Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Fatores Principais e Coroas de Grupos Finitos

Júlia Arêdes de Almeida

Orientador: Prof. Dr. Martino Garonzi

Brasília

2020

Júlia Arêdes de Almeida

Fatores Principais e Coroas de Grupos Finitos

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasíia, como parte dos requisitos para obtenção do grau de MESTRE em Matemática.

Orientador:
Prof. Dr. Martino Garonzi

Brasília

2020

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

AJ94f

Arêdes de Almeida, Júlia
Fatores Principais e Coroas de Grupos Finitos / Júlia Arêdes de Almeida; orientador Martino Garonzi. -- Brasília, 2020.
91 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2020.

1. Fatores Principais. 2. Coroas de Grupos Finitos. 3. Grupos Primitivos. I. Garonzi, Martino, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Fatores Principais e Coroas de Grupos Finitos

por

Júlia Aredes de Almeida*

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 10 de fevereiro de 2020.

Comissão Examinadora:

Prof. Dr. Martino Garonzi - MAT/UnB (Orientador)

Prof. Dr. Alex Carrazedo Dantas – MAT/UnB (Membro)

Profa. Dra. Ana Cristina Vieira – UFMG (Membro)

* O autor foi bolsista do CNPq durante a elaboração desta dissertação.

Agradecimentos

Primeiramente gostaria de agradecer a Deus.

Agradeço especialmente à minha mãe Jakeline, aos meus irmãos Lukas e Luísa e ao meu namorado Pedro por todo o apoio dado durante todos esses anos. À minha avó Eva, aos meus tios Maicon, Junior e Renata e ao restante dos meus familiares por todo o suporte dado nos momentos mais difíceis.

Ao meu orientador Martino por toda dedicação, compromisso e paciência durante a elaboração desse trabalho.

Aos professores que contribuíram para a minha formação como mestre, em especial à professora Aline Pinto e ao professor Célius Magalhães.

Aos meus colegas de curso, em especial à minha amiga Francisca.

Aos professores da banca Alex Carrazedo e Ana Cristina Vieira pelas sugestões para a melhoria deste trabalho.

Ao CNPq pelo apoio financeiro ao longo de todo o mestrado.

Meus sinceros agradecimentos a todos.

Resumo

Este trabalho apresenta um estudo de fatores principais e coroas de grupos finitos. Para fatores principais abelianos apresentamos a definição de coroa de um fator principal de um grupo solúvel dada por Gaschütz no artigo *Praefrattinigruppen* [7] e estudamos o número de complementos de um fator principal de uma série principal de um grupo solúvel. Para fatores principais não abelianos apresentamos os conceitos de G-grupos G-equivalentes, fatores principais G-relacionados e apresentamos a definição de coroa dada por Lafuente no artigo *Nonabelian crowns and schunck classes of finite groups* [11]. Também apresentamos a generalização do conceito de coroa dada por Jiménez-Seral e por Lafuente no artigo *On Complemented Nonabelian Chief Factors of a Finite Group* [10], e mostramos que essa definição é equivalente as duas definições anteriores, englobando assim os casos abeliano e não abeliano. Além disso estudamos grupos primitivos que são úteis para definir fatores principais G-relacionados e por consequência para entender a noção de G-equivalência.

Palavras-chave: Fatores principais, Coroa, Grupos primitivos.

Abstract

This work presents a study of chief factors and crowns of finite groups. For abelian chief factors we present the definition of crown of a chief factor of a soluble group given by Gaschütz in the article *Praefrattinigruppen* [7] and we study the number of complemented chief factors in a chief series of a finite soluble group. For non-abelian chief factors we present the concepts of G-equivalent G-groups, G-related chief factors and we present the definition of crown given by Lafuente in the article *Nonabelian crowns and schunck classes of finite groups* [11]. We also present the generalization of the concept of crown given by Jiménez-Seral and Lafuente in the article *On Complemented Nonabelian Chief Factors of a Finite Group* [10], and we show that this definition is equivalent to the previous two definitions, thus encompassing the abelian and non-abelian cases. In addition we study primitive groups which are useful for defining G-related chief factors and therefore for understanding the notion of G-equivalence.

Keywords: Chief factors, Crown, Primitive groups.

Sumário

Introdução

Seja $\{1\} \neq N$ um subgrupo normal de um grupo G. Dizemos que N é um subgrupo normal minimal de G se dado $L \leq N$ com $L \trianglelefteq G$ então $L = \{1\}$ ou $L = N$. Sejam agora $H, K \trianglelefteq G$ com $K \leq H$. Dizemos que H/K é um fator principal de G se H/K é um subgrupo normal minimal de G/K. Um fator principal H/K é complementado se existe um subgrupo M de G tal que $HM = G$ e $H \cap M = K$. Observe que se trata de uma propriedade reticular, ou seja, podemos ver se um fator é complementado apenas olhando o reticulado dos subgrupos de G.

Uma série

$$\{1\} = U_0 < U_1 < \ldots < U_r = G$$

de subgrupos $U_i \trianglelefteq G$ é dita uma série principal se U_i/U_{i-1} é um fator principal de G para $i = 1, 2, \ldots, r$. Este trabalho tem como motivação as perguntas

Pergunta 1: *O número de fatores principais complementados de duas séries principais de um grupo finito G é o mesmo?*

Pergunta 2: *Qual o número de complementos de um fator principal de um grupo finito G e esse número (a menos de permutação dos fatores) se altera ao passar de uma série para outra?*

Como veremos, a resposta para a pergunta 1 é sim no caso solúvel mas é não em geral. Também encontraremos uma resposta para a pergunta 2 no caso em que G é um grupo solúvel.

O subgrupo de Frattini $\Phi(G)$ de G é definido como $\{1\}$ quando $G = \{1\}$ e como

$$\Phi(G) = \bigcap\{M : M \text{ é maximal em } G\},$$

quando $G \neq \{1\}$. O Frattini de um grupo finito é sempre um grupo nilpotente. Um fator principal H/K de G é dito Frattini se $H/K \leq \Phi(G/K)$. Veremos que se um fator principal H/K de G for abeliano então ou H/K é complementado ou H/K é Frattini, e no caso em que H/K é complementado, H/K é complementado por um subgrupo maximal de G. Por outro lado veremos que um fator principal não abeliano é sempre não Frattini. No apêndice deste trabalho daremos um exemplo de fator principal não abeliano não complementado.

Dados dois grupos A e G, o grupo A é dito um G-grupo se é dado um homomorfismo

$$\begin{aligned} \gamma : G &\longrightarrow Aut(A) \\ g &\longmapsto \theta(g) : A \longrightarrow A \\ &\qquad\qquad\quad a \longmapsto a^g. \end{aligned}$$

que determina uma ação de G sobre A. O centralizador de A em G é dado por

$$C_G(A) = \{g \in G : a^g = a,\ \forall a \in A\} = \mathrm{Ker}(\theta).$$

Dois G-grupos A e B são ditos G-isomorfos se existe um isomorfismo $\varphi : A \to B$ tal que $(a^g)^\varphi = (a^\varphi)^g$, para quaisquer $a \in A$, $g \in G$. Neste caso dizemos que φ é um G-isomorfismo e denotamos $A \cong_G B$. Veremos que se dois G-grupos A e B são G-isomorfos então $C_G(A) = C_G(B)$.

Se H/K é um fator principal de G, o grupo G age por conjugação em H/K da seguinte forma: dado $h \in H$ e $g \in G$, temos $(hK)^g = h^g K$. Essa ação de G em H/K define um homomorfismo de grupos

$$\theta : G \to Aut(H/K)$$

de forma que H/K é um G-grupo. Neste sentido temos uma primeira resposta para a pergunta 1:

Teorema 3.7: ([4], Capítulo A, Teorema 9.13) *Sejam $\mathcal{H}_1$ e $\mathcal{H}_2$ duas séries principais de um grupo finito G. Então existe uma bijeção entre os fatores principais de $\mathcal{H}_1$ e os fatores principais de $\mathcal{H}_2$ tal que fatores correspondentes são G-isomorfos e os fatores principais Frattini de $\mathcal{H}_1$ correspondem aos fatores principais Frattini de $\mathcal{H}_2$.*

Apesar do Teorema acima, veremos que G-isomorfismo não preserva o fato do fator principal ser complementado.

O conceito de coroa de um grupo solúvel foi introduzido por W. Gaschütz em [7]. Considerando um fator principal H/K complementado de um grupo solúvel finito como um G-módulo irredutível A, Gaschütz definiu a A-coroa de G por C/R, onde $C = C_G(A)$ o centralizador de A em G e

$$R = R(A) = \bigcap \{T \trianglelefteq G : T < C, C/T \cong_G A, C/T \ \text{ é complementado}\}.$$

Considerando A como um G-módulo irredutível e $F = End_G(A)$ o anel de G-endomorfismos de A, pelo Lema de Schur, se $0 \neq f \in F$ então f é isomorfismo. Desta forma F é um anel de divisão e pelo Teorema de Wedderburn segue que F é um corpo. Assim A é um espaço vetorial sobre F com respeito a $fa = f(a)$, para quaisquer $f \in F$ e $a \in A$. Com isso Gaschütz obteve a seguinte fórmula que responde à primeira parte da pergunta 2 para um grupo finito solúvel G:

Proposição 3.15: ([6], Proposição 3) *Sejam G um grupo solúvel finito, H/K um fator principal de G complementado e G-isomorfo a A e C/R a coroa definida por A. O número de complementos de H/K em G/K é*

$$|A|^t \, |End_G(A)|^{m-1},$$

onde $t = 0$ se H/K é central, $t = 1$ se H/K não é central e m é o número de fatores G-isomorfos a A entre C e KR de uma série principal de G que passa por C e KR.

Neste caminho Barnes obteve uma resposta para a segunda parte da pergunta 2

Teorema 3.16: ([2], Teorema 1) *Considere duas séries principais de um grupo solúvel finito G. Então existe uma correspondência biunívoca entre os fatores das duas séries, tais que os fatores correspondentes são G-isomorfos e possuem o mesmo número de complementos.*

Agora introduziremos grupos primitivos que aparecerão no estudo de fatores principais não abelianos. Definimos o core normal de um subgrupo H de G por

$$H_G = \bigcap_{g \in G} H^g = \bigcap_{g \in G} g^{-1} H g.$$

Um grupo G é dito primitivo se existe um subgrupo maximal M de G com $M_G = \{1\}$. Sejam $L, N \leq G$. Se $G = LN$ dizemos que L é um suplemento para N em G. Se $G = LN$ e $L \cap N = \{1\}$ dizemos que L é um complemento para N em G. O socle de um grupo G, denotado por $Soc(G)$, é o subgrupo gerado pelos subgrupos normais minimais de G. R. Baer classificou os grupos primitivos em termo de seu socle da seguinte maneira:

Teorema 2.11: (Baer) *Sejam G um grupo primitivo e M é um subgrupo maximal de G com $M_G = \{1\}$. Então vale exatamente uma das condições abaixo*

(a) *$Soc(G) = S$ onde S é um subgrupo normal minimal abeliano auto-centralizado de G que é complementado por M;*

(b) *$Soc(G) = S$ onde S é um subgrupo normal minimal não abeliano de G que é suplementado por M;*

(c) *$Soc(G) = A \times B$ onde A e B são os dois únicos subgrupos normais minimais de G. A e B são não abelianos e ambos são complementados por M. Além disso $A = C_G(B)$, $B = C_G(A)$ e A, B e $AB \cap M$ são isomorfos como grupos, mas não são G-isomorfos.*

Veremos exemplos de cada tipo de grupo primitivo. Para grupos primitivos do tipo 1 veremos como exemplo o grupo afim de um grupo abeliano elementar, este caso abrange os grupos simétricos S_3 e S_4, os grupos da forma $C_p \rtimes C_{p-1}$ e consequentemente os diedrais D_{2n} com n primo. Para os grupos primitivos do tipo 2 veremos como exemplo os grupos simples não abelianos S, $Aut(L)$ onde L é uma potência de um grupo simples não abeliano S, qualquer grupo G tal que $L \leq G \leq Aut(L)$ com L normal minimal em G e o produto entrelaçado de grupos simétricos $S_n \wr S_m$ para $n \geq 5$. Para grupos primitivos do tipo 3 veremos o grupo $S \times S$, onde S é um grupo simples não abeliano e mais em geral o grupo

$$\delta_2(X) = \{(x_1, x_2) : x_1L = x_2L\},$$

onde X é um grupo primitivo do tipo 2 com socle L. Observe que $\delta_2(S) = S \times S$. Generalizando temos os grupos

$$\delta_n(X) = \{(x_1, x_2, \ldots, x_n) : x_1L = x_2L = \ldots = x_nL\},$$

onde X é um grupo primitivo do tipo 2 com socle L. Note que $\delta_n(X)$ não é um grupo primitivo para $n \geq 3$ por possuir n subgrupos normais minimais da forma

$$N_i = \{1\} \times \ldots \times \{1\} \times L \times \{1\} \times \ldots \times \{1\},$$

onde L aparece na i-ésima coordenada, $i = 1, \ldots, n$.

Dois fatores principais são ditos G-relacionados se eles são G-isomorfos ou se existe um quociente primitivo do tipo 3 de G onde cada subgrupo normal minimal do quociente é G-isomorfo, respectivamente, a um dos fatores principais. Note que os subgrupos normais minimais de $G = \delta_n(X)$ são G-relacionados. De fato,

$$\delta_n(X)/\{1\} \times \{1\} \times L \times \ldots \times L \cong \delta_2(X),$$

os subgrupos normais minimais de $\delta_2(X)$, $L \times \{1\}$ e $\{1\} \times L$, são G-isomorfos, respectivamente a N_1 e a N_2 e desta forma N_1 e N_2 são G-relacionados. Repetindo o processo obtemos que N_i e N_j são G-relacionados para todo $1 \leq i, j \leq n$. Por outro lado os fatores N_i não são G-isomorfos porque os seus centralizadores são dois a dois distintos.

Em [11] Lafuente definiu a coroa de um fator principal não abeliano H/K de um grupo finito G. Sejam $C = C_G(H/K)$, $R = HC$ e

$$\mathbb{E} = \{C\} \cup \{M_G \mid M <_{max} G, MH_1 = G, K_1 \leq H_1 \cap M, H/K \cong_G H_1/K_1\}.$$

Provaremos que

$$\mathbb{E} = \{C\} \cup \{E \trianglelefteq G \mid G/E \text{ é primitivo do tipo } 3, C/E \trianglelefteq_{min} G/E\},$$

e definimos a H/K-coroa de G como sendo R/S onde $S = \cap\mathbb{E}$. Neste sentido provaremos os seguintes resultados para fatores principais não abelianos de um grupo finito:

Proposição 4.17: ([11], Proposição 2.5) *Sejam G um grupo finito, H/K um fator principal não abeliano de G e R/S a H/K-coroa de G. Então $R/S = Soc(G/S)$.*

Corolário 4.21: ([11], Corolário 2.8) *Dois fatores principais de G definem a mesma coroa se, e somente se, são G-relacionados.*

Em [10], P. Jiménez-Seral e J. Lafuente introduzem o conceito de G-grupos G-equivalentes. Dois G-grupos A e B são G-equivalentes se existem um isomorfismo $\varphi : A \to B$ e um isomorfismo $\phi : GA \to GB$ tal que o diagrama abaixo comuta

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] \arrow[d, "\varphi"] & GA \arrow[r] \arrow[d, "\phi"] & G \arrow[r] \arrow[d, "1_G"] & 1 \\ 1 \arrow[r] & B \arrow[r] & GB \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

Onde GA e GB indicam os produtos semidiretos com a ação dada de G sobre, respectivamente, A e B. Denotaremos por $A \sim_G B$ quando A e B forem G-equivalentes. É fácil mostrar que $\sim_G$ é uma relação de equivalência. Veremos que se dois G-grupos são G-isomorfos então eles são G-equivalentes. Por outro lado veremos um exemplo de dois G-grupos G-equivalentes que não são G-isomorfos. Se A é um G grupo definimos

$$I_G(A) = \{g \in G : g \text{ induz um automorfismo interno em } A\}.$$

Iremos mostrar que se $A \sim_G B$ então $I_G(A) = I_G(B)$. Neste sentido provaremos o seguinte resultado, onde $\mathcal{CF}(G)$ é o conjunto dos fatores principais de G

Proposição 4.10: ([10], Proposição 1.4) *Sejam F_1, F_2 dois fatores principais de um grupo finito G. Então as seguintes afirmações são equivalentes:*

1. $F_1 \sim_G F_2$.
2. *F_1 e F_2 são G-relacionados.*
3. *Ou $F_1 \cong_G F_2$ ou existe $E_i \in \mathcal{CF}(G)$ tal que $F_i \cong_G E_i$, $i = 1, 2$, e E_1 e E_2 possuem um complemento em comum em G que é um subgrupo maximal em G.*
4. *Ou $F_1 \cong_G F_2$ ou existe $E_i \in \mathcal{CF}(G)$ tal que $F_i \cong_G E_i$, $i = 1, 2$, e E_1 e E_2 possuem um complemento em comum em G.*

Com isso dois fatores principais são G-equivalentes se, e somente se, são G-relacionados.

Seja H/K um fator principal de um grupo finito G. Provaremos que $I = I_G(H/K) = HC_G(H/K)$. Com isso em [10], P. Jiménez-Seral e J. Lafuente generalizam o conceito de coroa definindo

$$D = D_G(H/K) = \bigcap\{T \trianglelefteq G : T \leq I, I/T \sim_G H/K, I/T \nsubseteq \Phi(G/T)\},$$

e a H/K-coroa de G como sendo o quociente I/D. Esta generalização do conceito de coroa abrange os casos de fatores principais de um grupo solúvel e de fatores principais não abelianos.

Se $A = H/K$ é um fator principal não abeliano de G e $I/D = Soc(G/D)$ é a coroa de A veremos que cada fator da coroa é G-equivalente a A. Com isso a ideia da coroa de um fator principal A é juntar todos os fatores G-equivalentes a A no socle de um oportuno quociente de G, e isso permite ter um controle sobre a classe de equivalência de A. Denotamos por $\delta_G(A)$ o número de fatores da coroa. Desta forma I/D é um produto direto de $\delta_G(A)$ subgrupos normais minimais G-equivalentes a A. Se $\delta_G(A) = 1$ veremos que o fator principal A pode ser ou não complementado.

Um fator principal de G é dito m-complementado se é complementado por um subgrupo maximal de G. Neste sentido finalizaremos nosso trabalho mostrando que fixado A um fator principal não abeliano de um grupo finito G, se $\delta_G(A) > 1$ então todos os subgrupo normais minimais de G/S são m-complementados, onde $S = D_G(A)$.

Pensando na pergunta 1, o próximo passo de nossos estudos seria mostrar que dadas duas séries principais de um grupo finito G, o número de fatores principais m-complementados é o mesmo para as duas séries. Esse resultado, provado por J. Lafuente, é o item (iii) do Teorema 2.1 de *Maximal subgroups and the Jordan-Hölder Theorem* [12].

Capítulo 1

Preliminares

1.1 Ação de grupos

Antes de definirmos grupos primitivos vamos apresentar alguns conceitos básicos de ações de grupos. Seja G um grupo. Dizemos que G age a direita no conjunto X se é dada uma função $X \times G \to X$, $(x, g) \mapsto xg$ com as seguintes propriedades:

(i) $x1 = x$, para todo $x \in X$;

(ii) $(xg)h = x(gh)$, para todos $x \in X$ e para todo $g, h \in G$.

Da mesma forma pode-se definir G agindo no conjunto X à esquerda. Aqui iremos considerar todas as ações à direita. Dado $x \in X$ defina por

$$G_x = Stab(x) = \{g \in G : xg = x\} \leq G$$

o estabilizador de x e

$$O_G(x) = \{xg : g \in G\} \subseteq X$$

a G-órbita de x. A ação é dita ser transitiva se existe $x \in X$ tal que $O_G(x) = X$, isto é, se existe apenas uma G-órbita.

Proposição 1.1 (Princípio da contagem) *Se G age sobre X e $x \in X$ então*

$$[G : G_x] = |O_G(x)|\,.$$

Em particular, se a ação for transitiva então $O_G(x) = X$ e então $|X| = [G : G_x]$.

Demonstração: Queremos construir uma bijeção entre o conjunto

$$(G : G_x) = \{G_x g : g \in G\}$$

das classes laterais à direita de G_x em G e o conjunto $O_G(x)$. Defina

$$f : (G : G_x) \to O_G(x),$$

dada por $G_xg \mapsto xg$. Vamos mostrar que f é bem definida. Se $G_xg = G_xh$ então $gh^{-1} \in G_x$, assim $xgh^{-1} = x$. Então $xg = xh$, desta forma $f(G_xg) = f(G_xh)$ e f é bem definida. Além disso f é injetiva, pois se $xg = xh$, então $gh^{-1} \in G_x$, logo $G_xg = G_xh$, e f é sobrejetiva, pois se $xg \in O_G(x)$, então $xg = f(O_xg)$. Desta forma f é uma bijeção. ■

Se a ação for transitiva, temos $O_G(x) = X$ e a bijeção construída na proposição acima determina uma equivalência entre a ação de G sobre X e a sua ação no conjunto das classes laterais à direita de G_x por multiplicação à direita. De fato, vimos que $f : (G : G_x) \to X$ dada por $f(G_xg) = xg$ é bem definida e bijetiva. Assim $f^{-1} : X \to (G : G_x)$ dada por $f^{-1}(xg) = G_xg$ é tal que

$$f^{-1}((xg)h) = f^{-1}(x(gh)) = G_x(gh) = (G_xg)h = (f^{-1}(xg))h,$$

para todo $h \in G$.

Uma ação de G sobre X pode ser vista como um homomorfismo

$$\begin{aligned} \gamma : G &\longrightarrow Sym(X) \\ g &\longmapsto \quad \gamma_g : X \longrightarrow X \\ &\qquad\qquad x \longmapsto xg^{-1}. \end{aligned}$$

De fato, se G age sobre X a função $\gamma_g : X \to X$ é bijetiva, sendo $\gamma_{g^{-1}}$ sua inversa, já que $\gamma_g\gamma_{g^{-1}}x = \gamma_g(xg) = xgg^{-1} = x$ e $\gamma_{g^{-1}}\gamma_g(x) = \gamma_{g^{-1}}(xg^{-1}) = xg^{-1}g = x$. Logo $\gamma_g \in Sym(X)$. Além disso γ é um homomorfismo de grupos, pois se $x \in X$ e $g, h \in G$,

$$\gamma_{gh}(x) = x(gh)^{-1} = x(h^{-1}g^{-1}) = (xh^{-1})g^{-1} = \gamma_g(xh^{-1}) = \gamma_g(\gamma_h(x)),$$

isto é, $\gamma_{gh} = \gamma_g\gamma_h$. Por outro lado, se é dado um homomorfismo

$$\begin{aligned} \gamma\colon G &\longrightarrow Sym(X) \\ g &\longmapsto \gamma_g, \end{aligned}$$

podemos definir uma ação de G em X com a função

$$\begin{aligned} X \times G &\longrightarrow X \\ (x, g) &\longmapsto x\gamma_g. \end{aligned}$$

Esta função define uma ação pois $x(\gamma_g\gamma_h) = x\gamma_{gh}$, já que γ é um homomorfismo.

