UNIVERSIDADE FEDERAL DE MINAS GERAIS - UFMG
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Automorfismos de 2-grupos de Suzuki

José Luis Vilca Rodríguez

Belo Horizonte - MG
2015

UNIVERSIDADE FEDERAL DE MINAS GERAIS - UFMG
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

José Luis Vilca Rodríguez

Orientador: Csaba Schneider

Automorfismo de 2-Grupos de Suzuki

Dissertação apresentada ao Programa de Pós-Graduação em Matemática do Instituto de Ciências Exatas (ICEX) da Universidade Federal de Minas Gerais, como requisito parcial para obtenção de título de Mestre em Matemática.

Belo Horizonte - MG
2015

Agradecimentos

Gostaria de agradecer, primeiramente, ao meu orientador, o Prof. Csaba Schneider, pela sua paciência, compreensão e boa vontade com o trabalho que desenvolvemos.

Agradeço também aos professores e funcionários do Departamento de Matemática da UFMG, pelos conhecimentos transmitidos por eles e pelos seus favores infinitos. Em especial, agradeço aos membros da banca e a Kelli e Andréa.

Agradeço a CNPq, pelo apoio financeiro.

Agradeço aos meus familiares, por todo incentivo e ajuda em todos os momentos.

Finalmente, agradeço a todas as pessoas que direta ou indiretamente ajudaram para fazer possível este trabalho realidade.

Resumo

Os 2-grupos de Suzuki formam uma interessante classe de 2-grupos finitos. Eles foram introduzidos por Higman em 1961 e foram estudados por vários autores. Por definição, se G é um 2-grupo de Suzuki, então um subgrupo solúvel de $\mathrm{Aut}(G)$ permuta transitivamente as involuções de G. Higman identificou quatro famílias infinitas de 2-grupos de Suzuki e demonstrou que salvo isomorfismo todo 2-grupo de Suzuki pertence a uma destas famílias.

Esta dissertação é dedicada ao estudo dos automorfismos dos 2-grupos de Suzuki. Os principais teoremas descrevem os grupos de automorfismos dos grupos $A(n, \theta)$ e $\mathcal{B}(n)$ (o último isomorfo a um 2-subgrupo de Sylow de $\mathrm{SU}(3, 2^{2n})$). O resultado principal afirma que nestes casos o grupo de automorfismos é isomorfo ao produto semidireto de um 2-grupo abeliano elementar e um grupo isomorfo a $\Gamma\mathrm{L}(1, 2^m)$, onde $m = n$ no caso $A(n, \theta)$ e $m = 2n$ no caso $\mathcal{B}(n)$.

A descrição dos grupos de automorfismos é obtida usando métodos baseados em teoria de grupos de permutações e grupos lineares. A ideia nova na prova apresentada para os grupos $A(n, \theta)$, é usar a caracterização dada por Kantor dos grupos lineares que contém um ciclo de Singer. No caso de $\mathcal{B}(n)$, seguimos a prova dada por Landrock em 1974, a qual está também baseada em teoria de ciclos de Singer e num resultado devido a Hawkes, que descreve uma parte do grupo de automorfismos de um 2-grupo.

Obtemos, como consequência, um resultado que afirma que os 2-grupos de Suzuki que estudamos aqui, têm precisamente 3 subgrupos característicos, e assim verificamos parcialmente uma conjetura feita por Glasby, Pálfy and Schneider em 2011.

Abstract

Suzuki 2-groups form an interesting class of finite 2-groups. They were introduced by Higman in 1961 and further studied by various authors. By definition, if G is a Suzuki 2-group, then a solvable subgroup of $\mathrm{Aut}(G)$ permutes transitively the involutions of G. Higman identified four infinite families of Suzuki 2-groups and proved that each Suzuki 2-group belongs, up to isomorphism, to one of these families.

This dissertation is devoted to the study of the automorphisms of Suzuki 2-groups. The main theorems describes the automorphism groups of the groups $A(n,\theta)$ and $\mathcal{B}(n)$ (the latter is isomorphic to a Sylow 2-subgroup of $\mathrm{SU}(3,2^{2n})$). The main result states that in these cases the automorphism groups are isomorphic to the semidirect product of an elementary abelian 2-group and a group isomorphic to $\Gamma\mathrm{L}(1,2^m)$ where $m=n$ in the case of $A(n,\theta)$ and $m=2n$ in the case of $\mathcal{B}(n)$.

The description of the automorphism groups is obtained using a methodology based on the theory of permutation groups and linear groups. The novel idea in the proof presented here for the groups $A(n,\theta)$ is the use of the characterization by Kantor of the linear groups that contain a Singer cycle. In the case of $\mathcal{B}(n)$, we adopt the proof presented by Landrock in 1974, which is also based on the theory of Singer cycles and on a result by Hawkes that describe a certain part of the automorphism group of a 2-group.

We obtain, as a by-product, a result that states that the Suzuki 2-groups that we study have precisely 3 characteristic subgroups, and thus we partially verify a conjecture made by Glasby, Pálfy and Schneider in 2011.

Sumário

Lista de Notações

$\mathrm{Sym}(\Omega)$	Grupo simétrico de Ω
αf	Imagem de α via o homomorfismo f
αG	Órbita de α sob a ação de G
G_α	Estabilizador de α sob a ação de G
$G_{\{S\}}$	Estabilizador pontual de S em G
$\lvert X\rvert$	Número de elementos no conjunto X
$C_G(H)$	Centralizador de H em G
$N_G(H)$	Normalizador de H em G
$Z(G)$	Centro de G
$\Phi(G)$	Subgrupo de Frattini de G
$\overline{G}$	Grupo quociente $G/Z(G)$
$\lvert G:H\rvert$	Número de classes laterais de H em G
$H \rtimes N$	Produto semidireto dos grupos H e N
$\mathrm{Aut}(G)$	Grupo de automorfismos do grupo G
D_{2q}	Grupo diedral de ordem $2q$
$\ker\mu$	Núcleo da aplicação μ
$\mathrm{Im}\,\mu$	Imagem da aplicação μ
$\mathbb{F}_q$	Corpo com q elementos
$\mathrm{Aut}(\mathbb{F}_q)$	Grupo de automorfismos do corpo $\mathbb{F}_q$
$\mathrm{GL}(n,q)$	Grupo linear geral de ordem n sobre $\mathbb{F}_q$
$\mathrm{PGL}(n,q)$	Grupo linear geral grojetivo de ordem n sobre $\mathbb{F}_q$
$\mathrm{SL}(n,q)$	Grupo linear especial de ordem n sobre $\mathbb{F}_q$
$\mathrm{PSL}(n,q)$	Grupo linear especial projetivo de ordem n sobre $\mathbb{F}_q$
$\Gamma\mathrm{L}(n,q)$	Grupo semilinear geral de ordem n sobre $\mathbb{F}_q$
$\mathrm{P}\Gamma\mathrm{L}(n,q)$	Grupo semilinear projetivo de ordem n sobre $\mathbb{F}_q$

$V^\times$	Conjunto de elementos não nulos do espaço vetorial V
I_G	Conjunto de elementos de ordem menor ou igual a 2 no grupo G
a^θ	Imagem de a via o automorfismo θ
$\mathcal{A}$	Grupo de automorfismos de um 2-grupo de Suzuki G
K	Núcleo da aplicação natural de $\mathcal{A}$ em $\mathrm{Aut}(\overline{G})$
$\overline{\mathcal{A}}$	Grupo quociente $\mathcal{A}/K$
L	Núcleo da aplicação natural de $\mathcal{A}$ em $\mathrm{Aut}(I_G)$
$\overline{L}$	Grupo quociente L/K

Introdução

É um fato indiscutível que o estudo dos p-grupos é uma parte muito importante da teoria de grupos. Devemos também dizer que p-grupos formam uma classe muito grande de grupos. Sendo assim, para um estudo mais detalhado, frequentemente estudamos uma classe menor de p-grupos. Por exemplo, podemos considerar a classe de p-grupos G satisfazendo a seguinte condição: O grupo $\mathrm{Aut}(G)$, de automorfismos de G, permuta transitivamente o conjunto de subgrupos de ordem p de G. Agora, no estudo de p-grupos, o primo $p = 2$ frequentemente comporta-se de maneira diferente dos outros primos, no sentido que muitos dos teoremas para p-grupos, com p ímpar, não são válidos para 2-grupos. Por exemplo, Shult [1] mostrou que, se G é um p-grupo com p ímpar, satisfazendo a condição anterior, este deve ser abeliano. Isso não acontece se $p = 2$. Temos, por exemplo, o grupo $A(n, \theta)$, com $\theta \neq 1$, apresentado em [2, p. 294]. Sendo assim, consideremos os 2-grupos que satisfazem a condição anterior. Em 2-grupos, esta condição é equivalente a dizer que o grupo $\mathrm{Aut}(G)$ permuta transitivamente o conjunto das involuções de G. Se temos um 2-grupo não abeliano com uma única involução, este é isomorfo ao grupo dos quatérnios generalizados (veja [3, p. 14]). Os 2-grupos G não abelianos com mais de uma involução, nos quais um subgrupo solúvel de $\mathrm{Aut}(G)$ permuta o conjunto das involuções transitivamente, são chamados *2-grupos de Suzuki*. Estes grupos foram estudados por Higman em [4]. Neste artigo Higman classifica os 2-grupos de Suzuki em quatro classes: $A(n, \theta), B(n, \theta, \varepsilon), C(n, \theta)$ e $D(n, \theta, \varepsilon)$ (veja as definições na seção 2.1).

Este trabalho é dedicado ao estudo de grupos de automorfismos dos 2-grupos de Suzuki $A(n, \theta)$ e $\mathcal{B}(n)$, definidos na seção 2.4. Nosso teorema principal, teorema 3.1.1, é o seguinte:

Teorema. Seja G um 2-grupo de Suzuki isomorfo a $A(n, \theta)$ ou a $\mathcal{B}(n)$. Então

$$\mathrm{Aut}(G) \cong \begin{cases} (C_2)^{n^2} \rtimes \Gamma\,\mathrm{L}(1, 2^n), \text{ se } G \cong A\,(n, \theta) \\ (C_2)^{2n^2} \rtimes \Gamma\,\mathrm{L}(1, 2^{2n}), \text{ se } G \cong \mathcal{B}\,(n)\,. \end{cases}$$

Em particular, $\mathrm{Aut}(G)$ é solúvel.

A demonstração do teorema será apresentada no capítulo 3.

Os primeiros resultados sobre automorfismos de 2-grupos de Suzuki dos quais temos referência são os dados por Landrock [5] e por Bryukhanova [6]. Landrock no seu artigo dá a estrutura do grupo de automorfismos de uma classe de 2-grupos de Suzuki em termos do seu maior 2-subgrupo normal. O enfoque do Landrock é via *grupos de Singer* e o teorema de Hawkes [7]. No entanto, um resultado que é válido para todo 2-grupo de Suzuki é o dado por Bryukhanova, o qual afirma que o grupo de automorfismos de um 2-grupo de Suzuki é solúvel. Depois de Landrock e Bryukhanova, Kazarin e Sidel'nikov [8] deram uma determinação explícita do grupo de automorfismos de uma p-álgebra de Suzuki. No ano 2014 Lewis [9], inspirado pelas ideias de Bryukhanova e de Kazarin e Sidel'nikov, dá uma determinação explícita do grupo de automorfismos de $A(n, \theta)$. Lewis no seu artigo, usa fortemente o fato da solubilidade mostrado por Bryukhanova.

Nosso aporte neste trabalho será dar a mesma determinação do que Lewis para $A(n, \theta)$, porém nosso enfoque será muito diferente. Nós usaremos a teoria de grupos de Singer, teoria de *grupos lineares e semilineares* e o teorema de Kantor [10], e combinaremos estes com ideias de Kazarin e Sidel'nikov, e de Lewis. Nós não encontramos um enfoque parecido na literatura, se ele existir, não é fácil de encontrar. Embora Lewis, no seu artigo [9, Teorema 8.5], obteve a mesma determinação que obtemos para $A(n, \theta)$, ele usou o fato da solubilidade mostrado por Bryukhanova. Da maneira que vamos obter o grupo de automorfismos para $A(n, \theta)$, o fato da solubilidade é um corolário direto. Para a determinação do grupo de automorfismos de $\mathcal{B}(n)$ seguiremos a demonstração de Landrock, porém apresentamos a prova de maneira reorganizada e ampliada. Também, cremos que um fato relevante de nosso trabalho é escrever num mesmo contexto (até certo lugar) as demonstrações das afirmações para os automorfismos destes dois grupos.

No presente trabalho, apresentaremos no capítulo 1 os conceitos básicos para auxiliar um desenvolvimento posterior. Trataremos de ações de grupos e grupos de permutações, mencionando os resultados que precisaremos, grupos lineares e semilineares, e daremos uma demonstração do fato que o normalizador de $\mathrm{GL}(n, q)$ em $\mathrm{Sym}(\mathbb{F}_{q^n}^\times)$ é o grupo semilinear $\Gamma\mathrm{L}(n, q)$, teorema 1.3.1. Este será um resultado importante na determinação do grupo de automorfismos de $A(n, \theta)$. Também, estudaremos os grupos de Singer, os quais são fundamentais para este trabalho. Por último, neste mesmo capítulo, citaremos o teorema de Hawkes [7] e resultados relacionados com o subgrupo comutador e subgrupo de Frattini. No capítulo 2, apresentaremos os 2-grupos de Suzuki formalmente. Diferentemente de Higman [4], nós apresentamos estes como grupos de matrizes. Optamos por esta apresentação já que oferece pequenas vantagens. Mostraremos propriedades da estrutura destes grupos, e provaremos uns isomorfismos mencionados no artigo de Higman [4] sem prova. Finalmente, neste capítulo, introduziremos o grupo $\mathcal{B}(n)$. O capítulo 3, que será o último, é dedicado ao estudo dos grupos de automorfismos dos 2-grupos de Suzuki. Neste capítulo, primeiro discutiremos de maneira uniforme os automorfismos dos grupos $A(n,\theta)$ e $\mathcal{B}(n)$, depois, para a determinação do grupo de automorfismos, trataremos separadamente os grupos $A(n,\theta)$ e $\mathcal{B}(n)$, e com isto terminaremos este trabalho.

Uma motivação para este trabalho surgiu de um comentário feito no artigo [11]: "Os 2-grupos de Suzuki $A(n,\theta)$ são UCS", ou seja, eles têm somente três subgrupos característicos. Foi conjeturado que isso é valido para todos os 2-grupos de Suzuki. Os nossos resultados implicam que a conjetura é válida para os grupos $A(n,\theta)$ e $\mathcal{B}(n)$. A conjetura permanece aberta para os outros 2-grupos de Suzuki.

Consideramos que uma explicação da notação é necessária aqui. No decorrer deste trabalho usaremos sempre a ação de um grupo num conjunto à direita. Também homomorfismos serão aplicados à direita, ou seja, af representará a imagem de a via o homomorfismo f. No caso de corpos, a^θ representará a imagem de a via o automorfismo θ, nós optamos por esta notação já que os corpos tratados aqui serão finitos, e os automorfismo em corpos finitos comportam-se como expoentes.

O título deste trabalho não é inteiramente correto, um melhor título seria: "Uma Introdução aos elementos em Automorfismos de 2-grupos de Suzuki". A palavra elementos advertiria que nem tudo está tratado aqui, e a palavra introdução advertiria que o tratado aqui precisa ser completado.

Capítulo 1

Conceitos Básicos

Este primeiro capítulo é destinado a dar as bases do presente trabalho. Nós precisaremos destas ferramentas para uma melhor compreensão dos capítulos posteriores. Na seção 1.1 trataremos de ações de grupos e grupos de permutações. Na seção 1.2 vamos apresentar os grupos lineares e semilineares para logo, na seção 1.3, combinar isto com o tratado na primeira seção e obter resultados sobre normalizadores e centralizadores do grupo linear geral. Finalmente, na seção 1.4 trataremos os grupos cíclicos agindo irredutivelmente em um espaço vetorial de dimensão finita e também os grupos de Singer dos grupos lineares.

1.1 Ações de grupos e grupos de permutações

O objetivo desta seção é introduzir os conceitos elementares de grupos de permutações, ações de grupos, grupos transitivos e alguns resultados básicos envolvendo os mesmos.

Definição 1.1.1. Uma *permutação* de um conjunto Ω é uma bijeção de Ω em Ω.

O conjunto de todas as permutações em Ω tem a estrutura de grupo com a composição de funções, este grupo é chamado *grupo simétrico* de Ω, e é denotado por $\mathrm{Sym}(\Omega)$. Se $\Omega = \{1, ..., n\}$, nós representaremos o conjunto de todas as permutações de Ω por S_n.

Se $g \in \mathrm{Sym}(\Omega)$ e $\alpha \in \Omega$ denotaremos por αg a imagem de α via a permutação g. Sendo assim, a composição gh, das permutações g e h, significa aplicar primeiro a permutação g e depois a permutação h.

Definição 1.1.2. Dado um grupo G, uma *ação* de G em Ω é uma função de $\Omega \times G$ em Ω, $(\alpha, g) \mapsto \alpha g$, a qual satisfaz as seguintes condições:

a) $\alpha 1 = \alpha$, para todo $\alpha \in \Omega$.

b) $(\alpha g) h = \alpha (gh)$ para todo $\alpha \in \Omega$ e para todo $g, h \in G$.

Dada uma ação de G em Ω, dizemos que G age em Ω.

Para exemplificar, consideremos a aplicação $\Omega \times \mathrm{Sym}(\Omega) \to \Omega$ dada por $(\alpha, g) \mapsto \alpha g$, esta define uma ação de $\mathrm{Sym}(\Omega)$ em Ω. Quando considerarmos uma ação de $\mathrm{Sym}(\Omega)$ em Ω esta será sempre como a definida acima, exceto menção contrária.

A ação da definição 1.1.2 é chamada *ação à direita*, e de forma similar podemos definir ação à esquerda. Neste trabalho usaremos apenas ações à direita. Sendo assim, sempre que uma ação esteja implícita nós assumiremos que esta é uma ação à direita.

Nós também vamos usar a notação à direita no caso do homomorfismo de grupos. Se $f : G \to H$ é um homomorfismo de grupos, xf representará a imagem de x via f, e a composição (caso que seja possível) de homomorfismos fg, significará aplicar primeiro f e depois g. Além disso, se $A \subset G$ então $(A)f$ representará a imagem de A via f, isto é, $(A)f = \{af \mid a \in A\}$.

Dada uma ação de G em Ω e um elemento $\alpha \in \Omega$ o conjunto

$$\alpha G = \{\alpha g \mid g \in G\}$$

é chamado *órbita* de α; e o conjunto

$$G_\alpha = \{g \in G \mid \alpha g = \alpha\}$$

é chamado *estabilizador* de α.

Veja que o estabilizador de α é um subgrupo de G, e que dados α e β em Ω, com $\alpha G \neq \beta G$, se tem $\alpha G \cap \beta G = \emptyset$.

A definição de estabilizador, dada acima, não está isenta de generalização. Pois, dado um subconjunto S de Ω definimos o *estabilizador pontual* de S por:

$$G_{\{S\}} = \{g \in G \mid sg = s \text{ para todo } s \in S\}.$$

O seguinte resultado é um teorema clássico no estudo das ações de grupos. Uma demostração do mesmo pode ser encontrado em qualquer referência que trate deste tema. Sugerimos por exemplo [12, Teorema 1.4 A].

Teorema 1.1.1. *Seja G um grupo agindo em Ω. Então se verificam:*

i) Dados $\alpha, \beta \in \Omega$ e $g \in G$ tais que $\beta = \alpha g$, então $G_\beta = g^{-1} G_\alpha g$.

ii) (Teorema da Órbita-Estabilizador). Para qualquer $\alpha \in \Omega$ temos $|\alpha G| = |G : G_\alpha|$. Em particular, se G for finito, temos $|G| = |\alpha G|\,|G_\alpha|$.

Definição 1.1.3. Seja G um grupo agindo em Ω.

a) Dizemos que G é *transitivo*, ou que a ação de G em Ω é transitiva, se só existir uma única órbita.

b) O grupo G é chamado *semiregular*, ou a ação de G em Ω é semiregular, se $G_\alpha = 1$ para toda $\alpha \in \Omega$

c) O grupo G é chamado *regular*, ou a ação de G em Ω. é regular, se G é transitivo e semiregular.

Segue diretamente da definição que G é transitivo se, e somente se, dados $\alpha, \beta \in \Omega$ existe $g \in G$ que verifica $\alpha = \beta g$ se, e somente se, $\alpha G = \Omega$, para qualquer $\alpha \in \Omega$. Além disso, se G for finito e transitivo o item ii) do teorema 1.1.1 implica que $|\Omega| = |G : G_\alpha|$ para qualquer $\alpha \in \Omega$.

Por outro lado, se G é regular o mesmo teorema 1.1.1 implicará $|\Omega| = |G|$. O grupo G é semiregular se, e somente se, a identidade de G é o único elemento que fixa pontos de Ω.

Dado um grupo G fixemos um subgrupo H e denotamos por Γ_H o conjunto de todas as classes laterais direitas. Então podemos fazer agir G no conjunto Γ_H definindo a aplicação $\rho_H : \Gamma_H \times G \to \Gamma_H$ por $(Ha, g) \mapsto Hag$. Esta é de fato uma ação de G em Γ_H e é chamada *multiplicação à direita.*

Por outro lado, seja $K = N_G(H)$, então desde que $H \leq K \leq G$, K também age em Γ_H por multiplicação à direita. Embora esta ação possa dar-nos alguma informação temos interesse em definir uma outra ação de K em Γ_H. Sendo assim, definamos a aplicação $\lambda_H : \Gamma_H \times K \to \Gamma_H$ por $(Ha, x) \mapsto x^{-1}(Ha) = Hx^{-1}a$. Tal aplicação é uma ação e é chamada *multiplicação à esquerda.*

Toda ação de G em Ω pode pensar-se como um homomorfismo $\mu : G \to \mathrm{Sym}(\Omega)$. De fato, dada uma ação de G em Ω, $(\alpha, g) \mapsto \alpha g$, podemos definir $\mu : G \to \mathrm{Sym}(\Omega)$

por $g \mapsto g\mu$, onde $\alpha(g\mu) = \alpha g$. Do fato que $(\alpha, g) \mapsto \alpha g$ é uma ação segue que μ é um homomorfismo. Reciprocamente, dado um homomorfismo $\mu : G \to \mathrm{Sym}(\Omega)$ podemos definir a aplicação $(\alpha, g) \mapsto \alpha(g\mu)$; que é uma ação desde que μ é um homomorfismo. Nesta linguagem podemos ver as ações de G e K em Γ_H, do parágrafo anterior, como homomorfismos $\rho_H : G \to \mathrm{Sym}(\Gamma_H)$ e $\lambda_H : K \to \mathrm{Sym}(\Gamma_H)$.

Antes de continuar nossa digressão vamos lembrar umas definições de teoria de grupos.

Definição 1.1.4. Seja G um grupo e H um subgrupo de G.

i) O *centro* de G é o subgrupo

$$Z(G) = \{g \in G \mid gx = xg \text{ para todo } x \in G\}.$$

ii) O *centralizador* de H em G é o subgrupo

$$C_G(H) = \{g \in G \mid gh = hg \text{ para todo } h \in H\}.$$

iii) O *normalizador* de H em G é o subgrupo

$$N_G(H) = \{g \in G \mid gH = Hg\}.$$

Com as definições dadas acima vamos enunciar alguns resultados. Uma demonstração destes fatos e também um estudo mais completo sobre grupos permutações podem ser encontrados em [12].

O seguinte lema nos dá as principais propriedades dos homomorfismos ρ_H e λ_H .

Lema 1.1.2 ([12], Lema 4.2 A)**.** *Com a linguagem acima se verifica:*

i) $\ker \lambda_H = H$ *e* $(K)\lambda_H$ *é semiregular.*

ii) O centralizador C *de* $(G)\rho_H$ *em* $\mathrm{Sym}(\Gamma_H)$ *é* $(K)\lambda_H$*.*

iii) O elemento $H \in \Gamma_H$ *tem a propriedade que as órbitas dele em* $(K)\lambda_H$ *e* $(K)\rho_H$ *são iguais.*

iv) Se o grupo $(K)\lambda_H$ *é transitivo então* $K = G$*. Neste caso* $(G)\lambda_H$ *e* $(G)\rho_H$ *são conjugados em* $\mathrm{Sym}(\Gamma_H)$*.*

O corolário que segue é uma aplicação do lema anterior para normalizadores e centralizadores em $\mathrm{Sym}(\Omega)$.

Corolário 1.1.3 ([12], Teorema 4.2)**.** *Seja G um grupo transitivo em* $\mathrm{Sym}(\Omega)$ *e C o centralizador de G em* $\mathrm{Sym}(\Omega)$*. Então, para $\alpha \in \Omega$ temos:*

i) O grupo C é semiregular, e além disso se tem o isomorfismo $C \cong N_G(G_\alpha)/G_\alpha$.

ii) O grupo C é transitivo se, e somente se, G é regular.

iii) Se C é transitivo, então este é conjugado a G em $\mathrm{Sym}(\Omega)$*.*

iv) Se G é abeliano, então $C = G$.

Consideremos agora um grupo transitivo G de $\mathrm{Sym}(\Omega)$, e seja N o normalizador de G em $\mathrm{Sym}(\Omega)$. Podemos definir o homomorfismo $\Psi : N \to \mathrm{Aut}(G)$, onde $(n)\Psi : g \mapsto n^{-1}gn$. O núcleo de Ψ é o centralizador de G em $\mathrm{Sym}(G)$. Logo, o item i) do lema anterior diz que Ψ é injetiva quando $N(G_\alpha) = G_\alpha$ para $\alpha \in \Omega$.

O seguinte lema caracteriza os elementos de $\mathrm{Im}\Psi$ em termos dos estabilizadores de G. Na próxima seção determinaremos $\mathrm{Im}\Psi$ para um grupo G específico, e com isso vamos refletir a importância do próximo lema, já que vamos nos referir ao mesmo várias vezes em tal determinação.

Lema 1.1.4 ([12], Teorema 4.2 B)**.** *Seja G um grupo transitivo de* $\mathrm{Sym}(\Omega)$ *e Ψ o homomorfismo definido acima. Dado $\alpha \in \Omega$ e $\sigma \in \mathrm{Aut}(G)$ temos que $\sigma \in \mathrm{Im}\,\Psi$ se, e somente se, $(G_\alpha)\sigma$ é um estabilizador de G.*

1.2 Grupos Lineares e Semilineares

Dado um espaço vetorial V de dimensão n sobre o corpo $\mathbb{F}_q$, se define o *grupo linear geral* $\mathrm{GL}\,(V)$, como sendo o grupo de todas as transformações lineares $g : V \to V$ invertíveis.

Fixando uma base, este grupo é isomorfo ao grupo $\mathrm{GL}\,(n, q)$ de todas as matrizes invertíveis $n \times n$ com entradas em $\mathbb{F}_q$. Nós usaremos indistintamente estes dois grupos.

