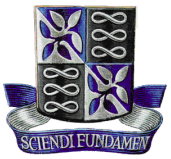
Universidade Federal da Bahia - UFBA
Instituto de Matemática - IM
Programa de Pós-Graduação em Matemática - PGMAT
Tese de Doutorado



A Estrutura do Grupo Adjunto e a Propriedade do Normalizador

Márcia Graci de Oliveira Matos

Salvador-Bahia
Fevereiro de 2016

A Estrutura do Grupo Adjunto e a Propriedade do Normalizador

Márcia Graci de Oliveira Matos

Tese de Doutorado apresentada ao Colegiado do Programa de Doutorado em Matemática da Universidade Federal da Bahia em Associação com a Universidade Federal de Alagoas, como requisito parcial para obtenção do título de Doutor em Matemática.

Orientador: Prof. Dr. Thierry Corrêa Petit Lobão.

Salvador-Bahia
Fevereiro de 2016

Matos, Márcia Graci de Oliveira,

M382 A Estrutura do Grupo Adjunto e a Propriedade do Normalizador / Márcia Graci de Oliveira Matos. – Salvador: UFBA, 2016.

– f. 62 : il.

Orientador: Prof. Dr. Thierry Corrêa Petit Lobão.

Tese (doutorado) – Universidade Federal da Bahia, Instituto de Matemática, Programa de Pós-graduação em Matemática, 2016.

Referências bibliográficas.

1. Anéis de grupo integrais - Validade da propriedade do normalizador. 2. Radical de Jacobson. 3. Grupo Adjunto - Estrutura. 4. Grupo geral linear. 5. Propriedade do normalizador I. Petit Lobão, Thierry. II. Universidade Federal da Bahia, Instituto de Matemática. III. Título.

CDD : 510

A Estrutura do Grupo Adjunto e a Propriedade do Normalizador

Márcia Graci de Oliveira Matos

Tese de Doutorado apresentada ao Colegiado do Programa de Doutorado em Matemática da Universidade Federal da Bahia em Associação com a Universidade Federal de Alagoas, como requisito parcial para obtenção do título de Doutor em Matemática, aprovada em 18 de fevereiro de 2016.

Banca examinadora:

Prof. Dr. Thierry Corrêa Petit Lobão (Orientador)
UFBA

Profa. Dra. Carmela Sica
UFBA

Profa. Dra. Manuela da Silva Souza
UFBA

Profa . Dra. Paula Murgel Veloso
UFF

Prof. Dr. Raul Antonio Ferraz
IME-USP

Aos meus pais Agostinho e Joseilda (in memorian)
A Ailton, Marcela e Letícia

"*Sem Sonhos a vida não tem brilho. Sem metas, os sonhos não têm alicerces. Sem prioridades os sonhos não se tornam reais. Sonhe, trace metas, estabeleça prioridades e corra riscos para executar seus sonhos. Melhor é errar por tentar do que errar por se omitir.*"

(Augusto Cury)

Agradecimentos

Não poderia deixar de reservar uma parte desse texto para agradecer a todos aqueles que direta ou indiretamente contribuíram para essa realização.

Agradeço em primeiro lugar a Deus que sempre me fortaleceu e iluminou toda minha caminhada e por ter me amparado nos momentos mais difíceis.

Aos meus pais, Agostinho e Joseilda(in memorian) que me deram a vida e me ensinaram a vivê-la com tantos valores e dignidade e a lutar pelos meus ideais.

A meu esposo, Ailton, que com muito carinho, apoio e compreensão não mediu esforços para que eu chegasse até esta etapa de minha vida; por estar sempre ao meu lado e por muitas vezes ter assumido o papel de pai e mãe durante as minhas ausências.

Às minhas filhas Marcela e Leticia que foram carinhosas, pacientes e compreensivas durantes esses anos, principalmente a Marcela que muitas vezes ajudava a cuidar da irmã mais nova para que eu pudesse desenvolver as minhas atividades como doutoranda.

Aos meus irmãos, irmãs, cunhados, cunhadas, meus sobrinhos e sobrinhas pelo carinho, pela amizade, pelas orações e por todo apoio moral principalmente nas horas mais angustiantes.

Aos meus tios, tias, primos e primas, em especial a Mirian e sua família pela acolhida em Maceió.

Agradeço ao meu orientador, professor Thierry Corrêa Petit Lobão, por toda a sua disposição, pela paciência na orientação e incentivo que tornaram possível a conclusão deste trabalho.

Agradeço às professoras Carmela Sica, Manuela da Silva Souza e Paula Murgel Veloso e ao professor Raul Antonio Ferraz por aceitarem participar da comissão julgadora de minha tese e pelas sugestões e correções para o texto.

A todos os professores do IM-UFBA pelos conselhos e sugestões que foram importantes no desenvolvimento desta tese.

Ao professor André Flores do IM-UFAL pela convivência e aprendizado oportunizado no decorrer da disciplina de Teoria de Grupos.

Aos colegas do Programa de Pós-Graduação em matemática da UFBA, Em especial a Elen, Edward, Jaqueline, Alejandra e Carina.

A Katia Lima Rocha, Luis Alberto e Aubedir Seixas pela amizade e companheirismo, principalmente no período que estivemos em Maceió.

A todos os funcionários da Pós-Graduação do IM-UFBA, pela competência, disposição e atenção.

A todos os meus colegas e companheiros de trabalho do DQE-UESB por terem me apoiado e incentivado incondicionalmente.

Aos amigos de Jequié, que escolhi para conviver, obrigada pelo incentivo e pelo apoio constantes.

Aos amigos que tive a oportunidade de conviver durantes esses anos em Salvador, obrigada pelo carinho e pelo apoio.

Finalmente, agradeço a Uesb pelo auxilio financeiro.

Resumo

Em um anel R, o conjunto de todos os elementos quaserregulares determina o, assim chamado, grupo adjunto G, cuja operação, conhecida como círculo, foi definida por S. Perlis como $x \circ y = x + y + xy$. Este trabalho, tem como objetivo determinar a estrutura do grupo adjunto G de um anel finito R e verificar a validade da propriedade do normalizador em anéis de grupo integrais (Nor) com respeito ao grupo geral linear. Explorando a decomposição do anel R em suas p_i-componentes, concluímos que G é produto direto dos grupos adjuntos, G_{p_i}, em cada p_i-componente R_{p_i} do anel; demonstraremos então, que para cada fator G_{p_i}, o quociente G_{p_i}/pR_{p_i}, admite uma decomposição como o produto semidireto (munido da operação círculo) de J_{p_i}/pR_{p_i}, em que J_{p_i} é o radical de Jacobson do anel R_{p_i}, por um produto direto de grupos gerais lineares. Uma vez estabelecida esta estrutura, aplicamos técnicas próprias da teoria de anéis de grupo integrais e mostramos a validade de (Nor) para o grupo geral linear, $GL(n, \mathbb{F}_{q_i})$, onde $\mathbb{F}_{q_i}$ é um corpo finito e $q_i = {p_i}^n$. Provamos que vale (Nor) para cada fator $GL(n, \mathbb{F}_{q_i})$ e portanto concluímos que o produto direto desses fatores, é solução para (Nor).

Palavras-chave: Anéis; Grupos; Radical de Jacobson; Anéis de Grupo Integrais; Grupo Adjunto; Grupo Geral Linear; Propriedade do Normalizador;

Abstract

In a ring R, the set of all quasi-regular elements determine the, so-called, adjoint group G whose operation, known as circle, was defined by S. Perlis as $x \circ y = x + y + xy$. This work, has as objective to determine the structure of the group G of a finite ring R and to verify the validity of the normalizer property (Nor) for integral group rings, with respect to the general linear groups, $GL(n, \mathbb{F}_{q_i})$. Exploring the decomposition of the ring R in their p_i-components, we conclude that G is a direct product of the adjoint groups, G_{p_i}, for each $p - i$-component R_{p_i} of the ring; then we demonstrate that for each factor G_{p_i}, the quotient G_{p_i}/pR_{p_i}, admits a decomposition as a semi direct product, (endowed with the circle operation) of J_{p_i}/pR_{p_i}, which J_{p_i} is the Jacobson radical of the ring R_{p_i}, by a direct product of general linear groups. Once established this structure, we apply proper techniques of the theory of integral group rings to investigate the validity of (Nor) to general linear groups, $GL(n, \mathbb{F}_{q_i})$, where $\mathbb{F}_{q_i}$ is a finite field and $q_i = {p_i}^n$. We proved the validity of (Nor) for each factor $GL(n, \mathbb{F}_{q_i})$ and therefore we conclude that the direct product of these factors is solutions for (Nor).

Keywords: Rings; Groups; Jacobson Radical; Integral Group Rings; Adjoint Group; General Linear Group; Normalizer Property;

Sumário

Introdução

Apresentamos neste trabalho temas relacionados tanto à teoria de Grupos, teoria de Anéis quanto à teoria de Anéis de Grupo. Mais especificamente, faremos um estudo da estrutura do grupo adjunto de um anel associativo e investigaremos a validade da propriedade do normalizador para o grupo geral linear, obtido por essa decomposição.

Dados um grupo G e um anel R, associativo com unidade, determinamos um novo anel chamado anel de grupo, denotado por RG, que consiste em um módulo livre tendo os elementos do grupo G como base e os coeficientes no anel R, com a adicional operação de multiplicação entre seus elementos, definida por distributividade. Utilizaremos aqui principalmente anéis de grupo integrais, denotados por $\mathbb{Z}G$, onde G é um grupo finito e $\mathbb{Z}$ é o anel dos inteiros.

Na teoria de Anéis de Grupo, encontramos várias questões interessantes; uma delas é o Problema do Isomorfismo, conhecido como (Iso), que consiste em verificar se dois grupos serão isomorfos sempre que seus anéis de grupo o forem. A questão vem sendo discutida desde 1940, a partir dos trabalhos de G. Higman com diversos anéis de coeficientes, conforme relata C. Polcino Milies e S. K. Sehgal, [18]; entretanto, vários resultados relevantes foram obtidos utilizando-se o anel dos inteiros e, assim, a questão do isomorfismo tornou-se uma conjectura para anéis de grupo integrais:

$$\text{(Iso)} \qquad \mathbb{Z}G \simeq \mathbb{Z}H \Rightarrow G \simeq H.$$

A Propriedade do Normalizador, ou (Nor) como é conhecida, é uma outra questão de destaque na teoria dos anéis de grupo integrais sobre grupos finitos. Dizemos que um grupo G satisfaz essa propriedade quando o normalizador de G em $\mathcal{U}(\mathbb{Z}G)$, grupo das unidades de $\mathbb{Z}G$, é o menor possível, ou seja, é o produto do grupo G pelo centro do grupo de unidades:

$$\text{(Nor)} \qquad \mathcal{N}_{\mathcal{U}}(G) = G \cdot \mathcal{Z}(\mathcal{U}(\mathbb{Z}G)).$$

Essa questão também foi apresentada como conjectura, e o primeiro resultado para esta foi obtido por Coleman [2] em 1964, que conseguiu provar a validade de (Nor) para p-grupos, e em seguida provou sua validade em grupos nilpotentes. Em 1987, Jackowski e Marciniak [10] alcançaram um resultado para grupos que possuem um 2-subgrupo de Sylow normal

e portanto, obtiveram a solução para (Nor) para grupos de ordem ímpar. Em 1995, foi revelada por M. Mazur [14] uma relação existente entre (Nor) e (Iso) no contexto dos grupos infinitos; percebeu-se que, em se encontrando um contraexemplo para (Nor), é possível, a partir deste, fabricar um contraexemplo para (Iso). Para as duas questões foram obtidas várias respostas positivas, até que, M. Hertweck em 2001 [9], apresentou contraexemplos para as duas questões (Nor) e (Iso), daí, então, ambas as questões perdem o status de conjectura, porém não a relevância, uma vez que o objetivo passou a busca das classes de grupos que são soluções para (Nor) ou satisfazem (Iso). Sandling [19], obteve resultados interessantes relacionando o (Iso) aos elementos quaserregulares, mais especificamente mostrando que o grupo dos elementos quaserregulares de um anel R, denominado grupo adjunto ao anel, G, é caracterizado pelo seu anel de grupo integral, ou seja satisfaz (Iso). Podemos verificar na literatura que o radical de Jacobson é o maior ideal quaserregular contido em G, dessa forma, existe uma ligação entre o estudo de grupo adjunto de um anel e o radical de Jacobson. Portanto, uma vez que o (Iso) para o grupo adjunto de um anel já havia sido estudado e resolvido por Sandling e, que ainda não existe na literatura investigação sobre (Nor) para grupos adjuntos, procuramos determinar a estrutura do grupo adjunto G de um anel R e, como através dessa estrutura obtemos um grupo B que é isomorfo a um produto direto de grupos gerais lineares, procuramos investigar a validade de (Nor) para o grupo geral linear, $GL(n, \mathbb{F}_q)$.

No primeiro capítulo, abordamos alguns aspectos da teoria geral de Anéis, teoria de Grupo, bem como teoria de Anéis de Grupo, apresentando o *Problema do Isomorfismo* (Iso), considerando os resultados mais importantes, entre eles, os desenvolvidos por Sandling [21], com a intenção de um capítulo preliminar.

O segundo capítulo, foi destinado à Estrutura do Grupo Adjunto de um p-anel; resultado original desse trabalho. Explorando a decomposição do anel finito R em suas p-componentes, demonstramos então que cada fator G_p admite uma decomposição como o produto do radical de Jacobson desta componente, J_p, por um grupo que é uma extensão do ideal pR_p, munido da operação círculo, por um produto direto de grupos gerais lineares. Ademais, provando que pR_p é um subgrupo normal de G_p, obtemos uma decomposição deste quociente como um produto semidireto de J_p por um produto direto de grupos gerais lineares .

Abordaremos no terceiro capítulo resultados fundamentais e relevantes relacionados com a *Propriedade do Normalizador* (Nor), os quais serão utilizados no capítulo seguinte.

No quarto capítulo apresentamos a prova da validade de (Nor) para o grupo geral linear, que também se constitui em um resultado original desse trabalho.

/

Capítulo 1

Preliminares

Neste capítulo, apresentaremos conceitos e resultados da teoria de Grupos, teoria de Anéis e teoria de Anéis de Grupo que são relevantes para o desenvolvimento deste trabalho. O anel R presente no trabalho será considerado finito, associativo e com unidade.

1.1 Grupos

Nesta seção, apresentaremos e dicutiremos alguns resultados relevantes da Teoria de Grupos que podem ser verificados, por exemplo, nas referências A. Garcia; Y. S. K. Lequain [8], C. Polcino Milies; S. K. Sehgal [18] e S. K. Sehgal [21].

Definição 1.1. *Seja H um subgrupo de um grupo G. Dizemos que H é* **normal** *em G, $(H \trianglelefteq G)$ se $g^{-1}Hg = H$ para todo $g \in G$.*

Definição 1.2. *Seja G um grupo e $x, y \in G$. Os elementos x e y são ditos* **conjugados** *em G se existe $g \in G$ tal que $y = gxg^{-1}$.*

Definição 1.3. *O* **centro** *de um grupo G é o subgrupo:*

$$\mathcal{Z}(G) = \{a \in G : ax = xa, \forall x \in G\}.$$

Definição 1.4. *Para um dado grupo G, o subgrupo $G' = \langle x^{-1}y^{-1}xy;\, x, y \in G\rangle$ é chamado o* **subgrupo derivado** *de G, o elemento $[x, y] := x^{-1}y^{-1}xy \in G$, é chamado o* **comutador** *de x e y.*

Definição 1.5. *Seja H um subgrupo do grupo G. Dado um elemento $g \in G$, os subconjuntos da forma*

$$Hg = \{hg \mid h \in H\} \quad e$$

$$gH = \{gh \mid h \in H\}$$

são denominados **classe lateral à esquerda** *e* **à direita** *de H representada por g, respectivamente.*

Definição 1.6. *Seja G um grupo e H um subgrupo normal de G. O grupo de suas classes laterais com a operação induzida de G é chamado* **grupo quociente** *de G por H e é denotado por G/H.*

Definição 1.7. *Um grupo G é chamado de* **metabeliano** *se contém um subgrupo normal A que seja abeliano e o quociente G/A também seja abeliano.*

O lema a seguir determina uma condição para a qual um grupo quociente é abeliano.

Lema 1.8. *Seja N um subgrupo normal do grupo G. Assim, o grupo quociente G/N é abeliano se, e somente se, $G' \subset N$.*

Definição 1.9. *Seja G um grupo multiplicativo. Um* **automorfismo** *de G é um isomorfismo $f : G \to G$. O conjunto dos automorfismo de G será denotado por $Aut(G)$. É fácil ver que $Aut(G)$ é um grupo cuja a operação é a composição de funções.*

Definição 1.10. *Um subgrupo H de um grupo G é dito* **subgrupo característico** *se $\phi(H) = H$ para todo automorfismo $\phi : G \to G$. (H car G).*

Definição 1.11. *Seja H um subgrupo de um grupo G, definimos o* **normalizador de H em** *G por*

$$\mathcal{N}_H(G) = \left\{ g \in G;\, g^{-1}Hg = H \right\}.$$

Seja G um grupo finito, cuja ordem é $|G| = p^n m$, em que p denota um inteiro positivo primo e m um inteiro positivo não divisível por p. Devido ao Teorema de Lagrange, sabemos que a ordem de um p-subgrupo de G deve ser menor ou igual a p^n. Dessa forma, existindo um subgrupo de ordem p^n, este deve ser maximal no conjunto dos p-subgrupos de G. Daí, temos a seguinte definição:

Definição 1.12. *Seja G um grupo finito tal que $|G| = p^n m$ em que $p \nmid m$. Um subgrupo de G que tenha ordem p^n chama-se um* **p-subgrupo de Sylow** *de G.*

Apresentamos a seguir um importante resultado que caracteriza subgrupos de Sylow para grupos finitos.

