UNIVERSIDADE FEDERAL DE MINAS GERAIS

ESPECIALIZAÇÃO EM MATEMÁTICA

SOBRE GRUPOS SOLÚVEIS FINITOS

Érika Helena Assis

Belo Horizonte - MG

2015

Sumário

Agradecimentos

Agradeço, primeiramente, a Deus por me suprir em todas as minhas necessidades, me amparar em todos os momentos e me possibilitar aprender lições maiores que as acadêmicas.

A minha mãe, por acreditar nos meus sonhos, por suas orações repletas de fé e por ser sempre um exemplo de fortaleza e perseverança nas dificuldades.

Aos meus familiares, pelo apoio e carinho de sempre.

A minha orientadora, Ana Cristina, pelo incentivo e intenso apoio que ecoam em minha mente sempre. Além disso, sou grata pelo carinho, pela paciência e tolerância, principalmente às dúvidas mais simples que me surgiram no árduo processo de conclusão desse trabalho.

Aos amigos que conquistei durante a minha gradução e a presente especialização e que contribuíram significativamente para realização deste sonho.

Resumo

Neste trabalho, apresentaremos os principais resultados sobre os grupos solúveis finitos e estudaremos os subgrupos transitivos e solúveis em grupos simétricos de grau primo.

Introdução

O problema de resolver equações polinômiais sempre fascinou os matemáticos e se tornou um grande foco de estudo da Álgebra. Há relatos históricos de que a fórmula para resolver a equação $ax^2 + bx + c = 0$ começou a ser estuda pelos Babilônios. Em meados de 1.500, os italianos Spcione del Ferro (1465 - 1526), Tartaglia (1499 - 1557), Girolomo Cardono (1501 - 1576) e Lodovico Ferrari (1522 - 1565) deram suas contribuições para a solução de polinômios de terceiro e quarto grau. Porém, uma fórmula para resolver os polinômios de grau maior ou igual a cinco ainda não tinha sido encontrada.

No ínicio do séc XIX, matemáticos como Leonhard Euler e Joseph-Louis Lagrange, também se dedicaram a tentar encontrar uma solução para os polinômios de grau cinco. Porém, os primeiro resultados foram publicados por Abel, em 1826. Abel demonstrou que não existem fórmulas simples para a solução de equações de grau superior a quatro. Sendo assim, abriu as portas, para anos mais tarde, Évariste Galois (1811 - 1832) formular um critério de solubilidade para equações algébricas da forma

$$a_n x^n + \ldots + a_1 x + a_0 = 0.$$

Galois deu origem à teoria dos grupos em 1832, esboçando o seu famoso trabalho sobre solubilidade por radicais.

A teoria de Galois associa cada polinômio $f(x) \in F[x]$ ao seu chamado Grupo de Galois de $f(x)$ sobre F, denominado assim em homenagem ao famoso matemático e denotado por $\mathcal{G}_f$ ou $Gal(f/F)$. É essencial enunciarmos um de seus principais teoremas:

Teorema 0.1. *Sejam F de característica zero e $f(x) \in F[x]$ um polinômio de grau $n > 1$. Se o polinômio é irredutível sobre F de grau n, então o seu grupo de Galois $Gal(f/F)$ é um subgrupo transitivo de S_n cuja ordem é divisível por n.*

Além disso, outro resultado importante é definir que uma extensão L de F é dita uma extensão radical se existe uma cadeia

$$F_0 = F \subseteq F_1 \subseteq F_2 \subseteq \ldots \subseteq F_t$$

tal que, para cada $i = 1, \ldots, t$, $F_i = F_{i-1}(u_i)$ e $u_i^{n_i} \in F_{i-1}$ para algum $n_i \in \mathbb{N}$. Diante disso, a equação $f(x) = 0$ é solúvel por radicais, se existe uma extensão radical F que contém o corpo de decomposição de $f(x)$.

A partir daí, Galois garante um critério de solubilidade para equações algébricas. Isto é, o polinômio $f(x)$ é solúvel por radicais, se, e somente se, o grupo $Gal(f/F)$ é solúvel. Portanto, o conhecimento sobre os grupos solúveis é de singular importância.

A presente monografia tem como objetivo apresentar os principais resultados sobre os grupos solúveis finitos. No capítulo 1, vamos relembrar algumas definições e resultados necessários para a compreensão dos capítulos subsequentes. No capítulo 2, vamos apresentar a definição e alguns exemplos dos grupos solúveis tais grupos e demonstrar seus principais resultados e propriedades. Além disso, vamos discutir proposições que determinam a solubilidade de um grupo a partir de sua ordem.

Por fim, no capítulo 3, discutiremos um teorema para identificar os subrupos solúveis de grupos simétricos.

Capítulo 1

Preliminares

Neste capítulo, começaremos com o estudo de alguns resultados básicos da Teoria de Grupo. Em seguida, vamos discutir conceitos inicias dos grupos simétricos. Nosso objetivo é abordar as principais definições e resultados que se farão úteis ao longo do nosso trabalho.

1.1 Grupos

Nesta seção, apresentaremos algumas definições e teoremas relacionados a grupos. Vamos apenas enunciar tais resultados. Ao leitor interessado, solicitamos consultar a referência indicada.

Teorema 1.1. *([3], Capítulo VI, Teorema 1) (Lagrange) Seja G um grupo finito e H um subgrupo de G então $|H|$ é um divisor de $|G|$, isto é, a ordem de H é um divisor da ordem de 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. O Teorema de Lagrange também mostra que $[G : H]$ é divisor de $|G|$. Além disso, segue como sua consenquência que todo grupo finito de ordem prima é cíclico, e, em particular, abeliano.

De acordo com seu índice no grupo, podemos afirmar a normalidade de um subgrupo. Recordaremos um resultado que discute as condições para garantirmos que um dado subgrupo é normal.

Teorema 1.2. *([3], Capítulo VI, Corolário 3 do Teorema 4) Seja G um grupo finito e p o menor divisor primo de $|G|$. Se existe um subgrupo H de G tal que $[G : H] = p$, então $H \trianglelefteq G$.*

Sendo assim, é claro que se H é um subgrupo de G tal que $[G : H] = 2$, então H é um subgrupo normal de G.

O próximo teorema garante a existência de elementos de determinada ordem em um grupo finito.

Teorema 1.3. *([3], Capítulo VI, Teorema 6) (Cauchy) Seja G grupo finito e $|G| = n$ e um primo tal que $p \mid n$. Então existe $x \in G$ tal que $\mathcal{O}(x) = p$*

Antes de enunciarmos outros resultados, vamos apresentar algumas definições básicas.

Definição 1.4. *Um grupo $G \neq \{1\}$ é simples se G e $\{1\}$ são seus únicos subgrupos normais.*

Definição 1.5. *O centro de um grupo, representado por $Z(G)$, é o conjunto dos elementos que comutam com todos os outros elementos em G, isto é,*

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

Analisando a definição do subgrupo $Z(G)$, podemos afirmar que ele é abeliano e normal em G. Além disso, por simples verificação, é possível constatar que se H é um subgrupo de $Z(G)$ e G/H cíclico, então G é abeliano.

Relembramos, também, que $G/Z(G)$ nunca tem ordem prima. De fato, pois se $|G/Z(G)| = p$, então $|G/Z(G)|$ é cíclico. Neste caso, note que G é abeliano, ou seja $G = Z(G)$, uma contradição.

Seja p um número primo e G um grupo finito. Se $|G| = p^n$, $n \in \mathbb{N}$, dizemos que G é um p-grupo. Pelo Teorema de Lagrange, um subgrupo de um p-grupo também é um p-grupo. Recordamos, também, que o centro de p-grupo nunca é trivial, para a demonstração consultar [1], página 410.

Por fim, ressaltamos que se $|G| = p^2$, segue que G é abeliano. Para comprovarmos a afirmação, basta mostrar que $Z(G) = G$. Como $Z(G) \leq G$, pelo Teorema de Lagrange, temos que $|Z(G)|$ divide $|G|$. Sendo assim, $|Z(G)| = 1$, p, p^2. Já comentamos que $Z(G) \neq \{1\}$ e também podemos afirmar que $|Z(G)| \neq p$. De fato, se $|Z(G)| = p$ temos $|G/Z(G)| = p$, uma contradição pois já mencionamos que $G/Z(G)$ não tem ordem prima. Logo $|Z(G)| = p^2 = |G|$ e, consequentemente, $Z(G) = G$, como queríamos.

Vamos enunciar um importante teorema.

Teorema 1.6. *([3], Capítulo VI, Teorema 5) (Teorema da Correspondência) Seja G e G' grupos e $\varphi : G \to G'$ um homomorfismo sobrejetivo, tal que $N = Ker(\varphi)$. Então,*

(a) Para todo $H \leq G$ tem-se $H' = \varphi(H) = \{\varphi(h) : h \in H\} \leq G'$. Mais ainda $H \trianglelefteq G \Rightarrow H' \trianglelefteq G'$.

(b) Para todo $H' \leq G'$ existe único $H = \varphi^{-1}(H') = \{g \in G : \varphi(g) \in H'\} \supseteq N, H \leq G$, tal que $\varphi(H) = H'$. Mais ainda $H' \trianglelefteq G' \Rightarrow H \trianglelefteq G$.

Como uma consequência do Teorema da Correspondência, temos que se 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 $\pi(H) = \overline{H}$ e $\pi : G \to \overline{G} = \overline{G}/N$ é a projeção canônica (H recebe o nome de pré-imagem de $\overline{H}$ em G). Mais ainda

$$\overline{H} \trianglelefteq \overline{G} \Leftrightarrow H \trianglelefteq G.$$

Definição 1.7. *([5], Capítulo 1) Seja X um subconjunto não vazio de um grupo G, o fecho normal de X em G, denotado por X^G, é a interseção de todos os subgrupos normais de G que contém X, equivalentemente,*

$$X^G = \langle g^{-1}Xg \mid g \in G \rangle.$$

O fecho normal de X em G é um subgrupo normal. Já o core de X em G, denotado por X_G, é definido pela interseção de todos os subgrupos normais de G contidos em X. Se não existe nenhum tal subgrupo, $X_G = \{1\}$.

Claramente, X^G é o menor subgrupo normal de G que contém X.

Definição 1.8. *Sejam G um grupo H um subgrupo de G. Definimos o normalizador de H em G como o conjunto*

$$N_G(H) = \{a \in G \mid aH = Ha\}.$$

A partir da definição acima, é claro que $X \subseteq N_G(H)$. Agora, vamos considerar a seguinte proposição dos normalizadores em p-grupos.

Proposição 1.9. *([2], Capítulo VI, Proposição VI.3.3) Seja G um grupo de ordem p^m e seja H um subgrupo de G de ordem p^r com $r < m$ então $H \lneq N_G(H)$. Ou seja, se H é um subgrupo próprio de um p-grupo finito então H está propriamente contido no seu normalizador.*

Estabeleceremos alguns resultados sobre ações de grupo sobre um conjunto.

Uma ação de um grupo G sobre um conjunto X é uma aplicação

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

tal que $1 \star x = x$ e $(g_1 \star g_2) \star x = g_1 \star (g_2 \star x)$, $\forall\ x \in X$ e $\forall\ g_1, g_2 \in G$. A aplicação

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

é chamada de transformação de X por g. Agora, vamos considerar a seguinte definição

Definição 1.10. *Seja X um conjunto não vazio. O conjunto*

$$Sim(X) = \{\ \sigma : X \longrightarrow X \mid \sigma \text{ bijetiva } \}$$

é um grupo com a operação composição de funções. Outra notação muito utilizada para $Sim(X)$ é $B_{ij}(X)$.

Uma maneira equivalente de expressar que $\varphi : G \times X \longrightarrow X$ é um ação de grupo é afirmando que

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

é um homomorfismo.

Definição 1.11. *([7], Capítulo 26, Definição 26.4) Suponha que G age sobre um conjunto X.*

(a) A equação $y = g \star x$ expressa que g move x para y.

(b) Dado $x \in X$ temos

$$Orb_G(x) := \{g \star x | g \in G\},$$

que é o conjunto de todos os elementos em X movidos a partir de x. Este conjunto é chamado de órbita de x em G. Por outro lado, os elementos em G que fixam x, formam um subgrupo de G denotado por

$$Stab_G(x) := \{g \in G | g \star x = x\},$$

chamado de estabilizador de x em G. Este é um subgrupo de G.

(c) A ação é transitiva se todos os elementos de X podem ser movidos, isto é, se para dois elementos $x, y \in X$ existe um elemento $g \in G$ onde $g \star x = y$.

(d) Dado $g \in G$, $x \in X$ é chamado de um ponto fixo de g se $g \star x = x$. Se $g \star x = x$, $\forall\ g \in G$ então x é chamado de ponto fixo da ação.

O próximo teorema mostra a relação entre a órbita e o estabilizador de um elemento. Já definida a ação do grupo finito G no conjunto X, temos:

Teorema 1.12. *([2], Capítulo VI, Teorema VI.1.4)(Órbita - Estabilizador) Seja $x \in X$ então*

$$| Orb_G(x) | = [G : Stab_G(x)] \text{ e assim, } |Orb_G(x)| \text{ divide } |G|.$$

Proposição 1.13. *([7], Capítulo 26, Proposição 26.6) Suponha que o grupo finito G age transitivamente em um conjunto finito X.*

(a) $|X|$ divide $|G|$.

(b) Se $N \lhd G$ é um subgrupo normal de G então todas as órbitas sob a ação de N tem a mesma cardinalidade. Daí o tamanho de uma N-órbita é um divisor de $|X|$.

Finalizaremos nossa primeira seção com os Teoremas de Sylow. O resultado garante a existência de certos subgrupos em um grupo. Enunciamos os teoremas de forma resumida e omitimos a demonstração, solicitamos que o leitor consulte as referências [1], [2] e [3].