O grupo $\mathrm{GL}(n, q)$ age naturalmente no espaço vetorial V: $(v, g) \mapsto vg$. Sempre que tratemos alguma ação de $\mathrm{GL}(n, q)$ em V será esta.

Dado um espaço vetorial V, sobre algum corpo, denotamos por $V^\times$ o conjunto de elementos não nulos em V, isto é $V^\times = \{v \in V \mid v \neq 0\}$.

A aplicação determinante $\det : \mathrm{GL}\,(n, q) \to \mathbb{F}_q^\times$ define um homomorfismo de $\mathrm{GL}\,(n, q)$ sobre $\mathbb{F}_q^\times$. O núcleo desta aplicação é o grupo

$$\mathrm{SL}\,(n, q) = \{g \in \mathrm{GL}\,(n, q) \mid \det g = 1\},$$

chamado *grupo linear especial.* Se tem que $\mathrm{GL}(n,q)/\mathrm{SL}(n,q) \cong \mathbb{F}_q^{\times}$, e logo

$$|\mathrm{GL}(n,q)/\mathrm{SL}(n,q)| = q-1.$$

Para cada $w \in \mathbb{F}_q^{\times}$ seja δ_w a matriz

$$\begin{pmatrix} w & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}. \tag{1.1}$$

O conjunto $M = \{\delta_w : w \in \mathbb{F}_q^{\times}\}$ é um grupo cíclico isomorfo a $\mathbb{F}_q^{\times}$, e além disso se tem $M \cap \mathrm{SL}(n,q) = \{1\}$. Desde que M normaliza $\mathrm{SL}(n,q)$, o produto $\mathrm{SL}(n,q)M$ é semidireto, e como $|\mathrm{GL}(n,q)| = |\mathrm{SL}(n,q)||M|$, teremos que

$$\mathrm{GL}(n,q) = \mathrm{SL}(n,q) \rtimes M. \tag{1.2}$$

Um hiperplano em V é um subespaço W de dimensão $\dim V - 1$. Se W é um hiperplano de V e $\tau \in \mathrm{GL}(n,q)$ é tal que $\tau|_W = 1_W$ e $v\tau - v \in W$, para todo $v \in V$, então dizemos que τ é uma transvecção, e que W é o espaço fixo de τ. Segue diretamente da definição que se τ é uma transvecção então $v\tau = v + (vf)w$, onde $w \in W$ e $f : V \to \mathbb{F}_q$ é um funcional linear tal que $(W)f = 0$.

As transvecções são importantes para o estudo dos grupos clássicos, o que segue é um lema que reflete esta importância, mas só no caso de $\mathrm{SL}(n,q)$. Uma demonstração para este lema pode ser encontrada, por exemplo, em [13].

Lema 1.2.1 ([13], Teorema 1.4)**.** *O conjunto de transvecções gera* $\mathrm{SL}(n,q)$.

Definimos o *grupo linear geral projetivo* $\mathrm{PGL}(n,q)$, como:

$$\mathrm{PGL}(n,q) = \mathrm{GL}(n,q)/Z(\mathrm{GL}(n,q)),$$

temos que $\mathrm{PGL}(n,q)$ é isomorfo ao grupo de automorfismos internos de $\mathrm{GL}(n,q)$.

Da mesma forma definimos o *grupo linear especial projetivo* por

$$\mathrm{PSL}(n,q) = \mathrm{SL}(n,q)/Z(\mathrm{SL}(n,q)),$$

aqui também se tem que $\mathrm{PSL}(n,q)$ é isomorfo ao grupo de automorfismos internos de $\mathrm{SL}(n,q)$.

Dado outro espaço vetorial V' dizemos que a aplicação $g : V \to V'$ é *semilinear* se existe um $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ tal que:

$$(x + y)g = xg + yg$$

$$(\lambda x)g = \lambda^\sigma (xg),$$

para quaisquer $x, y \in V$ e $\lambda \in \mathbb{F}_q$. Se $g \neq 0$, o automorfismo σ está unicamente determinado por g. Se g é semilinear e σ é o automorfismo determinado por g, então dizemos que g é semilinear relativamente a σ. Se $g, h : V \to V$ são aplicações semilineares relativas a σ, θ respectivamente, então gh é uma aplicação semilinear relativa a $\sigma\theta$. Além disso, se g é semilinear relativamente a σ e é invertível, então g^{-1} é semilinear relativamente σ^{-1}. Do anterior temos que o conjunto de todas as aplicações semilineares de V em V invertíveis formam um grupo $\Gamma\mathrm{L}(n, q)$ chamado *grupo geral semilinear*.

A aplicação $\Gamma\mathrm{L}(n, q) \to \mathrm{Aut}(\mathbb{F}_q)$, que faz corresponder a cada transformação semilinear g o automorfismo σ, com respeito do qual g é semilinear, é um homomorfismo sobre $\mathrm{Aut}(\mathbb{F}_q)$ com núcleo $\mathrm{GL}(n, q)$. Logo, se tem que $\mathrm{GL}(n, q)$ é um subgrupo normal de $\Gamma\mathrm{L}(n, q)$, e além disso $\Gamma\mathrm{L}(n, q)/\mathrm{GL}(n, q) \cong \mathrm{Aut}(\mathbb{F}_q)$. Seja $\{b_1, ..., b_n\}$ uma base do espaço V e $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$. A aplicação g_σ, que asocia a $v = \alpha_1 b_1 + \cdots + \alpha_n b_n$ o vetor $\alpha_1^\sigma b_1 + \cdots + \alpha_n^\sigma b_n$, é semilinear. Seja $\Sigma = \{g_\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{F}_q)\}$, dado um $g_\sigma \in \Sigma$ este é linear se, e somente se, $\sigma = 1$, e isto implica que $\Sigma \cap \mathrm{GL}(n, q) = \{1\}$. Desde que $\mathrm{GL}(n, q)$ é normal em $\Gamma\mathrm{L}(n, q)$ segue que produto $\mathrm{GL}(n, q)\Sigma$ é semidireto, e desde que $|\Gamma\mathrm{L}(n, q)| = |\mathrm{GL}(n, q)||\Sigma|$ teremos

$$\Gamma\mathrm{L}(n, q) = \mathrm{GL}(n, q) \rtimes \Sigma. \tag{1.3}$$

Dada uma base $\{b_1, ..., b_n\}$ de V e $g \in \Gamma\mathrm{L}(n, q)$ se tem que existem únicos $\lambda_{ij} \in \mathbb{F}_q$ tais que

$$b_i g = \sum_{j=1}^{n} \lambda_{ij} b_j.$$

A matriz $A_g = (\lambda_{ij})$ é chamada matriz da transformação semilinear g com respeito a base $\{b_1, ..., b_n\}$. Esta noção é uma generalização à noção de matriz de uma transformação linear.

Para $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ e uma matriz $A = (a_{ij})$ se define $A^\sigma = \left(a_{ij}^\sigma\right)$.

Lema 1.2.2. *Sejam $f, g \in \Gamma\,\mathrm{L}\,(n, q)$, onde g é semilinear relativamente a $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$. Então $A_{fg} = A_f^\sigma A_g$. Como consequência $A_{g^{-1}}^\sigma = A_g^{-1}$.*

Demonstração. Se $A_f = (\lambda_{ij})$ e $A_g = (\mu_{ij})$ então temos

$$\begin{aligned} b_i fg &= \left(\sum_{j=1}^{n} \lambda_{ij} b_j\right) g \\ &= \sum_{j=1}^{n} \lambda_{ij}^{\sigma} (b_j g) \\ &= \sum_{j=1}^{n} \left(\sum_{k=1}^{n} \lambda_{ij}^{\sigma} \mu_{jk}\right) b_k \\ &= \sum_{k=1}^{n} \left(\sum_{j=1}^{n} \lambda_{ij}^{\sigma} \mu_{jk}\right) b_k. \end{aligned}$$

Logo, $(A_{fg})_{ik} = \left(A_f^{\sigma} A_g\right)_{ik}$. Assim $A_{fg} = A_f^{\sigma} A_g$.

Agora,

$$I_n = A_1 = A_{g^{-1}g} = A_{g^{-1}}^{\sigma} A_g.$$

Logo, $A_{g^{-1}}^{\sigma} = A_g^{-1}$. □

Precisamos lembrar, da teoria de grupos, a definição de subgrupo característico. Seja G um grupo e $\operatorname{Aut}(G)$ o seu grupo de automorfismos. Um subgrupo H de G é *característico* se este é um subgrupo invariante pelo grupo $\operatorname{Aut}(G)$. Por exemplo, o centro e o subgrupo derivado de um grupo são subgrupos característicos. Com isso em mente vamos mostrar o seguinte lema.

Lema 1.2.3. *O grupo* $\mathrm{SL}(n, q)$ *é um subgrupo característico de* $\mathrm{GL}(n, q)$. *Consequentemente* $\mathrm{SL}(n, q) \trianglelefteq \Gamma\mathrm{L}(n, q)$.

Demonstração. Seja $G = \mathrm{GL}(n, q)$. No caso $(n, q) = (2, 2)$ temos $\mathrm{SL}(2, 2) = G$. Logo, $\mathrm{SL}(2, 2)$ é um subgrupo característico de G. Sendo assim, suponhamos que $(n, q) \neq (2, 2)$.

Desde que $\mathrm{SL}(n, q) \leq G$ se tem $\mathrm{SL}(n, q)' \leq G'$. E como $G/\mathrm{SL}(n, q) \cong \mathbb{F}_q^{\times}$, temos que $G' \leq \mathrm{SL}(n, q)$. Assumamos primeiro que $(n, q) \neq (2, 3)$. Por [13, Teorema 1.7] e [13, Corolário 1.8], temos que $\mathrm{SL}(n, q)' = \mathrm{SL}(n, q)$. De onde $\mathrm{SL}(n, q) = \mathrm{SL}(n, q)' \leq G' \leq \mathrm{SL}(n, q)$, é dizer, $G' = \mathrm{SL}(n, q)$. Assim, neste caso, $\mathrm{SL}(n, q)$ é um subgrupo característico de G. Para o caso $(n, q) = (2, 3)$ mostramos também, que $\mathrm{SL}(2, 3) = G'$. Para isso, somente resta mostrar que $\mathrm{SL}(2, 3) \leq G'$. Pelo lema 1.2.1 as transvecções geram $\mathrm{SL}(2, 3)$, e por [13, proposição 1.6], toda transvecção é conjugada a uma na forma

$$\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix},$$

com $a \in \mathbb{F}_3$. Então, desde que

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a/2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a/2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix},$$

toda transveção está em G', de onde segue que $\mathrm{SL}(2,3) \leq G'$. Logo, $G' = \mathrm{SL}(2,3)$. Assim, $\mathrm{SL}(2,3)$ é um subgrupo característico de G.

Agora, desde que $\mathrm{GL}(n,q) \trianglelefteq \Gamma\,\mathrm{L}(n,q)$, para cada $f \in \Gamma\,\mathrm{L}(n,q)$ se tem que a aplicação $\psi_f : \mathrm{GL}(n,q) \to \mathrm{GL}(n,q)$, definida por $g \mapsto f^{-1}gf$, é um automorfismo de $\mathrm{GL}(n,q)$. Como $\mathrm{SL}(n,q)$ é um subgrupo característico de $\mathrm{GL}(n,q)$, ele é invariante, em particular, pelo grupo $\{\psi_f \mid f \in \Gamma\,\mathrm{L}(n,q)\}$. Assim, temos que $f^{-1}\,\mathrm{SL}(n,q)f \leq \mathrm{SL}(n,q)$, para cada $f \in \Gamma\,\mathrm{L}(n,q)$. Logo, $\mathrm{SL}(n,q) \trianglelefteq \Gamma\,\mathrm{L}(n,q)$. $\square$

O seguinte lema determina explicitamente o centro e o centralizador de alguns grupos descritos anteriormente. Nós precisaremos posteriormente desta determinação. A demonstração que reproduzimos aqui pode ser encontrada em muitos textos que tratam de grupos clássicos. Sugerimos, por exemplo, [14, 3.2.6 p. 73].

Lema 1.2.4.

i) $C_{\Gamma\,\mathrm{L}(n,q)}\,(\mathrm{SL}(n,q)) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^\times\} = C_{\mathrm{GL}(n,q)}(\mathrm{SL}(n,q)) = Z(\mathrm{GL}(n,q))$.

ii) $Z(\mathrm{SL}(n,q)) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q$ *e* $\lambda^n = 1\}$.

Demonstração.

i) É claro que $\{\lambda I_n \mid \lambda \in \mathbb{F}_q^\times\} \subseteq C_{\Gamma\mathrm{L}(n,q)}\,(\mathrm{SL}(n,q))$. Para a outra inclusão, seja g uma aplicação semilinear relativa a σ que está em $C_{\Gamma\mathrm{L}(n,q)}\,(\mathrm{SL}(n,q))$, então $gf = fg$ para toda $f \in \mathrm{SL}(n,q)$. Logo, $A_{gf} = A_{fg}$, e aplicando o lema 1.2.2 temos $A_g A_f = A_f^\sigma A_g$. O que devemos mostrar é, primeiro que A_g é um múltiplo da identidade e segundo, que g é linear, isto é, $\sigma = 1$.

Para todo $i \neq j$, a matriz $I_n + E_{ij}$ está em $\mathrm{SL}(n,q)$, donde $E_{ij} = (e_{kl})$ é a (i,j)-ésima matriz elementar, isto é, a matriz com 1 na entrada (i,j) e zero em qualquer outra. Além disso $(I_n + E_{ij})^\sigma = I_n + E_{ij}$, o que implica $(I_n + E_{ij})\,A_g = A_g\,(I_n + E_{ij})$, e assim $E_{ij}A_g = A_g E_{ij}$. Se $A_g = (g_{ij})$, temos

$$e_{kj}g_{jl} = \sum_{s=1}^{n} e_{ks}g_{sl} = (E_{ij}A_g)_{kl} = (A_g E_{ij})_{kl} = \sum_{s=1}^{n} g_{ks}e_{sl} = g_{ki}e_{il},$$

Assim, se $k = i$ e $l = j$, então $g_{ii} = g_{jj}$, para $i \neq j$; e se $l = i = k$ se tem $g_{ji} = 0$ para $j \neq i$. Se $\lambda = g_{ii}$, então $A_g = \lambda I_n$. Resta mostrar que $\sigma = 1$. Desde que $A_g = \lambda I_n$ e $A_g A_f = A_f^\sigma A_g$ temos que $A_f = A_f^\sigma$, para toda matriz $A_f \in \mathrm{SL}(n,q)$. Logo, $\sigma = 1$. Assim, $C_{\Gamma\mathrm{L}(n,q)}(\mathrm{SL}(n,q)) \subseteq \{\lambda I_n \mid \lambda \in \mathbb{F}_q^\times\}$.

A próxima igualdade é clara, desde que $\{\lambda I_n \mid \lambda \in \mathbb{F}_q^\times\} \subseteq \mathrm{GL}(n,q)$.

Para a última igualdade notemos que $\{\lambda I_n \mid \lambda \in \mathbb{F}_q^\times\}$ está claramente contido em $Z(\mathrm{GL}(n,q))$. Para a inclusão recíproca observamos que

$$Z(\mathrm{GL}(n,q)) \subseteq C_{\mathrm{GL}(n,q)}(\mathrm{SL}(n,q)) = C_{\Gamma\mathrm{L}(n,q)}(\mathrm{SL}(n,q)).$$

iii) Temos que

$$\begin{aligned} Z(\mathrm{SL}(n,q)) &= C_{\mathrm{SL}(n,q)}(\mathrm{SL}(n,q)) \\ &= C_{\Gamma\mathrm{L}(n,q)}(\mathrm{SL}(n,q)) \cap \mathrm{SL}(n,q) \\ &= \{\lambda I_n \mid \lambda \in \mathbb{F}_q^\times\} \cap \mathrm{SL}(n,q) \\ &= \{\lambda I_n \mid \lambda^n = 1\}. \end{aligned}$$

□

O grupo $\mathrm{P}\Gamma\mathrm{L}(n,q) = \Gamma\mathrm{L}(n,q)/Z(\mathrm{GL}(n,q))$ é chamado *grupo semilinear projetivo.* Notemos a sutil diferença com o grupo linear projetivo: $\mathrm{P}\Gamma\mathrm{L}(n,q)$ não foi definido por $\Gamma\mathrm{L}(n,q)/Z(\Gamma\mathrm{L}(n,q))$, como no caso linear, a razão está fora do contexto deste trabalho. Para nossos fins vamos só aceitar sem explicação esta definição.

Como, pelo lema 1.2.3, $\mathrm{SL}(n,q) \trianglelefteq \Gamma\mathrm{L}(n,q)$, podemos definir o homomorfismo

$$F : \Gamma\mathrm{L}(n,q) \to \mathrm{Aut}(\mathrm{SL}(n,q)),$$

dado por $(f)F : g \mapsto f^{-1}gf$. O núcleo de F é $C_{\Gamma\mathrm{L}(n,q)}(\mathrm{SL}(n,q)) = Z(\mathrm{GL}(n,q))$. Desta forma podemos considerar a $\mathrm{P}\Gamma\mathrm{L}(n,q) = \Gamma\mathrm{L}(n,q)/Z(\mathrm{GL}(n,q))$ como um subgrupo de $\mathrm{Aut}(\mathrm{SL}(n,q))$. A seguinte proposição descreve $\mathrm{Aut}(\mathrm{SL}(n,q))$ em termos de $\mathrm{P}\Gamma\mathrm{L}(n,q)$.

Proposição 1.2.5 ([15], Lema 1.5). *Seja n um inteiro positivo e q uma potência de primo. Então:*

i) Se $n = 2$, $\mathrm{Aut}(\mathrm{SL}(n,q)) = \mathrm{P}\Gamma\mathrm{L}(n,q)$.

ii) Se $n \geq 3$, $\mathrm{Aut}(\mathrm{SL}(n,q)) = \mathrm{P}\Gamma\mathrm{L}(n,q) \rtimes \langle\phi\rangle$.

Onde $\phi : \mathrm{SL}(n,q) \to \mathrm{SL}(n,q)$ é o automorfismo definido por $x\phi = (x^{-1})^t$.

1.3 O normalizador de GL(n, q) em Sym$(V^{\times})$

Vamos agora focar no grupo de automorfismos de $\mathrm{GL}(n, q)$. Não pretendemos fazer um estudo completo deste grupo, nem dar uma determinação dele. Nos só precisamos entender o normalizador de $\mathrm{GL}(n, q)$ em $\mathrm{Sym}(V^{\times})$, onde $V = \mathbb{F}_q^n$. Para isto é preciso observar que tanto $\Gamma\mathrm{L}(n, q)$, como $\mathrm{GL}(n, q)$, permutam os elementos de $V^{\times}$, e assim podem ser considerados como subgrupos de $\mathrm{Sym}(V^{\times})$.

O nosso principal objetivo, nessa seção, será demonstrar o seguinte teorema:

Teorema 1.3.1. *Para $n \geq 2$ se tem que $N_{\mathrm{Sym}(V^{\times})}(\mathrm{GL}(n, q)) = \Gamma\,\mathrm{L}(n, q)$.*

Para isso precisamos de alguns resultados, que são aplicações da seção 1.1 e que mostraremos ao longo da seção.

Antes de continuar com esta seção vamos introduzir a notação a ser usada na mesma. Vamos fixar um inteiro $n \geq 2$, e uma potência q de algum primo p. Com isso, V denotará o espaço vetorial $\mathbb{F}_q^n$ sobre $\mathbb{F}$, e vamos assumir que $\{b_1, ..., b_n\}$ é uma base de V. Além disso, vamos denotar por G o grupo $\mathrm{GL}(n, q)$ e por N o normalizador de G em $\mathrm{Sym}(V^{\times})$.

O nosso plano específico é determinar primeiro o centralizador de G em $\mathrm{Sym}(V^{\times})$, e depois mostrar que $\mathrm{Im}\Psi = \mathrm{P}\Gamma\mathrm{L}(n, q)$, onde $\Psi : N \to \mathrm{Aut}(G)$ é o homomorfismo que está dado pela conjugação por elementos de N, isto é, $(n)\Psi : g \mapsto n^{-1}gn$. O teorema 1.3.1 vai ser uma consequência destes resultados.

Consideremos o grupo G como um subgrupo de $\mathrm{Sym}(V^{\times})$. Com a ação natural este grupo é transitivo. Para ver isto dados $u, v \in V^{\times}$ quaisquer, encontramos uma transformação linear invertível $g : V \to V$ tal que $ug = v$.

Da álgebra linear temos que existem $\{u = u_1, u_2, \cdots, u_n\}$ e $\{v = v_1, v_2, \cdots, v_n\}$ bases de V e uma única transformação linear invertível $g : V \to V$ tal que $u_i g = v_i$ para todo i, em particular $ug = v$. Logo, G é transitivo.

O estabilizador G_{b_1}, de b_1, é o conjunto $G_{b_1} = \{g \in G \mid b_1 g = b_1\}$, ou seja, o conjunto de todas as matrizes invertíveis da forma

$$g = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix}.$$

Vamos focar a nossa atenção, só por pouco tempo, no normalizador $N_G(G_{b_1})$, de G_{b_1} em G.

Lema 1.3.2. *Se tem que*

$$N_G(G_{b_1}) = \left\{ g = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix} \in G \mid a_{11} \in \mathbb{F}_q^{\times} \right\}.$$

Como consequência, $N_G(G_{b_1})/G_{b_1} \cong \mathbb{F}_q^{\times}$.

Demonstração. Seja

$$K = \left\{ g = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix} \in G \mid a_{11} \in \mathbb{F}_q^{\times} \right\}.$$

A aplicação $K \to \mathbb{F}_q^{\times}$, definida por $(a_{ij}) \mapsto a_{11}$, é um homomorfismo sobrejetivo, cujo núcleo é G_{b_1}. Assim temos que G_{b_1} é normal em K, o que implica $K \leq N_G(G_{b_1})$. Além disso $K/G_{b_1} \cong \mathbb{F}_q^{\times}$.

Basta mostrar $N_G(G_{b_1}) \leq K$. Seja $\mathrm{Fix}(G_{b_1}) = \{v \in V \mid v = vg \text{ para todo } g \in G_{b_1}\}$. Vamos mostrar que $\mathrm{Fix}(G_{b_1}) = \{\alpha b_1 \mid \alpha \in \mathbb{F}_q\} = \langle b_1 \rangle$. Seja $h_{i1} = I_n + E_{i1}$, onde $E_{i1} = (e_{kl})$ é a $(i,1)$-ésima matriz elementar. Para todo $i \geq 2$ se tem que $h_{i1} \in G_{b_1}$. Se $v = (v_1, ..., v_n) \in \mathrm{Fix}(G_{b_1})$ então $v(I_n + E_{i1}) = v$ para todo $i \geq 2$. Logo, multiplicando temos

$$(v_1 + v_i, v_2, ..., v_n) = v(I_n + E_{i1}) = v = (v_1, v_2, ..., v_n)$$

para todo $i \geq 2$. Assim, $v_1 + v_i = v_1$, o que implica que $v_i = 0$ para todo $i \geq 2$. Então, $v = (v_1, 0, ..., 0)$, e $\mathrm{Fix}(G_{b_1}) \subseteq \{\alpha b_1 \mid \alpha \in \mathbb{F}_q\} = \langle b_1 \rangle$. Por outro lado, é claro que $\langle b_1 \rangle \subseteq \mathrm{Fix}(G_{b_1})$, assim $\mathrm{Fix}(G_{b_1}) = \langle b_1 \rangle$. Agora, $\mathrm{Fix}(G_{b_1})$ é $N_G(G_{b_1})$-invariante. De fato, se $n \in N_G(G_{b_1})$ e $g \in G$, $g^{n^{-1}} \in G_{b_1}$, e se $v \in \mathrm{Fix}(G_{b_1})$ então teremos $vng = \left(vg^{n^{-1}}\right)n = vn$. Assim temos que $N_G(G_{b_1})$ preserva o subespaço $\langle b_1 \rangle$, o que por sua vez diz que

$N_G(G_{b_1}) \leq K$. As duas anteriores inclusões dizem que

$$N_G(G_{b_1}) = K = \left\{ g = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix} \in G \mid a_{11} \in \mathbb{F}_q^\times \right\}.$$

Logo, $N_G(G_{b_1})/G_{b_1} = K/G_{b_1} \cong \mathbb{F}_q^\times$. □

Lema 1.3.3. *Se verifica que* $C_{\mathrm{Sym}(V^\times)}(G) = Z(G)$.

Demonstração. Pelo corolário 1.1.3 (i) temos que

$$C_{\mathrm{Sym}(V^\times)}(G) \cong N_G(G_{b_1})/G_{b_1},$$

então, pelo lema 1.3.2, $C_{\mathrm{Sym}(V^\times)}(G) \cong \mathbb{F}_q^\times$, o que implica que $|C_{\mathrm{Sym}(V^\times)}(G)| = q-1$. Agora, pelo lema 1.2.4, $Z(G) = \{\lambda I : \lambda \in \mathbb{F}_q^\times\}$, o que implica $|Z(G)| = q-1$. É claro que $C_{\mathrm{Sym}(V^\times)}(G) \geq Z(G)$, isto implicará $C_{\mathrm{Sym}(V^\times)}(G) = Z(G)$. □

Consideremos o homomorfismo $\Psi : N \to \mathrm{Aut}(G)$, onde $(n)\Psi : g \mapsto n^{-1}gn$. Dado $\sigma \in \mathrm{Aut}(G)$ o lema 1.1.4 diz que $\sigma \in \mathrm{Im}\Psi$ se, e somente se, $(G_v)\sigma$ é um estabilizador para qualquer $v \in V^\times$, ou seja, $\mathrm{Im}\Psi$ permuta os estabilizadores de G.

Neste ponto vamos definir um homomorfismo $\Phi : \mathrm{Im}\Psi \to \mathrm{Aut}(\mathrm{SL}(n,q))$, por $\sigma\Phi = \sigma|_{\mathrm{SL}(n,q)}$. Este homomorfismo está bem definido, já que pelo lema 1.2.3 temos que $\mathrm{SL}(n,q)$ é um subgrupo característico de G. Agora surge uma pergunta natural: Qual é o núcleo deste homomorfismo? O resultado que segue vai responder esta pergunta, a demonstração dele é longa e está cheia de detalhes técnicos, mas é uma aplicação muito boa da teoria de permutações e grupos lineares até agora exposta.

Proposição 1.3.4. *Seja* $\Phi : \mathrm{Im}\,\Psi \to \mathrm{Aut}(\mathrm{SL}(n,q))$ *o homomorfismo definido acima, então* $\ker\Phi = \{1\}$. *Isto é,* Φ *é injetiva.*

Demonstração. Consideremos $\sigma \in \ker\Phi$ arbitrário, e lembremos da igualdade (1.2) que $\mathrm{GL}(n,q) = \mathrm{SL}(n,q) \rtimes M$, onde $M = \{\delta_w : w \in \mathbb{F}_q^\times\}$ e δ_w é dada por (1.1). Então, se $x \in \mathrm{SL}(n,q)$ temos que $x\sigma = x$. Seja δ_w em M, $w \neq 1$, e suponhamos que $\delta_w\sigma = \delta'$, onde $\delta' \in \mathrm{GL}(n,q)$. Para que Φ seja injetiva a nossa obrigação é mostrar que $\delta_w\sigma = \delta_w$.