Teorema 1.13. *Seja G um grupo finito de ordem $|G| = p^n m$, em que p é um inteiro primo que não divide m. Então:*

(i) G sempre contém p-subgrupos de Sylow e todo p-subgrupo de G está contido num outro p-subgrupo de Sylow de G.

(ii) Todos os p-subgrupos de Sylow de G são conjugados entre si em G.

(iii) Se n_p denota o número de p-subgrupos de Sylow de G, então

$$n_p \equiv 1 \,(mod\ p) \quad e \quad n_p \mid m.$$

Corolário 1.14. *Seja P um p-subgrupo de Sylow de um grupo G. Então,*

$$\mathcal{N}_G(\mathcal{N}_G(P)) = \mathcal{N}_G(P).$$

Definição 1.15. *Um grupo G é chamado* **nilpotente** *se contém uma série de subgrupos:*

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G,$$

tais que $G_{i-1} \trianglelefteq G$ e cada quociente $\dfrac{G_i}{G_{i-1}}$ está contido no centro de $\dfrac{G}{G_{i-1}}$, com $1 \leq i \leq n$.

Toda série de subgrupos de G que satisfaz a propriedade acima é chamada de **série central** de G.
Os grupos nilpotentes finitos podem ser caracterizados pelo seguinte resultado:

Teorema 1.16. *Seja G um grupo finito. As seguintes condições são equivalentes:*

(i) G é nilpotente;

(ii) Todo subgrupo de Sylow de G é normal em G;

(iii) G é o produto direto de seus subgrupos de Sylow.

Outros resultados importantes sobre grupos nilpotentes:

Lema 1.17. *Subgrupos e grupos quocientes de grupos nilpotentes são nilpotentes.*

Proposição 1.18. *Um p-grupo finito é nilpotente.*

Proposição 1.19. *Produtos diretos finitos de grupos nilpotentes são nilpotentes.*

1.2 Anéis, Módulos e Álgebras

Nesta seção, que é baseada em [18], apresentaremos as definições e resultados relevantes da teoria de Anéis que serão fundamentais para o desenvolvimento do nosso trabalho.

Definição 1.20. *Seja R um anel, definimos o* **grupo das unidades de** R *como*

$$\mathcal{U}(R) = \{x \in R;\ \exists\, y \in R \ e\ xy = yx = 1\}\,.$$

Definição 1.21. *Seja R um anel não necessariamente com unidade, definimos uma operação em R chamada* **operação círculo**, *por $x \circ y = x + y + xy$, para todo $x, y \in R$.*

Como essa operação é derivada da adição e do produto, em um anel, é fácil ver que ela é associativa e possui elemento neutro, 0.

Definição 1.22. *Seja R um anel. Um elemento $x \in R$ é chamado* **quaserregular à esquerda** *se existe $y \in R$ tal que $x \circ y = 0$, esse elemento y é dito ser um* **quase-inverso à esquerda** *de x. Analogamente $x \in R$ é dito* **quaserregular à direita**, *se existe $z \in R$ tal que $z \circ x = 0$.*

Definição 1.23. *Um elemento $x \in R$ é dito* **quaserregular**, *se ele é quaserregular à esquerda e à direita; Neste caso, pode-se provar que seus quase-inversos à esquerda e à direita são iguais.*

Podemos observar que, em um anel, todo elemento nilpotente é quaseregular à direita. Vejamos:
Seja $x \in R$ um elemento qualquer nilpotente, isto é, existe um número inteiro positivo n, tal que $x^n = 0$. Tomemos $y = -x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1}$, então

$$x \circ y = x+y+xy = x+(-x+x^2-x^3+\cdots+(-1)^{n-1}x^{n-1})+x(-x+x^2-x^3+\cdots+(-1)^{n-1}x^{n-1})$$

$$= x - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1} - x^2 + x^3 - x^4 + \cdots - (-1)^{n-1}x^{n-1} + (-1)^{n-1}x^n = 0.$$

Logo $y \in R$ é o quase-inverso à direita de x. Portanto todo elemento nilpotente é quaseregular á direita.
Analogamente podemos verificar que todo elemento nilpotente é quaserregular à esquerda. Contudo existem elementos quaserregulares que não são nilpotentes.

Exemplo 1.24. *Seja $\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \in \mathbb{Q} \,:\, (a,b) = 1,\ 2 \nmid b \right\}$.*
Este conjunto é um anel comutativo sobre as operações usuais de adição e multiplicação e contém o subanel $2\mathbb{Z}_{(2)}$, que está contido em $\mathbb{Q}$, ou seja, $2\mathbb{Z}_{(2)} \subset \mathbb{Q}$, logo nenhum dos elementos de $2\mathbb{Z}_{(2)}$ é nilpotente. Porém todos os elementos do subanel $2\mathbb{Z}_{(2)}$ são quaserregulares. De fato, tome $\frac{a}{b} \in 2\mathbb{Z}_{(2)}$, então $2|a$ e assim $2 \nmid (a+b)$, então $\frac{a}{a+b} \in 2\mathbb{Z}_{(2)}$. Daí, temos que:

$$\frac{a}{b} \circ \frac{-a}{a+b} = \frac{a}{b} - \frac{a}{a+b} - \frac{a^2}{(a+b)b} = 0,$$

ou seja $-\dfrac{a}{(a+b)}$ é o elemento quase-inverso de $\dfrac{a}{b}$.

Definição 1.25. *Seja R um anel. O* **radical de Jacobson** *de R, denotado por $J(R)$, é a interseção de todos os ideais maximais à esquerda de R.*

Proposição 1.26. *Seja R um anel. Então $J(R)$ é o único ideal à esquerda maximal quaserregular de R.*

Observemos, então, que esse resultado nos fornece uma definição equivalente para o Radical de Jacobson: "O Radical de Jacobson $J(R)$ de um anel R, é o ideal maximal que é composto por elementos quaserregulares."
Com base no resultado a seguir, podemos garantir que o radical de Jacobson contém qualquer ideal à esquerda nil.

Proposição 1.27. *Todo ideal à esquerda nil de um anel R está contido no radical de Jacobson $J(R)$.*

Definição 1.28. *Dizemos que um R-módulo M satisfaz a* **condição de cadeia descendente** *(D.C.C), se toda cadeia de submódulos de M:*

$$M_1 \supset M_2 \supset \cdots M_i \supset \cdots$$

estaciona, ou seja, existe um índice t tal que $M_t = M_{t+i}$ para todo inteiro positivo i. Se os submódulos de M satisfaz a (D.C.C), diz-se M é um **módulo artiniano***(Em homenagem a Emil Artin). Um anel R é chamado* **artiniano á esquerda** *se o módulo ${}_RR$ é artiniano e* **artiniano à direita** *se o módulo R_R é artiniano.*

Apresentaremos, a seguir, resultados relativos à semissimplicidade.

Definição 1.29. *Um R-módulo M é chamado* **semissimples** *se todo submódulo de M é um somando direto de M.*

Definição 1.30. *Um anel R é chamado* **semissimples** *se o módulo ${}_RR$ é semissimples.*

N. J. Divinsky, em [5], apresenta uma definição equivalente, para semissimplicidade, no caso dos anéis artinianos, relacionada a elementos quaserregulares:

Definição 1.31. *Um anel R artiniano que não possui ideais próprios formados por elementos quaserregulares é chamado* **semissimples***, ou seja, se R é semissimples, seu único ideal formado por elementos quaserregulares é o ideal nulo. Neste caso, dizemos que R é semissimples à Jacobson.*

Teorema 1.32. (**Wedderburn**) *Todo anel com divisão finito é um corpo.*

Teorema 1.33. (**Wedderburn-Artin**) *Um anel R é semissimples se, e somente se, é soma direta de anéis de matrizes sobre anéis de divisão:*

$$R \simeq M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_k}(D_k),$$

em que $M_{n_i}(D_i)$ é um anel de Matriz e cada D_i é um anel de divisão.

O resultado a seguir nos apresenta uma importante caracterização para um anel artiniano relacionando-o com anéis semissimples.

Teorema 1.34. *Seja R um anel semissimples. Então, R é artiniano e as seguintes condições valem:*
(i) R não contém ideal bilateral nilpotente.
(ii) R não contém ideal à esquerda nilpotente.
(iii) $J(R) = 0$.
Reciprocamente, se R é artiniano e alguma das condições acima vale, então R é semissimples.

A seguir, apresentaremos alguns resultados sobre álgebras finitas, cujas provas poderão ser conferidas em, Y. A. Drozd e V. V. Kirichenko, [6].

Definição 1.35. *Um polinômio irredutível, $p(x)$, sobre um corpo $\mathbb{F}$ é chamado* **separável** *se $p(x)$ não tem raízes múltiplas em qualquer extensão do corpo $\mathbb{F}$.*

Definição 1.36. *Um corpo $\mathbb{F}$ é chamado* **perfeito** *se cada extensão finita de $\mathbb{F}$ for separável ou, em outras palavras, se todo polinômio irredutível de $\mathbb{F}[x]$ é separável.*

Drozd e V. V. Kirichenko [6], estabelecem condições para que um corpo de característica p, com p primo, seja perfeito e além disso eles nos garantem que todo corpo finito é perfeito.

Teorema 1.37. *Todo corpo de característica 0 é perfeito. Um corpo $\mathbb{F}$ de característica p é perfeito se e somente se a equação $x^p = \alpha$ tem uma solução em $\mathbb{F}$ para cada $\alpha \in \mathbb{F}$.*

Corolário 1.38. *Todo corpo finito é perfeito .*

Definição 1.39. *Uma álgebra A sobre um corpo K é* **separável** *se, em qualquer extensão L de K, a álgebra $A \otimes L$ é semissimples(a Jacobson).*

Citaremos um importante resultado, o Teorema de Wedderburn-Malcev, onde apresenta uma decomposição para uma álgebra de dimensão finita, o qual nos auxiliará posteriormente.

Teorema 1.40. (**Wedderburn-Malcev**) *Seja S uma álgebra de dimensão finita sobre um corpo $\mathbb{F}$, com radical de Jacobson J, tal que S/J seja separável, então existe uma subálgebra S_0, tal que $S = S_0 \oplus J$ (como soma direta de subespaços vetoriais), em que $S_0 \simeq S/J$*

Teorema 1.41. *Se um corpo $\mathbb{F}$ é perfeito, então toda $\mathbb{F}$-álgebra semissimples é separável.*

1.2.1 Automorfismo de Frobenius

Os teoremas de Sylow nos dizem que todo p-subgrupo A de um grupo G, de ordem p^m, está contido em um p-subgrupo de Sylow, B, de G, contudo, para análise dos automorfismos que geram o grupo geral linear, essa informação quanto ao grupo de ordem p^m não é suficiente; para tanto, recorreremos a um resultado, ver [7], referente a automorfismos de Frobenius que nos auxilirá na análise desses automorfismos.

Definição 1.42. *Seja $q = p^m$, onde p é primo e seja E o fecho algébrico de $\mathbb{F}_q$. Para $\alpha \in E$, o* **automorfismo de Frobenius**, *$\sigma_1 : E \to E$ é definido por:*

$$\sigma_1(\alpha) = \alpha^q.$$

Teorema 1.43. *O grupo $G = Aut(\mathbb{F}_{p^m})$ de automorfismos de $\mathbb{F}_{p^m}$ é cíclico de ordem m, gerado pelo elemento que corresponde ao automorfismo de Frobenius $\sigma_1(\alpha) = \alpha^{p^m}$. Ou seja, $Aut(\mathbb{F}_{p^m}) \simeq C_m$, onde C_m é o grupo cíclico, dado por $C_m = \langle \sigma_1(\alpha) \rangle$.*

1.3 Anéis de Grupo

Nesta seção, apresentaremos conceitos e discutiremos alguns resultados importantes da teoria de Anéis de Grupo.

Definição 1.44. *Sejam G um grupo e R um anel com unidade. Denotamos por RG o conjunto de todas as combinações lineares formais como a seguir*

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

em que $a_g \in R$ e $\{a_g\}_{g \in G}$ é uma sequência quase nula, ou seja, $a_g \neq 0$ para uma quantidade finita de índices. O conjunto $(RG, +, \cdot)$, dotado das operações de adição, multiplicação e multiplicação por escalar definidas da forma a seguir, é um anel chamado **anel de grupo** *de G sobre R:*

(i) soma de dois elementos:

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

(ii) produto de dois elementos:

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

(iii) produto de um elemento por um escalar do anel R:

$$\lambda \cdot \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} (\lambda a_g) g, \ \forall \lambda \in R.$$

Note que temos $1_{RG} = 1_R 1_G$, ou seja, RG é um anel com identidade que, denotaremos por 1.

Facilmente verificamos que RG é um R-módulo e, se R é comutativo segue que RG é uma álgebra sobre R.

Definição 1.45. *Dado $\alpha = \sum_{g \in G} a_g g \in RG$, definimos o* **suporte** *de α como $supp(\alpha) = \{g \in G : \alpha_g \neq 0\}$, isto é, o conjuto dos elementos $g \in G$ que aparecem na composição de α de forma não trivial, ou seja, $\alpha_g \neq 0$.*

1.3.1 O ideal de Aumento

Definição 1.46. *Seja a função $\varepsilon : RG \to R$ dada por*

$$\varepsilon \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g.$$

Esta função é um homomorfismo de anéis, chamado **homomorfismo de aumento** *de RG.*

Definimos $\mathcal{U}_1(RG) = \{\alpha \in \mathcal{U}(RG); \varepsilon(\alpha) = 1\}$, como sendo o **subgrupo das unidades de aumento** 1 em $\mathcal{U}(RG)$, ou então, o **subgrupo das unidades normalizadas de** RG.

Observação 1.47. *Seja $u \in \mathcal{U}(\mathbb{Z}G)$, então $\varepsilon(u) = \pm 1$. Portanto, podemos escrever*

$$\mathcal{U}(\mathbb{Z}G) = \pm \ \mathcal{U}_1(\mathbb{Z}G).$$

Definição 1.48. *O núcleo do homomorfismo de aumento ε é denotado por $\Delta(G)$ e o chamaremos de* **ideal de aumento** *de RG.*

Observe que, para um elemento $\sum_{g \in G} a_g g \in \Delta(G)$, temos que $\varepsilon \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g = 0$. Logo, podemos escrever α na forma:

$$\alpha = \sum_{g \in G} a_g g = \sum_{g \in G} a_g (g - 1).$$

Como os elementos da forma $g-1$, com $g \in G$, pertencem a $\Delta(G)$ e considerando a observação acima, temos o seguinte resultado:

Proposição 1.49. *O conjunto $\{g-1; g \in G, g \neq 1\}$ é uma base de $\Delta(G)$ sobre R.*

Devido a esta proposição $\Delta(G)$ pode ser descrito por:

$$\Delta(G) = \left\{ \sum_{g \in G} \alpha_g (g-1);\ g \neq 1, \alpha_g \in R \right\}.$$

Definição 1.50. *Seja H um subgrupo de G . O ideal à esquerda de RG, gerado pelo conjunto $\{h-1;\ h \in H\}$, é denotado por $\Delta(G,H)$ e pode ser explicitado da seguinte forma:*

$$\Delta(G,H) = \left\{ \sum_{h \in H} \alpha_h (h-1); \alpha_h \in RG \right\}.$$

Observe que, pela definição acima, o ideal $\Delta(G,G)$ coincide com $\Delta(G)$. Sendo assim, considerando N um subgrupo normal em G, o homomorfismo canônico $\overline{\psi}_N : G \to G/N$ pode ser estendido a um homomorfismo de anéis $\psi_N : RG \to R(G/N)$ dado por:

$$\psi_N \left(\sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} \alpha_g \overline{\psi}_N(g).$$

Por isso, segue o resultado abaixo que apresenta uma caracterização alternativa para $\Delta(G,N)$, que, neste caso, é um ideal bilateral.

Proposição 1.51. *Seja G um grupo e N subgrupo normal em G, $(N \trianglelefteq G)$ e ψ_N definido da forma acima, então $ker(\psi_N) = \Delta(G,N)$.*

Corolário 1.52. *Seja G um grupo e N subgrupo normal em G, $(N \trianglelefteq G)$. Então,*

$$\frac{RG}{\Delta(G,N)} \simeq R\left(\frac{G}{N}\right).$$

Observação 1.53. *Pelo que foi visto até aqui, $\Delta(G,N)$ define uma aplicação dos subgrupos normais em ideais bilaterais; agora construiremos uma aplicação na direção oposta. Seja I um ideal de RG, consideremos o seguinte conjunto:*

$$\nabla(I) = \{g \in G : g-1 \in I\},\ \textit{isto é}\ \nabla(I) = G \cap (1+I).$$

A relação entre as duas aplicações é dada por:

Proposição 1.54. *Se H é um subgrupo de G, então $\nabla(\Delta(G,H)) = H$.*

Observação 1.55. *Observemos que, embora tenhamos $\nabla(\Delta(G,H)) = H$, as aplicações Δ e ∇, não são uma inversa da outra. De fato, como I é um ideal em RG, é fácil ver que $\Delta(G,\nabla(I)) \subset I$ e, além disso, considerando $I = RG$, temos que $\nabla(RG) = G \cap (1+RG) = G$. Portanto $\Delta(G,\nabla(RG)) = \Delta(G) \neq RG$.*

Definição 1.56. *Um isomorfismo $\psi : \mathbb{Z}G \to \mathbb{Z}H$ é chamado* **Isomorfismo Normalizado** *se para todo elemento $\alpha \in \mathbb{Z}G$, temos que $\varepsilon(\alpha) = \varepsilon(\psi(\alpha))$ ou, de forma equivalente, se para todo elemento $g \in G$, temos $\varepsilon(\psi(g)) = 1$.*

Capítulo 2

A Estrutura do Grupo Adjunto

2.1 O Grupo Adjunto de um Anel

Nessa seção apresentaremos definições e alguns resultados referentes a grupos adjuntos que podem ser conferidos em [18]. Retomando a operação círculo, $\circ$, $x \circ y = x+y+xy$, para todo $x, y \in R$, definida no capítulo anterior; lembremos que esta operação é associativa, tem elemento neutro, neste caso o 0, então é fácil concluir que o conjunto dos elementos quaserregulares do anel R, ou seja, aqueles elementos que possuem inverso em relação a esta propriedade, forma um grupo com essa operação.