Teorema 1.14. *(Teorema de Sylow)Considere G um grupo finito de ordem*

$$|G| = p^{\alpha}m, \text{ onde } \alpha \geq 1 \text{ e } mdc(p, m) = 1.$$

(1) *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.***

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

Vamos denotar por $Syl_p(G)$ o conjunto de todos os $p-$subgrupos de Sylow de G. Temos que: $P \in Syl_p(G) \Leftrightarrow |P| = p^\alpha$. Além disso, vamos denotar: $|Syl(G)| = n_p$. Dado $P \in Syl_p(G)$, temos $Syl_p(G) = \{P \mid g \in G\}$ e, como consequência do Teorema 1.12, segue que $n_p = [G : N_G(P)]$.

(3) *Temos:*

$$i) n_p \mid m \quad e$$
$$ii) \underbrace{n_p \equiv 1 (mod\ p)}_{p \mid n_p - 1}.$$

(4) *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 $H \leq P$.*

1.2 Grupos Simétricos

Nesta seção trataremos algumas definições e resultados básicos dos grupos simétricos, S_n. Como ponto de partida, vamos apresentar algumas definições, teorema e proposições sobre o grupo das permutações.

Na definição 1.10, comentamos sobre o grupo $Sim(X)$, ele é chamado de *Grupo das Permutações de um conjunto.* Agora, para o conjunto $S = \{1, 2, \ldots, n\}$ denotaremos esse grupo por S_n, *grupo simétrico de grau n.* A ordem de S_n é exatamente $n!$.

Definição 1.15. *Uma permutação $\sigma \in S_n$ é um r-ciclo de S_n, $n \geq 2$, se existem $i_1, i_2, \ldots, i_r$ distintos elementos de $\{1, 2, \ldots, n\}$ tais que*

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

$$e\ \sigma(j) = j\ \forall j \in \{1, 2, \ldots, n\}\ \text{-}\ \{i_1, i_2, \ldots, i_r\}.$$

Usaremos a notação $\sigma = (i_1 i_2 \ldots i_r) \in S_n$. Definimos, também, os ciclos de comprimento 2 como transposições.

Exemplo 1.16. *Considere $S = \{1, 2\}$ então temos $S_2 = \{\sigma_1, \sigma_2\}$ onde $\sigma_1 = 1$ e $\sigma_2 = (12)$. S_2 é abeliano.*

Proposição 1.17. *([3], Capítulo VI, Exemplo 3) Os grupos S_n, $n \geq 3$, não são abelianos.*

Demonstração. Basta verificar que $\sigma = (12)$ e $\tau = (123)$ não comutam em S_n. Isto é,

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

□

Os próximos teoremas e definições são úteis para demonstrarmos diversas propriedades a cerca dos grupos simétricos. Os teoremas serão apenas enunciados. Todas as referências estão indicadas.

Definição 1.18. *Sejam $\sigma = (i_1, i_2, \ldots, i_r)$ e $\tau = (j_1, j_2, \ldots, j_s)$ dois ciclos de S_n. Dizemos que σ e τ são dois ciclos disjuntos se $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \emptyset$.*

Observação 1.19. *Se σ e τ são dois ciclos disjuntos de S_n então como permutações de S_n eles comutam entre si, ou seja, $\sigma\tau = \tau\sigma$.*

Teorema 1.20. *([3], Capítulo VI, Teorema 10) Toda permutação $1 \neq \alpha \in S_n$ pode ser escrita de modo único (a menos da ordem) como um produto de ciclos disjuntos.*

A maneira única para a escrita de uma permutação como produto de ciclos disjuntos, determinada pelo Teorema 1.20, caracteriza a estrutura cíclica da permutação.

O fato de podermos escrever de maneira única todo elemento do grupo S_n como um produto de ciclos disjuntos auxilia nos cálculos no grupo S_n.

Vemos, ainda, que todo ciclo é um produto de transposições:

$$(i_1 i_2 \ldots i_k) = (i_1 i_k) \ldots (i_1 i_3)(i_1 i_2).$$

Portanto, toda permutação é um produto de transposições.

Definição 1.21. *Uma permutação que pode ser expressa como um produto de um número par de transposições é chamada de permutação par. Uma permutação que pode ser expressa como um produto de um número de ímpar de transposições é chamada de permutação ímpar.*

O conjunto A_n das permutações pares de S_n forma um subgrupo chamado subgrupo alternado de S_n. Tal grupo tem ordem $n!/2$ e é um subgrupo normal em S_n.

Definição 1.22. *Se σ e τ são suas permutações em S_n tais que:*

$$\sigma = (i_1 \ldots i_r) \ldots (j_1 \ldots j_s) \ldots (l_1 \ldots l_k) \text{ e } \tau = (i'_1 \ldots i'_r) \ldots (j'_1 \ldots j'_s) \ldots (l'_1 \ldots l'_k)$$

onde os ciclos em σ, e também em τ, são disjuntos. Dizemos que σ e τ possuem a mesma estrutura de ciclos.

Teorema 1.23. *([3], Capítulo VI, Proposição 13) Sejam σ e $\tau \in S_n$. Então σ e τ são conjugados em S_n se, e somente se, possuem a mesma estrutura de ciclos.*

Agora, apresentaremos dois teoremas referentes ao comprimento dos ciclos disjuntos, que compõem a estrutura cíclica de uma permutação, e a ordem desta permutação.

Teorema 1.24. *([1], Capítulo 5, Corolário) A ordem de uma permutação escrita na forma de ciclos disjuntos é o mínimo múltiplo comum dos comprimentos dos ciclos.*

Teorema 1.25. *([7], Capítulo 22, Proposição 22.4) Se n é um número primo, então os únicos elementos em S_n de ordem n são os n-ciclos.*

Seguem algumas informações sobre S_n e seu subgrupo alternado.

Teorema 1.26. *([3], Capítulo VI, Proposição 14 e Corolário 1)*
Os conjuntos $\{(12), (13), \ldots, (1n)\}$ e $\{(12), (12\ldots n)\}$ geram o grupo S_n.

Demonstração. Basta mostrar que toda transposição (ij) pertence a $\langle (12), (13), \ldots, (1n)\rangle$. Note que:

$$(ij) = (1i)(1j)(1i).$$

Se $1, i, j$ são distintos. E a primeira parte do resultado está provada. Para a segunda parte, seja $\tau = (12)$, $\sigma = (12\ldots n)$ e $G = \langle \tau, \sigma\rangle$, o grupo gerado por τ e σ. Logo, usando a conjugação temos que:

$$\begin{aligned}
\sigma^{-1}\tau\sigma &= (23)\\
\sigma^{-2}\tau\sigma^{2} &= (34)\\
\sigma^{-3}\tau\sigma^{3} &= (45)\\
&\vdots\\
\sigma^{-i}\tau\sigma^{i} &= (i+1\, i+2) \quad \forall i \in \{1, 2, \ldots, n-2\}
\end{aligned}$$

pertencem a G. Então G contém as transposições:

$$(12)(23)(12) = (23), (13)(34)(13) = (14), \ldots, (1\ n-1)(n-1\ n)(1\ n-1) = (1\ n).$$

Pela primeira parte do resultado temos que $G = S_n$. Portanto, o conjunto $\{(12), (12\ldots n)\}$ gera o grupo S_n. □

Teorema 1.27. *([3], Capítulo VI) 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 $\langle\{3-ciclos\}\rangle \subseteq G$. 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 1.23, 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 que o subgrupo alternado de S_n é simples, para $n \geq 5$.

Teorema 1.28. *([3], Capítulo VI) 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. Sendo assim, considerando o Teorema de Cauchy, seja p um primo que divide $|\ H\ |$ e tome $\sigma \in H$, tal que $|\ \sigma\ | = p$. Defina: $\sigma = (i_1\ i_2\ \cdots\ i_p)$ e escrevendo σ como um produto de ciclos disjuntos temos: $\sigma = (i_1\ i_2\ \cdots\ i_p) = \tau_1\tau_2\cdots\tau_m$. Pelo Teorema 1.24 segue que o $m.m.c$ dos ciclos disjuntos $\tau_j,\ j = 1, \cdots, m$ é p. E 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:

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

(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 $H \triangleleft A_n$, 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 1.23, 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:

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

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 à 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 à H, pois assim o resultado estará provado. De fato, note primeiramente que:

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

Além disso,

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

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 à H, como queríamos.
Neste ponto, nossa demonstração se reduz ao teorema anterior. Uma vez que H possui um 3-ciclo, ele possui todos os outros por conjugação. Portanto $H = A_n,\ n \geq 5$ e temos, finalmente, que A_n é simples. □

Os próximos resultados discutem sobre os subgrupos normais dos grupos: A_4, S_4 e S_n, para $n = 3$ ou $n \geq 5$. Tais resultados são necessários para demonstrarmos importantes proposições e teoremas que serão apresentados no capítulos subsequentes.

Proposição 1.29. *([2], Capítulo V, Teorema V.10.22) Os únicos subgrupos normais de A_4 são $\{1\}$, A_4 e K_4, sendo K_4:=$\{1,\ (12)(34),\ (13)(24),(14)(23)\}$ o Grupo de Klein.*

Demonstração. Escrevendo os elementos de A_4, observamos que seus elementos não triviais são 3-ciclos ou um produto disjunto de duas transposições. Suponha que H seja um subgrupo normal não trivial de A_4. Se este subgrupo normal H contém um 3-ciclo então, pelo Teorema 1.23, H contém todos os 3-ciclos. Em virtude do Teorema 1.27, A_4 é gerados pelos 3-ciclos logo $H = A_4$.

Por outro lado, se H não contém nenhum 3-ciclo, então ele contém um produto disjunto de duas transposições, digamos (12)(34). Logo, ele contém também (13)(24) pois segue que:

$$(13)(24) = (234)(12)(34)(234)^{-1}.$$

E também, (14)(23) pois temos:

$$(14)(23) = (12)(34)(13)(24).$$

Portanto, $H = K_4$. □

Proposição 1.30. *([2], Capítulo V, Corolário V. 10.23) Os únicos subgrupos normais de S_4 são $\{1\}$, A_4, S_4 e K_4, sendo K_4:=$\{1,\ (12)(34),\ (13)(24),(14)(23)\}$ o Grupo de Klein.*

Demonstração. Suponha que N é um subgrupo normal próprio e não trivial de S_4. Inicialmente, note que N não contém uma transposição, pois se existe uma

transposição $\tau \in N$, então, pelo Teorema 1.23, N contém todas as transposições. Consequentemente, $N = S_4$, pois, pelo Teorema 1.26, as transposições geram S_4.

Se N contém um 3-ciclo, logo N contém todos os 3-ciclos, pois eles são todos conjugados em S_4 e $N \lhd S_4$. Pelo Teorema 1.27, temos que A_n, para $n \geq 3$, é gerado pelos 3-ciclos então, $N = A_4$. Por outro lado, se N contém um 4-ciclo, a saber $(abcd)$, então ele contém seu conjugado $(bacd)$, e também o produto, isto é:

$$(bacd)(abcd) = (bdc) \in N.$$

Dessa forma, N contém um 3-ciclo e N também contém uma permutação ímpar. Diante disso, $N \neq A_4$ e assim $N = S_4$. Finalmente, se N não contém uma transposição, 3-ciclos ou 4-ciclos, mas ele contém um produto disjunto de duas transposições $(ab)(cd)$, então $N = K_4$. □

Proposição 1.31. *Os únicos subgrupos normais de S_n são $\{1\}$, A_n e S_n, para $n = 3$ ou $n \geq 5$.*

Demonstração. Sabemos que $\{1\} \lhd S_n$ e $S_n \lhd S_n$, pois $\{1\}$ e S_n são os subgrupos normais triviais de S_n. Note que $[S_n : A_n] = 2$, então $A_n \lhd S_n$.

Agora, seja N um subgrupo normal de S_n. Logo $A_n \cap N \lhd A_n$. Como A_n é simples, para $n \geq 5$, segue que $A_n \cap N = A_n$ ou $A_n \cap N = \{1\}$. Se $A_n \cap N = A_n$, então $N = A_n$ ou $N = S_n$. Por outro lado, se $A_n \cap N = \{1\}$ desejamos garantir que $N = \{1\}$.

Suponha, por absurdo, que existe $\tau \in N$ tal que $\tau \neq 1$. Como $\tau \notin A_n \cap N$, então τ é uma permutação ímpar. Mas $\tau^2 \in A_n$ e $\tau^2 \in N$ então $\tau \in A_n \cap N$, logo $\tau^2 = 1$. Temos que $N = \{1, \tau\}$. De fato, suponha que $\sigma \in N$, onde $\sigma \neq \tau$. Como $\sigma \notin A_n \cap N$ temos que σ é uma permutação ímpar. O produto $\sigma\tau$ é uma permutação par e, portanto, pertence a $A_n \cap N$ logo $\sigma\tau = 1$. Como $\tau \neq 1$ temos $\sigma = 1$.

Considerando a estrutura cíclica de τ, temos $\tau = \alpha_1\alpha_2 \ldots \alpha_k$, com cada α_i, sendo uma transposição pois τ tem ordem 2. Logo,

$$\tau = (i_1j_1)(i_2j_2) \ldots (i_kj_k).$$

Analisando as possibilidades para k, temos que para $k = 1$ segue que $\tau = (i_1j_1)$. Tomemos $j \in \{1, \ldots, n\}$ e $j \neq i_1, j_1$, como $N \lhd S_n$ então

$$\tau^{(i_1j_1)} = (i_1j_1)^{(i_1j)} = (jj_1) \neq \tau.$$

O que é um absurdo, pois contradiz N ser fechado por conjugação de elementos em S_n. Por outro lado, para k ímpares maiores que 2, tomamos a transposição

$(i_1 i_2) \neq \alpha_i$, sendo $\alpha_i' s$ as tranposições da estrutura cíclica de τ, observamos que

$$\tau^{(i_1 i_2)} = ((i_1 j_1)(i_2 j_2) \dots (i_k j_k))^{(i_1 i_2)} = (i_1 i_2)(i_2 i_1)(i_3 j_3) \dots (i_k j_k).$$

Logo, $\tau^{(i_1 i_2)}$ é um elemento em N diferente de τ. Novamente, um absurdo. Portanto, $N = \{1\}$, como queríamos. □

Para finalizar, notamos que o grupo S_n age sobre o conjunto $X = \{1, 2, \dots, n\}$. Esta ação é obviamente transitiva.

