Universidade Federal de Minas Gerais
Instituto de Ciências Exatas - ICEx
Programa de Pós-Graduação em Matemática
Monografia de Especialização

Sobre grupos simples finitos

Maria Luiza Oliveira Santos

Belo Horizonte, Brasil
2015

Maria Luiza Oliveira Santos

Sobre grupos simples finitos

Monografia submetida à banca examinadora, designada pelo Programa de Pós-Graduação em Matemática da UFMG, como requisito parcial para a obtenção do título de especialista em Matemática.

Orientadora: Ana Cristina Vieira

Belo Horizonte, Brasil
2015

Resumo

Este trabalho tem por objetivo discutir a definição e a importância dos grupos simples finitos na teoria de grupos, além de apresentar e tratar de resultados que comprovam a simplicidadade de grupos importantes, desenvolvendo suas respectivas demonstrações.

Palavras-Chaves : Grupos finitos, grupos simples finitos, grupos lineares, Teorema de Jordan-Dickson.

Índice

Introdução

O estudo dos grupos simples finitos iniciou-se em 1830 com os trabalhos de Évariste Galois (1811-1832) e a impossibilidade de solucionar equações polinomiais de quinto grau por radicais. Um grupo é chamado simples se é não trivial e possui somente subgrupos normais triviais.

A importância do estudo dos grupos simples decorre do fato deles serem considerados como os " blocos fundamentais " dos grupos finitos, já que podemos dizer que todos os grupos finitos são " construídos " a partir dos grupos simples finitos.

Podemos dizer que os grupos simples representam um papel na teoria dos grupos semelhante ao dos números primos na teoria dos números. De fato, da mesma forma que todo número inteiro pode ser decomposto em fatores primos, temos, de modo análogo, que todo grupo pode ser " decomposto " em uma série de fatores simples.

Vamos explicar melhor. Seja G um grupo finito. Uma série de subgrupos

$$G = G_0 \supset G_1 \supset \cdots \supset G_r$$

é dita ***subnormal*** se cada G_{i+1} é um subgrupo normal de $G_i, (i = 0, 1, \cdots, r-1)$, onde os grupos quocientes $G_i/G_{i+1}, (i = 0, 1, \cdots, r-1)$ são chamados ***fatores*** da série. Uma série subnormal com comprimento máximo é chamada série de composição.

Sendo assim, vamos escolher um subgrupo normal maximal G_1 de $G = G_0$ de tal modo que o fator G_0/G_1 é simples. Analogamente, escolheremos um subgrupo normal G_2 de G_1, de forma que G_1/G_2 também é simples e continuaremos dessa maneira até chegarmos em $G_r = \{1\}$. Os grupos simples $G_0/G_1, G_1/G_2, \cdots, G_{r-1}/G_r$ são os fatores desta série. O importante Teorema de Jordan-Hölder nos garante a unicidade destes fatores (a menos de permutação). Além disso, esta série possui comprimento máximo (série de composição) já que seus fatores são simples e, portanto, não podem ser mais reduzidos. Logo, é neste sentido que os grupos simples podem ser considerados como " blocos fundamentais " .

Portanto, em certas situações, muitas das propriedades de um grupo determinam-se pela natureza dos seus fatores de composição. E daí segue que muitas perguntas sobre grupos finitos podem reduzir-se à perguntas sobre grupos simples finitos.

Com isso, reconhecer a simplicidade de um grupo ou saber quais grupos são simples, se faz importante na teoria de grupos e é esta a motivação deste trabalho. Aqui, visamos definir, apresentar e comprovar a simplicidade de alguns grupos finitos.

Começamos nosso trabalho relembrando conceitos básicos de grupos, bem como propriedades importantes dos grupos simétricos e de corpos finitos, que serão utilizadas no decorrer do texto.

Posteriormente, no Capítulo 2, daremos a definição de grupos simples e abordaremos dois testes de simplicidade. Ainda neste capítulo, trataremos da simplicidade dos grupos alternados de grau n, isto é, os grupos de permutações pares sobre n elementos.

É importante ressaltar, que embora Galois tivesse formulado a definição de grupos simples e tivesse observado a simplicidade do grupo alternado sobre 5 elementos, os primeiros e principais resultados na teoria foram devido a Jordan. Em 1870, Jordan publicou o primeiro livro sobre teoria de grupos. Neste livro estabeleceu a existência de cinco famílias infinitas de grupos simples finitos. A primeira delas é justamente os grupos alternados, que denotaremos por A_n.

Logo após, caracterizamos os grupos simples de ordem menor que 60, um resultado que permite concluir que o A_5 é o menor grupo simples de ordem composta. Também mostramos que todo grupo simples de ordem 60 é isomorfo ao A_5.

No capítulo subsequente, apresentamos os grupos lineares. A segunda família de grupos simples finitos é a dos grupos lineares especiais projetivos sobre corpos finitos. Sendo assim, neste terceiro capítulo estaremos interessados em demonstrar o Teorema de Jordan-Dickson, que salvo alguns casos que veremos, garante a simplicidades desta família de grupos.

Nas considerações finais, narramos um pouco da história envolvendo o famoso Teorema de Classificação dos grupos simples finitos. Um resultado fundamental em teoria de grupos, que mobilizou esforço e dedicação de vários matemáticos ao longo dos anos, devido a sua difícil demonstração. O Teorema de Classificação, assim como bem sugerido pelo seu nome, tem por objetivo classificar todos os grupos simples finitos conforme uma das quatro categorias que citaremos mais tarde. Finalmente, culminanos com o enunciado do Teorema de Classificação.

Capítulo 1

Preliminares

Neste capítulo listaremos de forma breve e objetiva alguns dos resultados que serão utilizados ao longo deste trabalho. Destacamos que as demonstrações da maioria desses resultados serão omitidas, podendo ser encontradas nas referências deste trabalho.

1.1 Grupos

Nesta seção relembraremos informalmente os conceitos e resultados fundamentais a respeito de grupos. Recordemos primeiramente a seguinte definição

Definição 1.1. *Um conjunto G com a operação*

$$\begin{aligned} G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

é um grupo se as seguintes condições são satisfeitas:

(i) A operação é associativa, isto é, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todos $a,\ b,\ c\ \in G$.

(ii) Existe um elemento neutro, isto é, existe $e \in G$ tal que $e \cdot a = a \cdot e = a$, para todo $a \in G$.

(iii) Todo elemento possui inverso. Ou seja, para todo $a \in G$ existe $b \in G$ tal que $a \cdot b = b \cdot a = e$.

Além disso, se a operação acima é comutativa, ou seja, $a \cdot b = b \cdot a$, para quaisquer elementos a, b em G, então dizemos que G é um grupo abeliano.

Em geral usamos a notação multiplicativa, mas, ao longo deste texto, não indicaremos a operação do grupo, escrevendo apenas G para denotar o grupo $(G, \cdot)$. Também escreveremos ab no lugar de $a \cdot b$, a^{-1} para indicar o inverso do elemento a e 1 para indicar o elemento neutro.

A ordem de um grupo G, denotada por $|G|$, é igual ao número de elementos em G. Já a ordem de um elemento g pertencente a um grupo, denotada por $|g|$, é o menor natural

m, caso exista, tal que $g^m = 1$. Se tal m não existe, dizemos que o elemento tem ordem infinita. Uma propriedade útil da ordem de um elemento é que se existe algum inteiro k tal que $g^k = 1$, então $|g|$ divide k.

Dentre os resultados que envolvem a ordem de um grupo, podemos citar o *Teorema de Cauchy*, o qual nos diz que se G é um grupo finito de ordem n e p é um número primo que divide n, então G contém um elemento de ordem p. Outro é enunciado a seguir

Teorema 1.2. *Sejam G um grupo abeliano e $m = max\{|g|; g \in G\}$. Então $|g|$ divide m para todo $g \in G$. O número m é chamado expoente do grupo.*

Demonstração. Ver [3]. □

Dizemos que H é um subgrupo de um grupo G e denotamos por $H \leq G$, quando o conjunto H é um subconjunto não vazio de G que é também um grupo com relação à operação em G.

Um subgrupo H é dito **normal** em G e representado por $H \trianglelefteq G$, se as classes laterais à direita e à esquerda de H em G são iguais. A *classe lateral à esquerda* (respectivamente, *à direita*) de H em G definida por a é o seguinte subconjunto de G

$$aH = \{ah \mid h \in H\}$$

(respectivamente, $Ha = \{ha \mid h \in H\}$).

Um exemplo de subgrupo normal é o *centro* do grupo G, $Z(G)$, que consiste no conjunto dos elementos que comutam com todos os outros elementos em G. Isto é,

$$Z(G) = \{z \in G \mid \ zg = gz, \ \forall \ g \in G\}.$$

Um exemplo importante de subgrupo é o subgrupo normalizador de um grupo. Sendo H um subgrupo de G temos que o *normalizador* de H em G, representado por $N_G(H)$, é o conjunto dos elementos em G que normalizam H. Isto é,

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

Podemos notar que $H \trianglelefteq N_G(H)$ e que $H \trianglelefteq G$ se, e somente se, $N_G(H) = G$.

O número de classe laterais de um subgrupo H em um grupo G é representado por $[G : H]$ e denominado índice de H em G. Quando $H \trianglelefteq G$ o conjunto das classes laterais forma um grupo chamado *grupo quociente* de G em H e representado por G/H. A importância da existência de subgrupos normais em um grupo se dá exatamente pela formação de quocientes.

Temos ainda o *Teorema de Lagrange* que diz que se G é um grupo finito e H é um um subgrupo de G, então $|G| = |H|[G : H]$. Com isso, obtemos que a ordem e o índice de H dividem a ordem de G.

Denotamos o grupo cíclico G gerado pelo elemento g como $G = \langle g \rangle$. Observe que se G é cíclico e $H \leq G$, então H é cíclico. Além disso, se G é um grupo tal que $|G| = p$, p primo, então G é cíclico. É fácil ver que todo grupo cíclico é abeliano.

Quando um grupo possui ordem igual a potência de um primo, dizemos que este grupo é um $p-$grupo. Uma propriedade útil é que o centro de um $p-$grupo finito nunca

é trivial. Em particular, se G é um grupo de ordem p^2, desde que seu centro é não trivial e $G/Z(G)$ nunca tem ordem prima, temos que necessariamente G é abeliano.

Um *homomorfismo* entre dois grupos G e H é definido como uma função $\varphi : G \to H$ tal que $\varphi(ab) = \varphi(a)\varphi(b)$, para todos $a, b \in G$. Um *isomorfismo* $\varphi : G \to H$ é um homomorfismo bijetor e, neste caso, denotamos $G \cong H$.

Considerando o homomorfismo $\varphi : G \to H$, o conjunto $Ker(\varphi) = \{g \in G \mid \varphi(g) = 1\}$ é chamado núcleo do homomorfismo e é um subgrupo normal em G. Por outro lado, o conjunto $Im(\varphi) = \{\varphi(g) \mid g \in G\}$, chamado imagem do homomorfismo, é um subgrupo de H. Sendo assim, temos:

Teorema 1.3 (Teorema do Isomorfismo)**.** *Se $\varphi : G \to H$ é um homomorfismo e $K = Ker(\varphi)$, então $G/K \cong Im(\varphi)$.*

Outros dois resultados sobre homomorfismo de grupos são dados a seguir

Teorema 1.4 (Teorema da Correspondência)**.** *Sejam G_1 e G_2 grupos e $\varphi : G_1 \to G_2$ um homomorfismo sobrejetivo, tal que $N = Ker(\varphi)$. Então:*

(i) Para todo $H_1 \leq G_1$ tem-se $H_2 = \varphi(H_1) = \{\varphi(h) : h \in H_1\} \leq G_2$. Mais ainda, se $H_1 \trianglelefteq G_1$, então $H_2 \trianglelefteq G_2$.

(ii) Para todo $H_2 \leq G_2$ existe único $H_1 = \varphi^{-1}(H_2) = \{g \in G : \varphi(g) \in H_2\} \supseteq N$, $H_1 \leq G_1$, tal que $\varphi(H_1) = H_2$. Mais ainda, se $H_2 \trianglelefteq G_2$, então $H_1 \trianglelefteq G_1$.

Demonstração. Ver [7], página 148. □

Corolário 1.5 (Correspondência)**.** *Seja G um grupo e $N \trianglelefteq G$. Então, todo subgrupo do grupo quociente $\overline{G} = G/N$ é do tipo $\overline{H} = H/N$, onde H é o único subgrupo de G contendo N tal que $\pi(H) = \overline{H}$, onde $\pi : G \to \overline{G}$ é a projeção canônica. H recebe o nome de pré-imagem de $\overline{H}$ em G. Mais ainda*

$$\overline{H} \trianglelefteq \overline{G} \quad \textit{se, e somente se,} \quad H \trianglelefteq G.$$

Demonstração. Ver [7], página 148. □

Definição 1.6. *Uma ação de um grupo G em um conjunto X é uma aplicação*

$$\begin{aligned} \varphi : & G \times X \longrightarrow X \\ & (g, x) \longmapsto g * x, \end{aligned}$$

tal que $e * x = x$ e $(g_1 * g_2) * x = g_1 * (g_2 * x)$, para todo $x \in X$ e para todos $g_1, g_2 \in G$. A aplicação

$$\begin{aligned} \varphi_g : & X \longrightarrow X \\ & x \longmapsto g * x \end{aligned}$$

é chamada de transformação de X por g. Uma maneira equivalente de expressar que $\varphi : G \times X \longrightarrow X$ é uma ação de grupo é afirmando que

$$\begin{aligned} G &\longrightarrow Sim(X) \\ g &\longmapsto \varphi_g \end{aligned}$$

é um homomorfismo, onde $Sim(X)$ é o grupo das bijeções de X em X, com a operação composição.

Teorema 1.7 (Teorema de Sylow)**.** *Considere G um grupo finito de ordem n, p um primo tal que $p \mid n$ e $\alpha \geq 1,\ m \geq 1$, inteiros positivos tais que*

$$\underbrace{|G|}_{n} = p^{\alpha}m \quad e \quad mdc(p, m) = 1.$$

Então:

(i) Para cada $\beta \in \mathbb{N},\ 1 \leq \beta \leq \alpha$, existe um subgrupo H_β, tal que $|H_\beta| = p^\beta$. Um subgrupo de ordem p^α é chamado ***p-subgrupo de Sylow de G.***

(ii) Se P_1 e P_2 são $p-$subgrupos de Sylow de G, então existe $g \in G$, tal que $gP_1g^{-1} = P_2$. Ou seja, os $p-$subgrupos de Sylow de G são todos conjugados.