Desde que M normaliza $\mathrm{SL}(n,q)$ segue que $x^{\delta_w} = \delta_w^{-1}x\delta_w \in \mathrm{SL}(n,q)$, para todo $x \in \mathrm{SL}(n,q)$, e então $x^{\delta_w} = \left(x^{\delta_w}\right)\sigma = x^{\delta_w\sigma}$, isto diz que $\delta_w^{-1}(\delta_w\sigma) \in C_{\mathrm{GL}(n,q)}(\mathrm{SL}(n,q))$.

O lema 1.2.4 diz que $C_{\mathrm{GL}(n,q)}\left(\mathrm{SL}\left(n,q\right)\right) = Z\left(\mathrm{GL}\left(n,q\right)\right)$, e então $\delta_w^{-1}\left(\delta_w\sigma\right) \in Z\left(\mathrm{GL}\left(n,q\right)\right)$. Logo,

$$\delta_w\sigma = \delta_w z,$$

e se $z = \alpha I_n$, então

$$\delta_w\sigma = \begin{pmatrix} w\alpha & 0 & ... & 0 \\ 0 & \alpha & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & \alpha \end{pmatrix}.$$

Seja $U = \langle b_2, ..., b_n\rangle - \{0\}$, temos que $|U| = q^{n-1} - 1$. Consideremos o estabilizador pontual de U, $G_{\{U\}} = \bigcap_{u\in U} G_u$. Desde que

$$\delta_w = \begin{pmatrix} w & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & 1 \end{pmatrix},$$

temos que $\delta_w \in G_{\{U\}}$. Como G é transitivo vale o lema 1.1.4, e assim σ permuta estabilizadores; e dai existe um subconjunto $W \subseteq V^{\times}$, $|W| = q^{n-1} - 1$ (W não necessariamente é um subespaço de V), tal que $\delta_w\sigma \in G_{\{W\}} = \bigcap_{w\in W} G_w$. Aqui temos dois casos:

i) Existe um subespaço $\overline{W}$ de V de dimensão $n-1$, tal que $W \subseteq \overline{W}$.

ii) $W \subsetneq \overline{W}$ para todo subespaço $\overline{W}$ de V de dimensão $n-1$.

Se acontece ii) então teremos que $\langle W\rangle = V$, o que implicará $\delta_w\sigma \in \bigcap_{v\in V} G_v = \{1\}$. Logo, vamos ter $\delta_w\sigma = 1$, o que é uma contradição aos fatos de σ ser um automorfismo e $\delta_w \neq 1$.

Então, temos que aceitar i). Assim $W = \overline{W}^{\times}$, e $\delta_w\sigma \in G_{\{\overline{W}^{\times}\}} = \bigcap_{w\in\overline{W}^{\times}} G_w$. Isto diz que na matriz

$$\delta_w\sigma = \begin{pmatrix} w\alpha & 0 & ... & 0 \\ 0 & \alpha & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & \alpha \end{pmatrix},$$

existem pelo menos $n-1$ elementos da diagonal que são 1. Aqui vamos ter dois casos:

i) Se $n \geq 3$. Então pelo menos dois elementos da diagonal são 1, assim $\alpha = 1$, e $\delta_w\sigma = \delta_w$. Isto, junto com $x\sigma = x$ para todo $x \in \mathrm{SL}\left(n,q\right)$, diz que $\sigma = 1$.

ii) Se $n = 2$. Neste caso temos que pelo menos um elemento na diagonal é 1. Se $\mathbb{F}_q = \mathbb{F}_2$, se tem que $\delta_w = 1$, e neste caso $\delta_w\sigma = \delta_w$. Suponhamos então que $|\mathbb{F}_q| \geq 3$. Sendo assim, a matriz em questão fica

$$\delta_w\sigma = \begin{pmatrix} w\alpha & 0 \\ 0 & \alpha \end{pmatrix}.$$

Vejamos, se $w\alpha = 1$ então a $\alpha = w^{-1}$ e assim

$$\delta_w\sigma = \begin{pmatrix} 1 & 0 \\ 0 & w^{-1} \end{pmatrix},$$

Logo, como

$$\begin{pmatrix} w^{-1} & 0 \\ 0 & w \end{pmatrix}\begin{pmatrix} w & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix},$$

temos

$$\begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix}\sigma = \begin{pmatrix} w^{-1} & 0 \\ 0 & 1 \end{pmatrix},$$

isto desde que $\sigma|_{\mathrm{SL}(n,q)} = 1$. Agora, $\sigma \in \mathrm{Im}\Psi$ e pelo lema 1.1.4, σ permuta estabilizadores. Suponhamos que V tem como base $\{b_1, b_2\}$, e consideremos

$$\begin{aligned} G_{b_1} &= \left\{ \begin{pmatrix} 1 & 0 \\ x & y \end{pmatrix} \mid x \in \mathbb{F} \text{ e } y \in \mathbb{F}^\times \right\} \\ &= \left\langle \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & y \end{pmatrix} \mid x \in \mathbb{F} \text{ e } y \in \mathbb{F}^\times \right\rangle. \end{aligned}$$

Logo,

$$\begin{aligned} (G_{b_1})\,\sigma &= \left\langle \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}, \begin{pmatrix} y^{-1} & 0 \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{F} \text{ e } y \in \mathbb{F}^\times \right\rangle \\ &= \left\{ \begin{pmatrix} y^{-1} & 0 \\ xy^{-1} & 1 \end{pmatrix} \mid x \in \mathbb{F} \text{ e } y \in \mathbb{F}^\times \right\} \\ &= \left\{ \begin{pmatrix} y & 0 \\ x & 1 \end{pmatrix} \mid x \in \mathbb{F} \text{ e } y \in \mathbb{F}^\times \right\}, \end{aligned}$$

que não é um estabilizador. De fato, seja $v = (v_1, v_2)$ tal que $vg = v$ para todo $g \in (G_{b_1})\sigma$. Então, em particular

$$(v_1, v_2)\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = (v_1, v_2).$$

Logo, $v_2 = 0$. Assim, $v = (v_1, 0)$. Agora, desde que $|\mathbb{F}_q| \geq 3$ podemos escolher $y \in \mathbb{F}_q^{\times}$ com $y \neq 1$ e com isso considerar a matriz

$$h = \begin{pmatrix} y & 0 \\ 1 & 1 \end{pmatrix}.$$

Temos que $h \in (G_{b_1})\,\sigma$, então $(v_1, 0)\,h = (v_1, 0)$. Multiplicando temos $v_1 y = v_1$, o que implica $v_1\,(y-1) = 0$, e desde que $y \neq 1$ segue $v_1 = 0$. Logo $v = (0,0)$, o que diz que não existe vetor $v \in V^{\times}$ tal que $(G_{b_1})\,\sigma = G_v$. O que é uma contradição ao lema 1.1.4, que surgiu de supor que $w\alpha = 1$. Assim, temos que ter $\alpha = 1$ e então $\delta_w \sigma = \delta_w$.

Em qualquer caso $\delta_w \sigma = \delta_w$. Isto junto com $\sigma|_{\mathrm{SL}(n,q)} = 1$ nos dá $\ker \Phi = \{1\}$. Assim, Φ é injetiva. $\square$

A seguinte proposição será o último resultado antes de demonstrar o teorema principal, o qual enunciamos na introdução desta seção. Este teorema será uma consequêcia quase direta ao aplicar os resultados anteriores. A prova desta proposição ilustra bem como usar a proposição 1.2.5 para obter $\mathrm{Im}\,\Psi$.

Proposição 1.3.5. *Temos que* $\mathrm{Im}\,\Psi = \mathrm{P}\,\Gamma\,\mathrm{L}\,(n,q)$.

Demonstração. Pela proposição 1.3.4 a aplicação $\Phi : \mathrm{Im}\Psi \to \mathrm{Aut}(\mathrm{SL}(n,q))$ é injetiva, logo $\mathrm{Im}\Psi \leq \mathrm{Aut}(\mathrm{SL}\,(n,q))$.

Como $G \trianglelefteq \Gamma\mathrm{L}\,(n,q)$, segue que $\Gamma\mathrm{L}\,(n,q) \leq N$. O lema 1.3.3 diz que $\ker\Psi = C_{\mathrm{Sym}(V^{\times})}(G) = Z\,(G)$, e segue

$$\mathrm{P}\,\Gamma\,\mathrm{L}\,(n,q) = \frac{\Gamma\,\mathrm{L}\,(n,q)}{Z\,(G)} \leq \frac{N}{\ker\Psi} = \mathrm{Im}\Psi \leq \mathrm{Aut}(\mathrm{SL}(n,q)). \tag{1.4}$$

Agora, vamos usar a proposição 1.2.5. Sendo assim, temos dois casos:

i) Se $n = 2$, $\mathrm{Aut}(\mathrm{SL}\,(n,q)) = \mathrm{P}\Gamma\mathrm{L}\,(n,q)$. Logo, a desigualdade anterior implica $\mathrm{P}\Gamma\mathrm{L}\,(n,q) = \mathrm{Im}\Psi$.

ii) Se $n \geq 3$, $\mathrm{Aut}(\mathrm{SL}\,(n,q)) = \mathrm{P\Gamma L}\,(n,q) \rtimes \langle \phi \rangle$, onde $\phi : x \mapsto x^{-t}$. Pretendemos mostrar que neste caso também temos $\mathrm{P\Gamma L}\,(n,q) = \mathrm{Im}\Psi$. Como por (1.4) tenemos que $\mathrm{P\Gamma L}\,(n,q) \leq \mathrm{Im}\,\Psi$, basta mostrar que $\phi \notin \mathrm{Im}\Psi$ para ter $\mathrm{Im}\Psi \leq \mathrm{P\Gamma L}\,(n,q)$, e isto junto com $\mathrm{P\Gamma L}\,(n,q) \leq \mathrm{Im}\Psi$ dará $\mathrm{Im}\Psi = \mathrm{P\Gamma L}\,(n,q)$. Então, para terminar a demonstração só resta verificar que $\phi \notin \mathrm{Im}\Psi$.

O estabilizador

$$G_{b_1} = \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix} \in G \right\},$$

é um grupo. Logo ele é fechado para inversos. Se assumirmos que $\phi \in \mathrm{Im}\Psi$, então pelo lema 1.1.4, ϕ permuta estabilizadores, isto é,

$$\begin{aligned} (G_{b_1})\,\phi &= \left(G_{b_1}^{-1}\right)^t \\ &= (G_{b_1})^t \\ &= \{g^t \mid g \in G_{b_1}\} \\ &= \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix} \in G \right\}, \end{aligned}$$

é estabilizador de algum $v \in V^\times$. Mostremos que isso não é possível. Para isso é suficiente mostrar que não existe $v \in V^\times$ tal que $G_v = G_{b_1}^t$. Seja

$$\mathrm{Fix}\left(G_{b_1}^t\right) = \{v \in V \mid vg = v \text{ para todo } g \in G_{b_1}^t\}.$$

Se

$$g = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

temos que $g \in G_{b_1}^t$. Então, se $v = (v_1, v_2, ..., v_n) \in \mathrm{Fix}\big(G_{b_1}^t\big)$, devemos ter $vg = v$. Multiplicando temos

$$(v_1, v_1 + v_2, v_2 + v_3, ..., v_{n-1} + v_n) = (v_1, v_2, ..., v_n)\,,$$

o que implica $0 = v_1 = v_2 = \cdots = v_{n-1}$, é dizer, se $v \in \mathrm{Fix}\big(G_{b_1}^t\big)$, então $v = (0, 0, ..., 0, v_n)$. Agora, desde que $n \geq 3$, podemos considerar a matriz $h = I_n + E_{n2}$, onde E_{n2} é a $(n, 2)$-ésima matriz elementar. Se tem que h está em $G_{b_1}^t$. Então,

$$(0, v_n, 0, ..., 0, v_n) = (0, 0, ..., 0, v_n)\, h = (0, 0, ..., 0, v_n)\,,$$

de onde temos $v_n = 0$. Então $v = 0$, e temos mostrado assim que $\mathrm{Fix}\big(G_{b_1}^t\big) = \{0\}$. Logo, não existe $v \in V^{\times}$ tal que $vg = v$ para todo $g \in G_{b_1}^t$, o que vai implicar que não existe $v \in V^{\times}$ tal que $G_v = G_{b_1}^t$.

Em qualquer caso temos $\mathrm{Im}\Psi = \mathrm{P\Gamma L}\,(n, q)$. □

Demonstração do Teorema 1.3.1 Da definição do homomorfismo Ψ segue que $\ker\Psi = C_{\mathrm{Sym}(V^{\times})}(G)$. O lema 1.3.3 diz que $C_{\mathrm{Sym}(V^{\times})}\,(G) = Z(G)$, e da proposição 1.3.5 temos $\mathrm{Im}\Psi = \mathrm{P\Gamma L}(n, q)$. Com isso temos as seguintes igualdades:

$$\frac{N}{Z\,(G)} = \frac{N}{C_{\mathrm{Sym}(V^{\times})}\,(G)} = \frac{N}{\ker\Psi} \cong \mathrm{Im}\Psi = \mathrm{P\Gamma L}\,(n, q) = \frac{\Gamma\mathrm{L}\,(n, q)}{Z\,(G)}.$$

Como $\Gamma\mathrm{L}(n, q) \leq N$, podemos deduzir $N = \Gamma\mathrm{L}(n, q)$.

Assim, temos demostrado o teorema 1.3.1 e com isto nós terminamos esta seção.

1.4 Grupos de Singer

Nesta seção o foco principal será estudar os grupos cíclicos de maior ordem que agem irredutivelmente num espaço vetorial.

Dado um espaço vetorial V e um grupo G agindo em V, via a ação $V \times G \to V$, $(v, g) \mapsto vg$, dizemos que um subespaço W de V é *G-invariante* se $(W)g \subseteq W$ para todo $g \in G$. Se os únicos subespaços G-invariantes são $\{0\}$ e o próprio V então diremos que G age *irredutivelmente* em V. No que segue V denotará um espaço vetorial de dimensão n sobre $\mathbb{F}_q$ e G um subgrupo de $\mathrm{GL}\,(n, q)$. Além disso a ação que consideraremos será a ação natural $V \times G \to V$, dada por $(v, g) \mapsto vg$.

Com a definição acima podemos provar o seguinte lema, o qual dá condiciones suficientes para um grupo não agir irredutivelmente num espaço vetorial.

Lema 1.4.1. *Seja G um subgrupo de $\mathrm{GL}(n,q)$, que possui um p-subgrupo normal não trivial N, onde $q = p^r$ com p primo. Então G não é irredutível em $V = \mathbb{F}_{q^n}$.*

Demonstração. Suponhamos que a ação de G em V seja irredutível. Consideremos

$$\mathrm{Fix}\,(N) = \{v \in V \mid vn = v \text{ para todo } n \in N\}.$$

O conjunto $\mathrm{Fix}(N)$ é claramente um subespaço de V. Além disso, $\mathrm{Fix}(N)$ é G-invariante. De fato, dado $v \in \mathrm{Fix}(N)$ e $g \in G$ temos que $n^{g^{-1}} = gng^{-1} \in N$ para todo $n \in N$ pois N é normal, isto implica que

$$(vg)n = (vn^{g^{-1}})g = vg,$$

para todo $n \in N$. Como G age irredutivelmente em V e N é não trivial temos que $\mathrm{Fix}(N) = \{0\}$. Agora, temos que V é união disjunta de suas órbitas, e pelo teorema 1.1.1 ii), se tem que o tamanho de cada órbita é 1 ou é divisível por p. As órbitas de tamanho 1 são justamente os pontos fixos de N. Então $|V| = |\mathrm{Fix}(N)| + pm = 1 + pm$. Desde que $p \mid |V|$ segue que $p \mid |\mathrm{Fix}(N)| = 1$, o que é uma contradição. $\square$

Vamos precisar do seguinte lema, o qual dá a estrutura de um subgrupo abeliano irredutível de $\mathrm{GL}\,(n,q)$. Para uma demonstração do mesmo sugerimos [16, Satz 3.10 p. 165].

Lema 1.4.2. *Seja V um espaço vetorial de dimensão n sobre $\mathbb{F}_q$. Se A é um subgrupo abeliano de $\mathrm{GL}\,(n,q)$ que age irredutivelmente em V, então A é um grupo cíclico e além disso $|A| \equiv 0 \pmod{q^n - 1}$. Identificando adequadamente V com o espaço vetorial $\mathbb{F}_{q^n}$ temos que A age da seguinte forma:*

$$xa = \lambda_a x,$$

onde $x \in \mathbb{F}_{q^n}$, $a \in A$ e $\lambda_a \in \mathbb{F}_{q^n}^{\times}$. Se $A = \langle a_0 \rangle$ então teremos que $\mathbb{F}_{q^n} = \mathbb{F}_q(\lambda_{a_0})$. Além disso, o número n é o menor número natural tal que $|A| \equiv 0 \pmod{q^n - 1}$.

Vamos identificar o espaço vetorial V com $\mathbb{F}_{q^n}$ como no lema, e para cada α seja $\mu_\alpha : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ o homomorfismo definido por $x \mapsto \alpha x$. Temos que $\mu_\alpha \in \mathrm{End}(V)$, e que as aplicações μ_α comutam com todos os elementos de A. De fato, isto é uma consequência do lema anterior, já que a ação de cada elemento de A é a multiplicação por um escalar. Vamos chamar de centralizador de A em $\mathrm{End}(V)$ ao conjunto de todos os endomorfismos de V que comutam com A. Note que $\mathrm{End}(V)$ não necessariamente é um grupo.

Corolário 1.4.3. *Se A é como no lema anterior e C é o centralizador de A em* $\mathrm{End}_{\mathbb{F}_q}(V,V)$, *então $C = \{\mu_\alpha \mid \alpha \in \mathbb{F}_{q^n}\}$. Consequentemente $C \cong \mathbb{F}_{q^n}$.*

Demonstração. Pelo lema de Schur, ver [16, Lema 10.5, p. 56] temos que $C \leq \mathrm{End}_{\mathbb{F}_q}(V)$ é um anel de divisão, que é finito. Logo, C é um corpo. Com a ação natural teremos que V é um C-espaço vetorial, daqui temos $q^n = |V| \geq |C|$. Agora, vamos identificar o espaço vetorial V com $\mathbb{F}_{q^n}$ como no lema anterior. Seja

$$B = \{\mu_\alpha \mid \alpha \in \mathbb{F}_{q^n}\}.$$

Temos que $B \leq C$, para ver isto seja $x \in \mathbb{F}_{q^n}$ e $a \in A$, então $x\mu_\alpha a = (\alpha x)a = \lambda_a \alpha x = \alpha\lambda_a x = xa\mu_\alpha$, assim $\mu_\alpha a = a\mu_\alpha$. Logo, $q^n = |B| \leq |C|$, e isto junto com a desigualdade anterior dá $|C| = q^n$ e $C = B$. O fato $C \cong \mathbb{F}_q^n$ é imediato desde que a aplicação $\alpha \mapsto \mu_\alpha$ é um isomorfismo. □

Outro corolário do lema anterior é o seguinte.

Corolário 1.4.4. *Seja A um subgrupo cíclico de* $\mathrm{GL}(n,q)$ *com ordem r, onde r é primo. Então A age irredutivelmente em V se, e somente se, $r \mid q^n - 1$ e $r \nmid q^d - 1$ para todo inteiro positivo $d < n$.*

Demonstração. Uma direção é parte do lema anterior.

Para recíproca, assumimos que $r \mid q^n - 1$ e $r \nmid q^d - 1$ para todo inteiro positivo $d < n$. Seja

$$\mathrm{Fix}\,(A) = \{v \in V \mid va = v, \text{ para todo } a \in A\}.$$

Temos que $\mathrm{Fix}(A)$ é um subespaço de V, o que implica $|\mathrm{Fix}\,(A)| = q^i$, para algum i, com $1 \leq i \leq n$. Agora, V é a união disjunta de A-órbitas, e pelo teorema 1.1.1, toda órbita tem tamanho 1 ou r. As órbitas de tamanho 1 são justamente os pontos fixos de A. Então $|V| = |\mathrm{Fix}(A)| + rk$, e segue que $r \mid |V| - |\mathrm{Fix}\,(A)| = q^n - q^i = q^i\,(q^{n-i} - 1)$. A hipótese $r \mid q^n - 1 = |V|$ implica que $r \nmid q^i$, então devemos ter $r \mid q^{n-i} - 1$. Assim, desde que $r \nmid q^d - 1$ para todo $d < n$, temos que $i = 0$. O que implica $\mathrm{Fix}\,(A) = \{0\}$.

Agora, suponhamos que $U \neq \{0\}$ é um subespaço A-invariante, de dimensão m, de V. Como a única órbita de tamanho 1 é $\{0\}$, e U é união disjunta de suas órbitas segue que $q^m = |U| = 1 + rs$, o que implica $r \mid q^m - 1$. Pela hipótese em r, isto obriga a ter $m = n$. Logo, $U = V$. Assim, A age irredutivelmente em V. □

Existe um teorema da teoria de números devido a Zsigmondy, que é muito útil para demonstrar, usando o corolário anterior, que um grupo de um ordem dado é irredutível. Como nós teremos oportunidade de usá-lo enunciaremos este agora. Não daremos uma demonstração deste teorema, já que não está no contexto deste trabalho. Para ver uma prova deste sugerimos por exemplo [2, Teorema 8.3 p. 508].

Teorema 1.4.5 (Teorema de Zsigmondy)**.** *Sejam a e m inteiros maiores do que* 1. *Então, exceto para os casos $m = 2, a = 2^b - 1$ e $m = 6, a = 2$, existe um primo r com as seguintes propriedades:*

i) *r divide $a^m - 1$.*

ii) *r não divide $a^i - 1$ para $i < m$.*

iii) *r não divide m.*

Combinando o corolário 1.4.4 com teorema de Zsigmondy, podemos garantir a existência de grupos cíclicos irredutíveis em $\mathrm{GL}(n, q)$, com exceção de alguns casos.

Definição 1.4.1. Um grupo cíclico de ordem $q^n - 1$ em $\mathrm{GL}(n, q)$ é chamado *grupo de Singer* de $\mathrm{GL}(n, q)$, e um gerador dele é chamado *ciclo de Singer*.

Um exemplo de um grupo de Singer que nós podemos dar é o seguinte:

Exemplo 1.4.6. Se consideramos um subgrupo A de $\mathrm{GL}(n, q)$ como no lema 1.4.2, quer dizer, abeliano e agindo irredutivelmente em V, então

$$C_{\mathrm{GL}(n,q)}(A) = C_{\mathrm{End}(V)}(A) \cap \mathrm{GL}(n, q) = \{\mu_\alpha \mid \alpha \in \mathbb{F}_{q^n}\} \cap \mathrm{GL}(n, q) = \{\mu_\alpha \mid \alpha \in \mathbb{F}_{q^n}^\times\},$$

é um grupo de Singer.

Corolário 1.4.7. *Se G é um subgrupo de um grupo de Singer S de* $\mathrm{GL}(n, q)$ *que age irredutivelmente em V, então $C_{\mathrm{GL}(n,q)}(G) = S$.*

Demonstração. Pelo corolário 1.4.3 $|C_{\mathrm{GL}(n,q)}(G)| = q^n - 1$, e como S é abeliano temos $S \leq C_{\mathrm{GL}(n,q)}(G)$. Logo, $C_{\mathrm{GL}(n,q)}(G) = S$. □

O corolário anterior diz que identificando adequadamente V com o espaço vetorial $\mathbb{F}_{q^n}$, um grupo de Singer pode se considerar como o grupo $\{\mu_\alpha \mid \alpha \in \mathbb{F}_{q^n}^\times\}$, dado no exemplo 1.4.6. Sendo assim, se tem que todo grupo de Singer é isomorfo a $\mathbb{F}_{q^n}^\times$.

Identifiquemos o espaço vetorial V, de dimensão n sobre $\mathbb{F}_q$, com o corpo $\mathbb{F}_{q^n}$. Vamos considerar em $\mathbb{F}_{q^n}$ o automorfismo de Frobenius $\sigma : x \mapsto x^q$. A aplicação σ é $\mathbb{F}_q$-linear, e logo segue que $\sigma \in \mathrm{GL}(n,q)$. Com isto enunciamos o seguinte lema o qual faz parte de [16, Satz 7.3 p. 187].

Lema 1.4.8. *Se G é um subgrupo de um grupo de Singer S de $\mathrm{GL}(n,q)$ que age irredutivelmente em V, então $N_{\mathrm{GL}(n,q)}(G) = S \rtimes \langle\sigma\rangle$.*

Vamos usar os resultados anteriores para dar algumas propriedades dos grupos de Singer, as quais podem ser encontradas em [17].

Antes de continuar vamos introduzir uma notação, que será usada na demonstração da seguinte proposição. Se G é um grupo e p é um primo então $|G|_p$ é a ordem do p-subgrupo de Sylow de G.

Proposição 1.4.9. *Seja H um subgrupo abeliano de $\mathrm{GL}(n,q)$ e S um grupo de Singer de $\mathrm{GL}(n,q)$. Assumamos que a ordem de H divide q^n-1 e que $\mathrm{mcd}(|H|, |\mathrm{GL}(n,q) : S|) = 1$. Então algum conjugado de H está contido em S.*

Demonstração. Seja r um primo dividindo $|H| = m$, e seja T o r-subgrupo de Sylow de H. Como T é um r-grupo em $\mathrm{GL}(n,q)$ temos que existe $R \in \mathrm{Syl}_r(\mathrm{GL}(n,q))$ tal que $T \leq R$. Consideremos agora um elemento x de ordem r em T. Seja L o centralizador de $\langle x\rangle$ em $\mathrm{Hom}_{\mathbb{F}_q}(V,V)$. Desde que

$$|\mathrm{GL}(n,q)| = q^{\binom{n}{2}}(q^n-1)\left(q^{n-1}-1\right)\cdots(q-1),$$

$|\mathrm{GL}(n,q) : S| = q^{\binom{n}{2}}(q^{n-1}-1)\cdots(q-1)$. Por hipótese $\mathrm{mcd}(m, |\mathrm{GL}(n,q) : S|) = 1$, isto implicará que $r \nmid q^i - 1$ para todo inteiro positivo $i < n$. Logo, pelo corolário 1.4.4, $\langle x\rangle$ age irredutivelmente em V, e assim também R age irredutivelmente em V. Logo, pelo corolário 1.4.3, segue que $L \cong \mathbb{F}_{q^n}$, e

$$L^\times = C_{\mathrm{GL}(n,q)}(\langle x\rangle),$$

tem ordem q^n-1. Agora, $x \in T \leq L^\times$, e desde que o grupo H é abeliano teremos $H \leq C_{\mathrm{GL}(n,q)}(\langle x\rangle) = L^\times$.