Um subgrupo H de S_n é transitivo se $\forall\ i, j \in \{1, 2, \dots, n\}$ existe $\sigma \in H$ tal que $\sigma(i) = j$. Note que K_4 é um subgrupo transitivo de S_4.

Capítulo 2

Grupos Solúveis

2.1 Solubilidade

Quando estudava o problema de resolver equações algébricas polinomiais, o famoso matemático Evariste Galois (1811-1832) desenvolveu o conceito de grupo solúvel, um dos conceitos mais antigos na teoria de gupos. Galois teve a brilhante ideia de associar a cada equação um grupo, e tal equação tem solução mediante radicais se, e somente se, o grupo associado é solúvel. Portanto, vamos introduzir e discutir o conceito e importantes resultados a respeito dos grupos solúveis.

Definição 2.1. *Um grupo G diz-se solúvel se existe uma série de subgrupos*

$$\{1\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_{n-1} \leq G_n = G$$

tais que $G_{i-1} \lhd G_i$ e $G_i\,/G_{i-1}$ é abeliano, $\forall\ i \in \{1, \ldots, n\}$. Uma série como esta é dita série abeliana de G.

O comprimento da menor série abeliana de um grupo solúvel G é definido como grau de solubilidade de G.

Exemplo 2.2. *Todo grupo abeliano G é solúvel. Para comprovarmos, basta considerar a seguinte série abeliana: $\{1\} \leq G$.*

Agora, vamos destacar alguns exemplos de grupos solúveis.

Exemplo 2.3. *O $\mathfrak{D}_4$, grupo de simetrias do quadrado, é solúvel.*

Sabemos que $\mathfrak{D}_4 = \{1, \theta, \theta^2, \theta^3, \mathfrak{r}, \mathfrak{r}\theta, \mathfrak{r}\theta^2, \mathfrak{r}\theta^3\} = \langle \mathfrak{r}, \theta \rangle$, onde $\mathfrak{r}^2 = \theta^4 = 1$ e $\mathfrak{r}\theta = \theta^{-1}\mathfrak{r}$. Para este grupo, podemos considerar a série abeliana abaixo:

$$\{1\} \leq \langle \theta^2 \rangle \leq \langle \theta \rangle \leq \mathfrak{D}_4.$$

Note que $|\langle\theta^2\rangle| = [\langle\theta\rangle : \langle\theta^2\rangle] = [\mathfrak{D}_4 : \langle\theta\rangle] = 2$. *Diante disso, a série acima é uma séria abeliana para o grupo* $\mathfrak{D}_4$.

Observação 2.4. *Uma pergunta surge naturalmente: A série abeliana, que caracteriza a solubilidade de um grupo, é única?*

A resposta para a questão é não. O nosso exemplo anterior é útil para justificar que é possível um grupo possuir mais de uma série abeliana. Assim, vamos apresentar mais uma série do $\mathfrak{D}_4$*:*

$$\{1\} \leq \langle \mathfrak{r}\theta^2\rangle \leq \langle \mathfrak{r}, \theta^2\rangle \leq \mathfrak{D}_4$$

onde, também, temos $|\langle\mathfrak{r}\theta^2\rangle| = [\langle\mathfrak{r}, \theta^2\rangle : \langle\mathfrak{r}\theta^2\rangle] = [\mathfrak{D}_4 : \langle\mathfrak{r}, \theta^2\rangle] = 2$.

Exemplo 2.5. *É imprescindível mencionar que os grupos* S_3 *e* S_4 *são solúveis.*

Pela Proposição 1.31, temos que $A_3 \lhd S_3$ *e sabemos que* A_3 *é abeliano. Assim, temos a seguinte série abeliana do* S_3*:*

$$\{1\} \leq A_3 \leq S_3.$$

Analogamente, para o S_4 *consideramos a série:*

$$\{1\} \leq K_4 \leq A_4 \leq S_4.$$

De acordo com as Proposições 1.29 e 1.30, temos que $A_4 \lhd S_4$ *e* $K_4 \lhd A_4$*. Analisando as ordens dos quocientes, segue que* S_4/A_4 *e* A_4/K_4 *são abelianos. No decorrer do nosso trabalho, vamos concluir que dentre os simétricos* S_3 *e* S_4 *são os únicos solúveis.*

Uma definição muito importante no estudo dos grupos solúveis é a definição do comutador de dois elementos de um grupo G. Além disso, vamos definir o comutador de dois subgrupos de G.

Definição 2.6. *Seja* G *um grupo. Dados* $x, y \in G$*, definimos o comutador de* x *e* y *como elemento* $xyx^{-1}y^{-1} \in G$ *e será denotado por* $[x, y]$.

Definição 2.7. *O comutador de dois subgrupos* $X, Y \leq G$ *é definido como o subgrupo de* G *gerado por todos os comutadores* $[x, y]$ *onde* $x \in X$ *e* $y \in Y$*, isto é,*

$$[X, Y] =: \langle xyx^{-1}y^{-1} | x \in X, y \in Y\rangle.$$

Um caso especial de comutador de dois subgrupos é o subgrupo comutador $G' = [G, G]$ de um grupo G. Ou seja,

$$G' := \langle xyx^{-1}y^{-1} | x, y \in G \rangle.$$

O grupo G' é denominado *subgrupo derivado de* G. Agora, definimos que $G^{(0)} = G$ e $G^{(i+1)} = [\, G^{(i)} \,, G^{(i)}]$, sendo assim $G^{(i+1)}$ é o subgrupo derivado do grupo $G^{(i)}$, $\forall\ i \in \mathbb{N}$. Além disso, destacamos que o subgrupo $G^{(i)}$ é chamado o i-ésimo grupo derivado de G e a sequência

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(n)} \supseteq \ldots$$

é chamada de *série derivada de* G.

Veremos abaixo algumas propriedades do subgrupo derivado de um grupo G.

Proposição 2.8. *Valem as seguintes afirmações sobre o subgrupo derivado de* G*:*

(1) G *é abeliano* $\iff$ $G' = \{1\}$.

(2) $G' \lhd G$.

(3) G/G' *é abeliano.*

(4) Se $N \lhd G$ *e* G/N *é abeliano* $\Longrightarrow$ $G' \subseteq N$.

(5) Se $H \leq G$ *e* $G' \leq H \Longrightarrow H \lhd G$.

Demonstração. (1)

$$\begin{aligned} G \quad \textit{abeliano} &\iff xy = yx, \quad \forall \quad x, y \in G \\ &\iff xyx^{-1}y^{-1} = 1, \quad \forall \quad x, y \in G \\ &\iff [x, y] = 1, \quad \forall \quad x, y \in G \\ &\iff G' = 1. \end{aligned}$$

(2) Vamos mostrar que $G' \lhd G$. Assim, desejamos verificar que para $a \in G'$ e $\forall g \in G$ temos $a^g = gag^{-1} \in G'$. Como $a \in G'$, segue que

$$a = [x_{i1}, y_{i1}]^{\alpha_{i1}} \ldots [x_{is}, y_{is}]^{\alpha_{is}}.$$

Seja $g \in G$, então

$$\begin{aligned} a^g &= ([x_{i1}, y_{i1}]^{\alpha_{i1}} \dots [x_{is}, y_{is}]^{\alpha_{is}})^g = ([x_{i1}, y_{i1}]^{\alpha_{i1}})^g \dots ([x_{is}, y_{is}]^{\alpha_{is}})^g \\ &= ([x_{i1}, y_{i1}]^g)^{\alpha_{i1}} \dots ([x_{is}, y_{is}]^g)^{\alpha_{is}}. \end{aligned}$$

Desde que

$$\begin{aligned} [x, y]^g &= gxyx^{-1}y^{-1}g^{-1} \\ &= gx\underbrace{g^{-1}g}y\underbrace{g^{-1}g}x\underbrace{g^{-1}g}y^{-1}g^{-1} \\ &= x^g y^g (x^{-1})^g (y^{-1})^g \\ &= x^g y^g (x^g)^{-1} (y^g)^{-1} = [x^g, y^g]. \end{aligned}$$

Temos

$$a^g = ([x_{i1}^g, y_{i1}^g])^{\alpha_{i1}} \dots ([x_{is}^g, y_{is}^g])^{\alpha_{is}} \in G'.$$

(3) Sejam $x, y \in G$, então

$$\begin{aligned} [x, y] \in G &\Longrightarrow xyx^{-1}y^{-1} \in G' \Longrightarrow G'xyx^{-1}y^{-1} = G' \\ &\Longrightarrow G'xy = G'yx \Longrightarrow G'xG'y = G'yG'x. \end{aligned}$$

Portanto, G/G' é abeliano.

(4) Sejam $x, y \in G$. Logo $Nx, Ny \in G/N$. Como G/N é abeliano temos que

$$\begin{aligned} NxNy = NyNx &\Longrightarrow Nxy = Nyx \\ &\Longrightarrow xyx^{-1}y^{-1} \in N \Longrightarrow G' \subseteq N. \end{aligned}$$

(5) Sejam $h \in$ H e $g \in G$. Então

$$h^g = ghg^{-1} = (ghg^{-1})h^{-1}h = [g, h]h \in H, \quad pois \quad [g, h] \in G' \leq H.$$

Logo $H \lhd G$.

□

Já que estamos interessados em discutir os subgrupos solúveis em grupos simétricos e o estudo do subgupo derivado de um dado grupo é útil para o desenvolvimento do nosso trabalho, vamos verificar o subgrupo derivado dos grupos simétricos.

Proposição 2.9. *(a)* $S_n'=A_n$ *e* $A_n = A_n'$, *para* $n \geq 5$.

(b) $S_3'=A_3$ *e* $A_3' = \{1\}$.

(c) $S_4'=A_4$, $A_4' = K_4$ *e* $K_4' = \{1\}$.

Demonstração. (a) O subgrupo dos comutadores S_n' é normal em S_n e, portanto, pela Proposição 2.8, segue que $S_n' = \{1\}$, A_n ou S_n. Como S_n não é abeliano, logo $S_n' \neq \{1\}$. Obseve que $A_n \lhd S_n$ e S_n/A_n é abeliano. Pela proposição anterior, temos $S_n' \subseteq A_n$, então $S_n' \neq S_n$. Portanto, $S_n' = A_n$.

Analogamente, A_n' é um subgrupo normal de A_n. Assim, $A_n' = A_n$ ou $\{1\}$, pelo Teorema 1.28. Como A_n, para $n \geq 5$, não é abeliano, temos $A_n' \neq \{1\}$, e, logo, $A_n' = A_n$.

(b) Em S_3 os subgrupos normais são $\{1\}$, A_3 e S_3. Como S_3 não é abeliano temos que $S_3' \neq \{1\}$. Por outro lado, $A_3 \lhd S_3$ e S_3/A_3 abeliano. De acordo com a Proposição 2.8, segue que $S_3' \subseteq A_3$, então $S_3' \neq S_3$. Sendo assim, $S_3' = A_3$.

Pelo Teorema 1.28, A_3 é simples e, assim, seus subgrupos normais são A_3 e $\{1\}$. Note que $|A_3| = 3$ e A_3 é abeliano, então$A_3' = \{1\}$, pela Proposição 2.8.

(c) Mostramos, na Proposição 1.30, que os únicos subgrupos normais de S_4 são $\{1\}$, K_4, A_4 , S_4 . Como S_4 não é abeliano, logo $S_4' \neq \{1\}$. Note que $A_4 \lhd S_4$ e S_4/A_4 é abeliano, da Proposição 2.8, segue que $S_4' \subseteq A_4$. Diante disso, $S_4' = A_4$ ou $S_4' = K_4$.

Afirmamos que $S_4' \neq K_4$. De fato, considere $(12), (123) \in S_4$ então:

$$\begin{aligned}[(12),(123)] =&(12)(123)(12)^{-1}(123)^{-1} = \\ =&(123)^{(12)}(132) = (213)(132) = (123) \notin K_4.\end{aligned}$$

Diante disso, $S_4' = A_4$.

Agora, pela Proposição 1.29, os subgrupos normais de A_4 são $\{1\}$, K_4 e A_4. Note que $A_4 \neq \{1\}$, uma vez que A_4 não é abeliano. Observe que $K_4 \lhd A_4$ e $|A_4/K_4| = 3$, logo o quociente A_4/K_4 é abeliano. De acordo com a Proposição 2.8, $A_4' \subseteq K_4$, então $A_4' \neq A_4$. Portanto, $A_4' = K_4$.

Como $|K_4| = 4 = 2^2$, temos que K_4 é abeliano. Pela Proposição 2.8, segue que $K_4' = \{1\}$.

□

Vamos mostrar uma caracterização de solubilidade em termos da série derivada e da série de composição de um grupo finito. Inicialmente, é necessário definir e discutir a série de composição de um grupo.

Definição 2.10. *Uma série subnormal de G é uma cadeia de subgrupos*

$$\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G \ (\star)$$

onde $G_{i-1} \lhd G_i \ \forall \ i = 1,\ldots,n$.

Observação 2.11. *(1) Os grupos quocientes da série subnormal são os grupos G_i/G_{i-1} para $i = 1, ..., n$.*

(2) O comprimento da série subnormal é o número de inclusões estritas ou, equivalentemente, o número de grupos quocientes não-triviais.

(3) O refinamento de uma série subnormal é obtido a partir da inserção de alguns, possivelmente nenhum, subgrupos em uma dada série como em $(\star)$. O refinamento é chamado próprio se algum subgrupo distinto dos já existentes é inserido na série.