Denotamos por $Syl_p(G)$ o conjunto de todos os $p-$subgrupos de Sylow de G, isto é, $P \in Syl_p(G)$ se, e somente se, $|P| = p^\alpha$. Além disso, denotamos $n_p = |Syl(G)|$. Dado $P \in Syl_p(G)$, temos que $Syl_p(G) = \{gpg^{-1} \mid g \in G\}$ e, portanto,
$n_p = [G : N_G(P)]$.

(iii) Temos:

$$\begin{aligned} &1) n_p \mid m \quad e \\ &2) \underbrace{n_p \equiv 1 (mod\ p)}_{p \mid n_p - 1}. \end{aligned}$$

(iv) Um subgrupo de ordem $p^\gamma,\ \ 1 \leq \gamma \leq \alpha$, está contido em um $p-$subgrupo de Sylow. Isto é, se $H \leq G$ e $|H| = p^\gamma$, então existe $P \in Syl_p(G)$, tal que $H \leq P$.

Corolário 1.8. *Um $p-$subgrupo de Sylow de um grupo finito G é um subgrupo normal de G se, e somente se, ele é o único $p-$subgrupo de Sylow.*

1.2 Grupos Simétricos

Nesta seção, abordaremos grupos de funções de um conjunto S em si mesmo, chamados de grupos de permutações. Aqui serão destacados os principais resultados envolvendo estes grupos.

Definição 1.9. *Seja S um conjunto não vazio. O conjunto*

$$Sim(S) = \{f : S \to S \mid f \text{ bijetiva}\}.$$

munido de uma operação composição de funções é um grupo.

Esse grupo é chamado de grupo das permutações do conjunto S. Se $S = \{1, 2, \cdots, n\}$ denotaremos esse grupo por S_n, o grupo de todas as permutações de S, que é o chamado ***Grupo Simétrico de grau n****. O número de elementos de S_n é exatamente $n!$.*

Uma forma de representar as permutações é utilizando a notação em ciclos. Alguns resultados que utilizaremos dependem desta notação.

Definição 1.10. *Dizemos que uma permutação $\sigma \in S_n$ é um $r-$ciclo de S_n, $r \geq 2$, se existem $i_1,\ i_2, \cdots,\ i_r$ elementos distintos de $\{1,\ 2,\ \cdots,\ n\}$ tais que:*

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \cdots,\ \sigma(i_{r-1}) = i_r,\ \sigma(i_r) = i_1 \quad e$$

$$\sigma(j) = j,\ \forall\ j \in \{1, \cdots, n\} - \{i_1, \cdots, i_r\}.$$

Neste caso, usaremos a notação $\sigma = (i_1\ i_2\ \cdots\ i_r) \in\ S_n$.

Lema 1.11. *Os grupos S_n, $n \geq 3$, são grupos não abelianos.*

Demonstração. É suficiente verificarmos que $\sigma = (12)$ e $\tau = (123)$ não comutam em S_n. De fato,

$$\sigma\tau = (23) \neq (13) = \tau\sigma.$$

□

Teorema 1.12 (Produto de ciclos disjuntos)**.** *Toda permutação não trivial pode ser escrita (de maneira única a menos de ordenação) como um produto de ciclos disjuntos, isto é, não contém elementos comuns. Esta é a chamada* ***estrutura cíclica de uma permutação****.*

Demonstração. Ver [5], página 88. □

Teorema 1.13. *Duas permutações α e β em S_n, $n \geq 3$, são conjugadas em S_n se, e somente se, têm a mesma estrutura cíclica. Ou seja, duas permutações são conjugadas se, e somente se, podem ser escritas da mesma forma como produto de ciclos disjuntos.*

Demonstração. Ver [7], página 162. □

Teorema 1.14. *A ordem de uma permutação escrita na forma de ciclos disjuntos é o mmc dos comprimentos dos ciclos.*

Demonstração. Ver [5], página 89. □

Teorema 1.15. *Se o par de ciclos $\alpha = (a_1\ a_2 \cdots\ a_m)$ e $\beta = (b_1\ b_2 \cdots\ b_m)$ são disjuntos, então $\alpha\beta = \beta\alpha$.*

Demonstração. Ver [5], página 88. □

Ciclos de comprimento 2 são chamados de ***transposições*** e temos o seguinte resultado

Teorema 1.16. *Toda permutação S_n, $n \geq 1$, pode ser escrita, de maneira não necessariamente única, como um produto de transposições (não necessariamente disjuntas).*

Demonstração. Ver [5], página 90. □

Uma permutação é *ímpar* se pode ser escrita como um produto de um número ímpar de transposições. Analogamente, uma permutação é *par* se pode ser escrita como um produto de um número par de transposições.

O conjunto das permutações pares em S_n forma um subgrupo de S_n. O grupo das permutações pares de n elementos é denotado por A_n e é denominado ***Grupo Alternado de grau n***. Os grupos alternados têm ordem $n!/2$ e são exemplos de grupos importantes.

1.3 Corpos Finitos

Afim de descrever os grupos lineares, que será feito posteriormente, precisaremos de alguns resultados sobre a estrutura dos corpos finitos.

Definição 1.17. *Um corpo é composto de um conjunto F e de duas operações, "adição" $(+)$ e "multiplicação" $(\cdot)$, que satisfazem propriedades bem conhecidas, que resumiremos da seguinte forma:*

- *$(F, +)$ é um grupo abeliano com identidade aditiva 0 e*

- *$(F - \{0\}, \cdot)$ é um grupo abeliano com identidade multiplicativa 1.*

A multiplicação é distributiva com relação à adição.

Quando o conjunto F, citado acima, possui um número finito de elementos, dizemos que o corpo é finito. Denotaremos um corpo finito por $\mathbb{F}$.

Enunciaremos agora, alguns resultados sobre a estrutura dos corpos finitos. As provas podem ser encontradas em [9].

Teorema 1.18. *O número de elementos de um corpo finito $\mathbb{F}$ é sempre uma potência de um primo. Reciprocamente, para cada primo p e cada inteiro positivo n, existe, a menos de isomorfismo, um único corpo finito de ordem p^n.*

Definição 1.19. *A característica de um corpo F é o menor inteiro positivo m tal que, $m1 = \underbrace{(1 + 1 + \cdots + 1)}_{m \text{ vezes}} = 0$. Se tal m não existir, a característica do corpo é definida como sendo zero.*

Denotaremos a característica de um corpo finito $\mathbb{F}$ por $car(\mathbb{F})$.

Teorema 1.20. *A característica de um corpo finito $\mathbb{F}$ é um número primo.*

Demonstração. Seja $m \neq 0$ a característica de um corpo $\mathbb{F}$. Seja 1 a unidade desse corpo e suponhamos, por absurdo, que m seja composto, isto é, $m = pq, \quad p, q > 1$. Note que se trocarmos a unidade 1 por outro elemento não nulo a do corpo, temos $ma = 0$ se, e somente se, $maa^{-1} = 0$ se, e somente se, $m1 = 0$. Por isso, sem perda de generalidade, podemos considerar o produto

$$0 = m1 = (pq)1 = p1.q1 = \underbrace{(1 + 1 + \cdots + 1)}_{p \text{ vezes}}\underbrace{(1 + 1 + \cdots + 1)}_{q \text{ vezes}}.$$

Mas $0 = p1.q1$ se, e somente se, $p1 = 0$ ou $q1 = 0$, o que contraria a minimalidade de m, desde que claramente $q < m$ e $p < m$, absurdo. □

Exemplo 1.21. *Seja p um número primo. Então $\mathbb{Z}/p\mathbb{Z}$ é um corpo de característica p.*

Proposição 1.22. *Seja $\mathbb{K}$ um corpo, então um polinômio de grau n, com coeficientes no corpo $\mathbb{K}$, tem no máximo n raízes.*

Ver demonstração em [3].

Teorema 1.23. *Seja $\mathbb{K}$ um corpo e $\mathbb{K}^*$ o seu grupo multiplicativo. Se H é um subgrupo finito de $\mathbb{K}^*$, então H é cíclico.*

Demonstração. Como $\mathbb{K}$ é um corpo, $\mathbb{K}^*$ é um grupo abeliano. Assim, H é um subgrupo finito de um grupo abeliano. Seja $m = max\{|h|; h \in H\}$. Pelo Teorema 1.2, segue que $|h|$ divide m, e portanto $h^m = 1$, para todo $h \in H$. Deste modo, cada elemento de H é uma raiz do polinômio $p(x) = x^m - 1$ que, pela Proposição 1.22, tem no máximo m raízes. Daí segue que $|H| \leq m$. Por outro lado, o Teorema de Lagrange garante que m é um divisor da ordem de H, por isso, $m \leq |H|$. Pelas desigualdades anteriores, chegamos a $m = |H|$. Assim, temos que h é um elemento de H cuja ordem é a $|H|$ e, portanto, H é cíclico. □

Corolário 1.24. *O grupo multiplicativo de um corpo finito $\mathbb{F}$ é cíclico.*

Capítulo 2

Grupos Simples Finitos

Neste capítulo, iniciamos o estudo dos grupos simples finitos, discutindo sua definição e importância na teoria dos grupos finitos. Além disso, apresentaremos resultados que comprovam a simplicidade de alguns grupos importantes.

Definição 2.1. *Um grupo $G \neq \{1\}$ é dito simples, se seus únicos subgrupos normais são os triviais $\{1\}$ e G.*

Exemplo 2.2. *Note que todo grupo G de ordem p, p primo, é simples. De fato, pois se G possui um subgrupo normal H, pelo Teorema de Lagrange, $|H| = 1$ ou $|H| = p$.*

Exemplo 2.3. *Seja G um grupo abeliano, tal que $|G| = n$, onde $n > 1$ e n não é um número primo. Observe que todo subgrupo próprio H de G é normal, desde que $gH = Hg$, para todo $g \in G$. Logo, G não é simples.*

O estudo dos grupos simples finitos foi iniciado por Galois, há cerca de 185 anos. Como já dissemos, os grupos simples finitos são importantes devido ao fato de serem considerados os "blocos fundamentais"de todos os grupos finitos, algo semelhante à maneira como os números primos são os blocos fundamentais dos números inteiros. Essa importância fará mais sentido depois que apresentarmos o Teorema de Jordan-Hölder, um resultado fundamental sobre a estrutura dos grupos finitos. Antes de enunciá-lo, precisaremos de algumas definições:

Definição 2.4. *Seja G um grupo. Uma série de subgrupos*

$$G = G_0 \supset G_1 \supset \cdots \supset G_r$$

é dita ***subnormal*** *se cada G_{i+1} é um subgrupo normal de G_i, $(i = 0, 1, \cdots, r-1)$. Os grupos quocientes $G_i/G_{i+1}, (i = 0, 1, \cdots, r-1)$ são chamados* ***fatores*** *da série.*

Um ***refinamento*** de uma série subnormal é uma nova série subnormal obtida inserindo-se um número finito de subgrupos na série dada. Todo grupo finito possui uma série subnormal de comprimento máximo, isto é, que não pode ser mais refinada e terminando no grupo trivial:

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}.$$

Consideremos agora, duas séries subnormais terminando no grupo trivial:

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\} \text{ e}$$

$$G' = G'_0 \supset G'_1 \supset \cdots \supset G'_{r'} = \{1\}.$$

Diremos que estas séries são equivalentes se $r = r'$ e existe uma permutação dos índices $i = 1, \cdots, r-1$, representada por $i \longmapsto i'$, tal que:

$$G_i/G_{i+1} \cong G'_{i'}/G'_{i'+1}$$

Isto é, os fatores de ambas são os mesmos, a menos de uma permutação dos índices.

Teorema 2.5 (Schreier)**.** *Seja G um grupo. Quaisquer duas séries subnormais de subgrupos de G terminando no grupo trivial possuem refinamentos equivalentes.*

Demonstração. Ver [9], página 22. □

Teorema 2.6 (Jordan-Hölder)**.** *Sejam G um grupo e*

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

uma série subnormal tal que cada fator G_i/G_{i+1} é simples. Então qualquer outra série subnormal de G tendo a mesma propriedade é equivalente a esta. Em particular, ela tem comprimento máximo.

Demonstração. Ver [9], página 22. □

Uma série subnormal com comprimento máximo é chamada ***série de composição*** de G. Os fatores de uma série de composição de um grupo G, por serem simples, não podem ser mais reduzidos e, como são unicamente determinados por G, são invariantes de G. É neste sentido que os grupos finitos simples são considerados os "blocos fundamentais"na teoria dos grupos finitos.

Sendo assim, reconhecer a simplicidade de um grupo se faz necessário em algumas situações. Observamos que verificar se um determinado grupo é simples não se trata de uma tarefa fácil, mas existem testes que garantem a simplicidade ou não simplicidade de um grupo. Dentre eles destacam-se os seguintes

Teorema 2.7 (Teste de Sylow para não simplicidade)**.** *Seja G um grupo de ordem n, tal que n é um inteiro positivo que não é primo e seja p um primo que divide n. Se 1 é o único divisor de n que é congruente a 1 módulo p, então G não é simples.*

Demonstração. Por hipótese, já temos que $|G| = n$ e n não é primo. Se G é um grupo abeliano, então, como já vimos, G não é simples. Por isso, consideremos G não abeliano. Se n é uma potência de primo, então o centro de G é não trival e, por isso, G não é simples. Agora, se n não é uma potência de primo, então todo subgrupo de Sylow é próprio e, pelo Teorema de Sylow, sabemos que o número n_p de $p-$subgrupos de Sylow de G é congruente a 1 módulo p e divide n. Pela nossa hipótese, só poderemos ter $n_p = 1$, ou seja, o $p-$subgrupo de Sylow é único e o Corolário do Teorema de Sylow nos garante que esse $p-$subgrupo é normal em G. Com isso, concluímos que G não é simples. □

No exemplo a seguir veremos como utilizar o teste acima para verificar a não simplicidade de um grupo.