Afirmamos que R é cíclico. De fato, como $|\langle x\rangle| = r$ e $\langle x\rangle$ age irredutivelmente em V temos que $r \mid q^n-1$ e $r \nmid q^i-1$ para todo inteiro positivo $i < n$. De $r \mid q^n-1$ se tem que $r \nmid q$, já que em caso contrario $r = 1$. Logo, o único fator de $|\mathrm{GL}(n,q)| =$

$q^{\binom{n}{2}}(q^n-1)(q^{n-1}-1)\cdots(q-1)$ que tem como divisor r é $q^n-1=|S|$. Logo, segue imediatamente que $|\mathrm{GL}(n,q)|_r=|S|_r$. O anterior implica que todo r-subgrupo de Sylow de S é um r-subgrupo de Sylow de $\mathrm{GL}(n,q)$. Como S é cíclico, todo r-subgrupo de Sylow de S é cíclico, então todo r-subgrupo de Sylow de $\mathrm{GL}(n,q)$ é cíclico. Assim, R é cíclico. Logo teremos

$$L^{\times}=C_{\mathrm{GL}(n,q)}(\langle x\rangle)=C_{\mathrm{GL}(n,q)}(R).$$

Agora, R é conjugado a algum r-subgrupo de Sylow, que chamaremos de R_1, de S por um elemento de $y\in\mathrm{GL}(n,q)$, isto é, $R^y=R_1$. Pelo lema 1.4.7 temos que $C_{\mathrm{GL}(n,q)}(R_1)=S$. Logo,

$$\left(L^{\times}\right)^y=C_{\mathrm{GL}(n,q)}(R)^y=C_{\mathrm{GL}(n,q)}(R^y)=C_{\mathrm{GL}(n,q)}(R_1)=S,$$

e assim $H^y\leq S$ como queríamos provar. □

Sejam $S_1,\ S_2$ dois grupos de Singer, afirmamos que $|S_1\cap S_2|=q^m-1$. De fato, sejam $\overline{S}_1=S_1\cup\{0\}$ e $\overline{S}_2=S_2\cup\{0\}$, então $\overline{S}_1$ e $\overline{S}_2$ são corpos $\mathbb{F}_{q^n}$. Logo, $\overline{S}_1\cap\overline{S}_2$ é um subcorpo de $\mathbb{F}_{q^n}$, e segue que $|\overline{S}_1\cap\overline{S}_2|=q^m$ para algum divisor m de n. Assim, $|S_1\cap S_2|=q^m-1$, para algum divisor m de n.

Proposição 1.4.10. *Seja S um grupo de Singer de* $\mathrm{GL}(n,q)$. *Então, S é o único subgrupo de Singer de seu normalizador N em* $\mathrm{GL}(n,q)$.

Demonstração. Seja S_1 outro subgrupo de Singer de N. Como S_1 normaliza S temos que $SS_1\leq N$. Pelo lema 1.4.8, $N=S\rtimes\langle\sigma\rangle$, onde $\sigma:x\mapsto x^q$ é o automorfismo de Frobenius de $\mathbb{F}_{q^n}$. Logo, $|N|=n(q^n-1)$. Segue que

$$n(q^n-1)\geq|SS_1|=\frac{|S|\,|S_1|}{|S\cap S|}=\frac{(q^n-1)^2}{|S\cap S_1|},$$

o que implica $|S\cap S_1|\geq(q^n-1)/n$. Assumamos primeiro que n é primo. Afirmamos que neste caso a desigualdade é estrita. Suponhamos, por absurdo, que $|S\cap S_1|=(q^n-1)/n$. Pela observação antes desta proposição, temos que $|S\cap S_1|=q^n-1$ ou $|S\cap S_1|=q-1$. No primeiro caso, se $q^n-1=|S\cap S_1|=(q^n-1)/n$, e segue que $n=1$, o que contradiz a hipótese em n. No segundo caso, se $q-1=|S\cap S_1|=(q^n-1)/n$, então

$$q^{n-1}+q^{n-2}+\cdots+q+1=\frac{q^n-1}{q-1}=n,$$

isto obriga a ter $q=1$, o que contradiz ao fato que q é uma potência de primo.

Logo, temos que $|S \cap S_1| > (q^n - 1)/n$. Como n é primo, se tem $|S \cap S_1| = q^n - 1$. O que implica

$$S_1 = S \cap S_1 = S.$$

Agora suponhamos que n é arbitrário. Se mostramos que $|S \cap S_1| \geq (q^n - 1)/n > q^m - 1$ para todo divisor próprio m de n isto implicará que $|S \cap S_1| = q^n - 1$ o que dará $S = S_1$. Provemos então que $(q^n - 1)/n > q^m - 1$ para todo divisor próprio m de n, e concluamos assim a demonstração. Seja $n = mh$ onde $h \geq 2$ e definamos $m' = n/2$. Então temos que ter $m' = n/2 \geq m > 1$. Por indução podemos mostrar que $2^{m'} + 1 > 2m'$ para $m' > 1$, o que implica $q^{m'} + 1 > 2m'$, desde que $q \geq 2$, e multiplicando ambos lados desta desigualdade por $(q^{m'} - 1)/n$ teremos

$$(q^n - 1)/n = (q^{2m'} - 1)/n = (q^{m'} + 1)(q^{m'} - 1)/n > 2m'(q^{m'} - 1)/n > q^{m'} - 1 \geq q^m - 1.$$

$\square$

Seja V um espaço vetorial de dimensão n/s sobre o corpo $\mathbb{F}_{q^s}$. Logo, V pode ser identificado com $(\mathbb{F}_{q^s})^{n/s} \cong \mathbb{F}_{q^n}$. Assim, V tem dimensão n sobre $\mathbb{F}_q$.

Consideremos o grupo $\mathrm{GL}(n/s, q^s)$, de todas as transformações invertíveis de V em V as quais são $\mathbb{F}_{q^s}$-lineares. Considerando $\mathbb{F}_q$ como um subcorpo de $\mathbb{F}_{q^s}$, temos que toda transformação de V em V que seja $\mathbb{F}_{q^s}$-linear é $\mathbb{F}_q$-linear. Logo, podemos considerar o grupo $\mathrm{GL}(n/s, q^s)$ como um subgrupo de $\mathrm{GL}(n, q)$. Com isso em mente vamos enunciar o seguinte teorema devido a Kantor [10], e vamos terminar a seção. A prova deste teorema não será reproduzida, pois precisa de conceitos sobre grupos de permutações e ações de grupos que nós não introduzimos aqui. Para ver a prova deste teorema sugerimos o mesmo artigo de Kantor.

Teorema 1.4.11. *Se G é um subgrupo de $\mathrm{GL}(n, q)$ que contém um grupo de Singer, então existe um divisor s de n tal que $\mathrm{GL}(n/s, q^s) \trianglelefteq G$.*

Vamos chamar de Y o grupo $\mathrm{GL}(d, q^{n/d})$, e com isso enunciamos o seguinte lema.

Lema 1.4.12. *Temos que $Y = C_{\mathrm{GL}(n,q)}(Z(Y))$.*

Demonstração. Desde que $Y \leq \mathrm{GL}(n, q)$ e Y comuta com todos os elementos de $Z(Y)$ se tem que $Y \leq C_{\mathrm{GL}(n,q)}(Z(Y))$. Por outro lado, seja $g \in C_{\mathrm{GL}(n,q)}(Z(Y))$, nós devemos mostrar que g é uma aplicação $\mathbb{F}_{q^{n/d}}$-linear. Desde que $g \in C_{\mathrm{GL}(n,q)}(Z(Y))$ temos $gz = zg$

para todo $z \in Z(Y)$. Pelo lema 1.2.4 i) se tem $Z(Y) = \{\lambda I_n \mid \lambda \in \mathbb{F}_{q^{n/d}}^{\times}\}$. Assim, dado $\lambda \in \mathbb{F}_{q^{n/d}}$ existe $z \in Z(Y)$ tal que $vz = \lambda v$, para todo $v \in (\mathbb{F}_{q^{n/d}})^d \cong \mathbb{F}_{q^n}$. Portanto, dado $\lambda \in \mathbb{F}_{q^{n/d}}^{\times}$ temos que $(\lambda v)g = vzg = vgz = \lambda(vg)$, para todo $v \in \mathbb{F}_{q^n}$. Assim, g é uma aplicação $\mathbb{F}_{q^{n/d}}$-linear, e temos $C_{\mathrm{GL}(n,q)}(Z(Y)) \leq Y$. Logo, $Y = C_{\mathrm{GL}(n,q)}(Z(Y))$. □

1.5 Sobre p-grupos finitos

Esta seção está dedicada somente a dar resultados que serão usados posteriormente. Alguns destes são resultados conhecidos na teoria de grupos finitos, outros são resultados específicos num determinado assunto. Sendo assim, não daremos a prova da maioria destes, mas remitiremos para cada resultado uma referência.

Dado um grupo G e $x, y \in G$ se define o *comutador* de x e y como $[x, y] = x^{-1}y^{-1}xy$. O *grupo derivado* G' de G é definido como

$$G' = \langle [x, y] \mid x, y \in G \rangle.$$

O grupo G' é o menor subgrupo normal tal que G/G' é abeliano. Assim, G é abeliano se, e somente se, $G' = \{1\}$.

Lema 1.5.1. *Seja G é um grupo com expoente 2, então G é abeliano elementar.*

Demonstração. Dados quaisquer x, y em G temos que $x^2 = y^2 = 1$, então $x = x^{-1}$ e $y = y^{-1}$. Logo $[x, y] = x^{-1}y^{-1}xy = xyxy = (xy)^2 = 1$. Assim, G é abeliano, e assim, abeliano elementar. □

Um subgrupo H de G é dito *subgrupo maximal* se $H \neq G$ e dado um subgrupo L de G, tal que $H \leq L \leq G$ se tem $H = L$ ou $L = G$. O *subgrupo de Frattini* $\Phi(G)$ de G, se define como a interseção de todos os subgrupos maximais de G, se G tiver subgrupos maximais não triviais, e por G se G não tiver subgrupos maximais não triviais.

Os seguintes resultados são fatos conhecidos do subgrupo de Frattini, para uma prova destes sugerimos [16, Satz 3.14 p. 272].

Lema 1.5.2. *Se G é um p-grupo finito então:*

i) $\Phi(G) = G'G^p$, *onde* $G^p = \langle g^p \mid g \in G \rangle$.

ii) $G/\Phi(G)$ *é um grupo abeliano elementar, e* $\Phi(G)$ *é o menor subgrupo normal de* G *com grupo fator abeliano elementar.*

iii) Se G é um 2-grupo então $\Phi(G) = G^2$.

O seguinte é o último resultado desta seção. Este é um teorema devido a T. O. Hawkes, que trata da estrutura do grupo dos automorfismos de um 2-grupo. Nós precisaremos deste resultado posteriormente, já que no terceiro capítulo vamos estudar automorfismos de uma classe especial de 2-grupos.

Teorema 1.5.3 ([7])**.** *Seja G um 2-grupo e seja A o grupo de automorfismos de G que fixam as involuções de G, e seja B o maior 2-subgrupo normal de A. Então A/B é isomorfo a um subgrupo de $D_{2q_1} \times \cdots \times D_{2q_k}$, onde D_{2q_i} é um subgrupo diedral de ordem $2q_i$, com q_i potência de primo ímpar.*

Capítulo 2

2-Grupos de Suzuki

Os p-grupos G, com p ímpar, tais que $\mathrm{Aut}(G)$ permuta transitivamente o conjunto de subgrupos de ordem p foram estudados por Shult, em [1]. Shult mostrou que neste caso G é abeliano. Já no caso $p = 2$, isto não é verdade. Nós vamos estudar este caso. Por [3, teorema 1.2.6] temos que um 2-grupo não abeliano que tem uma única involução é isomorfo ao grupo dos quatérnios generalizados. Sendo assim, vamos dedicar este capítulo a um breve estudo dos 2-grupos G não abelianos com mais de uma involução para os quais $\mathrm{Aut}(G)$ permuta transitivamente o conjunto de subgrupos de ordem 2, ou seja, o conjunto de involuções. Na seção 2.1 vamos estudar quatro famílias de 2-grupos, e na seção 2.2 veremos que estes grupos são os únicos 2-grupos não abelianos para os quais $\mathrm{Aut}(G)$ permuta transitivamente o conjunto de involuções.

2.1 Quatro famílias de 2-Grupos

Antes de começar, vamos introduzir a notação que será usada ao longo da seção. Dado um grupo G, denotaremos por I_G o conjunto de todos os elementos de ordem menor ou igual a dois, e por $I_G^\times$ o conjunto das involuções de G, é dizer, $I_G^\times = I_G - \{1\}$. O símbolo $\mathbb{F}_{2^n}$, onde n é um inteiro positivo, denotará sempre o corpo com 2^n elementos. Dado $\theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$ e $a \in \mathbb{F}_{2^n}$ denotaremos por a^θ a imagem de a via o automorfismo θ. Assim por exemplo, se $\alpha \in \mathbb{Q}$, então $a^{\alpha\theta^n} = (a^\alpha)^{\theta^n}$ é a imagem de a via a composição de $a \mapsto a^\alpha$ e θ^n. Similarmente $a^{\alpha\theta^{n_1}+\beta\theta^{n_2}}$ significa $a^{\alpha\theta^{n_1}}a^{\beta\theta^{n_2}}$. Sendo assim, se $p(\theta)$, $q(\theta)$ são polinômios em $\mathbb{Q}[\theta]$, então

$$a^{p(\theta)+q(\theta)} = a^{p(\theta)}a^{q(\theta)} \quad \text{e} \quad a^{p(\theta)q(\theta)} = (a^{p(\theta)})^{q(\theta)}.$$

Por exemplo, 2θ significa a composição de $a \mapsto a^2$ e θ, e não a aplicação $\theta + \theta$.

No que segue vamos introduzir quatro famílias de grupos de matrizes triangulares superiores e mostraremos, sob algumas condições, que esses grupos tem um subgrupo de automorfismos que permuta transitivamente seu conjunto de involuções. Estes grupos são isomorfos aos grupos definidos por Higman em [4]. Ele define estes grupos como $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ e $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, com multiplicações adequadas que são definidas usando as operações em $\mathbb{F}_{2^n}$. A nossa definição tem a seguinte vantagem: Ao considerar estes grupos como grupos de matrizes, não necessitamos verificar a associatividade. Além disso, definiremos por conjugação de matrizes diagonais grupos de automorfismos destes grupos, os quais irão satisfazer uma propriedade especial. No entanto, se consideramos a definição em [4], nós teríamos que verificar associatividade, e também teríamos que verificar que as aplicações definidas em [4] são de fato automorfismos.

Definição 2.1.1. Vamos definir as seguintes famílias de matrizes triangulares superiores, as quais formam um grupo não abeliano com a multiplicação usual de matrizes.

1. Seja $\theta \in \mathrm{Aut}\,(\mathbb{F}_{2^n})$, não trivial. Definimos
$$A\,(n,\theta) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\theta \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{F}_{2^n} \right\}.$$
Se representamos por (a, b) o elemento
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\theta \\ 0 & 0 & 1 \end{pmatrix}$$
de $A\,(n,\theta)$, a multiplicação de dois elementos $(a_1, b_1), (a_2, b_2) \in A\,(n,\theta)$ é dada por:
$$(a_1, b_1)(a_2, b_2) = (a_1 + a_2, b_1 + b_2 + a_1 a_2^\theta). \tag{2.1}$$

2. Seja $\theta \in \mathrm{Aut}\,(\mathbb{F}_{2^n})$, e seja ε um elemento de $\mathbb{F}_{2^n}$, tal que $\varepsilon \neq \rho^{-1} + \rho^\theta$, para todo $\rho \in \mathbb{F}_{2^n}$. Definamos
$$B\,(n,\theta,\varepsilon) = \left\{ \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & \varepsilon b^\theta + a^\theta \\ 0 & 0 & 1 & b^\theta \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid a, b, c, \in \mathbb{F}_{2^n} \right\}.$$

Se representamos por (a, b, c) o elemento

$$\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & \varepsilon b^{\theta} + a^{\theta} \\ 0 & 0 & 1 & b^{\theta} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

de $B(n, \theta, \varepsilon)$, a multiplicação de $(a_1, b_1, c_1), (a_2, b_2, c_2) \in B(n, \theta, \varepsilon)$ é dada por:

$$(a_1, b_1, c_1)(a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2 + a_1 a_2^{\theta} + \varepsilon a_1 b_2^{\theta} + b_1 b_2^{\theta}). \tag{2.2}$$

3. Seja $\theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$ tal que $2\theta^2 = 1$ e seja ε um elemento de $\mathbb{F}_{2^n}$ tal que $\varepsilon \neq \rho^{2\theta+1} + \rho^{-1}$ para todo $\rho \in \mathbb{F}_{2^n}$. Então definimos:

$$C(n, \varepsilon) = \left\{ \begin{pmatrix} 1 & a & a^{1/2} & b & c \\ 0 & 1 & 0 & 0 & a^{\theta} \\ 0 & 0 & 1 & 0 & \varepsilon b^{2\theta} \\ 0 & 0 & 0 & 1 & b \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_{2^n} \right\}.$$

A propriedade $2\theta^2 = 1$ determina θ unicamente, veja o observação depois desta definição. Por isso, θ não aparece na notação $C(n, \varepsilon)$.

Se representamos por (a, b, c) o elemento

$$\begin{pmatrix} 1 & a & a^{1/2} & b & c \\ 0 & 1 & 0 & 0 & a^{\theta} \\ 0 & 0 & 1 & 0 & \varepsilon b^{2\theta} \\ 0 & 0 & 0 & 1 & b \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

de $C(n, \varepsilon)$, a multiplicação de $(a_1, b_1, c_1), (a_2, b_2, c_2) \in C(n, \varepsilon)$ é dada por

$$(a_1, b_1, c_1)(a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2 + a_1 a_2^{\theta} + \varepsilon a_1^{1/2} b_2^{2\theta} + b_1 b_2). \tag{2.3}$$

4. Seja $\theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$ não trivial tal que $\theta^5 = 1$ e seja ε um elemento de $\mathbb{F}_{2^n}$ tal que

$\varepsilon \neq \rho^{-1} + \rho^{\theta^4+\theta-1}$ para todo $\rho \in \mathbb{F}_{2^n}$. Então definimos:

$$D(n,\theta,\varepsilon) = \left\{ \begin{pmatrix} 1 & a & a^{\theta^3} & b & c \\ 0 & 1 & 0 & 0 & a^{\theta} \\ 0 & 0 & 1 & 0 & \varepsilon b^{\theta} \\ 0 & 0 & 0 & 1 & b^{\theta^2} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_{2^n} \right\}.$$

Se representamos por (a,b,c) o elemento

$$\begin{pmatrix} 1 & a & a^{\theta^3} & b & c \\ 0 & 1 & 0 & 0 & a^{\theta} \\ 0 & 0 & 1 & 0 & \varepsilon b^{\theta} \\ 0 & 0 & 0 & 1 & b^{\theta^2} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

de $D(n,\theta,\varepsilon)$, a multiplicação de $(a_1,b_1,c_1),(a_2,b_2,c_2) \in D(n,\theta,\varepsilon)$ é dada por

$$(a_1,b_1,c_1)(a_2,b_2,c_2) = (a_1+a_2, b_1+b_2, c_1+c_2+a_1a_2^{\theta}+\varepsilon a_1^{\theta^3}b_2^{\theta}+b_1b_2^{\theta^2}). \tag{2.4}$$

Não é difícil verificar que com as operações acima os conjuntos $A(n,\theta)$, $B(n,\theta,\varepsilon)$, $C(n,\varepsilon)$ e $D(n,\theta,\varepsilon)$ são de fato grupos, de ordem 2^{2n}, 2^{3n}, 2^{3n} e 2^{3n}, respectivamente. O fato de que os conjuntos $B(n,\theta,\varepsilon)$, $C(n,\varepsilon)$ e $D(n,\theta,\varepsilon)$ sejam grupos não depende da condição em ε, se pode observar que estes conjuntos são grupos para todo $\varepsilon \in \mathbb{F}_{2^n}$, porém a condição em ε será importante ao determinar as involuções dos respectivos grupos. Com a condição em ε o conjunto de involuções pode ser calculado facilmente, e além disso este será adequado para nosso fins.

Notemos que grupos $A(n,\theta)$ são definidos para qualquer automorfismo θ com $\theta \neq 1$. Na verdade, se $\theta = 1$, então $A(n,\theta)$ seria um grupo abeliano, mas nós não estamos interessados nesse caso. Grupos $B(n,\theta,\varepsilon)$ existem desde que exista $\varepsilon \neq \rho^{-1}+\rho^{\theta}$. Por outro lado, a existência de grupos $C(n,\varepsilon)$ está condicionada à existência de um automorfismo θ satisfazendo $2\theta^2 = 1$. Tal automorfismo θ existe somente quando n é ímpar. De fato, nós temos $\mathrm{Aut}(\mathbb{F}_{2^n}) = \langle\sigma\rangle$, onde $\sigma : a \mapsto a^2$ é o automorfismo de Frobenius, e $|\mathrm{Aut}(\mathbb{F}_{2^n})| = n$. Então, a condição $2\theta^2 = 1$ pode ser escrita, equivalentemente, como $\theta^2 = \sigma^{-1}$. Agora, a aplicação

$$\alpha \mapsto \alpha^2,$$

é um endomorfismo de $\mathrm{Aut}(\mathbb{F}_{2^n})$ que é um automorfismo se e somente se n é ímpar. Logo, se n for par, θ^2 não pode ser um gerador de $\mathrm{Aut}(\mathbb{F}_{2^n})$, em particular, $\theta^2 \neq \sigma^{-1}$. por outro lado, se n é ímpar existe um único θ tal que $\theta^2 = \sigma^{-1}$. Assim, θ está unicamente determinado e temos que $|\sigma| = |\sigma^{-1}| = |\theta^2|$ que é ímpar. Por último, grupos $D(n, \theta, \varepsilon)$ existem somente quando $5 \mid n$, já que neste caso existe $\theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$ tal que $\theta \neq 1$ e $\theta^5 = 1$, é dizer, $|\theta| = 5$.

A seguinte proposição nos diz qual é o conjunto I_G para os grupos $A(n, \theta)$, $B(n, \theta, \varepsilon)$, $C(n, \varepsilon)$ e $D(n, \theta, \varepsilon)$. Antes de enunciar a proposição notemos que $(0, 0)$ é o elemento identidade para $A(n, \theta)$, e que $(0, 0, 0)$ é o elemento identidade para os grupos $B(n, \theta, \varepsilon)$, $C(n, \varepsilon)$ e $D(n, \theta, \varepsilon)$.

Proposição 2.1.1.

1. *Se G é um grupo $A(n, \theta)$, então $I_G = \{(0, b) \mid b \in \mathbb{F}_{2^n}\}$.*

2. *Se G é algum grupo $B(n, \theta, \varepsilon)$, $C(n, \varepsilon)$ e $D(n, \theta, \varepsilon)$, então $I_G = \{(0, 0, c) \mid c \in \mathbb{F}_{2^n}\}$.*

Além disso, em qualquer caso $I_G \trianglelefteq G$.

Demonstração.

1. Seja G um grupo $A(n, \theta)$ e $(a, b) \in G$. Desde que $(a, b)^2 = \left(0, a^{\theta+1}\right)$ temos que $(a, b) \in I_G$ se, e somente se, $a^{\theta+1} = a^{\theta} a = 0$ o que equivale a dizer que $a = 0$, desde que $\theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$. Logo, $I_G = \{(0, b) \mid b \in \mathbb{F}_{2^n}\}$. A definição da multiplicação de G, dada por (2.1), implica que a aplicação $(a, b) \mapsto a$ é um homomorfismo de G no grupo aditivo de $\mathbb{F}_{2^n}$ com núcleo I_G. Logo, $I_G \trianglelefteq G$.

2. Aqui temos três casos:

   - Seja G um grupo $B(n, \theta, \varepsilon)$ e $(a, b, c) \in G$. Desde que

   $$(a, b, c)^2 = \left(0, 0, a^{\theta+1} + \varepsilon a b^{\theta} + b^{\theta+1}\right),$$

   temos que $(a, b, c) \in I_G$ se, e somente se $a^{\theta+1} + \varepsilon a b^{\theta} + b^{\theta+1} = 0$. Nós afirmamos que isso é equivalente a $a = b = 0$. Seja $(a, b, c) \in I_G$, é fácil ver que se um dos a ou b é zero o outro também o é. Por isso, assumamos que $a \neq 0$ e $b \neq 0$, isto implica $\varepsilon = a^{\theta} b^{-\theta} + (a^{-1} b) = (ab^{-1})^{-1} + (ab^{-1})^{\theta}$, contradizendo a hipótese sobre ε. Logo, $I_G = \{(0, 0, c) \mid \ c \in \mathbb{F}_{2^n}\}$.

- Seja G um grupo $C(n,\varepsilon)$ e $(a,b,c)\in G$. Desde que

$$(a,b,c)^2=\left(0,0,a^{\theta+1}+\varepsilon a^{1/2}b^{2\theta}+b^2\right),$$

temos que $(a,b,c)\in I_G$ se, e somente se, $a^{\theta+1}+\varepsilon a^{1/2}b^{2\theta}+b^2=0$. Afirmamos que isso é equivalente a $a=b=0$. Seja $(a,b,c)\in I_G$, é fácil ver que se um dos a ou b é zero o outro também o é. Por isso, assumamos que $a\neq 0$ e $b\neq 0$, isto vai implicar que $\varepsilon=a^{\theta+1/2}b^{-2\theta}+b^{2-2\theta}a^{-1/2}=a^{\theta+1/2}b^{-2\theta}+\left(b^{2\theta-2}a^{1/2}\right)^{-1}$. Desde que $2\theta^2=1$, temos $\left(b^{2\theta-2}a^{1/2}\right)^{2\theta+1}=b^{4\theta^2-4\theta+2\theta-2}a^{\theta+1/2}=b^{-2\theta}a^{\theta+1/2}$ e então $\varepsilon=\rho^{2\theta+1}+\rho^{-1}$, onde $\rho=b^{2\theta-2}a^{1/2}$, contradizendo a hipótese em ε. Logo, $I_G=\{(0,0,c)\mid\ c\in\mathbb{F}_{2^n}\}$.