Definição 2.1. *O grupo formado por todos os elementos quaserregulares de R com a operação $\circ$ é chamado* **grupo adjunto**.

Definição 2.2. *Se todos os elementos do anel R forem quaserregulares, alguns autores denominam esse grupo como* **grupo círculo** *e o anel R é chamado* **anel radical**.

Podemos verificar facilmente que, se 1 é a unidade do anel R, então -1 não é quaserregular. Sendo assim, neste trabalho, caso o anel tenha unidade, admitiremos sempre que essa unidade é diferente de 0, ou seja $1 \neq 0$.

Se um anel R tem unidade e é não trivial, então existe uma conexão entre o grupo adjunto de R e o grupo de unidades como veremos no resultado a seguir:

Proposição 2.3. *Sejam R um anel com unidade, $\mathcal{U}(R)$ o grupo das unidades de R e G o grupo adjunto de R. Então $\mathcal{U}(R) = 1 + G$ e $\mathcal{U}(R) \cong G$.*

Demonstração. Dado $g \in G$ arbitrário, considere $h \in G$ o quase-inverso de g, ou seja $g \circ h = h \circ g = 0$. assim temos que,

$$(1+g)(1+h) = 1+g+h+gh = 1+(g+h+gh) = 1+(g \circ h) = 1.$$

Analogamente, podemos verificar que $(1+h)(1+g)=1$. Logo $1+g \in \mathcal{U}(R)$, donde $1+G \subseteq \mathcal{U}(R)$. Por outro lado, dado $u \in \mathcal{U}(R)$, considere v seu inverso, ou seja, $uv = vu = 1$. Temos que

$$(u-1)\circ(v-1) = (u-1)+(v-1)+(u-1)(v-1)$$

$$= u-1+v-1+uv-u-v+1 = 0$$

Por um raciocínio análogo, prova-se que $(v-1)\circ(u-1)=0$, logo $u-1 \in G$, ou seja $u \in 1+G$. Portanto $\mathcal{U}(R) = 1+G$.
Agora, consideremos a aplicação:

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & \mathcal{U}(R) \\ & g & \longmapsto & 1+g \end{array}$$

Com base nas informações acima, podemos concluir que φ é uma bijeção.
A aplicação φ é, de fato, um homomorfismo de grupos, pois dados $g, h \in G$, temos:

$$\varphi(g\circ h) = 1+(g\circ h) = 1+(g+h+gh) = 1+g+h+gh = (1+g)(1+h) = \varphi(g)\varphi(h).$$

Portanto, $\mathcal{U}(R) \cong G$, isto é, $\mathcal{U}(R)$ e G são isomorfos.

□

Em nosso trabalho, lidaremos apenas com anéis com unidade; contudo, não queremos, simplesmente, desprezar anéis que eventualmente não apresentem unidade. Ocorre, entretanto, que um anel sem unidade, felizmente, pode sempre ser extendido de forma bastante natural a um anel com unidade (Extensão de Dorroh), a saber:
Tomando o conjunto $R_1 = \mathbb{Z}_q \times R$, em que q, é a característica de R, dados (n,r), $(m,s) \in \mathbb{Z}_q \times R$, definimos as operações de anel como a seguir:

Dados (n,r), $(m,s) \in \mathbb{Z}_q \times R$

- A adição é definida por coordenadas:

$$(n,r)+(m,s) := (n+m, r+s).$$

- A multiplicação é definida por:

$$(n,r)(m,s) = (nm, rs+mr+ns),$$

em que mr e ns são simplesmente as somas iteradas de r e s, dadas pelos inteiros m e n.

- O par $(0,0)$ é o neutro aditivo.
- O par $(1,0)$ é o elemento neutro multiplicativo.

Confirmando o neutro:

$$(n,r)(1,0) = (n.1, r.0 + 1.r + n.0) = (n,r).$$

- O elemento inverso pode ser obtido por: $(n,r)(m,s) = (1,0) \Leftrightarrow nm = 1$ e $rs + mr + ns = 0$ e $(nm)(rs + mr + ns) = 0$, enquanto $(mr) \circ (ns) = mr + ns + (mr)(ns) = mr + ns + \underbrace{(nm)}_{=1}(rs) = rs + mr + ns = 0$.

Dessa forma, mr é quaserregular e $mr = n^{-1}r \in G$, onde G é o grupo adjunto de R.

- O par $(n,r) \in \mathbb{Z}_q \times R = R_1$ é invertível $\Leftrightarrow n \in \mathcal{U}(\mathbb{Z}_q)$ e $n^{-1}r \in G$

Lembremos que $\mathcal{U}(\mathbb{Z}_q)$ é um grupo abeliano e tem ordem $\varphi(q)$ em que φ é a função de Euler.

O resultado a seguir garante que podemos obter o grupo adjunto do anel R_1 em função de grupo adjunto do anel R e das unidades em $\mathbb{Z}_q$.

Teorema 2.4. *Seja G_1, o grupo adjunto do anel R_1, G, o grupo adjunto do anel R e $\mathcal{U}(\mathbb{Z}_q)$ o grupo de unidades de $\mathbb{Z}_q$, então $G_1 \cong \mathcal{U}(\mathbb{Z}_q) \times G$.*

Demonstração. Sabemos, da proposição 2, 3, que $G_1 \cong \mathcal{U}(R_1)$ e, pelo discutido acima, podemos considerar a aplicação:

$$\begin{array}{rccc} \varphi: & \mathcal{U}(R_1) & \longrightarrow & \mathcal{U}(\mathbb{Z}_q) \times G \\ & (n,r) & \longmapsto & (n, n^{-1}r) \end{array}$$

Verifiquemos que esta aplicação é um homomorfismo de grupos:

$$\begin{aligned} \varphi[(n,r)(l,t)] &= \varphi(nl, rt + nt + lr) \\ &= (nl, (nl)^{-1}(rt + nt + lr)) = (nl, n^{-1}r + l^{-1}t + n^{-1}rl^{-1}t) \\ &= (nl, n^{-1}r \circ l^{-1}t) = (n, n^{-1}r)(l, l^{-1}t) = \varphi(n,r)\varphi(l,t). \end{aligned}$$

Logo, $\varphi[(n,r)(l,t)] = \varphi(n,r)\varphi(l,t)$.

Agora verifiquemos que a aplicação é bijetiva:
Considere $\varphi(n,r) = (1,0)$, então $(n, n^{-1}r) = (1,0)$, donde $n = 1$ e $n^{-1}r = 0$, assim, $r = 0$, ou seja, $(n,r) = (1,0)$. Dessa forma, $\ker\varphi = \{(1,0)\}$, o que garante que φ é injetiva.
Agora, consideremos $(n,r) \in \mathcal{U}(\mathbb{Z}_q) \times G$, ou seja, $n \in \mathcal{U}(\mathbb{Z}_q)$ e $r = n^{-1}(nr) \in G$. Então,

existe $(n, nr) \in \mathcal{U}(R_1)$ tal que $\varphi(n, nr) = (n, n^{-1}nr) = (n, r)$. Portanto, dado, $(n, r) \in \mathcal{U}(\mathbb{Z}_q) \times G$, existe $(n, nr) \in \mathcal{U}(R_1)$ tal que $\varphi(n, nr) = (n, r)$, garantindo assim que a aplicação φ é sobrejetiva.
Diante disto, podemos concluir que $G_1 \cong \mathcal{U}(\mathbb{Z}_q) \times G$ e portanto $G \cong G_1/\mathcal{U}(\mathbb{Z}_q)$. □

2.2 O problema do Isomorfismo

Na teoria de Anéis de Grupo, a questão de como a estrutura do grupo base determina as características do anel de grupo associado e, por outro lado, quais propriedades do grupo base podem ser dicernidas a partir da investigação do anel de grupo associado, se coloca naturalmente. Neste sentido, uma questão central na teoria é: "dados dois grupos G e H e um anel R, será que a existência de um isomorfismo de anéis, entre RG e RH implica que G é isomorfo a H?"
Inúmeros foram os resultados a respeito desta questão; algumas investigações foram direcionadas a grupos abelianos, considerando a álgebra sobre o corpo dos complexos. E assim, obteve-se como resultado que um grupo abeliano finito não é determinado pelo seu anel de grupo sobre o corpo dos complexos.
Segundo C. Polcino Milies e S. K. Sehgal, [18], o mencionado problema foi sugerido pela primeira vez em 1940 por Higman, em sua tese de Doutorado, referindo-se a anéis de grupo integral, ou seja, quando $R = \mathbb{Z}$. Mais tarde, em 1947 T.M. Thrall, apud [18], reformulou o problema da seguinte forma:
"*Dado um grupo G e um corpo $\mathbb{F}$, determine todos os grupos H tais que $\mathbb{F}G \cong \mathbb{F}H$.*"
As questões sobre quais propriedades de um grupo finito G se refletem sobre o anel de grupo RG já foram estudadas, conforme relatam Polcino Milies e Sehgal, [18], por diversos matemáticos: S. Perlis e G. Walker em 1950, provaram que grupos abelianos finitos são determinados pelos seus anéis de grupo sobre o corpo dos números racionais e W. E. Deskins em 1956, apud [18], mostrou que p-grupos abelianos finitos são determinados por seus anéis de grupo sobre qualquer corpo de característica p. Neste sentido alguns resultados parciais relacionados a grupos finitos não abelianos foram obtidos por B. Coleman(1962) apud [2] e D. Passman [14]. Esses resultados sugeriam que para uma determinada família de grupos seria possível obter um corpo para o qual o problema do isomorfismo tivesse resposta positiva. Entretanto em 1972, E. Dade, apud [18], obteve um exemplo de dois grupos não isomorfos tais que suas álgebras de grupo sobre qualquer corpo eram isomorfas. A partir daí descartou-se a possibilidade de R ser um corpo e passou-se a considerar o problema do isomorfismo quando o anel de coeficientes fosse o anel dos inteiros $\mathbb{Z}$. Em sendo assim, a questão passou a ser enunciada da seguinte forma:

$$\text{(ISO)} \qquad ZG \cong ZH \Rightarrow G \cong H.$$

O resultado a seguir esclarece uma das razões pelas quais seria interessante considerar em particular o anel $\mathbb{Z}$ para a conjectura acima:

Lema 2.5. *Sejam G e H dois grupos tais que $\mathbb{Z}G \cong \mathbb{Z}H$. então, $RG \cong RH$ para qualquer anel comutativo R. (como R-álgebra)*

Foram diversos os exemplos de grupos que responderam positivamente ao Problema do Isomorfismo. Todavia em 2001, M. Hertweck, [9], apresentou um contra-exemplo para o (Iso), ou seja, construiu dois grupos finitos, particulares e não isomorfos de forma que seus anéis de grupo integrais são isomorfos. Essa descoberta é extremamente importante, pois o Problema do Isomorfismo perde o status de conjectura, porém não a sua relevância. E, a partir daí, muda-se o foco da pesquisa, não mais se busca a validade da mencionada conjectura e sim quais as características que um grupo deve apresentar para ser determinado pelo seu anel de grupo integral.

2.2.1 Os Resultados de Sandling

R. Sandling, em seu trabalho, [19], apresenta diversos resultados relacionados a grupo círculo e grupo de unidades de um anel, dentre estes, destacaremos aqui apenas aqueles voltados a verificar que os grupos adjuntos finitos, os grupos círculos finitos e os grupos gerais lineares são determinados por seus anéis de grupo integrais.
Para obtermos os resultados desejados, é necessário que apresentemos alguns conceitos básicos e resultados técnicos.
Seja G um grupo adjunto do anel R, definamos um homomorfismo de grupos aditivo $\theta : \mathbb{Z}G \to R$ por

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

ou seja, cada elemento $x \in G$ é levado no próprio $x \in R$. Agora, vamos mostrar que θ restrito ao ideal de aumento $\Delta(G)$ é um homomorfismo de anéis e, para tanto, devemos mostrar que essa restrição é um homomorfismo multiplicativo.

$$\theta((g-1)(h-1)) = \theta(g \circ h - g - h + 1) = g \circ h - g - h = gh + g + h - g - h = gh.$$

Lembremos que o elemento identidade de G (1_G) é o elemento nulo (0) de R, de modo que um elemento da forma $g - 1_G \in \mathbb{Z}G$ é levado em $g \in R$, pela aplicação θ.
Obviamente $\theta(\Delta(G))$ é um subanel de R. Os resultados, a seguir que caracterizam um grupo adjunto, podem ser conferidos em [18],

Teorema 2.6. *Um grupo G é o grupo adjunto de um anel se, e somente se, é o grupo adjunto de um anel quociente de $\Delta(G)$ de $\mathbb{Z}G$.*

Demonstração. A validade da condição suficiente é imediata. Para mostrarmos a validade da condição necessária vamos assumir que G é o o grupo adjunto de um certo anel R. Considerando $\theta : \Delta(G) \to R$, o homomorfismo de anéis construído acima, temos, pelo teorema do isomorfismo, que

$$\frac{\Delta(G)}{\ker(\theta)} \simeq \theta(\Delta(G)).$$

Note que $\theta(\Delta(G))$ é um subanel de R contendo G; assim G é o grupo adjunto de $\theta(\Delta(G))$. Logo, pelo isomorfismo acima, segue que G também é o grupo adjunto de $\dfrac{\Delta(G)}{\ker(\theta)}$. □

Analogamente também podemos caracterizar o grupo círculo:

Teorema 2.7. *Seja G um grupo finito, então G é um grupo círculo se, e somente se, existe um ideal J de $\mathbb{Z}G$, contido em $\Delta(G)$, tal que:*
(i) O índice do subgrupo aditivo J em $\Delta(G)$ é igual a $|G|$, e,
ii) $(1 + J) \cap G = 1$.
Neste caso,

$$G \simeq 1 + \frac{\Delta(G)}{J}.$$

O resultado a seguir, apresentado por Polcino Milies e Sehgal [18], nos garante que para um isomorfismo normalizado $\phi : \mathbb{Z}G \to \mathbb{Z}H$ também vale que $(1+\phi(J))\cap H = 1$:

Lema 2.8. *Sejam G e H grupos finitos e seja $\phi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Sendo J um ideal de $\mathbb{Z}G$ tal que $(1 + J) \cap G = 1$. Então $(1 + \phi(J)) \cap H = 1$.*

Exibiremos a seguir os resultados em que Sandling, [19], prova que grupos círculo finitos, grupos adjuntos e os grupos de unidades de anéis finitos são determinados pelo seus anéis de grupo integral.

Teorema 2.9. *Um grupo círculo finito é determinado pelo seu anel de grupo integral.*

Demonstração. Seja G um grupo círculo finito, então, pelo teorema 2.7, existe um ideal $J \subseteq \Delta(G)$, tal que $(1 + J) \cap G = 1$ e $G \simeq 1 + \dfrac{\Delta(G)}{J}$. Seja H um outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$ e seja $\phi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado, então $\phi(J)$ é um ideal de $\mathbb{Z}H$, contido em $\Delta(H)$, logo, pelo lema anterior, temos que $(1 + \phi(J)) \cap H = 1$.
Sendo $\phi(\Delta(G)) = \Delta(H)$, segue que $[\Delta(H) : \phi(J)] = [\Delta(G) : J] = |G| = |H|$, dessa forma o Teorema 2.7 garante que H é um grupo círculo e é isomorfo a $1 + \Delta(H)/\phi(J)$.
Portanto, temos que

$$G \simeq 1 + \frac{\Delta(G)}{J} \cong 1 + \frac{\Delta(H)}{\phi(J)} \simeq H.$$

□

Lema 2.10. *Sejam G o grupo adjunto do anel R e J um ideal de um anel de grupo integral $\mathbb{Z}G$ tal que $(1+J)\cap G = 1$. Então G é isomorfo a um subgrupo do grupo das unidades do anel quociente $\mathbb{Z}G/J$.*

Demonstração. Considere a aplicação $\phi : G \to 1 + (\Delta(G) + J)/J$, dada por

$$\phi(x) = 1 + (x-1) + J.$$

Essa aplicação é um homomorfismo de grupos. De fato, dados g e $h \in G$, temos:

$$\phi(g)\phi(h) = (1 + (g-1) + J)(1 + (h-1) + J)$$

$$= 1 + (gh - 1) + J = \phi(gh).$$

Essa aplicação é injetiva; considere $g \in G$ tal que $\phi(g) = 1 + J \Rightarrow 1 + (g-1) + J = 1 + J$, então $g - 1 \in J$, assim $g \in (1 + J) \cap G = 1$.
Portanto, G é isomorfo a $\phi(G)$, que é um subgrupo do grupo de unidades de $\mathbb{Z}G/J$. □

Dado $G = \mathcal{U}(R)$, o grupo de unidades de um anel R e, considerando $R^{'}$ o subanel de R gerado por G, definimos um homomorfismo $\theta : \mathbb{Z}G \to R^{'}$, considerando $J = \ker(\theta)$ e usando o lema anterior prova-se a validade de (ISO) para $\mathcal{U}(R)$.