Exemplo 2.8. *Se G é um grupo tal que $|G| = pq$, com p, q primos, então G possui um subgrupo normal não-trivial, ou seja, G não é simples.*

Demonstração. De fato, note primeiramente que se $p = q$, então $|G| = p^2$ e, assim, G é abeliano e, consequentemente, G não é simples. Por isso, suponhamos que $p \neq q$. Podemos supor ainda, sem perda de generalidade, que $p > q$. Pelo Teorema de Sylow temos que:

$$\begin{cases} n_p \equiv 1 \bmod p \\ n_p \mid q \end{cases}$$

Desde que $p > q$, só podemos ter $n_p = 1$. Este único p- subgrupo de Sylow de G é próprio e é normal em G. Portanto, G não é simples. □

Teorema 2.9. *Seja G um grupo, tal que $|G| = p^\alpha m$, onde $\alpha > 0$, $m > 1$, p é um primo e o $mdc(p, m) = 1$. Se G é simples, então $|G|$ divide $n_p!$.*

Demonstração. Seja $P \in Syl_p(G)$. Pelo Teorema de Sylow temos que $n_p = [G : N_G(P)]$. Observe que $n_p \neq 1$, pois G é simples.

Considere $X = \{xN_G(P) \mid x \in G\}$ e a seguinte ação de grupos:

$$\begin{aligned} \varphi : G &\to Sim(X) \\ g &\mapsto \varphi_g : X \to X \\ & \quad xN_G(P) \mapsto gxN_G(P). \end{aligned}$$

Sabemos que $Ker\varphi \trianglelefteq G$ e, como G é simples, só podemos ter $Ker\varphi = \{1\}$ ou $Ker\varphi = G$. Mas $Ker\varphi = G$ contraria a simplicidade de G e, por isso, $Ker\varphi = \{1\}$. Logo, pelo Teorema do Isomorfismo:

$$\frac{G}{Ker\varphi} \simeq Im\varphi \leq Sim(X).$$

Isto é,

$$G \simeq Im\varphi \leq Sim(X)$$

Mas então $|G|$ divide $|Sim(X)|$ o que implica que $|G|$ divide $|X|!$ $\quad (*)$

Mas da ação sobre as classes laterais temos:

$$|X| = [G : N_G(P)] = n_p.$$

E, assim, de $(*)$ concluímos que $|G|$ divide $n_p!$.

□

Destacamos que a negativa do teorema acima, isto é, se $|G|$ não divide $n_p!$, então G não é simples, também é usada como um teste de não simplicidade. Utilizaremos esse fato no próximo exemplo.

Exemplo 2.10. *Um grupo G, de ordem 36, não é simples.*

Demonstração. Sabemos que $|G| = 36 = 2^2 3^2$. Pelo $3^{\underline{o}}$ item do Teorema de Sylow:

$$\begin{cases} n_2 \mid 3^2 \quad \text{e} \quad n_2 \equiv 1 \bmod 2, \text{ daí} \\ n_2 = 1, 3 \text{ ou } 3^2. \end{cases}$$

Onde n_2 é a quantidade de 2-subgrupos de Sylow de G.

Por outro lado,

$$\begin{cases} n_3 \mid 2^2 \quad \text{e} \quad n_3 \equiv 1 \bmod 3, \text{ daí} \\ n_3 = 1 \text{ ou } 2^2. \end{cases}$$

Onde n_3 é a quantidade de 3-subgrupos de Sylow de G.

Se $n_2 = 1$ e/ou $n_3 = 1$, pelo corolário do Teorema de Sylow, teremos pelo menos um subgrupo próprio e normal em G.

Se $n_2 \neq 1$ e $n_3 \neq 1$, temos que, pela negativa do teorema anterior, G não é simples. De fato, neste caso, temos necessariamente que $n_3 = 4$. Mas $n_3! = 4! = 24$ e $|G| = 36 \nmid 24$. □

2.1 A simplicidade de A_n, $n \geq 5$

Os grupos alternados A_n, $n \geq 5$, foram os primeiros grupos simples não abelianos a serem descobertos. A simplicidade de A_n foi reconhecida por Galois e foi fundamental para sua prova de que uma equação polinomial de grau 5 não pode ser resolvida por radicais.

Nesta seção, apresentaremos a demonstração do teorema que nos garante a simplicidade de A_n. Para isso, será necessário algumas propriedades de grupos simétricos vistas no Capítulo 1.

Teorema 2.11. *Seja $n = 3$ ou $n \geq 5$, então A_n é um grupo simples.*

O grupo A_3 tem ordem igual a 3 e é, portanto, simples. Para o caso A_n, $n \geq 5$ precisaremos do seguinte teorema:

Teorema 2.12. *Temos as seguintes informações sobre o subgrupo alternado:*

(a) A_n, $n \geq 3$ é gerado pelos 3-ciclos.

(b) Todos os 3-ciclos são conjugados em A_n, $n \geq 5$.

Demonstração. Se $(i\ j\ k)$ é um 3-ciclo qualquer, temos que $(i\ j\ k) = (i\ k)(i\ j)$ e assim $(i\ j\ k)$ pertence à A_n. E daí segue que $\langle \{3-ciclos\} \rangle \subseteq A_n$. Queremos mostrar a igualdade. Para isso, seja $\alpha \in A_n$, temos $\alpha = (i_1\ j_1)(i_2\ j_2)\cdots(i_k\ j_k)$ onde k é um número par. Se $|\{i_1, j_1, i_2, j_2\}| = 4$ então $(i_1\ j_1)(i_2\ j_2) = (i_1\ i_2\ j_2)(i_1\ j_1\ j_2)$. Por outro lado, se $|\{i_1, j_1, i_2, j_2\}| = 3$ então $(i_1\ j_1)(i_2\ j_2) = (i_1\ j_1)(i_1\ j_2) = (i_1\ j_2\ j_1)$ ou $(i_1\ j_1)(i_2\ j_2) = (i_1\ j_1)(i_2\ i_1) = (i_1\ i_2\ j_1)$. Repetindo esse raciocínio a cada duas transposições, concluímos a prova de (a).

(b) Considere dois 3-ciclos $\alpha = (r\ s\ t)$ e $\beta = (r'\ s'\ t')$ em A_n. Pelo Teorema 1.13, sabemos que existe $\gamma \in S_n$ tal que $\alpha^\gamma = \beta$. Se $\gamma \in A_n$ não há o que demonstrar. Caso contrário, tomamos $i, j \notin \{r, s, t\}$ e assim, $\gamma' = \gamma(i\ j) \in A_n$ e temos também $\alpha^{\gamma'} = \beta$. □

Agora estamos em condições de demonstrar o caso $n \geq 5$ do Teorema 2.11:

Teorema 2.13. *Se $n \geq 5$, então A_n é simples.*

Demonstração. Primeiramente, suponhamos que $H \neq \{1\}$ seja um subgrupo normal de A_n. Queremos mostrar que $H = A_n$ e, para isto, pelo item (b) do teorema anterior, basta mostrarmos que H contém um 3-ciclo.

Seja p um primo que divide $|H|$. Pelo Teorema de Cauchy, existe $\sigma \in H$, tal que $|\sigma| = p$. Como σ pode ser escrita como um produto de ciclos disjuntos, temos $\sigma = (i_1\ i_2\ \cdots\ i_p) = \tau_1\tau_2\cdots\tau_m$. Pelo Teorema 1.14 segue que o *mmc* dos ciclos $\tau_j,\ j = 1, \cdots, m$ é p. Portanto, cada τ_j só pode ser um $p-$ciclo. A partir destas considerações mostraremos que H contém um 3-ciclo. Para isso, analisaremos os seguintes casos:

Caso 1) Se $p = 2$, vamos ter que τ_i são transposições para todo i e que m é par (já que $\sigma \in H \leq A_n$). Digamos que $\tau_1 = (a\ b)$ e $\tau_2 = (c\ d)$. Mostraremos que:

(i) $(a\ b\ c)\sigma(a\ b\ c)^{-1}\sigma^{-1} = (a\ c)(b\ d) \in H$. De fato, pois

$$\begin{aligned}(a\ b\ c)\sigma(a\ b\ c)^{-1}\sigma^{-1} =& (a\ b\ c)(a\ b)(c\ d)(a\ c\ b)(c\ d)(a\ b)\\ =& (a\ c)(b\ d).\end{aligned}$$

Além disso, temos:

$$\underbrace{(a\ b\ c)\sigma(a\ b\ c)^{-1}}_{\in H,\ pois\ H\trianglelefteq A_n}\underbrace{\sigma^{-1}}_{\in H} = (a\ c)(b\ d) \in H.$$

(ii) Tomando $k \notin \{a, b, c, d\}$ temos $(a\ c\ k)(a\ c)(b\ d)(a\ c\ k)^{-1}(a\ c)(b\ d) = (a\ k\ c) \in H$. De fato, pois por (i) temos que $(a\ c)(b\ d) \in H$, logo: $(a\ c\ k)(a\ c)(b\ d)(a\ c\ k)^{-1} \in H$, já que $H \trianglelefteq A_n$, e portanto:

$$\underbrace{(a\ c\ k)(a\ c)(b\ d)(a\ c\ k)^{-1}}_{\in H}\underbrace{(a\ c)(b\ d)}_{\in H} = (a\ k\ c) \in H,$$

como queríamos.

Caso 2) Se $p = 3$. Podemos ter $m = 1$ e então H contém o 3-ciclo $\sigma = \tau_1$. Agora, se $m \geq 2$, escrevendo $\tau_1 = (a\ b\ c)$ e $\tau_2 = (d\ e\ f)$, temos que o 3-ciclo $(b\ d\ c)$ é disjunto de τ_i, para $i = 3, \cdots, m$, e assim, pelo Teorema 1.15, comuta com todos eles. Visto isso, queremos mostrar que $(b\ c\ d)\sigma(b\ c\ d)^{-1}\sigma^{-1}$ é um 5-ciclo que pertence à H. Sendo assim: $(b\ c\ d)\sigma(b\ c\ d)^{-1}\sigma^{-1} \in H$, pois:

$$\underbrace{(b\ c\ d)\sigma(b\ c\ d)^{-1}}_{\in H,\ pois\ H\trianglelefteq A_n}\underbrace{\sigma^{-1}}_{\in H}.$$

E também:

$$(b\ c\ d)\sigma(b\ c\ d)^{-1}\sigma^{-1} = (b\ c\ d)(a\ b\ c)(d\ e\ f)\tau_3\cdots\tau_m(b\ d\ c)\tau_m^{-1}\cdots\tau_3^{-1}(d\ f\ e)(a\ c\ b).$$

Como $(b\ d\ c)$ comuta com $\tau_i, i = 3, \ldots, m$:

$$\begin{aligned}(b\ c\ d)\sigma(b\ c\ d)^{-1}\sigma^{-1} =&(b\ c\ d)(a\ b\ c)(d\ e\ f)(b\ d\ c)\tau_3\cdots\tau_m\tau_m^{-1}\cdots\tau_3^{-1}(d\ f\ e)(a\ c\ b)\\ =&(b\ c\ d)(a\ b\ c)(d\ e\ f)(b\ d\ c)(d\ f\ e)(a\ c\ b)\\ =&(a\ d\ b\ c\ e).\end{aligned}$$

E, assim, obtemos um 5-ciclo pertencente a H e o resultado fica provado com o próximo caso.

Caso 3) Se $p > 3$, escrevendo $\tau_1 = (a_1\ a_2\ \cdots a_p)$, temos que o 3-ciclo $(a_2\ a_3\ a_4)$ é disjunto de τ_i, para $i = 2, \cdots, m$ e assim comuta com todos eles. Pretendemos mostrar que $(a_2\ a_3\ a_4)\sigma(a_2\ a_3\ a_4)^{-1}\sigma^{-1} = (a_2\ a_3\ a_5)$ é um 3-ciclo que pertence a H, pois assim o resultado estará provado. De fato, note primeiramente que:

$$\underbrace{(a_2\ a_3\ a_4)\sigma(a_2\ a_3\ a_4)^{-1}}_{\in H,\ pois\ H\trianglelefteq A_n}\underbrace{\sigma^{-1}}_{\in H}.$$

Além disso,

$(a_2\ a_3\ a_4)\sigma(a_2\ a_3\ a_4)^{-1}\sigma^{-1}$

$= (a_2\ a_3\ a_4)(a_1\ a_2\ \cdots a_p)\tau_2\cdots\tau_m(a_2\ a_4\ a_3)\tau_m^{-1}\cdots\tau_2^{-1}(a_1\ a_p\ \cdots a_2).$

E usando o fato de que $(a_2\ a_3\ a_4)$ comuta com $\tau_i,\ i = 2, \cdots, m$:

$$\begin{aligned}(a_2\ a_3\ a_4)\sigma(a_2\ a_3\ a_4)^{-1}\sigma^{-1} =&(a_2\ a_3\ a_4)(a_1\ a_2\ \cdots a_p)(a_2\ a_4\ a_3)(\tau_2\cdots\tau_m\tau_m^{-1}\cdots\tau_2^{-1})\\ &(a_1\ a_p\ \cdots a_2) = (a_2\ a_3\ a_4)(a_1\ a_2\ \cdots a_p)(a_2\ a_4\ a_3)\\ &(a_1\ a_p\ \cdots a_2) = (a_2\ a_3\ a_5),\end{aligned}$$

que é um 3-ciclo pertencente a H, como queríamos.
Com isso, nossa demonstração se reduz ao teorema anterior, já que se H possui um 3-ciclo, ele possui todos por conjugação. Assim, $H = A_n$, para todo $n \geq 5$ e, finalmente, concluímos que A_n é simples.

□

2.2 Grupos Simples de Ordem ≤ 60

Nesta seção faremos uma breve classificação de todos os grupos simples de ordem menor ou igual a 60. Antes, veremos mais alguns resultados envolvendo simplicidade e ordem de um grupo.

Teorema 2.14. *Seja G um grupo, tal que $|G| = pqr$, onde p, q e r são primos distintos. Então G não é simples.*

Demonstração. Por hipótese, já temos $|G| = pqr$, com p, q e r primos distintos. Podemos supor, sem perda de generalidade, que $p > q > r$. Suponhamos ainda, por absurdo, que

G é simples. Pelo Teorema de Sylow, temos as seguintes possibilidades para n_p, n_q e n_r, que correspondem a ordem de $Syl_p(G)$, $Syl_q(G)$ e $Syl_r(G)$, respectivamente.

$$n_p = q,\ r \text{ ou } qr$$
$$n_q = p,\ r \text{ ou } pr$$
$$n_r = p,\ q \text{ ou } pq.$$

Como estamos supondo G simples, temos $n_p \neq 1$, $n_q \neq 1$ e $n_r \neq 1$, o que justifica as possibilidades acima. Agora, observemos que $n_p \neq q$ e $n_p \neq r$, pois $p \mid (n_p - 1)$ e $p > q > r$. Logo, só poderemos ter $n_p = qr$. Por motivo análogo, temos $n_q \neq r$, já que $q \mid (n_q - 1)$ e $q > r$. Assim, obtemos que $n_q = p$ ou $n_q = pr$. Por fim, notemos que como G é simples, devemor ter que $|G|$ divide $n_r!$. Mas se $n_r = q$, então claramente $|G|$ não divide $q!$. Por isso, temos que $n_r = p$ ou $n_r = pq$. Com isso, concluímos que existem quatro casos possíveis:

Caso 1) $n_p = qr$, $n_q = p$ e $n_r = p$;

Caso 2) $n_p = qr$, $n_q = p$ e $n_r = pq$;

Caso 3) $n_p = qr$, $n_q = pr$ e $n_r = p$;

Caso 4) $n_p = qr$, $n_q = pr$ e $n_r = pq$.

