g \cdot g^{-1}F[A]g =$$
$$= \Delta(B) \cdot F[A],$$

visto que $B \lhd G$ e $A \lhd G$. Logo $\Delta BF[A]$ é ideal G-invariante.

Seja

$$\pi_2 : F[G] \longrightarrow F\left[\frac{G}{B}\right],$$

a projeção canônica.

Temos $\ker(\pi_2) = \Delta(B) \cdot F[G] = (\Delta(B) \cdot F[A]) \cdot F[G]$

Como $\Delta B \cdot F[A]$ é G-invariante e nil de grau limitado, pelo lema 4.14 $\Delta B \cdot F[G]$ é um ideal nil de grau limitado de $F[G]$. Por outro lado $\frac{A}{B}$ é um subgrupo de $\frac{G}{B}$ tal que

$$a^{-1}g^{-1}ag \in B,$$

e portanto $\frac{A}{B}$ é central em $\frac{G}{B}$.

Além disso $[\frac{G}{B} : \frac{A}{B}] = [G : A] < \infty$.

Assim $\dfrac{G}{B}$ tem um subgrupo central de índice finito, e $\dfrac{G'}{B} = \left(\dfrac{G}{B}\right)'$ é p-grupo (pois G' é p-grupo). Pela 1ª etapa, temos que $U(F[\frac{G}{B}])$ satisfaz uma identidade do tipo,

$$(u, v)^{p^l} = 1.$$

Agora $F[\dfrac{G}{B}] = \dfrac{F[G]}{ker(\pi_2)}$ e $ker(\pi_2)$ é nil de período limitado. Assim, pelo lema 4.13 $F[G]$ satisfaz uma identidade de grupo do tipo $(u, v)^{p^k} = 1$.

3ª etapa. *Se G é um grupo de torção, que tem um subgrupo normal p-abeliano A de índice finito, e G' é um p-grupo de período limitado então $U(F[G])$ satisfaz uma identidade de grupo do tipo $(u, v)^{p^k} = 1$.*

De fato, seja

$$\pi_3 : F[G] \longrightarrow F\left[\frac{G}{A'}\right],$$

o epimorfismo canônico. Como A' é p-grupo finito segue pelo lema 1.23 que $\ker(\pi_3)$ é nilpotente.

Por outro lado $\dfrac{G}{A'}$ tem um subgrupo normal abeliano de índice finito $\dfrac{A}{A'}$, e $\left(\dfrac{G}{A'}\right)' \cong \dfrac{G'}{A' \cap G'}$ é p-grupo de período limitado. Pela 2ª etapa podemos concluir que $U(F[\frac{G}{A'}])$ satisfaz uma identidade de grupo do tipo $(u, v)^{p^j} = 1$.

Assim, pelo lema 4.13, temos que $U(F[G])$ satisfaz uma identidade de grupo do tipo

$$(u, v)^{p^k} = 1,$$

concluindo assim a demonstração de (ii)$\Longrightarrow$(iii). ■

Como (iii)$\Longrightarrow$(i) é trivial concluimos a demonstração do teorema.

Bibliografia

[BRT] Y.Billig, D.Riley, e V.Tasic, *Non-matrix varieties and nil generated algebras whose units satisfy a group identity.* (preprint)

[DG97] M.A.Dokuchaev, e J.Z.Gonçalves, *Semigroup identity on units of integral group rings.* Glasgow Math. Journal, 39 (1997) pp 1-6

[GJV94] A.Giambruno, E.Jespers, e A.Valenti, *Group identities on units of rings.* Arch.Math. 63 (1994) pp 241-243

[GSV97] A.Giambruno, S.K.Sehgal, e A.Valenti, *Group algebras whose units satisfy a group identity.* Proceedings of The American Mathematical Society. 125, (1997) pp 629-634.

[JZG84] J.Z.Gonçalves, *Free groups of units in group rings.* Canadian Mathematical Bulletin 27 (1984) pp 309-312.

[GM91] J.Z.Gonçalves, e A.Mandel, *Semigroups identities on units of group algebras.* Arch.Math. 57 (1991) pp 539-545.

[GP96] J.Z.Gonçalves, D.S.Passman, *Construction of free subgroups in the groups of units of modular group algebra.* Comunications in Algebra, 24 (13), 4211-4215 (1996)

[HP80] B.Hartley, P.F.Pickel, *Free subgroups in the unit groups of integral group rings.* Canadian Journal of Mathematics, vol 32, num:6, (1980), pp 1342-1352.

[Lam91] T.Y.Lam, *A first course in non-comutative rings.* Springer Verlag, New York, 1991.

[KD93] H.Kopka e P.W.Daly, *A guide to Latex 2ϵ: document preparation from beginners and advanced users 2nd edition.* Addison-Wesley Publishing Company, 1993.

[Liu] C.H.Liu, *Group algebras with units satisfying a group identity.* (preprint)

[LS77] R.C.Lyndon, e P.E.Schupp, *Combinatorial group theory.* Springer Verlag, Berlin, 1977.

[MKS76] W.Magnus, A.Karras, e D.Solitar, *Combinatorial group theory: presentations of groups in terms of generators and relations.* Dover Publications Inc., New York, 1976.

[Pas71] D.S.Passman, *Group rings satisfying a polynomial identity II.* Pacific Journal of Mathmatics, 39 (1971) pp 425-438

[Pas77] D.S.Passman, *The algebraic struture of group rings.* John Willey and Sons, New York 1977.

[Pas97] D.S.Passman, *Group algebras whose units satisfy a group identity II.* Proceedings of The American Mathematical Society. 125, (1997) pp 657-662.

[Rob95] D.J.S.Robinson, *A course in the theory of groups 2nd edition.* Springer Verlag, New York, 1995.

[Row80] L.H.Rowen, *Polynomial identities in ring theory.* Academic Press, London-New York San Francisco. 1980.

[Sco87] W.R.Scott, *Group theory.* Dover Publications Inc., New York, 1987.

[Seh78] S.K.Sehgal, *Topics in group rings.* Marcel Dekker, New York, 1978.

[Seh93] S.K.Sehgal, *Units in integral group rings.* Longman, Essex, 1993.

[Tits72] J.Tits, *Free subgroups in linear groups.* Journal of Algebra, 20, (1972), pp 250-270.

[War81] D.S.Warhurst, *Topics in group rings.* Thesis Manchester, 1981.