(4) Chamamos a série subnormal de série de composição se ela não admite um refinamento próprio.

Proposição 2.12. *Todo grupo finito $G \neq \{1\}$ admite uma série de composição.*

Para demonstrar a proposição desejada vamos considerar a seguinte afirmação:

Afirmação. Existe um subgrupo G_1 de G que satisfaz a propriedade $G_1 \subsetneqq G$ e $G_1 \lhd G$, G_1 é maximal para a propriedade, ou seja, se existe H tal que $G_1 \subseteq H \subsetneqq G$ e $H \lhd G$, então $G_1 = H$.

Demonstração. (da Afirmação) Temos $\{1\} \subsetneqq G$ e $\{1\} \lhd G$. Se $\{1\}$ é maximal para esta propriedade, podemos tomar $G_1 = \{1\}$. Caso contrário, por definição, existe um subgrupo H tal que $\{1\} \subseteq H$ que satisfaz $H \subseteq G$ e $H \lhd G$. Caso H seja maximal, para esta propriedade, podemos tomar $G_1 = H$. Caso contrário, por definição, existe um subgrupo H_1 tal que $H \subseteq H_1$ que satisfaz $H_1 \subseteq G$ e $H_1 \lhd G$. Caso H seja maximal para esta propriedade, podemos tomar $G_1 = H_1$. Caso contrário, continuamos o processo. Observamos que o processo é finito, pois obtemos subgrupos H, H_1, $H_2, \ldots$ cada vez maiores e G é um grupo finito. □

Agora, estamos aptos para demosntrar a Proposição 2.12.

Demonstração. (da Proposição 2.12) De acordo com a Afirmação provada acima, existe um grupo G_1 de G que satisfaz $G_1 \subsetneqq G$ e $G_1 \lhd G$, onde G_1 é maximal com essas características. Se $G_1 = \{1\}$, então $\{1\} = G_1 \lhd G$ é a série de composição. Se $G_1 \neq \{1\}$, aplicamos a afirmação no grupo G_1 e obtemos um subgrupo G_2 de G_1 que satisfaz $G_2 \subsetneqq G_1$ e $G_2 \lhd G_1$, onde G_2 é maximal para esta propriedade. Se $G_2 = \{1\}$, então $\{1\} = G_2 \lhd G_1 \lhd G$ é a série de composição. Se $G_2 \neq \{1\}$, continua-se o processo, aplicando a afirmação no grupo G_2. O processo termina, pois obtemos subgrupos G_1, G_2, G_3, ... cada vez menores e o grupo G é finito. □

2.2 Caracterização de Solubilidade

Neste momento, vamos demonstrar uma caracterização de solubilidade. Ela é muito útil para verificar alguns resultados sobre os grupos solúveis finitos.

Teorema 2.13. *(Caracterização de Solubilidade). Seja G um grupo finito. As seguintes condições são equivalentes:*

(1) O grupo G é solúvel.

(2) Existe um natural n tal que $G^{(n)} = \{1\}$.

(3) O grupo G possui uma série de composição cujos grupos quocientes são abelianos (e, portanto, são cíclicos de ordem prima).

Demonstração. Inicialmente, vamos verificar que *(1)* $\Longrightarrow$ *(2)*.

Se G solúvel, então existe uma série subnormal com $G_i \,/G_{i-1}$ abeliano, $\forall\ i \in \{1, \ldots, n\}$, isto é,

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_{n-1} \lhd G_n = G.$$

Como G_n/G_{n-1} é abeliano, segue que $G^{(1)} = (G_n)' \subseteq G_{n-1}$, da Proposição 2.8 parte (4). Analogamente, se $G_{n-1} \,/G_{n-2}$ é abeliano temos que

$$G^{(2)} = ((G_n)')' \subseteq (G_{n-1})' \subseteq G_{n-2}.$$

Continuando, obtemos $G^{(i)} \subseteq G_{n-i}$, $\forall\ i \in \{1, \ldots, n\}$. Em particular, temos $G^{(n)} \subseteq G_0 = \{1\}$, e, logo $G^{(n)} = \{1\}$.

Agora, vamos demonstrar que *(2)* $\Longrightarrow$ *(1)*. Considere a série derivada de G

$$\{1\} = G^{(n)} \lhd G^{(n-1)} \lhd G^{(n-2)} \lhd \ldots \lhd G^{(1)} \lhd G^{(0)} = G \quad (\star\star).$$

Como $G^{(i+1)} = [G^{(i)}\ ,\ G^{(i)}\ ]$, temos que $G^{(i+1)} \lhd G^{(i)}$ e o $G^{(i)}/G^{(i+1)}$ é abeliano $\forall\ i = 0, \ldots, n-1$, pela Proposição 2.8, parte (2) e (3). Portanto, a série em $(\star\ \star)$ é subnormal e satisfaz as condições da definição 2.1. Diante disso, G é solúvel.

A implicação *(3)* $\Longrightarrow$ *(1)* é trivial. Por fim, vamos comprovar que *(1)* $\Longrightarrow$ *(3)*. Se G solúvel, então existe

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_{n-1} \lhd G_n = G$$

uma série subnormal com G_i/G_{i-1} abeliano, $\forall\ i \in \{1, \ldots, n\}$. Como G é um grupo finito, então cada quociente G_i/G_{i-1} é um grupo abeliano também finito. Logo, pela Proposição 2.12, podemos obter uma série de composição deste grupo quociente, isto é, uma série de subgrupos entre G_i e G_{i-1} tal que cada grupo quociente desta série é cíclico de ordem prima. Assim, podemos considerar:

$$G_{i-1} = G_{i_0} \lhd G_{i_1} \lhd \ldots \lhd G_{i_{s-1}} \lhd G_{i_s} = G_i$$

onde cada G_i/G_{i-1} é cíclico de ordem prima. Aplicando a Proposição 2.12, para todo índice $i = 1, \ldots, n$, obtemos

$$\begin{aligned}\{1\} = G_0 \lhd G_1 =& G_{2_0} \lhd G_{2_1} \lhd \ldots \lhd G_{2_{s_n-1}} \lhd G_{2_{s_n}} \lhd \ldots \lhd G_{n-1} \\ =& G_{n_0} \lhd G_{n_1} \lhd \ldots \lhd G_{n_{s_1-1}} \lhd G_{n_{s_1}} = G_n = G\end{aligned}$$

ou seja, temos uma série de composição de G cujos grupos quocientes são cíclicos de ordem prima. □

Apresentaremos importantes propriedades dos grupos solúveis. Elas mostram que a imagem homomórfica de grupo solúvel é solúvel, subgrupos de grupos solúveis são solúveis e que o produto direto de grupos solúveis é ainda solúvel.

Teorema 2.14. *Seja G um grupo finito e $H \leq G$. Se G é solúvel, então H é solúvel.*

Demonstração. Sejam $x, y \in H \leq G$. Então $[x, y]$ é um comutador de elementos de G. Sendo assim, temos

$$[x, y] \in G^{(1)},\ \forall\ x, y \in H.$$

Portanto, $H^{(1)} \subseteq G^{(1)}$. Com o mesmo raciocínio e por indução, segue que

$$H \leq G \Longrightarrow H^{(i)} \subseteq G^{(i)},\ \forall\ i = 1, \ldots, n.$$

Agora, se G é solúvel, então existe n tal que $G^{(n)} = \{1\}$, pelo Teorema 2.13. Logo $H^{(n)} \subseteq G^{(n)} = \{1\}$. Portanto, $H^{(n)} = \{1\}$, então H é solúvel. □

Exemplo 2.15. *S_n não é solúvel, para $n \geq 5$.*

De acordo com a Proposição 2.9, temos que $A_n' = A_n$. Consequentemente, $A_n = A_n^{(k)}$ $\forall$ $k \in \mathbb{N}$. Pelo Teorema 2.13, segue que A_n não é solúvel. Assim, basta observar que $A_n \leq S_n$, então S_n não é solúvel.

O próximo teorema garante que a imagem homomórfica de um grupo solúvel é solúvel.

Teorema 2.16. *Seja G um grupo finito. Se $\varphi : G \longrightarrow H$ é um homomorfismo e G é solúvel, então $\varphi(G)$ é solúvel.*

Para demonstrar o teorema acima, vamos mostrar o seguinte lema:

Lema 2.17. *1. Seja G um grupo finito. Se $\varphi : G \longrightarrow H$ é um homomorfismo, então $\varphi(G^{(k)}) \subset (\varphi(G))^{(k)}$, $\forall$ $k \geq 1$.*

2. Seja G um grupo finito. Se $\varphi : G \longrightarrow H$ é um homomorfismo sobrejetivo, então $\varphi(G^{(k)}) = (H)^{(k)}$, $\forall$ $k \geq 1$.

Demonstração. 1. A demonstração da inclusão é por indução sobre k. Sendo assim, vamos considerar $k = 1$ e provar que $\varphi(G^{(1)}) \subset (\varphi(G))^{(1)}$. Sejam $x, y \in G$, então $[x, y] \in G^{(1)}$. Assim,

$$\varphi([x,y]) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = [\varphi(x), \varphi(y)] \in (\varphi(G))^{(1)}.$$

Diante disso, $\varphi(G^{(1)}) \subset (\varphi(G))^{(1)}$ e o resultado é válido. Agora, vamos supor $k = n$. Então, pela hipótese de indução, $\varphi(G^{(n)}) \subset (\varphi(G))^{(n)}$. Sejam $[x, y] \in G^{(n+1)}$ tais que $x, y \in G^{(n)}$, logo

$$\varphi([x,y]) = [\varphi(x), \varphi(y)] \in (\varphi(G))^{(n+1)}$$

pois $\varphi(x), \varphi(y) \in (\varphi(G))^{(n)}$. Portanto, $\varphi(G^{(k)}) \subset (\varphi(G))^{(k)}$, $\forall$ $k \geq 1$.

2. A demonstração também é por indução. Inicialmente, considere $k = 1$, vamos provar que $\varphi(G^{(1)}) = H^{(1)}$. Sejam $a, b \in H$. Como φ é um homorfismo sobrejetivo, existem $x, y \in G$ tais que $\varphi(x) = a$ e $\varphi(y) = b$. Assim, $[a, b] = [\varphi(x), \varphi(y)]$. Verificamos, no item anterior, que $[\varphi(x), \varphi(y)] = \varphi([x, y])$. Então,

$$[a,b] = [\varphi(x), \varphi(y)] = \varphi([x,y]) \in \varphi(G^{(1)}).$$

Logo, $[a, b] \in \varphi(G^{(1)})$, $\forall$ $a, b \in \varphi(G)$. Sendo assim, $H^{(1)} \subset \varphi(G^{(1)})$. De acordo com o item anterior, temos que $\varphi(G^{(1)}) \subset H^{(1)}$. Concluimos que $\varphi(G^{(1)}) = H^{(1)}$, quando φ é um homomorfismo sobrejetivo.

Agora, suponhamos $k = n$. Pela hipótese de indução, temos que $\varphi(G^{(n)}) = H^{(n)}$ e vamos provar que $\varphi(G^{(n+1)}) = H^{(n+1)}$. Como φ é sobrejetivo e $\varphi(G^{(n)}) = H^{(n)}$, podemos considerar o homomorfismo sobrejetivo $G^{(n)} \longrightarrow H^{(n)}$. Diante disso, podemos repetir o raciocínio utilizado no caso $k = 1$ e temos que $(\varphi(G^{(n)}))^{(1)} = (H^{(n)})^{(1)}$. De acordo com a definição, $(H^{(n)})^{(1)} = [H^{(n)}, H^{(n)}] = H^{(n+1)}$. Além disso, devemos observe que

$$(\varphi(G^{(n)}))^{(1)} = [\varphi(G^{(n)}), \varphi(G^{(n)})] = \varphi([G^{(n)}, G^{(n)}]) = \varphi(G^{(n+1)}).$$

Sendo assim, de $(\varphi(G^{(n)}))^{(1)} = (H^{(n)})^{(1)}$ verificamos que $\varphi(G^{(n+1)}) = H^{(n+1)}$. Desta maneira, completamos a demonstração e segue o resultado desejado.

□

Agora, estamos prontos para demonstrar o teorema almejado.

Demonstração. Como G é solúvel, pelo Teorema 2.13, segue que existe n tal que $G^{(n)} = \{1\}$. Claramente, $G \longrightarrow \varphi(G)$ é um homomorfismo sobrejetivo. Pelo item (2) do lema anterior, segue que $\varphi(G^{(n)}) = (\varphi(G))^{(n)}$. Assim, temos que

$$\varphi(G^{(n)}) = (\varphi(G))^{(n)} \Longrightarrow \varphi(\{1\}) = (\varphi(G))^{(n)} \Longrightarrow 1 = (\varphi(G))^{(n)}.$$

Logo $\varphi(G)$ é solúvel.