Teorema 2.11. *O grupo das unidades de um anel finito é determinado por seu anel de grupo integral.*

Demonstração. Conforme citamos acima, seja $G = \mathcal{U}(R)$ o grupo de unidades de um anel R e tomando $R^{'}$ o subanel de R gerado por G., consideremos a aplicação:

$$\theta : \mathbb{Z}G \to R^{'}, \qquad \text{definida por:}$$

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

É sabido que as multiplicações de G e $R^{'}$ são as mesmas, assim segue que θ é um homomorfismo de anéis e então vale que $\theta(\mathbb{Z}G) = R^{'}$. Se denotamos $J = \ker(\theta)$; temos que $R^{'} = \theta(\mathbb{Z}G) \simeq \mathbb{Z}G/J$.
Agora considere um outro grupo H tal que $\mathbb{Z}G \simeq \mathbb{Z}H$ e seja $\phi : \mathbb{Z}G \simeq \mathbb{Z}H$ um homorfismo normalizado. Então $\mathbb{Z}G/J \simeq \mathbb{Z}H/\phi(J)$. Como $(1+J)\cap G = \{1\}$, temos, pelo teorema 2.7, que $(1+\phi(J))\cap H = \{1\}$. Daí, segue, pelo lema 2.9, que H é isomorfo a um subgrupo do grupo de unidades de $\mathbb{Z}H/\phi(J) \simeq \mathbb{Z}G/J \simeq R^{'}$. Como o grupo das unidades de $R^{'}$ é o próprio G, segue que H é isomorfo a um subgrupo de G e, desde que estes grupos têm a mesma ordem e são finitos, podemos concluir que $H \simeq G$. □

Sandling, estende este resultado para o grupo geral linear $GL(n, R)$, quando $n > 1$, através do seguinte resultado:

Corolário 2.12. *Seja R um anel finito com unidade e seja $n>1$. O grupo Geral Linear $GL(n,R)$ é caracterizado pelo seu anel de grupo integral.*

Demonstração. Sabemos que é finito o anel de matrizes $M(n,R)$, com R finito e, como $GL(n,R)$ é o grupo de unidades de $M(n,R)$, o resultado segue imediatamente pelo Teorema anterior. □

Também podemos estender esse resultado para o grupo adjunto de um anel finito mesmo que o anel não tenha unidade.

Teorema 2.13. *O grupo adjunto de um anel finito é determinado por seu anel de grupo integral.*

Demonstração. Seja G o grupo adjunto de um anel finito R.
Caso 1: Se R tem unidade, então, pela proposição 2.3 segue que G é isomorfo ao grupo de unidades de R e então pelo teorema anterior G é determinado pelo seu anel de grupo integral.
Caso 2: Se R não tem unidade, podemos mergulhar o anel R em um anel com unidade R_1 de modo que $R_1 = \mathbb{Z}_q \times R$, em que q é a característica do anel R e usaremos o Teorema 2.4 para concluirmos que $G_1 = G \times C_q$, ou seja, $G \simeq G_1/C_q$, onde G_1 é grupo adjunto de R_1 e $\mathcal{U}(\mathbb{Z}_q) = C_q$ é um grupo cíclico de ordem q.

Seja H um outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então,

$$\mathbb{Z}G_1 \simeq \mathbb{Z}[G \times C_q] \simeq \mathbb{Z}G \otimes_{\mathbb{Z}} \mathbb{Z}C_q \simeq \mathbb{Z}H \otimes_{\mathbb{Z}} \mathbb{Z}C_q \simeq \mathbb{Z}[H \times C_q]$$

daí segue que $\mathbb{Z}G_1 \simeq \mathbb{Z}[H \times C_q]$.

Como $G_1 \simeq (\mathcal{U}(R_1))$ que é o grupo de unidades de R_1, segue, pelo teorema anterior, que $G_1 \simeq H \times C_q$.
Logo, $H \simeq G_1/C_q$. Porém, por outro lado, pelo teorema 2.4, Assim, $G \simeq G_1/C_q \simeq H$.
Portanto, concluímos que $G \simeq H$. □

2.3 Uma Decomposição do Anel em p-anéis

Considerando R um anel finito com unidade, a estrutura $(R,+)$ forma um grupo abeliano, logo podemos escrevê-lo como soma direta de seus p_i subgrupos de Sylow:

$$(R,+) = R_{p_1} \oplus R_{p_2} \oplus \cdots \oplus R_{p_n},$$

em que $R_{p_1}, R_{p_2}, \cdots, R_{p_n}$ são p_i-subgrupos de Sylow.
Provaremos, a seguir, que cada um destes p_i-subgrupos é um ideal de R.

Lema 2.14. *Seja R_{p_i} um p_i-subgrupo de Sylow do grupo abeliano $(R,+)$, então R_{p_i} é um ideal de R.*

Demonstração. Sejam $x \in R_{p_i}$ e $y \in R_{p_j}$, com $o(x) = p_i^m$ e $o(y) = p_j^n$.
Se $i \neq j$, temos que $\underbrace{(xy + xy + \cdots + xy)}_{p_i^m \text{ vezes}} = (x + x + \cdots + x)\, y = 0$.
Por outro lado, $\underbrace{(xy + xy + \cdots + xy))}_{p_j^n \text{ vezes}} = x(y + y + \cdots + y) = 0$. Dessa forma, $o(xy)|p_i^m$ e $o(xy)|p_j^n$, porém p_i e p_j são relativamente primos, daí segue que $o(xy) = 1$, assim $xy = 0$.
Se tomarmos $i = j$ no desenvolvimento acima, podemos concluir que $o(xy)|p_i^m$ e $o(xy)|p_i^n$, então $xy \in R_{p_i}$. Dados $x \in R_{p_i}$ e $r \in R$, temos que $xr = x(r_1 + r_2 + \cdots + r_m) = xr_i \in R_{p_i}$. Analogamente, $rx = (r_1 + r_2 + \cdots + r_m)x = r_i x \in R_{p_i}$. Portanto R_{p_i} é um ideal de R. □

Lembrando que sendo R fechado pela operação círculo, esse é pelo menos um monóide, daí, veremos no resultado a seguir que, quando tomamos a interseção de cada R_{p_i} com o grupo adjunto G, de R, obtemos um subgrupo normal em G.

Lema 2.15. *Se G é o grupo adjunto de R e $G_{p_i} = G \cap R_{p_i}$, então $G_{p_i} \trianglelefteq G$.*

Demonstração. Provaremos que $G_{p_i} \leq G$ e, em seguida, que G_{p_i} é normal em G.

i) $G_{p_i} \neq \emptyset$
ii) Dados $x, y \in G_{p_i}$, temos que $x \circ y \in G$ e além disso, $x \circ y = \underbrace{x + y + xy}_{\in R_{p_i}}$, então $x \circ y \in R_{p_i}$
Portanto $x \circ y \in G_{p_i}$.
iii) Considere $x \in G_{p_i}$ e x' seu quase-inverso. Provar que $x' \in G_{p_i}$.
$0 = x \circ x' = x + x' + xx'$, ou seja, $x' = \underbrace{-x - xx'}_{\in R_{p_i}}$. Dessa forma $x' \in G_{p_i}$.
Portanto, podemos concluir que G_{p_i} é um subgrupo de G.
Agora provaremos que G_{p_i} é normal em G
Sejam $g \in G$, $x \in G_{p_i}$ e g' o quase-inverso de G, temos que $g' \circ x \circ g \in G$ e, além disso, $g' \circ x \circ g = g' + x + g'x + g + g'g + xg + g'xg = \underbrace{g' + g + g'g}_{=0} + x + g'x + g'xg$
Dessa forma $g' \circ x \circ g = x + g'x + g'xg \in R_{p_i}$, então segue que, $g' \circ x \circ g \in R_{p_i} \cap G = G_{p_i}$
Portanto o subgrupo G_{p_i} é normal em G. □

No grupo G_{p_i} definido acima todos os elementos são quaserregulares, logo, no resultado a seguir, verificaremos que este é o grupo adjunto do anel R_{p_i}:

Lema 2.16. *Seja G o grupo do anel R, e $G_{p_i} = G \cap R_{p_i}$, como no lema anterior, então G_{p_i} é o grupo adjunto de R_{p_i}.*

Demonstração. Seja $x \in R_{p_i}$ quaserregular, então existe $y \in R_{p_i}$, tal que $x \circ y = y \circ x = 0$. Dessa forma $x \in G$, e portanto $x \in G_{p_i}$. Logo G_{p_i} é o grupo adjunto de R_{p_i}. □

No resultado seguinte, considerando a decomposição da parte aditiva de R, $R = R_{p_1} \oplus R_{p_2} \oplus \cdots \oplus R_{p_n}$, podemos obter uma decomposição para cada grupo adjunto G, como produto direto dos G_{p_i}:

Proposição 2.17. *Seja R um anel finito com unidade, G o grupo adjunto de R e G_{p_i} o grupo adjunto de R_{p_i}, então podemos escrever G como o seguinte produto*

$$G = G_{p_1} \circ \cdots \circ G_{p_n}.$$

Demonstração. Considerando a decomposição $R = R_{p_1} \oplus R_{p_2} \oplus \cdots \oplus R_{p_n}$, podemos tomar $u \in U(R)$, com $u = r_1 + r_2 + \cdots + r_n$, onde $r_i \in R_{pi}$ e assim $\exists s \in R$, com $s = s_1 + s_2 + \cdots + s_n$ tal que $u \cdot s = 1$. Então, segue que, $1 = (r_1 + r_2 + \cdots + r_n) \cdot (s_1 + s_2 + \cdots + s_n) = r_1 s_1 + r_2 s_2 + \cdots + r_n s_n$, uma vez que $r_i s_j = 0$, para $i \neq j$.

Dessa forma, $1_1 + 1_2 + \cdots + 1_n = r_1 s_1 + r_2 s_2 + \cdots + r_n s_n$, em que cada 1_i é um idempotente primitivo de R_{p_i}.
Assim, devido a unicidade da decomposição, tem-se que $r_i \cdot s_i = 1_i$. Logo r_i é uma unidade em R_{p_i}, isto é, $r_i \in U(R_{p_i})$. Portanto, concluímos que $U(R) \simeq U(R_{p_i}) \times \cdots \times U(R_{p_i})$.
Como $U(R) \cong G$ e cada $G_{p_i} \cong U(R_{p_i})$, segue que G é descrito pelo seguinte produto direto

$$G \simeq G_{p_1} \circ \cdots \circ G_{p_n}.$$

□

Salientamos que o objetivo da operação adotada para descrever o produto direto acima foi simplesmente ressaltar a operação circulo ($\circ$).
Com base nesta proposição, vamos reduzir nosso trabalho a um anel do tipo p-anel, ou seja, $\forall r \in R \Rightarrow p^k r = 0$, para algum k.

2.4 A Estrutura do Grupo Adjunto para um p-anel

Nesta seção, coletamos uma série de resultados iniciais, extremamente técnicos, com o objetivo de obter a estrutura do grupo adjunto do anel R, uma vez que esse apresenta uma estrutura muito particular. O radical de Jacobson, $J(R)$, do anel R e o conjunto definido por $pR = \{pr, r \in R\}$, serão essenciais para obtermos esses resultados.

Estamos nos referindo a um p-anel, R, ou seja, p é um inteiro positivo tal que $\forall r \in R \Rightarrow p^k r = 0$, para algum k.

Lema 2.18. *Seja R um p-anel, então pR é ideal de R.*

Demonstração. Sendo R um anel com unidade, é claro que $pR \neq \emptyset$.
Seja $x \in pR$ e $r \in R \Rightarrow \exists y \in R$ tal que $x = p.y$, então $xr = p.yr = (py)r = rx \in p$.
Portanto, pR é ideal de R. □

Lema 2.19. *Sendo $J(R)$ o radical de Jacobson do anel R, então, $pR \subseteq J(R)$*

Demonstração. É sabido que $\forall r \in R \Rightarrow p^k r = 0$, para algum k, dessa forma, temos que $(pr)^k = p^k \cdot \underbrace{r^k}_{r_1} = 0$, para todo $pr \in pR$
Assim pr é nilpotente. Como pr é um elemento arbitrário de $pR \trianglelefteq R$, todo elemento de pR é nilpotente, então pR é um ideal nil, logo $pR \subseteq J(R)$. □

Lema 2.20. *Seja $J(R/pR)$ o radical de Jacobson do anel R/pR e $J(R)$ o radical de Jacobson do anel R, então $J(R/pR) = J(R)/pR$*

Demonstração. Tome $a + pR \in J(R)/pR$. Como $a \in J(R)$, $\exists\, a^{'}; a \circ a^{'} = 0$. Podemos escrever $(a^{'} + pR) \circ (a + pR) = (a^{'} + a + aa^{'}) + pR = 0 + pR$, daí segue que $a + pR$ é quaserregular em R/pR. E assim $J(R)/pR$ é um ideal quaserregular em R/pR, logo está contido em $J(R/pR)$.
Para a recíproca, consideremos $I^{'}$ um ideal quaserregular de R/pR, então existe um ideal I de R que contém pR tal que $I^{'} = I/pR$, pelo Teorema do Homomorfismo para anéis.
Se $a \in I \trianglelefteq R$, $a + pR \in I/pR$, que é quaserregular em R/pR, então existe o quase-inverso de $a + pR$, seja ele: $b + pR$, isto é $(a + pR) \circ (b + pR) = (a + b + ab) + pR = 0 + pR$, então $a + b + ab \in pR \subseteq J(R)$, que é um ideal quaserregular, então $a + b + ab$ é quaserregular em R. Assim, $\exists c \in R$ tal que $a + b + ab + c + (a + b + ab)c = 0$. Dessa forma, temos que $a + (b + c + bc) + a(b + c + bc) = 0$ e assim $a \circ (b + c + bc) = 0$. Então a é quaserregular em R. Como $a \in I$ é arbitrário, segue que I é quaserregular em R, então $I \subseteq J(R)$ e assim $I/pR \subseteq J(R)/pR$.
Dessa forma, todo ideal quaserregular de R/pR está em $J(R)/pR$. Em particular $J(R/pR)$, ou seja $J(R/pR) \subseteq J(R)/pR$.
Portanto, segue que $J(R/pR) = J(R)/pR$. □

Lema 2.21. *Seja $J(R)$ o radical de Jacobson do anel R, então $J(R)$ é um subgrupo normal de G, com relação à operação $\circ$.*

Demonstração. Provaremos que $J(R) \leq G$ e, em seguida que $J(R)$ é normal em G.
i) Lembrando que $J(R)$ é um ideal quaserregular em R, então temos que $J(R)$ é fechado para a operação "$\circ$", logo dados $a, b \in J(R)$, $a \circ b = a + b + ab \in J(R)$.
ii) Seja $a^{'}$ o quase-inverso de a em $J(R)$, daí segue que $0 = a \circ a^{'} = a + a^{'} + aa^{'}$ e assim $a^{'} = -a - aa^{'} \in J(R)$, como $J(R)$ é ideal em R, segue que $a^{'} \in J(R)$.
Logo $J(R) \leq G$.
Agora provaremos que $J(R)$ é normal em G.
Sejam $a \in J(R)$, $g \in G$ e $g^{'}$ o quase-inverso de g em G, então $g^{'} \circ a \circ g \in G$ e, além disso,
$g^{'} \circ a \circ g = g^{'} + a + g^{'}a + g + g^{'}g + ag + g^{'}ag = \underbrace{a}_{\in J(R)} + \underbrace{g^{'}a}_{\in J(R)} + \underbrace{ag}_{\in J(R} + \underbrace{g^{'}ag}_{\in J(R)} \in J(R)$
Assim $g^{'} \circ a \circ g \in J(R)$ e portanto $J(R)$ é um subgrupo normal em G. □

O teorema de Wedderburn-Malcev não se aplica a R pois, não temos a garantia de que R é uma álgebra finita sobre um corpo perfeito $\mathbb{F}$, entretanto podemos verificar que R/pR é uma $\mathbb{Z}_p$-álgebra, de fato, sendo R um p-anel, com unidade, podemos garantir que R contém uma cópia de $\mathbb{Z}_{p^m}$, para algum m, que é determinado pela característica de R, ou seja $\exists A \ \subseteq R$, tal que $A \cong \mathbb{Z}_{p^m}$. No entanto, para simplificar, diremos que $\mathbb{Z}_{p^m} \subseteq R$.
Como $\mathbb{Z}_{p^m} = \dfrac{\mathbb{Z}}{p^m\mathbb{Z}}$, segue que $\mathbb{Z}_{p^m}/p\mathbb{Z}_{p^m} = \dfrac{\mathbb{Z}/p^m\mathbb{Z}}{p\mathbb{Z}/p^m\mathbb{Z}} \cong \mathbb{Z}_p$. Se $\mathbb{Z}_{p^m} \subseteq R$, então, $p\mathbb{Z}_{p^m} \subseteq pR$. Daí temos que $\mathbb{Z}_p \cong \mathbb{Z}_{p^m}/p\mathbb{Z}_{p^m} \subseteq R/pR$, pois tanto $\mathbb{Z}_{p^m} \subset R$ quanto $p\mathbb{Z}_{p^m} \subset pR$.
Logo $\mathbb{Z}_p \subseteq R/pR$, ou melhor, existe um subanel $A^{'}$ de R/pR tal que $\mathbb{Z}_p \cong A^{'}$.
Portanto, existe uma cópia de $\mathbb{Z}_p$ em R/pR.
Agora, com base no teorema de Wedderburn-Malcev, podemos obter uma decomposição para R/pR:

Lema 2.22. *Seja R um anel e $J(R)$ o radical de Jacobson de R, então $\dfrac{R}{pR} = \dfrac{J(R)}{pR} \oplus \dfrac{\tilde{A}}{pR}$, onde $\tilde{A}$ é um subanel de R que contém pR.*

Demonstração. Como $\dfrac{R/pR}{J(R/pR)}$ é semissimples e R/pR contém uma cópia de $\mathbb{Z}_p$, então $\dfrac{R/pR}{J(R/pR)}$ é uma álgebra semissimples sobre $\mathbb{Z}_p$, que é um corpo perfeito, logo, pelo Teorema 1.40 $\dfrac{R/pR}{J(R/pR)}$) é uma álgebra semissimples separável, portanto, o teorema de Wedderburn-Malcev garante que existe uma subalgebra A, tal que $R/pR = J(R/pR) \oplus A$ (como soma direta de espaços vetoriais), e $A \cong \dfrac{R/pR}{J(R/pR)}$.
Uma vez que $J(R/pR) = J(R)/pR$, pelo Lema 2.20, temos que $A \cong \dfrac{R/pR}{J(R)/pR} \cong \dfrac{R}{J(R)}$, ou seja, $A \cong \dfrac{R}{J(R)}$ e $\dfrac{R}{pR} = J\left(\dfrac{R}{pR}\right) \oplus A$, com $A \subseteq R/pR$.