- Seja G um grupo $D(n,\theta,\varepsilon)$ e $(a,b,c)\in G$. Desde que

$$(a,b,c)^2=\left(0,0,a^{\theta+1}+\varepsilon a^{\theta^3}b^{\theta}+b^{\theta^2+1}\right),$$

temos que $(a,b,c)\in I_G$ se, e somente se, $a^{\theta+1}+\varepsilon a^{\theta^3}b^{\theta}+b^{\theta^2+1}=0$. Afirmamos que isso é equivalente a $a=b=0$. Seja $(a,b,c)\in I_G$, é fácil ver que se um dos a ou b é zero o outro também o é. Por isso, assumamos que $a\neq 0$ e $b\neq 0$, isto implica que $\varepsilon=a^{\theta+1-\theta^3}b^{-\theta}+a^{-\theta^3}b^{\theta^2-\theta+1}$. Desde que $\theta^5=1$ temos que $\left(a^{\theta^3-\theta-1}b^{\theta}\right)^{\theta^4+\theta-1}=a^{-\theta^3}b^{\theta^2-\theta+1}$, e assim $\varepsilon=(a^{\theta^3-\theta-1}b^{\theta})^{-1}+(a^{\theta^3-\theta-1}b^{\theta})^{\theta^4+\theta-1}$, contradizendo a hipótese sobre ε. Logo, $I_G=\{(0,0,c)\mid c\in\mathbb{F}_{2^n}\}$.

Pelas formas das multiplicações dadas em (2.2), (2.3) e (2.4) temos que a aplicação $(a,b,c)\mapsto(a,b,0)$ é um homomorfismo de G em $\mathbb{F}_{2^n}\oplus\mathbb{F}_{2^n}$, com núcleo I_G. Assim, $I_G\trianglelefteq G$.

Assim, a proposição está demonstrada. $\square$

O que faremos agora, será construir um subgrupo de automorfismos para os grupos $A(n,\theta)$, $B(n,\theta,\varepsilon)$, $C(n,\varepsilon)$ e $D(n,\theta,\varepsilon)$.

Dado $\lambda\in\mathbb{F}_{2^n}^{\times}$, chamemos de H_λ a seguinte matriz diagonal:

$$\begin{pmatrix} 1 & 0 & 0\\ 0 & \lambda & 0\\ 0 & 0 & \lambda^{\theta+1}\end{pmatrix}.$$

Consideremos o elemento $(a,b) \in A(n,\theta)$. Desde que

$$\begin{aligned} H_\lambda^{-1}\,(a,b)\,H_\lambda &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda^{-1} & 0 \\ 0 & 0 & \lambda^{-\theta-1} \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\theta \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^{\theta+1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \lambda a & \lambda^{\theta+1} b \\ 0 & 1 & (\lambda a)^\theta \\ 0 & 0 & 1 \end{pmatrix} \\ &= \left(\lambda a, \lambda^{\theta+1} b\right), \end{aligned}$$

se tem que $H_\lambda \in N_{\mathrm{GL}(3,2^n)}(A\,(n,\theta))$. Logo, a aplicação

$$(a,b) \mapsto H_\lambda^{-1}\,(a,b)\,H_\lambda = \left(\lambda a, \lambda^{\theta+1} b\right),$$

é um automorfismo de $A\,(n,\theta)$.

Da mesma forma, se $\lambda \in \mathbb{F}_{2^n}^\times$ chamaremos P_λ a matriz diagonal:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda^{\theta+1} \end{pmatrix}.$$

Consideremos um $(a,b,c) \in B(n,\theta,\varepsilon)$, então

$$\begin{aligned} P_\lambda^{-1}\,(a,b,c)\,P_\lambda &= \begin{pmatrix} 1 & \lambda a & \lambda b & \lambda^{\theta+1} c \\ 0 & 1 & 0 & \varepsilon\,(\lambda b)^\theta + (\lambda a)^\theta \\ 0 & 0 & 1 & (\lambda b)^\theta \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ &= \left(\lambda a, \lambda b, \lambda^{\theta+1} c\right). \end{aligned}$$

Então temos que $P_\lambda \in N_{\mathrm{GL}(4,2^n)}\,(B\,(n,\theta,\varepsilon))$ e, a aplicação

$$(a,b,c) \mapsto \left(\lambda a, \lambda b, \lambda^{\theta+1} c\right),$$

é um automorfismos de $B(n,\theta,\varepsilon)$.

Agora, dado $\lambda \in \mathbb{F}_{2^n}^{\times}$ e $\theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$, tal que $2\theta^2 = 1$; chamemos N_λ a matriz diagonal

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & \lambda^{1/2} & 0 & 0 \\ 0 & 0 & 0 & \lambda^{(\theta+1)/2} & 0 \\ 0 & 0 & 0 & 0 & \lambda^{\theta+1} \end{pmatrix}.$$

Consideremos $(a, b, c) \in C(n, \theta)$, então temos

$$N_\lambda^{-1}(a, b, c) N_\lambda = \begin{pmatrix} 1 & \lambda a & (\lambda a)^{1/2} & \lambda^{(\theta+1)/2} b & \lambda^{\theta+1} c \\ 0 & 1 & 0 & 0 & (\lambda a)^\theta \\ 0 & 0 & 1 & 0 & \varepsilon \lambda^{\theta+1/2} b^{2\theta} \\ 0 & 0 & 0 & 1 & \lambda^{(\theta+1)/2} b \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

e desde que $2\theta^2 = 1$, se tem $\varepsilon \left(\lambda^{(\theta+1)/2} b\right)^{2\theta} = \varepsilon \lambda^{\theta^2+\theta} b^{2\theta} = \varepsilon \lambda^{1/2+\theta} b^{2\theta}$, e segue que

$$\begin{aligned} N_\lambda^{-1}(a, b, c) N_\lambda &= \begin{pmatrix} 1 & \lambda a & (\lambda a)^{1/2} & \lambda^{(\theta+1)/2} b & \lambda^{\theta+1} c \\ 0 & 1 & 0 & 0 & (\lambda a)^\theta \\ 0 & 0 & 1 & 0 & \varepsilon(\lambda^{(\theta+1)/2} b)^{2\theta} \\ 0 & 0 & 0 & 1 & \lambda^{(\theta+1)/2} b \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ &= \left(\lambda a, \lambda^{(\theta+1)/2} b, \lambda^{\theta+1} c\right). \end{aligned}$$

Isto implica que $N_\lambda \in N_{\mathrm{GL}(5,2^n)}(C(n, \theta))$. Logo, a aplicação

$$(a, b, c) \mapsto \left(\lambda a, \lambda^{(\theta+1)/2} b, \lambda^{\theta+1} c\right),$$

é um automorfismo de $C(n, \theta)$.

Por último, dado $\lambda \in \mathbb{F}_{2^n}^{\times}$ e $\theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$, tal que $\theta^5 = 1$; chamemos E_λ a seguinte matriz diagonal

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 & 0 \\ 0 & 0 & \lambda^{\theta^3} & 0 & 0 \\ 0 & 0 & 0 & \lambda^{\theta^4-\theta^2+1} & 0 \\ 0 & 0 & 0 & 0 & \lambda^{\theta+1} \end{pmatrix}.$$

Consideremos $(a,b,c) \in D(n,\theta,\varepsilon)$, então

$$E_\lambda^{-1}(a,b,c)\,E_\lambda = \begin{pmatrix} 1 & \lambda a & (\lambda a)^{\theta^3} & \lambda^{\theta^4-\theta^2+1}b & \lambda^{\theta+1}c \\ 0 & 1 & 0 & 0 & (\lambda a)^\theta \\ 0 & 0 & 1 & 0 & \varepsilon\lambda^{-\theta^3+\theta+1}b^\theta \\ 0 & 0 & 0 & 1 & \lambda^{-\theta^4+\theta^2+\theta}b^{\theta^2} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Tendo em conta que $\theta^5 = 1$, segue que $\left(\lambda^{\theta^4-\theta^2+1}b\right)^{\theta^2} = \lambda^{\theta^6-\theta^4+\theta^2}b^{\theta^2} = \lambda^{\theta-\theta^4+\theta^2}b^{\theta^2}$ e $\varepsilon\left(\lambda^{\theta^4-\theta^2+1}b\right)^\theta = \varepsilon\lambda^{\theta^5-\theta^3+\theta}b^\theta = \varepsilon\lambda^{1-\theta^3+\theta}b^\theta$. Logo

$$\begin{aligned} E_\lambda^{-1}(a,b,c)\,E_\lambda &= \begin{pmatrix} 1 & \lambda a & (\lambda a)^{\theta^3} & \lambda^{\theta^4-\theta^2+1}b & \lambda^{\theta+1}c \\ 0 & 1 & 0 & 0 & (\lambda a)^\theta \\ 0 & 0 & 1 & 0 & \varepsilon\left(\lambda^{\theta^4-\theta^2+1}b\right)^\theta \\ 0 & 0 & 0 & 1 & \left(\lambda^{\theta^4-\theta^2+1}b\right)^{\theta^2} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ &= \left(\lambda a, \lambda^{\theta^4-\theta^2+1}b, \lambda^{\theta+1}c\right). \end{aligned}$$

Logo, a aplicação

$$(a,b,c) \mapsto \left(\lambda a, \lambda^{\theta^4-\theta^2+1}b, \lambda^{\theta+1}c\right),$$

é um automorfismo de $D(n,\theta,\varepsilon)$.

Assim, para cada $\lambda \in \mathbb{F}_{2^n}^\times$ temos definido um automorfismo ξ_λ para os grupos $A\,(n,\theta)$, $B\,(n,\theta,\varepsilon)$, $C\,(n,\varepsilon)$ e $D\,(n,\theta,\varepsilon)$.

Vamos resumir toda a informação relevante que temos sobre grupos $A\,(n,\theta)$, $B\,(n,\theta,\varepsilon)$, $C\,(n,\varepsilon)$ e $D\,(n,\theta,\varepsilon)$ na seguinte tabela:

	θ	ξ_λ
$A\,(n,\theta)$	$\theta \neq 1$	$(a,b) \mapsto \left(\lambda a, \lambda^{\theta+1}b\right)$
$B\,(n,\theta,\varepsilon)$	$-$	$(a,b,c) \mapsto \left(\lambda a, \lambda b, \lambda^{\theta+1}c\right)$
$C\,(n,\varepsilon)$	$2\theta^2 = 1$	$(a,b,c) \mapsto \left(\lambda a, \lambda^{(\theta+1)/2}b, \lambda^{\theta+1}c\right)$
$D\,(n,\theta,\varepsilon)$	$\theta^5 = 1, \theta \neq 1$	$(a,b,c) \mapsto \left(\lambda a, \lambda^{\theta^4-\theta^2+1}b, \lambda^{\theta+1}c\right)$

Tabela 2.1: θ e ξ_λ para os 2-grupos de Suzuki

	ε	$(a,b)^2$ ou $(a,b,c)^2$
$A(n,\theta)$	$-$	$\left(0,a^{\theta+1}\right)$
$B(n,\theta,\varepsilon)$	$\varepsilon \neq \rho^{-1}+\rho^{\theta}$	$\left(0,0,a^{\theta+1}+\varepsilon ab^{\theta}+b^{\theta+1}\right)$
$C(n,\varepsilon)$	$\varepsilon \neq \rho^{-1}+\rho^{2\theta+1}$	$\left(0,0,a^{\theta+1}+\varepsilon a^{1/2}b^{2\theta}+b^{2}\right)$
$D(n,\theta,\varepsilon)$	$\varepsilon \neq \rho^{-1}+\rho^{\theta^4+\theta-1}$	$(0,0,a^{\theta+1}+\varepsilon a^{\theta^3}b^{\theta}+b^{\theta^2+1})$

Tabela 2.2: ε e o quadrado de um elemento para os 2-grupos de Suzuki

Esta tabela contém o nome do grupo na primeira coluna. Na segunda coluna encontramos as condições requeridas para θ, a terceira nos dá para cada $\lambda \in \mathbb{F}_{2^n}^{\times}$ um automorfismo ξ_λ, do grupo respectivo. Na quarta coluna estão as condições que ε satisfaz; por exemplo, $\varepsilon \neq \rho^{-1}+\rho^{\theta}$ significa que não existe $\rho \in \mathbb{F}_{2^n}$ tal que $\varepsilon = \rho^{-1}+\rho^{\theta}$. Por último, a quinta coluna contém os quadrados dos elementos do respectivo grupo.

Seja $X = \{\xi_\lambda \mid \lambda \in \mathbb{F}_{2^n}^{\times}\}$. O conjunto X é fechado por composição. De fato, dados $\xi_\lambda, \xi_\mu \in X$, pelas definições dadas na tabela 2.1 se verifica que $\xi_\lambda\xi_\mu = \xi_{\lambda\mu}$. Além disso $\xi_{\lambda^{-1}} = {\xi_\lambda}^{-1}$. Logo, X é um grupo.

Definamos a aplicação $\lambda \mapsto \xi_\lambda$ do grupo $\mathbb{F}_{2^n}^{\times}$ no grupo $X = \{\xi_\lambda \mid \lambda \in \mathbb{F}_{2^n}^{\times}\}$. Desde que $\xi_\lambda\xi_\mu = \xi_{\lambda\mu}$, a aplicação assim definida é um homomorfismo, o qual é sobrejetivo. Agora, como em todos os casos ξ_λ age na primeira coordenada por multiplicação por λ; se tem que $\xi_\lambda = 1$ se, e somente se, $\lambda = 1$. Assim esta aplicação é injetiva. Logo, $\mathbb{F}_{2^n}^{\times}$ e X são isomorfos, e segue que X é cíclico. Provamos assim a seguinte proposição.

Proposição 2.1.2. *Seja G um grupo $A(n,\theta), B(n,\theta,\varepsilon), C(n,\theta), D(n,\theta,\varepsilon)$. Então temos que $X = \{\xi_\lambda \mid \lambda \in \mathbb{F}_{2^n}^{\times}\}$ é um subgrupo cíclico de* $\mathrm{Aut}(G)$.

Embora os automorfismos ξ_λ sejam os automorfismos que estamos procurando neste momento, é necessário dizer que existem mais automorfismo que podem se encontrar somente por observação. Por exemplo, dado um automorfismo σ de $\mathbb{F}_{2^n}$, podemos definir a aplicação $\varphi_\sigma : A(n,\theta) \to A(n,\theta)$ por $(a,b) \mapsto (a^\sigma, b^\sigma)$. Sejam $(a_1,b_1), (a_2,b_2) \in A(n,\theta)$, então

$$\begin{aligned} ((a_1,b_1)(a_2,b_2))\varphi_\sigma &= \left(a_1+a_2, b_1+b_2+a_1a_2^{\theta}\right)\varphi_\sigma \\ &= \left((a_1+a_2)^{\sigma}, \left(b_1+b_2+a_1a_2^{\theta}\right)^{\sigma}\right) \end{aligned}$$

$$
\begin{aligned}
&= \left(a_1^\sigma + a_2^\sigma, b_1^\sigma + b_2^\sigma + a_1^\sigma a_2^{\theta\sigma}\right) \\
&= \left(a_1^\sigma, b_1^\sigma\right)\left(a_2^\sigma, b_2^\sigma\right) \\
&= \left(a_1, b_1\right)\varphi_\sigma \left(a_2, b_2\right)\varphi_\sigma,
\end{aligned}
$$

o que diz que φ_σ é um homomorfismo, e desde que σ é um automorfismo de $\mathbb{F}_{2^n}$ segue que φ_σ é um automorfismo de $A(n,\theta)$. Assim, obtemos o subgrupo de automorfismos de $A(n,\theta)$:

$$\Sigma = \{\varphi_\sigma \mid \sigma \in \mathrm{Aut}\,(\mathbb{F}_{2^n})\}.$$

Temos que Σ normaliza X. De fato, dado $(a,b) \in G$ observamos que

$$
\begin{aligned}
(a,b)\varphi_\sigma^{-1}\xi_\lambda\varphi_\sigma &= (a^{-\sigma}, b^{-\sigma})\xi_\lambda\varphi_\sigma \\
&= (\lambda a^{-\sigma}, \lambda^{\theta+1}b^{-\sigma})\varphi_\sigma \\
&= (\lambda^\sigma a, \lambda^{\sigma(\theta+1)}b) \\
&= (a,b)\xi_{\lambda^\sigma},
\end{aligned}
$$

ou seja, $\varphi_\sigma^{-1}\xi_\lambda\varphi_\sigma = \xi_{\lambda^\sigma} \in X$. Todo elemento não trivial de X tem somente $(0,0)$ como ponto fixo, mas $(1,1)$ é ponto fixo de todo elemento de Σ, e assim $X \cap \Sigma = \{1\}$. Logo $X \rtimes \Sigma$ é um subgrupo do grupo de automorfismos de $A(n,\theta)$.

Da mesma forma, se G é algum dos grupos $B\,(n,\theta,\varepsilon)$, $C\,(n,\varepsilon)$ e $D\,(n,\theta,\varepsilon)$ podemos mostrar a aplicação $\varphi_\sigma : G \to G$, definida por $(a,b,c)\varphi_\sigma = (a^\sigma, b^\sigma, c^\sigma)$, é um automorfismo de G. Obtendo o subgrupo do grupo de automorfismos de G

$$\Sigma = \{\varphi_\sigma \mid \sigma \in \mathrm{Aut}\,(\mathbb{F}_{2^n})\}.$$

Também se pode mostrar da mesma maneira que $X \rtimes \Sigma$ é um subgrupo do grupo de automorfismos de G. Nós não pretendemos tratar mais sobre automorfismos neste momento. No capítulo 3 nós estudaremos com um pouco mais de detalhe os automorfismos de alguns destes grupos.

O nosso objetivo é mostrar que sob algumas condições os grupos dados na definição 2.1.1 são 2-grupos que tem um subgrupo de automorfismos permutando transitivamente o conjunto de involuções. Para isso vamos precisar de um lema sobre corpos finitos. A demonstração deste, que será reproduzida aqui, é a mesma que a dada em [2, Teorema 6.9 p. 296]. Antes de enunciar o lema lembremos que dado um corpo $\mathbb{F}$ e $\theta \in \mathrm{Aut}(\mathbb{F})$ o corpo fixo de θ e o conjunto $\mathrm{Fix}(\theta) = \{a \in \mathbb{F} \mid a^\theta = a\}$. Notemos que $\mathrm{Fix}(\theta)$ é um subcorpo de $\mathbb{F}$.

Lema 2.1.3. *Seja $\mathbb{F}$ um corpo finito de característica 2 e θ um automorfismo de $\mathbb{F}$. Então, a aplicação $\chi : \mathbb{F}^{\times} \to \mathbb{F}^{\times}$ dada por $a \mapsto a^{\theta+1}$ é bijetiva se, e somente se, θ é de ordem ímpar.*

Demonstração. A aplicação χ é claramente um endomorfismo de $\mathbb{F}^{\times}$. Se $\ker \chi \neq \{1\}$, existe um $a \neq 1$ tal que $a^{\theta} = a^{-1}$. Como a ordem de $\mathbb{F}^{\times}$ é ímpar $a \neq a^{-1}$. Logo, $a^{\theta^i} = a$ se i é par, e $a^{\theta^i} = a^{-1}$ se i é ímpar. Assim, a ordem de θ é par.

Reciprocamente, se a ordem de θ é par, então temos que $\langle\theta\rangle > \langle\theta^2\rangle$ e pelo Teorema Fundamental da Teoria de Galois, ver [18, Teorema 1.2 p. 262], $\mathrm{Fix}(\theta) \subset \mathrm{Fix}(\theta^2)$. Denotemos por $\mathbb{K}_1 = \mathrm{Fix}(\theta)$. Assim, existe um $a \in \mathbb{F}\backslash\mathbb{K}_1$ tal que $a^{\theta} \neq a$ e $a^{\theta^2} = a$. Desde que $\left(a^{\theta+1}\right)^{\theta} = a^{\theta^2+\theta} = a^{\theta+1}$ temos que $a^{\theta+1} \in \mathbb{K}_1^{\times}$, e do fato que $|\mathbb{K}_1^{\times}|$ é ímpar, tem que existir $b \in \mathbb{K}_1^{\times}$ tal que $b^2 = a^{\theta+1}$. Seja $c = ab^{-1}$; $c \neq 1$ desde que $a \notin \mathbb{K}_1$ e $b \in \mathbb{K}_1$. Da definição de b temos que $ba^{-1} = a^{\theta}b^{-1}$. Assim, $c^{\theta} = (ab^{-1})^{\theta} = \left(a^{\theta}\right)\left(b^{\theta}\right)^{-1} = a^{\theta}b^{-1} = ba^{-1} = c^{-1}$. Obtemos então $c^{\theta+1} = 1$, e $c \in \ker\chi\backslash\{1\}$. De onde χ não é injetiva. □

A seguinte proposição diz em quais condições o grupo X permuta transitivamente o conjunto $I_G^{\times}$, das involuções dos grupos definidos em 2.2.1.

Proposição 2.1.4. *Se G é um grupo $A(n,\theta)$, $B(n,\theta,\varepsilon)$, $C(n,\varepsilon)$ ou $D(n,\theta,\varepsilon)$ e θ é um automorfismo de ordem ímpar de $\mathbb{F}_{2^n}$, então X permuta transitivamente o conjunto $I_G^{\times}$.*

Demonstração. Seja θ de ordem ímpar. Pelo lema 2.1.3, $\{\lambda^{\theta+1} \mid \lambda \in \mathbb{F}_{2^n}\} = \mathbb{F}_{2^n}$. Logo, pela terceira coluna da tabela 2.1 temos que a órbita em X de $(0,1)$, no caso de $A(n,\theta)$, e de $(0,0,1)$ nos outros casos, é igual a $I_G^{\times}$. Assim, a ação de X em $I_G^{\times}$ é transitiva. □

Notemos que pela observação feita depois da definição 2.1.1 que os grupos $C(n,\varepsilon)$ satisfazem as hipóteses do lema, já que neste caso θ tem ordem ímpar. Assim, sempre que existam, os grupos $C(n,\varepsilon)$ tem um subgrupo de automorfismos que permuta transitivamente seu conjunto de involuções. O mesmo é verdade para os grupos $D(n,\theta,\varepsilon)$, no caso existam, já que θ, neste caso, tem ordem 5.

2.2 2-grupos de Suzuki

Nesta seção vamos definir uma classe especial de 2-grupos: os 2-grupos de Suzuki. Na verdade, na seção anterior, ao definir as quatro famílias de grupos, nós já tivemos contato com eles. O que será feito nesta seção é definir os 2-grupos de Suzuki formalmente, para depois disso usar um teorema dado por Higman [4], o qual classifica estes grupos. Com o teorema em mãos nós daremos algumas propriedades da estrutura destes grupos, para assim dar exemplos de 2-grupos de Suzuki isomorfos.

Definição 2.2.1. Um 2-grupo de Suzuki é um grupo G com as seguintes propriedades:

1. G é um 2-grupo finito não abeliano.

2. G tem mais de uma involução.

3. Existe um grupo solúvel de automorfismos de G que permuta transitivamente o conjunto das involuções.

O próximo resultado vai caracterizar os 2-grupos de Suzuki. Uma direção deste é o teorema de Higman, do qual falamos na introdução desta seção. A outra direção será consequência da seção anterior. Uma prova do teorema de Higman, na verdade a única que temos referência, pode ser encontrada em [4, Teorema 1].

Teorema 2.2.1. *Se $\theta \in \mathrm{Aut}(\mathbb{F}_{2^n})$ e $\varepsilon \in \mathbb{F}_{2^n}$ satisfazem as condições das tabelas 2.1 e 2.2 e θ tem ordem ímpar, então $A(n,\theta)$, $B(n,\theta,\varepsilon)$, $C(n,\theta)$ e $D(n,\theta,\varepsilon)$ são 2-grupos de Suzuki. Reciprocamente, todo 2-grupo de Suzuki é isomorfo a algum dos grupos $A(n,\theta)$, $B(n,\theta,\varepsilon)$, $C(n,\theta)$ e $D(n,\theta,\varepsilon)$ com θ, ε satisfazendo as condições das tabelas 2.1 e 2.2, e θ de ordem ímpar.*

Demonstração. Suponhamos primeiro que θ, ε satisfazem as condições das tabelas 2.1 e 2.2 e θ tem ordem ímpar. Se G é algum grupo $A(n,\theta)$, $B(n,\theta,\varepsilon)$, $C(n,\theta)$ ou $D(n,\theta,\varepsilon)$, então G tem mais de uma involução e, pelas regras de multiplicação, dadas por (2.1), (2.2), (2.3) e (2.4), ele não é abeliano. Pela proposição 2.1.4, o grupo X, que é cíclico e por isso solúvel, permuta transitivamente o conjunto de involuções de G. Logo, G é um 2-grupo de Suzuki.

Reciprocamente, se G é um 2-grupo de Suzuki, então pelo teorema de Higman, [4, Teorema 1], G é isomorfo a algum dos grupos $A(n,\theta)$, $B(n,\theta,\varepsilon)$, $C(n,\theta)$ ou $D(n,\theta,\varepsilon)$, com θ, ε satisfazendo as condições das tabelas 2.1 e 2.2 e θ de ordem ímpar. □

Muitas das propriedades dos 2-grupos de Suzuki podem ser provadas da definição formal, sem usar a classificação dada por Higman, ver por exemplo [2] e [4]. O teorema anterior nos permite dar propriedades dos 2-grupos de Suzuki analisando somente os grupos $A\,(n,\theta)$, $B\,(n,\theta,\varepsilon)$, $C\,(n,\theta)$ e $D\,(n,\theta,\varepsilon)$. Uns dos principais resultados desta seção será mostrar que em todo 2-grupo de Suzuki se tem $G' = \Phi\,(G) = Z\,(G) = I_G$. Este resultado não será difícil de provar, mas é importante na determinação de isomorfismos entre 2-grupos de Suzuki. Para a prova dele vamos precisar de um lema auxiliar de corpos finitos.

Lema 2.2.2. *Seja $\mathbb{F}$ um corpo finito e $\theta \in \mathrm{Aut}(\mathbb{F})$ não trivial. Então,*

$$\{a \in \mathbb{F} \mid ab^\theta = a^\theta b \text{ para todo } b \in \mathbb{F}\} = \{0\}.$$

Demonstração. Pelo absurdo, suponhamos que existe $a \neq 0$ em $\mathbb{F}$ tal que $ab^\theta = a^\theta b$ para todo $b \in \mathbb{F}$. Em particular, $ab^\theta = a^\theta b$ para todo $b \neq 0$. Logo, $b^{\theta-1} = a^{\theta-1}$ para todo $b \neq 0$, o que diz que o endomorfismo $\zeta : \mathbb{F}^\times \to \mathbb{F}^\times$, definido por $b \mapsto b^{\theta-1}$, é constante. Logo, desde $1\zeta = 1$, temos $\mathrm{Im}\,\zeta = \{1\}$. Assim, $b^{\theta-1} = 1$ para todo $b \neq 0$ em $\mathbb{F}$, o que implica que $b^\theta = b$ para todo $b \neq 0$. De onde, o automorfismo θ é trivial. Mas isso contradiz a hipótese em θ. Assim, temos que ter $\{a \in \mathbb{F} \mid ab^\theta = a^\theta b \text{ para todo } b \in \mathbb{F}\} = \{0\}$. $\square$

Proposição 2.2.3. *Se G é um 2-grupo de Suzuki, então $G' = \Phi\,(G) = G^2 = Z\,(G) = I_G$.*

Demonstração. Seja G algum dos grupos $A\,(n,\theta)$, $B\,(n,\theta,\varepsilon)$, $C\,(n,\theta)$ ou $D\,(n,\theta,\varepsilon)$. Primeiro notemos que se N é um subgrupo característico de G tal que $N \leq I_G$, então $N = I_G$. De fato, se $N < I_G$ então existem involuções dentro e fora de N, o que não é possível, pois $\mathrm{Aut}(G)$ permuta transitivamente I_G e deixa invariante N. Assim, $N = I_G$.