O núcleo de uma ação de G sobre X é por definição igual ao núcleo do homomorfismo $G \to Sym(X)$ correspondente. Uma ação é dita fiel se seu núcleo é trivial. Seja $\gamma : G \to Sym(X)$ o homomorfismo correspondente a uma ação de G sobre X. O núcleo da ação será então

$$\mathrm{Ker}(\gamma) = \{g \in G : \gamma_g = id_X\} = \{g \in G : \gamma_g(x) = x, \forall x \in X\} =$$
$$\{g \in G : xg = x, \forall x \in X\} = \bigcap_{x \in X} G_x.$$

Logo o núcleo de uma ação é igual à interseção dos estabilizadores.

Definição 1.2 *Seja G um grupo agindo sobre um conjunto X. Um subconjunto $B \subseteq X$ é dito um bloco de imprimitividade se $\forall\ g \in G$ temos $Bg = B$ ou $Bg \cap B = \emptyset$.*

A partir de agora nos referiremos aos blocos de imprimitividade apenas como blocos. Dado um grupo G agindo sobre um conjunto X, os exemplos triviais de blocos são $\emptyset$, X e qualquer subconjunto com um único elemento $\{x\}$, para qualquer $x \in X$. Em particular, qualquer órbita de G é um bloco. Se B é um bloco, então Bg também é um bloco para todo $g \in G$, esses blocos são chamados de translados de B e eles formam uma partição em X, mais ainda $|B| = |Bg|$ para todo $g \in G$ e assim $|B|$ divide $|X|$ se $|X|$ é finito.

Exemplo 1.1 *Considere $\sigma = (123456)$, $G = \langle \sigma \rangle < S_6$, $X = \{1,2,3,4,5,6\}$ e ação de G sobre X sendo a ação natural.*

Temos $\sigma^2 = (135)(246)$, $\sigma^3 = (14)(25)(36)$, $\sigma^4 = (153)(264)$, $\sigma^5 = (165432)$ e $\sigma^6 = 1$.

Seja $B_1 = \{1,3,5\}$. Vamos calcular $B_1 g$, para todo $g \in G$.

$$B_1\sigma = \{2,4,6\} = B_1\sigma^3 = B_1\sigma^5 \text{ e } B_1\sigma^2 = \{1,3,5\} = B_1\sigma^4 = B_1.$$

Assim para todo $g \in G$, $B_1 g = B_1$ ou $B_1 g \cap B_1 = \emptyset$. Logo B_1 é um bloco de X. Observe que B_1 e $B_1\sigma$ formam uma partição em X.

Seja agora $B_2 = \{1,4\}$. Vamos calcular $B_2 g$, para todo $g \in G$.

$$B_2\sigma = \{2,5\} = B_2\sigma^3,\ B_2\sigma^2 = \{3,6\} = B_2\sigma^5 \text{ e } B_2\sigma^3 = \{1,4\} = B_2.$$

Assim para todo $g \in G$, $B_2 g = B_2$ ou $B_2 g \cap B_2 = \emptyset$. Logo B_2 é um bloco de G. Observe que B_2, $B_2\sigma$ e $B_2\sigma^2$ formam uma partição em X.

Como $|X| = 6$ e $|B|$ divide $|X|$, os blocos obtidos acima junto com os blocos triviais são os únicos blocos de imprimitividade da ação dada.

Proposição 1.3 *Sejam G um grupo agindo sobre um conjunto X e $x \in X$. Se a ação é transitiva, então existe uma bijeção*

$$\{ \text{ bloco } B \text{ de } X : x \in B \ \} \to \{ \ H \leq G : G_x \leq H \ \}$$

que preserva relação de inclusão.

Demonstração: Dado um bloco B em X tal que $x \in B$, então $G_B = \{g \in G : Bg = B\}$ é um subgrupo de G. De fato, se $g, h \in G_B$ obtemos $B(gh) = (Bg)h = Bh = B$ e $B = B(gg^{-1}) = (Bg)g^{-1} = Bg^{-1}$, ou seja, $gh, g^{-1} \in G_B$. Seja agora $g \in G_x$, vamos mostrar que $g \in G_B$. Como $g \in G_x$ temos $xg = x$, assim $x \in B \cap B_g$ o que implica que $B \cap B_G \neq \emptyset$. Como B é um bloco temos então que $B = B_g$ e assim $g \in G_B$. Logo $G_x \leq G_B$.

Reciprocamente, se H é um subgrupo de G contendo G_x, então o conjunto $B = \{xh : h \in H\}$ é um bloco de X. De fato, suponha que dado $g \in G$ temos $Bg \cap B \neq \emptyset$. Então existe $y \in Bg \cap B$ de forma que $y = xh_1$ e $y = xh_2g$, com $h_1, h_2 \in H$. Assim $xh_1 = xh_2g$ e então $x = xh_2gh_1^{-1}$. Portanto $h_2gh_1^{-1} \in G_x \leq H$, ou seja $h_2gh_1^{-1} = h_3 \in H$. Portanto $g \in H$ o que implica que $Bg = \{(xh)g : h \in H\} = \{x(hg) : h \in H\} = B$, pois $hg \in H$. Logo $Bg = B$ ou $Bg \cap B = \emptyset$. Além disso, como $1 \in H$ temos que $x = x1 \in B$. ∎

Definição 1.4 *Seja H um subgrupo de um grupo G. Definimos o core de H em G como*

$$H_G = \bigcap_{g \in G} H^g = \bigcap_{g \in G} g^{-1}Hg.$$

Temos que H_G é o maior subgrupo normal de G contido em H.

Definição 1.5 *Seja G um grupo agindo transitivamente sobre um conjunto X. Se a ação não possui blocos além dos triviais, então esta ação é dita primitiva.*

Teorema 1.6 *Sejam G um grupo, X um conjunto com G agindo transitivamente sobre X e $H = G_x \leq G$ o estabilizador de $x \in X$. São equivalentes:*

1. *A ação de G sobre X é primitiva e fiel;*

2. *H é um subgrupo maximal de G e o core de H em G é trivial.*

Demonstração: $1 \Rightarrow 2$. Suponha que a ação de G sobre X é primitiva e fiel. Como a ação de G em X é transitiva, essa ação é equivalente a ação de G no conjunto das classes laterais a direita de G_x em G. Seja agora $g \in G_x$, isto é $xg = x$. Dado qualquer $l \in G$, $(xl)g^l = (xl)l^{-1}gl = (xg)l = xl \in X$. Desta forma $g^l \in G_{xl}$, isto é, $G_x^l \subseteq G_{xl}$. Por outro lado se $g \in G_{xl}$ então $xlg = xl$ e assim $xlgl^{-1} = x$. Então $lgl^{-1} \in G_x$ e logo $g \in l^{-1}G_xl = G_x^l$. Portanto $G_{xl} \subseteq G_x^l$ e então $G_x^l = G_{xl}$. Assim o core de G_x é tal que

$$(G_x)_G = \bigcap_{l \in G} G_x^l = \bigcap_{x \in X} G_x = 1,$$

onde na última igualdade usamos que o núcleo da ação é igual a interseção dos estabilizadores e que a ação é fiel. Pela Proposição 1.3, se K é um subgrupo de G contendo G_x, existe um bloco $B = \{xk : k \in K\}$ de X tal que $x \in B$ e $K = G_B = \{g \in G : Bg = B\}$. Como G não possui blocos não triviais, ou $B = \{x\}$ ou $B = X$. Se $B = \{x\}$, então $G_x = K$ e se $B = X$ então $K = G$. Logo o estabilizador G_x é um subgrupo maximal com core trivial em G.

$2 \Rightarrow 1$. Se H é um subgrupo maximal com core trivial em G, então a ação de G no conjunto das classes laterais à direita de H é fiel e transitiva. Pela maximalidade de H, essa ação não possui blocos não triviais pela Proposição 1.3. ∎

1.2 Subgrupos Normais minimais

O objetivo desta seção é mostrar que um subgrupo normal minimal de um grupo finito é um produto direto de um número finito de cópias de um grupo simples. Esta seção foi baseada no livro *A Course in the Theory of Groups* [16].

Definição 1.7 *Sejam G um grupo e $\{1\} \neq N \leq G$. N é dito ser um subgrupo normal minimal de G se N é normal em G e se para qualquer subgrupo normal K de G com $K \leq N$ temos $K = N$ ou $K = \{1\}$.*

Se N é um subgrupo normal minimal de G e $\alpha \in Aut(G)$ então N^α é um subgrupo normal minimal de G. De fato, $N^\alpha \trianglelefteq G$ e se $K \leq N^\alpha$ com $K \trianglelefteq G$, então $K^{\alpha^{-1}} \leq N$ e $K^{\alpha^{-1}} \trianglelefteq G$. Como N é um subgrupo normal minimal, temos $K^{\alpha^{-1}} = 1$ ou $K^{\alpha^{-1}} = N$. Desta forma $K = (K^{\alpha^{-1}})^\alpha = 1$ ou $K = (K^{\alpha^{-1}})^\alpha = N^\alpha$ o que implica que N^α é um subgrupo normal minimal de G. Além disso, $N \cong N^\alpha$, já que α restrita a N possui núcleo trivial e imagem N^α.

Definição 1.8 *Um grupo não trivial G é dito caracteristicamente simples se os únicos subgrupos característicos de G são G e $\{1\}$.*

Vamos denotar por $K \trianglelefteq_c G$ quando K for um subgrupo característico de G. Observe que $K \trianglelefteq_c N \trianglelefteq G$ implica $K \trianglelefteq G$.

Proposição 1.9 *Sejam G um grupo e N um subgrupo normal minimal de G. Então N é um grupo caracteristicamente simples.*

Demonstração: Seja L um subgrupo característico de N. Então $L \trianglelefteq_c N \trianglelefteq G$ o que implica que $L \trianglelefteq G$. Portanto, como $L \leq N$ e N é um subgrupo normal minimal de G, obtemos que $L = N$ ou $L = \{1\}$. Logo N é um grupo caracteristicamente simples. ■

Definição 1.10 *Seja G um grupo abeliano. Dizemos que G é um (p-)grupo abeliano elementar se $g^p = 1$, $\forall g \in G$, para algum primo p.*

Seja $(A, +)$ um grupo abeliano. Na notação aditiva, A é um grupo abeliano elementar se $pa = 0$, $\forall a \in A$.

Proposição 1.11 *Seja $(A, +)$ um grupo abeliano. São equivalentes:*

1. *A é abeliano elementar;*
2. *Existe um primo p e um espaço vetorial V sobre $\mathbb{Z}/p\mathbb{Z}$ tal que $A \cong V^+$, onde $V^+ = (V, +)$ é o grupo aditivo de V.*

Demonstração: Seja A um grupo abeliano elementar. Então existe um primo p tal que $pa = 0$, $\forall a \in A$. Definimos um espaço vetorial V sobre $\mathbb{Z}/p\mathbb{Z}$ como se segue. Os elementos de V são os elementos de A. A soma de dois vetores de V é definida como a soma de dois elementos de A. Sejam $\bar{n} \in \mathbb{Z}/p\mathbb{Z}$ e n um inteiro na classe residual $\bar{n}$. Então $\forall a \in V$ o produto por escalar $\bar{n}a$ é definido como o elemento $na \in A$. Este produto não depende da escolha de n na classe residual $\bar{n}$. De fato, se $m \equiv n \; mod \; p$, existe um inteiro s tal que $m = n + ps$. Assim

$$ma = (n + ps)a = na + psa = na,$$

já que $sa \in A$ e $pa = 0$, $\forall a \in A$. Agora é fácil checar que V é um espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$. Desta forma, como grupos,

$$A \cong V^+.$$

Reciprocamente, seja V um espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$. Então V^+ é um grupo abeliano. Mais ainda, como $pv = 0$ para todo $v \in V$, V^+ é um grupo abeliano elementar. Portanto, como $A \cong V^+$, obtemos que A é abeliano elementar. ■

Proposição 1.12 *Seja $(A, +)$ um grupo abeliano finito, $A \neq \{0\}$. Então A é caracteristicamente simples se, e somente se, A é abeliano elementar.*

Demonstração: Suponha que A é caracteristicamente simples. Seja p um primo divisor de $|A|$ e seja

$$B = \{a \in A : pa = 0\}.$$

Como A é abeliano, temos $B \leq A$. Sejam $b \in B$ e $\alpha \in Aut(A)$. Então

$$p(\alpha(b)) = \alpha(b) + \ldots + \alpha(b) = \alpha(pb) = \alpha(0) = 0.$$

Logo $\alpha(b) \in B$. Desta forma B é um subgrupo característico de A. Pelo Teorema de Cauchy, existe um elemento $a \neq 0$ em A com ordem p. Então $0 \neq a \in B$. Desta forma $B \neq \{0\}$. Como A é caracteristicamente simples segue que $B = A$. Logo A é abeliano elementar.

Reciprocamente, suponha que A é abeliano elementar. Pela Proposição 1.11, podemos supor que $A = V^+ = (V, +)$, onde V é um espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$ para algum primo p. Como A é finito, V possui dimensão finita. Suponha que W é um subgrupo não-trivial característico de V^+ e seja $0 \neq w \in W$. Seja $0 \neq v \in V^+$. Então v e w são elementos de bases de V. Desta forma existe uma transformação linear inversível $T : V \to V$ tal que $v = T(w)$. Então como $T \in Aut(V^+)$ e W é característico em V^+, obtemos que $v \in W$. Logo $W = V^+$. Portanto V^+ é caracteristicamente simples. ■

Proposição 1.13 *Sejam G um grupo, $N_1, \ldots, N_n$ subgrupos normais minimais de G e $N = N_1 N_2 \ldots N_n$. Então existe um subconjunto $\{i_1, \ldots, i_m\}$ de $\{1, \ldots, n\}$ tal que $N = \prod_{j=1}^{m} N_{i_j}$, isto é, é o produto direto de $N_{i_1}, \ldots, N_{i_m}$.*

Demonstração: Seja I o conjunto de todos os subconjuntos não-vazios $\{i_1, \ldots, i_m\}$ de $\{1, \ldots, n\}$ tal que $i_1, \ldots, i_m$ são distintos e $N_{i_1}N_{i_2}\ldots N_{i_m} = \prod_{j=1}^{m} N_{i_j}$. Trivialmente, $\{j\} \in I$ para cada $j = 1, \ldots, n$.

Agora escolha $\{i_1, \ldots, i_m\} \in I$ com m maior possível e seja $L = N_{i_1}\ldots N_{i_m} = \prod_{j=1}^{m} N_{i_j}$.

Temos que N e L são subgrupos normais de G e $L \leq N$. Se $N \neq L$, então existe um inteiro $l \in \{1, \ldots, n\}$ tal que $N_l \nleq L$. Como N_l é normal minimal e $L \trianglelefteq G$ segue que $N_l \cap L = \{1\}$. Desta forma $N_lL \trianglelefteq G$ e $N_lL = N_l \times L$.

Seja $i_{m+1} = l$. Como $N_{i_j} \leq L$, para $j = 1, \ldots, m$, obtemos que i_{m+1} é distinto de $i_1, \ldots, i_m$ e

$$N_{i_1}\ldots N_{i_m}N_{i_{m+1}} = LN_l = L \times N_l = \prod_{j=1}^{m+1} N_{i_j}.$$

Então $\{i_1, \ldots, i_m, i_{m+1}\} \in I$. Mas isso contradiz a escolha de m. Logo $N = L$ e isso completa a prova da proposição. ■

Definição 1.14 *Um grupo G é dito ser completamente redutível se ou $G = \{1\}$ ou G é um produto direto de um número finito de grupos simples.*

Em particular, todo grupo simples é completamente redutível.

Lema 1.15 *Seja G um grupo finito não trivial. Suponha que G é um grupo completamente redutível, $G = \prod_{j=1}^{n} N_j$, onde, para cada $j = 1, \ldots, n$, N_j é um subgrupo simples normal de G. Se N_j é não abeliano, para todo $j = 1, \ldots, n$, então $N_1, \ldots, N_n$ são os únicos subgrupos normais minimais de G.*

Demonstração: Para cada $j = 1, \ldots, n$, N_j é um subgrupo normal simples de G, logo N_j é normal minimal em G.

Suponha por contradição que existe um subgrupo L normal minimal de G distinto dos $N_1, \ldots, N_n$. Então, para cada $j = 1, \ldots, n$,

$$N_j \cap L = 1,$$

e, como N_j e L são normais em G, obtemos que $[N_j, L] \leq N_j \cap L = 1$. Portanto, para cada $j = 1, \ldots, n$, $N_j \leq C_G(L)$. Então

$$C_G(L) \geq N_1N_2\ldots N_n = G,$$

isto é

$$L \leq Z(G) = Z(N_1) \times \ldots \times Z(N_n) = 1,$$

uma contradição. Então $N_1, \ldots, N_n$ são os únicos subgrupos normais minimais de G. ■

Teorema 1.16 *Seja G um grupo finito não trivial. Então G é caracteristicamente simples se, e somente se, G é um produto direto de um número finito de cópias de um grupo simples.*

Demonstração: Suponha que G é caracteristicamente simples. Seja N_1 um subgrupo normal minimal de G. Para cada $\alpha \in Aut(G)$, N_1^α é um subgrupo normal minimal de G e $N_1^\alpha \cong N_1$. Como G é finito, existe um número finito de subgrupos distintos de G da forma N_1^α com $\alpha \in Aut(G)$, digamos n deles: $N_1, \ldots, N_n$. Seja

$$N = N_1 N_2 \ldots N_n.$$

Agora seja $\gamma \in Aut(G)$. Para cada $j \in \{1, \ldots, n\}$, $N_j = N_1^\alpha$ para algum $\alpha \in Aut(G)$. Como $\alpha\gamma \in Aut(G)$, $N_j^\gamma = N_1^{\alpha\gamma} = N_l$ para algum $l \in \{1, \ldots, n\}$. Mais ainda, se $i, j \in \{1, \ldots, n\}$, com $i \neq j$, então $N_i^\gamma \neq N_j^\gamma$. Desta forma $\{N_1^\gamma, \ldots, N_n^\gamma\} = \{N_1, \ldots, N_n\}$, e portanto

$$N^\gamma = N_1^\gamma N_2^\gamma \ldots N_n^\gamma = N_1 N_2 \ldots N_n = N.$$

Como $N^\gamma = N$ para qualquer $\gamma \in Aut(G)$, obtemos que $N \trianglelefteq_c G$. Como $1 < N_1 \leq N$ e G é caracteristicamente simples segue que $N = G$.

Pela Proposição 1.13, segue que G é um produto direto de alguns dos subgrupos $N_1, \ldots, N_n$. Vamos fixar a notação

$$G = \prod_{j=1}^{m} N_j,$$

onde $m \leq n$.

Agora qualquer subgrupo normal de N_1 é normal em G. Logo, como N_1 é normal minimal, segue que N_1 é simples. Sendo $N_j \cong N_1$ para cada $j = 1, \ldots, m$, G é um produto direto de m cópias isomorfas ao grupo simples N_1.

Reciprocamente, suponha que G é um produto direto de m cópias de grupos isomorfos a N_1, onde m é um inteiro positivo e N_1 é um grupo simples. Desta forma

$$G = \prod_{j=1}^{m} N_j,$$

onde para cada $j = 1, \ldots, m$, $N_j \cong N_1$.

Se N_1 é abeliano, então $|N_1| = p$, para algum primo p. Assim $|N_j| = p$, para cada $j = 1, \ldots, m$, e G é um grupo abeliano elementar de ordem p^m. Como visto na Proposição 1.12, G é caracteristicamente simples.

Se N_1 não é abeliano então G é um produto direto de grupos simples não abelianos e $Z(G) = 1$. Seja N um subgrupo característico não trivial de G. Então N contém um subgrupo normal minimal de G e então, pelo Lema 1.15, $N \geq N_i$, para algum $i \in \{1, \ldots, m\}$. Sem perda de generalidade, podemos supor que $N \geq N_1$.

Se $m \geq 2$, seja $j \in \{2, \ldots, m\}$. Existe um isomorfismo

$$\varphi : N_1 \to N_j.$$

Cada elemento de G possui uma expressão única da forma $n_1 n_2 \ldots n_m$, com $n_i \in N_i$ para cada $i = 1, \ldots, m$. Então podemos definir uma aplicação $\alpha : G \to G$ dada por

$$\alpha : n_1 n_2 \ldots n_{j-1} n_j n_{j+1} \ldots n_m \mapsto n_j^{\varphi^{-1}} n_2 \ldots n_{j-1} n_1^{\varphi} n_{j+1} \ldots n_m$$

para todo $n_1 \in N_1$, ..., $n_m \in N_m$. Desta forma, α é um automorfismo de G com

$$N_1^{\alpha} = N_j.$$

Como N é característico em G, $N = N^{\alpha} \geq N_1^{\alpha} = N_j$. Então $N \geq N_j$, para todo $j = 1, \ldots, m$, e $N \geq N_1 \ldots N_m = G$. Logo $N = G$, assim os únicos subgrupos característicos de G são G e $\{1\}$, ou seja, G é caracteristicamente simples. ■

Segue do teorema acima que todo grupo finito caracteristicamente simples é completamente redutível. Por outro lado, sem a hipótese do grupo G ser finito o teorema pode não ser verdadeiro. Por exemplo, seja F um corpo e considere $F^+ = (F, +)$ o grupo aditivo de F. O grupo abeliano F^+ é caracteristicamente simples. De fato, seja

$$\lambda_a : F^+ \to F^+$$

dada por $\lambda_a(x) = ax$, com $0 \neq a \in F$ e $x \in F^+$. Como F é um corpo temos que $\lambda_a(x+y) = a(x+y) = ax + ay = \lambda_a(x) + \lambda_a(y)$, com $x, y \in F^+$ e $(\lambda_a)^{-1} = \lambda_{a^{-1}}$. Portanto $\lambda_a \in Aut(F^+)$. Além disso $\lambda_a(x) = ax = xa$. Seja então $K \leq F^+$ com $K \trianglelefteq_c F$. Temos $K = K^{\lambda_a}$ e portanto $\lambda_a(k) = ak \in K$, $\forall a \in F$ e $\forall k \in K$. Então $\lambda_{k^{-1}}(k) = k^{-1}k = 1 \in K$. Portanto $\lambda_a(1) = a1 = a \in K$, $\forall a \in F$. Assim $F^+ \leq K \leq F^+$, ou seja, $K = F^+$. Logo F^+ é caracteristicamente simples.