□

Teorema 2.18. *O produto direto de grupos finitos é solúvel se, e somente se, todos os seus fatores são solúveis.*

Novamente, para demonstrar o teorema vamos enunciar e demonstrar um lema. Portanto, temos:

Lema 2.19. *Se $G = \prod_{i=1}^{m} G_i$ é um produto direto de grupos $G_i's$, então*

$$G^{(k)} = \prod_{i=1}^{m} G_i^{(k)}, \ \forall \ k \geq 1.$$

Demonstração. A demonstração do lema é por indução sobre k. Suponha $k = 1$. Vamos mostrar a inclusão $G^{(1)} \subset \prod_{i=1}^{m} G_i^{(1)}$. Sejam $x, y \in G$, então $x = (x_1, \ldots, x_m)$

e $y = (y_1, \ldots, y_m)$, onde $x_i, y_i \in G_i$, $\forall\ i = 1, \ldots, m$. Assim,

$$\begin{aligned}
[x, y] &= [(x_1, \ldots, x_m), (y_1, \ldots, y_m)] \\
&= (x_1, \ldots, x_m)^{-1}(y_1, \ldots, y_m)^{-1}(x_1, \ldots, x_m)(y_1, \ldots, y_m) \\
&= (x_1^{-1}, \ldots, x_m^{-1})(y_1^{-1}, \ldots, y_m^{-1})(x_1, \ldots, x_m)(y_1, \ldots, y_m) \\
&= (x_1^{-1}y_1^{-1}x_1y_1, \ldots, x_m^{-1}y_m^{-1}x_my_m) \\
&= ([x_1, y_1], \ldots, [x_m, y_m]) \\
&= ([x_1, y_1], 1_{G_2}, \ldots, 1_{G_m}) \ldots (1_{G_1}, 1_{G_2}, \ldots, [x_m, y_m]).
\end{aligned}$$

Diante disso, cada comutador em $G = \prod_{i=1}^{m} G_i$ é o produto direto de um comutador em G_1, em G_2, ..., em G_m. Portanto, $G^{(1)} \subset \prod_{i=1}^{m} G_i^{(1)}$. Agora, vamos mostrar a inclusão contrária, isto é, $\prod_{i=1}^{m} G_i^{(1)} \subset G^{(1)}$. Seja $(g_1, g_2, \ldots, g_m) \in \prod_{i=1}^{m} G_i^{(1)}$, então $g_1 = [x_1, y_1] \in G_1^{(1)}$, $g_2 = [x_2, y_2] \in G_2^{(1)}$, ..., $g_m = [x_m, y_m] \in G_m^{(1)}$. Sendo assim,

$$\begin{aligned}
(g_1, g_2, \ldots, g_m) &= ([x_1, y_1], [x_2, y_2], \ldots, [x_m, y_m]) \\
&= (x_1^{-1}y_1^{-1}x_1y_1, x_2^{-1}y_2^{-1}x_2y_2, \ldots, x_m^{-1}y_m^{-1}x_my_m) \\
&= (x_1^{-1}, x_2^{-1}, \ldots, x_1^{-1})(y_1^{-1}, y_2^{-1}, \ldots, y_1^{-1})(x_1, x_2, \ldots, x_1)(y_1, y_2, \ldots, y_1) \\
&= (x_1, x_2, \ldots, x_1)^{-1}(y_1, y_2, \ldots, y_1)^{-1}(x_1, x_2, \ldots, x_1)(y_1, y_2, \ldots, y_1) \\
&= [(x_1, \ldots, x_m), (y_1, \ldots, y_m)].
\end{aligned}$$

Observe que $(x_1, \ldots, x_m), (y_1, \ldots, y_m) \in G = \prod_{i=1}^{m} G_i$. Além disso, é possível notar que o produto direto de um comutador em G_1, com um comutador em G_2 e, assim sucessivamente, até G_m é um comutador em $\prod_{i=1}^{m} G_i$. Então, $G^{(1)} \subset \prod_{i=1}^{m} G_i^{(1)}$. Como esperávamos, $G^{(1)} = \prod_{i=1}^{m} G_i^{(1)}$.

Agora, suponhamos que o resultado é válido para algum $n > 1$, isto é, $G^{(n)} = \prod_{i=1}^{m} G_i^{(n)}$. Inicialmente, vamos verificar que $G^{(n+1)} \subset \prod_{i=1}^{m} G_i^{(n+1)}$. Sejam $x, y \in G^{(n)}$, tais que $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_m)$. Por hipótese de indução, temos que $x_1, y_1 \in G_1^{(n)}$, $x_2, y_2 \in G_2^{(n)}$, ..., $x_m, y_m \in G_m^{(n)}$. Assim,

$$\begin{aligned}
[x, y] &= [(x_1, \ldots, x_m], (x_m, \ldots, y_m)] \\
&= ([x_1, y_1], \ldots, [x_m, y_m]) \in \prod_{i=1}^{m} G_i^{(n+1)}.
\end{aligned}$$

Portanto, $G^{(n+1)} \subset \prod_{i=1}^{m} G_i^{(n+1)}$. Para finalizar a demonstração do lema, resta verificar que $\prod_{i=1}^{m} G_i^{(n+1)} \subset G^{(n+1)}$. Sejam $(g_1, \ldots, g_m) \in \prod_{i=1}^{m} G_i^{(n+1)}$, logo $g_i \in G_i^{(n+1)}$, onde $g_i = [x_i, y_i]$ com $x_i, y_i \in G_i^{(n)}$, $\forall\ i = 1, \ldots, m$. Por hipótese de indução, $G^{(n)}$=$\prod_{i=1}^{m} G_i^{(n)}$, então

$$(g_1, \ldots, g_m) = [(x_1, \ldots, x_m), \ldots, (y_1, \ldots, y_m)] \in \prod_{i=1}^{m} G_i^{(n+1)}.$$

Dessa maneira, concluímos que $G^{(k)} = \prod_{i=1}^{m} G_i^{(k)}$, $\forall\ k \geq 1$. □

Neste momento, estamos prontos para provar o Teorema 2.18.

Demonstração. Se G é solúvel, então existe n tal que $G^{(n)} = \{1\}$. Pelo Lema 2.19, temos que

$$\{1\} = G^{(n)} = \prod_{i=1}^{m} G_i^{(n)}.$$

Então, $G_i^{(n)} = \{1\}$ $\forall\ i$. Assim, G_i é solúvel $\forall\ i$, como queríamos.

Por outro lado, se G_i é solúvel $\forall\ i = 1, \ldots, m$, então existem $n_1, n_2, \ldots, n_m$ tais que

$$G_1^{(n_1)} = \{1\}, G_2^{(n_2)} = \{1\}, \ldots, G_m^{(n_m)} = \{1\}.$$

Seja $n = \text{máx}\{n_1, n_2, \ldots, n_m\}$. Logo, pelo Lema 2.19 temos que

$$\{1\} = \prod_{i=i}^{m} G_i^{(n)} = G^{(n)}.$$

Então, G é solúvel. □

Vamos apresentar mais um importante critério de solubilidade.

Teorema 2.20. *Seja $N \trianglelefteq G$. Então G é solúvel se, e somente se, N e G/N são solúveis.*

Demonstração. Suponha G solúvel e seja n tal que $G^{(n)} = \{1\}$. Seja

$$\pi : G \longrightarrow G/N \text{ o homomorfismo canônico.}$$

Note que se $N \leq G$ e G é solúvel, então N é solúvel, pelo Teorema 2.14. Sendo assim, $N^{(n)} \subseteq G^{(n)} = \{1\}$, logo $N^{(n)} = \{1\}$.

Pelo Lema 2.17, $(G/N)^{(n)} = \pi(G^{(n)})$. Como G é solúvel, temos

$$(G/N)^{(n)} = \pi(G^{(n)}) = \pi(\{1\}) = \{1\}.$$

Portanto, N e G/N são solúveis.

Agora, suponha N e G/N solúveis e sejam n e m naturais, tais que $N^{(n)} = \{1\}$ e $(G/N)^{(m)} = \{1\}$. Note que se$\{1\} = (G/N)^{(m)} = \pi(G^{(n)})$, então $G^{(n)} \subseteq Ker(\pi) = N$. Assim, se $G^{(n+m)} = (G^{(m)})^{(n)} \subseteq N^{(n)} = \{1\}$, então G é solúvel. □

2.3 Relação entre Ordem e Solubilidade de um Grupo

Nesta seção, vamos discutir resultados que mostram que a ordem de um grupo pode implicar sua solubilidade.

Proposição 2.21. *Todo p-grupo finito é solúvel.*

Demonstração. Seja G um p-grupo tal que $|G| = p^m$, $m \geq 1$. Vamos provar o resultado por indução sobre m. Se $m = 1$, se |G| $= p$, então G é abeliano, e, logo, solúvel. Agora, vamos considerar $m > 1$ e o resultado válido para um p-grupo J, tal que $|J| = p^k$, $m > k$.

No caso G abeliano, temos G solúvel. Já para G não abeliano, temos que $Z(G) \neq G$ e $Z(G) \neq 1$. Além disso, sabemos que $Z(G)$ é abeliano e $Z(G) \lhd G$, e, assim, podemos considerar $G/Z(G)$. Note que tais subgrupos são p-grupos cujas ordens são menores que p^m. Portanto, pela nossa hipótese de indução, ambos são solúveis. Assim, pelo Teorema 2.20, temos que G é solúvel. □

Proposição 2.22. *Sejam p, q primos.Todo grupo de ordem pq é solúvel.*

Demonstração. Seja G um grupo, tal que $|G| = pq$. Se $p = q$, então $|G| = p^2$ e G é um p-grupo. Pela Proposição 2.21, segue G é solúvel e temos o resultado desejado.

Agora, considere $p \neq q$. Sem perda de generalidade, suponha $p < q$. Como q é primo, temos que existe $1 \neq x \in G$ tal que $\mathcal{O}(x) = q$, pelo Teorema de Cauchy. Considere $H = \langle x \rangle$ e como $|H| = q$, então H é cíclico. Logo, H é abeliano e, portanto, solúvel.

Observe que $[G : H] = p$, então $H \trianglelefteq G$, pela Proposição 1.2. Considrere o grupo quociente de G por H, note que $|G/H| = p$, então G/H é solúvel. Como $H \trianglelefteq G$, temos H e G/H solúveis, segue que G é solúvel, de acordo com o Teorema 2.20. □

Proposição 2.23. *Sejam p, q primo. Todo grupo de ordem $p^m q$ é solúvel.*

Demonstração. Se $p = q$, então G é solúvel, pois, neste caso, ele é um p-grupo finito. Agora, vamos considerar $p \neq q$. Suponhamos, por absurdo, que G não é solúvel. Vamos considerar $|G| = p^m q$ minimal para essa característica do grupo.

Neste caso, afirmamos que G é um grupo simples. De fato, se G não é simples, considere N um subgrupo próprio, normal e não trivial de G. Como todo grupo com a ordem menor que G é solúvel, pela minimalidade definida, temos que N e G/N são solúveis. De acordo com o Teorema 2.20, temos que G também é solúvel, o que é um absurdo.

Pelo Teorema de Sylow, temos que n_p, o número de p-subgrupos de Sylow de G, divide q então $n_p = 1$ ou $n_p = q$. Note que $n_p = q$, pois se $n_p = 1$ segue que existe um único subgrupo de G com p^m elementos e tal subgrupo é normal em G, contradizendo a simplicidade de G.

Sendo assim, existem q p- subgrupos de Sylow de G, tais que $|P_i| = p^m$, $\forall\ i = 1, \ldots, q$. Vamos supor que a interseção de quaisquer dois p-subgrupos de Sylow distintos seja trivial. Note que contando o número de elementos não triviais contidos nos p-subgrupos de Sylow de G temos que $q(p^m - 1) = p^m q - q$. Os outros elementos de G totalizam um conjunto de q elementos, isto é, formam um único q-subgrupo de Sylow de G. Este raciocíno, novamente, contradiz a simplicidade de G.

Diante disso, vamos considerar P_1 e P_2 dois p-subgrupos de Sylow de G distintos tais que a interseção entre eles seja a máxima possível. Denote $I = P_1 \cap P_2$. Observe que $I \neq \{1\}$ é um subgrupo próprio de p-grupos. Pela Proposição 1.9, temos $I \lneq N_{P_1}(\mathrm{I})$ e $I \lneq N_{P_2}(\mathrm{I})$. Denote $J = \langle N_{P_1}(I), N_{P_2}(I)\rangle$. Observe que $J \leq N_G(I)$, logo $I \lhd J$. Note que se J é um p-grupo, segue que ele está contido em algum p-subgrupo de Sylow de G, a saber P_3. Assim temos que

$$P_1 \cap P_3 \geq P_1 \cap J \geq N_{P_1}(I) \gneq I \ (\star)$$

Note que $(\star)$ contradiz a maximalidade da ordem de I. Logo, J não é um p-grupo, então q divide $|J|$. Considere Q um q-subgrupo de Sylow de J, então $P_1 \cap Q = \{1\}$. Além disso, $|P_1Q| = p^m q$ e $G = P_1Q$. Vamos considerar o I^G, o fecho normal da interseção I em G, note que

$$\{1\} \neq I \leq I^G = I^{P_1Q}.$$

Como $J \leq Q$ e $Q \leq N_G(I)$, então $I^J = I$. Sendo assim,

$$\{1\} \neq I \leq I^G = I^{P_1Q} = I^{P_1} \leq P_1 \lneq G.$$

Observe que $\{1\} \neq I^G$ e sabemos que I^G é um subgrupo normal próprio de G. Absurdo, pois contradiz que G é simples. Diante disso, temos G solúvel. □

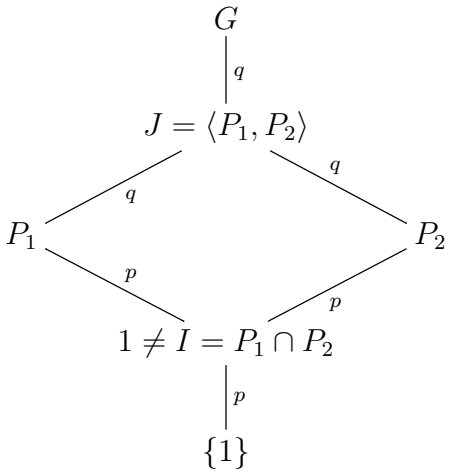
Proposição 2.24. *Sejam p, q primos. Todo grupo de ordem p^2q^2 é solúvel.*

Demonstração. Se $p = q$, então $|G| = p^4$. Neste caso, G é um p-grupo finito e, logo, solúvel. Agora, vamos considerar $p \neq q$. Suponhamos, por absurdo, que G não é solúvel, cuja ordem é p^2q^2.

Pelo Teorema de Lagrange, se $N \neq G$, $N \neq \{1\}$ e $N \trianglelefteq G$, temos que $|N|$ pode ser $p, p^2, pq, p^2q, q, q^2, pq^2$. Para todas as ordens possíveis já demonstramos que N é solúvel, e, consequentemente, G/N também é solúvel. Assim, G é solúvel, pelo Teorema 2.20. Diante disso, podemos assumir G simples e, sem perda de generalidade, $p > q$.