Mostremos agora que $G' = \Phi(G) = I_G$. Dado $x \in G$, pela tabela 2.2, temos que $x^2 \in I_G$. Agora, desde que G é um 2-grupo o lema 1.5.2 iii) diz que

$$\Phi(G) = G^2 = \langle x^2 \mid x \in G\rangle.$$

Logo, $\Phi(G) \leq I_G$, e como pelo lema 1.5.2 i) temos que $G' \leq \Phi(G)$, segue que

$$G' \leq \Phi(G) \leq I_G,$$

e desde que G' e $\Phi(G)$ são subgrupos característicos de G temos que $G' = \Phi(G) = I_G$.

Falta mostrar que $Z(G) = I_G$. Da definição de multiplicação para os quatro grupos se tem que $I_G \leq Z(G)$. Resta mostrar que $Z(G) \leq I_G$. Aqui vamos analisar os quatro casos separadamente.

i) Seja G um grupo $A(n,\theta)$ e $(a_1,b_1)\in Z(G)$, mostremos que $(a_1,b_1)\in I_G$, isto é, mostremos que $a_1=0$. Como $(a_1,b_1)\in Z(G)$, então $(a_1,b_1)(a_2,b_2)=(a_2,b_2)(a_1,b_1)$ para todo $(a_2,b_2)\in G$, e assim, pela regra de multiplicação (2.1), temos

$$\left(a_1+a_2,b_1+b_2+a_1a_2^{\theta}\right)=\left(a_2+a_1,b_2+b_1+a_2a_1^{\theta}\right),$$

isto implica que $a_1a_2^{\theta}=a_2a_1^{\theta}$, para todo $a_2\in\mathbb{F}_{2^n}$, mas desde que θ não é trivial, o lema 2.2.2 implica que $a_1=0$. Assim, $Z(G)\leq I_G$. Concluindo assim esta parte da demonstração.

ii) Seja G algum $B(n,\theta,\varepsilon)$. Dado $(a_1,b_1,c_1)\in Z(G)$, este comuta, em particular, com todo elemento da forma $(0,b_1,c_2)$. Logo,

$$(0,b_1,c_2)(a_1,b_1,c_1)=(a_1,b_1,c_1)(0,b_1,c_2),$$

e pela regra de multiplicação, dada em (2.2), temos

$$\left(a_1,0,c_1+c_2+b_1^{\theta+1}\right)=\left(a_1,0,c_1+c_2+\varepsilon a_1b_1^{\theta}+b_1^{\theta+1}\right),$$

o que vai implicar $\varepsilon a_1b_1^{\theta}=0$. Pela hipótese em ε se tem $\varepsilon\neq0$, e assim devemos ter $a_1=0$ ou $b_1=0$. Se $a_1=0$, então $(0,b_1,c_1)\in Z(G)$, e este comuta em particular com todo elemento da forma $(a_2,0,c_2)$, ou seja,

$$(0,b_1,c_1)(a_2,0,c_2)=(a_2,0,c_2)(0,b_1,c_1).$$

Logo, pela regra de multiplicação, dada em (2.2), devemos ter

$$(a_2,b_1,c_1+c_2)=\left(a_2,b_1,c_1+c_2+\varepsilon a_2b_1^{\theta}\right),$$

e isto implica que $\varepsilon a_2b_1^{\theta}=0$ para todo $a_2\in\mathbb{F}_{2^n}$. Desde que $\varepsilon\neq0$, vamos ter $a_2b_1^{\theta}=0$ para todo $a_2\in\mathbb{F}_{2^n}$, e isto implica que $b_1=0$. Da mesma forma se prova que se $b_1=0$, então $a_1=0$. Logo $(a_1,b_1,c_1)=(0,0,c_1)$, e $Z(G)\leq I_G$.

iii) Seja G algum $C(n,\varepsilon)$. Dado $(a_1,b_1,c_1)\in Z(G)$, este comuta, em particular, com elementos da forma $(0,b_2,c_2)$. Logo,

$$(a_1,b_1,c_1)(0,b_2,c_2)=(0,b_2,c_2)(a_1,b_1,c_1),$$

e pela regra de multiplicação, dada em (2.3), temos

$$\left(a_1,b_1+b_2,c_1+c_2+\varepsilon a_1^{1/2}b_2^{2\theta}+b_1b_2\right)=(a_1,b_2+b_1,c_2+c_1+b_1b_2),$$

o que vai implicar $\varepsilon a_1^{1/2} b_2^{2\theta} = 0$ para todo $b_2 \in \mathbb{F}_{2^n}$. Pela hipótese em ε, se tem $\varepsilon \neq 0$, de onde segue $a_1 = 0$. Assim, $(0, b_1, c_1) \in Z(G)$. Dado (a_2, b_2, c_2) se tem

$$(0, b_1, c_1)(a_2, b_2, c_2) = (a_2, b_2, c_2)(0, b_1, c_1),$$

e pela regra de multiplição, dada por (2.3), segue que

$$(a_2, b_1 + b_2, c_1 + c_2 + b_1 b_2) = \left(a_2, b_2 + b_1, c_2 + c_1 + \varepsilon a_2^{1/2} b_1^{2\theta} + b_2 b_1\right),$$

de onde $\varepsilon a_2^{1/2} b_1^{2\theta} = 0$ para todo $a_2 \in \mathbb{F}_{2^n}$. Como $\varepsilon \neq 0$, temos $b_1 = 0$. Logo, $(a_1, b_1, c_1) = (0, 0, c_1)$, ou seja, $Z(G) \leq I_G$.

iv) Seja G algum $D(n, \theta, \varepsilon)$. Dado $(a_1, b_1, c_1) \in Z(G)$, este comuta em particular com elementos em G da forma $(0, b_1, c_2)$. Então,

$$(a_1, b_1, c_1)(0, b_1, c_2) = (0, b_1, c_2)(a_1, b_1, c_1),$$

e pela regra de multiplicação, dada por (2.4), temos

$$\left(a_1, 0, c_1 + c_2 + \varepsilon a_1^{\theta^3} b_1^{\theta} + b_1^{\theta^2+1}\right) = \left(a_1, 0, c_2 + c_1 + b_1^{\theta^2+1}\right),$$

de onde temos $\varepsilon a_1^{\theta^3} b_1^{\theta} = 0$. Como nos casos anteriores, a hipótese em ε implica $\varepsilon \neq 0$, o que a sua vez diz que $a_1 = 0$ ou $b_1 = 0$. Se $a_1 = 0$, então $(0, b_1, c_1) \in Z(G)$, e assim este comuta com todo elemento da forma (a_2, b_1, c_2) em G, ou seja,

$$(0, b_1, c_1)(a_2, b_1, c_2) = (a_2, b_1, c_2)(0, b_1, c_1),$$

e pela regra de multiplicação, dada por (2.4), temos

$$\left(a_2, 0, c_1 + c_2 + b_1^{\theta^2+1}\right) = \left(a_2, 0, c_2 + c_1 + \varepsilon a_2^{\theta^3} b_1^{\theta^2} + b_1^{\theta^2+1}\right),$$

o que implica que $\varepsilon a_2^{\theta^3} b_1^{\theta^2} = 0$ para todo $a_2 \in \mathbb{F}_{2^n}$. Como $\varepsilon \neq 0$, temos $b_1 = 0$. Da mesma forma se mostra que $b_1 = 0$ implica $a_1 = 0$. Assim $(a_1, b_1, c_1) = (0, 0, c_1)$, é dizer, $Z(G) \leq I_G$.

Assim, em todos os casos se tem $Z(G) = I_G$. Concluindo assim a prova da proposição. $\square$

Como uma consequência da proposição anterior temos o seguinte corolário.

Corolário 2.2.4. *Se e G é um 2-grupo de Suzuki, então $Z(G)$ e $\overline{G} = G/Z(G)$ são 2-grupos abelianos elementares.*

Demonstração. Seja G algum grupo $A(n,\theta)$, $B\,(n,\theta,\varepsilon)$, $C\,(n,\varepsilon)$ ou $D\,(n,\theta,\varepsilon)$. Pela proposição 2.2.3, $Z\,(G) = I_G$, de onde temos que $Z(G)$ tem expoente 2. Assim, $Z(G)$ é abeliano elementar. Por outro lado, a tabela 2.2 mostra que $x^2 \in I_G$ para todo $x \in G$. Sendo assim, $(xZ(G))^2 = Z(G)$, de onde se tem que o expoente de $\overline{G} = G/Z\,(G)$ é 2. Assim, como $\overline{G}$ é abeliano, $\overline{G}$ é abeliano elementar. □

Se temos que G é um grupo $A(n,\theta)$, então dado $(a,b) \in G$ podemos escrever este como $(a,b) = (a,0)(0,b)$. Assim, $(a,b)Z(G) = (a,0)Z(G)$ para todo $b \in \mathbb{F}_{2^n}$. Consequentemente

$$\overline{G} = G/Z(G) = \{(a,0)Z(G) \mid a \in \mathbb{F}_{2^n}\}, \tag{2.5}$$

e como $|\overline{G}| = 2^n$, segue que a representação de um elemento de $\overline{G}$ na forma $(a,0)Z(G)$ é única.

Da mesma forma, se G é algum dos grupos $B\,(n,\theta,\varepsilon)$, $C\,(n,\varepsilon)$ ou $D\,(n,\theta,\varepsilon)$, e (a,b,c), é um elemento de G, então pelas regras de multiplicação, dadas por (2.2), (2.3) e (2.4), se tem que $(a,b,c) = (a,b,0)(0,0,c)$. Assim, $(a,b,c)Z(G) = (a,b,0)Z(G)$ para todo $c \in \mathbb{F}_{2^n}$. Consequentemente

$$\overline{G} = G/Z(G) = \{(a,b,0)Z(G) \mid a,b \in \mathbb{F}_{2^n}\}, \tag{2.6}$$

e desde que, neste caso, $|\overline{G}| = 2^{2n}$, segue que a representação de un elemento de $\overline{G}$ na forma $(a,b,0)Z(G)$ é única.

2.3 Isomorfismo entre 2-grupos de Suzuki

No que segue vamos focar-nos em saber quando os 2-grupos de Suzuki de tipo 1 e tipo 2 podem ser isomorfos. Para isso vamos precisar de um lema auxiliar em 2-grupos, o qual pode ser encontrado em [2, Teorema 6.6, p. 294]. Este lema vai nos dar condições que irão implicar que dois 2-grupos são isomorfos.

Lema 2.3.1. *Sejam G_1, G_2 2-grupos. Suponhamos que:*

i) Existe H_i um subgrupo abeliano elementar do centro de G_i tal que G_i/H_i é abeliano elementar, $i = 1,2$.

ii) Existem isomorfismos $\rho : G_1/H_1 \to G_2/H_2$ e $\sigma : H_1 \to H_2$ tais que se $(xH_1)\,\rho = yH_2$, então se tem $(x^2)\,\sigma = y^2$.

Então existe um isomorf ismo de G_1 em G_2 o qual leva H_1 em H_2 e induz ρ, σ em G_1/H_1, H_1 respectivamente.

A seguinte proposição nos dá alguns exemplos de 2-grupos de Suzuki isomorfos. A demostração deste será uma aplicação do lema anterior para os grupos $A(n,\theta)$, $B(n,\theta,\varepsilon)$, e $D(n,\theta,\varepsilon)$. No caso de $C(n,\varepsilon)$ não temos um resultado parecido, já que o automorfismo θ está unicamente determinado. Esses isomorfismos são enunciados por Higman em [4] sem demonstração.

Proposição 2.3.2. *Temos os seguintes isomorfismos entre 2-grupos de Suzuki.*

i) $A(n,\theta) \cong A(n,\theta^{-1})$.

ii) $B(n,\theta,\varepsilon) \cong B(n,\theta^{-1},\varepsilon^{\theta^{-1}})$.

iii) $D(n,\theta,\varepsilon) \cong D(n,\theta^{-1},\varepsilon^{\theta^{-1}})$.

Demonstração. Primeiro, notemos que se $A(n,\theta)$ existe, também vai existir $A(n,\theta^{-1})$, desde que se $|\theta| = |\theta^{-1}|$. Agora, se $B(n,\varepsilon,\theta)$ existe então ε satisfaz a hipótese da tabela 2.2. Para mostrar que $B(n,\theta^{-1},\varepsilon^{\theta^{-1}})$ existe devemos de mostrar que $\varepsilon^{\theta^{-1}}$ também satisfaz a hipótese da tabela 2.2, é dizer $\varepsilon^{\theta^{-1}} \neq \rho^{-1}+\rho^{\theta}$ para todo $\rho \in \mathbb{F}_{2^n}$. Suponhamos que existe $\rho \in \mathbb{F}_{2^n}$ tal que $\varepsilon^{\theta^{-1}} \neq \rho^{-1}+\rho^{\theta}$, então $\varepsilon = (\rho^{\theta})^{-1} + (\rho^{\theta})^{\theta}$. Contradizendo a hipótese de ε. Assim, sempre que $B(n,\theta,\varepsilon)$ existe, $B(n,\theta^{-1},\varepsilon^{\theta^{-1}})$ também vai existir. Por último para mostrar que se $D(n,\theta,\varepsilon)$ existe, então $D(n,\theta^{-1},\varepsilon^{\theta^{-1}})$ também existe, devemos mostrar que $\theta^{-1},\varepsilon^{\theta^{-1}}$ satisfazem as hipóteses das tabelas 2.1 e 2.2. Desde que $\theta \neq 1$ e $\theta^5 = 1$, se tem que $\theta^{-1} \neq 1$ e $(\theta^{-1})^5 = 1$, ou seja, θ^{-1} satisfaz as hipóteses da tabela 2.1. Para o caso de $\varepsilon^{\theta^{-1}}$, suponhamos que exista $\rho \in \mathbb{F}_{2^n}$ tal que $\varepsilon^{\theta^{-1}} = \rho^{-1} + \rho^{\theta^4+\theta-1}$. Logo, $\varepsilon = (\rho^{\theta})^{-1} + (\rho^{\theta})^{\theta^4+\theta-1}$. Contradizendo a hipótese de ε. Então, $\varepsilon^{\theta^{-1}} \neq \rho^{-1} + \rho^{\theta^4+\theta-1}$ para todo $\rho \in \mathbb{F}_{2^n}$, uo seja, $\varepsilon^{\theta^{-1}}$ satisfaz a hipótese da tabela 2.2. Mostramos assim, que sempre que $D(n,\theta,\varepsilon)$ exista, $D(n,\theta^{-1},\varepsilon^{\theta^{-1}})$ também existirá.

Pelo corolário 2.2.4, se G é um 2-grupo de Suzuki, então $Z(G)$ e $\overline{G} = G/Z(G)$ são 2-grupos abelianos elementares. Assim, G verifica i) do lema 2.3.1. Nosso seguinte passo será definir para cada caso isomorfismos σ e ρ que verifiquem o lema 2.3.1. Logo, como consequência desse lema, teremos os isomorfismos requeridos.

Sejam G e H os grupos nos lados de um dos isomorfismos i), ii) ou iii). Nos consideramos G e H iguais como conjuntos, mas com multiplicações diferentes. Denotaremos a multiplicação em G por $\cdot$ e multiplicações de H por $\circ$.

Definamos as seguintes aplicações:

1. Se $G = A(n, \theta)$ e $H = A(n, \theta^{-1})$, definamos

$$\sigma_1 : Z(G) \to Z(H) \text{ por } (0, b) \mapsto (0, b^{\theta^{-1}}); \text{ e}$$

$$\rho_1 : \overline{G} \to \overline{H} \text{ por } (a, 0)\, Z(G) \mapsto (a, 0)\, Z(H).$$

2. Se $G = B(n, \theta, \varepsilon)$ e $H = B(n, \theta^{-1}, \varepsilon^{\theta^{-1}})$, definamos

$$\sigma_2 : Z(G) \to Z(H) \text{ por } (0, 0, c) \mapsto (0, 0, c^{\theta^{-1}}); \text{ e}$$

$$\rho_2 : \overline{G} \to \overline{H}\, (a, b, 0) \text{ por } Z(G) \mapsto (b, a, 0)\, Z(H).$$

3. Se $G = D(n, \theta, \varepsilon)$ e $H = D(n, \theta^{-1}, \varepsilon^{\theta^{-1}})$, definamos

$$\sigma_3 : Z(G) \to Z(H) \text{ por } (0, 0, c) \mapsto (0, 0, c^{\theta^{-1}}); \text{ e}$$

$$\rho_3 : \overline{G} \to \overline{H} \text{ por } (a, b, 0)\, Z(G) \mapsto (a, b^{\theta}, 0) Z(H).$$

Desde que θ é um automorfismo se tem que σ_i e ρ_i são isomorfismos, para $i = 1, 2, 3$. Mostremos que σ_i, ρ_i verificam a parte ii) do lema 2.3.1. Assim, teremos os isomorfismos desejados.

1. Se $((a, 0)\, Z(G))\, \rho_1 = (a, 0)\, Z(H)$, então

$$\begin{aligned} ((a, 0) \cdot (a, 0))\, \sigma_1 &= \left(0, a^{\theta+1}\right) \sigma_1 \\ &= (0, a^{\theta^{-1}+1}) \\ &= (a, 0) \circ (a, 0). \end{aligned}$$

   Assim, pelo lema 2.3.1 se tem que $A(n, \theta) \cong A(n, \theta^{-1})$, provando assim i).

2. Se $((a, b, 0)\, Z(G))\, \rho_2 = (b, a, 0)\, Z(H)$, então

$$\begin{aligned} ((a, b, 0) \cdot (a, b, 0))\, \sigma_2 &= \left(0, 0, a^{\theta+1} + \varepsilon a b^{\theta} + b^{\theta+1}\right) \sigma_2 \\ &= (0, 0, a^{\theta^{-1}+1} + \varepsilon^{\theta^{-1}} a^{\theta^{-1}} b + b^{\theta^{-1}+1}) \\ &= (b, a, 0) \circ (b, a, 0). \end{aligned}$$

   Assim, pelo lema 2.3.1 se tem que $B(n, \theta, \varepsilon) \cong B(n, \theta^{-1}, \varepsilon^{\theta^{-1}})$, mostrando ii).

3. Se $((a, b, 0)\, Z(G))\, \rho_3 = \left(a, b^\theta, 0\right) Z(H)$, então

$$\begin{aligned} ((a, b, 0) \cdot (a, b, 0))\, \sigma_3 &= (0, 0, a^{\theta+1} + \varepsilon a^{\theta^3} b^\theta + b^{\theta^2+1})\sigma_3 \\ &= (0, 0, a^{\theta^4+1} + \varepsilon^{\theta^4} a^{\theta^2} b + b^{\theta+\theta^4}) \\ &= \left(a, b^\theta, 0\right) \circ \left(a, b^\theta, 0\right). \end{aligned}$$

Assim, pelo lema 2.3.1 se tem que $D\,(n, \theta, \varepsilon) \cong D(n, \theta^{-1}, \varepsilon^{\theta^{-1}})$, mostrando assim $iii)$.

Concluímos desta maneira a prova da proposição. □

2.4 Um 2-subgrupo de Sylow do grupo $\mathrm{SU}(3, q^2)$

Nesta seção vamos introduzir um grupo de matrizes 3×3, e mostraremos sob algumas condições, que esse grupo é isomorfo ao grupo $B(n, 1, \varepsilon)$, para um ε adequado.

Seja $q = 2^n$, consideremos o grupo

$$\mathcal{B}(n) = \left\{ (a, b) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^q \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{F}_{q^2} \text{ e } b^q + b + a^{q+1} = 0 \right\}.$$

Temos que $\mathcal{B}(n)$ é um grupo com a multiplicação usual de matrizes. De fato,

$$(a_1, b_1)(a_2, b_2) = (a_1 + a_2, b_1 + b_2 + a_1 a_2^q).$$

É interessante notar que se V é um espaço vetorial de dimensão 3 sobre $\mathbb{F}_{q^2}$, com base $\{e_1, w, f_1\}$ e $B : V \times V \to \mathbb{F}_{q^2}$ é forma bilinear hermitiana definida por $1 = B(w, w) = B(e_1, f_1)$ e $B(e_1, e_1) = B(f_1, f_1) = B(e_1, w) = B(w, f_1) = 0$ e estendida linearmente, então $\mathcal{B}(n)$ é um subgrupo do grupo:

$$\mathrm{SU}(3, q^2) = \{g \in \mathrm{GL}(3, q^2) \mid \det g = 1 \text{ e } B(vg, wg) = B(v, w) \text{ para todo } v, w \in V\},$$

chamado *grupo especial unitário*. De fato $\mathcal{B}(n)$ é um 2-subgrupo de Sylow de $\mathrm{SU}(3, q^2)$

Para continuar com o estudo deste grupo, nós precisamos do seguinte lema, o qual vai nos dar algumas propriedades do corpo $\mathbb{F}_{q^2}$.

Lema 2.4.1. *Seja $\mathbb{F}_{q^2}$ o corpo com q^2 elementos, onde $q = 2^n$. Então* *i)* $\{\lambda^{q+1} \mid \lambda \in \mathbb{F}_{q^2}\} = \mathbb{F}_q$.

ii) *A aplicação* $\mu : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$, *definida por* $\lambda \mapsto \lambda + \lambda^q$, *é* $\mathbb{F}_q$*-linear. Além disso,* $\dim_{\mathbb{F}_q}(\ker \mu) = 1$. *Consequentemente* $\ker \mu = \mathbb{F}_q$.

iii) *Para todo* $a \in \mathbb{F}_q$ *temos que*

$$|\{\lambda \in \mathbb{F}_{q^2} \mid \lambda\mu = a\}| = q.$$

Demonstração.

i) Observemos que $\mathbb{F}_{q^2}^{\times}$ é cíclico de ordem $q^2-1 = (q+1)(q-1)$. Consideremos $\mathbb{F}_q$ como um subcorpo de $\mathbb{F}_{q^2}$, então $\mathbb{F}_q^{\times}$ é o único subgrupo cíclico de ordem $q-1$ de $\mathbb{F}_{q^2}$. Agora, desde que o grupo $\{\lambda^{q+1} \mid \lambda \in \mathbb{F}_{q^2}\}$ é cíclico e tem ordem $q-1$ se tem que $\{\lambda^{q+1} \mid \lambda \in \mathbb{F}_{q^2}^{\times}\} = \mathbb{F}_{q^2}^{\times}$. Logo, $\{\lambda^{q+1} \mid \lambda \in \mathbb{F}_{q^2}\} = \mathbb{F}_q$.

ii) Dados $a, b \in \mathbb{F}_{q^2}$ e $\alpha \in \mathbb{F}_q$ se tem

$$(a+b)\mu = (a+b) + (a+b)^q = a + a^q + b + b^q = a\mu + b\mu \text{ e}$$

$$(\alpha a)\mu = \alpha a + \alpha^q a^q = \alpha a + \alpha a^q = \alpha(a + a^q) = \alpha(a\mu).$$

Logo, μ é $\mathbb{F}_q$-linear. Notemos que para todo $a \in \mathbb{F}_q$ se tem que $a + a^q = a + a = 0$, isto é, $\mathbb{F}_q \subseteq \ker \mu$ e desde que a aplicação não é nula segue que $\dim_{\mathbb{F}_q} \ker \mu = 1$. Assim, $\ker \mu = \mathbb{F}_q$.

iii) Desde que o conjunto $\{\lambda \in \mathbb{F}_{q^2} \mid \lambda\mu = a\}$ é uma classe lateral de $\ker \mu$, se tem que $\{\lambda \in \mathbb{F}_{q^2} \mid \lambda\mu = a\} = |\ker \mu| = q$. □

Lema 2.4.2. *O grupo* $\mathcal{B}(n)$ *tem ordem* q^3.

Demonstração. Vamos contar o número de possibilidades para $a, b \in \mathbb{F}$ satisfazendo a definição de $\mathcal{B}(n)$. Seja $(a, b) \in \mathcal{B}(n)$, então $b + b^q + a^{q+1} = 0$. Pelo lema 2.4.1 i), dado $a \in \mathbb{F}_{q^2}$ se tem que $a^{q+1} \in \mathbb{F}_q$, e pela parte iii) do mesmo lema, dado $a \in \mathbb{F}_{q^2}$ existem q escolhas para b satisfazendo $b + b^q + a^{q+1} = 0$. Assim, como temos q^2 escolhas para a e q escolhas para b, temos que $|\mathcal{B}(n)| = q^3$. □

O próximo lema vai nos dizer porque é tão importante estudar o grupo $\mathcal{B}(n)$. O lema mostrará que o grupo $\mathcal{B}(n)$ é um 2-grupo de Suzuki.

Lema 2.4.3. *Dado $\eta \in \mathbb{F}_{q^2}$ de ordem $q+1$, se tem que $\mathcal{B}(n)$ é isomorfo ao 2-grupo de Suzuki $B(n, 1, \eta + \eta^q)$.*

Demonstração. Dado $(a, b) \in \mathcal{B}(n)$ se tem que $(a, b)^2 = (0, a^{q+1})$. Logo, (a, b) é uma involução se, e somente se, $a^{q+1} = 0$, isto implica que $b + b^q = 0$, é dizer, $b \in \mathbb{F}_q$. Assim, $I_{\mathcal{B}(n)} \leq \{(0, b) \mid b \in \mathbb{F}_q\}$, e pela regra de multiplicação $\{(0, b) \mid b \in \mathbb{F}_q\} \leq I_{\mathcal{B}(n)}$. Logo,

$$I_{\mathcal{B}(n)} = \{(0, b) \mid b \in \mathbb{F}_q\}.$$

Se tem que $I_{\mathcal{B}(n)}$ é um subgrupo de $\mathcal{B}(n)$ de expoente 2. Logo, pelo lema 1.5.1, $I_{\mathcal{B}(n)}$ é abeliano elementar. Pela regra de multiplicação se tem que $I_{\mathcal{B}(n)} \leq Z(\mathcal{B}(n))$. Assim, $I_{\mathcal{B}(n)} \trianglelefteq \mathcal{B}(n)$. Desde que $|\mathcal{B}(n)| = q^3$ e $|I_{\mathcal{B}(n)}| = q$, segue que $|\mathcal{B}(n)/I_{\mathcal{B}(n)}| = q^2$. Como $(a, 0)I_{\mathcal{B}(n)} \in \mathcal{B}(n)/I_{\mathcal{B}(n)}$ para todo $a \in \mathbb{F}_{q^2}$, se tem que

$$\mathcal{B}(n)/I_{\mathcal{B}(n)} = \{(a, 0)I_{\mathcal{B}(n)} \mid a \in \mathbb{F}_{q^2}\},$$

e como $(a, 0)^2 \in I_{\mathcal{B}(n)}$, se tem que o expoente de $\mathcal{B}(n)/I_{\mathcal{B}(n)}$ é 2. Assim, pelo lema 1.5.1, $\mathcal{B}(n)/I_{\mathcal{B}(n)}$ é abeliano elementar. Assim, os grupos $\mathcal{B}(n)$ e $B(n, 1, \eta + \eta^q)$ satisfazem i) do lema 2.3.1.