Considerando $F = \mathbb{Q}$, temos então que $(\mathbb{Q}, +)$ é caracteristicamente simples. Por outro lado $(\mathbb{Q}, +)$ não é um produto direto de cópias de um grupo simples. De fato, suponha que $\mathbb{Q}$ é um produto direto de grupos simples isomorfos a um dado grupo simple S. Então S é um grupo simples abeliano e logo é finito de ordem prima, isto é, $(\mathbb{Q}, +) \cong \prod \mathbb{Z}/p\mathbb{Z}$, onde p é um número primo. Considere uma projeção $f : (\mathbb{Q}, +) \to \mathbb{Z}/p\mathbb{Z} = \langle \overline{1} \rangle$. Como f é sobrejetiva, existe $a \in \mathbb{Q}$ tal que $f(a) = \overline{1}$. Temos então que $\overline{1} = f(a) = f(ap/p) = pf(a/p) = \overline{0}$, absurdo. Desta forma existem grupos infinitos abelianos caracteristicamente simples que não são produto direto de cópias de um grupo simples.

Seja então N um subgrupo normal minimal de um grupo finito G. Na Proposição 1.9, vimos que N é caracteristicamente simples. O Teorema 1.16 mostra que N é um produto direto de um número finito de cópias de um grupo simples, isto é, $N \cong S^n$, com S um grupo simples. Mais ainda, pela Proposição 1.12, se N é abeliano então N é um grupo abeliano elementar, isto é, $N \cong C_p^n$, com p primo e n um inteiro positivo. No caso em que G é um grupo solúvel temos S isomorfo a um subgrupo de G implicando então que S é solúvel. Então o subgrupo derivado $S' \neq S$ e como S é simples, $S' = \{1\}$. Portanto S é abeliano e então $S \cong C_p$ com p primo. Logo um subgrupo normal minimal N de um grupo solúvel finito G é um grupo abeliano elementar.

1.3 Automorfismos internos e Ω-grupos

Seja G um grupo. Dado $g \in G$, a aplicação

$$\begin{aligned} \rho_g \colon G &\longrightarrow G \\ h &\longmapsto h^g = g^{-1}hg, \end{aligned}$$

para todo $h \in G$ é um automorfismo de G. A aplicação ρ_g é dita um automorfismo interno induzido por g. Um automorfismo α de G é dito interno se $\alpha = \rho_g$ para algum $g \in G$. O conjunto de todos os automorfismos internos de G é denotado por $Inn(G)$.

Dados $\alpha \in Aut(G)$ e $\rho_g \in Inn(G)$ temos que

$$h^{\alpha^{-1}\rho_g\alpha} = (g^{-1}h^{\alpha^{-1}}g)^\alpha = (g^{-1})^\alpha h g^\alpha = (g^\alpha)^{-1}g(g^\alpha) = h^{\rho_{g^\alpha}},$$

para todo $h \in G$. Desta forma $\alpha^{-1}\rho_g\alpha = \rho_{g^\alpha} \in Inn(G)$, ou seja, $Inn(G) \trianglelefteq Aut(G)$. O quociente $Aut(G)/Inn(G)$ é indicado como $Out(G)$ e chamado de grupo dos automorfismos externos de G.

Considere a aplicação

$$\begin{aligned} \rho \colon G &\longrightarrow Aut(G) \\ g &\longmapsto \rho_g, \end{aligned}$$

para todo $g \in G$. ρ é um homomorfismo de grupos, pois dados $g_1, g_2 \in G$, $h^{\rho_{g_1}\rho_{g_2}} = (g_1^{-1}hg_1)^{\rho_{g_2}} = g_2^{-1}g_1^{-1}hg_1g_2 = h^{\rho_{g_1g_2}}$, para todo $h \in G$, ou seja, $\rho_{g_1}\rho_{g_2} = \rho_{g_1g_2}$.

Além disso

$$\begin{gathered} \mathrm{Ker}(\rho) = \{g \in G : \rho_g = 1_G\} = \{g \in G : h^{\rho_g} = h, \forall h \in G\} = \\ \{g \in G : ghg^{-1} = h, \forall h \in G\} = \{g \in G : gh = hg, \forall h \in G\} = Z(G) \end{gathered}$$

e $\mathrm{Im}(\rho) = Inn(G)$. Pelo Teorema do Isomorfismo, $G/Z(G) \cong Inn(G)$.

Seja Ω um conjunto. Um grupo G é dito um Ω-grupo se existe, associado para cada elemento $\omega \in \Omega$, um endomorfismo de G denotado por

$$g \mapsto g^{\omega},$$

para todo $g \in G$. Um subgrupo H de G é dito Ω-admissível se $h^{\omega} \in H$ para quaisquer $h \in H$ e $\omega \in \Omega$. Se N é um subgrupo normal Ω-admissível de G, então o grupo quociente G/N pode ser visto como um Ω-grupo se definirmos

$$(Ng)^{\omega} = Ng^{\omega},$$

para todos $g \in G$ e $\omega \in \Omega$. Se G e H são Ω-grupos, um homomorfismo $\alpha : G \to H$ é dito um Ω-homomorfismo se

$$(g^{\omega})^{\alpha} = (g^{\alpha})^{\omega},$$

para todos $g \in G$ e $\omega \in \Omega$. Além disso, se α é bijetiva então dizemos que α é um Ω-isomorfismo.

Se $\Omega = \emptyset$, então todo grupo é um Ω-grupo e todo homomorfismo é um Ω-homomorfismo. Se $\Omega = End(G)$, então G é um Ω-grupo onde os endomorfismos de G operam em G de maneira natural. Da mesma forma, se $\Omega = Aut(G)$, G é um Ω-grupo e os subgrupos Ω-admissíveis são os subgrupos característicos de G e se $\Omega = Inn(G)$, G é um Ω-grupo e os subgrupos Ω-admissíveis são os subgrupos normais de G.

1.4 Séries e o Teorema de Jordan-Hölder

Seja G um Ω-grupo. Uma Ω-série em G é uma sequência finita de subgrupos G_i Ω-admissíveis, $0 \leq i \leq n$, tais que

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G.$$

Os subgrupos $G_0, G_1, \ldots, G_n$ são chamados de termos da série e os grupos quocientes G_i/G_{i-1}, $i = 1, \ldots, n$, são os fatores da série.

Considere o conjunto de todos as Ω-séries de um Ω-grupo G. Esse conjunto é não vazio por conter a série $\{1\} \trianglelefteq G$. Se $\mathcal{S}$ e $\mathcal{T}$ são Ω-séries de G, dizemos que $\mathcal{S}$ é um refinamento de $\mathcal{T}$ se todo termo de $\mathcal{S}$ é também um termo de $\mathcal{T}$. Se existe pelo menos um termo de $\mathcal{S}$ que não é um termo de $\mathcal{T}$, então $\mathcal{S}$ é um refinamento próprio de $\mathcal{T}$. Uma Ω-série que não possui refinamento próprio é dita uma Ω-série de composição.

Um Ω-grupo G é dito Ω-simples se $\{1\}$ e G são os únicos Ω-subgrupos normais de G. Pode-se provar que uma Ω-série é uma Ω-série de composição se, e somente se, todos os seus fatores são Ω-simples.

Duas Ω-séries $\mathcal{S}$ e $\mathcal{T}$ de um Ω-grupo G são ditas Ω-isomorfas se existe uma bijeção entre o conjunto dos fatores de $\mathcal{S}$ e o conjunto dos fatores de $\mathcal{T}$ tal que os fatores correspondentes são Ω-isomorfos.

Lema 1.17 (Lei Modular de Dedekind) *Seja G um grupo e sejam A, B e C subgrupos de G tais que $B \leq A$. Então*

$$A \cap BC = B(A \cap C)$$

(Aqui não estamos assumindo que BC e $B(A \cap C)$ são subgrupos de G).

Demonstração: Como $B \leq A$ e $A \cap C \leq A, C$ temos que $B(A \cap C) \subseteq A$ e $B(A \cap C) \subseteq BC$, desta forma $B(A \cap C) \subseteq A \cap BC$. Seja agora $a \in A \cap BC$. Então $a \in A$ e $a = bc$ para algum $b \in B$ e $c \in C$. Assim $c = b^{-1}a \in A \cap C$ pois $B \leq A$. Então $a = bc \in B(A \cap C)$. Logo $A \cap BC \subseteq B(A \cap C)$. Portanto $A \cap BC = B(A \cap C)$. ∎

Teorema 1.18 (Teorema de Jordan-Hölder, [14], 3.1.4) *Seja G um Ω-grupo e sejam*

$$1 = U_0 \trianglelefteq U_1 \trianglelefteq \ldots \trianglelefteq U_r = G$$
$$1 = V_0 \trianglelefteq V_1 \trianglelefteq \ldots \trianglelefteq V_s = G$$

duas Ω-séries de composição de G. Então $r = s$, e existe uma permutação $\pi \in Sym(r)$ tal que para cada $i = 1, \ldots, r$, o fator U_i/U_{i-1} é Ω-isomorfo a $V_{\pi(i)}/V_{\pi(i)-1}$.

Tomando $\Omega = Inn(G)$, os subgrupos Ω-admissíveis de G são os subgrupo normais de G e os subgrupos Ω-simples de G são os subgrupos normais minimais de G. Então a Ω-série de composição

$$1 = U_0 \trianglelefteq U_1 \trianglelefteq \ldots \trianglelefteq U_r = G$$

de G é tal que U_i/U_{i-1} é um subgrupo normal minimal de G/U_{i-1}, para cada $i = 1, \ldots, r$. A Ω-série de composição acima é dita uma série principal de G.

1.5 Subgrupos de Fitting e Frattini

Definição 1.19 *Sejam G um grupo finito e p um primo dividindo $|G|$. Defina*

$$O_p(G) = \bigcap \{P : P \in Syl_p(G)\},$$

onde $Syl_p(G)$ é o conjunto dos p-subgrupos de Sylow de G.

Pode-se mostrar que $O_p(G)$ é um subgrupo característico de G e que $O_p(G)$ é o maior p-subgrupo normal de G. Se p é um número primo, denotamos por p' o conjunto dos números primos diferentes de p.

Definição 1.20 *Sejam σ, π dois conjuntos de primos e G um grupo finito. O subgrupo característico $O_\pi(G)$ de G é definido como*

$$O_\pi(G) = \langle N : N \trianglelefteq G \text{ e } N \text{ é um } \pi\text{-grupo} \rangle .$$

O subgrupo $O_{\pi,\sigma}(G)$ é definido como

$$O_{\pi,\sigma}(G)/O_\pi(G) = O_\sigma(G/O_\pi(G)).$$

Definição 1.21 *Seja G um grupo. O subgrupo gerado por todos os subgrupos normais nilpotentes de G é chamado de subgrupo de Fitting de G e será denotado por $F(G)$.*

Teorema 1.22 (Fitting, [16], Teorema 7.63) *Sejam G um grupo e H, K dois subgrupos normais nilpotentes de G. Então HK é um subgrupo normal nilpotente de G.*

Pelo Teorema de Fitting, se G é um grupo finito, então $F(G)$ é o maior subgrupo normal nilpotente de G.

Lema 1.23 *Seja G um grupo finito. Se N é um subgrupo normal minimal de G então $F(G) \leq C_G(N)$. Mais ainda, se N é abeliano então $N \leq Z(F(G))$.*

Demonstração: Temos que o subgrupo derivado $N' \leq N$ e $N' \trianglelefteq G$. Como N é normal minimal em G obtemos que $N' = \{1\}$ ou $N' = N$.

Caso 1: $N' = \{1\}$. Neste caso, N é abeliano e assim $N \leq F(G)$. Desta forma $[F(G), N] \leq F(G) \cap N = N$. Temos que $[F(G), N] \trianglelefteq G$. Como N é normal minimal em G, temos que $[F(G), N] = \{1\}$ ou $[F(G), N] = N$. Considere a série central inferior $\gamma_i(F(G))$, $i \geq 1$, e suponha que $[F(G), N] = N \leq [F(G), F(G)] = \gamma_2(F(G))$. Temos que $[F(G), [F(G), N]] = [F(G), N] = N \leq [F(G), [F(G), F(G)]] = \gamma_3(F(G))$. Como $F(G)$ é nilpotente, existe $c \in \mathbb{N}$ tal que $\gamma_{c+1}(F(G)) = \{1\}$. Prosseguindo obtemos que

$$[F(G), [F(G), \ldots, [F(G), N] \ldots]] = N \leq \gamma_{c+1}(F(G)) = \{1\},$$

contradição. Assim $[F(G), N] = \{1\}$, o que implica que $F(G) \leq C_G(N)$ e como $N \leq F(G)$, temos que $N \leq Z(F(G))$.

Caso 2: $N' = N$. Neste caso N não pode ser nilpotente, pois não existe $c \in \mathbb{N}$ tal que $\gamma_{c+1}(N) = 1$. Desta forma, $N \nsubseteq F(G)$. Como $N \cap F(G) \trianglelefteq G$ e $N \cap F(G) \leq N$, obtemos que $N \cap F(G) = \{1\}$ ou $N \cap F(G) = N$. Se $N \cap F(G) = N$, obtemos $N \subseteq F(G)$, contradição. Logo $N \cap F(G) = \{1\}$. Assim $[N, F(G)] \leq N \cap F(G) = \{1\}$, o que implica que $F(G) \leq C_G(N)$. ∎

Definição 1.24 *Seja G um grupo finito. O subgrupo de Frattini $\Phi(G)$ de G é definido como $\{1\}$ quando $G = \{1\}$ e como*

$$\Phi(G) = \bigcap \{M : M \text{ é maximal em } G\},$$

quando $G \neq \{1\}$.

Temos que $\Phi(G)$ é um subgrupo característico de G.

Definição 1.25 *Sejam G um grupo e $M, N \leq G$. Se $G = MN$, dizemos que M é um suplemento para N em G. Se $G = MN$ e $M \cap N = \{1\}$, dizemos que M é um complemento para N em G.*

Teorema 1.26 *Seja G um grupo finito.*

(a) ([14], 5.2.12) *Seja $S \subseteq G$. Então $G = \langle S \rangle$ se, e somente se, $G = \langle S, \Phi(G) \rangle$;*

(b) ([16], 11.4) *Seja $N \trianglelefteq G$. Então N possui um suplemento distinto de G em G se, e somente se, N não é subgrupo de $\Phi(G)$;*

(c) ([14], 5.2.13 (ii) e (iii)) *Se $N \trianglelefteq G$, então $\Phi(N) \leq \Phi(G)$ e $\Phi(G)N/N \leq \Phi(G/N)$. Mais ainda, se $N \leq \Phi(G)$ então $\Phi(G/N) = \Phi(G)/N$.*

Teorema 1.27 *Seja G um grupo finito.*

(a) ([8], III, 3.6) *$\Phi(G)$ é nilpotente, em particular $\Phi(G) \leq F(G)$;*

(b) ([8], III, 4.2) *Se $N \trianglelefteq G$ e $N \leq \Phi(G)$ então $F(G/N) = F(G)/N$.*

Proposição 1.28 *Seja G um grupo finito. Se G é solúvel, então $\Phi(G) \neq F(G)$.*

Demonstração: G possui um subgrupo normal minimal. Como G é solúvel, esse subgrupo normal minimal é abeliano elementar, e desta forma ele está contido no subgrupo de Fitting de G, ou seja, $F(G) \neq \{1\}$. Agora, como $\Phi(G) \trianglelefteq G$ e G é solúvel, temos $G/\Phi(G)$ solúvel. Assim $F(G/\Phi(G)) \neq \Phi(G)/\Phi(G)$. Por outro lado, pelo Item (b) do Teorema 1.27, temos $F(G/\Phi(G)) = F(G)/\Phi(G)$. Logo $F(G) \neq \Phi(G)$. ∎

1.6 Anéis e módulos

Incluiremos nesta seção alguns fatos básicos sobre anéis e módulos que usaremos no Capítulo 3.

Definição 1.29 *Seja R um anel com unidade. Um R-módulo M é dito simples, ou irredutível, se os únicos submódulos de M são $\{0\}$ e M.*

Definição 1.30 *Seja R um anel com unidade. Um R-módulo M é dito semissimples, ou completamente redutível, se é uma soma direta de módulos simples.*

Definição 1.31 *Sejam R um anel com unidade, M um R-módulo e $N \subseteq M$ um submódulo de M. Dizemos que L é um complemento para N em M se $M = N + L$ e $N \cap L = \{0\}$.*

O próximo lema é um resultado conhecido da Teoria de Módulos.

Lema 1.32 *Seja M um R-módulo. Então M é semissimples se, e somente se, todo submódulo de M possui complemento em M.*

Proposição 1.33 *Seja M um R-módulo. Se M é semissimples, então todo submódulo de M é semissimples e todo quociente de M é semissimples.*

Demonstração: Seja $L \subseteq M$ um submódulo de M. Vamos mostrar que todo submódulo de L admite complemento em L. Se $K \subseteq L \subseteq M$ então K tem complemento C em M, isto é $M = C + K$ e $C \cap K = \{0\}$. Assim pela lei de Dedekind $(L \cap C) + K = L \cap (C + K) = L \cap M = L$ e $K \cap (L \cap C) = K \cap C = \{0\}$, isto é $L \cap C$ é um complemento de K em L. Logo L é semissimples.

Seja agora $N \leq M$. Como N é submódulo de M, N possui um complemento H em M. Desta forma $M/N \cong H$. Como H é semissimples, M/N é semissimples. ∎

Lema 1.34 (Schur) *Se $f : A \to B$ é um morfismo de módulos simples e $f \neq 0$, então f é isomorfismo.*

Demonstração: Como $\mathrm{Ker}(f) \subseteq A$ e A é simples então $\mathrm{Ker}(f) = A$ ou $\mathrm{Ker}(f) = \{0\}$. Como $f \neq 0$, temos $\mathrm{Ker}(f) \neq A$. Assim $\mathrm{Ker}(f) = \{0\}$. Como $\mathrm{Im}(f) \subseteq B$ e B é simples, então $\mathrm{Im}(f) = B$ ou $\mathrm{Im}(f) = \{0\}$. Como $f \neq 0$, temos $\mathrm{Im}(f) = B$. Logo f é isomorfismo. ∎

Seja $(A, +, \cdot)$ um anel com unidade 1. Dizemos que A é um anel de divisão quando para todo $a \in A \backslash \{0\}$ existe $a^{-1} \in A \backslash \{0\}$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Teorema 1.35 (Wedderburn, [9] página 453) *Um anel de divisão finito é um corpo.*

Definição 1.36 *Seja K um corpo e A um anel unitário. A é uma K-álgebra se existe um homomorfismo de anéis*

$$\varphi : K \to A$$

tal que $\varphi(K) \subseteq Z(A)$. Com isso A tem uma estrutura de espaço vetorial sobre K onde a multiplicação por escalar é dada por

$$\lambda v = \varphi(\lambda) v,$$

para $\lambda \in K$ e $v \in A$.

Definição 1.37 (Álgebra de grupo) *Seja G um grupo finito (com notação multiplicativa) e K um corpo. A álgebra de grupo KG consiste do conjunto de todas as combinações lineares formais $\sum\limits_{g \in G} m_g g$, com escalares $m_g \in K$. O conjunto KG é então visto como um espaço vetorial sobre K com base $\{g : g \in G\}$, e multiplicação definida estendendo a multiplicação em G da forma*

$$\left(\sum_{g \in G} m_g g \right) \left(\sum_{h \in G} n_h h \right) = \sum_{g,h \in G} m_g n_h gh,$$

com $m_g, n_h \in K$ e $g, h \in G$.

Temos que KG é um anel com unidade que contém K no seu centro. Mais ainda, KG é uma K-álgebra.

Capítulo 2

G-grupos e Grupos primitivos

2.1 G-grupos e G-isomorfismos

Dados dois grupos A e G, o grupo A é dito um G-grupo se é dado um homomorfismo

$$\begin{aligned} \gamma : G &\longrightarrow Aut(A) \\ g &\longmapsto \theta(g) : A \longrightarrow A \\ & \qquad\qquad\quad a \longmapsto a^g. \end{aligned}$$

para quaisquer $g \in G$ e $a \in A$.

O centralizador de A em G é dado por

$$C_G(A) = \{g \in G : a^g = a, \ \forall a \in A\} = \mathrm{Ker}(\theta).$$

Observe que se $N \trianglelefteq G$ então N é um G-grupo com θ sendo a ação de conjugação de G em N.

Dois G-grupos A e B são ditos G-isomorfos, denotado por $A \cong_G B$, se existe um isomorfismo $\varphi : A \to B$ tal que $(a^g)^\varphi = (a^\varphi)^g$, para quaisquer $a \in A$, $g \in G$. Neste caso dizemos que φ é um G-isomorfismo.

Note que se $\varphi : A \to B$ é um G-isomorfismo, então $\varphi^{-1} : B \to A$ também é um G-isomorfismo. De fato, sejam $a \in A$, $b \in B$ tais que $a^\varphi = b$. Então

$$(b^g)^{\varphi^{-1}} = ((a^\varphi)^g)^{\varphi^{-1}} = ((a^g)^\varphi)^{\varphi^{-1}} = a^g = (b^{\varphi^{-1}})^g.$$

Lema 2.1 *Sejam A e B dois G-grupos. Se $A \cong_G B$ então $C_G(A) = C_G(B)$.*

Demonstração: Suponha que $A \cong_G B$, onde $\varphi : A \to B$ é o G-isomorfismo.

Seja $g \in C_G(A)$, isto é, $a^g = a$, para todo $a \in A$. Temos então que $(a^\varphi)^g = (a^g)^\varphi = a^\varphi$, para todo $a \in A$. Como φ é um isomorfismo, obtemos que $g \in C_G(B)$, isto é, $C_G(A) \subseteq C_G(B)$.

Seja agora $g \in C_G(B)$, isto é, $b^g = b$, para todo $b \in B$. Temos então que $(b^{\varphi^{-1}})^g = (b^g)^{\varphi^{-1}} = b^{\varphi^{-1}}$, para todo $b \in B$. Como φ^{-1} é um isomorfismo, obtemos que $g \in C_G(A)$, isto é, $C_G(B) \subseteq C_G(A)$. ∎

Pelo lema acima, obtemos que se A e B são dois G-grupos com $C_G(A) \neq C_G(B)$, então A e B não são G-isomorfos.

Sejam A um G-grupo e $H \leq A$. Dizemos que H é um G-subgrupo se $h^g \in H$ para todos $h \in H$ e $g \in G$. A é dito um G-grupo simples se os únicos G-subgrupos de A são $\{1\}$ e A.

Proposição 2.2 *Sejam A e B dois G-grupos. Se A é um G-grupo simples e $A \cong_G B$, então B também é um G-grupo simples.*

Demonstração: Seja $\varphi : B \to A$ um G-isomorfismo. Seja N um G-subgrupo de B e $\varphi(N) = L \leq A$. Dados $g \in G$ e $l \in L$, existe $n \in N$ com $l = n^\varphi$ e além disso, como N é um G-subgrupo, $n^g \in N$. Então

$$l^g = (n^\varphi)^g = (n^g)^\varphi \in L,$$

assim L é um G-subgrupo. Como A é um G-grupo simples, temos que $L = \{1\}$ ou $L = A$. Se $L = \{1\}$, então $\varphi(N) = \{1\}$ o que implica $N = \{1\}$. Se $L = A$, então $\varphi(N) = A$ o que implica $N = B$. Logo B é um G-grupo simples. ∎

Pela proposição acima obtemos que se dois subgrupos normais A, B de um grupo G são tais que A é um subgrupo normal minimal de G e $A \cong_G B$ então B também é um subgrupo normal minimal de G.