Pelo Teorema do Homomorfismo de anéis, podemos garantir que $\exists\, \tilde{A}$ subanel de R que contém pR tal que $\dfrac{\tilde{A}}{pR} \cong A$ e assim $\dfrac{R}{pR} = \dfrac{J(R)}{pR} \oplus \dfrac{\tilde{A}}{pR}$, com $\tilde{A}/pR \cong \dfrac{R/pR}{J(R)/pR} \cong R/J(R)$. □

Logo, podemos escrever $R = \tilde{A} + J(R)$, com $\tilde{A} \cap J(R) = pR$.
A fim de obtermos uma decomposição para o grupo adjunto G de R, vamos considerar o subconjunto B de G tal que $B = G \cap \tilde{A}$ e verificarmos que $B \leq G$.

Lema 2.23. *Defina $B = G \cap \tilde{A}$. Então B é um subgrupo de G com relação à operação $\circ$.*

Demonstração. Verificaremos que B satisfaz as propriedades de subgrupo.

i) $0 \in G$ e $0 \in \tilde{A}$, então $0 \in G \cap \tilde{A} = B \Rightarrow B \neq \emptyset$

ii) Dados $a, b \in B$, segue que $a, b \in G$ e $a, b \in \tilde{A}$, dessa forma, $a \circ b \in G$ e além disso $a \circ b = a + b + ab \in \tilde{A}$, pois $\tilde{A}$ é anel. Sendo assim $a \circ b \in G \cap \tilde{A} = B$.

iii) Seja $b \in B$ e b' o seu quase-inverso, é imediato que $b' \in G$, provaremos que $b' \in \tilde{A}$ e portanto $b' \in B$. Para esta propriedade, consideraremos dois casos distintos:
Caso 1: Se $b \in pR \trianglelefteq R$, segue que $0 = b \circ b' = b + b' + bb'$, então $b' = -b - bb' \in pR \subseteq \tilde{A}$, assim $b' \in \tilde{A}$. Logo $b' \in B$.
Caso 2: Se $b \notin pR$, segue que $b' \notin J(R)$. Pois, senão como $b = -b' - bb'$, segue que $b \in J(R) \cap \tilde{A}$, então $b \in pR$, logo uma contradição. No entanto, $b' = j + a$, onde $j \in J(R)$ e $a \in \tilde{A}$, então podemos garantir que $a \notin J(R)$ e assim $a \notin pR$.
Por outro lado, temos que $0 = b \circ b' = b \circ (j + a) = b + j + a + bj + ba = \underbrace{b + a + ba}_{\in \tilde{A}} + \underbrace{j + bj}_{\in J(R)}$. Dessa forma, segue que $\underbrace{b + a + ba}_{\in \tilde{A}} = \underbrace{-j(1 + b)}_{\in J(R)}$. Logo $b + a + ba \in pR$ e $-j(1 + b) \in pR$. Porém $(1 + b)(1 + b') = 1$ e pR é ideal de R. Então $j = -j(1 + b)[-(1 + b')] \in pR \subseteq \tilde{A}$, e assim $j \in \tilde{A}$, logo $b' \in \tilde{A}$, implicando em $b' \in B$.
Portanto , concluímos que $B \leq G$. □

A partir desse fato e, utilizando a decomposição obtida no Lema 2.22, obteremos uma decomposição para o grupo adjunto G de R.

Lema 2.24. *Seja G o grupo adjunto do anel R, então $G = J(R) + B$ e $B \cap J(R) = pR$.*

Demonstração. Tome $g \in G$ e o seu quase-inverso $g' \in G$ de forma que $g = h + a$ com $h \in J(R)$ e $a \in \tilde{A}$ e $g' = f + c$, com $f \in J(R)$ e $c \in \tilde{A}$. Assim temos que

$$0 = g \circ g' = (h + a) \circ (f + c) = h + a + f + c + hf + hc + af + ac,$$

dessa forma $\underbrace{a+c+ac}_{\in \tilde{A}} = \underbrace{-h-f-hf-hc-af}_{\in J(R)}$.
Logo $a+c+ac \in \tilde{A} \cap J(R) = pR \subseteq J(R)$, ou seja, $a+c+ac$ é quaserregular, então $\exists\ a^{'} \in R$ tal que $(a+c+ac) \circ a^{'} = 0 \ \Rightarrow\ a+c+ac+a^{'}+aa^{'}+ca^{'}+aca^{'} = 0$. Dessa forma, $a+(c+a^{'}+ca^{'})+a(c+a^{'}+ca^{'}) = 0$, ou seja $a \circ (c+a^{'}+ca^{'}) = 0$, e daí segue que a é quaserregular em R, então $a \in G$. Logo $a \in G \cap \tilde{A} = B$. Portanto podemos concluir que $g \in J(R)+B \ \Rightarrow\ G = J(R)+B$. Agora, suponha que $a \in B \cap J(R)$, então $a \in G \cap \tilde{A}$ e $a \in J(R)$, logo $a \in J(R) \cap \tilde{A} = pR$. Então $B \cap J(R) \subseteq pR$. Por outro lado, $pR \subseteq B \cap J(R)$, portanto, concluímos que $B \cap J(R) = pR$. □

Sendo $J(R)$ um subgrupo normal em G, $J(R) \trianglelefteq G$ somos induzidos a tentar obter a estrutura do grupo G como um produto de $J(R)$ por um outro subgrupo de G, digamos B. Porém não obteremos um produto semidireto, uma vez que obteremos $J(R) \cap B = pR$. No entanto, obteremos um produto semidireto quando tomamos o quociente por pR. Com base nisto provaremos o seguinte resultado:

Teorema 2.25. *Seja R um anel. Se G é o grupo adjunto de R, então podemos escrever*

$$G/pR = \left(\frac{J(R)}{pR}\right) \rtimes \left(\frac{B}{pR}\right),$$

onde $J(R)$ é o radical de Jacobson de R e B/pR é um subgrupo de G/pR isomorfo ao produto direto de grupos gerais lineares.

Demonstração. Inicialmente, provaremos que $J(R)+B = J(R) \circ B$, ou seja, a decomposição tanto pode ser feita com operação de adição quanto com a operação círculo. É imediato que $J(R) \circ B \leq G(R)$, uma vez que $J(R) \trianglelefteq G$, com a operação $\circ$ e $B \leq G$. E pelo Lema anterior, temos que $G(R) = J(R)+B$. Logo $J(R) \circ B \subseteq B+J$.
Por outro lado, se $B^{'}$ é o quase-inverso de b, temos $b+h = b+h+(b \circ b^{'})h = b+h+bh+b^{'}h+bb^{'}h = b+(h+b^{'}h)+b(h+b^{'}h)$. Então $b+h = \underbrace{b}_{\in B} \circ \underbrace{(h+b^{'}h)}_{\in J(R)} \in B \circ J(R)$, para quaisquer $b \in B$ e $h \in J(R)$. Logo, $B+J(R) \subseteq B \circ J(R)$.
Portanto, concluímos que $B+J = B \circ J$.
Dessa forma, segue que $G = B \circ J(R)$ e $B \cap J(R) = pR$, em que pR é subgrupo normal de G. Portanto, tomando o quociente por pR, temos o seguinte produto semidireto

$$G/pR = \left(\frac{J(R)}{pR}\right) \rtimes \left(\frac{B}{pR}\right).$$

□

Vamos agora verificar a estrutura de B/pR:

Lema 2.26. *$B/pR \cong GL(n_1, \mathbb{F}_{q_1}) \times GL(n_2, \mathbb{F}_{q_2}) \times \cdots \times GL(n_k, \mathbb{F}_{q_k})$, onde cada q_i é uma potência de p.*

Demonstração. Lembremos que $B = G \cap \tilde{A}$, daí segue que $B/pR = G/pR \cap \tilde{A}/pR$, onde $\tilde{A}/pR \cong R/J(R)$.
Tome $a \circ pR \in B/pR$, então $a \in G \cap \tilde{A}$, dessa forma, existe $a^{'}$ tal que $a \circ a^{'} = 0$ implicando que $a^{'} \in B$. Sendo $a \circ pR$ quaserregular em B/pR, segue que $a \circ pR = \{a + pr + apr \ / r \in R\} = a + pR$. Então $a \circ pR = a + pR$ em $\tilde{A}/pR$ e existe $a^{'} \circ pR = a^{'} + pR$ tal que $(a \circ pR) \circ (a^{'} \circ pR) = pR$. Portanto, podemos afirmar que um elemento de B/pR está univocamente associado a um elemento em $\tilde{A}/pR$ que é quaserregular. No grupo B/pR temos $(a \circ pR) + (a^{'} \circ pR) + (aa^{'} \circ pR) = pR$, enquanto no anel $\tilde{A}/pR$ temos que $(a + pR) \circ (a^{'} + pR) = pR$. Pelo Teorema de Wedderburn-Artin,

$$\frac{R}{J(R)} \cong M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_k}(D_k),$$

onde cada D_i é um anel de divisão. Ora, se o anel R/pR é finito assim também serão estes anéis de divisão; logo, serão corpos finitos, que denotaremos por $D_i = \mathbb{F}_{q_i}$, $q_i = p^{k_i}$ Dessa forma, $\tilde{A}/pR \cong \dfrac{R}{J(R)} = M_{n_1}(\mathbb{F}_{q_1}) \oplus M_{n_2}(\mathbb{F}_{q_2}) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_{q_k})$. Os elementos quaserregulares de $\tilde{A}/pR$ formam um grupo quaserregular em $R/J(R)$, que é B/pR e, sendo R um anel com unidade, segue que esse grupo é isomorfo a $\mathcal{U}(R/J(R))$. Assim temos que $B/pR \cong \mathcal{U}(R/J(R)) = \mathcal{U}(M_{n_1}(\mathbb{F}_{q_1}) \oplus M_{n_2}(\mathbb{F}_{q_2}) \oplus \cdots \oplus M_{n_k}(\mathbb{F}_{q_k}))$. Dessa forma, $B/pR \cong \mathcal{U}(M_{n_1}(\mathbb{F}_{q_1})) \times \mathcal{U}(M_{n_2}(\mathbb{F}_{q_2})) \times \cdots \times \mathcal{U}(M_{n_k}(\mathbb{F}_{q_k}))$, em que $\mathcal{U}(M_{n_i}(\mathbb{F}_{q_i}))$ é o grupo de unidades em $M_{n_1}(\mathbb{F}_{q_1})$, ou seja é o grupo geral linear $GL(n_1, \mathbb{F}_{q_1})$. Logo B/pR é isomorfo ao produto direto de grupos gerais lineares:

$$B/pR \cong GL(n_1, \mathbb{F}_{q_1}) \times GL(n_2, \mathbb{F}_{q_2}) \times \cdots \times GL(n_k, \mathbb{F}_{q_k}).$$

□

Portanto, podemos concluir que G/pR pode ser escrito como produto semidireto de J/pR por um produto direto de grupos lineares gerais.

Conseguimos um resultado bastante relevante, que é o produto semi-direto onde a base é um p-grupo, logo satisfaz (Nor), por um produto de grupos gerais lineares. Diante disso, procuramos investigar a validade de (Nor) para o grupo geral linear obtendo assim a validade de (Nor) também para o topo, desse produto semi-direto.

Capítulo 3

A Propriedade do Normalizador

Apresentaremos neste capítulo uma das questões centrais na teoria de Anéis de Grupo, mais especificamente, Anéis de Grupo Integrais, que é a Propriedade do Normalizador, conhecida como (Nor). Essa tem sido tema de diversos estudos na área de Anéis de Grupo e já foram obtidas muitas descobertas ao seu respeito.

Dado um grupo G e $H \leq G$, uma pergunta natural que surge é como se localiza o H dentro do grupo G, mais precisamente como se determina $\mathcal{N}_G(H)$, o normalizador de H em G. Considerando $\mathcal{U} := \mathcal{U}(\mathbb{Z}G)$, o grupo das unidades do anel de grupo integral, é fácil ver que G é subgrupo de $\mathcal{U}$. Dessa forma, podemos investigar o normalizador de G em $\mathcal{U}$. O centro de $\mathcal{U}$, $\zeta := \mathcal{Z}(\mathcal{U})$, também está contido em $\mathcal{N}_{\mathcal{U}}(G)$, logo $G \cdot \zeta \subseteq \mathcal{N}_{\mathcal{U}}(G)$. A propriedade do normalizador diz que estes determinam todo o normalizador, ou seja, o normalizador é o menor possível.

Essa propriedade é apresentada em Sehgal, [21] da seguinte forma:

$$\text{(Nor)} \qquad\qquad \mathcal{N}_{\mathcal{U}}(G) = G \cdot \zeta.$$

Diversos foram os estudos intencionados a verificar a validade desta questão para diversas classes de grupos. Apresentaremos aqui alguns dos principais resultados, referentes à Propriedade do Normalizador, que serão fundamentais para desenvolvimento do nosso trabalho.

Destacaremos abaixo uma versão apresentada por [21], para o Teorema Fundamental de Coleman:

Teorema 3.1. (Coleman, 1964) *Seja G um p-grupo finito contido em um grupo finito G tal que $u \in \mathcal{N}_{\mathcal{U}}(G)$. então existe $y \in G$ tal que $u^{-1}gu = y^{-1}gy$, para todo $g \in P$.*

Os autores S. Jackowski e Z. Marciniak [10], alcançaram um resultado, para anéis de grupo integrais, o que representou um grande desenvolvimento para pesquisa pois, revela que a propriedade é verdadeira para grupos que possuem um 2-subgrupo de

Sylow normal e portanto, segue a solução para (Nor) para grupos de ordem ímpar.
Dado $u \in \mathcal{N}_{\mathcal{U}}(G)$, denotamos por $\varphi_u : G \to G$ o automorfismo $\varphi_u(g) = u^{-1}gu$, e por $Aut_{\mathcal{U}}(G)$ o grupo dos automorfismos definidos desse modo. É imediato que $Inn(G) \subset Aut_{\mathcal{U}}(G)$, em que $Inn(G)$ consiste em automorfismos internos de G. Agora, (Nor) é válida se, e somente se, $\forall u \in \mathcal{N}_{\mathcal{U}}(G)$, temos que $u = g_0 \cdot z$, com $g_0 \in G$ e $z \in \zeta$. Logo, $u^{-1}gu = \varphi_u(g) = z^{-1}g_0^{-1}gg_0z = g_0^{-1}gg_0$, isto equivale a afirmar que φ_u é um automorfismo interno de G, ou seja, $Aut_{\mathcal{U}}(G) \subset Inn(G)$.
Portanto, a propriedade do normalizador para um grupo finito G foi apresentada, segundo Jackowski e Marciniak, [10] da seguinte forma:

$$\text{(Nor)} \qquad Aut_{\mathcal{U}}(G) = Inn(G)?,$$

Utilizando a forma acima apresentada para (Nor), citamos um importante resultado de Jackowski e Marciniak [10], que garante a validade de (Nor) para os grupos que possuem ordem ímpar, ver [21]:

Teorema 3.2. *Se G é um grupo de ordem ímpar, então $Aut_{\mathcal{U}}(G) = Inn(G)$.*

A partir desse resultado, passou-se a investigar a validade de (Nor) apenas para grupos que possuem ordem par.
Os autores supracitados, apresentaram mais outra forma de verificar a validade de (Nor) para um determinado grupo G, analisando um conjunto de automorfismos φ_u em $Aut_{\mathcal{U}}(G)$ a partir de um 2-subgrupo de Sylow S, fixo em G.
Para isto definiram o subconjunto I_S das involuções de ordem 2 em $Aut_{\mathcal{U}}(G)$ que mantêm S fixo:

$$I_S := \left\{\varphi_u \in Aut_{\mathcal{U}}(G) : \varphi_u^2 = id, \varphi_u|_S = id\right\},$$

A partir deste conjunto, Jackowski e Marciniak [10] obtiveram um importante resultado que garante a validade de (Nor) sempre que $I_S \subseteq Inn(G)$:

Teorema 3.3. *Se I_S está contido em $Inn(G)$ para um 2-subgrupo de Sylow $S \subseteq G$, então $Aut_{\mathcal{U}}(G) = Inn(G)$.*

Outro resultado que merece destaque é o teorema a seguir, de Jackowski e Marciniak [10], que garante a validade de (Nor) para um grupo G que possui um 2-subgrupo de Sylow normal:

Teorema 3.4. *Se G é um grupo finito que possui um 2-subgrupo de Sylow normal, então vale a propriedade do normalizador para G.*

Apresentaremos a seguir um resultado bastante interessante que pode ser visto como uma versão restrita da propriedade do normalizador, obtido por Petit Lobão, T. e Sehgal, S. K, [16].

Lema 3.5. *Se $u \in \mathcal{N}_{\mathcal{U}}(G)$, então $\varphi_u(g) = u^{-1}gu$ é um conjugado a g, para qualquer $g \in G$, isto é, existe $h \in G$ tal que $u^{-1}gu = h^{-1}gh$, com h fixo, mas dependendo do g.*

Este resultado pode ser considerado uma versão restrita (ou pontual) de (Nor), pois, $\varphi_u(g) \sim_G g$ significa que $\forall\, g \in G, \exists\, x \in G$, x depende de g, tal que $\varphi_u(g) = u^{-1}gu = x^{-1}gx$.
Enquanto o teorema 3.1, corresponde a uma versão local, já que temos $Aut_{\mathcal{U}}(G) \subset Inn(G)$ para p-subgrupos do grupo G.
Sabemos que grupos nilpotentes podem ser escritos como produto de seus subgrupos de Sylow, então, a partir do resultado acima segue que:

Corolário 3.6. *Seja G um grupo nilpotente finito, então vale (Nor) para G, isto é, $\mathcal{N}_{\mathcal{U}}(G) = G \cdot \mathcal{Z}$.*

No capítulo anterior, escrevemos o grupo adjunto G como produto direto de seus subgrupos normais, G_{p_i}, então a proposição a seguir, que pode ser conferida em [12], nos possibilita trabalhar com estes subgrupos, uma vez que, verificada a validade de (Nor) para estes, podemos estender para todo G.