O que faremos agora será definir aplicações que satisfazem a parte ii) do lema 2.3.1. Consequentemente teremos o isomorfismo desejado. Desde que η tem ordem $q+1$ se tem que $\{1, \eta\}$ é uma base de $\mathbb{F}_{q^2}$ sobre $\mathbb{F}_q$. Seja $G = B(n, 1, \eta + \eta^q)$, definamos as aplicações

$$\sigma : I_{\mathcal{B}(n)} \to I_G, \text{ por } (0, c) \mapsto (0, 0, c) \text{ e}$$

$$\rho : \mathcal{B}(n)/I_{\mathcal{B}(n)} \to G/I_G, \text{ por } (a + b\eta)I_{\mathcal{B}(n)} \mapsto (a, b, 0)I_G.$$

É imediato ver que σ e ρ são isomorfismos. Vamos verificar que estas aplicações satisfazem ii) do lema 2.3.1. Vejamos, se $((a + b\eta, 0)I_{\mathcal{B}(n)})\rho = (a, b, 0)I_G$, então

$$\begin{aligned}
((a + b\eta)^2, 0)\sigma &= (0, (a + b\eta)(a + b\eta)^q)\sigma \\
&= (0, a^2 + ab(\eta + \eta^q) + b^2\eta^{q+1})\sigma \\
&= (0, a^2 + ab(\eta + \eta^q) + b^2)\sigma \\
&= (0, 0, a^2 + ab(\eta + \eta^q) + b^2) \\
&= (a, b, 0)^2,
\end{aligned}$$

é dizer, σ, ρ satisfazem o lema 2.3.1. Assim, se tem $\mathcal{B}(n) \cong B(n, 1, \eta + \eta^q)$.

Agora, desde que $\mathcal{B}(n) \cong B(n,1,\eta+\eta^q)$ temos que $|I_{\mathcal{B}(n)}| = |I_{B(n,1,\eta+\eta^q)}|$ e desde que $|I_{\mathcal{B}(n)}| = q$, devemos ter $|I_{B(n,1,\eta+\eta^q)}| = q$. Isto implica que $\eta+\eta^q \neq x+x^{-1}$ para todo $x \in \mathbb{F}_q$. De fato, se $\eta+\eta^q = x+x^{-1}$ para algum $x \in \mathbb{F}_q$, então o elemento $(x,1,0) \in B(n,1,\eta+\eta^q)$ está em $I_{B(n,1,\eta+\eta^q)}$, mas também os elementos da forma $(0,0,c)$ para $c \in \mathbb{F}_q$, estão em $I_{B(n,1,\eta+\eta^q)}$, o que implicará que $|I_{B(n,1,\eta+\eta^q)}| > q$. O que é uma contradição ao fato $|I_{B(n,1,\eta+\eta^q)}| = q$, que surgiu ao supor que $\eta+\eta^q = x+x^{-1}$ para algum $x \in \mathbb{F}_q$. Sendo assim, devemos ter que $\eta+\eta^q \neq x+x^{-1}$ para todo $x \in \mathbb{F}_{2^n}$. Assim, $\eta+\eta^q$ satisfaz a condição da tabela 2.2. Logo, $B(n,1,\eta+\eta^q)$ é um 2-grupo de Suzuki, e $\mathcal{B}(n)$ também o é. $\square$

É importante notar que os grupos $B(n,\theta,\varepsilon)$ foram definidos como matrizes 4×4, porém existe a classe de grupos $B(n,1,\eta+\eta^q)$ que tem uma representação matricial de ordem 3×3. Também notemos que o grupo $\mathcal{B}(n)$ pode ser considerado como um subgrupo de $A(2n,\alpha)$, onde $\alpha : a \mapsto a^q$. Embora $A(2n,\alpha)$ não seja um 2-grupo de Suzuki, existe o subgrupo $B(n,1,\eta+\eta^q)$ dele, que é um 2-grupo de Suzuki, e que não é da forma $A(n',\theta')$. Isto último, também diz que subgrupos de $A(n,\theta)$ não necessariamente são da forma $A(n',\theta')$.

Como $\mathcal{B}(n) \cong B(n,1,\eta+\eta^q)$ temos que existe um subgrupo de automorfismo de $\mathcal{B}(n)$ isomorfo ao grupo X, definido na seção 2.1. que permuta transitivamente o conjunto $I_{\mathcal{B}(n)}$, das involuções de $\mathcal{B}(n)$. No entanto, nós estamos interssados em outro subgrupo de automorfismo de $\mathcal{B}(n)$ que será usado no capítulo 3.

Já foi observado que o grupo $\mathcal{B}(n)$ é um subgrupo de $A(2n,\alpha)$, onde $\alpha : a \mapsto a^q$, e nós já conhecemos um subgrupo X de automorfismos de $A(2n,\alpha)$. Se queremos descobrir algum subgrupo de automorfismos de $\mathcal{B}(n)$, o que mais natural que considerar o grupo induzido por X? Sendo assim, consideremos para cada $\lambda \in \mathbb{F}_{q^2}^{\times}$ o automorfismo ξ_λ definido por $(a,b) \mapsto (\lambda a, \lambda^{q+1} b)$. Mostremos que estes automorfismos deixam invariante $\mathcal{B}(n)$. De fato, desde que $\lambda^{q+1}b + (\lambda^{q+1}b)^q + (\lambda a)^{q+1} = \lambda^{q+1}(b^q + b + a^{q+1}) = 0$ se tem que ξ_λ deixa invariante $\mathcal{B}(n)$. Assim o grupo

$$X = \{\xi_\lambda \mid \lambda \in \mathbb{F}_{q^2}^{\times}\}$$

é um subgrupo cíclico, e por isso solúvel, de automorfismos de $\mathcal{B}(n)$ que permuta transitivamente o conjunto de involuções $I_{\mathcal{B}(n)}$.

Agora, ao considerar automorfismos de $A(2n,\alpha)$ também vimos que dado $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^2})$

existe o automorfismo φ_σ de $A(2n,\alpha)$, definido por $(a,b) \mapsto (a^\sigma, b^\sigma)$. Desde que $b^{q\sigma} + b^\sigma + a^{(q+1)\sigma} = (b^q + b + a^{q+1})^\sigma = 0$, se tem que φ_σ é um automorfismo de $\mathcal{B}(n)$. Assim, vamos ter que

$$\Sigma = \{\varphi_\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{F}_{q^2})\}$$

é outro subgrupo de automorfismos de $\mathcal{B}(n)$.

Notemos também, da seção 2.1, que Σ normaliza X. Logo, o produto $X \rtimes \Sigma$ é um subgrupo do grupo de automorfismos de $\mathcal{B}(n)$.

Capítulo 3

Automorfismos de 2-Grupos de Suzuki

O primeiro trabalho, do qual temos referência, que trata sobre este assunto é o artigo Landrock [5], o qual dá uma descrição da estrutura do grupo de automorfismos e de seu 2-grupo normal maximal para grupos $A(n, \theta)$ e para os grupos $\mathcal{B}(n)$. Um resultado que vale para todo 2-grupo de Suzuki é o dado por Bryukhanova [6], o qual mostra que o grupo de automorfismos de 2-grupos de Suzuki é solúvel. Depois de Bryukhanova, Kazarin e Sidel'nikov [8] obtiveram explicitamente o grupo de automorfismos de uma p-álgebra de Suzuki, $p > 2$. Nós não necessitamos explicar aqui que é uma p-álgebra de Suzuki, só vamos dizer que esse artigo e o anterior inspiraram Mark Lewis [9] a dar uma determinação explícita do grupo de automorfismos de grupos $A(n, \theta)$. Lewis, no seu resultado, usa fortemente o fato da solubilidade mostrado por Bryukhanova. O que nós faremos neste capítulo será determinar o grupo de automorfismo de grupos $A(n, \theta)$, porém não usaremos o fato da solubilidade. Em troca disso vamos combinar algumas ideias de Kazarin e Sidel'nikov e de Lewis com a teoria até agora estudada, para determinar o grupo de automorfismos de grupos $A(n, \theta)$, e reproduzimos a prova de Landrock para determinar o grupo de automorfismos de $\mathcal{B}(n)$.

3.1 Automorfismos de $A(n, \theta)$ e $\mathcal{B}(n)$

Nesta seção vamos fazer um estudo geral da estrutura dos grupos de automorfismos dos 2-grupos de Suzuki $A(n, \theta)$ e $\mathcal{B}(n)$. Esta será uma preparação para as próximas seções, onde nós determinaremos os grupos de automorfismos destes grupos.

Nesta seção, vamos assumir que G denotará indistintamente o grupo $A(n, \theta)$ ou $\mathcal{B}(n)$. Lembrando que I_G é o conjunto de elementos com ordem menor ou igual do que 2, $\overline{G}$ denotará o grupo G/I_G. A classe lateral de um elemento x de G em $\overline{G}$ será denotada por $\overline{x}$. O grupo de automorfismos de G será denotado por $\mathcal{A}$.

Nós mostramos, na proposição 2.2.3, que $I_G = Z(G) = G^2 = G'$; e no corolário 2.2.4, que I_G e $\overline{G}$ são 2-grupos abelianos elementares. Também mostramos que se $G = A(n, \theta)$, então

$$\overline{G} = \{\overline{(a, 0)} \mid a \in \mathbb{F}_{2^n}\} \quad \text{e} \quad I_G = \{(0, b) \mid b \in \mathbb{F}_{2^n}\},$$

e se $G = \mathcal{B}(n)$, então

$$\overline{G} = \{\overline{(a, 0)} \mid a \in \mathbb{F}_{2^{2n}}\} \quad \text{e} \quad I_G = \{(0, b) \mid b \in \mathbb{F}_{2^n}\}.$$

Como $\overline{G}$ e I_G são abelianos elementares, eles podem ser considerados como espaços vetoriais sobre $\mathbb{F}_2$, onde a soma é a operação de grupo e o produto por um escalar é definido naturalmente. Vamos denotar por $m = m_G$ a dimensão de $\overline{G}$ sobre $\mathbb{F}_2$. Assim,

$$m = m_G = \begin{cases} n, \text{ se } G = A(n, \theta) \\ 2n, \text{ se } G = \mathcal{B}(n) \end{cases}.$$

A aplicação $\overline{(a, 0)} \mapsto a$ de $\overline{G}$ em $\mathbb{F}_{2^m}$ é um isomorfismo $\mathbb{F}_2$-linear. Sendo assim, vamos identificar $\overline{G}$ com $\mathbb{F}_{2^m}$. Da mesma forma a aplicação $I_G \to \mathbb{F}_{2^n}$, definida por $(0, b) \mapsto b$, é um isomorfismo $\mathbb{F}_2$-linear, e assim podemos identificar I_G com $\mathbb{F}_{2^n}$.

Dado um $\varphi \in \mathcal{A}$ denotaremos por $\overline{\varphi}$ o automorfismo de $\overline{G}$ induzido por φ, isto é, $\overline{\varphi} : \overline{x} \mapsto \overline{x\varphi}$. Agora, desde que $\overline{G}$ é abeliano elementar de dimensão m, se tem que $\mathrm{Aut}(\overline{G}) = \mathrm{GL}(m, 2)$. Assim, $\overline{\varphi}$ pode ser considerado como um elemento de $\mathrm{GL}(m, 2)$. Similarmente desde que I_G é abeliano elementar de dimensão n, se tem que $\mathrm{Aut}(I_G) = \mathrm{GL}(n, 2)$. Como I_G é característico, dado $\varphi \in \mathcal{A}$ temos que $\varphi|_{I_G}$ pode ser considerado como um elemento de $\mathrm{GL}(n, 2)$.

Vamos denotar por K o núcleo da aplicação $\varphi \mapsto \overline{\varphi}$ de $\mathcal{A}$ em $\mathrm{Aut}(\overline{G}) = \mathrm{GL}(m, 2)$. Sendo assim, o grupo $\overline{\mathcal{A}} = \mathcal{A}/K$ pode ser considerado como um subgrupo de $\mathrm{GL}(m, 2)$. Vamos ter assim a seguinte sequência exata curta

$$1 \longrightarrow K \xrightarrow{i} \mathcal{A} \xrightarrow{\pi} \overline{\mathcal{A}} \longrightarrow 1.$$

O objetivo neste capítulo será mostrar o seguinte teorema

Teorema 3.1.1. *Temos K é abeliano elementar de ordem 2^{nm} e $\overline{\mathcal{A}}$ é isomorfo a $\Gamma\mathrm{L}(1, 2^m)$.*

Este teorema dará a estrutura completa do grupo de automorfismos dos grupos $A(n, \theta)$ e $\mathcal{B}(n)$. Demonstraremos parcialmente este teorema na primeira seção, onde somente mostraremos a primeira afirmação. A demonstração deste fato é essencialmente a mesma para os dois grupos, e não precisamos introduzir mais conceitos para demonstrar este. A demonstração do teorema será completada nas duas próximas seções. Embora a segunda afirmação feita no teorema seja a mesma para os dois grupos, a demonstração em cada caso será muito diferente. Porém, nos dois casos usaremos a teoria do capítulo 1.

Notemos que dado $\varphi \in \mathcal{A}$, o mesmo está em K se, e somente se, para cada $x \in G$ existe $z_x \in I_G$ tal que $x\varphi = xz_x$.

Lembremos que I_G é característico. Assim, podemos definir a aplicação $\varphi \mapsto \varphi|_{I_G}$ de $\mathcal{A}$ em $\mathrm{Aut}(I_G) = \mathrm{GL}(n, 2)$. Denotemos por L o núcleo desta aplicação.

Lema 3.1.2. *Temos que $K \leq L$.*

Demonstração. Dado $\varphi \in K$ temos que $x\varphi = xz_x$, onde $z_x \in I_G$, e segue que $x^2\varphi = (xz_x)^2$. Agora, pela proposição 2.2.3 temos que $Z(G) = I_G = G^2$; é dizer, toda involução é central; isto vai implicar que

$$x^2\varphi = (xz_x)^2 = x^2 z_x^2 = x^2.$$

Assim, $x^2\varphi = x^2$ para todo $x \in G$. Logo, desde que toda involução é um quadrado, segue que $\varphi|_{I_G} = 1$. Portanto $K \leq L$ como foi afirmado. □

Nós vimos que dado $\varphi \in K$, temos que para cada $x \in G$ existe $z_x \in I_G$ tal que $x\varphi = xz_x$. Mostremos que a escolha de z_x é independente da classe de x em $\overline{G}$, isto é, se $\overline{x} = \overline{y}$ então $z_x = z_y$. Vejamos, sejam $x, y \in G$ tais que $\overline{x} = \overline{y}$, então existe $z' \in I_G$ tal que $x = yz'$. Desde que $K \leq L$ e toda involução é central, vamos ter

$$yz'z_x = xz_x = x\varphi = (yz')\,\varphi = (y\varphi)\,(z'\varphi) = yz_yz' = yz'z_y.$$

De onde podemos concluir $z_x = z_y$, e assim a escolha de z_x não depende da classe de x. Agora, desde que toda involução é central, dados $x, y \in G$ temos que

$$xyz_{xy} = (xy)\varphi = (x\varphi)(y\varphi) = (xz_x)(yz_y) = xy(z_xz_y),$$

o que implica $z_{xy} = z_xz_y$. Logo, a aplicação $\zeta_\varphi : \overline{G} \to I_G$, definida por $\overline{x}\zeta_\varphi = z_x$, é um elemento de $\mathrm{Hom}_{\mathbb{F}_2}(\overline{G}, I_G)$, e podemos escrever $x\varphi = x(\overline{x}\zeta_\varphi)$.

O seguinte lema vai dar como consequência a primeira afirmação do teorema 3.1.1. Este mostrará que K é isomorfo a $\mathrm{Hom}_{\mathbb{F}_2}(\overline{G}, I_G)$.

Lema 3.1.3. *Se tem que $K \cong \mathrm{Hom}_{\mathbb{F}_2}(\overline{G}, I_G)$. Consequentemente, K é abeliano elementar e $|K| = 2^{nm}$.*

Demonstração. Definamos a aplicação $\Lambda : K \to \mathrm{Hom}(\overline{G}, I_G)$ por $\varphi \mapsto \zeta_\varphi$, e mostremos que Λ é um isomorfismo.

i) Λ é um homomorfismo: Se $\varphi, \psi \in K$ são tais que $x\varphi = xz_x$ e $x\psi = xz'_x$, ou seja $\overline{x}\zeta_\varphi = z_x$ e $\overline{x}\zeta_\psi = z'_x$. Então

$$x(\overline{x}\zeta_{\varphi\psi}) = x\varphi\psi = (xz_x)\,\psi = (x\psi)\,(z_x\psi) = xz'_x z_x = xz_x z'_x = x(\overline{x}\zeta_\varphi)(\overline{x}\zeta_\psi).$$

Por tanto $(\overline{x}\zeta_{\varphi\psi}) = (\overline{x}\zeta_\varphi)(\overline{x}\zeta_\psi)$, o que implica $\zeta_{\varphi\psi} = \zeta_\varphi\zeta_\psi$. Assim, Λ é um homomorfismo.

ii) Λ é injetiva: Seja $\varphi \in K$ tal que $\overline{x}\zeta_\varphi = 1$, para todo $\overline{x} \in \overline{G}$. Então $x\varphi = x(\overline{x}\zeta_\varphi) = x$ para todo $x \in G$. Logo, φ é a aplicação identidade e o núcleo de Λ é trivial. Assim, Λ é injetiva.

iii) Λ é sobrejetivo: Dada $\zeta \in \mathrm{Hom}\big(\overline{G}, I_G\big)$ podemos definir $\varphi : G \to G$ por $x\varphi = x(\overline{x}\zeta)$. Este φ é um homomorfismo:

$$(xy)\,\varphi = xy(\overline{xy}\zeta) = xy(\overline{x}\zeta)(\overline{y}\zeta) = (x(\overline{x}\zeta))\,(y(\overline{y}\zeta)) = (x\varphi)\,(y\varphi)\,.$$

Para mostrar que φ é um automorfismo resta só mostrar que φ é injetiva. Seja $x \in G$ tal que $x\varphi = 1$, então $x(\overline{x}\zeta) = 1$, o que implica que $x = (\overline{x}\zeta)^{-1} \in I_G$. Logo $\overline{x}\zeta = \overline{1} = 1$, o que por sua vez diz que $x = 1$. Assim, φ é injetiva.

Assim, Λ é um isomorfismo.

Como $K \cong \mathrm{Hom}_{\mathbb{F}_2}(\overline{G}, I_G)$, K é abeliano elementar, e $|K| = |\,\mathrm{Hom}_{\mathbb{F}_2}(\overline{G}, I_G)| = 2^{nm}$. Culminando assim a prova do lema e da primeira afirmação do teorema 3.1.1. $\square$

Vamos lembrar do capitulo 2, na seção 2.1 para $G = A(n, \theta)$ e na seção 2.4 para $G = \mathcal{B}(n)$, que temos os seguintes subgrupos de $\mathcal{A}$

$$X = \{\xi_\lambda \mid \lambda \in \mathbb{F}_{2^m}^\times\}, \text{ onde } \quad (a, b)\xi_\lambda = (\lambda a, \lambda^{\theta+1} b)$$

$$\Sigma = \{\varphi_\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{F}_{2^m})\}, \text{ onde } \quad (a,b)\varphi_\sigma = (a^\sigma, b^\sigma).$$

No caso de $G = \mathcal{B}(n)$ temos que θ é o automorfismo $a \mapsto a^{2^n}$.

Também mostramos, nessas mesmas seções, que

$$X \rtimes \Sigma \leq \mathcal{A}.$$

Vamos chamar de $\overline{X}$ e $\overline{\Sigma}$ os grupos induzidos em $\overline{\mathcal{A}}$ por X e Σ, respectivamente, isto é, $\overline{X} = \{\overline{\xi_\lambda} \mid \lambda \in \mathbb{F}_{2^m}^\times\}$ e $\overline{\Sigma} = \{\overline{\varphi_\sigma} \mid \sigma \in \mathrm{Aut}(\mathbb{F}_{2^n})\}$, onde $\overline{\xi_\lambda} : \overline{(a,0)} \mapsto \overline{(\lambda a, 0)}$ e $\overline{\varphi_\sigma} : \overline{(a,0)} \mapsto \overline{(a^\sigma, 0)}$. Temos que $(X \rtimes \Sigma) \cap K = \{1\}$. De fato, dado $\xi_\lambda \varphi_\sigma \in X \rtimes \Sigma$, este está em K se, e somente se, $\lambda^\sigma a^\sigma = a$ para todo $a \in \mathbb{F}_{2^n}$. Se $a = 1$ temos $\lambda^\sigma = 1$, o que implica $\lambda = 1$, substituindo isto temos $a^\sigma = a$ para todo $a \in \mathbb{F}_{2^n}$, o que dá $\sigma = 1$. Logo, $(X \rtimes \Sigma) \cap K = \{1\}$. Assim

$$X \rtimes \Sigma \cong \frac{X \rtimes \Sigma}{(X \rtimes \Sigma) \cap K} \cong \frac{(X \rtimes \Sigma)K}{K} = \overline{X} \rtimes \overline{\Sigma} \leq \overline{\mathcal{A}}, \tag{3.1}$$

ou seja, $\overline{X} \rtimes \overline{\Sigma}$ é uma copia isomorfa em $\mathcal{A}$ de $X \rtimes \Sigma$.

Com a identificação $\overline{(a,0)} \mapsto a$, de $\overline{G}$ com $\mathbb{F}_{2^m}$, as aplicações $\overline{\xi_\lambda}$ e $\overline{\varphi_\sigma}$ podem ser consideradas como aplicações lineares de $\mathbb{F}_{2^m}$ em $\mathbb{F}_{2^m}$ dadas por $\mu_\lambda : a \mapsto \lambda a$ e o próprio σ, respectivamente. Sendo assim, $\overline{X}$ pode ser considerado como sendo $\{\mu_\lambda \mid \lambda \in \mathbb{F}_{2^m}^\times\}$, e $\overline{\Sigma}$ pode ser considerado como $\mathrm{Aut}(\mathbb{F}_{2^m})$. É importante notar que, desde que $\overline{X}$ é cíclico de ordem $2^m - 1$, temos que $\overline{X}$ é um grupo de Singer em $\mathrm{GL}(m,2)$, e que, pelo lema 1.4.8, $\overline{X} \rtimes \overline{\Sigma}$ é o seu normalizador em $\mathrm{GL}(m,2)$, e assim $\overline{X} \rtimes \overline{\Sigma}$ é isomorfo a $\Gamma\mathrm{L}(1, 2^m)$. O grupo $\overline{X} \rtimes \overline{\Sigma}$ será denotado por $\overline{D}$. Com isto temos mostrado o seguinte lema.

Lema 3.1.4. *O grupo $\overline{\mathcal{A}}$ contém um subgrupo isomorfo a $\Gamma\,\mathrm{L}(1, 2^m)$.*

Este lema contém uma afirmação que sugere que estamos pelo caminho certo, este já é um primeiro passo para mostrar a segunda afirmação do teorema 3.1.1.

Vamos terminar esta seção mostrando um corolário do teorema 3.1.1, que vale tanto para $A(n,\theta)$ como para $\mathcal{B}(n)$, e cuja demonstração é a mesma para os dois casos. Evidentemente vamos assumir o teorema 3.1.1.

Corolário 3.1.5. *Seja G é algum grupo $A(n,\theta)$ ou $\mathcal{B}(n)$ e $\mathcal{A} = \mathrm{Aut}(G)$, então $\mathcal{A}$ é solúvel. Além disso, $\mathcal{A} = K \rtimes (X \rtimes \Sigma)$.*

Demonstração. Do teorema 3.1.1 temos que $\overline{\mathcal{A}} = \mathcal{A}/K$ é isomorfo a $\Gamma\mathrm{L}(1, 2^n)$ e que K é abeliano. Logo, $\overline{\mathcal{A}}$ e K são solúveis, de onde se tem que $\mathcal{A}$ é solúvel.

Nós já mostramos que $(X \rtimes \Sigma) \cap K = \{1\}$ e como $K \trianglelefteq \mathcal{A}$, segue que $K \rtimes (X \rtimes \Sigma) \leq \mathcal{A}$. Pelo teorema 3.1.1 temos que $|\mathcal{A}| = |K||\Gamma \mathrm{L}(1, 2^n)| = 2^{n^2}(2^n - 1)n = |K \rtimes (X \rtimes \Sigma)|$. Logo, $\mathcal{A} = K \rtimes (X \rtimes \Sigma)$. $\square$

Uma observação importante que podemos fazer é que determinando o grupo $\mathcal{A}$ da maneira que nós fizemos o teorema enunciado por Bryukhanova, ver [6, Teorema 2] (o qual afirma que o grupos de automorfismos dos 2-grupos de Suzuki são solúveis) é um corólario direto, como já mostramos, de nossa determinação. Embora Lewis, no seu artigo [9, Teorema 8.5], tenha obtido a mesma determinação que obtemos para o caso $A(n, \theta)$, ele usou o fato da solubilidade e nós usamos a teoria de grupos de Singer, e demos como corolário o fato da solubilidade mostrado por Bryukhanova.

Como uma aplicação do teorema 3.1.1 damos o seguinte corolário. Este corolário verfica parcialmente a conjetura feita por Glasby, Pálfy e Schneider em [11].