Analisaremos cada caso acima, fazendo uma contagem de elementos do grupo, e mostraremos que nenhum caso é possível.

Caso 1) $n_p = qr$, $n_q = p$ e $n_r = p$. Desde que cada subgrupo de Sylow tem ordem prima, temos que o único elemento em comum entre eles é a identidade. Dessa forma, temos que o número de elementos de ordem p no grupo G é $qr(p-1)$, o número de elementos com ordem q é $p(q-1)$ e o número de elementos com ordem r é $p(r-1)$. Assim, temos

$$\begin{aligned} qr(p-1) + p(q-1) + p(r-1) &= pqr - qr + pq - p + pr - p \\ &= pqr + (pq - qr) + (pr - 2p). \end{aligned}$$

Note que $pq - qr$ é positivo desde que $p > r$. Além disso, $pr - 2p$ é positivo se $r > 2$ e zero, caso contrário. Assim, obtemos pqr mais algum número positivo de elementos, uma clara contradição desde que excede o número de elementos em G. Logo, esse caso não pode ocorrer.

Caso 2) $n_p = qr$, $n_q = p$ e $n_r = pq$. Procedendo como acima, neste caso, temos que o número de elementos de ordem p no grupo G é $qr(p-1)$, o número de elementos com ordem q é $p(q-1)$ e o número de elementos com ordem r é $pq(r-1)$. Logo,

$$\begin{aligned} qr(p-1)+p(q-1)+pq(r-1) &= pqr-qr+pq-p+pqr-pq \\ &= pqr+pqr-qr-p \\ &= pqr+qr(p-1)-p. \end{aligned}$$

Temos que $qr(p-1)-p$ é positivo e, novamente, obtemos pqr mais algum número positivo de elementos em G, uma contradição. Logo, esse caso também não ocorre.

Caso 3) $n_p = qr$, $n_q = pr$ e $n_r = p$. Aqui, temos que o número de elementos de ordem p no grupo G é $qr(p-1)$, o número de elementos com ordem q é $pr(q-1)$ e o número de elementos com ordem r é $p(r-1)$ e, assim,

$$\begin{aligned} qr(p-1)+pr(q-1)+p(r-1) &= pqr-qr+pqr-pr+pr-p \\ &= pqr+qr(p-1)-p. \end{aligned}$$

Obtemos um resultado idêntico ao caso anterior e, portanto, esse caso também não pode ocorrer.

Caso 4) $n_p = qr$, $n_q = pr$ e $n_r = pq$. Por fim, neste caso, temos que o número de elementos de ordem p no grupo G é $qr(p-1)$, o número de elementos com ordem q é $pr(q-1)$ e o número de elementos com ordem r é $pq(r-1)$ e, assim,

$$\begin{aligned} qr(p-1)+pr(q-1)+pq(r-1) &= pqr-qr+pqr-pr+pqr-pq \\ &= pqr+(pqr-qr)+[pqr-p(q+r)]. \end{aligned}$$

Claramente, $pqr-qr$ é positivo. E note que $[pqr-p(q+r)]$ é positivo se $(q+r)<qr$, que é verdade para q e r distintos e maiores ou iguais a 2. Assim, chegamos novamente em uma contradição, desde que encontramos pqr mais um número positivo de elementos.

Diante do exposto, concluímos que G não é um grupo simples, como afirmado.

□

Teorema 2.15. *Seja G um grupo, tal que $|G| = p^3q$, onde p e q são primos distintos. Então G não é simples.*

Demonstração. Já temos que $|G| = p^3q$ e vamos assumir que G é simples. Pelo Teorema de Sylow temos as seguintes possibilidades para n_p e n_q, que correspodem a ordem dos grupos $Syl_p(G)$ e $Syl_q(G)$, respectivamente.

$$n_p \mid q \text{ e } n_p \equiv 1 \; mod \; p \Rightarrow n_p = 1 \text{ ou } q,$$

$$n_q \mid p^3 \text{ e } n_q \equiv 1 \; mod \; q \Rightarrow n_q = 1,\ p,\ p^2 \text{ou } p^3.$$

Como G é simples temos, necessariamente, que $n_p \neq 1$ e $n_q \neq 1$. Logo, temos $n_p = q$ e $n_q = p$, p^2 ou p^3. Daí segue que $q > p$, desde que p divide $(q-1)$. Vamos analisar as possibilidades para n_q.

Se $n_q = p$, então q deve dividir $(p-1)$, um absurdo, desde que $q > p$.

Se $n_q = p^3$, então existem p^3 q-subgrupos de Sylow de ordem q, cuja a interseção é trivial. Dessa forma, existem $p^3(q-1)$ elementos com ordem q. Vamos denotar por α o número restante de elementos em G. Assim,

$$|G| = \alpha + p^3(q-1) \Rightarrow \alpha = p^3q - p^3q + p^3 \Rightarrow \alpha = p^3.$$

Isso implica que existem elementos suficientes que não são de ordem q e que se encaixam em um único p-subgrupo de Sylow. Sabemos, pelo Teste de Sylow, que este único p-subgrupo de Sylow, que é próprio, deve ser normal em G, o que contraria a simplicidade do grupo. Logo, $n_q \neq p^3$.

Resta-nos que $n_q = p^2$. Então

$$q \mid (p^2-1) \Rightarrow q \mid (p-1)(p+1) \Rightarrow q \mid (p+1) \text{ ou } q \mid (p-1).$$

Desde que $q > p$, só podemos ter q divide $(p+1)$ que implica em $p < q < (p+1)$. Com isso, concluímos que p e q são primos consecutivos. Mas, sabemos que os únicos primos consecutivos são 2 e 3. Logo, se G é simples, a única possibilidade é $p = 2$ e $q = 3$. Vamos mostrar que um grupo de ordem $2^3 3$ não é simples e, assim, obtemos a contradição desejada. De fato, suponha $|G| = 2^3 3$ e que G é simples, então sendo n_2 o número de 2-subgrupos de Sylow de G, temos que

$$n_2 \mid 3 \text{ e } n_2 \equiv 1 \; mod \; 2 \Rightarrow n_2 = 1 \text{ ou } 3.$$

A simplicidade de G implica em $n_2 = 3$. Mas note que $|G| = 24$ não divide 3!, uma contradição. Logo, temos necessariamente que $n_2 = 1$ e, portanto, G não é simples.

Finalmente, concluímos que nenhum dos casos descritos acima pode ocorrer e que, portanto, G não é um grupo simples.

□

Chegamos em um dos principais teoremas desta seção, que caracteriza os grupos simples de ordem menor que 60. Como consequência imediata deste teorema, obtemos que A_5 é o menor grupo simples de ordem composta.

Teorema 2.16. *Se $|G| < 60$, então G é simples se, e somente se, a ordem de G é um número primo.*

Demonstração. ($\Leftarrow$) Segue diretamente do Teorema de Lagrange.

($\Rightarrow$) Seja $|G| = m$ e suponhamos que m não é um número primo. Desde que m é menor que 60, vamos analisar suas possíves decomposições em números primos.

(i) $|G| = p^n$, $n \geq 1$. Para o caso $n = 1$ não há nada o que provar, logo suponhamos que $n \neq 1$. Temos que G é um $p-$ grupo e, assim, $Z(G) \neq \{1\}$. Então, a simplicidade de G implica que $Z(G) = G$. Mas então G é abeliano e o Teorema de Cauchy nos garante a existência de um subgrupo próprio normal em G, contrariando nossa hipótese. Logo, neste caso, só podemos $n = 1$, isto é, $|G| = p$.

(ii) $|G| = m = p^2q^2$, com p e q primos distintos. Neste caso, o único grupo com ordem menor que 60 que possui a configuração $|G| = p^2q^2$ é o grupo de ordem 36 que, como vimos no Exemplo 2.10, não é simples, o que contraria nossa hipótese.

(iii) $|G| = m = p^3q$, com p e q primos distintos. Se a ordem de G tem essa decomposição en números primos, então como vimos no Teorema 2.15 anerior, G não é simples.

(iv) $|G| = m = pqr$, com p, q e r. Se a ordem de G tem essa decomposição en números primos, então como vimos no Teorema 2.14, G não é simples.

(v) $|G| = m = p^2q$, com p e q primos distintos. Mostraremos que, neste caso, também obtemos que G não é simples. De fato, pelo Teorema de Sylow,

$$\begin{cases} n_p \mid q \quad \text{e} \quad n_p \equiv 1 \text{ mod p, daí} \\ n_p = 1 \text{ ou } p. \end{cases}$$

Por outro lado:

$$\begin{cases} n_q \mid p^2 \quad \text{e} \quad n_q \equiv 1 \text{ mod q, daí} \\ n_q = 1, \ p \text{ ou } p^2. \end{cases}$$

Pelas possiblidade descritas acima, temos que analisar os seguintes casos

Caso 1) Se $p > q$, não poderíamos ter $n_p = q$, pois caso contrário $p \mid q - 1$. Portanto, $n_p = 1$ e assim existe um único $p-$subgrupo de Sylow de G, contrariando a sua simplicidade.

Caso 2) Se $q > p$, vamos analisar as possibilidades para n_q. Se $n_q = p$, então q divide $p - 1$, o que não é possível, já que $q > p$. Agora, se $n_q = p^2$, teremos que fazer uma contagem. Note que teremos $p^2(q - 1)$ elementos de ordem q, já que temos p^2 subgrupos de Sylow de ordem q e a interseção entre eles é trivial. Isto implica que sobram apenas p^2 elementos para formar um único $p-$subgrupo de Sylow de G. E assim, necessariamente, temos que $n_p = 1$ ou $n_q = 1$, onde concluímos que G não é simples.

(vi) $|G| = m = p^4q$,com p e q primos distintos. Desde que $m < 60$, neste caso, só poderemos ter $p = 2$ e $q = 3$. Ou seja, $|G| = m = 2^43$. Sendo assim, seja n_2 o número de 2-subgrupos de Sylow de G, temos

$$n_2 \mid 3 \text{ e } n_2 \equiv 1 \ mod \ 2 \Rightarrow n_2 = 1 \text{ ou } 3.$$

A simplicidade de G implica que $n_2 = 3$. Mas, nesta situação, $|G| = 48$ não divide 3!. Por isso, um grupo de ordem 2^43 não é simples.

Diante do exposto, concluímos que dado um grupo de ordem menor que 60, ele só será simples se tiver ordem prima, como queríamos. Com isso, finalizamos nossa demonstração.

□

O próximo teorema nos permite identificar como é a estrutura de um grupo finito simples de ordem igual a 60.

Teorema 2.17. *Seja G um grupo simples de ordem 60. Então, G é isomorfo ao A_5.*

Para essa demosntração precisaremos do lema seguinte.

Lema 2.18. *Se G é um grupo simples de ordem 60, então existe um subgrupo H de G que possui exatamente 5 conjugados.*

Demonstração. Seja n_2 o número de 2-subgrupos de Sylow de G. Sabemos do Terceiro Teorema de Sylow que

$$n_2 \equiv 1 \mod 2 \text{ e } n_2 \mid 15 \Rightarrow n_2 = 1,\ 3,\ 5 \text{ ou } 15.$$

Como G é simples, temos $n_2 \neq 1$, pois caso contrário teríamos um único 2-subgrupo de Sylow, o que implicaria em G normal, contrariando nossa hipótese.

Se n_2 fosse igual a 3 teríamos um absurdo, como veremos. Denote por C_3 o conjunto dos 2-subgrupos de Sylow, os quais são conjugados entre si e considere o seguinte homomorfismo:

$$\begin{aligned} \varphi : G &\to Sim(C_3) \simeq S_3 \\ g &\mapsto \varphi_g : C_3 \to C_3 \\ H_i &\mapsto gH_ig^{-1}, \end{aligned}$$

onde $Sim(C_3)$ é o grupo das permutações de C_3. Pelo Teorema do Isomorfismo temos: $\frac{G}{Ker\varphi} \simeq \varphi(G) \subset S_3$. Como $|S_3| = 6$ e $|G| = 60$ só poderemos ter $Ker\varphi \neq \{1\}$, o que é impossível, pois $Ker\varphi \trianglelefteq G$, o qual é simples.

Caso $n_2 = 5$, podemos escolher qualquer um dos 2-subgrupos de Sylow para ser H.

Se $n_2 = 15$, começamos observando que devem existir 2-subgrupos de Sylow distintos K_1 e K_2 tais que $K_1 \cap K_2 \neq \{1\}$. Pois, caso contrário, G possuíria $15.3 = 45$ elementos de ordem potência de 2. Do fato de G ser simples, segue que ele deve possuir seis 5-subgrupos de Sylow, logo terá $6.4 = 24$ elementos de ordem 5. Desse modo, G possuíria pelo menos $45 + 24 + 1 = 70$ elementos, o que é um absurdo já que $|G| = 60$. Sendo assim, existem dois subgrupos K_1 e K_2, tais que $|K_1| = 4 = |K_2|$ e $|K_1 \cap K_2| = 2$. Daí segue que $K_1 \cap K_2 \trianglelefteq K_1$ e $K_1 \cap K_2 \trianglelefteq K_2$, pois subgrupos de índice 2 são sempre normais. Seja $\langle K_1, K_2\rangle$ o subgrupo gerado por K_1 e K_2. Temos que como $K_1 \cap K_2 \trianglelefteq K_1$ e $K_1 \cap K_2 \trianglelefteq K_2$ segue que $\langle K_1, K_2\rangle \subset N_G(K_1 \cap K_2)$, onde N_G é o normalizador de $K_1 \cap K_2$

em G. Denotemos $H = \langle K_1, K_2 \rangle$ e consideremos o seguinte diagrama:

$$\begin{array}{c} G \\ \shortparallel \\ N_G(K_1 \cap K_2) \\ | \\ \langle K_1, K_2 \rangle = H \\ \diagup \quad \diagdown \\ K_1 \quad K_2 \\ \triangledown \quad \triangledown \\ K_1 \cap K_2. \end{array}$$

Como G é simples, $N_G(K_1 \cap K_2) \neq G$, pois caso contrário, $K_1 \cap K_2 \trianglelefteq G$. Sendo assim, a ordem de H só poderá ser 20 ou 12. Mas, pelo Teorema 2.9, a ordem de H é diferente de 20, pois senão teríamos $H \subseteq G$ e $[G : H] = 3$ e, como 60 não divide 3!, teríamos que G não é simples, ou seja, um absurdo. Assim, a ordem de H é 12. Como H não pode ser normal em G, temos que $N_G(H) = H$. Com isto, H possui exatamente 5 conjugados, já que $[G : N_G(H)] = [G : H] = 5$. □

Agora, estamos em condições de demonstrar o Teorema 2.17.