Lema 2.3 *Sejam G um grupo e $A, N \trianglelefteq G$. Então $AN/N \cong_G A/A \cap N$.*

Demonstração: Considere φ a composição $A \rightarrowtail AN \twoheadrightarrow AN/N$. Sejam $a \in A$ e $g \in G$. Como $A \trianglelefteq G$ por um lado $(a^g)^\varphi = (a^g)N$, e por outro lado $(a^\varphi)^g = (aN)^g = a^g N$. Desta forma $(a^g)^\varphi = (a^\varphi)^g$. Como $\mathrm{Ker}(\varphi) = A \cap N$, obtemos então que $A/A \cap N \cong_G AN/N$. ∎

Lema 2.4 *Seja G um grupo, $A \leq G$ e $N \trianglelefteq G$. Se $N \leq A$ então $C_{G/N}(A/N) = C_G(A/N)/N$.*

Demonstração: A demonstração é imediata. ∎

2.2 Grupos primitivos

Definimos grupos primitivos da seguinte maneira:

Definição 2.5 *Um grupo G é dito primitivo se possui um subgrupo maximal M tal que $M_G = \{1\}$, onde M_G é o core normal de M em G.*

Com isso, o Teorema 1.6 nos diz que um grupo G é primitivo se, e somente se, G admite uma ação primitiva e fiel.

Lema 2.6 *Sejam G um grupo e $N \trianglelefteq G$. Se $N \leq H \leq G$, então $(H/N)_{G/N} = H_G/N$.*

Demonstração: Temos que

$$(H/N)_{G/N} = \bigcap_{gN \in G/N} (H/N)^{gN} = \bigcap_{g \in G} H^g/N = (\bigcap_{g \in G} H^g)/N = H_G/N,$$

provando o lema. ■

Teorema 2.7 *Seja G um grupo finito não trivial.*

(a) Se M é um subgrupo maximal de G, então G/M_G é primitivo;

(b) Se $K \trianglelefteq G$ e G/K é primitivo, então G possui um subgrupo maximal M tal que $K = M_G$.

Demonstração:

(a) Temos que M/M_G é maximal em G/M_G pois M é maximal em G. Além disso, o core de M/M_G é trivial, pois pelo Lema 2.6, $(M/M_G)_{G/M_G} = M_G/M_G$;

(b) Seja M/K maximal em G/K com core trivial. Pelo Lema 2.6, temos $(M/K)_{G/K} = M_G/K$. Logo M é maximal em G e $M_G = K$.

■

Definição 2.8 *Seja G um grupo primitivo. Um grau de primitividade de G é dado pelo índice $[G : M]$, onde M é um subgrupo maximal de G com $M_G = \{1\}$.*

Um grupo primitivo pode possuir mais de um grau de primitividade porque pode conter mais de um subgrupo maximal com core trivial.

O primeiro exemplo de grupo primitivo que iremos ver será o grupo simétrico S_n para $n \geq 3$. Para isto precisamos do seguinte lema:

Lema 2.9 *Se $n \geq 3$, $H < S_n$ e $H \neq A_n$ então $[S_n : H] \geq n$, com exceção de $n = 4$ e H o diedral com 8 elementos.*

Demonstração: Seja $m = [S_n : H]$. A ação de S_n, por multiplicação à direita, no conjunto $X = \{Hx : x \in S_n\}$ é uma ação transitiva e como $|X| = m$, essa ação gera um homomorfismo $\varphi : S_n \to S_m$. Temos que $\mathrm{Ker}(\varphi) = H_G \leq H$, $\mathrm{Ker}(\varphi) \trianglelefteq S_n$. Como $H \neq A_n$ temos que $m \geq 3$ e assim $[G : \mathrm{Ker}(\varphi)] \geq 3$. Se $n \neq 4$, o único subgrupo normal próprio de S_n é A_n, logo $\mathrm{Ker}(\varphi) = \{1\}$. Pelo Teorema de Lagrange, temos que $|S_n| = n!$ divide $|S_m| = m!$, isto é, $n \leq m$ e, portanto, $[S_n : H] = m \geq n$. Se $n = 4$ podemos ter $\mathrm{Ker}(\varphi) = \{1\}$ ou $\mathrm{Ker}(\varphi) = V_4$, onde V_4 é o subgrupo de Klein. Se $\mathrm{Ker}(\varphi) = \{1\}$, então pelo mesmo argumento $n \leq m$. Se $\mathrm{Ker}(\varphi) = V_4$, então $H = V_4$ ou $H = D$, onde D é o diedral com 8 elementos. Se $H = V_4$ então $[S_n : H] = 6 > 4$ e se $H = D$ então $[S_n : H] = 3 < 4$. ∎

Exemplo 2.1 *Seja $G = S_n$, $n \geq 3$. Considere a ação natural de G sobre o conjunto $X = \{1, 2, \ldots, n\}$. Seja $M = Stab(i) = \{g \in G : ig = i\}$ o estabilizador de $i \in X$. Temos que $M \cong S_{n-1}$ e assim $[G : M] = n!/(n-1)! = n$. Vejamos que M é maximal em S_n. De fato, suponha que existe $K < G$ com $M < K < G$. Temos que $[G : K] < [G : M] = n$ e então pelo Lema 2.9, $K = A_n$ (note que no caso $n = 4$ K não pode ser o diedral com 8 elementos, pois o diedral não contém subgrupos L tais que $[S_4 : L] = 4$). Logo $K = A_n$ para todo $n \geq 3$. Então $M < A_n$, mas qualquer 2-ciclo que fixa i está contido em M mas não está contido em A_n, contradição. Logo M é maximal em G. Por outro lado, $g^{-1}Mg = Stab(ig)$ é o estabilizador do elemento ig. Agora, para quaisquer $i, j \in X$, existe $g \in G$ tal que $ig = j$. Desta forma $M_G = \bigcap_{g \in G} g^{-1}Mg = \{1\}$. Logo G é um grupo primitivo de grau n.*

Definição 2.10 *O socle de um grupo G, denotado por $Soc(G)$, é o subgrupo gerado pelos subgrupos normais minimais de G.*

Note que se G é um grupo finito e A e B são subgrupos normais de G, então $\langle A, B\rangle = AB$. Desta forma, se G é um grupo finito, o socle de G é igual ao produto de seus subgrupos normais minimais. Como a interseção de dois subgrupos normais minimais é trivial, o socle de um grupo finito G é o produto direto alguns dos subgrupos normais minimais de G.

O teorema seguinte, devido a R. Baer, classifica os grupos primitivos em termo do seu socle.

Teorema 2.11 (Baer)
1. *Um grupo G é primitivo se, e somente se, existe um subgrupo U de G tal que $G = UN$ para todo subgrupo normal minimal N de G.*
2. *Sejam G um grupo primitivo, M um subgrupo maximal de G, com $M_G = \{1\}$, e N um subgrupo não trivial normal de G. Então $C_G(N) \cap M = \{1\}$. Mais ainda, $C_G(N) = \{1\}$ ou $C_G(N)$ é um subgrupo normal minimal de G.*
3. *Se G é um grupo primitivo e M é um subgrupo maximal de G com $M_G = \{1\}$, então vale exatamente uma das condições abaixo*

(a) *Soc*$(G) = S$, *onde* S *é um subgrupo normal minimal abeliano auto-centralizado de* G *que é complementado por* M*;*

(b) *Soc*$(G) = S$, *onde* S *é um subgrupo normal minimal não abeliano de* G *que é suplementado por* M*;*

(c) *Soc*$(G) = A \times B$, *onde* A *e* B *são os dois únicos subgrupos normais minimais de* G. A *e* B *são não abelianos e ambos são complementados por* M. *Além disso,* $A = C_G(B)$, $B = C_G(A)$ *e* A, B *e* $AB \cap M$ *são isomorfos como grupos, mas não são* G*-isomorfos.*

Demonstração:

1. Sejam G um grupo primitivo e M é um subgrupo maximal de G com $M_G = \{1\}$. Temos $G = MN$ para todo subgrupo normal minimal N de G. De fato, como M é maximal em G, segue que $MN = M$ ou $MN = G$. Se $MN = M$, então $N \subseteq M$ e assim $N \subseteq M_G = \{1\}$, contradição. Logo $MN = G$. Reciprocamente, se existe um subgrupo U de G tal que $G = NU$ para todo normal minimal N de G e M é um subgrupo maximal de G tal que $U \leq M$, segue que M não pode conter nenhum subgrupo normal minimal de G, pois se M contivesse algum subgrupo N normal minimal de G teríamos $UN = G \subseteq M$, o que dá $M = G$. Desta forma M não contém nenhum subgrupo normal não trivial. Logo M é um subgrupo maximal de G com $M_G = \{1\}$.

2. Como $M_G = \{1\}$, temos que $MN = G$. Como N é normal em G, temos $C_G(N) \trianglelefteq G$. Dessa forma $C_G(N) \cap M \trianglelefteq M$. Como $C_G(N) \cap M$ centraliza N, $C_G(N) \cap M$ é normalizado por M e N e segue que $C_G(N) \cap M \trianglelefteq G = MN$. Logo $C_G(N) \cap M \subseteq M_G = \{1\}$. Assim $C_G(N) \cap M = \{1\}$. Se $C_G(N) \neq \{1\}$, considere X normal minimal em G tal que $X \leq C_G(N)$. Como $X \nsubseteq M$ temos $G = XM$. Então pela Lei de Dedekind

$$C_G(N) = C_G(N) \cap XM = X(C_G(N) \cap M) = X.$$

Logo $C_G(N)$ é um subgrupo normal minimal de G.

3. Sejam N_1, N_2 e N_3 três subgrupos normais minimais de G distintos. Como $N_1 \cap N_2 = N_1 \cap N_3 = \{1\}$ temos que $N_2, N_3 \leq C_G(N_1)$. Assim $N_2N_3 \leq C_G(N_1)$, mas $C_G(N_1)$ é um subgrupo normal minimal de G, contradição.

Suponha que N não trivial é um subgrupo abeliano normal de G. Então $N \leq C_G(N)$. Vimos em 2 que $C_G(N)$ é um subgrupo normal minimal de G, segue então $N = C_G(N)$, isto é, N é auto-centralizado. N é único pois se existisse outro subgrupo abeliano T normal em G, novamente teríamos $C_G(T) = T$ e T normal minimal. Assim $N \cap T = \{1\}$ o que implica $[N, T] = \{1\}$, já que ambos são normais em G. Assim $T \leq C_G(N) = N$ e $N \leq C_G(T) = T$, logo $T = N$. Vamos agora mostrar que M complementa N em G. Como $\{1\} \neq N \trianglelefteq G$ e $M_G = \{1\}$, obtemos que $N \nsubseteq M$. Assim $M < MN \leq G$ e pela maximalidade de M em G temos que

$MN = G$. Como $N \trianglelefteq G$, temos $M \cap N \trianglelefteq M$. Como N é abeliano, $M \cap N \trianglelefteq N$. Desta forma $M \cap N \trianglelefteq MN = G$ e então $M \cap N \leq M_G = \{1\}$, isto é, $M \cap N = \{1\}$ e logo M é um complemento para N em G.

Se existe um único subgrupo N normal minimal de G, com N não abeliano, então $C_G(N) = \{1\}$. Além disso como $\{1\} \neq N \trianglelefteq G$ e $M_G = \{1\}$ obtemos que $N \nsubseteq M$. Assim $M < MN \leq G$ e, pela maximalidade de M em G, temos que $MN = G$, isto é, M suplementa N em G.

Se existem dois subgrupos A e B normais minimais de G, então $A \cap B = \{1\}$, e, portanto, $A \leq C_G(B)$ e $B \leq C_G(A)$. Como $C_G(A)$ e $C_G(B)$ são subgrupos normais minimais de G temos que $A = C_G(B)$ e $B = C_G(A)$. Agora $A \cap M = C_G(B) \cap M = \{1\}$ e $B \cap M = C_G(A) \cap M = \{1\}$. Portanto M complementa A e B. Como $A = C_G(B)$, segue que B é não abeliano. Analogamente segue que A é não abeliano. Agora temos que $A(AB \cap M) = AB \cap AM = AB \cap G = AB$, analogamente $B(AB \cap M) = AB$. Assim

$$A \cong_G A/A \cap B \cong_G AB/B = B(AB \cap M)/B \cong AB \cap M.$$

Observe que o último isomorfismo não é um G-isomorfismo pois $AB \cap M$ não é um G-grupo por conjugação, já que M não é normal em G. Analogamente $B \cong AB \cap M$. Assim $A \cong B \cong AB \cap M$. Por outro lado, A e B não são G-isomorfos pois $B = C_G(A) \neq C_G(B) = A$.

■

Definição 2.12 *Um grupo primitivo G é dito ser:*

1. *um grupo primitivo do tipo 1 se G possui um único subgrupo normal minimal e tal subgrupo é abeliano;*

2. *um grupo primitivo do tipo 2 se G possui um único subgrupo normal minimal e tal subgrupo é não abeliano;*

3. *um grupo primitivo do tipo 3 se G possui exatamente dois subgrupos normais minimais e tais subgrupos são não abelianos.*

Podemos também denotar por $G \in P_i$ se G é um grupo primitivo do tipo i, com $i \in \{1, 2, 3\}$. O Teorema de Baer implica que todo grupo primitivo é de tipo 1, 2 ou 3.

Já visto que S_n é um grupo primitivo para $n \geq 3$, como os grupos S_3 e S_4 são solúveis temos que esses são primitivos do tipo 1. Já para $n \geq 5$, o único subgrupo normal minimal de S_n é A_n e este é não abeliano, ou seja, S_n é primitivo do tipo 2.

Nos grupos primitivos do tipo 1 ou 3, o subgrupo maximal de core trivial complementa cada subgrupo normal minimal. Desta forma, se N é um subgrupo normal minimal de G primitivo do tipo 1 ou 3, $[G : M] = |N|$, e desta forma G possui apenas um grau de primitividade. Por outro lado isso não acontece nos grupos primitivos do tipo 2. De fato, seja S um grupo simples não abeliano. Em particular S não pode ser um p-grupo, pois todo p-grupo finito é nilpotente, assim existem dois divisores primos p e q da ordem de S. Seja M um subgrupo maximal de S contendo um p-subgrupo de Sylow de S e seja H um subgrupo maximal de S contendo um q-subgrupo de Sylow de S. Os índices de M e H em S são distintos, pois q divide $|S : M|$ mas não divide $|S : H|$, e M e H possuem core idêntico, sendo S um grupo simples. Desta forma S é um grupo primitivo. Segue que S é primitivo do tipo 2, pois S possui um único subgrupo normal minimal não abeliano, o próprio S. Desta forma esses dois índices são graus de primitividade distintos de S.

Vamos agora ver uma caracterização dos grupos primitivos do tipo 1 ou 3 dada por Lafuente em [11].

Proposição 2.13 *Seja G um grupo. São equivalentes:*

(a) G é um grupo primitivo do tipo 1 ou 3;

(b) existe um subgrupo normal minimal N de G complementado por um subgrupo M que também complementa $C_G(N)$;

(c) existe um subgrupo normal minimal N de G tal que G é isomorfo ao produto semidireto $N \rtimes G/C_G(N)$.

Demonstração: $(a) \Rightarrow (b)$. Vimos no Teorema 2.11.

$(b) \Rightarrow (a)$. Note que como $N \cap M = \{1\}$, obtemos que $N \cap M_G = \{1\}$. Como $N, M_G \trianglelefteq G$, temos que $M_G \leq C_G(N)$. Mas $C_G(N) \cap M = \{1\}$, então $C_G(N) \cap M_G = \{1\}$. Desta forma $M_G = \{1\}$. Suponha agora que S é um subgrupo próprio de G tal que $M \leq S$. Então o subgrupo $S \cap N$ é normal em S. Além disso $S \cap N$ é normalizado por $C_G(N)$. Desta forma $S \cap N$ é normal em $SC_G(N) = G$. Pela minimalidade de N, temos que $S \cap N = \{1\}$. Assim S também complementa N em G. Temos que $|S| = |G/N| = |M|$ e então $S = M$. Então M é um subgrupo maximal de G com core trivial. Portanto, G é um grupo primitivo. Note que o subgrupo normal minimal de um grupo primitivo do tipo 2 possui centralizador trivial. Logo G é um grupo primitivo do tipo 1 ou 3.

$(b) \Rightarrow (c)$. Note que $G = NM$, com $N \cap M = \{1\}$. Além disso $M \cong G/C_G(N)$. A aplicação $\alpha : G \to N \rtimes G/C_G(N)$ dada por $(nm)^\alpha = (n, mC_G(N))$ é um isomorfismo. De fato, dados $g_1 = n_1m_1$, $g_2 = n_2m_2$ em G temos que

$$g_1g_2 = n_1m_1n_2m_2 = n_1m_1n_2m_1^{-1}m_1m_2 = n_1n_2^{m_1^{-1}}m_1m_2 \in NM.$$

Por outro lado, $(n_1, m_1C_G(N))(n_2, m_2C_G(N)) = (n_1n_2^{m_1^{-1}}, m_1m_2C_G(N))$. Então

$$(g_1g_2)^\alpha = (n_1n_2^{m_1^{-1}}, m_1m_2C_G(N)) = (n_1, m_1C_G(N))(n_2, m_2C_G(N)) = (m_1n_1)^\alpha(m_2n_2)^\alpha.$$

Assim α é um homomorfismo. Temos que $\operatorname{Ker}\alpha = \{nm \in G : (n, mC_G(N)) = (1, C_G(N))\}$. Assim se $nm \in \operatorname{Ker}\alpha$ então $n = 1$ e $m \in M \cap C_G(N) = \{1\}$, ou seja, $nm = 1$ e logo $\operatorname{Ker}\alpha = \{1\}$, isto é, α é injetiva. Agora dado $(\bar{n}, \bar{m}C_G(N)) \in N \rtimes G/C_G(N)$, como cada $g \in G = NM$ pode ser escrito unicamente como um produto de um $n \in N$ e $m \in M$ temos que existe $\bar{g} = \bar{n}\bar{m} \in NM$ com $\bar{g}^\alpha = (\bar{n}, \bar{m}C_G(N))$, isto é, α é sobrejetiva. Logo α é um isomorfismo.

$(c) \Rightarrow (b)$. Escrevemos $C = C_G(N)$. Assuma que existe um isomorfismo

$$\alpha : N \rtimes G/C \to G$$

e considere os seguintes subgrupos,

$$N^* = \{(n, C) : n \in N\},$$

$$M^* = \{(1, gC) : g \in G\} \text{ e}$$

$$C^* = \{(n, gC) : ng \in C\}.$$

Para cada $n \in N$, o elemento (n^{-1}, nC) é um elemento não trivial de C^*. Então $C^* \neq 1$.

Vamos mostrar que N^* é um subgrupo normal minimal de $N \rtimes G/C$. Primeiro, dados $(n_1, C) \in N^*$ e $(n, gC) \in N \rtimes G/C$ temos que

$$(n, gC)^{-1}(n_1, C)(n, gC) = ((n^{-1})^g, g^{-1}C)(n_1 n, gC) =$$
$$((n^{-1})^g (n_1 n)^g, g^{-1}gC) = ((n^{-1}n_1 n)^g, C) \in N^*,$$

isto é $N^* \trianglelefteq N \rtimes G/C$. Além disso, se existe $K^* \leq N^*$ com $K^* \trianglelefteq N \rtimes G/C$ então $K = \{k : (k, C) \in K^*\} \leq N$. Além disso, como $K^* \trianglelefteq N \rtimes G/C$, para quaisquer $g \in G$ e $(k, C) \in K^*$, $(1, gC)^{-1}(k, C)(1, gC) = (k^g, C) \in K^*$, ou seja, $k^g \in K$ para quaisquer $g \in G$ e $k \in K$. Desta forma $K \trianglelefteq G$. Como N é normal minimal em G obtemos que $K = \{1\}$ ou $K = N$. Logo $K^* = \{(1, C)\}$ ou $K^* = N^*$, isto é, N^* é normal minimal em $N \rtimes G/C$.

Temos que $C^* = C_{N \rtimes G/C}(N^*)$. De fato, dados $(n, gC) \in C^*$ e $(n_1, C) \in N^*$, como feito acima temos $(n, gC)^{-1}(n_1, C)(n, gC) = ((n^{-1}n_1 n)^g, C) = ((ng)^{-1}n_1(ng), C)$. Como pela definição de C^* o elemento $ng \in C$, obtemos que $(n, gC)^{-1}(n_1, C)(n, gC) = (n_1, C)$. Assim $C^* \subseteq C_{N \rtimes G/C}(N^*)$. Por outro lado, se $(n, gC) \in C_{N \rtimes G/C}(N^*)$, para provar que $(n, gC) \in C^*$ basta mostar que $ng \in C$. Para todo $(n_1, C) \in N^*$ temos $(n, gC)^{-1}(n_1, C)(n, gC) = (n_1, C)$. Como $(n, gC)^{-1}(n_1, C)(n, gC) = ((ng)^{-1}n_1(ng), C)$ obtemos que $(ng)^{-1}n_1(ng) = n_1$, para todo $n_1 \in N$. Assim $ng \in C = C_G(N)$. Desta forma $C_{N \rtimes G/C}(N^*) \subseteq C^*$.

Agora M^* complementa N^*. De fato, dado $(n, gC) \in N \rtimes G/C$, existem $(n, C) \in N^*$ e $(1, gC) \in M^*$ tais que $(n, gC) = (n, C)(1, gC)$ e se $(x, yC) \in N^* \cap M^*$, então $x = 1$ e $yC = C$. Além disso M^* complementa C^*. De fato, dados $(n, gC) \in N \rtimes G/C$

existem $(n, n^{-1}C) \in C^*$ e $(1, ngC) \in M^*$ tais que $(n, gC) = (n, n^{-1}C)(1, ngC)$ e se $(x, yC) \in C^* \cap M^*$ então $x = 1$, $xy = y \in C$, ou seja, $(x, yC) = (1, yC) = (1, C)$.

Logo como α é um isomorfismo, $(N^*)^\alpha$ é um subgrupo normal minimal de G, $(C^*)^\alpha = (C_{N \rtimes G/C}(N^*))^\alpha = C_G((N^*)^\alpha)$, e $(M^*)^\alpha$ complementa $(N^*)^\alpha$ e $(C^*)^\alpha$ em G. ∎

Agora vejamos uma caracterização dos grupos primitivos do tipo 2 dada por Lafuente em [11].