Pelo Teorema de Sylow, temos que $n_p \equiv 1 \mod p$ e $n_p | q^2$, então $n_p = 1$ ou $n_p = q$ ou $n_p = q^2$. Observe que $n_p \neq q$, pois $p > q$ e $n_p \equiv 1 \mod p$. Além disso, $n_p \neq 1$, pois G é simples. Sendo assim, $n_p = q^2$.

Agora, suponhamos que existem P_1 e P_2 dois p-subgrupos de Sylow de G distintos tais que $I = P_1 \cap P_2 \neq \{1\}$. Note que $|P_i| = p^2$, então P_i é abeliano $\forall\ i$. Sendo assim, $I \trianglelefteq P_1$ e $I \trianglelefteq P_2$. Observe o diagrama abaixo:



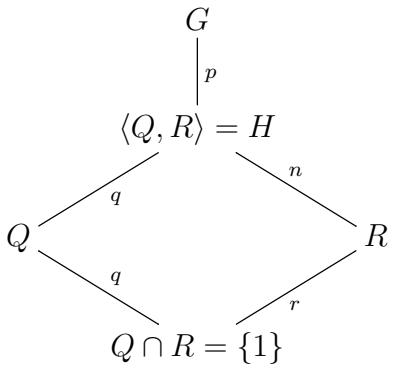
Seja $J = \langle P_1, P_2 \rangle$, então $I \trianglelefteq J$. Diante disso, $J \neq G$. Como $J \neq G$, temos $[G : J] = q$. Pela Proposição 1.2, segue que $J \lhd G$, o que é um absurdo. Assim, quaisquer dois p-subgrupos de Sylow de G têm interseção trivial.

Contando o número de elementos não triviais contidos nos p-subgrupos de Sylow de G, temos que $q^2(p^2 - 1) = q^2p^2 - q^2$. Logo, os outros elementos de G totalizam um conjunto de q^2 elementos, isto é, formam um único q-subgrupo de Sylow de G. Este raciocínio, novamente, contradiz a simplicidade de G. Portanto, concluímos que G tem que ser solúvel. □

Proposição 2.25. *Sejam p, q, r primos. Todo grupo de ordem pqr é solúvel.*

Demonstração. Se $p = q = r$, então $|G| = p^3$. Sendo assim, G é um p-grupo finito, e, logo, solúvel. Agora, se $p \neq q = r$, então $|G| = pq^2$. Neste caso, G é solúvel, pelo Teorema 2.23. Por fim, sejam p, q, r primos distintos. Suponha, sem perda de generalidade, que $p < q < r$. Considere Q um q-subgrupo de Sylow de G e R um

r-subgrupo de Sylow de G, temos $R \cap Q = \{1\}$.



Considere o subgrupo $H = \langle Q, R\rangle$ de G, logo $|H| = qr$. Note que $[G : H] = p$, isto é, o menor primo que divide a ordem de G. Assim, $H \lhd G$, pela Proposição 1.2. De acordo com a Proposição 2.22, segue que H é solúvel.

Agora, tome o grupo quociente de G por H logo $|G/H| = p$. Diante disso, temos que G/H é solúvel. Como H e G/H são solúveis, temos que G é solúvel. □

Além das proposições apresentadas, que relacionam a ordem de um grupo e sua solubilidade, vamos enunciar dois resultados famosos na teoria dos grupos finitos. O primeiro deles foi demonstrado por W. Burnside, no início do século. O matemático usou teoria de representações e caracteres para prova o seguinte teorema:

Teorema 2.26. *(Burnside-1904). Sejam p, q primos distintos e a, b números naturais. Todo grupo de ordem $p^a q^b$ é solúvel.*

Em 1911 Miller-Burnside fizeram a seguinte conjectura: todo grupo de ordem ímpar é solúvel. Tal conjectura foi estudada e comprovada pelos matemáticos W.Feit e J. Thompson, no início da década de 1960. Segundo alguns matemáticos, foi um dos trabalhos mais celebrados na teoria de gupos finitos e é lembrado por apresentar uma demonstração de mais de 200 páginas, foi publicado no Pacific Journal of Mathematics em 1963. Portanto, este é o outro famoso resultado que vamos destacar:

Teorema 2.27. *(W. Feit & J. Thompson - 1963) Todo grupo de ordem ímpar é solúvel.*

Note que o Teorema 2.27 garante que se G for não solúvel, então G possui um elemento de ordem 2.

Capítulo 3

Subgrupos Solúveis de Grupos Simétricos

Neste capítulo, vamos provar um resultado que caracteriza os subgrupos solúveis transitivos em um grupo simétrico S_p, quando p é primo. Basearemos na referência [7].

3.1 Subgrupos Afins

Considere $Bij(\mathbb{Z}_n)$ o grupo $\{f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \mid f \text{ bijeção}\}$, onde $\mathbb{Z}_n$ é o grupo das classes dos restos módulo n. Além disso, relembramos que um inteiro a tem um inverso multiplicativo módulo n se, e somente se, a e n são relativamente primos. Então, para cada $n > 1$, definimos $\mathcal{U}(\mathbb{Z}_n)$ o conjunto de todos os inteiros positivos menores que n e relativamente primo a n.

Agora, vamos definir um subgrupo afim de um grupo simétrico. Para isso, começaremos com a seguinte definição:

Definição 3.1. *Seja $n \in \mathbb{N}$. O grupo de permutação afim, $Aff(n)$, é definido como o subgrupo de $Bij(\mathbb{Z}_n)$, que consiste de todas as funções $\sigma_{a,b} : x \longmapsto ax + b$ tal que $a \in \mathcal{U}(\mathbb{Z}_n)$ e $b \in \mathbb{Z}_n$.*

Além disso, para todos os $a, c, e \in \mathcal{U}(\mathbb{Z}_n)$ e $b, c, d \in \mathbb{Z}_n$ verificamos que

(i) A operação composição de função é fechada em Aff(n). De fato,

$$\begin{aligned}(\sigma_{a,b} \circ \sigma_{c,d})(x) =& \sigma_{a,b}(cx + d)\\ =& a(cx + d) + b\\ =& (ac)x + (ad + b) = \sigma_{ac,ad+b}(x).\end{aligned}$$

(ii) Associatividade

$$\begin{aligned}[(\sigma_{a,b} \circ \sigma_{c,d}) \circ \sigma_{e,f}](x) &= (\sigma_{ac,ad+b} \circ \sigma_{e,f})(x) \\ &= a(ce)x + a(cf+d) + b \\ &= (\sigma_{a,b} \circ \sigma_{ce,cf+d})(x) \\ &= [\sigma_{a,b} \circ (\sigma_{c,d} \circ \sigma_{e,f})](x).\end{aligned}$$

(iii) O Elemento neutro de Aff(n) é $\sigma_{1,0}$. De fato, $\sigma_{1,0}\ (x) = 1x + 0 = x$, $\forall\ x \in \mathbb{Z}_n$.

(iv) Cada elemento $\sigma_{a,b} \in$ Aff(n) admite um inverso. Isto é, $(\sigma_{a,b})^{-1} = \sigma_{a^{-1},-ba^{-1}}$.

Definição 3.2. *Um subgrupo G de S_n é chamado afim, se $\{1, 2, \ldots, n-1, n\}$ pode se identificado com $\mathbb{Z}_n$ de tal maneira que G pode ser visto como um subgrupo de Aff(n).*

Mais especificamente, $\{1,\ 2,\ ...,\ n-1, n\}$ pode ser identificado com $\mathbb{Z}_n$ como estabelecemos abaixo

$$\begin{aligned} 1 &\longmapsto \overline{1} \\ 2 &\longmapsto \overline{2} \\ &\vdots \\ n-1 &\longmapsto \overline{n-1} \\ n &\longmapsto \overline{0} \end{aligned}$$

Diante disso, vemos que existe um isomorfismo entre S_n e Bij($\mathbb{Z}_n$). Se $G \leq S_n$, cada elemento de G é uma permutação de S_n. Para $\sigma \in G$ e identificando $\{1, 2, \ldots, n-1, n\}$ com $\mathbb{Z}_n$, temos que σ permuta $\mathbb{Z}_n$. Sendo assim, podemos ver σ como um elemento de Bij($\mathbb{Z}_n$) e G é visto como um subgrupo de Bij($\mathbb{Z}_n$). Ou seja,

$$\begin{aligned} S_n &\longrightarrow Bij(\mathbb{Z}_n) \\ \sigma &\longmapsto \overline{\sigma}. \end{aligned}$$

Assim, $G \hookrightarrow$ Aff(n), G está isomorficamente imerso em Aff(n). Portanto, podemos dizer que $g = \sigma_{a,b}$, $\forall\ g \in G$ e para algum $a \in \mathcal{U}(\mathbb{Z}_n)$ e $b \in \mathbb{Z}_n$.

Exemplo 3.3. *Um subgrupo cíclico de S_n gerado por um n-ciclo $\sigma = (i_1, i_2, \ldots, i_n)$*

é afim. Inicialmente, vamos identificar $\{1, 2, \ldots, n-1, n\}$ *com* $\mathbb{Z}_n$ *via*

$$\begin{aligned} i_1 &\longmapsto [0] \\ i_2 &\longmapsto [1] \\ i_3 &\longmapsto [2] \\ &\vdots \\ i_n &\longmapsto [n-1]. \end{aligned}$$

Dessa forma, σ *é identificado como uma aplicação* $\overline{\sigma} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ *dada por*

$$\overline{\sigma}([k]) = \overline{\sigma(i_{k+1})} = \overline{i_{k+2}} = [\, k + 1] = [k] + [1].$$

Sendo assim, $\overline{\sigma}$ *é uma "translação"* $x \longmapsto x + 1$*, ou seja,* $\overline{\sigma} = \sigma_{1,1}$*. Além disso, note que* $\overline{\sigma^k} = (\overline{\sigma})^k = \sigma_{1,k}$*, onde que* k *é tomado módulo* n*.*

Observação 3.4. *Considerando* $\mathbf{G} = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathcal{U}(\mathbb{Z}_n) \text{ e } b \in \mathbb{Z}_n \right\}$

e $\varphi : G \longrightarrow Aff(n)$*, onde* $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \longmapsto \sigma_{a,b}$*. Afirmamos que* φ *é um isomorfismo.*

De fato, sejam $\mathbf{A}$, $\mathbf{B} \in \mathbf{G}$, tais que $\mathbf{A} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ e $\mathbf{B} = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$. Observe que

$$\varphi(\mathbf{AB}) = \varphi \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \varphi \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix} = \sigma_{ac,ad+b}.$$

Por outro lado,

$$\varphi(\mathbf{A})\varphi(\mathbf{B}) = \varphi \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \varphi \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \sigma_{a,b} \circ \sigma_{c,d} = \sigma_{ac,ad+b}.$$

Assim, φ é um homomorfismo.

Note que $\mathbf{Ker}\ (\varphi) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \sigma_{1,0} \right\}$. Então, temos que

$$\begin{aligned} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathbf{Ker}(\varphi) \Longrightarrow & \varphi \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \sigma_{1,0} \Longrightarrow \sigma_{a,b}(x) = \sigma_{1,0}(x) \\ & \Longrightarrow ax + b = x \Longrightarrow a = 1, b = 0. \end{aligned}$$

Logo, $\mathbf{Ker}\ \varphi = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. Diante disso, é possível garantir que φ é injetiva. Claramente, φ é sobrejetiva, então, $\mathbf{G} \cong \mathrm{Aff}(n)$.

Agora, vamos mostrar que $\mathbf{G} = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathcal{U}(\mathbb{Z}_n) \text{ e } b \in \mathbb{Z}_n \right\}$ é solúvel. Considere o subgrupo derivado $\mathbf{G}' = [\ \mathbf{G}, \mathbf{G}]$, ou seja,

$$[\ \mathbf{G}, \mathbf{G}] = \left\langle\ [\ \mathbf{A}, \mathbf{B}] \;\middle|\; \mathbf{A},\mathbf{B} \in \mathbf{G} \right\rangle .$$

Temos

$$\begin{aligned}
\left[\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \right] &= \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}^{-1} = \\
&= \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -ba^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c^{-1} & -dc^{-1} \\ 0 & 1 \end{pmatrix} = \\
&= \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1}c^{-1} & -da^{-1}c^{-1} - ba^{-1} \\ 0 & 1 \end{pmatrix} = \\
&= \begin{pmatrix} 1 & -d-cb+ad+b \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Considere $\mathbf{X}$ uma matriz da forma $\begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix}$, onde X é a expressão $-d-cb+ad+b$. Assim, $\mathbf{G}^{(2)} = [\ \mathbf{G}', \mathbf{G}'] = \left\langle\ [\ \mathbf{X}, \mathbf{Y}] \;\middle|\; \mathbf{X},\mathbf{Y} \in \mathbf{G}' \right\rangle$. Observe que

$$\begin{aligned}
\left[\begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & Y \\ 0 & 1 \end{pmatrix} \right] &= \begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & Y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & Y \\ 0 & 1 \end{pmatrix}^{-1} = \\
&= \begin{pmatrix} 1 & Y+X \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -X \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -Y \\ 0 & 1 \end{pmatrix} = \\
&= \begin{pmatrix} 1 & Y+X \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -Y-X \\ 0 & 1 \end{pmatrix} = \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Logo, G é solúvel e com o grau de solubilidade ≤ 2.

O próximo teorema apresenta a relevância dos grupos afins no contexto dos grupos solúveis.