Demonstração. Seja H o subgrupo do lema anterior e $C = \{\text{conjugados de } H\}$. Temos que a quantidade de elementos em C é 5. Consideremos o seguinte homomorfismo:

$$\begin{aligned} \tilde{\varphi} : G &\to Sim(C) \simeq S_5 \\ g &\mapsto \tilde{\varphi}_g : C \to C \\ H_i &\mapsto g H_i g^{-1}. \end{aligned}$$

Lembrando que $Sim(C)$ é o grupo das permutações de C, o qual é isomorfo a S_5.

O subgrupo $Ker\tilde{\varphi}$ é um subgrupo normal diferente de G, pois $Ker\tilde{\varphi} \subseteq N_G(H) \subsetneq G$. Como G é um grupo simples, temos $Ker\tilde{\varphi} = \{1\}$. Assim, $\tilde{\varphi}(G)$ é um subgrupo de S_5 de ordem 60. Logo, $\tilde{\varphi}(G) = A_5$, pois A_5 é o único subgrupo deS_5 de ordem 60 cujo índice é 2. Como $\tilde{\varphi}$ é injetivo $G \simeq \tilde{\varphi}(G) \simeq A_5$, logo, concluímos que $G \simeq A_5$. □

Capítulo 3

A Simplicidade de $PSL(n, \mathbb{F})$

Os grupos lineares especiais projetivos foram a segunda família de grupos finitos simples a serem estudados, depois dos grupos alternados, e foram construídos como transformações lineares fracionárias. Neste capítulo, trataremos de alguns resultados que nos garantem a simplicidades dos grupos lineares especiais projetivos. Para tanto, será necessário desenvolvermos alguns resultados de álgebra linear ao longo da seguinte seção.

3.1 Grupos Lineares

Nesta seção apresentaremos os grupos lineares e suas propriedades.

Definição 3.1. *Seja F um corpo. O conjunto $GL(n, F)$ é formado pelas matrizes A, $n \times n$, com entradas em F e tais que* $\det(A) \neq 0$.

O conjunto $GL(n, F)$ forma um grupo com a operação de multiplicação, pois como $det(A) \neq 0$, a matriz A possui inversa. O elemento neutro é a matriz identidade, que representaremos por I, e os outros requisitos para ser grupo seguem diretamente da definição de multiplicação entre matrizes e do fato de que $det(AB) = [det(A)].[(det(B)]$.

O conjunto $GL(n, F)$ é denominado **Grupo Linear Geral de grau n**.

Definição 3.2. *O conjunto de todas as matrizes A, $n \times n$, com entradas em um corpo F e tais que $det(A) = 1$ formam um subgrupo de $GL(n, F)$ denotado por $SL(n, F)$.*

O conjunto $SL(n, F)$ é denominado **Grupo Linear Especial de grau n**.

Teorema 3.3. *O centralizador de $SL(n, F)$ em $GL(n, F)$ é o grupo das matrizes escalares não-nulas, isto é, o grupo das matrizes da forma $A = aI$, onde $a \in F^*$.*

Demonstração. É de imediata verificação que uma matriz escalar comuta com qualquer matriz em $GL(n, F)$. Sendo assim, resta-nos mostrar que se uma matriz A pertence ao centralizador de $SL(n, F)$ em $GL(n, F)$, então A é múltipla da identidade. De fato, seja E_{ij} , com $i \neq j$, a matriz elementar $n \times n$ contendo 1 na posição (i, j) e 0 nas posições restantes. Como $i \neq j$, então $I + E_{ij}$ pertence a $SL(n, F)$, e assim a matriz A comuta

com $I + E_{ij}$. Daí segue que $A(I + E_{ij}) = (I + E_{ij})A$, o que implica $AE_{ij} = E_{ij}A$. Mas o elemento da posição (k, j) de AE_{ij} é a_{ki}:

$$AE_{ij} = \begin{pmatrix} a_{11} & \cdots & a_{1i} & \cdots & a_{1n} \\ \vdots & & & & \vdots \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} \\ \vdots & & & & \vdots \\ a_{n1} & & \cdots & & a_{nn} \end{pmatrix} \begin{pmatrix} 0 & & \cdots & & 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & \cdots & a_{1i} & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & a_{ii} & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & a_{ni} & \cdots & 0 \end{pmatrix}.$$

Enquanto que o elemento da posição (k, j) de $E_{ij}A$ é igual a 0 se $k \neq i$ e igual a a_{jj} se $k = i$:

$$E_{ij}A = \begin{pmatrix} 0 & & \cdots & & 0 \\ \vdots & & & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & & \cdots & & 0 \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1i} & \cdots & a_{1n} \\ \vdots & & & & \vdots \\ a_{i1} & \cdots & a_{ii} & \cdots & a_{in} \\ \vdots & & & & \vdots \\ a_{n1} & & \cdots & & a_{nn} \end{pmatrix}$$
$$= \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ a_{j1} & \cdots & a_{jj} & \cdots & a_{jn} \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}.$$

E, assim, como $AE_{ij} = E_{ij}A$, concluímos que $a_{ki} = 0$ se $k \neq i$ e $a_{ii} = a_{jj}$ se $k = i$, mostrando que A é uma matriz escalar. □

Teorema 3.4. *O centro de $GL(n, F)$, denotado por $Z(GL(n, F))$, é o grupo das matrizes escalares aI não-nulas. O centro de $SL(n, F)$ representado por $Z(SL(n, F))$ é o grupo das matrizes escalares aI, onde $a^n = 1$.*

Demonstração. Se A está em $Z(GL(n, F))$ então A comuta com todas as matrizes de $GL(n, F)$ e, em particular, comuta com as matrizes em $SL(n, F)$. Mas então pelo teorema anterior, a matriz A só pode ser da forma $A = aI, a \neq 0$. Por outro lado, para uma matriz B pertencer ao centro de $SL(n, F)$, além de comutar com todas as matrizes de $SL(n, F)$ ela precisa ter determinante igual a 1. Desse modo, concluímos que B deve ser da forma $B = aI$, onde $a^n = 1$. □

Definição 3.5. *O* ***Grupo Linear Geral Projetivo****, representado por* $PGL(n, F)$*, de grau* n *sobre o corpo* F *é definido para ser:*

$$PGL(n, F) = \frac{GL(n, F)}{Z(GL(n, F))}.$$

E o ***Grupo Linear Especial Projetivo****, representado por* $PSL(n, F)$*, é definido como:*

$$PSL(n, F) = \frac{SL(n, F)}{Z(SL(n, F))}.$$

Observação 3.6. *Quando* $\mathbb{F}$ *for um corpo finito vamos considerar que ele possui* q *elementos e escreveremos* $|\mathbb{F}| = q$*. Além disso, passaremos a utilizar a seguinte notação:* $GL(n, q)$*,* $PGL(n, q)$*,* $SL(n, q)$ *e* $PSL(n, q)$*. Ou seja, trocaremos* $\mathbb{F}$ *por* q *nas expressões anteriores.*

Teorema 3.7. *Suponha que* $\mathbb{F}$ *seja um corpo finito com* q *elementos, então:*

1. $|GL(n, q)| = (q^n - 1).(q^n - q) \cdots (q^n - q^{n-1})$.

2. $|SL(n, q)| = \dfrac{|GL(n, q)|}{(q - 1)} = |PGL(n, q)|$.

3. $|PSL(n, q)| = \dfrac{|GL(n, q)|}{d(q - 1)}$ *, onde* $d = mdc(n, q - 1)$.

Demonstração. 1. Se $A \in GL(n, q)$, então $det(A) \neq 0$. Seja A_i a i-ésima linha de A. Temos que $det(A) \neq 0$ se, e somente se, A_i não pode ser escrita como combinação linear de outras linhas. Dessa forma, para construirmos a matriz A, podemos escolher a primeira linha de $q^n - 1$ maneiras, já que a linha com todas as entradas nulas não é permitida. A segunda linha, por sua vez, poderá ser preenchida de $q^n - q$ maneiras, pois nenhum múltiplo da primeira linha é permitido. Para a terceira linha teremos $q^n - q^2$ possiblidades, já que não é permitida combinação linear das duas primeiras linhas. Seguindo este raciocínio, teremos $q^n - q^{n-1}$ maneiras de preencher a n-ésima linha, pois não podemos considerar nenhuma combinação linear das $(n - 1)$ linhas anteriores. Ao multiplicarmos esses números obtemos que:

$$|GL(n, q)| = (q^n - 1).(q^n - q).(q^n - q^2) \cdots (q^n - q^{n-1}).$$

2. Seja:

$$\begin{aligned} \varphi : GL(n, q) &\longrightarrow \mathbb{F}^* \\ A &\longrightarrow det(A), \quad onde \quad \mathbb{F}^* = \mathbb{F} - \{0\}. \end{aligned}$$

Notemos que $\mathbb{F}^*$ está sendo considerado como um grupo com a operação de multiplicação existente no corpo $\mathbb{F}$. Como $det(AB) = [det(A)].[(det(B)]$ temos que φ é um

homomorfismo de grupos. O $Ker\varphi = SL(n,q)$ e como φ é sobrejetor, pelo Teorema do Isomorfismo temos:

$$\frac{GL(n,q)}{SL(n,q)} \cong \mathbb{F}^* \Rightarrow |SL(n,q)| = \frac{|GL(n,q)|}{|\mathbb{F}^*|} = \frac{|GL(n,q)|}{(q-1)}.$$

Além disso, como $PGL(n,q) = \dfrac{GL(n,q)}{Z(GL(n,q))}$ pelo Teorema 3.4, teremos que

$$|Z(GL(n,q))| = (q-1) \Rightarrow |PGL(n,q))| = \frac{|GL(n,q))|}{(q-1)}.$$

3. Sabemos que $PSL(n,q) = \dfrac{SL(n,q)}{Z(SL(n,q))}$, sendo assim para determinarmos a ordem de $PSL(n,q)$ precisamos saber a ordem de $Z(SL(n,q))$. O Teorema 3.4, nos garante que essa ordem equivale a quantidade de $a's$ em $\mathbb{F}^*$ tais que $a^n = 1$. Mostraremos que essa quantidade é $d = mdc(n, q-1)$.

   De fato, considere:

$$H = \{a \in \mathbb{F}^* \mid a^n = 1\}$$

   Note que $|H| = |Z(SL(n,q)|$ e que H é um subgrupo de $\mathbb{F}^*$. Pelo Teorema 1.24, $\mathbb{F}^*$ é um grupo cíclico e suponha que g seja seu elemento gerador. Daí segue que H também é cíclico. Seja h o gerador de H, tal que $|H| = |h| = x$. Pelo Teorema de Lagrange, temos que $x \mid (q-1)$ e como $h^n = 1$, então $x \mid n$, e portanto, $x \mid d = mdc(n, q-1)$. Por outro lado, seja:

$$1 \neq a = g^{\frac{q-1}{d}} \Rightarrow a^n = \left(g^{\frac{q-1}{d}}\right)^n = g^{\left(\frac{q-1}{d}\right)n} = (g^{q-1})^{\frac{n}{d}} = 1.$$

   Então $a \in H$ e $|a| = d$. E assim $d \mid x$. Então diante do exposto, só poderemos ter $d = x$. Como x é a ordem de H, o resultado está provado.

□

3.2 Teorema de Jordan-Dickson

Nesta seção, desenvolveremos os resultados necessários para provar o Teorema de Jordan-Dickson, o qual nos garante a simplicidade do grupo linear especial projetivo. Ressaltamos que tais resultados e demonstrações terão como base os apresentados em [10]. Nosso principal objetivo será demonstrar os seguintes teoremas:

Teorema 3.8. *Seja $\mathbb{F}$ um corpo finito e N um subgrupo normal de $SL(n,q)$, o qual não está contido no centro. Se $n \geq 2$ e $|\mathbb{F}| = q > 3$, então $N = SL(n,q)$.*

Teorema 3.9 (Jordan-Dickson)**.** *Se $n \geq 2$ e $|\mathbb{F}| = q > 3$, então $PSL(n,q)$ é simples.*

Veremos posteriormente que o Teorema de Jordan- Dickson seguirá como corolário do Teorema 3.8. Mas para tal, ainda precisaremos desenvolver alguns resultados.

Definição 3.10. *Se $a \neq 0$ e $a \in F$, uma matriz da forma $I + aE_{ij}$, onde $i \neq j$, é chamada de transvecção. Ela difere da matriz identidade unicamente pelo fato de que na posição (i, j) está a não nulo.*

Observação 3.11. *Note que as transvecções pertencem a $SL(n, q)$ e que a inversa de uma transvecção $I + aE_{ij}$ é $I - aE_{ij}$, a qual também é uma transvecção. Sua importância se deve ao fato de que a multiplicação de uma matriz A à esquerda por $I + aE_{ij}$ tem o efeito de adicionar a vezes a j-ésima linha sobre a i-ésima linha.*

Teorema 3.12. *Se $n > 1$, então as transvecções geram $SL(n, q)$.*

Demonstração. Afirmamos que se $n > 1$, então toda matriz $A \in SL(n, q)$ pode ser escalonada até obtermos a identidade usando apenas multiplicação por transvecções.

Ao provarmos essa afirmação, finalizamos nossa demonstração, pois considerando transvecções T_l, $1 \leq l \leq k$, tais que $T_k \cdots T_2 T_1 A = I$, temos:

$$T_k \cdots T_2 T_1 A = I \Leftrightarrow A = T_1^{-1} \cdots T_{k-1}^{-1} T_k^{-1}.$$

Daí segue que A é um produto de transvecções e, portanto, as transvecções geram $SL(n, q)$.