Proposição 2.14 *Para um grupo G são equivalentes:*

(a) G é um grupo primitivo do tipo 2;

(b) G possui um subgrupo normal minimal N tal que $C_G(N) = \{1\}$;

(c) Existe um grupo X primitivo do tipo 3 tal que $G \cong X/A$ para um subgrupo normal minimal A de X.

Demonstração: $(a) \Rightarrow (b)$. Imediato pelo Teorema 2.11.

$(b) \Rightarrow (a)$. Suponha que G possui um outro subgrupo normal minimal $K \neq N$. Então $[K, N] \leq K \cap N = \{1\}$. Assim $K \leq C_G(N) = \{1\}$, contradição. Logo o único subgrupo normal minimal de G é N. Como $C_G(N) = \{1\}$, N é não abeliano. Se $N \leq \Phi(G)$, onde $\Phi(G)$ é o subgrupo de Frattini de G, então N é nilpotente. Desta forma $N' \neq N$, onde N' é o subgrupo derivado de N. Agora, como N' é característico em N, temos que $N' \trianglelefteq G$ e como N é normal minimal, obtemos que $N' = \{1\}$ o que implica que N é abeliano, contradição. Então $N \nleq \Phi(G)$ e existe um subgrupo maximal M de G não contendo N. Se $M_G \neq \{1\}$, como $M_G \trianglelefteq G$, existe um subgrupo normal minimal de G contido em M_G. Como N é o único subgrupo normal minimal de G temos que $N \leq M_G \leq M$, contradição. Logo $M_G = \{1\}$ e G é um grupo primitivo do tipo 2.

$(a) \Rightarrow (c)$. Seja G um grupo primitivo do tipo 2 com subgrupo normal minimal N e $C_G(N) = \{1\}$. Considere $X = N \rtimes G$. Seja $L = \{(a, 1) : a \in N\} \cong N$. Temos que L é um subgrupo normal minimal de X. Agora $C_X(L) = \{(n, g) : (n, g)^{-1}(a, 1)(n, g) = (a, 1), \forall a \in N\}$. Assim se $(n, g) \in C_X(L)$, então $g^{-1}n^{-1}ang = a$, para todo $a \in N$. Assim se $(n, g) \in C_X(L)$, então $ng \in C_G(N) = \{1\}$. Logo $g = n^{-1}$ e então $C_X(L) \subseteq \{(n, n^{-1}) : n \in N\}$. Por outro lado, $\{(n, n^{-1}) : n \in N\} \subseteq C_X(L)$. Então $C_X(L) = \{(n, n^{-1}) : n \in N\} \cong N \cong L$. Portanto $X = N \rtimes G \cong L \rtimes X/L$ e então pela Proposição 2.13, X é um grupo primitivo do tipo 3.

$(c) \Rightarrow (a)$. Seja X um grupo primitivo do tipo 3 com subgrupos normais minimais A e B tais que $C_X(A) = B$ e $C_X(B) = A$. Temos $AB/A \cong_X B/A \cap B = B/\{1\} \cong_X B$ é um subgrupo normal minimal de X/A. Seja agora $xA \in C_{X/A}(AB/A)$. Temos $x^{-1}bxA = bA$, para todo $b \in B$. Assim $[b, x] \in A$ para todo $b \in B$. Então $[b, x] \in A \cap B = \{1\}$, e assim $x \in C_X(B) = A$. Então $C_{G/A}(AB/A) = A/A$. Pelo que foi provado na implicação $(b) \Rightarrow (a)$, $X/A \cong G$ é um grupo primitivo do tipo 2. ∎

Corolário 2.15 *Seja G um grupo. As seguintes condições são equivalentes:*

(a) G é um grupo primitivo do tipo 3;

(b) O grupo G possui dois subgrupos normais minimais distintos N_1, N_2, tais que

(i) N_1 e N_2 possuem complemento comum em G;

(ii) O quociente G/N_i, para $i = 1, 2$, é um grupo primitivo do tipo 2.

Demonstração: $(a) \Rightarrow (b)$. Se G é um grupo primitivo do tipo 3, então G possui dois subgrupos normais minimais distintos N_1 e N_2 tais que $C_G(N_1) = N_2$, $C_G(N_2) = N_1$, além disso N_1 e N_2 possuem complemento comum M em G, com M maximal em G de core trivial. Como visto na Proposição 2.14, $N_2N_1/N_1 \cong N_2$ é um subgrupo normal minimal de G/N_1 com $C_{G/N_1}(N_1N_2/N_1) = N_1/N_1$, ou seja, G/N_1 é um grupo primitivo do tipo 2. Note que $G/N_1 \cong M$.

$(b) \Rightarrow (a)$. Seja M um complemento comum de N_1 e N_2. Então $G/N_1 \cong M$ é um grupo primitivo do tipo 2 tal que $Soc(G/N_1) = N_1N_2/N_1$ e $C_{G/N_1}(N_1N_2/N_1) = N_1/N_1$. Então $C_G(N_1N_2/N_1) = N_1$. Desta forma para $n_1 \in N_1$ e $n_2 \in N_2$, $n^{-1}n_2n_1N_1 = n_2N_1$, isto é, $[n_2, n_1] \in N_1$. Como $N_2 \trianglelefteq G$, $[n_2, n_1] \in N_1 \cap N_2 = \{1\}$. Assim $N_1 \leq C_G(N_2)$. Por outro lado, dado $x \in C_G(N_2)$, $x^{-1}n_2x = n_2$, para todo $n_2 \in N_2$. Assim $x^{-1}n_2xN_1 = n_2N_1$, ou seja, $x \in C_G(N_1N_2/N_1) = N_1$. Então $C_G(N_2) = N_1$. Analogamente, G/N_2 é um grupo primitivo do tipo 2 com $C_G(N_1) = N_2$. Logo pelo item (b) da Proposição 2.13, G é um grupo primitivo do tipo 3. ∎

Consequentemente, se M é um subgrupo maximal de core trivial de um grupo G primitivo do tipo 3, então M é um grupo primitivo do tipo 2 e $Soc(M)$ é isomorfo a um subgrupo normal minimal de G.

2.3 Grupos primitivos do tipo 1

Pelo que foi visto no Capítulo 1, sabemos que se N é um subgrupo normal minimal abeliano de um grupo finito G, então N é um grupo abeliano elementar. Desta forma, se G é um grupo primitivo do tipo 1 e N é o subgrupo normal minimal de G, então $N = Soc(G) \cong C_p^n \cong \mathbb{F}_p^n$. O grupo G age sobre N por conjugação, assim se $n_1, n_2 \in N$ e $g \in G$ temos que $(n_1n_2)^g = g^{-1}n_1n_2g = g^{-1}n_1gg^{-1}n_2g = (n_1)^g(n_2)^g \in N$. Na notação aditiva temos que

$$(n_1 + n_2)^g = (n_1)^g + (n_2)^g.$$

Essa ação é $\mathbb{F}_p$-linear. De fato, sejam $\lambda \in \mathbb{F}_p$, $n \in N$ e $g \in G$. Podemos escrever $\lambda = 1 + 1 + \ldots + 1$. Desta forma

$$(\lambda n)^g = (n + n + \ldots + n)^g = n^g + n^g + \ldots + n^g = (1 + 1 + \ldots + 1)n^g = \lambda n^g.$$

Com isto, dado $g \in G$, podemos definir um isomorfismo $\mathbb{F}_p$-linear $\gamma_g : N \to N$ dado por $\gamma_g(n) = n^g$, para todo $n \in N$. Vimos, no Teorema de Baer, que $G = N \rtimes H$, onde H é um subgrupo maximal de G com $H_G = \{1\}$. Considere então

$$\varphi : H \to GL(N)$$

dada por $h \mapsto \gamma_h$, onde $GL(N)$ é o grupo dos isomorfismos $\mathbb{F}_p$-lineares de N em N. Temos que

$$\text{Ker}(\varphi) = \{h \in H : \gamma_h = 1_N\} = \{h \in H : h^{-1}nh = h, \; \forall\, n \in N\} = C_H(N) = \{1\},$$

onde $C_H(N) = C_G(N) \cap H = N \cap H = \{1\}$, pois $C_G(N) = N$ e H complementa N em G. Desta forma H é isomorfo a um um subgrupo de $GL(N)$ e podemos olhar $G = N \rtimes H$ como um subgrupo de $N \rtimes GL(N)$ a partir do monomorfismo

$$N \rtimes H \rightarrowtail N \rtimes GL(N)$$

dado pela inclusão $(n, h) \mapsto (n, h)$, onde $N \rtimes GL(N) \overset{def}{=} AGL(N)$ é o grupo afim de N. Desta forma temos que $N \leq G \leq AGL(N)$.

Proposição 2.16 *Se $G = AGL(\mathbb{F}_p^n) = \mathbb{F}_p^n \rtimes GL(\mathbb{F}_p^n)$, então G é um grupo primitivo do tipo 1.*

Demonstração: Primeiro vamos mostrar que $\mathbb{F}_p^n$ é um subgrupo normal minimal de G. Temos que $(\mathbb{F}_p^n, +)$ é um grupo finito abeliano elementar. Então pela Proposição 1.12, $(\mathbb{F}_p^n, +)$ é caracteristicamente simples. Seja K um subgrupo próprio de $\mathbb{F}_p^n$ com $K \trianglelefteq G$. Como $\mathbb{F}_p^n$ é abeliano temos que $k^\lambda = k$ para quaisquer $k \in K$ e $\lambda \in \mathbb{F}_p^n$. Dado $g \in G$ podemos escrever $g = \lambda\gamma$, com $\lambda \in \mathbb{F}_p^n$ e $\gamma \in GL(\mathbb{F}_p^n)$. Desta forma dado $k \in K$, $k^g = k^{\lambda\gamma} = k^\gamma \in K$, pois $K \trianglelefteq G$. Como $\lambda \in GL(\mathbb{F}_p^n)$ é um isomorfismo $\mathbb{F}_p$-linear de $\mathbb{F}_p^n$ para $\mathbb{F}_p^n$ temos que $\lambda \in Aut(\mathbb{F}_p^n)$. Como $g \in G$ é arbitrário, obtemos que $K \trianglelefteq_c \mathbb{F}_p^n$, contradição. Logo $\mathbb{F}_p^n$ é um subgrupo normal minimal de G.

Agora vamos mostrar que $C_G(\mathbb{F}_p^n) = \mathbb{F}_p^n$. Como $\mathbb{F}_p^n$ é um grupo abeliano temos que $\mathbb{F}_p^n \leq C_G(\mathbb{F}_p^n)$. Seja agora $g \in C_G(\mathbb{F}_p^n)$. Temos que para todo $\eta \in \mathbb{F}_p^n$, $\eta^g = \eta$. Como $G = \mathbb{F}_p^n \rtimes GL(\mathbb{F}_p^n)$, podemos escrever $g = \lambda\gamma$, com $\lambda \in \mathbb{F}_p^n$ e $\gamma \in GL(\mathbb{F}_p^n)$. Dessa forma

$$\eta^g = \eta^{\lambda\gamma} = \eta^\gamma = \eta,$$

ou seja $\eta^\gamma = \eta$, e assim $\gamma \in GL(\mathbb{F}_p^n)$ é a aplicação identidade. Logo $g = \lambda \in \mathbb{F}_p^n$ e assim $C_G(\mathbb{F}_p^n) \leq \mathbb{F}_p^n$. Portanto $C_G(\mathbb{F}_p^n) = \mathbb{F}_p^n$.

Desta forma obtemos que $\mathbb{F}_p^n = C_G(\mathbb{F}_p^n)$ é um subgrupo normal minimal de G complementado por $GL(\mathbb{F}_p^n)$. Segue pela Proposição 2.13 que G é um grupo primitivo do tipo 1. ■

Vamos agora dar alguns exemplos para a proposição acima.

Exemplo 2.2 *Seja $n = 1$, então $G = \mathbb{F}_p \rtimes GL(\mathbb{F}_p)$ é um grupo primitivo do tipo 1. Temos que $\mathbb{F}_p \cong C_p$ e qualquer elemento $0 \neq a \in C_p$ é inversível, ou seja, $GL(\mathbb{F}_p) \cong C_{p-1}$. Desta forma $G \cong C_p \rtimes C_{p-1}$ é um grupo primitivo do tipo 1 de ordem $p(p-1)$. Além disso, se q é um primo que divide $p-1$ então $C_p \rtimes C_q$ também é um grupo primitivo do tipo 1. Com isso, como para $p > 2$, $p-1$ é um número par, 2 divide $p-1$ e assim o grupo diedral $C_p \rtimes C_2$ é um grupo primitivo do tipo 1. Por outro lado, se n não é primo ou potência de primo, o diedral com $2n$ elementos, $D_{2n} = C_n \rtimes C_2$, não é um grupo primitivo, pois para cada primo r dividindo n, C_r é um subgrupo normal minimal de D_{2n}, e como existem pelo menos dois primos dividindo n, D_{2n} possui pelo menos dois subgrupos normais minimais distintos. Como D_{2n} é um grupo solúvel, se D_{2n} fosse um grupo primitivo, D_{2n} admitiria no máximo um subgrupo normal minimal. Logo n é um primo p ou uma potência desse primo p. Agora, se n é uma potência de p, chamando de $N = C_p$ o subgrupo normal minimal de D_{2n} temos que N é o único subgrupo de C_n de ordem p. Além disso $C_n \leq C_G(N) = N \leq C_n$, isto é, $C_n = C_p$ e então $n = p$. Portanto D_{2n} é um grupo primitivo se, e somente se, n é primo.*

Exemplo 2.3 *Já vimos que os grupos simétricos S_3 e S_4 são grupos primitivos do tipo 1 e que grupos primitivos do tipo 1 com socle N mergulham em $AGL(N)$. Vamos mostrar que S_3 e S_4 são da forma $AGL(\mathbb{F}_p^n)$. Temos que $S_3 = C_3 \rtimes C_2 \cong AGL(\mathbb{F}_3^1)$. Agora $S_4 = V_4 \rtimes S_3$, onde V_4 é o subgrupo de Klein. Temos que $V_4 \cong \mathbb{F}_2^2$. Por outro lado $|GL(\mathbb{F}_2^2)| = (2^2-1)(2^2-2) = 6$. Desta forma $GL(\mathbb{F}_2^2) \cong S_3$ e então $S_4 \cong AGL(\mathbb{F}_2^2)$.*

Note que se G é um grupo solúvel e primitivo, então G é primitivo do tipo 1, já que se N é um subgrupo normal minimal de G, então N é um grupo abeliano elementar. Para grupos primitivos solúveis temos o seguinte teorema.

Teorema 2.17 *Seja G um grupo finito. Suponha que G é solúvel e primitivo com M maximal em G e $M_G = \{1\}$. Então:*

(a) G possui um único subgrupo normal minimal N, M complementa N em G, e $N = C_G(N) = F(G)$;

(b) Se p é o primo dividindo $|N|$, então $O_p(M) = \{1\}$;

(c) Todos os complementos de N em G são conjugados a M.

Demonstração:

(a) Como G é um grupo primitivo do tipo 1, pelo Teorema 2.11, G possui um único subgrupo normal minimal N, M complementa N e N é tal que $N = C_G(N)$. Pelo Lema 1.23, temos que $F(G) \leq C_G(N) = N$. Como N é abeliano e $N \trianglelefteq G$, obtemos que $N \leq F(G)$. Assim $N = F(G)$.

(b) Seja $P = O_p(M) \trianglelefteq M$. Tanto P quanto $N = C_p^n$ são p-grupos, e como $|PN| = |P|\,|N|\,/\,|P \cap N|$, temos que PN é um p-grupo o que implica que PN é nilpotente.

Vamos mostrar que $PN \trianglelefteq G$. Sejam $g \in G$ e $xn \in PN$, com $x \in P$ e $n \in N$. Como $G = MN$, podemos escrever $g = m_1 n_1$ com $m_1 \in M$ e $n_1 \in N$. Assim

$$gxng^{-1} = m_1 n_1 xnn_1^{-1} m_1^{-1} = m_1[xx^{-1}n_1 xnn_1^{-1}]m_1^{-1} =$$
$$m_1 x n_2 m_1^{-1} = m_1 x m_1^{-1} m_1 n_2 m_1^{-1} \in PN,$$

onde $n_2 = x^{-1} n_1 xnn_1^{-1} \in N$. Assim PN é um subgrupo normal nilpotente de G, logo $PN \subseteq F(G) = N$, o que implica que $P \subseteq N$. Assim $P \subseteq M \cap N = \{1\}$. Logo $P = \{1\}$.

(c) Seja L um complemento de N em G, isto é, $LN = G$ e $L \cap N = \{1\}$. Se $L = \{1\}$, então $G = N$ e assim $M = \{1\} = L$. Podemos então supor que $L \neq \{1\}$ e assim $N < G$. Vamos inicialmente mostrar que L é um subgrupo maximal de G. Seja K um subgrupo maximal de G tal que $L \leq K < G$. Se $N \leq K$ então $NL = K < G$, contradizendo que L complementa N em G. Então $N \nsubseteq K$. Desta forma $NK = G$. Agora, $N \cap K \leq N$, $N \cap K \trianglelefteq K$ pois $N \trianglelefteq G$ e $N \cap K \trianglelefteq N$ pois N é abeliano. Assim $N \cap K \trianglelefteq KN = G$. Como N é normal minimal, $N \cap K = \{1\}$ ou $N \cap K = N$. Se $N \cap K = N$ então $N \subseteq K$, contradição. Assim $N \cap K = \{1\}$. Desta forma, K complementa N em G. Assim $L \cong G/N \cong K$, o que implica que $|L| = |K|$. Como $L \leq K$ obtemos que $L = K$ e assim L é um subgrupo maximal de G.

Vamos agora mostrar que $N = O_p(G)$. Temos que $N = C_p^n$. Pelo Teorema de Sylow, existe P um p-subgrupo de Sylow de G tal que $N \subseteq P$. Assim

$$O_p(G) = \bigcap_{g \in G} gPg^{-1} \supseteq \bigcap_{g \in G} gNg^{-1} = \cap N = N,$$

ou seja, $N \leq O_p(G)$ e além disso $N \trianglelefteq O_p(G)$, já que $N \trianglelefteq G$. Por outro lado, $O_p(G)/N \trianglelefteq G/N \cong M$. Temos que $O_p(G)/N$ é um p-subgrupo e pelo item anterior, o único p-subgrupo normal de M é o trivial. Assim $O_p(G)/N = N/N$ o que implica que $O_p(G) \leq N$. Desta forma, $O_p(G) = N$. Seja agora $R = O_{p,p'}(G)$, isto é,

$$R/N = O_{p'}(G/N) \trianglelefteq G/N.$$

Desta forma $N \subseteq R$. Vamos mostrar que $N < R$. Tome S/N normal minimal em G/N. Se S/N é um p-subgrupo de G/N, então S é um p-subgrupo normal de G de modo que $N = O_p(G) \subseteq S$. Mas $O_p(G)$ é o maior p-subgrupo normal de G, assim $S = N$, contradizendo que S/N é um subgrupo normal minimal de G/N. Desta forma S/N não pode ser um p-subgrupo de G/N, logo $S/N \subseteq O_{p'}(G/N)$ porque S/N é um q-subgrupo, para algum primo $q \neq p$. Assim $N/N \neq O_{p'}(G/N) = R/N$, isto é, $N < R$. Desta forma obtemos que $1 \neq [R : N] = |R/N|$ é um p'-número. Além disso, $O_{p'}(G) = \{1\}$. De fato, se $O_{p'}(G) \neq \{1\}$, como $O_{p'}(G) \trianglelefteq G$ e G é finito, $O_{p'}(G)$ contém um subgrupo normal minimal de G. Como N é o único normal minimal de G obtemos que $N \subseteq O_{p'}(G)$, absurdo. Logo $O_{p'}(G) = \{1\}$.

Agora, $N(L \cap R) = NL \cap R = G \cap R = R$ e $N \cap (L \cap R) = (N \cap L) \cap R = \{1\} \cap R = \{1\}$, isto é, $L \cap R$ é um complemento para N em R. Temos então que $L \cap R \cong R/N$ é um p'-subgrupo de G. Como $R \trianglelefteq G$ temos $L \cap R \trianglelefteq L$, assim $L \leq N_G(L \cap R) \leq G$. Suponha que $N_G(L \cap R) = G$, isto é, $L \cap R \trianglelefteq G$. Assim $L \cap R$ é um p'-subgrupo normal de G, isto é, $L \cap R \leq O_{p'}(G) = \{1\}$. Desta forma $N = R$, contradição. Então $L \leq N_G(L \cap R) < G$. Vimos que L é um subgrupo maximal de G, desta forma $L = N_G(L \cap R)$. Analogamente obtemos que $M \cap R$ é um complemento de N em R e que $M = N_G(M \cap R)$.

Note que $mdc(|N|, |R/N|) = 1$, já que $N = C_p^n$ e $|R/N|$ é um p'-número. Como N é solúvel, $M \cap R$ e $L \cap R$ são complementos para N em R, pelo Teorema de Shur-Zassenhaus existe $r \in R$ tal que $r(L \cap R)r^{-1} = (M \cap R)$. Então

$$rLr^{-1} = rN_G(L \cap R)r^{-1} = N_G(r(L \cap R)r^{-1}) = N_G(M \cap R) = M,$$

isto é, L e M são conjugados em G.

■

2.4 Grupos primitivos do tipo 2

Pelo Teorema 2.11, o socle de um grupo primitivo do tipo 2 é um subgrupo normal minimal não abeliano e, como visto no Capítulo 1, é um produto direto de cópias de um grupo simples não abeliano.