Corolário 3.1.6. *Se G é um 2-grupo de Suzuki isomorfo a $A(n, \theta)$ ou a $\mathcal{B}(n)$, então G tem somente três subgrupos característicos.*

Demonstração. Por [11, teorema 4] é suficiente mostrar que $\mathrm{Aut}(G)$ age irredutivelmente em I_G e em $\overline{G}$. Como $A(n, \theta)$ e $\mathcal{B}(n)$ são 2-grupos de Suzuki a ação de $\mathrm{Aut}(G)$ age transitivamente, logo irredutivelmente, em I_G. Agora, como o grupo $X = \{\xi_\lambda \mid \lambda \in \mathbb{F}_{2^m}^\times\}$, age em ambos casos em $\overline{G}$ por multiplicação por λ, se tem que X age transitivamente, logo irredutivelmente, em $\overline{G}$. $\square$

3.2 Demonstração do teorema 3.1.1 para $G = A(n, \theta)$

Nesta seção vamos demonstrar a segunda afirmação do teorema 3.1.1 para o caso que G é o 2-grupo de Suzuki $A(n, \theta)$. Neste caso vamos ter que $m = \dim_{\mathbb{F}_2} \overline{G} = n$. Lembremos, do capítulo 2, que o automorfismo θ é de ordem ímpar, e que

$$G = \left\{ (a, b) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^\theta \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{F}_{2^n} \right\},$$

com a multiplicação definida por

$$(a_1, b_1)(a_2, b_2) = (a_1 + a_2, b_1 + b_2 + a_1 a_2^\theta).$$

Vamos agora analisar um automorfismo de G usando as ideias Kazarin e Sidel'nikov [8], e de Lewis [9]. Seja $\varphi \in \mathcal{A}$, da proposição 2.2.3 temos que $I_G = \{(0,b) \mid b \in \mathbb{F}_{2^n}\}$. Desde que I_G é um subgrupo característico de G se tem que $(I_G)\varphi = I_G$. Logo, existe $h_\varphi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ tal que $(0,b)\,\varphi = (0, bh_\varphi)$. Desde que $\varphi|_{I_G}$ é um automorfismo de I_G se tem que h_φ é linear e bijetiva. Agora, sejam f_φ e g_φ as aplicações tais que $(a,0)\,\varphi = (af_\varphi, ag_\varphi)$. Por (2.5), se tem que $\overline{G} = G/I_G = \{\overline{(a,0)} \mid a \in \mathbb{F}_{2^n}\}$. O automorfismo φ induz um automorfismo em $\overline{G}$ dado por $\overline{(a,0)} \mapsto \overline{(a,0)\,\varphi} = \overline{(af_\varphi, ag_\varphi)} = \overline{(af_\varphi, 0)}$, isto implica que a aplicação f_φ é uma tranformação linear bijectiva. Desde que $(a,b) = (a,0)(0,b)$ se tem que $(a,b)\varphi = (af_\varphi, ag_\varphi + bh_\varphi)$. Agora, dado $(a,0) \in G$ se tem que

$$\begin{aligned} ((a,0)^2)\varphi &= ((a,0)\,\varphi)^2 \\ &= (af_\varphi, ag_\varphi)^2 \\ &= \left(0, (af_\varphi)^{\theta+1}\right). \end{aligned}$$

Por outro lado

$$\begin{aligned} ((a,0)^2)\varphi &= \left(0, a^{\theta+1}\right)\varphi \\ &= \left(0, \left(a^{\theta+1}\right) h_\varphi\right). \end{aligned}$$

Assim, f_φ, h_φ satisfazem $\left(a^{\theta+1}\right) h_\varphi = (af_\varphi)^{\theta+1}$.

Temos mostrado assim as partes i) e ii) do seguinte lema.

Lema 3.2.1 ([9], Lema 8.1)**.** *Seja φ um automorfismo de G. Então existem bijeções $\mathbb{F}_2$-lineares f_φ, h_φ de $\mathbb{F}_{2^n}$ e uma aplicação $g_\varphi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ tais que*

i) $(a,b)\varphi = (af_\varphi, ag_\varphi + bh_\varphi)$.

ii) $\left(a^{\theta+1}\right) h_\varphi = (af_\varphi)^{\theta+1}$, *para todo* $a \in \mathbb{F}_{2^n}$.

iii) $(0)\,g = 0$.

iv) Se $(a_1^\theta a_2)h_\varphi = (a_1 f_\varphi)^\theta\,(a_2 f_\varphi)$ *para todo* $a_1, a_2 \in \mathbb{F}_{2^n}$*, então a aplicação* g_λ *é linear.*

A demonstração dos itens iii) e iv) não é tão importante para nossos fins, já que $\mathcal{A}$ pode se obter sem usar estes itens. Sendo assim, nós não provaremos estes. Uma demonstração completa deste lema pode ser encontrada em [9].

Chamemos de $\chi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ a aplicação definida por $a \mapsto a^{\theta+1}$. Notemos que, desde que θ tem ordem ímpar, o lema 2.1.3 diz que χ é uma bijeção. Sendo assim, a condição em f_φ, h_φ pode ser escrita como $(a\chi)h = (af)\chi$ para todo $a \in \mathbb{F}_{2^n}$, ou seja $\chi h_\varphi = f_\varphi \chi$; equivalentemente $(f_\varphi)^\chi = \chi^{-1} f_\varphi \chi = h_\varphi$.

Lema 3.2.2. *A aplicação $\chi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, definida por $a \mapsto a^{\theta+1}$, não é aditiva.*

Demonstração. Suponhamos que χ seja aditiva, então para todo $a, b \in \mathbb{F}$ devemos ter $a\chi + b\chi = (a+b)\chi$, e desde

$$a\chi + b\chi \;=\; a^{\theta+1} + b^{\theta+1},$$

e

$$(a+b)\chi \;=\; (a+b)^{\theta+1} = (a+b)^\theta (a+b) = a^{\theta+1} + b^{\theta+1} + a^\theta b + ab^\theta,$$

segue que $a^\theta b = ab^\theta$ para todo $a, b \in \mathbb{F}_{2^n}$, mas isso é uma contradição ao lema 2.1.3. Assim, χ não é aditiva. □

Na seção anterior vimos que um dado um $\varphi \in \mathcal{A}$ podemos considerar $\overline{\varphi} \in \overline{\mathcal{A}}$ como um elemento de $\mathrm{GL}(n, 2)$. Com o lema anterior em mãos vamos dar uma descrição mais exata disso. Dado um $\varphi \in \mathcal{A}$, pelo lema 3.2.1, existe f_φ, h_φ e g_φ tais que $(a, b)\varphi = (af_\varphi, ag_\varphi + bh_\varphi)$. Sendo assim, $\overline{(a, 0)}\overline{\varphi} = \overline{(af_\varphi, 0)}$. Com a identificação $\overline{(a, 0)} \mapsto a$ de $\overline{G}$ com $\mathbb{F}_{2^n}$, podemos considerar $\overline{\varphi}$ como sendo a transformação linear f_φ. Notemos que no caso que $\varphi \in \overline{X}$ se tem $f_\varphi = \mu_\lambda : a \mapsto \lambda a$, e no caso de $\varphi \in \Sigma$ se tem $f_\varphi = \sigma$, como já foi visto na seção anterior.

Desde que $\overline{X} \leq \overline{\mathcal{A}} \leq \mathrm{GL}(n, 2)$, é dizer, $\overline{\mathcal{A}}$ contém o grupo de Singer $\overline{X}$ de $\mathrm{GL}(n, 2)$, segue do teorema 1.4.11, que existe um divisor d de n tal que $\mathrm{GL}(d, 2^{n/d}) \trianglelefteq \overline{\mathcal{A}}$, onde nós consideramos o espaço $\mathbb{F}_{2^n}$ como sendo $(\mathbb{F}_{2^{n/d}})^d$ e $\mathbb{F}_{2^{n/d}}$ como um subcorpo de $\mathbb{F}_{2^n}$. Para abreviar um pouco a notação vamos chamar de Y o grupo $\mathrm{GL}(d, 2^{n/d})$.

Notemos que $Z(Y) \leq \overline{X}$. De fato, pelo lema 1.2.4, $Z(Y) = \{\lambda I_n \mid \lambda \in \mathbb{F}_{2^{n/d}}^\times\}$, então dado $z \in Z(Y)$ existe um $\lambda \in \mathbb{F}_{2^{n/d}}^\times$, tal que $vz = \lambda v$ para todo $v \in (\mathbb{F}_{2^{n/d}})^d \cong \mathbb{F}_{2^n}$. Assim, $z = \mu_\lambda$, e segue que $z \in \overline{X}$.

O seguinte lema vai mostrar que a aplicação χ normaliza Y. Este será o último passo antes de demonstrar que $\overline{\mathcal{A}}$ é isomorfo a $\Gamma\mathrm{L}(1, 2^n)$.

Lema 3.2.3. *A aplicação χ normaliza Y.*

Demonstração. Primeiro mostremos que χ normaliza $\overline{X}$. De fato, dado $\mu_\lambda \in \overline{X}$ temos que

$$a\chi^{-1}\mu_\lambda\chi = (\lambda(a\chi^{-1}))\chi = (\lambda\chi)a = a\mu_{\lambda\chi}.$$

Logo, $\chi^{-1}\mu_\lambda\chi = \mu_{\lambda\chi} \in \overline{X}$, e χ normaliza $\overline{X}$. Agora, desde que $Z(Y) \leq \overline{X}$, vamos ter $Z(Y)^\chi \leq \overline{X}^\chi = \overline{X}$. Desde que $\overline{X}$ é cíclico, ele têm um único subgrupo de ordem $|Z(Y)| = |Z(Y)^\chi|$. Logo, $Z(Y)^\chi = Z(Y)$, e pelo lema 1.4.12 vamos ter

$$Y = C_{\mathrm{GL}(n,2)}(Z(Y)) = C_{\mathrm{GL}(n,2)}(Z(Y)^\chi) = Y^\chi.$$

Assim, χ normaliza Y. □

O que segue é a demonstração da segunda parte do teorema 3.1.1. Com os resultados anteriores em mãos este não será difícil de demonstrar. Antes disso, é necessário lembrar que desde que os elementos de $\mathrm{GL}(d, 2^{n/d})$ permutam os elementos de $\mathbb{F}_{2^n} = (\mathbb{F}_{2^{n/d}})^d$ e fixam $\{0\}$, ele pode ser considerado como subgrupo de $\mathrm{Sym}(\mathbb{F}_{2^n}^\times)$.

Demonstração do teorema para o caso $G = A(n, \theta)$

Do lema 3.2.3, temos que χ normaliza Y. Assumamos que $d \geq 2$, então o teorema 1.3.1 diz que $\Gamma\mathrm{L}\big(d, 2^{n/d}\big)$ é o normalizador de Y em $\mathrm{Sym}\big(\mathbb{F}_{2^n}^\times\big)$, assim $\chi \in \Gamma\mathrm{L}\big(d, 2^{n/d}\big)$. Logo, teremos que $(u+v)\chi = u\chi + v\chi$ para todo $u, v \in \mathbb{F}_q$, é dizer, χ é aditiva, o que é uma contradição ao lema 3.2.2. Assim, devemos ter $d = 1$. Logo, $Y = \mathrm{GL}(1, 2^n) \leq \overline{\mathcal{A}} \leq \mathrm{GL}(n, 2)$, mas desde que $|Y| = 2^n - 1$, se tem que Y é um ciclo de Singer em $\mathrm{GL}(2, n)$. Como $Y \lhd \overline{\mathcal{A}}$ se tem que $A \leq N_{\mathrm{GL}(n,2)}(Y)$, e desde que $N_{\mathrm{GL}(n,2)}(Y)$ é isomorfo a $\Gamma\mathrm{L}(1, 2^n)$ temos que $\overline{\mathcal{A}}$ é isomorfo a um subgrupo de $\Gamma\mathrm{L}(1, 2^n)$. Agora, pelo lema 3.1.4, $\overline{\mathcal{A}}$ contém um subgrupo isomorfo a $\Gamma\mathrm{L}(1, 2^n)$. Logo, podemos concluir que $\mathcal{A}$ é isomorfo a $\Gamma\mathrm{L}(1, 2^n)$. Culminando assim a demonstração do teorema 3.1.1.

3.3 Demonstração do teorema 3.1.1 para $G = \mathcal{B}(n)$

Nesta seção vamos demonstrar a segunda afirmação do teorema 3.1.1 para o caso $G = \mathcal{B}(n)$. Observemos que neste caso vamos ter $m = 2n$. Como já foi dito, o que faremos nesta seção será seguir a prova dada por Landrock [5, Teorema 1.1].

Lembremos do capítulo 2 que

$$G = \left\{ (a,b) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & a^{2^n} \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{F}_{2^{2n}} \text{ e } b^{2^n} + b + a^{2^n+1} = 0 \right\},$$

com multiplicação dada por

$$(a_1, b_1)(a_2, b_2) = (a_1 + a_2, b_1 + b_2 + a_1 a_2^{2^n}).$$

Da seção 3.1 temos que $\overline{D} = \overline{X} \rtimes \overline{\Sigma} \leq \overline{\mathcal{A}} \leq \mathrm{GL}(2n, 2)$, onde

$$\overline{X} = \{\mu_\lambda \mid \lambda \in \mathbb{F}_{2^{2n}}^\times\} \quad \text{e} \quad \overline{\Sigma} = \mathrm{Aut}(\mathbb{F}_{2^{2n}}),$$

são cópias isomorfas a

$$X = \{\xi_\lambda \mid \lambda \in \mathbb{F}_{2^{2n}}\} \quad \text{e} \quad \Sigma = \{\varphi_\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{F}_{2^{2n}})\},$$

no grupo $\overline{\mathcal{A}}$.

É importante, neste momento, notar que o grupo X que temos acima não é o mesmo que o considerado por Landrock, [5, p. 202]. Ele considera o grupo $\mathcal{X} = \{\phi_\lambda \mid \lambda \in \mathbb{F}_{2^{2n}}^\times\}$, onde $\phi_\lambda : (a, b) \mapsto (\lambda^{2^{n+1}-1} a, \lambda^{2^n+1} b)$. Embora este grupo tenha ordem $2^{2n} - 1$ ele não tem uma cópia isomorfa em $\overline{\mathcal{A}}$, e não pode ser considerado como um grupo de Singer em $\mathrm{GL}(2n, 2)$.

Seja $\overline{C}$ o subgrupo cíclico de ordem $2^n + 1$ do grupo de Singer $\overline{X}$. Vamos mostrar que o grupo $\overline{C}$ age irredutivelmente no $\mathbb{F}_2$-espaço vetorial $\overline{G}$. Aplicando o teorema de Zsigmondy temos que existe um primo r tal que $r \mid 2^{2n} - 1$ e $r \nmid 2^i - 1$ para $i < 2n$, exceto no caso $2n = 6$. Sendo assim, se $n \neq 3$ temos que $\overline{C}$ age irredutivelmente em $\overline{G}$. Analisamos o caso $n = 3$ separadamente. Como $\overline{X} = \{\mu_\lambda \mid \lambda \in \mathbb{F}_{2^{2n}}^\times\}$, onde $\mu_\lambda : a \mapsto \lambda a$, se tem que $\overline{X}$ é semiregular no conjunto de vetores não nulos (ver seção 1.1), e segue que $\mathrm{Fix}(\overline{C}) = \{0\}$. Suponhamos que exista um subespaço U de $\overline{G}$ não nulo de $\overline{G}$, que seja $\overline{C}$-invariante, com $|U| = 2^r$ e $r > 0$. Então, como $|\overline{C}| = 2^3 + 1 = 9$, pelo teorema 1.1.1 se tem que o tamanho de cada órbita de U é 1 ou 9, e a única órbita de tamanho 1 é $\{0\}$. Assim, temos que

$$|U| - 1 = 9k,$$

ou seja, $9 \mid 2^r - 1$, mas isso é possível somente se $r = 6$. Logo, $U = \overline{G}$. Assim $\overline{C}$ age irredutivelmente em $\overline{G}$. Assim, sempre temos que $\overline{C}$ age irredutivelmente em $\overline{G}$.

Como $\overline{C}$ age irredutivelmente em $\overline{G}$, o corolário 1.4.7 implica que

$$C_{\overline{\mathcal{A}}}(\overline{C}) = C_{\mathrm{GL}(2n,2)}(\overline{C}) \cap \overline{\mathcal{A}} = \overline{X} \cap \overline{\mathcal{A}} = \overline{X}, \tag{3.2}$$

e o lema 1.4.8 implica que

$$N_{\overline{\mathcal{A}}}(\overline{C}) = N_{\mathrm{GL}(2n,2)}(\overline{C}) \cap \overline{\mathcal{A}} = \overline{D} \cap \overline{\mathcal{A}} = \overline{D}. \tag{3.3}$$

Vamos dar o primeiro passo na demonstração da segunda parte do teorema 3.1.1. O lema que segue dará informação sobre a estrutura de $\overline{D}$, que precisaremos para provar o resultado principal.

Lema 3.3.1. *Não existe subgrupo H de $\overline{D}$, e subgrupo normal N de H satisfazendo $H/N \cong (C_2)^k$ com $k \geq 2$.*

Demonstração. Suponhamos que existem H e N tais que $H \leq \overline{D}$ e $N \trianglelefteq H$, com $H/N \cong (C_2)^k$. Primeiro vejamos que todo 2-subgrupo de Sylow de $\overline{D} = \overline{X} \rtimes \overline{\Sigma}$ tem que ser cíclico. Seja S um 2-subgrupo de Sylow de $\overline{D}$. Como $2^{2n} - 1$ é ímpar, S é conjugado a um subgrupo de $\overline{\Sigma}$, e assim S é cíclico. Agora, seja S_1 um 2-subgrupo de Sylow de H. Temos que S_1 é cíclico, já que ele está contido em algum 2-subgrupo de Sylow de $\overline{D}$. Se tem que S_1N/N é 2-subgrupo de Sylow de H/N, logo $(C_2)^k = S_1N/N \cong S_1/(N \cap S_1)$. Como S_1 é cíclico e todo quociente de S_1 é cíclico, isso implica que $k = 1$. $\square$

Lembremos, da seção 3.1, que L é o núcleo da aplicação $\mathcal{A} \to \mathrm{Aut}(I_G)$, definida por $\varphi \mapsto \varphi|_{I_G}$; e também que $K \leq L$. Desde que $K \trianglelefteq \mathcal{A}$ segue que $K \trianglelefteq L$. Logo, o grupo $\overline{L} = L/K$ é um subgrupo normal de $\overline{\mathcal{A}}$. Mostremos que $\overline{X} \cap \overline{L} = \overline{C}$. Dado $\mu_\lambda \in \overline{X}$, ele está em $\overline{L}$ se, e somente se, seu respectivo ξ_λ está em L, ou seja, dado $(0, b) \in I_G$ se tem $(0, \lambda^{2^n+1})(0, b)\xi_\lambda = (0, b)$. Isto dá $b = \lambda^{2^n+1}b$, de onde $\lambda^{2^n+1} = 1$. Assim, $\xi_\lambda \in C$, onde C é o subgrupo de X que corresponde a $\overline{C}$. Assim, $X \cap L \leq C$. Claramente, dado um $\xi_\lambda \in C$ se tem que o mesmo fixa as involuções de G. Logo, devemos ter $X \cap L = C$. De onde segue $\overline{X} \cap \overline{L} = \overline{C}$. Aplicando o corolário 1.4.7 temos que

$$C_{\overline{L}}(\overline{C}) = C_{\mathrm{GL}(2n,2)}(\overline{C}) \cap \overline{L} = \overline{X} \cap \overline{L} = \overline{C}. \tag{3.4}$$

Neste ponto precisamos da estrutura do grupo $\overline{L}$. A diferença com o método da seção anterior começa aqui. O lema que segue vai nos dar a estrutura do maior 2-subgrupo normal em $\mathcal{A}$, este lema é indispensável para a demonstração que seguiremos. Nós não precisamos de um resultado deste tipo na seção anterior para a determinação de $\mathcal{A}$. Este mesmo resultado no caso $G = A(n, \theta)$ pode ser obtido como corolário da nossa determinação.

Lema 3.3.2. *O maior* 2*-subgrupo normal de* $\mathcal{A}$ *é* K*.*

Demonstração. Vamos mostrar que o maior 2-subgrupo normal de $\overline{\mathcal{A}} = \mathcal{A}/K$ é $\{1\}$. Isto implicará imediatamente que o maior 2-subgrupo normal de $\mathcal{A}$ é K. Lembremos que a ação de $\overline{X} = \{\mu_\lambda \mid \lambda \in \mathbb{F}_{q^2}^\times\}$ em $\overline{G}$ está dada por $a\mu_\lambda = \lambda a$. Assim, o subgrupo X age transitivamente, logo irredutivelmente, em $\overline{G}$. De onde segue que $\overline{\mathcal{A}}$ age irredutivelmente em $\overline{G}$. Assim, pelo lema 1.4.1 segue que o único 2-subgrupo normal de $\overline{\mathcal{A}}$ é $\{1\}$, de onde segue o afirmado no lema. □

Pelo lema 3.3.2 o maior 2-subgrupo normal de $\mathcal{A}$ é K, e como $L \trianglelefteq \mathcal{A}$ e o maior 2-subgrupo normal de L é característico, segue que, o maior 2-subgrupo normal de L é K. Para continuar com a nossa digressão vamos precisar do teorema de Hawkes, teorema 1.5.3. Aplicando este teorema para nosso caso, temos que $\overline{L} = L/K$ pode ser considerado como um subgrupo de $D_{2q_1} \times \cdots \times D_{2q_k}$, onde D_{2q_i} é um subgrupo diedral de ordem $2q_i$, com q_i potência de primo ímpar.

Lema 3.3.3. *Se tem* $\overline{C} \trianglelefteq \overline{L}$ *e* $\overline{L}/\overline{C} \cong C_2$*. Em particular* $|\overline{L}| = 2(q+1)$ *e* $\overline{C}$ *é caraterístico em* $\overline{L}$*.*

Demonstração. Pelo teorema 1.5.3 podemos considerar $\overline{L}$ como contido no grupo $R = D_{2q_1} \times \cdots \times D_{2q_k}$, onde $D_{2q_i} = C_{q_i} \rtimes C_2$ é um subgrupo diedral de ordem $2q_i$, com q_i potência de primo ímpar. Seja $R_1 = C_{q_1} \times \cdots \times C_{q_k}$. Então, desde que $C_{q_1} \trianglelefteq D_{2q_i}$, temos que R_1 é subgrupo abeliano e normal de R, com quociente R/R_1 isomorfo a $(C_2)^k$. Logo, $\overline{C}/(\overline{C} \cap R_1) \cong \overline{C}R_1/R_1 \leq R/R_1$. Como $\overline{C}$ tem ordem ímpar e $|R/R_1| = 2^k$, temos que $\overline{C}/(\overline{C} \cap R_1) = 1$, o que implica $\overline{C} \leq R_1$, e desde que $\overline{C} \leq \overline{L}$ se tem $\overline{C} \leq R_1 \cap \overline{L}$. Por outro lado, desde que R_1 é abeliano $\overline{L} \cap R_1 \leq C_{\overline{L}}(\overline{C}) = \overline{C}$ (ver 3.4), e assim $\overline{C} = \overline{L} \cap R_1$, e desde que R_1 é normal em R, e $\overline{L} \leq R$, vamos ter $\overline{C} \trianglelefteq \overline{L}$. Agora, $\overline{L}/\overline{C} = \overline{L}/(R_1 \cap \overline{L}) \cong \overline{L}R_1/R_1 \leq R/R_1$ e assim $\overline{L}/\overline{C}$ é isomorfo a um produto direto $(C_2)^{k'}$. Por outro lado, desde que $\overline{C} \trianglelefteq \overline{L}$, segue que $\overline{L} \leq N_{\overline{\mathcal{A}}}(\overline{C}) = \overline{D}$(ver 3.3) . Pelo lema 3.3.1, $\overline{D}$ não contém nenhuma seção na forma $C_2 \times C_2$. Assim, temos que ter $k' = 1$. Desde que $\overline{L}/\overline{C}$ é isomorfo a $C_2^{k'} = C_2$, se tem $|\overline{L}| = 2(q+1)$.

Como $\overline{C}$ tem ordem ímpar e índice 2 em $\overline{L}$, $\overline{C}$ é o único subgrupo normal com índice 2. Logo, $\overline{C}$ é caraterístico em $\overline{L}$. $\square$

Agora estamos em condições de mostrar a segunda afirmação do teorema 3.1.1, esta vai ser uma consequência dos resultados mostrados anteriormente.

Demonstração do teorema para o caso $G = \mathcal{B}(n)$

Desde que $\overline{L}$ é um subgrupo normal em $\overline{\mathcal{A}}$ e $\overline{C}$ é um subgrupo característico de $\overline{L}$, segue que $\overline{C}$ é um subgrupo normal de $\overline{\mathcal{A}}$. Como $\overline{D} = N_{\mathrm{GL}(2n,2)}(\overline{X}) = N_{\mathrm{GL}(2n,2)}(\overline{C})$, se tem $\overline{\mathcal{A}} \leq \overline{D}$, e desde que $\overline{D} \leq \overline{\mathcal{A}}$ temos que $\overline{\mathcal{A}} = \overline{D}$. Como $\Gamma\mathrm{L}(1, 2^{2n})$ é isomorfo ao normalizador do grupo de Singer $\overline{X}$ temos que $\overline{\mathcal{A}}$ é isomorfo a $\Gamma\mathrm{L}(1, 2^{2n})$. Culminando assim a demonstração.

Consideramos que a prova deste teorema é uma boa maneira de terminar esta seção, e assim também este trabalho.

Referências Bibliográficas

[1] E. E. Shult, "On finite automorphic algebras," *Illinois J. Math.*, vol. 13, pp. 625–653, 1969.

[2] B. Huppert and N. Blackburn, *Finite groups. II*, vol. 242 of *Grundlehren der Mathematischen Wissenschaften.* Springer-Verlag, Berlin-New York, 1982. AMD, 44.

[3] G. O. Michler, *Theory of finite simple groups*, vol. 8 of *New Mathematical Monographs.* Cambridge University Press, Cambridge, 2006.

[4] G. Higman, "Suzuki 2-groups," *Illinois J. Math.*, vol. 7, pp. 79–96, 1963.

[5] P. Landrock, "Finite groups with a quasisimple component of type PSU(3, 2^n) on elementary abelian form," *Illinois J. Math.*, vol. 19, pp. 198–230, 1975.

[6] E. G. Bryukhanova, "Automorphism groups of 2-automorphic 2-groups," *Algebra i Logika*, vol. 20, no. 1, pp. 5–21, 123, 1981.

[7] T. Hawkes, "On the automorphism group of a 2-group," *Proc. London Math. Soc. (3)*, vol. 26, pp. 207–225, 1973.

[8] L. S. Kazarin and V. M. Sidel′nikov, "On the automorphism group of the Suzuki p-algebra," *Mat. Zametki*, vol. 80, no. 4, pp. 526–535, 2006.

[9] M. L. Lewis, "Bounding group orders by large character degrees: a question of Snyder," *J. Group Theory*, vol. 17, no. 6, pp. 1081–1116, 2014.

[10] W. M. Kantor, "Linear groups containing a Singer cycle," *J. Algebra*, vol. 62, no. 1, pp. 232–234, 1980.

[11] S. P. Glasby, P. P. Pálfy, and C. Schneider, "p-groups with a unique proper non-trivial characteristic subgroup," *J. Algebra*, vol. 348, pp. 85–109, 2011.

[12] J. D. Dixon and B. Mortimer, *Permutation groups*, vol. 163 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1996.

[13] L. C. Grove, *Classical groups and geometric algebra*, vol. 39 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 2002.

[14] D. J. S. Robinson, *A course in the theory of groups*, vol. 80 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1982.

[15] S. Kohl, "Counting the orbits on finite simple groups under the action of the automorphism group—Suzuki groups vs. linear groups," *Comm. Algebra*, vol. 30, no. 7, pp. 3515–3532, 2002.

[16] B. Huppert, *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967.

[17] A. Cossidente and M. J. de Resmini, "Remarks on Singer cyclic groups and their normalizers," *Des. Codes Cryptogr.*, vol. 32, no. 1-3, pp. 97–102, 2004.

[18] S. Lang, *Algebra*, vol. 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third ed., 2002.