Vamos demonstrar a afirmação acima. Para isso, usaremos indução sobre o tamanho n das matrizes:

i) Se $A \in SL(2, q)$, podemos utilizar apenas transvecções para escaloná-la:

De fato, seja: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, onde $ad - bc = 1$. Vamos verificar os seguintes casos:

1º Caso) Se $c \neq 0$ e $a \neq 1$, tome $T_1 = I + \left(\frac{1-a}{c}\right) E_{12}$ e faça

$$T_1 A = \begin{pmatrix} 1 & b + d\left(\frac{1-a}{c}\right) \\ c & d \end{pmatrix}.$$

Substituindo $ad - bc = 1$:

$$T_1 A = \begin{pmatrix} 1 & d - 1 \\ c & d \end{pmatrix}.$$

Agora, tome $T_2 = I - cE_{21}$,

$$T_2 T_1 A = \begin{pmatrix} 1 & \frac{d-1}{c} \\ 0 & 1 \end{pmatrix}.$$

Finalmente, multiplicando o resultado acima por $T_3 = I - \left(\frac{d-1}{c}\right) E_{12}$ obteremos a identidade: $T_3 T_2 T_1 A = I$. E desse modo, $A = T_1^{-1} T_2^{-1} T_3^{-1}$, isto é, A é um produto de transvecções.

Note que $c \neq 0$ e $a = 1$ se reduz a esse mesmo caso.

2^{o} Caso) Se $c = 0$ e $a \neq 1$, então: $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, onde $ad = 1$. (Logo $a \neq 0$). Fazendo a multiplicação de $T_1 = I + \left(\frac{1}{a} - 1\right) E_{21}$ por A,

$$T_1 A = \begin{pmatrix} a & b \\ 1-a & \frac{1-ab+b}{a} \end{pmatrix}.$$

Como o $det(T_1 A) = 1$ e $1 - a \neq 0$, podemos repetir os cálculos do caso anterior e escalonaremos A.

3^{o} Caso) Se $c = 0$ e $a = 1$, então $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, e daí teremos $d = 1$. Assim, $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ e tomando $T_1 = I - bE_{12}$ teremos que $T_1 A = I$.

Portanto, se $A \in SL(2,q)$ conseguimos escaloná-la utilizando apenas multiplicações à esquerda por transvecções.

ii) Suponhamos que para $B \in SL(n-1,q)$ nossa afirmação seja verdadeira.

iii) Vamos mostrar que é possível escalonar $A \in SL(n,q)$ usando apenas transvecções.

De fato, temos que algum $a_{jn} \neq 0$, pois $det(A) = 1$. Logo, fazendo $T = I + \left(\frac{1-a_{nn}}{a_{jn}}\right) E_{nj}$ chegamos que:

$$TA = \begin{pmatrix} 1 & 0 & \cdots & & 0 \\ 0 & \ddots & & & \vdots \\ \vdots & & 1 & & \\ & & & \ddots & 0 \\ 0 & \cdots & \left(\frac{1-a_{nn}}{a_{jn}}\right) & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & \ddots & & & \vdots \\ a_{j1} & \cdots & a_{jj} & \cdots & a_{jn} \\ \vdots & & & \ddots & \vdots \\ a_{n1} & & \cdots & & a_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} & & & a_{1n} \\ & \overline{A} & & \vdots \\ & & & a_{jn} \\ & & & \vdots \\ \overline{a}_{n1} & \overline{a}_{n2} & \cdots & 1 \end{pmatrix}, \text{onde } \overline{a}_{nk} = \left(\frac{1-a_{nn}}{a_{jn}}\right) a_{jk} + a_{nk},\ k = 1, \ldots, n.$$

Agora se na matriz TA obtida acima temos $\overline{a}_{in} \neq 0$, tome $T_i = I - a_{in}E_{in}$, para $i = 1, \ldots, n-1$ e faça $T_{n-1} \cdots T_2 T_1 TA$. Caso $a_{jn} = 0$, o fator T_j não aparece na sequência de multiplicações. Sendo assim:

$$M = T_{n-1} \cdots T_2 T_1 TA = \begin{pmatrix} & & & 0 \\ & A' & & \vdots \\ & & & 0 \\ & & & \vdots \\ \overline{a}_{n1} & \overline{a}_{n2} & \cdots & 1 \end{pmatrix}.$$

Vamos calcular o determinante de $T_{n-1}\cdots T_2T_1TA$ utilizando o método dos cofatores(Teorema de Laplace) e para isso escolheremos a n-ésima coluna. Sendo assim:

$$\begin{aligned} det(T_{n-1}\cdots T_2T_1TA) &= (-1)^{n+n}.det(A') \\ det(T_{n-1})\cdots det(T_1)det(T)det(A) &= det(A'). \text{ Assim, temos que} \\ det(A') &= 1 \end{aligned}$$

Portanto A' está em $SL(n-1,q)$ e usando a hipótese de indução ii), existem transvecções $\tilde{T}_k,\cdots,\tilde{T}_1$ em $SL(n-1,q)$, tais que $\tilde{T}_k,\cdots,\tilde{T}_1A' = I$. Logo,

$$T'_k\cdots T'_2T'_1M = \begin{pmatrix} & & & 0 \\ & I & & \vdots \\ & & & 0 \\ & & & \vdots \\ \overline{a}_{n1} & \overline{a}_{n2} & \cdots & 1 \end{pmatrix},$$

onde cada $T'_i = \begin{pmatrix} \tilde{T}_i & 0 \\ 0 & 1 \end{pmatrix}$ é uma transvecção em $SL(n,q)$.

Agora, tomamos as transvecções $\overline{T}_j = I - \overline{a}_{nj}E_{nj}$ para $j = 1, ..., n-1$ e consideramos a seguinte sequência de multiplicações que, finalmente, obteremos a identidade:

$$\overline{T}_{n-1}\cdots\overline{T}_1T'_k\cdots T'_2T'_1M = \begin{pmatrix} & & & & 0 \\ & I & & & \vdots \\ & & & & 0 \\ & & & & \vdots \\ 0 & \cdots & 0 & \cdots & 1 \end{pmatrix},$$

ou seja, existe um produto de transvecções P, tal que $PA = I$.

Como demonstramos a afirmação, temos que toda matriz A pertencente a $SL(n,q)$ pode ser escrita como um produto de transvecções e portanto, concluímos que as transvecções geram $SL(n,q)$ quando $n > 1$.

□

Observação 3.13. *Perceba que a importância das transvecções destacada na Observação 3.11 se faz presente nos cálculos da demonstração anterior.*

Teorema 3.14. *Se $n > 2$, quaisquer duas transvecções são conjugadas em $SL(n,q)$.*

Demonstração. Começaremos mostrando que $I + aE_{ij}$ e $I + bE_{ij}$ são conjugadas:
Considere $c = a^{-1}b$ e seja D uma matriz diagonal $n \times n$, definida como:

$$\begin{aligned} D &= I + (c-1)E_{jj} + (c^{-1}-1)E_{kk} \text{ e temos :} \\ D^{-1} &= I + (c^{-1}-1)E_{jj} + (c-1)E_{kk}. \end{aligned}$$

Note que $D \in SL(n,q)$ e fazendo a conjugação:

$$\begin{aligned} D^{-1}(I + aE_{ij})D =& I + D^{-1}aE_{ij}D = I + (aE_{ij})D \\ =& I + aE_{ij} + a(c-1)E_{ij} \\ =& I + bE_{ij}, \end{aligned}$$

como queríamos.

Agora consideremos as transvecções $I + aE_{ij}$ e $I + aE_{rj}$, com $i \neq r$ e seja P a matriz $n \times n$, definida por

$$\begin{aligned} P =& I + E_{ir} - E_{ri} - E_{ii} - E_{rr}, \quad \text{e daí} \\ P^{-1} =& I + E_{ri} - E_{ir} - E_{ii} - E_{rr}. \end{aligned}$$

A matriz P está em $SL(n,q)$ e fazendo a conjugando:

$$\begin{aligned} P^{-1}(I + aE_{ij})P =& I + P^{-1}aE_{ij}P = I + aE_{ij} - aE_{rj} - aE_{ij} \\ =& I + aE_{rj}. \end{aligned}$$

De maneira análoga definimos $Q = I + E_{js} - E_{sj} - E_{jj} - E_{ss}$ de modo que $Q^{-1}(I + aE_{rj})Q = I + aE_{rs}$, onde $j \neq s$.

Resta-nos provar que $I + aE_{ij}$ e $I + bE_{rs}$, com $i \neq r$ e $j \neq s$ são conjugadas. De fato, já sabemos que existe P em $SL(n,q)$ tal que:

$$P^{-1}(I + bE_{rs})P = I + bE_{is}, \qquad r \neq i.$$

Por outro lado, existe Q em $SL(n,q)$ satisfazendo:

$$Q^{-1}(I + bE_{is})Q = I + bE_{ij}, \qquad s \neq j.$$

Usando as relações acima, chegamos que:

$$I + bE_{ij} = Q^{-1}P^{-1}(I + bE_{rs})PQ. \qquad (*)$$

Também já vimos que existe D em $SL(n,q)$, tal que:

$$D^{-1}(I + aE_{ij})D = I + bE_{ij}.$$

E substituindo $(*)$ na igualdade acima:

$$\begin{aligned} D^{-1}(I + aE_{ij})D =& Q^{-1}P^{-1}(I + bE_{rs})PQ \\ I + aE_{ij} =& DQ^{-1}P^{-1}(I + bE_{rs})PQD^{-1}, \end{aligned}$$

onde concluímos que $I + aE_{ij}$ e $I + bE_{rs}$ são conjugadas.

Dessa forma, todas as transvecções são conjugadas em $SL(n,q)$, $n > 2$. □

Lema 3.15. *Seja $\mathbb{F}$ um corpo finito com q elementos, tal que para todo l pertencente a $\mathbb{F}^*$ temos $l^4 = 1$. Então, $q = 5, q = 3$ ou $q = 2$.*

Demonstração. Sabendo que $\mathbb{F}^*$ é um grupo cíclico finito, seja $g \in \mathbb{F}^*$ o gerador. Logo, $g^4 = 1$ e assim $|g| = 4$, $|g| = 2$ ou $|g| = 1$. Dessas três possibilidades segue que $q = 5, q = 3$ ou $q = 2$. □

Teorema 3.16. *Seja $\mathbb{F}$ um corpo, onde $q \neq 2$. Se um subgrupo normal N de $SL(2, q)$ contém uma transvecção, então $N = SL(2, q)$.*

Demonstração. Como o subgrupo N contém uma transvecção, suponhamos que ela seja do seguinte tipo:

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

Queremos provar que $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N$, $\forall\, x \in \mathbb{F}^*$, pois se isso ocorre, conjugando $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ por $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ temos que:

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ -1 & -x \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -x & 1 \end{pmatrix} \in N,\ \forall x \in \mathbb{F}, \end{aligned}$$

desse modo todas as transvecções pertencem a N e o Teorema 3.12 assegura que $N = SL(2, q)$.

Conjugando $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ por $\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$:

$$\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}^{-1} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} x & ax \\ 0 & x^{-1} \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix}.$$

E assim, N contém a matriz:

$$\begin{aligned} \begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & ay^2 \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -ay^2 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a(x^2 - y^2) \\ 0 & 1 \end{pmatrix}, \forall\ x, y \in \mathbb{F}^*. \end{aligned}$$

Denotaremos por $car(\mathbb{F})$ a característica de $\mathbb{F}$ e estudaremos dois casos:

i) $\mathbb{F}$ tem característica diferente de 2. Se isto ocorre, dado $b \in \mathbb{F}$ reescreva b como:

$$b = \left(\frac{b+1}{2}\right)^2 - \left(\frac{b-1}{2}\right)^2 = \frac{(b+1)^2}{4} - \frac{(b-1)^2}{4}.$$

E assim, $\begin{pmatrix} 1 & ab \\ 0 & 1 \end{pmatrix} \in N$, $\forall\ b \in \mathbb{F}$. Como $a \neq 0$, temos que ab percorre todos os elementos em $\mathbb{F}$ e portanto, todas as transvecções da forma $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \in N$, $\forall\, c \in \mathbb{F}^*$.

ii) $\mathbb{F}$ tem característica igual a 2. N contém $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ e $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$, onde $r = ax^2$. Conjugando estas matrizes por $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, temos:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \in N.$$

e

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & r \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \in N.$$

Além disso, N também contém:

$$\begin{aligned}\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} &= \begin{pmatrix} 1 & m \\ a & am+1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1+mr & m \\ a+r(am+1) & am+1 \end{pmatrix}, \qquad (*)\end{aligned}$$

onde $a^{-1}m$ é um quadrado.

Pelo lema anterior, sabemos que se $l^4 = 1 \ \forall \ l \in \mathbb{F}^*$, então $q = 5$, $q = 3$ ou $q = 2$. Pela nossa hipótese, só poderíamos ter $q = 5$ ou $q = 3$. Como estamos considerando a característica de $\mathbb{F}$ igual a 2, isto não é possível. Logo, existe l pertencente à $\mathbb{F}$ tal que $l^4 \neq 1$. Com isso, definimos $m = a^{-1}(1 + l^{-2})$ e $r = al^2$, os quais satisfazem:

$$\begin{aligned}amr &= aa^{-1}(1+l^{-2})al^2 \\ &= \quad al^2 + a = a + r\end{aligned}$$

e $a^{-1}m = [a^{-1}(1 + l^{-1})]^2$, pois

$$\begin{aligned}[a^{-1}(1+l^{-1})]^2 &= (a^{-1})^2(1 + \underbrace{2l^{-1}}_{0} + l^{-2}) \\ &= (a^{-1})^2(1+l^{-2}) \\ &= a^{-2}[1 + (l^{-1})^2] = a^{-1}m.\end{aligned}$$

Com os valores de m e r definidos acima, $(*)$ torna-se $\begin{pmatrix} 1+mr & m \\ 0 & 1+am \end{pmatrix}$. E para y arbitrário, N contém:

$$\left[\begin{pmatrix} 1+mr & m \\ 0 & 1+am \end{pmatrix}, \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\right] =$$

$$\begin{pmatrix} \frac{1}{1+mr} & \frac{m}{(1+am)(1+mr)} \\ 0 & \frac{1}{1+am} \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1+mr & m \\ 0 & 1+am \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & my(r+a)(1+mr)^{-1} \\ 0 & 1 \end{pmatrix}. \qquad (**)$$

Sabendo que $mr = a^{-1}(1 + l^{-2})al^2 = l^2 + 1$ e que $am = [(a^{-1})(1 + l^{-2})] = 1 + l^{-2}$ temos:

$$\begin{aligned} my(r-a)(1-mr)^{-1} =& (amy + myr)(1 + 1 + l^2)^{-1} = l^{-2}[y(1 + l^{-2}) + y(l^2 + 1)] \\ =& l^{-2}y(1 + l^{-2} + l^2 + 1) = yl^{-4} + y \\ =& y(l^{-4} + 1). \end{aligned}$$

E, assim, $(**)$ torna-se $\begin{pmatrix} 1 & y(l^{-4}+1) \\ 0 & 1+am \end{pmatrix}$. Como $l^4 \neq 1$ temos que $y(l^{-4} + 1)$ varia sobre todo x em $\mathbb{F}$, como queríamos.