Proposição 2.18 *Seja S um grupo simples não abeliano e $L = S \times S \times \ldots \times S$. Se $L \leq G \leq Aut(L)$ e L é um subgrupo normal minimal de G, então G é um grupo primitivo do tipo 2. Em particular, L é um subgrupo normal minimal de $Aut(L)$ e $Aut(L)$ é um grupo primitivo do tipo 2. Reciprocamente, se G é um grupo primitivo do tipo 2 com $Soc(G) = L$, então, identificando G como um subgrupo de $Aut(L)$ por meio do homomorfismo que associa a cada $g \in G$ a conjugação por g, temos $L \leq G \leq Aut(L)$.*

Demonstração: Como L é o produto direto de um número finito de cópias de um grupo simples S, temos que L é caracteristicamente simples. Considerando o homomorfismo

$$\begin{aligned} \gamma : L &\longrightarrow Aut(L) \\ l &\longmapsto \quad \gamma_l : L \longrightarrow L \\ &\qquad\qquad x \longmapsto lxl^{-1}. \end{aligned}$$

Temos que $\operatorname{Ker}\gamma = Z(L) = Z(S) \times \ldots \times Z(S) = \{1\} \times \ldots \times \{1\}$. Assim $L \cong \gamma(L) = Inn(L) \trianglelefteq Aut(L)$. Suponha que existe $R \leq L$ com $R \trianglelefteq Aut(L)$. Seja $\varphi \in Aut(L)$, vamos mostrar que $\varphi(R) = R$. Se $r \in R$, como $R \trianglelefteq Aut(L)$, existe $t \in R$ com $\varphi\gamma_r\varphi^{-1} = \gamma_t$. Temos que $\varphi\gamma_r\varphi^{-1}(l) = \varphi(r\varphi^{-1}(l)r^{-1}) = \varphi(r)l\varphi(r)^{-1} = \gamma_{\varphi(r)}(l)$, para todo $l \in L$. Assim $\varphi\gamma_r\varphi^{-1} = \gamma_{\varphi(r)}$. Desta forma, $\gamma_{\varphi(r)} = \gamma_t$, isto é, $\gamma(\varphi(r)) = \gamma(t)$, como o homomorfismo γ é injetivo, $\varphi(r) = t \in R$, logo $\varphi(R) \subseteq R$. Aplicando as mesmas contas para $\varphi^{-1} \in Aut(L)$

obtemos que $\varphi^{-1}(R) \subseteq R$, ou seja, $R \subseteq \varphi(R)$. Desta forma $R = \varphi(R)$ e obtemos que $R \trianglelefteq_c L$, contradizendo que L é caracteristicamente simples. Desta forma L é um subgrupo normal minimal de $Aut(L)$. Seja agora $\varphi \in C_{Aut(L)}(L)$. Assim $\varphi\gamma_l = \gamma_l\varphi$, para todo $l \in L$. Então $\varphi\gamma_l(x) = \gamma_l\varphi(x)$, para quaisquer $l, x \in L$. Portanto $\varphi(lxl^{-1}) = l\varphi(x)l^{-1}$, ou seja, $\varphi(x) = \varphi(l)^{-1}l\varphi(x)l^{-1}\varphi(l)$. Assim $\varphi(l)^{-1}l \in Z(L) = \{1\}$. Portanto, $\varphi(l) = l$, para todo $l \in L$, ou seja, $\varphi = 1_L$. Então $C_{Aut(L)}(L) = \{1\}$. Portanto $C_G(L) \subseteq C_{Aut(L)}(L) = \{1\}$. Logo pelo Item (b) da Proposição 2.14, G e $Aut(L)$ são grupos primitivos do tipo 2.

Reciprocamente, se G é um grupo primitivo do tipo 2 com $Soc(G) = L$, G pode ser visto como subgrupo de $Aut(L)$ já que o homomorfismo canônico $G \to Aut(L)$ dado pela conjugação, possui núcleo igual a $C_G(L) = \{1\}$. ■

Em particular se $L = S$, onde S é um grupo simples não abeliano, então $Aut(S)$ e qualquer grupo G tal que $S \leq G \leq Aut(S)$ são grupos primitivos do tipo 2 (com subgrupo normal minimal igual a S). Além disso, se G é um grupo primitivo do tipo 2 com $Soc(G) = S$, então identificando G com um subgrupo de $Aut(S)$ por meio do homomorfismo que associa a cada $g \in G$ a conjugação por g, temos $S \leq G \leq Aut(S)$. Um grupo almost-simple G é um subgrupo de $Aut(S)$ para algum grupo simples S, tal que $S \leq G$.

Seja S um grupo simples não abeliano. Veremos que os grupos da forma $Aut(S^n)$ são isomorfos ao produto entrelaçado entre $Aut(S)$ e S_n.

Definição 2.19 *Sejam H e K dois grupos e suponha que $K \leq S_n$. O produto entrelaçado $H \wr K$, é o produto semidireto $H^n \rtimes K$, onde H^n é o produto direto de n cópias de H, e K age em H^n permutando as coordenadas. Mais especificamente, $\pi \in K$ age em H^n por*

$$(h_1, \ldots, h_n)^\pi = (h_{1\pi^{-1}}, \ldots, h_{n\pi^{-1}})$$

para quaisquer $h_i \in H$, $i = 1, \ldots, n$.

Vamos mostrar que essa ação se trata de uma ação de grupo. Se $\pi, \tau \in K$, definindo $t_i = h_{i\pi^{-1}}$ temos que $t_{i\tau^{-1}} = h_{i\tau^{-1}\pi^{-1}} = h_{i(\pi\tau)^{-1}}$, então

$$((h_1, \ldots, h_n)^\pi)^\tau = (h_{1\pi^{-1}}, \ldots, h_{n\pi^{-1}})^\tau = (h_{1(\pi\tau)^{-1}}, \ldots, h_{n(\pi\tau)^{-1}}) = (h_1, \ldots, h_n)^{\pi\tau}.$$

Lembrando que o expoente por π significa a conjugação por π. O subgrupo H^n é dito a base do grupo $H \wr K$.

Proposição 2.20 *Seja S um grupo simples não abeliano e escreva $S^n = S \times \ldots \times S$, o produto direto de n cópias de S, para algum inteiro positivo n. Então os subgrupos normais minimais de S^n são $N_i = \{1\} \times \ldots \times \{1\} \times S \times \{1\} \times \ldots \{1\}$, onde apenas a i-ésima coordenada é igual a S, para qualquer $i = 1, \ldots, n$.*

Demonstração: Para cada $i = 1, \ldots, n$, os subgrupos N_i são normais em S^n. De fato, dados $s = (s_1, \ldots, s_n) \in S^n$ e $x = (1, \ldots, x_i, \ldots, 1) \in N_i$, temos que

$$s^{-1}xs = (s_1^{-1}s_1, \ldots, s_i^{-1}x_is_i, \ldots, s_n^{-1}s_n) = (1, \ldots, s_i^{-1}x_is_i, \ldots, 1) \in N_i.$$

Além disso os subgrupos N_i são normais minimais em S^n pois se existe $K_i \leq N_i$ com $K_i \trianglelefteq S^n$, o subgrupo $K \leq S$ formado pelos elementos da i-ésima coordenada de K_i é tal que K é normal no grupo simples S. Desta forma $K = \{1\}$ ou $K = S$ e então $K_i = \{1\} \times \ldots \times \{1\}$ ou $K_i = N_i$.

Seja agora N um subgrupo normal minimal de S^n diferente dos N_i. Então $N \cap N_i = \{1\}$ para todo $i = 1, \ldots, n$. Como N e N_i são normais em S^n, temos que $[N, N_i] \leq N \cap N_i = \{1\}$, desta forma N centraliza todos os N_i e assim $N \leq Z(S^n) = \{1\} \times \ldots \times \{1\}$, contradição. Logo os únicos subgrupos normais minimais de S^n são os N_i, $i = 1, \ldots, n$. ■

Lema 2.21 (Lema de Imersão, [15], Resultado (4.1)) *Sejam H um subgrupo de um grupo finito G, $x_1, \ldots, x_n$ um transversal à direita para H em G, e ξ qualquer homomorfismo com domínio H. Então a aplicação $f : G \to \xi(H) \wr S_n$ dada por*

$$x \mapsto (\xi(x_1 x x_{1\pi}^{-1}), \ldots, \xi(x_n x x_{n\pi}^{-1}))\pi,$$

onde $\pi \in S_n$ é a única permutação que satisfaz $x_i x \in H x_{i\pi}$ para todo $i = 1, \ldots, n$, é um homomorfismo bem definido com núcleo igual ao core $(\operatorname{Ker}\xi)_G$.

Demonstração: A permutação correspondente a $x = 1$ é a permutação identidade (1) já que $x_i = x_i 1 \in H x_i$, e dessa forma $f(1) = (\xi(x_1 1 x_1^{-1}), \ldots, \xi(x_n 1 x_n^{-1}))(1) = (1, \ldots, 1)(1)$. Sejam agora $x, y \in G$ e assuma que $x_i x x_{i\pi}^{-1} \in H$ e $x_i y x_{i\tau}^{-1} \in H$, para todo $i = 1, \ldots, n$. Então aplicando $i\pi$ na segunda expressão obtemos que $x_{i\pi} y x_{i\pi\tau}^{-1} \in H$, para todo $i = 1, \ldots, n$. Então $x_i x y x_{i\pi\tau}^{-1} = (x_i x x_{i\pi}^{-1})(x_{i\pi} y x_{i\pi\tau}^{-1}) \in H$. Segue que a permutação correspondente a xy é $\pi\tau$ e

$$\begin{aligned}
f(xy) &= (\xi(x_1 x y x_{1\pi\tau}^{-1}), \ldots, \xi(x_n x y x_{n\pi\tau}^{-1}))\pi\tau \\
&= (\xi(x_1 x x_{1\pi}^{-1} x_{1\pi} y x_{1\pi\tau}^{-1}), \ldots, \xi(x_n x x_{n\pi}^{-1} x_{n\pi} y x_{n\pi\tau}^{-1}))\pi\tau \\
&= (\xi(x_1 x x_{1\pi}^{-1})\xi(x_{1\pi} y x_{1\pi\tau}^{-1}), \ldots, \xi(x_n x x_{n\pi}^{-1})\xi(x_{n\pi} y x_{n\pi\tau}^{-1}))\pi\tau \\
&= ((\xi(x_1 x x_{1\pi}^{-1}), \ldots, \xi(x_n x x_{n\pi}^{-1}))(\xi(x_{1\pi} y x_{1\pi\tau}^{-1}), \ldots, \xi(x_{n\pi} y x_{n\pi\tau}^{-1})))\pi\tau \\
&= (\xi(x_1 x x_{1\pi}^{-1}), \ldots, \xi(x_n x x_{n\pi}^{-1}))\pi\pi^{-1}(\xi(x_{1\pi} y x_{1\pi\tau}^{-1}, \ldots, \xi(x_{n\pi} y x_{n\pi\tau}^{-1}))\pi\tau \\
&= f(x) \cdot \pi^{-1}(\xi(x_{1\pi} y x_{1\pi\tau}^{-1}), \ldots, \xi(x_{n\pi} y x_{n\pi\tau}^{-1}))\pi\tau \\
&= f(x)(\xi(x_{1\pi} y x_{1\pi\tau}^{-1}), \ldots, \xi(x_{n\pi} y x_{n\pi\tau}^{-1}))^{\pi}\tau \\
&= f(x)(\xi(x_{1\pi^{-1}\pi} y x_{1\pi^{-1}\pi\tau}^{-1}), \ldots, \xi(x_{n\pi^{-1}\pi} y x_{n\pi^{-1}\pi\tau}^{-1}))\tau \\
&= f(x)(\xi(x_1 y x_{1\tau}^{-1}), \ldots, \xi(x_n y x_{n\tau}^{-1}))\tau \\
&= f(x)f(y).
\end{aligned}$$

Além disso $f(x) = (1, \ldots, 1)(1)$ se, e somente se, a permutação π correspondente a x é a permutação identidade e $x_i x x_i^{-1} \in \operatorname{Ker}(\xi)$ para todo $i = 1, \ldots, n$. Então $x \in \operatorname{Ker}(f)$ se, e somente se, $x \in x_i^{-1}\operatorname{Ker}(\xi)x_i$, para todo $i = 1, \ldots, n$. Desta forma $x \in \operatorname{Ker}(f)$ se, e somente se, $x \in \bigcap_{i=1}^{n} x_i^{-1}\operatorname{Ker}(\xi)x_i$. Como $x_1, \ldots, x_n$ formam um transversal à direita para

H em G, temos que para cada $g \in G$ existe $h \in H$ tal que $g = hx_i$. Além disso como $\mathrm{Ker}(\xi) \trianglelefteq H$ obtemos que $x \in \mathrm{Ker}(f)$ se, e somente se,

$$x \in \bigcap_{\substack{i=1,\dots,n \\ h \in H}} x_i^{-1} h^{-1} \,\mathrm{Ker}(\xi) h x_i = \bigcap_{g \in G} g^{-1} \,\mathrm{Ker}(\xi) g = (\mathrm{Ker}(\xi))_G.$$

Logo $\mathrm{Ker}(f) = (\mathrm{Ker}\,\xi)_G$. ∎

Proposição 2.22 *Seja S um grupo simples não abeliano e escreva S^n para o produto direto de n cópias de S, para algum inteiro positivo n. Então $Aut(S^n) \cong Aut(S) \wr S_n$, onde S_n é o grupo simétrico de grau n.*

Demonstração: Considere a aplicação

$$\psi : Aut(S) \wr S_n \to Aut(S^n)$$

dada por

$$\psi : (\varphi_1, \dots, \varphi_n)\sigma \mapsto \alpha$$

onde $\varphi_1, \dots, \varphi_n \in Aut(S)$ e $\sigma \in S_n$. A aplicação $\alpha \in Aut(S^n)$ é dada por

$$(s_1, \dots, s_n)^\alpha = (s_1\varphi_1, \dots, s_n\varphi_n)^\sigma = (s_{1\sigma^{-1}}\varphi_{1\sigma^{-1}}, \dots, s_{n\sigma^{-1}}\varphi_{n\sigma^{-1}}),$$

onde $(s_1, \dots, s_n) \in S^n$.

Vamos mostrar que ψ é um homomorfismo. Sejam $(\varphi_1, \dots, \varphi_n), (\gamma_1, \dots, \gamma_n) \in Aut(S)^n$, $\sigma, \tau \in S_n$ e $(s_1, \dots, s_n) \in S^n$. Temos que

$$\begin{aligned}
&(\varphi_1, \dots, \varphi_n)\sigma(\gamma_1, \dots, \gamma_n)\tau \\
&\qquad = (\varphi_1, \dots, \varphi_n)\sigma(\gamma_1, \dots, \gamma_n)\sigma^{-1} \cdot \sigma\tau \\
&\qquad = (\varphi_1, \dots, \varphi_n)(\gamma_1, \dots, \gamma_n)^{\sigma^{-1}} \cdot \sigma\tau \\
&\qquad = (\varphi_1, \dots, \varphi_n)(\gamma_{1\sigma}, \dots, \gamma_{n\sigma}) \cdot \sigma\tau \\
&\qquad = (\varphi_1\gamma_{1\sigma}, \dots, \varphi_n\gamma_{n\sigma}) \cdot \sigma\tau.
\end{aligned}$$

Então

$$\begin{aligned}
&(s_1, \dots, s_n)((\varphi_1, \dots, \varphi_n)\sigma(\gamma_1, \dots, \gamma_n)\tau) \\
&\qquad = (s_1, \dots, s_n)((\varphi_1\gamma_{1\sigma}, \dots, \varphi_n\gamma_{n\sigma}) \cdot \sigma\tau) \\
&\qquad = (s_1\varphi_1\gamma_{1\sigma}, \dots, s_n\varphi_n\gamma_{n\sigma})^{\sigma\tau} \\
&\qquad = (s_{1\tau^{-1}\sigma^{-1}}\varphi_{1\tau^{-1}\sigma^{-1}}\gamma_{1\tau^{-1}\sigma^{-1}\sigma}, \dots, s_{n\tau^{-1}\sigma^{-1}}\varphi_{n\tau^{-1}\sigma^{-1}}\gamma_{n\tau^{-1}\sigma^{-1}\sigma}) \\
&\qquad = (s_{1\tau^{-1}\sigma^{-1}}\varphi_{1\tau^{-1}\sigma^{-1}}\gamma_{1\tau^{-1}}, \dots, s_{n\tau^{-1}\sigma^{-1}}\varphi_{n\tau^{-1}\sigma^{-1}}\gamma_{n\tau^{-1}}).
\end{aligned}$$

Por outro lado,

$$\begin{aligned}
&((s_1,\ldots,s_n)(\varphi_1,\ldots,\varphi_n)\sigma)(\gamma_1,\ldots,\gamma_n)\tau\\
&\qquad= ((s_1\varphi_1,\ldots,s_n\varphi_n)^\sigma)(\gamma_1,\ldots,\gamma_n)\tau\\
&\qquad= (s_{1\sigma^{-1}}\varphi_{1\sigma^{-1}},\ldots,s_{n\sigma^{-1}}\varphi_{n\sigma^{-1}})(\gamma_1,\ldots,\gamma_n)\tau\\
&\qquad= (s_{1\sigma^{-1}}\varphi_{1\sigma^{-1}}\gamma_1,\ldots,s_{n\sigma^{-1}}\varphi_{n\sigma^{-1}}\gamma_n)^\tau\\
&\qquad= (s_{1\tau^{-1}\sigma^{-1}}\varphi_{1\tau^{-1}\sigma^{-1}}\gamma_{1\tau^{-1}},\ldots,s_{n\tau^{-1}\sigma^{-1}}\varphi_{n\tau^{-1}\sigma^{-1}}\gamma_{n\tau^{-1}}).
\end{aligned}$$

Com isso mostramos que

$$(s_1,\ldots,s_n)((\varphi_1,\ldots,\varphi_n)\sigma(\gamma_1,\ldots,\gamma_n)\tau) = ((s_1,\ldots,s_n)(\varphi_1,\ldots,\varphi_n)\sigma)(\gamma_1,\ldots,\gamma_n)\tau,$$

isto é, $\psi((\varphi_1,\ldots,\varphi_n)\sigma(\gamma_1,\ldots,\gamma_n)\tau) = \psi((\varphi_1,\ldots,\varphi_n)\sigma)\circ\psi((\gamma_1,\ldots,\gamma_n)\tau)$, ou seja, ψ é homomorfismo de grupos.

Seja agora $(\varphi_1,\ldots,\varphi_n)\sigma \in \operatorname{Ker}\psi$. Desta forma

$$(s_1,\ldots,s_n)((\varphi_1,\ldots,\varphi_n))\sigma = (s_{1\sigma^{-1}}\varphi_{1\sigma^{-1}},\ldots,s_{n\sigma^{-1}}\varphi_{n\sigma^{-1}}) = (s_1,\ldots,s_n),$$

isto é $s_{i\sigma^{-1}}\varphi_{i\sigma^{-1}} = s_i$, para todo $i = 1,\ldots,n$ e para todo s_i. Escolha $s_j = 1$, para todo $j \neq i$ e $s_i = s \in S$ com $s \neq 1$. Se $i\sigma \neq i$ então $s_{i\sigma} = 1$ e assim $s_{(i\sigma)\sigma^{-1}}\varphi_{(i\sigma)\sigma^{-1}} = s_{i\sigma} = 1$, então $s_i\varphi_i = 1$, e como φ_i é um automorfismo obtemos que $s_i = 1$, contradição. Logo $i\sigma = i$, para todo $i = 1,\ldots,n$, ou seja, σ é a permutação identidade (1). Desta forma $s_i\varphi_i = s_i$, para todo $i = 1,\ldots,n$ e para todo s_i. Como φ_i é um automorfismo temos então que φ_i é a aplicação identidade 1_S para todo $i = 1,\ldots,n$. Desta forma $(\varphi_1,\ldots,\varphi_n)\sigma = (1_S,\ldots,1_S)(1)$, ou seja, $\operatorname{Ker}\psi$ é trivial.

Com isso obtemos que $Aut(S) \wr S_n$ é isomorfo a um subgrupo de $Aut(S^n)$. Para concluirmos a proposição vamos recorrer ao Lema de Imersão 2.21. Vimos na Proposição 2.18 que S^n é um subgrupo normal minimal de $Aut(S^n)$ e vimos na Proposição 2.20 que os subgrupos normais minimais de S^n são da forma $N_i = \{1\}\times\ldots\times\{1\}\times S\times\{1\}\times\ldots\times\{1\}$, onde a i-ésima coordenada de N_i é igual a S. Seja $\beta \in Aut(S^n)$. Então β leva um subgrupo normal minimal de S^n em outro subgrupo normal minimal de S^n, isto é, $N_i^\beta = N_j$, para algum j. Temos que $N_i \leq S^n \leq Aut(S^n)$. Agora considere a ação por conjugação de $Aut(S^n)$ em $\{N_1,\ldots,N_n\}$. Essa ação é transitiva. De fato, se $\{N_{i1},\ldots,N_{ik}\}$ é uma órbita então $N_{i1}\times\ldots\times N_{ik} \trianglelefteq Aut(S^n)$. Mas $N_{i1}\times\ldots\times N_{ik} \leq S^n \leq Aut(S^n)$ e S^n é normal minimal em $Aut(S^n)$. Logo existe apenas uma órbita. Agora, como a ação é de conjugação, o estabilizador de N_1 corresponde ao normalizador $N_{Aut(S^n)}(N_1)$. Seja $H = N_{Aut(S^n)}(N_1)$. Temos então que o índice de H em $Aut(S^n)$ é o número de conjugados de N_1 em $Aut(S^n)$, isto é, $[Aut(S^n) : H] = n$.

Agora, como H normaliza N_1 e $N_1 \cong S$, considere $\xi : H \to Aut(S)$ o homomorfismo canônico. Temos que $\mathrm{Ker}(\xi) = C_{Aut(S^n)}(N_1)$. Vamos calcular o core de $\mathrm{Ker}(\xi)$ em $Aut(S^n)$.

$$(\mathrm{Ker}(\xi))_{Aut(S^n)} = (C_{Aut(S^n)}(N_1))_{Aut(S^n)} = \bigcap_{\beta \in Aut(S^n)} (C_{Aut(S^n)}(N_1))^\beta =$$

$$\bigcap_{\beta \in Aut(S^n)} C_{Aut(S^n)}(N_1^\beta) = (C_{Aut(S^n)}(N_1)) \cap \ldots \cap (C_{Aut(S^n)}(N_n)) = C_{Aut(S^n)}(S^n) = \{1\}.$$

Então pelo Lema de Imersão 2.21 o homomorfismo

$$f : Aut(S^n) \to Aut(S) \wr S_n$$

tem núcleo $\mathrm{Ker}(f) = (\mathrm{Ker}(\xi))_{Aut(S^n)} = \{1\}$. Portanto $Aut(S^n)$ é isomorfo a um subgrupo de $Aut(S) \wr S_n$. Logo $Aut(S^n) \cong Aut(S) \wr S_n$. ∎

Agora que já definimos o produto entrelaçado vamos mostrar que $G = S_n \wr S_m$ é um grupo primitivo do tipo 2, para $n \geq 5$ e $m \geq 1$.