Proposição 3.7. *Seja G o produto direto dos grupos G_1 e G_2, $G = G_1 \times G_2$. Então a propriedade do normalizador vale para G se, e somente se, ela vale para G_1 e G_2.*

Demonstração. Denote por $\varphi_i : G \to G_i$ a projeção natural de G em G_i. Destacamos que a extensão de φ_i aos anéis de grupo também será indicada por φ_i. Para $i \neq j$, observe que $G_i = Ker(\varphi_j)$. Suponha que (Nor) vale para G e seja $u \in \mathcal{N}_{\mathcal{U}(\mathbb{Z}G_i)}(G_i)$ uma unidade no normalizador de G_i. Então $u \in \mathcal{N}_{\mathcal{U}}(G)$ e consequentemente $u = wg$, com $g \in G$, $w \in \zeta(\mathcal{U}(\mathbb{Z}G))$. Logo, temos que $u = \varphi_i(u) = \varphi_i(w)\varphi_i(g)$ e então, vale a propriedade do normalizador para G_i.
Agora, verificaremos que a condição é também suficiente. Suponha que a propriedade do normalizador vale para os grupos G_1 e G_2, e seja $u \in \mathcal{N}_{\mathcal{U}}(G)$ uma unidade no normalizador de G. Sendo $u_i = \varphi_i(u)$, temos que $u_i \in \mathcal{N}(G_i)$ e assim $u_i = w_i g_i$, onde w_i é uma unidade central em $\mathbb{Z}G_i$ e $g_i \in G_i$. Como G é o produto direto de G_1 e G_2, temos que w_i é também uma unidade central em $\mathbb{Z}G$. Definindo $w = uu_1^{-1}u_2^{-1}$, verificaremos que w é central em $\mathbb{Z}G$. Observe que $w = uw_1^{-1}w_2^{-1}g_1^{-1}g_2^{-1}$ está no no normalizador de G, e $\varphi_i(w) = \pm 1$. Logo, segue que, para todo $g \in G$, $[w, g] = g_0$ para algum $g_0 \in G$. Quando aplicamos φ_i em ambos os lados da expressão acima, obtemos $\varphi_i(g_0) = \varphi_i(w^{-1})\varphi_i(g^{-1})\varphi_i(w)\varphi_i(g) = 1$. Assim $g_0 = 1$ e portanto w é uma unidade central de $\mathbb{Z}G$. Temos então que $u = u_2u_1w = g_2g_1w - 2w_1w_2 \in G \cdot \zeta$, e portanto vale a propriedade do normalizador para G.

□

Lembremos que a estrutura do Grupo adjunto, G/pR foi obtida como produto semidireto onde a base é nilpotente, logo vale (Nor) e o topo é um produto direto de

grupos gerais lineares. No capítulo seguinte, provaremos a validade de (Nor) para cada um dos grupos gerais lineares e utilizaremos o resultado anterior, para concluir que a propriedade é válida também para o topo desse produto semidireto.

Capítulo 4

A Propriedade do Normalizador para o Grupo Geral Linear

Neste capítulo, provaremos que vale a propriedade do normalizador para o grupo geral linear $GL(n, \mathbb{F}_q)$, definido sobre o corpo $\mathbb{F}_q$, em que $q = p^m$, com p primo.
Introduziremos alguns conceitos e resultados referentes ao grupo geral inear que serão fundamentais para concluirmos a prova.

4.0.1 O Grupo Geral Linear - Estrutura Básica

Seja $\mathbb{F}_q$ um corpo finito e seja $n \in \mathbb{N}$. Denotamos por $\mathcal{M}_n(\mathbb{F}_q)$ o conjunto de todas as matrizes quadradas de ordem $n \times n$ com entrada no corpo $\mathbb{F}_q$, escrevemos tal matriz como $M = (m_{ij})$, onde $m_{ij} \in \mathbb{F}_q$.
Definimos o *grupo geral linear* $GL(n, \mathbb{F}_q)$ como o subconjunto de $\mathcal{M}_n(\mathbb{F}_q)$ consistindo de todas as matrizes quadradas invertíveis, de ordem $n \times n$, ou seja, matrizes que têm determinante não-nulo. $GL(n, \mathbb{F}_q)$ forma um grupo com a multiplicação usual de matrizes, cujo elemento identidade é dado por I_n.
A seguir exibiremos alguns conceitos e resultados encontrados em J. P. Alperin; R. B. Bell, [1] e S. K. Sehgal em [21] que descrevem a ordem do grupo $GL(n, \mathbb{F})$ e os geradores desse grupo.

Definição 4.1. *O grupo especial linear $SL(n, \mathbb{F})$ é o subgrupo de $GL(n, \mathbb{F})$ formado pelas matrizes cujo determinante é* 1.

Proposição 4.2. *Seja $n \in \mathbb{N}$ e seja q uma potência prima. Então*

$$|GL(n, \mathbb{F}_q)| = \Pi_{k=1}^{n}(q^n - q^{k-1}) = q^{\frac{n(n-1)}{2}}(q^n - 1) \cdot \ldots \cdot (q - 1).$$

Definição 4.3. *Seja $X_{ij}(\alpha) = I_n + \alpha E_{ij}$, com $\alpha \in \mathbb{F}_q^*$, em que E_{ij}, com $i \neq j$ é a matriz da base canônica do espaço de matrizes. Também poderíamos definir a matriz $X_{ij}(\alpha)$, como sendo a matriz cuja (k, l)-entrada é igual a α se $(k, l) = (i, j)$ e igual a δ_{kl} para*

todas as demais entradas (k, l).

Por exemplo, a matriz $X_{12}(\alpha) = \begin{bmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Definimos transvecções como sendo os conjugados de $X_{ij}(\alpha)$*, no grupo* $GL(n, \mathbb{F}_q)$*, isto é,* $N^{-1}X_{ij}(\alpha)N$*, onde* $N \in GL(n, \mathbb{F}_q)$.

Teorema 4.4. *O grupo* $G = GL(n, \mathbb{F}_q)$ *é gerado pelo conjunto de todas as transvecções e todas as matrizes diagonais invertíveis.*

Teorema 4.5. *Sejam* $GL(n, \mathbb{F}_q)$ *o grupo geral linear sobre o corpo finito* $\mathbb{F}_q$ *com* $q = p^m$*, p primo, e* $SL(n, \mathbb{F}_q)$ *o grupo especial linear, então, valem as seguintes afirmações:*

(i) $GL(n, \mathbb{F}_q) = SL(n, \mathbb{F}_q) \times {\mathbb{F}_q}^*$*;*

(ii) $SL(n, \mathbb{F}_q)$ *é gerado pelas transvecções.*

Observação 4.6. *Se q é uma pptência de p, um p-subgrupo de Sylow de* $GL(n, \mathbb{F}_q)$ *é dado pelas matrizes unitriangulares superiores, denotada por* T_S*:*

$$T_S = \begin{bmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & 1 & a_{23} & \cdots & a_{2n} \\ 0 & 0 & 1 & \cdots & a_{3n} \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Ou seja, $a_{ij} = 0$*, se* $j > i$*,* $a_{ij} = 1$*, se* $j = i$ *e* $a_{ij} \in \mathbb{F}_q$ *são quaisquer se* $i > j$.
O p-subgrupo de Sylow determinado, analogamente, pelas matrizes uinitriangulares inferiores é denotado por T_I.

4.0.2 Automorfismos do Grupo Geral Linear

As primeiras discussões sobre os automorfismos do grupo geral linear sobre um corpo comutativo devem-se a O. Schreier e van der Waerden, apud[3] em seguida esses resultados foram estendidos para corpos não comutativos por J. Dieudonnné. Tomando como base o trabalho de Dieudonné, P. M. Cohn, 1969, em [3], apresenta os quatro tipos de geradores do grupo de automorfismos de $GL(n, \mathbb{F}_q)$:

Lema 4.7. *Se* $G = GL(n, \mathbb{F}_q)$ *é o grupo geral linear sobre o corpo finito* $\mathbb{F}_q$ *com* $q = p^m$*, p primo, então* $Aut(G)$ *é gerado pelos seguintes automorfismos:*

1. *Automorfismos internos:* $\varphi_1(M) = N^{-1}MN$*, onde N é uma matriz invertível, compondo o subgrupo normal* $Inn(G) = \Phi_1 \trianglelefteq Aut(G)$

2. *Automorfismos induzidos por automorfismos do corpo $\mathbb{F}_q$.*
   Se $\lambda : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, é um automorfismo de $\mathbb{F}_q$ e $M = [a_{ij}]$ é um elemento genérico de G, λ induz o automorfismo de G, dado por $\varphi_2(M) = [\lambda(a_{ij})]$; estes automorfismos determinam o subgrupo $\Phi_2 \leq Aut(G)$.

3. *Automorfismos radiais ou homotetias, também conhecidos como automorfismos centrais:*
   Dado o homomorfismo de grupos $\chi : G \longrightarrow \mathcal{Z}(G) \simeq \mathbb{F}_q^* \simeq C_{q-1}$, define-se $\varphi_3(M) = \chi(M)M$, tal que $\chi(\alpha I) = \alpha^{-1} \Leftrightarrow \alpha = 1$. Esses forma o subgrupo $\Phi_3 \leq Aut(G)$.

4. *Automorfismo contragradiente φ_4, dado por $\varphi_4(M) = (M^{-1})^t = (M^t)^{-1}$; este automorfismo, obviamente, tem ordem 2.*

Vale notar que a expressão φ_i é utilizada para indicar apenas o "tipo"de automorfismo, enquanto Φ_i, indica o conjunto desses automorfismos.
A seguir, alguns fatos importantes referentes a estes automorfismos:

Fato 4.8. *Automorfismos em Φ_2 comutam com o automorfismo φ_4.*
Estendendo o automorfismo, $\lambda : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, ao grupo $GL(n, \mathbb{F}_q)$, como no item 2 do lema anterior, como $MM^{-1} = I_n$, então $\lambda(MM^{-1}) = \lambda(I) = I_n$. Dessa forma, $\lambda(M)\lambda(M^{-1}) = I_n$, garantindo que $\lambda(M^{-1}) = \lambda(M)^{-1}$.

Com base nisto, podemos garantir que

$$\varphi_4(\varphi_2(M)) = \varphi_4(\lambda(M)) = (\lambda(M)^t)^{-1} = [\lambda(M^t)^{-1}] = \lambda(\varphi_4(M)) = \varphi_2(\varphi_4(M)).$$

$$\varphi_2 \circ \varphi_4(M) = \varphi_4 \circ \varphi_2(M).$$

Logo, concluímos que os automorfismos dos tipos 2 comutam com φ_4.

Fato 4.9. *Automorfismos em Φ_3 geram um subgrupo normal em $Aut(G)$: $\Phi_3 \trianglelefteq Aut(G)$.*
Para $\varphi_3(M) = \chi(M)M$, onde $\chi(M) \in \mathbb{F}_q{}^*$, temos $\varphi_3(M)M^{-1} = \chi(M)I_n$, que é uma matriz escalar, logo temos que $\varphi_3(M)M^{-1}$ é central. Agora, consideremos um automorfismo qualquer em $GL(n, \mathbb{F}_q)$, a saber, ψ e definamos uma nova aplicação por $\psi' = \psi \circ \varphi_3 \circ \psi^{-1}$ e daí, segue que,

$$\psi'(N) = \psi(\varphi_3(\psi^{-1}(N))) = \psi(\varphi_3(\psi^{-1}(N)))N^{-1}N = \psi(\varphi_3(\psi^{-1}(N)))\psi(\psi^{-1}(N^{-1}))N =$$

$$= \psi(\varphi_3(\psi^{-1}(N))(\psi^{-1}(N))^{-1})N.$$

Como $\varphi_3(\psi^{-1}(N)))(\psi^{-1}(N))^{-1}$ é uma matriz escalar, logo central, segue que

$$\chi'(N) = \psi(\varphi_3(\psi^{-1}(N))(\psi^{-1}(N))^{-1}), \text{ também o será.}$$

Verificaremos que χ' é um homomorfismo de grupos:

$$\chi'(N_1N_2) = \psi(\varphi_3(\psi^{-1}(N_1N_2))(\psi^{-1}(N_1N_2))^{-1}) =$$

$$= \psi(\varphi_3(\psi^{-1}(N_1)\psi^{-1}(N_2))(\psi^{-1}(N_1)\psi^{-1}(N_2))^{-1}) =$$

$$= \psi(\varphi_3(\psi^{-1}(N_1))\underbrace{\varphi_3(\psi^{-1}(N_2))(\psi^{-1}(N_2))^{-1}}_{\text{é central}}(\psi^{-1}(N_1))^{-1})$$

$$= \psi(\varphi_3(\psi^{-1}(N_1)))\psi(\psi^{-1}(N_1))^{-1}\psi(\varphi_3(\psi^{-1}(N_2))(\psi^{-1}(N_2))^{-1})$$

$$= \psi(\varphi_3(\psi^{-1}(N_1))(\psi^{-1}(N_1))^{-1})\psi(\varphi_3(\psi^{-1}(N_2))(\psi^{-1}(N_2))^{-1}) = \chi'(N_1)\chi'(N_2).$$

Dessa forma, concluímos que $\psi'(N) = \chi'(N)N$ em que $\chi'(N)$ é uma matriz escalar. Definimos χ'' tal que $\chi'' \in {\mathbb{F}_q}^*$ e $\chi''.I_n = \chi'$. A aplicação $\chi'' : GL(n, \mathbb{F}_q) \longrightarrow \mathbb{F}_q^*$ é tal que $\chi''(N) = k$, com $k \in \mathbb{F}_q^*$. Logo $\psi'(N) = \chi'(N)N = \chi''(N)I_nN = \chi''(N)N$ é uma homotetia, ou seja, é um automorfismo do tipo 3.
Portanto, os automorfismos do tipo 3 geram um subgrupo normal, bem como os automorfismos do tipo 1 também geram um subgrupo normal.

O fato de que φ_2 e φ_4 comutam e o fato de que φ_1 e φ_3 geram subgrupos normais, nos levam a conclusão que para qualquer $\varphi \in Aut(G)$, φ é decomposto da seguinte forma: $\varphi_1 \circ \varphi_2 \circ \varphi_3$ ou $\varphi_1 \circ \varphi_2 \circ \varphi_3 \circ \varphi_4$, com $\varphi_i \in \Phi_i, i \in \{1, 2, 3\}$, em que φ_i pode ser a identidade; esta ordem de decomposição pode ser qualquer.
Ainda podemos observar que automorfismos de Φ_1 comutam com os de Φ_3.

Fato 4.10. *Automorfismos em Φ_3 preservam conjugações, isto é, $\varphi_3(N^{-1}AN) = N^{-1}\varphi_3(A)N$, donde $\chi(N^{-1}AN) = \chi(A)$.*
De fato, $\varphi_3(N^{-1}AN) = \varphi_3(N^{-1})\varphi_3(A)\varphi_3(N) = \varphi_3(N)^{-1}\varphi_3(A)\varphi_3(N) = N^{-1}\chi(N)^{-1}\varphi_3(A)\chi(N)N$, em que $\chi(N) \in \mathcal{Z}(G)$. Logo $\varphi_3(N^{-1}AN) = N^{-1}\varphi_3(A)N$.

Apresentaremos a seguir um Lema que nos auxiliará na análise dos automorfismos do tipo 2:

Lema 4.11. *Seja $\lambda : \mathbb{F}_q \to \mathbb{F}_q$ dado por $\lambda(a) = a^{-1}$, para todo $a \neq 0$. Então λ é um automorfismo se e somente se $q = 2$, ou $q = 3$ ou $q = 4$.*

Demonstração. É evidente que $\mathbb{F}_2 = \{0, 1\}$; $\lambda : \mathbb{F}_2 \to \mathbb{F}_2$, leva $0 \mapsto 0$, $1 \mapsto 1$ em que $1^{-1} = 1$.
Para $\mathbb{F}_3 = \{0, 1, -1\}$. $\lambda : \mathbb{F}_3 \to \mathbb{F}_3$, leva $0 \mapsto 0$, $1 \mapsto 1$ e $-1 \mapsto -1$, em que $1^{-1} = 1e{-}1^{-1} = -1$. Enquanto, $\mathbb{F}_4 = \{0, 1, a, 1 + a\}$, sendo a o gerador de ${\mathbb{F}_4}^*$ é tal que: $a.a = 1 + a$. $(1 + a)(1 + a) = 1 + a + a + a.a = (1 + a) + a + (1 + a) = 2 + (a + a) + a = a$, pois $Char(\mathbb{F}_4) = 2$. $a.(1 + a) = a + a^2 = a + (1 + a) = \underbrace{a + a}_{=0} + 1 = 1$.
Portanto, $\lambda : \mathbb{F}_4 \to \mathbb{F}_4$, leva $0 \mapsto 0$, $1 \mapsto 1$, $a \mapsto 1 + a$ e $1 + a \mapsto a$, em que $a^{-1} = 1 + a$ e

$(1+a)^{-1} = a$.
Dito isto, seja $\lambda(a) = a^{-1}$, $\forall a \neq 0$.
Se $\lambda = {\sigma_1}^k$, para $1 \leq k \leq m$, então ${\sigma_1}^k(a) = a^{p^k} = A^{-1}$ donde $a^{p^k+1} = 1$, $\forall a \neq 0$.
Lembremos do Automorfismo de Frobenius, visto no Teorema 1.43, temos que, ${\mathbb{F}_q}^* \simeq C_{p^m-1}$, então $\forall a \neq 0$, segue que $a^{p^m-1} = 1$, em que $q = p^m$.
Sendo assim, se a é gerador de ${\mathbb{F}_q}^*$, essa é a menor potência tal que $a^{p^m-1} = 1$, logo $p^m - 1 | p^k + 1$, para algum k.
Conclusão:

1. Se $k < m$, como $(p^m - 1)|(p^k + 1)$, então $p^m - 1 \leq p^k + 1$.
   Logo $p^m - p^k \leq 2$. Assim $p = 2$. Consideremos $k + r = m$, $r > 0$. Como $2^m - 2^k \leq 2$, segue que
   $$2^{k+r} - 2^k \leq 2 \Rightarrow 2^k.2^r - 2^k \leq 2 \Rightarrow 2^k(2^r - 1) \leq 2.$$
   Nessas condições, temos que $k = 1$ e $r = 1$. Logo $p = 2$ e $m = 2$. Portanto, $\mathbb{F}_q$ é tal que $\mathbb{F}_q = \mathbb{F}_{p^m} = \mathbb{F}_4$.