□

Para os próximos resultados precisaremos usar a forma canônica racional de uma matriz. Para isto, apresentaremos a seguinte definição:

Definição 3.17. *Seja $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ um polinômio mônico de grau $n \geq 1$. Sua matriz companheira é definida como:*

$$M(p) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \vdots & 0 \\ 0 & 0 & 0 & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix}$$

a matriz $n \times n$ com a última linha dada pelos simétricos dos coeficientes de $p(x)$(com exceção do coeficiente líder que é sempre igual a 1), e subdiagonal $(j, j + 1)$ igual a 1.

Teorema 3.18 (Teorema da Forma Canônica Racional)**.** *Toda matriz A é semelhante a uma matriz $R(A)$ formada por blocos diagonais que são matrizes companheiras de certos polinônios mônicos p_1, p_2, $\cdots$, p_t, unicamente determinados pela condição de que cada um divide o subsequente.*

A matriz $R(A)$ referida acima é chamada de **forma racional** de A.

Observação 3.19. *O Teorema da Forma Canônica Racional assegura que qualquer matriz $A \in SL(n, q)$ é conjugada em $GL(n, q)$ a uma matriz em blocos B:*

$$B = \begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & M_S \end{pmatrix}.$$

Onde cada M_i é uma matriz companheira de algum polinômio mônico, assim como definimos acima.

Pelo Teorema 3.18 sabemos que existe uma matriz $P \in GL(n,q)$, tal que $A = P^{-1}BP$. Mas, podemos considerar que essa matriz P que faz a conjugação está em $SL(n,q)$. De fato, denote por b o determinante de P. A matriz $P' = \frac{IP}{\sqrt[n]{b}}$ é tal que $det(P') = 1$ e $A = P'^{-1}BP'$, já que $detP' = det\left(\frac{IP}{\sqrt[n]{b}}\right) = \left(\frac{1}{\sqrt[n]{b}}\right)^n detP = 1$ e $A = P^{-1}BP = \frac{1}{\sqrt[n]{b}}P'^{-1}B\sqrt[n]{b}P' = P'^{-1}BP'$. Logo, concluímos que toda matriz em $SL(n,q)$ é conjugada a uma matriz da forma B que também está em $SL(n,q)$.

Note que tivemos que utilizar a forma canônica racional ao invés da forma canônica de Jordan. Isto porque a forma de Jordan só é válida em corpos algebricamente fechados, o que não é o nosso caso. Já a forma racional é válida para espaços vetoriais sobre qualquer corpo.

Agora estamos em condições de demonstrar o Teorema 3.8. Vamos dividi-lo em dois teoremas para propiciar um melhor entendimento da demonstração.

Teorema 3.20. *Seja N um subgrupo normal do $SL(2,q)$, o qual não está contido no centro e seja $q > 3$. Então, $N = SL(2,q)$.*

Demonstração. Como N não está contido no centro, existe $A' \in N$, tal que $A' \notin Z(SL(n,q))$. Seja $P \in SL(n,q)$ tal que $P^{-1}A'P = A$, onde A está na forma canônica racional. Como o subgrupo N é normal temos que $A \in N$. Observe que a nossa demonstração se resume em encontrar uma transvecção que pertença a N, pois o restante seguirá do Teorema 3.16. Sendo assim, suponhamos, por absurdo, que N não contém tranvecções. Vamos analisar as formas possíveis para a matriz $A \in N$:

i) Se $A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, onde $a \neq a^{-1}$. Seja $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, então N contém o comutador :

$$[A,B] = A^{-1}B^{-1}AB = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} a^{-1} & -a^{-1} \\ 0 & a \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1-a^{-2} \\ 0 & 1 \end{pmatrix}.$$

Observe que a matriz obtida é uma transvecção, já que $a \neq a^{-1}$ implica $a^2 \neq 1$.

ii) Agora se tivermos $A = \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}$, como $det(A) = 1$, então: $A = \begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix}$ e

$A^{-1} = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$. Para $x \in \mathbb{F}^*$, calculemos:

$$\begin{aligned}\left[A^{-1}, \begin{pmatrix} 1 & x^2 \\ 0 & 1 \end{pmatrix}\right] &= \begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix}\begin{pmatrix} 1 & x^2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -x^2 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & -x^2+a \end{pmatrix}\begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -x^2 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -x^2 & 1 \end{pmatrix}\begin{pmatrix} 1 & -x^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -x^2 \\ -x^2 & 1+x^4 \end{pmatrix} \in N,\ \forall x \in \mathbb{F}^*.\end{aligned}$$

Conjugando esse resultado pela matriz $\begin{pmatrix} x^{-1} & -x^{-1} \\ 0 & x \end{pmatrix}$ temos:

$$\begin{aligned}\begin{pmatrix} x & x^{-1} \\ 0 & x^{-1} \end{pmatrix}\begin{pmatrix} 1 & -x^2 \\ -x^2 & 1+x^4 \end{pmatrix}\begin{pmatrix} x^{-1} & -x^{-1} \\ 0 & x \end{pmatrix} &= \begin{pmatrix} 0 & -x^{-1} \\ -x & x^{-1}+x^3 \end{pmatrix}\begin{pmatrix} x^{-1} & -x^{-1} \\ 0 & x \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & 2+x^4 \end{pmatrix}.\end{aligned}$$

E portanto, para todos x, y não-nulos, N contém a matriz:

$$\begin{pmatrix} 0 & 1 \\ -1 & 2+x^4 \end{pmatrix}^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 2+y^4 \end{pmatrix} = \begin{pmatrix} 1 & x^4-y^4 \\ 0 & 1 \end{pmatrix}.$$

Como por hipótese, N não contém transvecções, temos que $x^4 - y^4 = 0$, isto é, $x^4 = 1,\ \forall\ x \in \mathbb{F}^*$. Assim sendo, pelo Lema 3.15, $q = 5$, $q = 3$ ou $q = 2$. No nosso caso só poderemos ter $q = 5$. Considerando agora $q = 5$, continuaremos na tentativa de encontrar uma transvecção em N. Já sabemos que $\begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix} \in N$. Calculando o seguinte comutador:

$$\begin{aligned}\left[\begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix}, \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}\right] &= \begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ -1 & -2+a \end{pmatrix}\begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -2 \\ -2 & 5 \end{pmatrix},\end{aligned}$$

que é igual à $\begin{pmatrix} 1 & -2 \\ -2 & 0 \end{pmatrix}$, pois $q = 5$ e assim a característica de $\mathbb{F}$ é 5. A matriz $\begin{pmatrix} 2 & -1 \\ -2 & -1 \end{pmatrix} \in SL(n,q)$ e utilizando-a para conjugar a matriz $\begin{pmatrix} 1 & -2 \\ -2 & 0 \end{pmatrix}$:

$$\begin{pmatrix} \frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}\begin{pmatrix} 1 & -2 \\ -2 & 0 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in N.$$

Finalmente, do fato que $\begin{pmatrix} 0 & 1 \\ -1 & a \end{pmatrix} \in N$, segue que $\begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix} \in N$ e portanto:

$$\begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in N.$$

Como $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ é uma transvecção, concluímos a demonstração. □

Teorema 3.21. *Seja $\mathbb{F}$ um corpo finito e N um subgrupo normal do $SL(n, q)$, o qual não está contido no centro. Se $n \geq 2$, então $N = SL(n, q)$.*

Demonstração. Como $N \nsubseteq Z(SL(n, q))$, então existe $A' \in N$, tal que $A' \notin Z(SL(n, q))$. Sabemos que existe $P \in SL(n, q)$ de modo que $A' = PAP^{-1}$, onde:

$A = \begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & M_S \end{pmatrix}$ e os M_i são as matrizes companheiras.

Temos que $A = P^{-1}A'P$ e como N normal $A \in N$. Queremos mostrar que o fato de A pertencer A N implica que teremos uma transvecção em N. Com isso, chegaremos que como N é normal, N vai conter todas as transvecções em $SL(n, q)$, pois o Teorema 3.14 nos garante que se $n \geq 2$, qualquer duas transvecções são conjugadas. E, finalmente, o Teorema 3.12 diz que se $n > 1$, as transvecções geram $SL(n, q)$, onde concluíremos que $N = SL(n, q)$. Logo, nossa demonstração se baseia em encontrar uma transvecção em N. Para isso, vamos supor primeiramente que cada bloco M_i de A é 1×1, isto é, A é diagonal:

$$A = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}.$$

Como $A \notin Z(SL(n, q))$ temos que pelo menos dois dos $a_i's$ são distintos. Vamos supor que $a_1 \neq a_2$, pois se isso não ocorre podemos fazer uma mudança de base e a nova matriz será conjugada a A, logo pertencerá a N. Calculando $[A, I + E_{12}]$, obtemos:

$$\begin{aligned} [A, I + E_{12}] &= A^{-1}(I + E_{12})^{-1}A(I + E_{12}) = (A^{-1} - A^{-1}E_{12})(A + AE_{12}) = \\ &= I + A^{-1}a_1E_{12} - a_1^{-1}a_2E_{12} - a_1^{-1}E_{12}a_1E_{12} = I + (1 - a_1^{-1}a_2)E_{12}, \end{aligned}$$

que é uma transvecção.

Agora suponhamos que alguma matriz companheira M_i de A tenha tamanho $r > 1$. Iremos supor que $i = 1$, pois caso não seja, conjugamos por uma permutação e obtemos

tal configuração. Então:

$$A = \begin{pmatrix} \overline{A} & 0 \\ 0 & * \end{pmatrix}, onde\ \overline{A} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \vdots & 0 \\ 0 & 0 & 0 & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{r-1} \end{pmatrix}_{r\times r} = M_1.$$

Como $det(A) = 1$ temos $a_0 \neq 0$. Sendo assim, analisaremos dois casos: $r > 2$ e $r = 2$.

i) Suponhamos primeiramente que $r > 2$. Sabemos que N contém:

$$\begin{aligned} [A, I - E_{r1}] =& A^{-1}(I - E_{r1})^{-1}A(I - E_{r1}) \\ =& (A^{-1} + A^{-1}E_{r1})(A - AE_{r1}) \\ =& I - E_{r1} + A^{-1}E_{r1}A + A^{-1}E_{r1}AE_{r1} \\ =& I - E_{r1} + A^{-1}E_{r2} + A^{-1}E_{r2}E_{r1} \\ =& I - E_{r1} + a_0^{-1}E_{12}. \end{aligned}$$

Além disso, N contém:

$$\begin{aligned} [I + a_0^{-1}E_{12} - E_{r1}, I - E_{r1}] =& (I - a_0^{-1}E_{12} + E_{r1} - a_0^{-1}E_{r2})(I + E_{r1}) \\ & (I + a_0^{-1}E_{12} - E_{r1})(I - E_{r1}) \\ =& (I + E_{r1} - a_0^{-1}E_{12} + E_{r1} - a_0^{-1}E_{r2}) \\ & (I - E_{r1} + a_0^{-1}E_{12} - E_{r1}) \\ =& I + a_0^{-1}E_{r2}, \end{aligned}$$

que é uma transvecção, como queríamos.

ii) Agora vamos supor $r = 2$. Neste caso, temos $\overline{A} = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$ e $a \neq 0$, pois $det(A) = 1$. Já vimos que em $SL(2,q)$ as matrizes que estão no centro são múltiplas da identidade. Desse modo, existe $C \in SL(2,q)$ tal que C não comuta com $\overline{A}$. Calculando o comutador:

$$\left[\begin{pmatrix} \overline{A} & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} C & 0 \\ 0 & I_{(n-2)\times(n-2)} \end{pmatrix}\right] = \begin{pmatrix} \overline{B} & 0 \\ 0 & I_{(n-2)\times(n-2)} \end{pmatrix} = B \in N.$$

Daí segue que $\overline{B} \neq I_2$, pois $\overline{A}C \neq C\overline{A}$. Podemos considerar que $\overline{B}$ está na forma racional, pois caso contrário basta fazermos uma mudança de base. Como $det(B) = 1$, temos as seguintes possibilidades para $\overline{B}$:

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & c \end{pmatrix} e \begin{pmatrix} -a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Se $\overline{B} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ temos que $\mathbb{F}$ não tem característica 2, isso porque $\overline{B} \neq$ -$\overline{B}$, senão $B = I_2$ o que não ocorre. Efetuando:

$$\left[\begin{pmatrix} -I_{2\times 2} & 0 \\ 0 & I_{(n-2)\times(n-2)} \end{pmatrix}, I + E_{23}\right] = I + 2E_{23},$$

conseguimos uma transvecção, já que a característica de $\mathbb{F}$ é diferente de 2. Se $\overline{B} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, computando:

$$\begin{aligned}\left[\begin{pmatrix} \overline{B} & 0 \\ 0 & I \end{pmatrix}, I + E_{12}\right] =& \begin{pmatrix} \overline{B}^{-1} & 0 \\ 0 & I \end{pmatrix}(I - E_{12})\begin{pmatrix} \overline{B} & 0 \\ 0 & I \end{pmatrix}(I + E_{12}) \\ =&(I + (a^{-1} - 1)E_{11} + (a - 1)E_{22} - a^{-1}E_{12}) \\ &(I + (a - 1)E_{11} + (a^{-1} - 1)E_{22} + aE_{12}) \\ =&I + (1 - a^{-2})E_{12}.\end{aligned}$$

Também obtemos uma transvecção pertencente a N.