Proposição 2.23 *Sejam $n \geq 5$ e m um inteiro positivo. Então $G = S_n \wr S_m$ é um grupo primitivo do tipo 2 de grau n^m.*

Demonstração: Lembre que $G = S_n \wr S_m = (S_n)^m \rtimes S_m$, um elemento de G é da forma $(\sigma_1, \ldots, \sigma_m)\tau$, com $\sigma_i \in S_n$, $i = 1, \ldots, m$ e $\tau \in S_m$, e o produto de $(\sigma_1, \ldots, \sigma_m)\tau$ por $(\gamma_1, \ldots, \gamma_m)\rho$ em G é dado por

$$\begin{gathered}(\sigma_1, \ldots, \sigma_m)\tau(\gamma_1, \ldots, \gamma_m)\rho = \\ (\sigma_1, \ldots, \sigma_m)\tau(\gamma_1, \ldots, \gamma_m)\tau^{-1}\tau\rho = \\ (\sigma_1, \ldots, \sigma_m)(\gamma_1, \ldots, \gamma_m)^{\tau^{-1}}\tau\rho = \\ (\sigma_1, \ldots, \sigma_m)(\gamma_{1\tau}, \ldots, \gamma_{m\tau})\tau\rho = \\ (\sigma_1\gamma_{1\tau}, \ldots, \sigma_m\gamma_{m\tau})\tau\rho.\end{gathered}$$

Como $n \geq 5$ temos que A_n é o único subgrupo normal próprio de S_n, então $N = (A_n)^m$ é um subgrupo normal não abeliano de G. Vamos agora mostrar que N é um subgrupo normal minimal de G. Sejam N_i, N_j subgrupos normais minimais de N com $i \neq j$. Então a permutação $(ij) \in S_m$ é tal que $N_i^{(ij)} = N_j$. Seja agora $\{1\} \neq K \leq N$ com $K \trianglelefteq G$. Como K é normal em N existe i tal que $N_i \leq K$. Agora, como $K \trianglelefteq G$, temos que $K^g = K$, para todo $g \in G$. Tome $g = 1(ij)$. Obtemos então que $N_j \leq K$, para todo j. Desta forma $K = N$ e logo N é um subgrupo normal minimal de G. Vamos agora mostrar que $C_G(N) = \{1\}$. Sejam $g = (\sigma_1, \ldots, \sigma_m)\tau \in G$, $n = (1, \ldots, 1, a, 1, \ldots, 1) \in N$, temos que $n^g \neq n$ se $\tau \neq (1)$. Desta forma $C_G(N) \leq S_n^m$. Assim $C_G(N) \leq C_{S_n^m}(A_n^m) = (C_{S_n}(A_n))^m = (\{1\})^m$. Logo A_n^m é um subgrupo normal minimal de G com centralizador trivial. Pelo Item (b) da Proposição 2.14, G é um grupo primitivo do tipo 2.

Seja $X = \{1, \ldots, n\}$ e considere a ação de G no conjunto $X^m = \{(i_1, \ldots, i_m) : i_k \in \{1, \ldots, n\}, 1 \leq k \leq m\}$ dada por $(i_1, \ldots, i_m)(\sigma_1, \ldots, \sigma_m)\tau = (i_{1\tau}\sigma_{1\tau}, \ldots, i_{m\tau}\sigma_{m\tau})$. Essa ação é transitiva pois dado $(i_1, \ldots, i_m) \in X^m$, como $(\sigma_1, \ldots, \sigma_m) \in (S_n)^m$ temos que $(i_1, \ldots, i_m)(\sigma_1, \ldots, \sigma_m)(1) = (i_1\sigma_1, \ldots, i_m\sigma_m)$ e então

$$X^n \subseteq \{(i_1\sigma_1, \ldots, i_m\sigma_m) : \sigma_i \in S_n, \} \subseteq O_G((i_1, \ldots, i_m)) = \{(i_1, \ldots, i_m)g : g \in G\} \subseteq X^n.$$

Agora vamos construir um subgrupo maximal M com core trivial e índice n^m. Considere $Stab((i, \ldots, i)) \leq G$, onde $i \in \{1, \ldots, n\}$. Temos que $Stab((i, \ldots, i)) = Stab(i) \wr S_m$, onde $Stab(i) \leq S_n$ e $Stab(i) \cong S_{n-1}$. De fato, se $(\sigma_1, \ldots, \sigma_m)\tau \in Stab((i, \ldots, i))$ então $(i_\tau\sigma_{1\tau}, \ldots, i_\tau\sigma_{m\tau}) = (i, \ldots, i)$, ou seja $i_\tau\sigma_{k\tau} = i$, para todo $k = 1, \ldots, m$. Como τ apenas permuta as coordenadas temos que $i\sigma_k = i$, para todo $k = 1 \ldots, m$, isto é, $\sigma_k \in Stab(i)$. Então $(\sigma_1, \ldots, \sigma_m)\tau \in Stab(i) \wr S_m$. Com as mesmas contas prova-se que $Stab(i) \wr S_m \subseteq Stab(i, \ldots, i)$. Defina então $M = Stab(i, \ldots, i) \cong S_{n-1} \wr S_m$. Como S_{n-1} não contém A_n temos que $M_G = \{1\}$. Além disso $[G : M] = (n!)^m m!/((n-1)!)^m m! = n^m$. Nos resta mostrar que M é um subgrupo maximal de G.

Sejam agora $K = (S_{n-1})^m$ e $B = (S_n)^m$. Temos que $G = B \rtimes S_m$, $M = K \rtimes S_m$ e $K \leq B$. Vamos mostrar que $M = N_G(K)$. Como $K \trianglelefteq M$ temos que $M \leq N_G(K)$. Note que

$$N_G(K) \cap B = N_B(K) = N_{S_n^m}(S_{n-1}^m) = (N_{S_n}(S_{n-1}))^m = S_{n-1}^m = K,$$

onde $N_{S_n}(S_{n-1}) = S_{n-1}$, já que S_{n-1} é um subgrupo não normal maximal de S_n. Além disso dado $(\sigma_1, \ldots, \sigma_m) \in K$, com $\sigma_i \in S_{n-1}$, $i = 1, \ldots, m$, e $\tau \in S_m$ temos que

$$\tau^{-1}(\sigma_1, \ldots, \sigma_m)\tau = (\sigma_1, \ldots, \sigma_m)^\tau = (\sigma_{1\tau^{-1}}, \ldots, \sigma_{m\tau^{-1}}) \in K,$$

ou seja, $S_m \subseteq N_G(K)$. Assim $BN_G(K) \supseteq BS_m = G$ e então $G = BN_G(K)$. Portanto

$$[G : N_G(K)] = |G| \,/\, |N_G(K)| = |BN_G(K)| \,/\, |N_G(K)| =$$
$$|B|\,|N_G(K)| \,/\, |N_G(K)|\,|N_G(K) \cap B| = |B| \,/\, |K| = (n!)^m/((n-1)!)^m = n^m.$$

Com isso $M \leq N_G(K)$ e $[G : M] = [G : N_G(K)]$, ou seja, $M = N_G(K)$.

Seja agora H um subgrupo maximal de G contendo M. Note que como $B \trianglelefteq G$, $H \cap B \trianglelefteq H$ e se $H \cap B = K$ então $K \trianglelefteq H$ e $H \subseteq N_G(K) = M$, ou seja, $H = M$ e M é um subgrupo maximal de G. Nos resta então mostrar que $H \cap B = K$. Observe que $K \subseteq M \subseteq H$ e $K \subseteq B$, ou seja, $K \subseteq H \cap B$. Por outro lado, escrevendo $B = B_1 \times B_2 \times \cdots \times B_m$ e $R_i = \{1\} \times \cdots \times \{1\} \times B_i \times \{1\} \times \cdots \times \{1\}$, $i = 1, \ldots, m$, a ação de conjugação de G sobre o conjunto $\Omega = \{R_1, \ldots, R_m\}$ é tal que

$$R_i^{(\sigma_1, \ldots, \sigma_m)\tau} = R_i^\tau = R_j,$$

com $i, j = 1, \ldots, m$. Desta forma a ação é transitiva e o núcleo dessa ação é formado pelos elementos $(\sigma_1, \ldots, \sigma_m) \in B$. Agora, como $G = BM$ temos também que $G = BH$. Assim dado $g \in G$, podemos escrever $g = hb$, com $h \in H$ e $b \in B$. Então dados $R_i, R_j \in \Omega$, existe $g \in G$ tal que $R_i^g = R_j$. Como $g = hb$, com $h \in H$ e $b \in B$, e o núcleo da ação é

B obtemos que $R_i^h = R_j$. Então podemos considerar a ação de conjugação de H sobre Ω, onde essa ação é transitiva.

Fixando R_i e R_j, existe $h \in H$ com $(R_i)^h = R_j$. Considere então as projeções

$$\pi_i : B \to R_i,$$

dadas por

$$(b_1, \ldots, b_m) \mapsto (1, \ldots, b_i, \ldots, 1),$$

para todo $i = 1, \ldots, m$. Restringindo cada π_i para $H \cap B$ temos que

$$\pi_i|_{H\cap B} : H \cap B \twoheadrightarrow \pi_i(H \cap B),$$

é um homomorfismo sobrejetor com núcleo $(\prod\limits_{t\neq i} R_t) \cap H$. Assim pelo Teorema do Isomorfismo,

$$\pi_i(H \cap B) \cong H \cap B/(\prod_{t\neq i} R_t) \cap H.$$

Vamos mostrar que $\pi_i(H\cap B)$ é isomorfo a $\pi_j(H\cap B)$ para todos $i, j = 1, \ldots, m$. Considere a aplicação

$$\varphi : H \cap B \xrightarrow{\lambda} H \cap B \twoheadrightarrow H \cap B/(\prod_{t\neq j} R_t) \cap H,$$

dada pela composição de λ e $\pi_j|_{H\cap B}$, onde λ é a conjugação por $h \in H$ fixado tal que $(R_i)^h = R_j$ e λ é um isomorfismo pois $H \cap B \trianglelefteq H$. Note que $x \in \operatorname{Ker}\varphi$ se, e somente se, $(x^h)_j = 1$, ou seja, a i-ésima coordenada de x é trivial. Assim $\operatorname{Ker}\varphi = (\prod\limits_{t\neq i} R_t) \cap H$ e dessa forma pelo Teorema do Isomorfismo

$$\pi_i(H \cap B) \cong H \cap B/(\prod_{t\neq i} R_t) \cap H \overset{\varphi}{\cong} H \cap B/(\prod_{t\neq j} R_t) \cap H \cong \pi_j(H \cap B).$$

Desta forma $\pi_i(H \cap B) \cong \pi_j(H \cap B)$ para todos $i, j = 1, \ldots, m$.

Agora, como $K \subseteq H \cap B$ temos que $S_{n-1} \cong \pi_i(K) \subseteq \pi_i(H \cap B) \subseteq S_n$ e como S_{n-1} é um subgrupo maximal de S_n temos que $\pi_i(H \cap B) \cong S_{n-1}$ ou $\pi_i(H \cap B) = S_n$. Vamos analisar os dois casos. Suponha que $\pi_i(H \cap B) \cong S_{n-1}$ para todo $i = 1, \ldots, m$. Temos que

$$|H \cap B| \leq \prod_{i=1}^{m} |\pi_i(H \cap B)| = (n-1)!^m = |K|.$$

Mas como $K \subseteq H \cap B$ temos que $K = H \cap B$.

Suponha agora que $\pi_i(H\cap B) = S_n$. Vamos mostrar que $H\cap R_i \trianglelefteq R_i$. Tome $y \in H\cap R_i$, temos que $\pi_j(y) = 1$ para todo $j \neq i$. Seja $r \in R_i$, como $\pi_i|_{H\cap B} : H \cap B \to S_n \cong R_i$

é sobrejetiva, existe $x \in H \cap B$ tal que $\pi_i(x) = r$. Como $r = (1, \ldots, 1, r_i, 1, \ldots, 1)$, $y = (1, \ldots, 1, y_i, 1, \ldots, 1)$, $x = (x_1, x_2, \ldots, x_n)$ e $\pi_i(x) = r$ temos que $r^{-1}yr = x^{-1}yx$, desta forma $r^{-1}yr \in H$ pois $x, y \in H$. Por outro lado, $r^{-1}yr = x^{-1}yx \in R_i$, pois $r, y \in R_i$. Segue então que $r^{-1}yr = x^{-1}yx \in H \cap R_i$ e então $H \cap R_i \trianglelefteq R_i \cong S_n$. Agora, como $H \cap R_i$ contém $K_i \cong S_{n-1}$, $H \cap R_i \trianglelefteq R_i \cong S_n$ e S_{n-1} é um subgrupo maximal não normal de S_n, obtemos que $H \cap R_i \cong S_n$. Assim $H \cap R_i = R_i$ e então $R_i \leq H$ para todo $i = 1, \ldots, m$. Como $B = \prod_{i=1}^{m} R_i$ temos que $B \subseteq H$. Desta forma $BH = H < G$, contradição. Logo não podemos ter $\pi_i(H \cap B) = S_n$. Então $\pi_i(H \cap B) = S_{n-1}$ o que implica que $H \cap B = K$, provando a proposição. ∎

2.5 Grupos primitivos do tipo 3

Agora iremos tratar dos grupos primitivos do tipo 3. O primeiro exemplo dado será $G = S \times S$, onde S é um grupo simples não abeliano.

Exemplo 2.4 *Seja $G = S \times S$, onde S é um grupo simples não abeliano. Vimos na Proposição 2.20 que os subgrupos normais minimais de G são $N_1 = S \times \{1\}$ e $N_2 = \{1\} \times S$. Temos que $G/N_1 \cong S$ e que S é um grupo primitivo do tipo 2, ou seja, G/N_1 é um grupo primitivo do tipo 2. Tomando $M = \{(s, s) : s \in S\} \leq G$ temos que $g = (x, y) \in G$ pode ser escrito como $(xy^{-1}, 1)(y, y) \in N_1M$, ou seja, $G = N_1M$. Além disso, se $(x, y) \in N_1 \cap M$ temos que $y = 1$ e $x = y$, ou seja, $(x, y) = (1, 1)$ e assim $N_1 \cap M = \{1\} \times \{1\}$. Desta forma M complementa N_1 em G. Da mesma maneira G/N_2 é um grupo primitivo do tipo 2 e M complementa N_2 em G. Logo pelo Corolário 2.15 temos que G é um grupo primitivo do tipo 3.*

Agora, se X é um grupo primitivo do tipo 2, podemos nos perguntar se $G = X \times X$ é um grupo primitivo do tipo 3. Como X é um grupo primitivo do tipo 2, existe um único subgrupo L normal minimal em X. Desta forma os subgrupos $L \times \{1\}$ e $\{1\} \times L$ são subgrupos normais minimais de G. Se $L = X$ estamos no caso em que X é um grupo simples não abeliano pois L é não abeliano e X não possui subgrupos normais próprios, e como vimos no exemplo acima, G é um grupo primitivo do tipo 3. Agora se $L \neq X$ temos que $C_{X \times X}(L \times \{1\}) = C_X(L) \times C_X(\{1\}) = \{1\} \times X \neq \{1\} \times L$. Com isso se $X \neq L$, G não é um grupo primitivo do tipo 3. Por outro lado, veremos na seguinte proposição que $G = \{(x, y) \in X \times X : xL = yL\}$ é um grupo primitivo do tipo 3.

Proposição 2.24 *Seja X um grupo primitivo do tipo 2 com subgrupo normal minimal L. Então $G = \{(x, y) \in X \times X : xL = yL\}$ é um grupo primitivo do tipo 3.*

Demonstração: Os subgrupos normais minimais de G são $N_1 = L \times \{1\}$ e $N_2 = \{1\} \times L$. Note que

$$C_G(N_1) = \{(x, y) \in X \times X : x \in C_X(L), xL = yL\} = \{(1, y) \in X \times X : L = yL\} =$$
$$\{(1, y) \in X \times X : y \in L\} = \{1\} \times L = N_2,$$

já que $C_X(L) = \{1\}$. Analogamente, $C_G(N_2) = N_1$. Tome $H = \{(x, x) \in G\}$. Dado $g = (x, y) \in G$, temos que $xL = yL$, assim $xy^{-1} \in L$ e então $g = (xy^{-1}, 1)(y, y) \in N_1H$, mostrando que $G = N_1H$. Por outro lado, se $(x, y) \in N_1 \cap H$ então $y = 1$ e $x = y$, ou seja, $(x, y) = (1, 1)$ e assim $N_1 \cap H = \{1\} \times \{1\}$. Desta forma H complementa N_1 em G. Da mesma forma H complementa $N_2 = C_G(N_1)$ em G. Pela Proposição 2.13, G é um grupo primitivo do tipo 1 ou 3. Como $C_G(N_1) = N_2 \neq N_1$ obtemos que G é um grupo primitivo do tipo 3. ■

Agora, se
$$G = \{(x_1, \ldots, x_n) \in X^n : x_1L = \ldots = x_nL\},$$
com $n \geq 3$, onde X é um grupo primitivo do tipo 2, então G não é um grupo primitivo pois G possui mais que dois subgrupos normais minimais. O grupo G é denotado por $\delta_n(X)$. Como vimos na proposição acima, $\delta_2(X)$ é um grupo primitivo do tipo 3, desta forma o quociente
$$\delta_n(X)/(\{1\} \times \{1\} \times L \times \ldots \times L) \cong \delta_2(X)$$
é um grupo primitivo do tipo 3, e o quociente
$$\delta_n(X)/(\{1\} \times L \times \ldots L \cong \delta_1(X)) \cong X$$
é um grupo primitivo do tipo 2.

Capítulo 3

Complementos de fatores principais de um grupo solúvel

3.1 Fatores principais

Definição 3.1 *Sejam G um grupo e $H, K \trianglelefteq G$ tais que $K \leq H$. Dizemos que H/K é um fator principal de G se H/K é um subgrupo normal minimal de G/K.*

Seja G um grupo finito. Como H/K é um subgrupo normal minimal de G/K, H/K é um produto direto de cópias de grupos simples. Temos duas possibilidades: no primeiro caso H/K é abeliano, assim existe um primo p tal que H/K é um p-grupo abeliano elementar; no segundo caso H/K é não abeliano, desta forma existe um grupo simples não abeliano S tal que $H/K \cong S \times \cdots \times S$.

Um fator principal H/K de G é dito central se $H/K \leq Z(G/K)$.

Dado um grupo G e um fator principal H/K de G, o grupo G age por conjugação em H/K: para $h \in H$ e $g \in G$, temos $(hK)^g = h^g K$. Essa ação de G em H/K define um homomorfismo de grupos

$$\theta : G \to Aut(H/K)$$

tal que

$$\mathrm{Ker}(\theta) = \{g \in G : h^g K = hK,\ \forall\ h \in H\} = C_G(H/K).$$

Desta forma H/K é um G-grupo. Então se H_1/K_1, H_2/K_2 são dois fatores principais de G, uma aplicação $\varphi : H_1/K_1 \to H_2/K_2$ será um G-isomorfismo se φ for um isomorfismo de grupos e $((h_1K_1)^g)^\varphi = ((h_1K_1)^\varphi)^g$ para quaisquer $h_1K_1 \in H_1/K_1$ e $g \in G$.

Note que se A/B é normal em G/B e é G-isomorfo a um fator principal de G, então pela Proposição 2.2, A/B é também um fator principal de G.

Definição 3.2 *Seja H/K um fator principal de um grupo finito G. Dizemos que H/K é complementado se existe um subgrupo L de G tal que $HL = G$ e $H \cap L = K$. Neste caso L é dito um complemento de H/K em G .*

Exemplo 3.1 1. *Seja $G = C_p \times C_p$ onde p é um número primo, $H = C_p \times \{1\}$, $K = \{1\} \times \{1\}$. Tomando $L = \{1\} \times C_p$, temos que $HL = G$ e $H \cap L = K$. Assim L é um complemento de H/K em G.*

2. *Seja G um p-grupo cíclico finito de ordem p^n e sejam H, K dois subgrupos de G com $K \leq H$ e $|H : K| = p$. Então G/K é um p-grupo cíclico, logo H/K é complementado em G/K se, e somente se, $H = G$, em tal caso, o único complemento é K/K.*

Definição 3.3 *Seja H/K um fator principal de um grupo finito G. Dizemos que H/K é Frattini se $H/K \leq \Phi(G/K)$.*

Note que o fator principal H/K não pode ser simultaneamente complementado e Frattini, pois pelo Teorema 1.26 - (b), se $H/K \leq \Phi(G/K)$, então o único suplemento de H/K em G/K é G/K, isto é, não existe um subgrupo próprio L de G tal que $HL = G$.

Por outro lado, se H/K é um fator principal não abeliano de G, então $H/K \nleq \Phi(G/K)$. De fato, suponha que $H/K \leq \Phi(G/K)$. Como $\Phi(G/K)$ é um grupo nilpotente e subgrupo de grupo nilpotente é nilpotente obtemos que H/K é nilpotente. Então o subgrupo derivado $[H/K, H/K]$ é diferente de H/K. Como H/K é um subgrupo normal minimal de G/K, $[H/K, H/K] \trianglelefteq G$ e $[H/K, H/K] < H/K$ obtemos que $[H/K, H/K] = K/K$, ou seja, H/K é um fator principal abeliano de G, contradição.

Agora veremos que se H/K é um fator principal abeliano de G, então ou ele é complementado ou ele é Frattini.

Proposição 3.4 *Seja H/K um fator principal abeliano de um grupo finito G. Então*

(a) H/K ou é complementado ou é Frattini, e

(b) se H/K é complementado, então cada complemento é um subgrupo maximal de G.

Demonstração:

(a) Suponha que $H/K \nleq \Phi(G/K)$. Vamos mostrar que o subgrupo normal minimal H/K de G/K é complementado em G/K. Sem perda de generalidade podemos supor que $K = \{1\}$. Como $H \nleq \Phi(G)$, existe um subgrupo maximal M de G tal que $H \nleq M$. Desta forma temos que $M \leq MH$ e $M \cap H < H$. Como M é um subgrupo maximal de G, obtemos que $G = MH$. Além disso, $M \cap H \trianglelefteq M$, pois $H \trianglelefteq G$ e H é abeliano. Logo $M \cap H \trianglelefteq G$. Como H é um subgrupo normal minimal de G, obtemos que $M \cap H = \{1\}$.

(b) Novamente vamos supor que $K = \{1\}$. Seja M um complemento de H em G e seja L um subgrupo maximal de G tal que $M \leq L < G$. Se $H \leq L$, então $HM = L < G$, contradizendo que M complementa H em G. Então $H \nleq L$. Desta forma $HL = G$. Agora, $H \cap L \leq H$, $H \cap L \trianglelefteq L$ pois $H \trianglelefteq G$ e H é abeliano. Assim $H \cap L \trianglelefteq HL = G$. Como H é normal minimal em G, $H \cap L = \{1\}$ ou $H \cap L = H$. Se $H \cap L = H$ então $H \leq L$, contradição. Assim $H \cap L = \{1\}$. Desta forma, L complementa H em G. Assim $L \cong G/H \cong M$, o que implica que $|M| = |L|$. Como $M \leq L$, obtemos que $M = L$ e M é um subgrupo maximal de G.

■

Um exemplo de um fator principal não abeliano não complementado será dado no apêndice desse trabalho.

Lembre que uma série

$$1 = U_0 \trianglelefteq U_1 \trianglelefteq \ldots \trianglelefteq U_r = G$$

é dita uma série principal se $U_i \trianglelefteq G$ e os fatores U_i/U_{i-1} são fatores principais de G, para todo $i = 1, 2, \ldots, r$. Para finalizar esta seção, vamos mostrar que dadas duas séries principais de um grupo finito G, existe uma bijeção entre os fatores principais dessas duas séries de tal forma que os fatores correspondentes são G-isomorfos e os fatores principais Frattini da primeira série correspondem aos fatores principais Frattini da segunda série.