2. Se k = m, temos que $(p^m - 1)|(p^m + 1)$, donde $p^m - 1 = 1$ ou $p^m - 1 = 2$. Dessa forma, $p^m = 2$ ou $p^m = 3$.
   Nessas condições, temos que $m = 1 = k$ e $p = 2$ ou $p = 3$.
   Portanto, exceto para $\mathbb{F}_2$, $\mathbb{F}_3$ e $\mathbb{F}_4$, o automorfismo $\lambda : a \mapsto a^{-1}$ não existe.

□

4.0.3 A validade de (Nor) para o Grupo Geral Linear

Teorema 4.12. *Se $G = GL(n, \mathbb{F}_q)$ é o grupo geral linear sobre o corpo finito $\mathbb{F}_q$, com $q = p^m$, em que p é primo, então vale a Propriedade do Normalizador (Nor) para G.*

Demonstração. Se $n = 1$, segue que $GL(n, \mathbb{F}_q) = {\mathbb{F}_q}^*$, que é cíclico, logo abeliano, então vale (Nor) em $GL(1, \mathbb{F}_q)$. Para $n \geq 2$, pela proposição 4.2, a ordem de $GL(n, \mathbb{F}_q)$ é par, logo não se encaixa no Teorema 3.2 e $GL(n, \mathbb{F}_q)$ consiste em matrizes de ordem maior ou igual a $n \times n$.
O argumento para esta prova baseia-se fortemente na estrutura do $Aut(G)$ (Lema 4.7), no resultado de Coleman para p-grupos, (teorema 3.1), apud [21], nos resultados de Jackowski e Marciniak [10] (teoremas 3.2, 3.4 e 3.5) e no resultado de Petit Lobão e Sehgal [16] (Lema 3.6).
Dividiremos nossa prova em dois casos:
Iniciaremos considerando matrizes de ordem $n > 2$ e em seguida provaremos (Nor) para matrizes de ordem $n = 2$.

- **Caso n>2**

Mostraremos que todos os automorfismos de $GL(n,\mathbb{F}_q)$, provenientes de uma unidade normalizada são internos, ou seja $Aut_{\mathcal{U}}(G) = Inn(G)$. Para isso, utilizaremos a técnica de Jackowski e Marciniak, [10], supondo que esses automorfismos estão em $I_S \subseteq Aut_{\mathcal{U}}(G)$. Ademais, todo raciocínio será desenvolvido sobre os geradores de $GL(n,\mathbb{F}_q)$, que são as transvecções e as matrizes diagonais invertíveis.
Consideremos a matriz $X_{ij}(\alpha) = I + \alpha E_{ij}$, apresentada na Definição 4.3. Como $X_{ij}(\alpha) \in T_S$, para $j > i$, este elemento tem ordem igual a uma potência de p, $|X_{ij}(\alpha)| = p^r$.
Por outro lado, sabemos que $\varphi_3(X_{ij}(\alpha)) = kX_{ij}(\alpha)$, com $k \in \mathbb{F}_q^* \simeq C_{q-1}$.
Se a ordem de $X_{ij}(\alpha)$ é p^r, elevando a equação $\varphi_3(X_{ij}(\alpha)) = kX_{ij}(\alpha)$ a p^r, temos que

$$\underbrace{(\varphi_3(X_{ij}(\alpha)))^{p^r} = k^{p^r} X_{ij}(\alpha)^{p^r}}_{\text{uma vez que } kI_n \text{ é central}}.$$

Sendo φ_3 um automorfismo, segue que,
$(\varphi_3(X_{ij}(\alpha)))^{p^r} = \varphi_3(X_{ij}(\alpha)^{p^r}) = \varphi_3(I_n) = I_n$. Logo, $I_n = k^{p^r} I_n$, o que implica que $k^{p^r} = 1$.
Como $k \in \mathbb{F}_q^* \simeq C_{q-1}$, com $q = p^m$, temos que $k^{p^m-1} = 1$, porém, como o $mdc\{p^m-1, p^r\} = 1$ segue que $k = 1$. Donde, φ_3 fixa $X_{ij}(\alpha)$, analogamente, fixa todo elemento de T_S ou T_I e, pelo Fato 4.10, fixa todas as transvecções.
Iniciemos analisando o automorfismo $\varphi_1 \circ \varphi_2 \circ \varphi_3 \circ \varphi_4$. Uma vez que $\varphi_4(X_{ij}(\alpha)) \in T_I$, como é fácil verificar pelas propriedades desas matrizes, segue que: $\varphi_1 \circ \varphi_2 \circ \varphi_3 \circ \varphi_4(X_{ij}(\alpha)) = \varphi_1 \circ \varphi_2(X_{ji}(-\alpha))$, uma vez que, $(X_{ij}(\alpha))^{-1} = X_{ij}(-\alpha)$ e $(X_{ij}(\alpha))^t = X_{ji}(\alpha)$.
Por outro lado, aplicando o teorema fundamental de Coleman, Teorema 3.1, [21], a T_S, temos

$$\varphi_1 \circ \varphi_2 \circ \varphi_3 \circ \varphi_4(X_{ij}(\alpha)) = {L_S}^{-1} X_{ij}(\alpha) L_S,$$

Sendo L_S uma matriz que depende apenas de T_S.
Dessa forma, temos:

$$\varphi_1 \circ \varphi_2(X_{ji}(-\alpha)) = {L_S}^{-1} X_{ij}(\alpha) L_S$$

$$N^{-1}(X_{ji}(-\lambda(\alpha)))N = {L_S}^{-1} X_{ij}(\alpha) L_S$$

$$(X_{ji}(-\lambda(\alpha)))N{L_S}^{-1} = N{L_S}^{-1} X_{ij}(\alpha).$$

Sendo φ_1 a conjugação por N e $\varphi_2(A) = \lambda(A)$, com $\lambda : \mathbb{F}_q \to \mathbb{F}_q$.
Apenas para facilitar a compreensão por parte do leitor, desenvolveremos esse raciocínio, particularmente para matrizes de ordem 3×3, porém é fácil verificar que esse argumento estende-se a matrizes de ordem superior a 3×3, todavia ele não se aplica a matriz de

ordem 2×2. Consideremos a matriz

$$X_{12}(\alpha) = \begin{bmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

E a matriz $NL_S{}^{-1} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$. Do fato de

$$(X_{ji}(-\lambda(\alpha)))NL_S{}^{-1} = NL_S{}^{-1}X_{ij}(\alpha),$$

temos que $\begin{bmatrix} 1 & 0 & 0 \\ -\lambda(\alpha) & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Daí, efetuando as devidas operações, obtemos:

$$\begin{bmatrix} a & b & c \\ -\lambda(\alpha)a + d & -\lambda(\alpha)b + e & -\lambda(\alpha)c + f \\ g & h & i \end{bmatrix} = \begin{bmatrix} a & \alpha a + b & c \\ d & \alpha d + e & f \\ g & \alpha g + h & i \end{bmatrix}.$$

Da 2^a linha, temos: $-\lambda(\alpha)a + d = d \Rightarrow a = 0$; $\quad -\lambda(\alpha)c + f = f \Rightarrow c = 0$. Analogamente, para $X_{13}(\alpha)$, teremos $X_{31}(-\lambda(\alpha))NL_S{}^{-1} = NL_S{}^{-1}X_{13}(\alpha)$. $\qquad (I)$

Observação 4.13. *A matriz L_S é a mesma, pois, devido ao teorema 3.1, depende apenas do p-subgrupo de Sylow.*

Da equação (I) acima temos:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -\lambda(\alpha) & 0 & 1 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

assim, $\begin{bmatrix} a & b & c \\ d & e & f \\ -\lambda(\alpha)a + g & -\lambda(\alpha)b + h & -\lambda(\alpha)c + i \end{bmatrix} = \begin{bmatrix} a & b & \alpha a + c \\ d & e & \alpha d + f \\ g & h & \alpha g + i \end{bmatrix}$. Da 3^a linha, obtemos:

$$-\lambda(\alpha)b + h = h \Rightarrow b = 0, \text{ donde } a = b = c = 0.$$

O que é impossível. Logo não existem automorfismos do tipo $\varphi_1 \circ \varphi_2 \circ \varphi_3 \circ \varphi_4$, independentemente de quais sejam φ_1, φ_2 e φ_3.

Agora resta analisar os automorfismos do tipo $\varphi_1 \circ \varphi_2 \circ \varphi_3$.

Aplicaremos este automorfismo às matrizes geradoras de $GL(n, \mathbb{F}_q)$, isto é, às transvec-

ções e às matrizes diagonais invertíveis, devido ao Fato 4.10, os automorfismos do tipo 3, φ_3 preservam conjugações e, como já vimos acima, estes fixam matrizes do tipo $X_{ij}(\alpha)$. Logo, φ_3 é trivial nas transvecções.
Dessa forma, o automorfismo $\varphi_1 \circ \varphi_2 \circ \varphi_3$ se reduz a $\varphi_1 \circ \varphi_2$, no que diz respeito a estas matrizes. Portanto, analisemos o que ocorre quando aplicamos esse automorfismo às matrizes diagonais, que estão definidas, no caso geral, como :

$$D(\alpha_1, \alpha_2, \alpha_3, \cdots \alpha_n) = \begin{bmatrix} \alpha_1 & 0 & 0 & \cdots & 0 \\ 0 & \alpha_2 & 0 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & \alpha_n \end{bmatrix},$$

com $\alpha_i \in {\mathbb{F}_q}^*$.

Fato 4.14. *As matrizes diagonais invertíveis caracterizam-se por apresentarem elementos não nulos ao longo da diagonal. Elas são o produto de matrizes diagonais elementares $D_i(\alpha)$, em que os elementos na diagonal são todos iguais a 1, exceto na posição ii que é igual a α.*

$$D_i(\alpha) = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & \cdots & \alpha & \cdots & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Em particular, consideremos, apenas por ilustração, uma matriz de ordem 3×3. Observemos que,

$$D(\alpha, \beta, \gamma) = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{bmatrix} = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \gamma \end{bmatrix}.$$

Fato 4.15. *É fácil verificar que matrizes diagonais elementares $D_k(\alpha)$, $D_l(\alpha)$, são conjugadas por matrizes permutação, que são involuções, ou seja, têm ordem 2, dadas por $P = (p_{ij})$, com $p_{ii} = 1$, se $k \neq i \neq j$, $p_{ii} = 0$, se $i = k$ ou $i = j$; $p_{ij} = 0$, para $i \neq j$, exceto em que $p_{kl} = 1 = p_{lk}$.*

Como ${\mathbb{F}_q}^* \simeq C_{q-1}$, consideremos α um gerador de um r-subgrupo de Sylow de ${\mathbb{F}_q}^*$,

e, uma vez mais com um exemplo de matriz de ordem 3×3, a matriz $D_1(\alpha) = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.
Daremos um exemplo em que as matrizes $D_1(\alpha)$ e $D_2(\alpha)$ são conjugadas. Para isto, consideremos uma matriz de permutação dada por:

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

É fácil ver que ela é sua própria inversa. Vamos fazer a conjugação de $D_1(\alpha)$ por esta matriz:

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

E assim concluímos que $D_1(\alpha)$ e $D_2(\alpha)$ são conjugadas.
Analogamente ao conjugarmos $D_1(\alpha)$ pela matriz $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$, obtemos a matriz $D_3(\alpha)$.

Observação 4.16. *As matrizes $D_1(\alpha)$ e $D_i(\alpha)$, para $i \neq 1$ estão no mesmo r-subgrupo de Sylow de $\mathbb{F}_q{}^*$, devido à sua ordem e ao fato de comutarem entre si.*

Dessa forma, existe uma matriz L, que depende apenas do r-subgrupo de Sylow que contém as matrizes $D_i(\alpha)$, $\forall i \in \{1, 2, \cdots, n\}$, tal que $\varphi_1 \circ \varphi_2 \circ \varphi_3(D_i(\alpha)) = L^{-1} D_i(\alpha) L$. Por outro lado, devido ao lema 3.6, de Petit Lobão e Sehgal [16]:

$$\varphi_1 \circ \varphi_2 \circ \varphi_3(D_i(\alpha)) = N^{-1} \lambda(k) D(\lambda(\alpha)) N,$$

Em que N é a matriz associada a φ_1, λ é o automorfismo associado a φ_2 e k é o escalar associado a φ_3. Então, $\lambda(k) D(\lambda(\alpha)) N L^{-1} = N L^{-1} D_i(\alpha)$.
Ou seja, usando uma vez mais uma ilustração para matrizes de ordem 3×3, que pode ser generalizada para qualquer matriz de ordem superior a 3×3, temos:

$$\lambda(k) \begin{bmatrix} \lambda(\alpha) & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Efetuando as devidas operações, obtemos:

$$\lambda(k)\begin{bmatrix} \lambda(\alpha)a & \lambda(\alpha)b & \lambda(\alpha)c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} \alpha a & b & c \\ \alpha d & e & f \\ \alpha g & h & i \end{bmatrix}$$

Se e, f, h ou $i \neq 0$, segue $\lambda(k) = 1$, logo $k = 1$.
Caso $e = f = h = i = 0$, segue que $d \neq 0$ e $g \neq 0$, e assim obtemos $\lambda(k) = \alpha$ e esta informação não é suficiente para nossa conclusão.
Como as demais colunas e as demais linhas também foram alteradas, delas não podemos retirar nenhuma informação relevante, assim, é necessário trabalharmos com outra linha e, para isto, vamos considerar a matriz $D_2(\alpha)\begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}$, que necessariamente pertence ao mesmo p-subgrupo de Sylow que contém a matriz anterior $\begin{bmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.
Dessa forma, temos

$$\lambda(k)\begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda(\alpha) & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} a & b & c \\ d & 0 & 0 \\ g & 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & 0 & 0 \\ g & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Logo,

$$\lambda(k)\begin{bmatrix} a & b & c \\ \lambda(\alpha)d & 0 & 0 \\ g & 0 & 0 \end{bmatrix} = \begin{bmatrix} a & \alpha b & c \\ d & 0 & 0 \\ g & 0 & 0 \end{bmatrix}.$$

Como $g \neq 0$, mais uma vez podemos concluir que $\lambda(k) = 1$ e então $k = 1$. Portanto, φ_3 é trivial em todas as matrizes diagonais, uma vez que $D_i(\alpha)$ geram as matrizes diagonais.
Observamos que o mesmo resultado pode ser obtido facilmente para uma matriz de ordem $n \times n$, com $n > 3$, uma vez que, ao multiplicarmos uma matriz do tipo $D(\alpha)$ à direita de uma matriz N, uma coluna desta última é substituída por um múltiplo e analogamente ocorre com relação à esquerda, para uma das linhas.
Portanto, reduzimos a questão aos automorfismos do tipo $\varphi_1 \circ \varphi_2$.

Apliquemos $\varphi_1 \circ \varphi_2$ à matriz αI.

$$\underbrace{\varphi_1 \circ \varphi_2(\alpha I) = \varphi_1((\lambda(\alpha)I)) = N^{-1}(\lambda(\alpha)I)N = \lambda(\alpha)I}_{\text{uma vez que } {}_{\alpha}\mathrm{I} \text{ é central}}.$$

Pelo resultado de Petit Lobão e Sehgal, lema 3.6. temos que $\exists\, L$ que depende de αI, tal que

$$\underbrace{\varphi_1 \circ \varphi_2(\alpha I) = L^{-1}(\alpha I)L = \alpha I}_{\text{uma vez que } {}_{\alpha}\mathrm{I} \text{ é central}}.$$

Comparando as duas expressões obtemos:

$$\lambda(\alpha)I = \alpha I \;\Rightarrow\; \lambda(\alpha) = \alpha.$$

Logo, φ_2 é a identidade.
Dessa forma, os automorfismos do tipo $\varphi_1 \circ \varphi_2 \circ \varphi_3$ se reduzem a automorfismos do tipo φ_1 que são internos.

- **Caso** $n = 2$

Fato 4.17. *Para $n = 2$, ou seja, em $GL(2, \mathbb{F}_q)$, o automorfismo contragradiente φ_4, como pode ser facilmente verificado, fica reduzido à composição $\varphi_1 \circ \varphi_3$, sendo $\varphi_3(A) = \dfrac{1}{detA}A$ e φ_1 a conjugação por $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, cujo inverso é $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.*

Devido a este fato, basta analisarmos o automorfismo $\varphi_1 \circ \varphi_2 \circ \varphi_3$.
Pode-se reproduzir o mesmo raciocínio do caso $n > 2$ para concluir-se que φ_3 é trivial nas transvecções, logo basta analisarmos as matrizes diagonais. Para tanto, reproduziremos o mesmo argumento utilizado no caso anterior, considerando matrizes diagonais elementares.
Pelo Lema 3.6, resultado de Petit Lobão e Sehgal [16], temos que:

$$\varphi_1 \circ \varphi_2 \circ \varphi_3 \left(\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} \right) = L^{-1} \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} L, \text{ em que } L \text{ depende de } \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}.$$

Por outro lado,

$$\varphi_1 \circ \varphi_2 \circ \varphi_3 \left(\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} \right) = N^{-1}\lambda(k) \begin{bmatrix} \lambda(\alpha) & 0 \\ 0 & 1 \end{bmatrix} N.$$

Logo,

$$L^{-1}\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} L = N^{-1}\lambda(k)\begin{bmatrix} \lambda(\alpha) & 0 \\ 0 & 1 \end{bmatrix} N.$$

Daí obtemos, $\lambda(k)\begin{bmatrix} \lambda(\alpha) & 0 \\ 0 & 1 \end{bmatrix} NL^{-1} = NL^{-1}\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}$, sendo φ_1 a conjugação por N.
Vale ressaltar que N é a matriz associada a φ_1, λ é o automorfismo associado a φ_2 e k é o escalar associado a φ_3.
Considerando a matriz $NL^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, obtemos a seguinte equação:

$$\lambda(k)\begin{bmatrix} \lambda(\alpha) & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}.$$

Então,

$$\lambda(k)\begin{bmatrix} \lambda(\alpha)a & \lambda(\alpha)b \\ c & d \end{bmatrix} = \begin{bmatrix} \alpha a & b \\ \alpha c & d \end{bmatrix}.$$

Dessa igualdade, obtemos:

$$\lambda(k)\lambda(\alpha)a = \alpha a, \quad \lambda(k)\lambda(\alpha)b = b, \quad \lambda(k)c = \alpha c, \quad \text{e} \quad \lambda(k)d = d.$$

Vamos analisar os casos $d \neq 0$ e $d = 0$.