Teorema 3.5. *Se H é um subgrupo de S_n e H é afim, então H é solúvel.*

Demonstração. Se $H \leq S_n$, então H pode ser identificado com um subgrupo de Bij($\mathbb{Z}_n$). Como H é afim, então $H \hookrightarrow$ Aff(n). Além disso, a Observação 3.4 nos mostra que existe um isomorfismo $\varphi : \mathbf{G} \longrightarrow$ Aff(n), onde

$$\mathbf{G} = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; \text{a} \in \mathcal{U}(\mathbb{Z}_n) \text{ e b} \in \mathbb{Z}_n \right\}.$$

Portanto, H é identificado como um subgrupo de um grupo solúvel . Pelo Teorema, 2.14 segue que H é solúvel. □

3.2 Subgrupos Solúveis em S_p

Agora, vamos concentrar nos grupos simétricos S_p onde p é um primo.

Proposição 3.6. *Seja p um número primo. Suponha G um subgrupo transitivo de S_p e que nenhum elemento $\sigma \neq 1$ em G tem mais que um ponto fixo.*

(1) Se $\sigma \in G$ é livre de pontos fixos então σ é um p-ciclo.

(2) Existe um p-ciclo σ tal que os elementos de G livre de pontos fixos são exatamente $p-1$ elementos: $\sigma, \sigma^2, \ldots, \sigma^{p-1}$.

(3) G é afim.

Demonstração. (1) Seja $\sigma = \sigma_1 \ldots \sigma_n$ a decomposição de σ em ciclos disjuntos e seja $\sigma_1 = (i_1 \ldots i_r)$ o menor ciclo da decomposição de σ. Observe que $\mathcal{O}(\sigma_1) = r$. Como σ é livre de pontos fixos, segue que $r \geqslant 2$. Note que $i_1, \ldots, i_r$ são pontos fixos de σ_1^r e, portanto, de σ^r. Pela hipótese, temos que $\sigma^r = 1$ e assim

$$\sigma_2^r = \cdots = \sigma_n^r = 1.$$

De acordo com a minimalidade de $\mathcal{O}(\sigma_1) = r$, todos os ciclos $\sigma_1, \ldots, \sigma_n$ tem o mesmo comprimento r. Como cada elemento de $\{1, 2, \ldots, r\}$ ocorre em exatamente cada um dos ciclos σ_i, $\forall\ i = 1, \ldots, n$, segue que $p = rn$. Como p é primo e $r \geqslant 2$, então $r = p$ e $m = 1$. Diante disso, segue que σ é um p-ciclo.

(2) Considere a $Orb_G(i)$ para cada $i \in \{1, ..., p\}$. Como G é transitivo, segue que $Orb_G(i) = \{1, \ldots, p\}$ $\forall\ i$. Sendo assim, temos que $|Orb_G(i)| = p$. Pelo teorema da Órbita - Estabilizador, temos que

$$|Stab_G(i)| = \tfrac{|G|}{|Orb_G(i)|} \Longrightarrow |Stab_G(i)| = \tfrac{|G|}{p},\ (*)$$

$\forall\, i = 1, \ldots, n$ e $1 \leq i \leq p$. Por hipótese, nenhum elemento $\sigma \neq 1$ em G tem dois pontos fixos. Assim, $Stab_G(i) \cap Stab_G(j) = \{1\}$, sempre que $i \neq j$. Se listarmos os elementos dos estabilizadores $Stab_G(1), \ldots, Stab_G(p)$, então cada elemento de G aparece exatamente uma vez, exceto o elemento neutro que aparece p vezes. Então,

$$|Stab_G(1) \cup \ldots \cup Stab_G(p)| = |Stab_G(1)| + \ldots + |Stab_G(p)| \text{ - } (p-1).$$

De $(*)$, segue que

$$\begin{aligned} |Stab_G(1)| + \ldots + |Stab_G(p)| - (p-1) &= |G|/p + \ldots + |G|/p - (p-1) \\ &= |G| - (p-1). \end{aligned}$$

Note que o complemento da $\bigcup_{i=1}^{p} Stab_G(i)$, que consiste de todos os elementos de G livres de pontos fixos, são $p-1$ elementos. Tome um desses elementos, a saber σ. Pelo item (1), temos que σ é um p-ciclo. Considere as potências $\sigma^2, \ldots, \sigma^{p-1}$ de σ. Estes são os elementos remanescentes de G e livres de pontos fixos.

(3) Mostrar que G é afim equivale a verificar que $G \hookrightarrow \mathrm{Aff}(n)$, isto é, $\forall\, g \in G$ temos $g = \sigma_{a,b}$, para algum $a \in \mathcal{U}(\mathbb{Z}_n)$ e $b \in \mathbb{Z}_n$. Sem perda de generalidade, podemos assumir $\sigma = (\ 1\ 2\ \ldots p)$, na parte (2). Agora, tome $g \in$ G e considere $g\sigma g^{-1}$. Afirmamos que o elemento $g\sigma g^{-1}$ é livre de pontos fixos. De fato, se existe x ponto fixo do elemento $g\sigma g^{-1}$, segue que

$$(g\sigma g^{-1})(x) = x \Longrightarrow \sigma((g^{-1})(x)) = ((g^{-1})(x)).$$

Então, $((g^{-1})(x))$ é ponto fixo de σ, absurdo. Diante disso, $g\sigma g^{-1}$ é livre de ponto fixo. De acordo com a parte (2), σ e suas potências são os únicos elementos de G livres de pontos fixos. Sendo assim, $g\sigma g^{-1} = \sigma^k$, para algum k tal que $1 \leq k \leq p-1$. Logo, $g\sigma = \sigma^k g$ $(\star)$. Observamos que

$$\begin{gathered} g(\sigma(1)) = g(2) \\ g(\sigma(2)) = g(3) \\ \vdots \\ g(\sigma(p-1)) = g(p) \\ g(\sigma(p)) = g(1). \end{gathered}$$

Assim, $g\sigma = \begin{pmatrix} 1 & 2 & ... & p \\ g(2) & g(3) & ... & g(1) \end{pmatrix}$.

Por outro lado, temos que

$$\sigma(i) = i + 1$$
$$\sigma^2(i) = i + 2$$
$$\vdots$$
$$\sigma^k(i) = i + k, \forall \text{ i.}$$

Logo, observamos que $\sigma^k(g(i)) = g(i) + k$.

Assim, $\sigma^k g = \begin{pmatrix} 1 & 2 & ... & p \\ g(1)+k & g(2)+k & ... & g(p)+k \end{pmatrix}$.

De $(\star)$, segue que

$$\begin{pmatrix} 1 & 2 & ... & p \\ g(2) & g(3) & ... & g(1) \end{pmatrix} = \begin{pmatrix} 1 & 2 & ... & p \\ g(1)+k & g(2)+k & ... & g(p)+k \end{pmatrix}$$
$$\Longrightarrow (g(i+1)) = g(i) + k \quad \forall i$$
$$\Longrightarrow (g(2)) = g(1) + k$$
$$\Longrightarrow (g(3)) = g(2) + k = g(1) + 2k$$
$$\vdots$$
$$\Longrightarrow (g(i)) = g(1) + (i-1)k = ik + (g(1) - k).$$

Logo, g é identificado como um elemento de Aff(n), isto é, $g = \sigma_{k,g(1)-k}$. Portanto, G é afim.

□

Proposição 3.7. *Seja G um subgrupo transitivo de S_p, onde p é um número primo. Então G é solúvel se, e somente se, G é afim.*

Demonstração. Se G é afim, então G é solúvel, pelo Teorema 3.5. Vamos estabelecer a implicação contrária. Se G é solúvel, então existe uma série

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

onde cada quociente G_i/G_{i+1} é cíclico de ordem prima , $\forall\ i$. Inicialmente, vamos demonstrarque cada grupo G_0 , G_1 , ... , G_{n-1} é transitivo. A demonstração é por indução sobre i. Como $G_0 = G$, por hipótese, G_0 é transitivo.

Agora, suponha G_i transitivo, vamos mostrar que G_{i+1} é transitivo. Como $G_i \trianglerighteq G_{i+1}$, então todas as órbitas de G_{i+1} tem a mesma cardinalidade, pela Proposição 1.13. Sendo assim, a cardinalidade é um divisor de $p = |X|$. Assim, as órbitas de G_{i+1} tem comprimento 1 ou p.

Afirmamos que se $G_{i+1} \neq \{1\}$, então G_{i+1} é transitivo. De fato, para $G_{i+1} \neq \{1\}$ existe alguma órbita de G_{i+1} não trivial. Diante disso, $|Orb_G(i)| = p$, $\forall\ k \in \{1, 2, \ldots, p\}$. Portanto, G_{i+1} é transitivo.

Como $G_{n-1}/G_n \cong G_{n-1}$ é cíclico de ordem prima e transitivo, então G_{n-1} é gerado por um ciclo. A sua transitividade nos permite garantir que tal ciclo é um p-ciclo. Sendo assim, $G_{n-1} = \langle \tau \rangle$.

Do Exemplo 3.3, segue que G_{n-1} é afim. Precisamente, podemos identificar $\{1, 2, \ldots, p\}$ com $\mathbb{Z}_p$ de tal maneira que $\tau : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ e $\tau(x) = x + 1$, com $\tau = \sigma_{1,1}$. Esta identificação é muito útil para o restante da demonstração. Sendo assim, vamos fixa-lá até o final da prova da proposição e das demonstrações subsequentes.

Agora, vamos mostrar que se G_i é afim, então G_{i-1} é afim. Consequentemente, como G_{n-1} é afim vamos concluir indutivamente que $G = G_0$ é afim, como desejamos demonstrar. Inicialmente, tome $\sigma \in G_{i-1}$. Como $G_{i-1} \trianglerighteq G_i$ e $\tau = \sigma_{1,1}$, segue que

$$\sigma^{-1}\sigma_{1,1}\sigma = \sigma^{-1}\tau\sigma \in \sigma^{-1}G_{n-1}\sigma \subseteq \sigma^{-1}G_i\sigma \subseteq G_i.$$

Como G_i é afim, então existem a, b tais que $a \in \mathcal{U}(\mathbb{Z}_n)$ e $b \in \mathbb{Z}_n$, onde $\sigma^{-1}\sigma_{1,1}\sigma = \sigma_{a,b}$ $(**)$. Note que

$$\sigma_{a,b}^p = \underbrace{(\sigma^{-1}\sigma_{1,1}\sigma)(\sigma^{-1}\sigma_{1,1}\sigma)\ldots(\sigma^{-1}\sigma_{1,1}\sigma)}_{p \quad vezes} = \sigma^{-1}\ \sigma_{1,1}^p\ \sigma.$$

Além disso, observe que

$$\sigma_{1,1}^p = \tau^p = 1 \Longrightarrow \sigma_{a,b}^p = \sigma^{-1}\ \sigma_{1,1}^p\ \sigma = \sigma^{-1}\ 1\ \sigma = 1.\ (\star\star)$$

Da observação 3.4 e de $(\star\star)$, temos que

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} a^p & \sum_{i=1}^{p} a^{p-i}b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Logo, $a^p = 1$ em $\mathbb{Z}_p$. Por outro lado, do Pequeno Teorema de Fermat, segue que $a^{p-1} \equiv 1 \pmod{p}$. Assim, $a^p = a$, e, portanto, $a = 1$. Então, em $(**)$ temos

$$\sigma^{-1}\sigma_{1,1}\sigma = \sigma_{1,b} \Longrightarrow \sigma_{1,1}\sigma = \sigma\ \sigma_{1,b}.$$

Isto significa que

$$\sigma(x) + 1 = \sigma(x + b), \forall\ x \in \mathbb{Z}_p.\ (\star)$$

Utilizando a relação em $(\star)$, observamos que

$$\begin{aligned}
\sigma(kb) &= \sigma((k-1)b + b) \\
&= \sigma((k-1)b) + 1 \\
&= \sigma((k-2)b) + 1 + 1 \\
&= \quad \vdots \\
&= \sigma((k-k)b) \underbrace{+1 + 1 + \ldots + 1}_{k \quad vezes} \\
&= \sigma(0) + k,\ \forall\ x\ \in\ \mathbb{Z}_p.
\end{aligned}$$

Note que $b \neq 0$ tem inverso em $\mathcal{U}(\mathbb{Z}_p)$. Agora, vamos definir $k := xb^{-1}$. Sendo assim, $\sigma(x) = \sigma(0) + xb^{-1}$, $\forall\ x \in \mathbb{Z}_p$. Então, $\sigma = \sigma_{\alpha,\beta}$, onde $\alpha := b^{-1}$ e $\beta := \sigma(0)$. Isso mostra que G_{i-1} é um subgrupo afim de S_p, como queríamos. □

Proposição 3.8. *Seja G um subgrupo transitivo de S_p, onde p é um número primo. Então G é afim se, e somente se, nenhum elemento $\sigma \neq 1$ em G tem mais que um ponto fixo.*

Demonstração. Provamos, na Proposição 3.6, que se nenhum elemento $\sigma \neq 1$ em G tem mais que um ponto fixo, então G é afim. Reciprocamente, suponha que G é afim e que existe $\sigma \in G$ tal que σ tem dois pontos fixos. Identificando σ com a função afim $\sigma_{a,b}$, de $\mathbb{Z}_p$ em $\mathbb{Z}_p$, segue que existem dois elementos distinto $i, j \in \mathbb{Z}_p$ tais que

$$\begin{aligned}
ai + b &= i \quad (1) \\
aj + b &= j \quad (2).
\end{aligned}$$

Subtraindo (2) de (1), temos que $a(i - j) = i - j$. Como $i - j \neq 0$, temos que $i - j \in \mathcal{U}(\mathbb{Z}_p)$. Diante disso, $a = 1$. Além disso, $b = 0$ e, portanto, $\sigma = \sigma_{1,0} = 1$. Logo, nenhum $\sigma \neq 1$ em G tem mais que um ponto fixo. □

Proposição 3.9. *Seja G um subgrupo transitivo de S_p, onde p é um número primo. Se G é afim, então $|G| \leq p(p-1)$.*

Demonstração. Por definição Aff(p) é um subgrupo de Bij$(\mathbb{Z}_p)$, que consiste de todas as funções $\sigma_{a,b}$: $\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$, definidas por $\sigma_{a,b}(x) = ax + b$ tais que $a \in \mathcal{U}(\mathbb{Z}_n)$ e

$b \in \mathbb{Z}_p$. Sendo assim, o número de elementos de Aff(p) são todas as combinações possíveis entre as possibilidades para os números a e b. Como $a \in \mathcal{U}(\mathbb{Z}_n)$, então as possibilidades para a são $p-1$, ou seja, todas os $k \in \mathbb{Z}_p$ tal que $k \neq$. As possibilidades para b são os p elementos de $\mathbb{Z}_p$. Pelo Princípio Multiplicativo, segue que $|\text{Aff}(p)| = p(p-1)$ elementos. Como G é afim, então G pode ser identificado como um subgrupo de Aff(p), tal que $|G| \leq |\text{ Aff}(p) | = p(p-1)$. □

Proposição 3.10. *Seja G um subgrupo transitivo de S_p, onde p é um número primo. Se $|G| \leq p(p-1)$, então $|G| = pm$, para algum número natural $m < p$.*

Demonstração. Como $|G| \leq p(p-1)$ e G age transitivamente em $X = \{1, 2, \ldots, p\}$, então $|G|$ é divisível por p, de acordo com a Proposição 1.13. Sendo assim, $|G| = pm$, para algum número natural $m < p$ □

Proposição 3.11. *Seja G um subgrupo transitivo de S_p, onde p é um número primo. Se $|G| = pm$, para algum número natural $m < p$, então G é afim.*

Demonstração. Seja $|G| = mp$ com $m < p$ e seja P um p - subgrupo de Sylow de G. Logo, $|P| = p$ e P é gerado por um elemento σ de mesma ordem. Sendo assim, $\sigma \in S_p$. Pelo Teorema 1.25, sabemos que os únicos elementos de S_p de ordem p são os p-ciclos, assim σ é um p-ciclo. Sem perda de generalidade, podemos assumir que $\sigma = (1, 2, \ldots, p)$.