Agora, se $\overline{B}$ é da forma $\begin{pmatrix} 0 & 1 \\ -1 & c \end{pmatrix}$, então N contém o seguinte comutador:

$$\begin{aligned}\left[I - E_{13}, \begin{pmatrix} \overline{B} & 0 \\ 0 & I_{(n-2)\times(n-2)} \end{pmatrix}\right] =&(I + (c - 1)E_{11} - E_{12} + E_{13} + E_{21} + E_{22}) \\ &(I - E_{11} - E_{21} + (c - 1)E_{22} - E_{13} + E_{12}) \\ =&I + (1 - c)E_{13} - E_{23}.\end{aligned}$$

E, por fim, calculando o comutador:

$$\begin{aligned}[I + (1 - c)E_{13} - E_{23}, I + E_{12}] =&(I + (1 - c)E_{13} + E_{23}) \\ &(I - E_{12})(I + (1 - c)E_{13} - E_{23})(I + E_{12}) \\ =&(I - E_{12} + (c - 1)E_{13} + E_{23})(I + E_{12}(1 - c)E_{13} - E_{23}) \\ =&I + E_{13},\end{aligned}$$

obtemos $I + E_{13}$, que é uma transvecção em N. E portanto, concluímos a demonstração.

□

Corolário 3.22 (Jordan-Dickson)**.** *Se $n \geq 2$ e $|\mathbb{F}| > 3$, então $PSL(n,q)$ é simples.*

Demonstração. Sabemos que o $PSL(n,q) = \dfrac{SL(n,q)}{Z(SL(n,q))}$. Sendo assim, seja $\overline{N} \trianglelefteq \dfrac{G}{Z(G)}$, onde $G = SL(n,q)$. Pelo Teorema da Correspondência temos que existe $N \trianglelefteq G$, com $Z(G) \leq N$ e tal que $\overline{N} = \dfrac{N}{Z(G)}$. Mas se $N = Z(G)$, então $\overline{N} = 1$. Por outro lado, se $N \neq Z(G)$, pelo teorema anterior segue que $\overline{N} = PSL(n,q)$. Logo, $PSL(n,q)$ é simples nestas condições e, por isso, o Teorema de Jordan- Dickson segue como corolário dos Teoremas 1.20 e 1.21. □

Agora vamos utilizar o Teorema de Jordan-Dickson para analisar alguns exemplos:

Exemplo 3.23. *Primeiramente verificaremos o que ocorre com os casos não abordados pelo Teorema de Jordan-Dickson, isto é, $PSL(2,2)$ e $PSL(2,3)$. De acordo com o Teorema 3.7 temos que $|PSL(2,2)| = 6$ e portanto ele não é um grupo simples, pois é isomorfo a S_3, o grupo de permutações de 3 elementos. Já o $PSL(2,3)$ tem ordem 12 e é isomorfo a A_4 e, por isso, não é simples.*

Exemplo 3.24. *Os grupos $PSL(2,4)$ e $PSL(2,5)$ são isomorfos, pois $|PSL(2,4)| = |PSL(2,5)| = 60$ e então pelo Teorema 2.17 eles são isomorfos à A_5.*

Exemplo 3.25. *A simplicidade de $PSL(2,7)$ é garantida pelo Teorema de Jordan-Dickson e ele é um grupo simples diferente daqueles que vimos na seção anterior, já que $|A_5| < 168 < |A_6|$. Um outro exemplo é o $PSL(3,3)$ que possui ordem 5616.*

O próximo exemplo é interessante, pois mostra que existem grupos simples com mesma ordem, mas que não são isomorfos.

Exemplo 3.26. *Os grupos $PSL(3,4)$ e A_8 possuem a mesma ordem, mas não são isomorfos.*

De fato, o grupo A_8 possui ordem igual a $\frac{1}{2}8!$ e pelo Teorema 3.7, $|PSL(3,4)| = \frac{1}{2}8!$. O grupo A_8 possui o elemento $(12345)(678)$, cuja ordem é 15. Se A_8 fosse isomorfo a $PSL(3,4)$, então existiria A pertencente a $PSL(3,4)$ tal que $|A| = 15$. Mostraremos que isso não ocorre. Para tal, suponhamos por absurdo, que existe A em $PSL(3,4)$ cuja ordem é 15.

Seja A' uma matriz na forma canônica racional, satisfazendo $A' = P^{-1}AP$, logo $|A| = |A'|$. Dessa forma, podemos supor que A está na forma racional. E assim, existem as seguintes possibilidades para A:

$$\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix} e \begin{pmatrix} a & 0 \\ 0 & \begin{pmatrix} 0 & 1 \\ b & c \end{pmatrix} \end{pmatrix}, \text{ onde } a, a_1, a_2, a_3 \in \mathbb{F}^* \text{ e } b, c \in \mathbb{F}$$

Se $A = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & a_3 \end{pmatrix}$, *temos que* $A^3 = \begin{pmatrix} a_1^3 & 0 & 0 \\ 0 & a_2^3 & 0 \\ 0 & 0 & a_3^3 \end{pmatrix} = I$, *pois como $\mathbb{F}$ possui 4 elementos, então $\mathbb{F}^*$ possui ordem 3.*

Agora, se $A = \begin{pmatrix} a & 0 \\ 0 & \begin{pmatrix} 0 & 1 \\ b & c \end{pmatrix} \end{pmatrix}$ *teremos:*

$$A^3 = \begin{pmatrix} a^3 & 0 \\ 0 & \begin{pmatrix} 0 & 1 \\ b & c \end{pmatrix}^3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \begin{pmatrix} 0 & 1 \\ b & c \end{pmatrix}^3 \end{pmatrix},$$

e assim para que A tenha ordem 15, deveremos ter $B = \begin{pmatrix} 0 & 1 \\ b & c \end{pmatrix} \in PSL(2,4)$ *e tal que $|B| = 15$. Mas, $PSL(2,4) \simeq A_5$, porém A_5 não possui elemento de ordem 15. Concluímos que não existe elemento de ordem 15 em $PSL(3,4)$ e, portanto, $PSL(3,4)$ e A_8 não são isomorfos.*

Considerações Finais: A Classificação dos Grupos Simples Finitos

A teoria dos grupos finitos atingiu a maturidade com o Teorema de Classificação dos Grupos Simples Finitos, o qual afirma que todos os grupos simples finitos pertencem a uma das quatro categorias que citaremos posteriormente. Ele é o resultado do empenho de várias gerações de matemáticos ao longo de mais de 100 anos. Segundo estimativas, sua demonstração ocupa 10.000 páginas impressas e distribuídas ao longo de 500 artigos individuais.

Pode-se considerar que este projeto teve início em 1892, quando Otto Hölder sugeriu em uma palestra que seria interessante se fosse possível descrever uma coleção de grupos simples finitos.

Um dos pioneiros desta área foi Richard Brauer, tendo começado os estudos sobre a simplicidade de grupos finitos no final da década de 40. Nos anos subsequentes, Brauer foi praticamente o único a trabalhar com grupos simples finitos, exceto pelo importante trabalho de Claude Chevally, em 1955, sobre os grupos de tipo Lie que teve considerável impacto na área.

Um resultado importante que proporcionou novas perspectivas na área dos grupos simples finitos e que apontou a direção para a sua classificação é o célebre teorema de Walter Feit e John Thompson de 1962, o qual garante que todo grupo finito de ordem ímpar é solúvel e cuja demonstração ocupa um volume de 255 páginas.

Em 1965, surgiu o primeiro grupo esporádico: o grupo J_1 de Zvonimir Janko, aguçando ainda mais o interesse dos matemáticos na teoria dos grupos simples finitos. Os grupos esporádicos são denominados assim devido ao fato de que eles não são membros de uma família infinita de grupos simples finitos, isto é, aparecem de forma isolada.

Apesar do grupo J_1 conter somente 75.560 elementos, um número pequeno diante do padrão da teoria dos grupos simples finitos, permaneceu desconhecido por um século, isto porque, em 1861, Emil Mathieu já havia descoberto os primeiros 5 grupos esporádicos. Sendo assim, ao longo dos 10 anos seguintes, mais de 20 grupos esporádicos foram encontrados. Destaque para o grupo de Bernd Fisher e Robert Griess, que é o maior de todos, tendo uma ordem de aproximadamente 10^{54} e, por isso, conhecido como o grupo "Monstro".

Em 1981, Daniel Gorestein anunciou que a classificação estava completa. No entanto, por volta de 1986, Michael Aschbacher notou que o artigo de Geoff Mason, que tratava

de um dos casos que aparecem no problema de classificação, estava incompleto. Mas foi em 1996 que Aschbacher e Stephen Smith assumiram a tarefa de melhorar o artigo de Mason. A publicação deste artigo seria o marco final da demonstração do Teorema de Classificação.

Contudo, a comunidade matemática ainda expressa certo incômodo com a abordagem empregada para classificar os grupos simples finitos, devido a sua extensa demonstração de 10.000 páginas.

Vale ressaltar que houve um movimento de revisão e de redução do tamanho da demonstração. Isto porque muitos dos artigos que compõe a demonstração foram escritos em uma época em que alguns métodos valiosos, usados hoje, ainda não haviam sido completamente elaborados.

Finalmente, temos que o Teorema de Classificação tem aplicações em muitos ramos da matemática, já que problemas sobre a estrutura dos grupos finitos as vezes podem ser reduzidos a problemas sobre grupos simples finitos. Ou seja, graças ao teorema, alguns problemas podem ser resolvidos verificando cada família de grupos simples e cada grupo esporádico.

Entretanto, muitas vezes os grupos simples finitos abrangidos pela demonstração, são referidos como "grupos simples finitos conhecidos", enfatizando assim a desconfiança com respeito ao Teorema de Classificação. Com isso, resultados que dependeriam da classificação e que, a princípio, valeriam para todos os grupos finitos, passam a valer pelo menos para os grupos finitos cujos fatores na série de composição são grupos simples finitos conhecidos.

Agora, citaremos de forma breve e superficial as categorias de grupos simples abrangidas pelo teorema e enunciaremos o Teorema de Classificação [1].

3.3 Grupos Finitos de Tipo Lie

Os grupos ***lineares, unitários, simpléticos e ortogonais*** são conjuntamente conhecidos como ***grupos clássicos***. Esses grupos, quando definidos sobre um corpo finito são, além dos grupos alternados que apresentamos na seção 1 do Capítulo 2, os exemplos mais elementares de grupos simples finitos.

Esta classe de grupos foi generalizada primeiramente por Claude Chevalley e depois por Robert Steinberg, Michio Suzuki, Remhak Ree e Jacques Tits e hoje é composta de 16 famílias infinitas de grupos simples finitos que foram chamados de ***grupos finitos de tipo Lie***. Tal generalização faz uso da teoria das álgebras de Lie complexas simples e descreve de forma unificada os grupos clássicos sobre corpos finitos.

Por fim, temos que os grupos finitos de tipo Lie consistem dos grupos clássicos e dos grupos de Chevalley, os quais não definiremos aqui.

3.4 Grupos Esporádicos

Nem sempre os grupos simples finitos aparecem em séries infinitas e tais exceções são conhecidas como ***grupos esporádicos***. Esse termo foi usado por Burnside para se referir aos grupos de Mathieu, que formam uma mini-série de 5 grupos.

Existem 26 grupos esporádicos que ainda não estão definitivamente organizados sob um único ponto de vista. O maior de todos eles é o chamado Monstro, já citado aqui. Dentre os 26 grupos esporádicos, 20 estão envolvidos nele como subquocientes e formam, segundo Robert Griess, a "Happy Family", que é dividida em 3 gerações.

A primeira geração é composta dos 5 grupos de Mathieu. A segunda consiste de três grupos de Conway, juntamente com o grupo de Higman-Sims, o grupo de McLaughlin, o grupo de Hall-Janko e o grupo de Suzuki. A terceira geração é formada pelos 8 grupos esporádicos que estão envolvidos no Monstro, sendo eles: os 4 grupos de Fisher, o grupo de Held, o grupo de Harada-Norton e o grupo de Thompson.

Os 6 grupos restantes não estão envolvidos no Monstro e, portanto, não fazem parte da "Happy Family" e são chamados de "Parias". São eles a mini-série dos 3 grupos de Janko, o grupo de Lyons, o grupo de Rudvalis e o grupo de O'Nan.

3.5 Teorema de Classificação

Finalmente, segue abaixo o enunciado do importante Teorema de Classificação dos Grupos Simples Finitos, a principal motivação deste trabalho.

Teorema 3.27 (Classificação dos Grupos Simples Finitos)**.** *Seja G um grupo simples finito. Então G é um dos seguintes grupos:*

(i) um grupo cíclico de ordem prima,

(ii) um grupo alternado de grau $n \geq 5$,

(iii) um grupo finito de tipo Lie na forma adjunta ou

(iv) um dos 26 grupos esporádicos.

Note que os grupos alternados de grau $n \geq 5$, abordados na Seção 1 do Capítulo 2, compõe o item (ii) do teorema acima.

Já os grupos de ordem menor que 60 que apresentamos na Seção 2 do Capítulo 2, se encaixam no item (i) do Teorema de Classificação, pois sabemos que o fato de possuirem ordem prima implica que são cíclicos.

Por fim, os grupos lineares especiais projetivos que destacamos no Capítulo 3, fazem parte dos grupos finitos de tipo Lie na forma adjunta (isto é, cujo centro é igual a 1).

Referências Bibliográficas

[1] ANTONELI, F. M. *Grupos finitos e quebra de simetria no código genético*, tese de doutorado, USP-2003.

[2] DUMMIT, D. S; FOOTE, R.M. *Abstract Algebra*, 2004.

[3] GAZZOLI, G. L ; SILVA, B.R. *Corpos Finitos e seus Grupos Multiplicativos*, 2013.

[4] GARCIA, A.; LEQUAIN Y. *Elementos de Álgebra*, 6.ed. Rio de Janeiro: IMPA (Projeto Euclides), 2013.

[5] GALLIAN, J. A. *Contemporary Abstract Algebra*, 2nd ed. Canada, 1990.

[6] GALLIAN, J. A. *The Search for Finite Simple Groups*, Mathematics Magazine, p.163-179, Vol. 49, 1976.

[7] GONÇALVES, A. *Introdução à Álgebra*, 5.ed. Rio de Janeiro: IMPA(Projeto Euclides), 2009.

[8] ISAACS, I. M. *Algebra, A Graduate Course*, Cole Publishing Company.

[9] LANG, S. *Algebra*, 3nd ed. Massachusetts, 1993.

[10] ROBINSON, D. J. S. *A course in the theory of groups*, 2nd ed. Springer, 1995.