Caso 1: Se $d \neq 0$, obviamente temos que $\lambda(k) = 1$. logo $k = 1$. Lembrando que $\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}$ e $\begin{bmatrix} 1 & 0 \\ 0 & \alpha \end{bmatrix}$ são conjugadas e que φ_3 preserva conjugação, temos que φ_3 age como a identidade em $\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}$ e $\begin{bmatrix} 1 & 0 \\ 0 & \alpha \end{bmatrix}$, o que implica que φ_3 é trivial nas matrizes diagonais.
Sendo α o gerador de $\mathbb{F}_q{}^* \simeq C_{q-1}$, concluímos que $\varphi_1 \circ \varphi_2 \circ \varphi_3$ reduz-se, no caso $d \neq 0$, a $\varphi_1 \circ \varphi_2$.
Mais uma vez, utilizando o mesmo raciocínio da seção anterior, podemos aplicar $\varphi_1 \circ \varphi_2$ à matriz αI e obtemos $\varphi_1 \circ \varphi_2(\alpha I) = \alpha I$, assim $\lambda(\alpha) = \alpha$, $\forall \alpha \in \mathbb{F}_q{}^*$. Logo, φ_2 é trivial e $\varphi_1 \circ \varphi_2$ reduz-se a φ_1. E daí o resultado segue.

Caso 2: Para $d = 0$, devemos ter $b \neq 0$ e $c \neq 0$ e, assim obtemos $\lambda(k) = \alpha$ e $\lambda(k)\lambda(\alpha) = 1$.
Logo, $\lambda(\alpha) = \alpha^{-1}$. Porém já vimos, pelo Lema 4.11, que esse automorfismo só existe para os corpos $\mathbb{F}_2$, $\mathbb{F}_3$ e $\mathbb{F}_4$.
Portanto, devemos analisar cada corpo separadamente.

- Corpo $\mathbb{F}_2$

Os automorfismos do tipo φ_2 e φ_3 são triviais.
Logo $\varphi_1 \circ \varphi_2 \circ \varphi_3$ se reduz a φ_1, que é um automorfismo interno. E assim o resultado segue.

- Corpo $\mathbb{F}_3$

Para o caso $\mathbb{F}_3$, φ_2 é trivial donde $\varphi_1 \circ \varphi_2 \circ \varphi_3$ se reduz a $\varphi_1 \circ \varphi_3$ e, lembrando que, pelo teorema 4.5, $GL(2,\mathbb{F}_3) = SL(2,\mathbb{F}_3) \rtimes {\mathbb{F}_3}^*$, e pela proposição 4.2, $|GL(2,\mathbb{F}_3)| = 48 = 3.16$.
Com isso, podemos garantir que um 2-subgrupo de Sylow de $GL(2,\mathbb{F}_3)$ tem ordem 16. É sabido que este 2-subgrupo de Sylow é isomorfo ao chamado grupo semidiedral com 16 elementos, $Q_8 \rtimes C_2$, vide [4] e é gerado por

$$\left\langle A, B : A^8 = B^2 = 1, BAB = A^3 \right\rangle,$$

em que

$$A = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \text{ e } B = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$$

E então $GL(2,\mathbb{F}_3) = \langle Q_8 \rtimes C_2, C_3 \rangle$,com apresentação dada por:

$$GL(2,\mathbb{F}_3) = \left\langle A, B, C : A^8 = B^2 = C^3 = 1, BAB = A^3, CAC = B \right\rangle.$$

em que A e B já foram definidos acima e $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Portanto, em $\mathbb{F}_3$, $\varphi_3(X) = X$ ou $\varphi_3(X) = -X, \quad \forall\, X \in GL(2,\mathbb{F}_3)$.
Como a ordem da matriz C é 3, $\varphi_3(C) = C$.
E para potências pares de elementos quaisquer, o sinal associado a φ_3 é positivo, ou seja $\varphi_3(X^2) = X^2$, $\forall X \in GL(2,\mathbb{F})$.
Observemos que estamos utilizando a técnica de Jackowski e Marciniak, [10] (considerando automorfismos em $I_S \subseteq Aut_{\mathcal{U}}(G)$, a partir de um 2-subgrupo de Sylow S, fixo em G). Para tanto, consideramos que o S fixo em $GL(2,\mathbb{F}_3)$ é o 2-subgrupo de Sylow com 16 elementos gerado por A e B, citado acima.
Vamos aplicar $\varphi_1 \circ \varphi_3$ a potências pares: Seja $A^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. e temos $\varphi_1 \circ \varphi_3$ em I_S. Então $\varphi_1 \circ \varphi_3(A^2) = A^2$, enquanto um elemento de I_S fixa os elementos de S:

$$\varphi_1 \circ \varphi_3 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Por outro lado,

$$\varphi_1 \circ \varphi_3 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = N^{-1}\varphi_3 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} N.$$

$$\text{Daí, } N^{-1}\varphi_3 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} N = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$\text{ou seja, } \varphi_3 \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} N = N \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Então,

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Assim, obtemos a seguinte equação

$$\begin{bmatrix} -c & -d \\ a & b \end{bmatrix} = \begin{bmatrix} b & -a \\ d & -c \end{bmatrix}$$

daí, temos $b = -c$ e $a = d$. Portanto, $N = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$.

Se $\varphi_3(X) = X$, $\forall X \in GL(2, \mathbb{F}_3)$ temos que o automorfismo $\varphi_1 \circ \varphi_3$ reduz-se a φ_1 que é um automorfismo interno e completamos a prova.

Porém, caso $\varphi_3(A) = -A$, temos, por um lado que:

$$\varphi_1 \circ \varphi_3 \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}. \qquad \text{(I)}$$

E, por outro lado,

$$\varphi_1 \circ \varphi_3 \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = N^{-1}\varphi_3 \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} N = N^{-1} \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix} N. \qquad \text{(II)}$$

Assim, comparando (I) e (II), obtemos:

$$\begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix} N = N \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}.$$

Lembrando que $N = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, obtemos:

$$\begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}.$$

Então obtemos a seguinte equação:

$$\begin{bmatrix} -a+b & -b-a \\ a+b & b-a \end{bmatrix} = \begin{bmatrix} a-b & a+b \\ -b-a & a-b \end{bmatrix}.$$

Logo,

$$\begin{bmatrix} -(a-b) & -(a+b) \\ a+b & -(a-b) \end{bmatrix} = \begin{bmatrix} a-b & a+b \\ -b-a & a-b \end{bmatrix}.$$

Dessa forma, temos que $a-b=-(a-b)$ e $a+b--(a+b)$, então $a-b=0$ e $a+b=0$ $\Rightarrow a=b=0$. Que é uma contradição, uma vez que N é invertível.
Portanto, φ_3 age trivialmente em A.
Agora, para estudarmos a ação de $\varphi_1 \circ \varphi_3$ em B, basta lembrarmos, na apresentação do grupo $GL(2,\mathbb{F}_3)$, da seguinte equação $CAC=B$. Aplicando φ_3 a ambos os lados dessa equação, obtemos $\varphi_3(CAC)=\varphi_3(B)$.
Como já verificamos que φ_3 fixa A e fixa C, temos que $\varphi_3(CAC)=CAC=B$.
Logo, como φ_3 age trivialmente nos três geradores de $GL(2,\mathbb{F}_3)$, concluímos que φ_3 é trivial em $GL(2,\mathbb{F}_3)$. Portanto, todo automorfismo em $Aut_{\mathcal{U}}(GL(2,\mathbb{F}_3))$ reduz-se a um automorfismo interno, isto é vale (Nor) em $GL(2,\mathbb{F}_3)$.

- **Corpo** $\mathbb{F}_4$

Para o caso $\mathbb{F}_4$, pelo Teorema 4.5, $GL(2,\mathbb{F}_4)=SL(2,\mathbb{F}_4)\rtimes {\mathbb{F}_4}^*$, e pela Proposição 4.2, $GL(2,\mathbb{F}_4)$ é um grupo com 180 elementos.
Para estudarmos o caso $GL(2,\mathbb{F}_4)$, usaremos argumentos que podem ser conferidos em W. R. Scott, [20]. Como ${\mathbb{F}_4}^*=\{1,a,a^2=1+a\}\simeq C_3$ e $|{\mathbb{F}_4}^*|=3$, então $|SL(2,\mathbb{F}_4)|=60$.
por W. R. Scott,[20], $SL(2,\mathbb{F}_4)\simeq Alt_5$.
Além disso, ${\mathbb{F}_4}^*=\left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, \begin{bmatrix} a^2 & 0 \\ 0 & a^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right\}$.

Como essas matrizes são centrais segue que o produto é direto, isto é,
$GL(2,\mathbb{F}_4)=SL(2,\mathbb{F}_4)\times {\mathbb{F}_4}^*=Alt_5\times C_3$.

Sendo C_3 abeliano, logo vale (Nor) para C_3. Como pela Proposição 3.9 (Nor) preserva produto direto, basta provar que vale (Nor) para Alt_5.
Sabemos que $Alt_5\leq Sym_5$, além disso, $Aut(Alt_5)\simeq Sym_5$.

Em Sym_5 existe uma classe de conjugação Γ, que em Alt_5 se quebra em duas, digamos Γ_1 e Γ_2, que consistem em ciclos de tamanho 5. Por exemplo Γ_1 é representada por [12345] enquanto Γ_2 é representada por [13524].
Suponhamos que não vale (Nor) em Alt_5, então existe $u\in\mathcal{U}(\mathbb{Z}(Alt_5))$ que cria uma auto-

morfismo φ_u que não é interno, isto é, $\varphi_u \in Aut(Alt_5)\backslash Inn(Alt_5)$, então esse automorfismo é da forma $\sigma(12)$ com $\sigma \in Alt_5$. Quando conjugamos a classe Γ_1 ou Γ_2 por $\sigma(12)$, é facil ver que σ não altera seus elementos, pois ele já esta em Alt_5, porém, conjugando Γ_1 pela transposição (12), obtemos Γ_2 e conjugando Γ_2 pela transposição (12), obtemos Γ_1. Dessa forma, obtem-se que φ_u leva elementos de uma classe, Γ_1, em outra classe distinta, Γ_2. Porém isso contradiz o lema 3.6, resultado de Petit Lobão e Sehgal [16].
Logo, não existe tal $u \in \mathcal{U}(\mathbb{Z}(Alt_5))$. Portanto, todos os automorfismos em Alt_5 são internos. Com isto, provamos que vale (Nor) para $GL(2, \mathbb{F}_4)$.
Portanto, pelo que vimos até agora, concluímos a prova da validade de(Nor) para $GL(n, \mathbb{F}_q)$, em que $q = p^m$, e isto completa a prova do teorema.

□

Conclusão

Abordamos em nosso trabalho o grupo adjunto de um anel finito e a Propriedade do Normalizador, essa última trata-se de uma importante questão na teoria de anéis de grupo integrais e possui uma relação com outra questão central, o *Problema do Isomorfismo*. O estudo do *Grupo Adjunto* de um anel, associado à *Propriedade do Normalizador* foi essencialmente motivado pelo fato de que o *Problema do Isomorfismo* para o grupo adjunto de um anel já havia sido estudado e resolvido por Sandling e, que ainda não existe na literatura investigação sobre a *Propriedade do Normalizador*, para grupos adjuntos.

Conseguimos determinar a estrutura grupo adjunto G como produto direto de grupos menores, G_{p_i}, que são os grupos adjuntos, de cada p-componente do anel R, ou seja, grupos adjuntos de cada R_{p_i} e, quando fazemos o quociente de cada R_p por pR_p, obtemos a estrutura $G_p/pR_p = J(R_p)/pR_p \rtimes B$, em que $B \cong (GL(n_1, \mathbb{F}_{q_1}) \times GL(n_2, \mathbb{F}_{q_2}) \times \cdots \times GL(n_k, \mathbb{F}_{q_k}))$. Uma vez estabelecida esta estrutura, aplicamos técnicas próprias da teoria de anéis de grupo integrais e conseguimos mostrar a validade de (Nor) para o grupo geral linear, $GL(n, \mathbb{F}_q)$, onde $\mathbb{F}_q$ é um corpo finito e $q = p^n$. Observemos que cada subgrupo $G_p \subset R_p$ que é um p-anel finito e portanto a quantidade de elementos desse subgrupo é uma potência de p; além disso, pR é um ideal do p-anel, R_p, então a quantidade de elementos desse ideal é também uma potência de p, assim, pR é um p-subgrupo de G_p. Ademais $J(R_p)$ é um ideal de R_p e também um subgrupo de G_p, então é um p-subgrupo de G_p, logo o quociente, $J(R_p)/pR_p$ é um p-subgrupo de G_p. Ressaltamos que ao retomarmos a estrutura obtida para o grupo adjunto, concluímos que o primeiro fator do produto semidireto é um p-grupo e, então vale (Nor). Quanto ao segundo fator, este é um produto direto de grupos gerais lineares, em que para cada um deles provamos que vale (Nor). Uma vez verificada a validade de (Nor) para cada $GL(n, \mathbb{F}_{q_i})$, podemos concluir que vale (Nor) também para o topo(ou complemento) do produto semidireto, desde que (Nor) preserva produto direto.

Portanto, acreditamos ter nos aproximado muito solução de (Nor) para o grupo adjunto, G/pR, uma vez que provamos a validade de (Nor) tanto para a base(ou núcleo) do produto semireto quanto para o topo (ou complemento), a partir daí basta considerar o produto direto: $G = G_{p_1} \circ \cdots \circ G_{p_n}$, obter a estrutura do grupo maior G/pR e aplicaremos técnicas próprias da teoria de anéis de grupo integrais para investigar a validade de (Nor) para G.

Referências

[1] ALPERIN, J. P.; BELL, R.B. *Groups and Representations.* New York: Springer-Verlag, 1995.

[2] COLEMAN, D. B. On the modular group ring og a p-group, *Proceedings of the American Mathematical Society*, v. 15, n. 4, p. 511-514, 1964.

[3] COHN, P. M. *Automorphisms of two-dimensional linear groups over Euclidean Domains,The Journal of The London Mathematical Society*, v. 1, n. 2, p. 279-292, 1969.

[4] CONWAY, J. H.; et al. *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Claredon Press. Oxford. 1985

[5] DIVINSKY, N. J. *Rings and Radicals. Toronto*: University of Toronto Press, 1965.

[6] DROZD, Y. A.; KIRICHENKO, V. V. *Finite Dimensional Algebras. Berlin: Springer-Verlag, 1994.*

[7] GARRET, P. Abstract Algebra, Disponível em: http://www.math.umn.edu/ garrett/m/algebra/notes/Whole.pdf

[8] GARCIA, A.; LEQUAIN. Y. *Elementos de Álgebra Publicações de Instituto de Matemática Pura e Aplicada(Projeto Euclides)*, Rio de Janeiro, 2010.

[9] HERTWECK, M. *A counterexample to the isomorphism problem for integral group rings*, *Annals of Mathematics*, v. 154, n. 1, p. 115-138, 2001.

[10] JACKOWSKI, S.; MARCINIAK, Z. *Group automorphisms inducing the identity map on cohomology*, *Journal of Pure and Applied Algebra*, v. 44, n. 1-3, p. 241-250, 1987.

[11] LI, Y.; PARMENTER, M. M.; SEHGAL, S. K. *On the normalizer property for integral group rings. Communications in Algebra*, v. 27, n. 9, p. 4217-4223, 1999.

[12] MCCONNELL, N. R.; STOKES, T. *Generalising Quaseregularity for Rings*, Australian Mathematical Society Gazette, vol. ..., n. ,p. 250-252, 1998.

[13] MAZUR, M. *On the isomorphism problem for integral group rings of infinite groups*, *Expo. Math.*, v. 13, n. 5, p. 433-445, 1995.

[14] PASSMAN, D. S. *The Algebraic Structure of Group Rings*, New York: Wiley-Interscience, 1977.

[15] PERLIS, S. *A characterization of the radical of an Algebra*, Bull. *Amer. Math. Soc.*, vol. 48, n. 2, p. 128-132, 1942.

[16] PETIT LOBÃO, T.; SEHGAL, S. K. *The Normalizer Property for Integral Group Rings of Complete Monomial Groups*, *Communications in Algebra*, v. 31, n. 6, p. 2971-2983, 2003.

[17] POLCINO MILIES, C. *Anéis e Módulos*, Publicações de Instituto de Matemática e Estatística da Universidade de São Paulo, São Paulo, 1972.

[18] POLCINO MILIES, C.; SEHGAL, S. K. , *An Introduction to Group Rings*, Dordrecht: Kluwer Academic Publishers, 2002.

[19] SANDLING, R. *Group rings of circle and unit groups*, *Math. Z.*, vol 140, p. 195-202, 1974.

[20] SCOTT, W. R. *Group Theory*, New York: Dover Publications. 1987.

[21] SEHGAL, S. K., *Units in Integral Group Rings*, Harlow: Longman Scientific and Technical, 1993.