Do Teorema de Sylow, temos que $n_p \equiv 1 \pmod{p}$ e $n_p \mid m$, sendo n_p o número de p-subgrupos de Sylow de G. Note que $1 + kp$ tal que $k \in \mathbb{N}_0$ representa a forma do número de p-subgrupos de Sylow de G. Assim, $1 + kp \mid m$. Consequentemente, $k = 0$ e $n_p = 1$, então P é o único p-subgrupo de Sylow de G, daí $G \trianglerighteq P$. Seja g um elemento arbitrário de G, então

$$g\sigma g^{-1} \in gPg^{-1} = P \; ; \; g\sigma g^{-1} = \sigma^k$$

para algum $1 \leq k \leq p-1$. Logo, $g\sigma = g^{-1}\sigma^k$. Repetindo o argumento da Proposição 3.6, parte (3), segue que $g = \sigma_{k,g(1)-k}$. Como g foi arbitrariamente escolhido, temos que G um grupo afim. □

Os resultados apresentados nas proposições acima estabelecem condições necessárias e suficientes para satisfazer as equivalências do teorema abaixo. Ele fornece a identificação dos subgrupos transitivos e solúveis de S_p, onde p é primo.

Teorema 3.12. *([7], Capítulo 28, Teorema 28.23) Seja G um subgrupo transitivo de S_p onde p é um número primo. Então as seguintes condições são equivalentes.*

(1) G é solúvel.

(2) G é afim.

(3) Nenhum $\sigma \neq 1$ em G tem mais que um ponto fixo.

(4) $|G| \leq p(p-1)$.

(5) $|G| = pm$ para algum número natural $m < p$.

Agora, vamos identificar os subgrupos transitivos e solúveis de S_5 e S_7. Mas antes precisamos mostrar a seguinte proposição:

Proposição 3.13. *Seja G um subgrupo próprio de S_p e $G \neq A_p$. Então $[S_p : G] \geq p$, isto é, $|G| \leq (p-1)!$, para $p > 3$(ou p maior ou igual a 5).*

Demonstração. Inicialmente, denote $d = [S_p : G]$ e considere $X = \{\sigma G | \sigma \in S_p\}$. Assim, definimos a seguinte ação de S_p sobre nas classes laterais de G

$$\begin{aligned} \varphi : S_p &\longrightarrow Sim(X) \\ \sigma &\longmapsto \varphi_\sigma : X \longrightarrow X \\ &\qquad (xG) \longmapsto \sigma(xG). \end{aligned}$$

Observe que $Ker\varphi = \{\sigma \in S_p \mid \varphi_\sigma(\sigma G) = \sigma G, \forall\ \sigma \in S_p\}$ e $Stab_{S_p}(G) = \{\sigma \in S_p \mid \sigma G = G\}$. Diante disso, é possível observar que o $Ker\varphi$ é a interseção dos estabilizadores das permutações de X. Em particular, o $Ker\varphi$ está contido em G.

Por outro lado, sabemos que $Ker\varphi \triangleleft S_p$, então $Ker\varphi = \{1\}$, S_p ou A_p. Como G não contém S_p ou A_p, segue que $Ker\varphi = \{1\}$. Agora, pelo Teorema do Isomorfismo:

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

Isto é,

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

Sendo assim, $\mid G \mid \leq \mid Sim(X) \mid$. Logo, $p! \leq d!$ ou $p \leq d$, como queríamos demonstrar. □

Exemplo 3.14. *Os subgrupos transitivos e solúveis de S_5.*

Suponha G um subgrupo transitivo e solúvel de S_5. Mostramos que S_5 e A_5 não são solúveis, logo G é um subgrupo próprio de S_5 e $G \neq A_5$. Pelo teorema acima, temos que

$$|G| = 5k, \text{ onde } 1 \leq k \leq 4.$$

Note que para todas as possíveis ordens determinadas acima, já demonstramos que o subgrupo G é solúvel.

Por Sylow, existe um subgrupo P de G tal que $|P| = 5$. Note que para $k = 1$, 2 ou 3, $[G : P]$ será o menor primo que divide a ordem de G. Neste caso, temos $P \lhd G$.

Agora, para $k = 4$, temos $n_5 = 1$. Então, $P \lhd G$. Diante do exposto, P é um subgrupo normal em G, isto é, $G \subseteq N_{S_5}(P)$.

Como P é cíclico, podemos assumir que $P = \langle\sigma\rangle$, onde σ tem ordem 5. Observe que $P \leq G \leq S_5$, pela Proposição 1.25, σ é um 5-ciclo. Sem perda de generalidade, podemos assumir σ = (1 2 3 4 5).

Observe que se $\rho \in N_{S_5}(P)$, então $\rho\sigma\rho^{-1} = \sigma^n$, onde $1 \leq n \leq p-1$, pela Proposição 3.6. Assim, para σ^2, temos ρ = (2 3 5 4) um elemento que conjuga σ para σ^2.

Note que A_5 não normaliza P, pois $|A_5| = 60$. Da proposição anterior, $|N_{S_5}(P)| \leq 24$, logo $N_{S_5}(P)$ não contém nenhum 3-ciclo. Mas por outro lado, $\langle\sigma, \rho\rangle$ é um subgrupo de $N_{S_5}(P)$, isomorfo a $\mathbb{Z}_4 \ltimes \mathbb{Z}_5$ e de ordem 20. Assim, novamente pela proposição acima, temos que $N_{S_5}(P) = \langle\sigma, \rho\rangle$. Portanto,

$$\langle\sigma\rangle \subseteq G \subseteq \langle\sigma, \rho\rangle.$$

Logo as possibilidades para G são $\langle\sigma\rangle \cong \mathbb{Z}_5$ e $\langle\sigma, \rho\rangle \cong \mathbb{Z}_4 \ltimes \mathbb{Z}_5$. Além disso, observe que $|\rho| = 4$, então $|\rho^2| = 2$. Claramente, $\langle\sigma, \rho^2\rangle \subseteq \langle\sigma, \rho\rangle$. Assim, o subgrupo $\langle\sigma, \rho^2\rangle = \mathfrak{D}_5$, onde $\mathfrak{D}_5 = \langle\sigma, \rho^2 | \sigma^5 = 1, \rho^2 = 1, \sigma^\rho = \sigma^{-1}\rangle$, também é uma possibilidade para G.

Exemplo 3.15. *Vamos identificar, analogamente ao exemplo anterior, os subgrupos transitivos e solúveis de S_7.*

Suponha G um subgrupo transitivo e solúvel de S_7. Como S_7 e A_7 não são solúveis, segue que G é um subgrupo próprio de S_7 e $G \neq A_7$. Pelo teorema 3.12, temos que

$$|G| = 7k, \text{ onde } 1 \leq k \leq 6.$$

Note que para todas as possíveis ordens: $|G| = 7, 7.2, 7.3, 7.2^2, 7.5$ e $7.2.3$, o subgrupo G é solúvel.

Sendo assim, existe um subgrupo P de G tal que $|P| = 7$, de acordo com o Teorema de Sylow. Note que para $k = 1$, 2, 3 ou 5, o $[G : P]$ será o menor primo que divide a ordem de G. Logo, $P \lhd G$. Agora, para $k = 4$ e $k = 6$, temos $n_7 = 1$. Assim, também, segue que $P \lhd G$. Diante do exposto, P é um subgrupo normal em G, isto é, $G \subseteq N_{S_7}(P)$.

Note que P é cíclico, logo $P = \langle\tau\rangle$, onde τ tem ordem 7. Pela Proposição 1.25, τ é um 7-ciclo e vamos assumir que τ = (1 2 3 4 5 6 7).

Além disso, γ = (2 4 3 7 5 6) é o elemento que conjuga τ para τ^3.

Temos, também, que A_7 não normarliza G, pois basta verificar que proposição anterior garante que $|N_{S_7}(P)|$ é menor que 6!. Como $\langle\tau,\gamma\rangle$ é um subgrupo de $N_{S_7}(P)$, isomorfo a $\mathbb{Z}_6 \ltimes \mathbb{Z}_7$ e de ordem 42, temos que $N_{S_7}(P) = \langle\tau,\gamma\rangle$. Logo,

$$\langle\tau\rangle \subseteq G \subseteq \langle\tau,\gamma\rangle.$$

As possibilidades para G são:

(1) $\langle\tau\rangle \cong \mathbb{Z}_7$.

(2) $\langle\tau,\gamma^2\rangle$. Note que é o grupo de Frobenius de ordem 42.

(3) $\langle\tau,\gamma\rangle \cong \mathbb{Z}_6 \ltimes \mathbb{Z}_7$. Note que é o grupo de Frobenius de ordem 21.

(4) $\mathfrak{D}_7 = \langle\tau,\gamma^3\rangle$.

Considerações Finais

A fim de relembrarmos os resultados mencionados da teoria de Galois, destacamos o seguinte teorema:

Teorema 3.16. *Sejam F um corpo de característica zero e um polinômio $f(x) \in F[x]$. Se o polinômio é irredutível sobre de grau $n > 1$, então o seu grupo de Galois $Gal(f/F)$ é um subgrupo transitivo de S_n, cuja ordem é divisível por n.*

Além disso, a teoria estabelece que a equação $f(x) = 0$ é *solúvel por radicais*, se existe uma extensão radical de F que contém o corpo de decomposição de $f(x)$. Isto é, se existe uma cadeia

$$F_0 = F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_t$$

tal que $F_i = F_{i-1}(u_i)$ e $u_i^{n_i} \in F_{i-1}$, para algum $n_i \in \mathbb{N}$ e para cada $i = 1, \ldots, t$.

Assim, associando cada polinômio a um grupo, os resultados de Galois garantem um critério de solubilidade para equações algébricas $f(x) = 0$, sobre corpos de característica zero e que dependem da estrutura do seu grupo de Galois . Sendo assim, enunciamos o seguinte resultado

Critério 3.17. *O polinômio $f(x)$ é solúvel por radicais, se, e somente se, o grupo $Gal(f/F)$ é solúvel.*

O critério acima é conhecido como *Critério de Galois.*

Vamos considerar $f(x) = x^7 - 14x^5 + 56x^3 - 56x^3 - 56x + 22$ e $F = \mathbb{Q}$. Sabemos que $Gal(f/\mathbb{Q})$ sobre $\mathbb{Q}$ é o grupo de Frobenius de ordem 21, para mais detalhes sugerimos a referência [6]. De acordo com o exemplo 3.15, temos que o $Gal(f/\mathbb{Q})$ é um subgrupo solúvel e transitivo do S_7. Sendo assim, o Critério de Galois garante que $f(x)$ é solúvel por radicais.

Agora, seja $p(x) = 2x^5 - 10x + 5$, o $Gal(p/\mathbb{Q})$ sobre $\mathbb{Q}$ é o S_5. Neste caso, $p(x)$ não é solúvel por radicais, pois mostramos que S_5 não é solúvel.

É notoria a importância dos grupos solúveis na Teoria de Galois. No decorrer do trabalho, procuramos estudar os principais resultados sobre os grupos solúveis

e discutir o teorema que tem como objetivo identificar os subrupos transitivos e solúveis de S_p, onde p é primo. Contudo, é perceptível a extensão do tema, ainda há muitos resultados a serem discutidos. A nossa monografia é apenas uma introdução aos estudos iniciais sobre os grupos solúveis finitos.

Referências Bibliográficas

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

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

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

[4] GOODMAM, F. M. *Algebra Abstract and Concrete*, 2.6 ed. Iowa City, 2014.

[5] ROBINSON, D. J. S. *A course in the theory of groups*, 2nd ed. United States of America, 1995.

[6] SANTOS, C. A. M. *Calculando Grupo de Galois sobre os Racionais*. UFPB - 1999.

[7] SPINDLER, K. *Abstract algebra with applications*. Vector spaces and Groups, Vol I. Darmstadt, Germany, 1994.