Lema 3.5 ([4], Capítulo A, Lema 9.11) *Sejam K e N subgrupos normais de um grupo finito G com $N \leq K$ e K nilpotente. Se $K/N \leq \Phi(G/N)$, então $K \leq \Phi(G)N$.*

Lema 3.6 *Sejam N_1 e N_2 subgrupos normais minimais distintos de um grupo finito G. Então existe uma bijeção*

$$\tau : \{N_1, N_1N_2/N_1\} \to \{N_2, N_1N_2/N_2\}$$

tal que os fatores principais correspondentes são G-isomorfos e os fatores principais Frattini correspondem aos fatores principais Frattini.

Demonstração: Seja $N = N_1N_2$ e suponha que $N_1 \leq \Phi(G)$. Temos que $N/N_2 = N_1N_2/N_2 \leq \Phi(G)N_2/N_2 \leq \Phi(G/N_2)$, ou seja, N/N_2 é Frattini. Se N/N_1 também é Frattini, isto é, $N/N_1 \leq \Phi(G/N_1) = \Phi(G)/N_1$, então $N \leq \Phi(G)$ e logo $N_2 \leq N_1N_2 \leq \Phi(G)$. Desta forma os quatro fatores principais são Frattini e a aplicação τ com $\tau N_1 = N/N_2$ e $\tau(N_1N_2/N_1) = N_2$ satisfaz o lema. Por outro lado, se N/N_1 não é Frattini, então $N/N_1 \nleq \Phi(G/N_1) = \Phi(G)/N_1$, logo $N_2 \leq N \nleq \Phi(G)$, isto é, N_2 não é Frattini e a mesma escolha de τ é suficiente. Se todos os fatores principais não são Frattini tomamos o mesmo τ.

Resta agora considerar o caso onde $N_1 \cap \Phi(G) = N_2 \cap \Phi(G) = \{1\}$ e, sem perda de generalidade, $N/N_2 \leq \Phi(G/N_2)$. Como N/N_2 é um subgrupo normal minimal de G/N_2,

$N/N_2 \leq \Phi(G/N_2)$ que é um grupo nilpotente, segue que N/N_2 é abeliano (elementar). Como N_1, N_2 são ambos normais minimais em G temos que $N_1 \cap N_2 = \{1\}$ e assim $N/N_2 \cong_G N_1$, ou seja, N_1 é abeliano. Como N_1 é abeliano e não é Frattini, pela Proposição 3.4, existe um complemento M para N_1 em G, onde M é um subgrupo maximal de G. Seja $N_3 = M \cap N$, vamos mostrar que $N_3 \trianglelefteq G$. Temos que $N = N_1 \times N_2$ e N_1 é abeliano, assim $N_1 \leq Z(N)$. Como $N_3 = M \cap N \leq N$ temos que N_1 normaliza N_3. Assim $N_3 = M \cap N \trianglelefteq M$ e $N_1 \leq N_G(N_3)$ e logo $N_3 \trianglelefteq MN_1 = G$. Além disso $N_3N_1 = (M \cap N)N_1 = MN_1 \cap N = G \cap N = N$, $N_1 \cap N_3 = N_1 \cap (M \cap N) = \{1\} \cap N = \{1\}$ e então

$$N_3 \cong_G N_3/N_1 \cap N_3 \cong_G N_3N_1/N_1 = N/N_1 \cong_G N_2.$$

Segue que N_3 é um subgrupo normal minimal de G, assim $N_2 \cap N_3 = \{1\}$. Se $N_3 = N_2$, então M/N_2 é um complemento em G/N_2 para N/N_2, pois $M \cap N = N_2$ e $MN = MN_1N_2 = GN_2 = G$, o que contradiz que N/N_2 é Frattini. Portanto $N_3 \neq N_2$. Segue então que M não contém N_2, pois $N_3 = M \cap N$ e N contem N_2, logo $MN_2 = G$ e isso implica que $N_3N_2 = (M \cap N)N_2 = N$. Assim $N_3 \cong_G N/N_2 \cong_G N_1$.

Logo N_2, N_3 e consequentemente N são abelianos. Pelo Lema 3.5, como $N/N_2 \leq \Phi(G/N_2)$ temos que $N \leq \Phi(G)N_2$. Dessa forma

$$N_2(N \cap \Phi(G)) = N_2\Phi(G) \cap N = N = N_2N_3. \qquad (*)$$

Seja agora $A = N \cap \Phi(G)$. Como M é um subgrupo maximal de G, $\Phi(G) \leq M$ e assim $A \leq N \cap M = N_3$. Intersectando os dois lados da equação (*) por N_3 obtemos que

$$N_3 = N_2A \cap N_3 = (N_2 \cap N_3)A = A.$$

Então $N \cap \Phi(G) = N_3$ e portanto que

$$N/N_1 = N_3N_1/N_1 = (N \cap \Phi(G))N_1/N_1 = N_1\Phi(G) \cap N/N_1 \leq N_1\Phi(G)/N_1 \leq \Phi(G/N_1)$$

é Frattini e os quatro fatores principais são G-isomorfos. Tomando $\tau N_1 = N_2$ e $\tau(N/N_1) = N/N_2$ o lema segue. ∎

Teorema 3.7 *Sejam $\mathcal{H}_1$ e $\mathcal{H}_2$ duas séries principais de um grupo finito G. Então existe uma bijeção entre os fatores principais de $\mathcal{H}_1$ e os fatores principais de $\mathcal{H}_2$ tal que fatores correspondentes são G-isomorfos e os fatores principais Frattini de $\mathcal{H}_1$ correspondem aos fatores principais Frattini de $\mathcal{H}_2$.*

Demonstração: Pelo Teorema de Jordan-Hölder temos que $\mathcal{H}_1$ e $\mathcal{H}_2$ possuem o mesmo comprimento e então podemos denotar

$$\mathcal{H}_1 : G = U_0 > U_1 > \cdots > U_r = 1$$

$$\mathcal{H}_2 : G = V_0 > V_1 > \cdots > V_r = 1$$

Vamos provar o teorema por indução sobre r. Para $r = 1$ o resultado segue trivialmente.

Seja $r > 1$ e suponha que o teorema vale para todos os grupos com séries principais de comprimento $\leq r - 1$.

Se $U_{r-1} = V_{r-1}$, a hipótese de indução aplicada a G/U_{r-1} produz uma correspondência adequada entre os fatores das duas séries situados acima de U_{r-1} e fazendo U_{r-1} corresponder a V_{r-1} temos a conclusão desejada.

Suponha agora que os subgrupos normais minimais U_{r-1} e V_{r-1} são distintos e seja $N = U_{r-1}V_{r-1}$. Como $U_{r-1} \cap V_{r-1} = \{1\}$ pois U_{r-1} e V_{r-1} são subgrupos normais minimais de G segue que $N/U_{r-1} \cong_G V_{r-1}$ e $N/V_{r-1} \cong_G U_{r-1}$ são fatores principais de G. Desta forma existem duas séries principais $\mathcal{H}_3$ e $\mathcal{H}_4$ da seguinte maneira

$$\mathcal{H}_3 : G = W_0 > \cdots > W_{r-3} > N > U_{r-1} > 1$$

$$\mathcal{H}_4 : G = W_0 > \cdots > W_{r-3} > N > V_{r-1} > 1$$

Vamos dizer que duas séries principais são equivalentes se existe uma bijeção satisfazendo o teorema. Isto define uma relação de equivalência nas séries principais de G. Como $\mathcal{H}_1$ e $\mathcal{H}_3$ possuem o subgrupo normal minimal U_{r-1} em comum, como foi feito anteriormente, essas duas séries são equivalentes. Analogamente as séries $\mathcal{H}_2$ e $\mathcal{H}_4$ são equivalentes. Mais ainda, como as séries $\mathcal{H}_3$ e $\mathcal{H}_4$ coincidem até N, segue do Lema 3.6 que $\mathcal{H}_3$ e $\mathcal{H}_4$ são também equivalentes. Logo $\mathcal{H}_1$ e $\mathcal{H}_2$ são equivalentes. ∎

Por outro lado, G-isomorfismo não preserva o fato do fator principal ser complementado. Como exemplo considere o grupo abeliano $G = C_{p^2} = \langle x \rangle$, onde p é um número primo. Note que, por G ser um grupo abeliano dois fatores principais são G-isomorfos se, e somente se, são isomorfos. Seja $K = \langle x^p \rangle$. Temos $K \cong C_p$ e $G/K \cong C_p$. Assim $G/K \cong K$ e então $G/K \cong_G K$. Por um lado temos que K não é complementado em G, pois todos os subgrupos de G são G, K e $\{1\}$. Por outro lado temos que G/K é complementado em G por K pois $GK = G$ e $G \cap K = K$.

3.2 Complementos de fatores principais de um grupo solúvel

Esta seção se baseia no artigo *On complemented chief factors of finite soluble groups* [2] de D. W. Barnes.

Um G-módulo A é por definição um G-grupo abeliano. Seja H/K um fator principal abeliano de um grupo finito G. Vimos no Capítulo 1, que H/K é um grupo abeliano elementar, isto é, $H/K \cong C_p^n$, onde p é um número primo. Como H/K é um G-grupo abeliano temos que H/K é um G-módulo e então H/K pode ser visto como um $\mathbb{F}_pG$-módulo no significado usual de módulo sobre um anel unitário, assim a teoria usual dos módulos se aplica ao nosso caso. Observe também que um subgrupo normal minimal abeliano de um grupo finito G é um G-módulo irredutível.

Definição 3.8 *Sejam G um grupo solúvel finito, A um G-módulo irredutível que aparece como um fator principal abeliano complementado de G e $C = C_G(A)$ o centralizador de A em G. Defina*

$$R = R(A) = \bigcap\{T \trianglelefteq G : T < C,\ C/T \cong_G A,\ C/T \ \ \textit{é complementado}\}.$$

Dizemos que C/R é a A-coroa de G ou a coroa definida por A.

Considerando o monomorfismo

$$\varphi : C/R \hookrightarrow \prod_{C/T \cong_G A,\ C/T \text{ é complementado}} C/T,$$

temos que C/R é isomorfo a um subgrupo de $\prod_{C/T \cong_G A,\ C/T \text{ é complementado}} C/T$, isto é, existe $d \in \mathbb{Z}^+$ tal que $C/R \cong_G A^d$. Definimos $\delta_G(A) = d$. Desta forma a coroa definida por A, vista como um G-módulo, é semissimples.

Lema 3.9 *Sejam $A, B \leq G$. Se $[A, B] \leq A$ então $B \leq N_G(A)$.*

Demonstração: Temos que $a^{-1}b^{-1}ab \in A$, para quaisquer $a \in A$ e $b \in B$. Assim $b^{-1}abA = aA = A$, isto é, $b^{-1}ab \in A$,para quaisquer $a \in A$ e $b \in B$, ou seja, $b \in N_G(A)$. Logo $B \leq N_G(A)$. ■

Lema 3.10 *Sejam G um grupo finito, H/K um fator principal abeliano de G e M um complemento de H/K. Seja $C = C_G(H/K)$ e considere $S = C_M(H/K)$. Então $S = M_G$, G/S é um grupo primitivo do tipo 1 e C/S é o único subgrupo normal minimal de G/S. Mais ainda $C = HS$, $H \cap S = K$ e C/S é G-isomorfo a H/K.*

Demonstração: Pelo Item (b) da Proposição 3.4 temos que M é um subgrupo maximal de G. Como $[H, M_G] \leq H \cap M = K$ segue que $M_G \leq C_M(H/K)$.

Por outro lado, $[H, C_M(H/K)] \leq K$ e $K \leq C_M(H/K)$, assim $[H, C_M(H/K)] \leq C_M(H/K)$. Pelo Lema 3.9, $H \leq N_G(C_M(H/K))$. Como $C_M(H/K) = C \cap M \trianglelefteq M$ obtemos que $C_M(H/K) \trianglelefteq HM = G$ e então $C_M(H/K) \leq M_G$. Logo $S = C_M(H/K) = M_G$. Pelo Item (a) da Proposição 2.7 temos que G/S é um grupo primitivo.

Agora, sendo H/K abeliano, $H \leq C = C_G(H/K)$. Temos $C \cap M = C_M(H/K)$, assim $C = C \cap G = C \cap HM = H(C \cap M) = HC_M(H/K) = HS$. Além disso $H \cap C_M(H/K) \geq K$ e $H \cap C_M(H/K) \leq H \cap M = K$. Logo $H \cap C_M(H/K) = H \cap S = K$.

Com isso obtemos que $C/S = HS/S \cong_G H/H \cap S = H/K$. Em particular C/S é um subgrupo normal minimal abeliano de G/S. Assim G/S é primitivo do tipo 1 e pelo Teorema de Baer C/S é o único subgrupo normal minimal de G/S. ■

Lema 3.11 *Seja G um grupo finito. Se N é um subgrupo normal minimal abeliano de G e M é um subgrupo próprio de G com $MN = G$, então $M \cap N = \{1\}$.*

Demonstração: Temos que $M \cap N \trianglelefteq M$. Como N é abeliano temos que $M \cap N \trianglelefteq N$. Logo $M \cap N \trianglelefteq MN = G$, $M \cap N < N$, pois se $M \cap N = N$ teríamos $N \subseteq M$ e $G \neq MN$. Como N é um subgrupo normal minimal de G obtemos então que $M \cap N = \{1\}$. ■

Lema 3.12 *Sejam G um grupo finito solúvel, H/K um fator principal de G, A um G-módulo irredutível e C/R a coroa definida por A. Então H/K é complementado e G-isomorfo a A se, e somente se, $C \geq HR > KR$ e nesse caso $HR/KR \cong_G H/K$ e H/K tem uma classe de conjugação de complementos para cada escolha de um submódulo maximal D/KR de C/KR não contendo HR/KR.*

Demonstração: Suponha que $H/K \cong_G A$ e seja M um complemento de H/K em G. Pelo Lema 3.10, $H \cap M_G = K$, $HM_G = C_G(H/K) = C_G(A) = C$ e $M_G = C_M(H/K)$. Além disso $H/K = H/H \cap M_G \cong_G HM_G/M_G = C/M_G$ e M/M_G é um complemento de C/M_G em G/M_G. Como $A \cong_G C/M_G$, pela definição de R temos que $R \leq M_G \leq C$. Assim $KR \leq HR \leq HM_G = C$. Se $KR = HR$ então

$$M_G \cap HR = (M_G \cap H)R = KR = HR.$$

Desta forma $KR = HR \subseteq M_G$. Assim, $M_G = (KR)M_G = (HR)M_G = HM_G = C$ e portanto $K = H \cap M_G = H \cap C = H$, contradição. Logo $KR < HR$. Portanto obtemos $C \geq HR > KR$.

Reciprocamente, suponha que $C \geq HR > KR$. Vamos mostrar que $HR/KR \cong_G H/K$. Temos $HR/KR \neq 1$ e $HR/KR = H(KR)/KR \cong_G H/H \cap KR = H/K(H \cap R)$, isto é, $HR/KR \cong_G H/K(H \cap R)$. Temos $K \leq K(H \cap R) = H \cap KR \leq H$. Como H/K é um fator principal de G segue que $K(H \cap R) = H$ ou $K(H \cap R) = K$, pois caso contrário H/K não seria normal minimal em G/K. Se $K(H \cap R) = H$ então $1 \neq HR/KR \cong_G H/H$, contradição. Logo $K(H \cap R) = K$ e então $HR/KR \cong_G H/K$.

Agora, como $C/R \cong_G A^d$ e $H/K \cong_G HR/KR$ é um fator principal de G entre C e R temos que $HR/KR \cong_G A$. Desta forma $H/K \cong_G A$.

Vamos mostrar agora que H/K é complementado. Como C/KR é G-isomorfo a uma soma direta de cópias de A obtemos que C/KR é semissimples, pelo Lema 1.32, existe um complemento D/KR de HR/KR em C/KR, isto é, $C/KR = (HR/KR) \cdot (D/KR)$ e $(HR/KR) \cap (D/KR) = KR/KR$. Além disso D/KR é um G-submódulo maximal de C/KR pois $D/KR < (HR/KR) \cdot (D/KR) = C/KR$ e $\frac{(HR/KR)\cdot(D/KR)}{1\cdot(D/KR)} \cong_G \frac{HR}{KR}$ que é simples.

Dessa forma $A \cong_G HR/KR \cong_G (C/KR)/(D/KR) \cong_G C/D$, ou seja, $C/D \cong_G A$. Temos então que $C_G(C/D) = C_G(A) = C$ e assim $C_{G/D}(C/D) = C/D$.

Como $C/D \cong_G A$ é normal minimal em G/D temos pelo Lema 1.23 que $F(G/D) \leq C_{G/D}(C/D) = C/D$ e como C/D é abeliano, logo nilpotente, pela definição do subgrupo de fitting $C/D \leq F(G/D)$. Assim $F(G/D) = C/D$. Pelo item (a) do Teorema 1.27 temos $\Phi(G/D) \leq F(G/D) = C/D$. Agora não podemos ter $C/D \leq \Phi(G/D)$, pois neste caso, $\Phi(G/D) = F(G/D)$, contradizendo a Proposição 1.28.

Assim $C/D \nleq \Phi(G/D)$, isto é, C/D é um fator principal não Frattini de G. Desta forma, pelo Teorema 3.4, existe um complemento M/D para C/D em G/D e M/D é um subgrupo maximal de G/D. Além disso, como M/D complementa o subgrupo normal minimal $C/D = C_{G/D}(C/D)$ de G/D segue do item (b) da Proposição 2.13 que G/D é um grupo primitivo do tipo 1 ou 3. Como C/D é abeliano, não podemos ter G/D um grupo primitivo do tipo 3. Assim G/D é um grupo primitivo do tipo 1 e segue do Teorema 2.17 que todos os complementos de C/D em G/D são conjugados.

Vamos agora mostrar que M complementa H/K. Como M/D é um subgrupo maximal de G/D temos que M é um subgrupo maximal de G, assim $MH = G$ ou $M \supseteq H$. Se $M \supseteq H$ temos que $M \supseteq HR$ pois $M \supseteq D \supseteq R$ e $D = C \cap M \supseteq HR$, assim $KR = D \cap HR = HR$, contradição. Além disso, como $MH = G$ obtemos que $(M/K)(H/K) = G/K$. Assim pelo Lema 3.11, $(M/K) \cap (H/K) = K/K$ e então $M \cap H = K$. Com isso mostramos que H/K é um fator principal de G complementado e G-isomorfo a A.

$$
\begin{tikzcd}
G \arrow[dr, dash] \arrow[dd, dash] & \\
& M \arrow[dd, dash] \\
C \arrow[dr, dash] \arrow[dd, dash] & \\
& D \arrow[dd, dash] \\
HR \arrow[dr, dash] & \\
& KR
\end{tikzcd}
$$

Vamos agora mostrar que todos os complementos de H/K são obtidos por meio do procedimento acima, completando assim a demonstração do lema. Seja M um complemento de H/K em G com $H/K \cong_G A$. Tomando $D = M_G$ temos $C/D \cong_G A$ como visto na primeira parte da demonstração. Vamos mostrar que D/KR complementa HR/KR para isso vamos mostrar que D não contém HR. Se $D \supseteq HR$ então $M \supseteq D \supseteq HR \supseteq H$ e então $MH = M \neq G$, contradição. Sendo $C/D \cong_G A$ um G-grupo simples, segue que D/KR é maximal (como G-submódulo) em C/KR. ∎

Sejam G é um grupo finito, A é um G-módulo irredutível finito e $F = End_G(A)$ o anel dos G-endomorfismos de A com as operações de soma e composição. Como A é um G-módulo irredutível segue do Lema de Schur que se $0 \neq f \in F$ então f é isomorfismo. Desta forma F é um anel de divisão e pelo Teorema de Wedderburn segue que F é um corpo. Mais ainda, A é um espaço vetorial sobre F com respeito a $fa = f(a)$, para quaisquer $f \in F$ e $a \in A$. Note que para uma soma direta de cópias de A (que pode ser visto como um F-espaço vetorial), G-submódulo e F-subespaço vetorial são noções distintas. Isso acontece porque dado $g \in G$ a função

$$\begin{aligned} A &\longrightarrow A \\ a &\longmapsto a^g = g^{-1}ag. \end{aligned}$$

não é G-homomorfismo em geral. Para a função acima ser um G-homomorfismo precisamos que $(a^g)^h = (a^h)^g$ para quaisquer $g, h \in G$ e para todo $a \in A$. Note que se o grupo G é um grupo abeliano então a função acima é um G-homomorfismo.

Lema 3.13 *Sejam G um grupo finito, A um G-módulo irredutível e $F = End_G(A)$. Seja V uma soma direta de d cópias de A e seja H um submódulo minimal de V. Então o número de submódulos maximais de V não contendo H é q^{d-1}, onde $q = |F|$.*

Demonstração: Temos $V = \{(a_1, \ldots, a_d) \mid a_i \in A\}$ e aplicações

$$\varepsilon_i : A \to V,$$

definidas por $\varepsilon_i(a) = (0, 0, \ldots, 0, a, 0, \ldots, 0)$ onde a entrada não nula está na i-ésima coordenada.

Seja M um submódulo maximal de V sobre F. Então existe um G-homomorfismo sobrejetivo

$$\alpha : V \to A$$

com $M = \operatorname{Ker} \alpha$.

Para cada i, temos $\lambda_i \in F$ definidos por

$$\lambda_i = \alpha\varepsilon_i : A \to A.$$

Assim

$$\alpha(a_1, \ldots, a_d) = \alpha(a_1, 0, \ldots, 0) + \ldots + \alpha(0, \ldots, 0, a_d) =$$

$$\alpha\varepsilon_1(a_1) + \ldots + \alpha\varepsilon_d(a_d) = \sum_{i=1}^{d} \alpha\varepsilon_i(a_i) = \sum_{i=1}^{d} \lambda_i(a_i).$$

Em particular os λ_i não podem ser todos nulos pois α não é nulo. Pela expressão acima, $(a_1, \ldots, a_d) \in \operatorname{Ker} \alpha = M$ se, e somente se, $\displaystyle\sum_{i=1}^{d} \lambda_i(a_i) = 0$.

Vamos também mostrar que α é F-linear. Seja $\lambda \in F$. Obtemos, pelo Teorema de Wedderburn, que F é um corpo, assim a operação de composição em F é comutativa, então para qualquer $\lambda_i \in F$ temos que $\lambda\lambda_i = \lambda_i\lambda$. Desta forma

$$\alpha(\lambda a_1, \ldots, \lambda a_d) = \sum_{i=1}^{d} \lambda_i(\lambda(a_i)) =$$
$$\sum_{i=1}^{d}(\lambda_i\lambda)(a_i) = \sum_{i=1}^{d}(\lambda\lambda_i)(a_i) =$$
$$\lambda(\sum_{i=1}^{d}(\lambda_i(a_i))) = \lambda\alpha(a_1, \ldots, a_d).$$

Por outro lado, para quaisquer $\lambda_1, \ldots, \lambda_d \in F$, não todos nulos, definimos

$$\alpha \colon V \longrightarrow A$$
$$(a_1, \ldots, a_d) \longmapsto \sum_{i=1}^{d} \lambda_i(a_i).$$

Vamos mostrar que α é um G-homomorfismo sobrejetor. Dado $g \in G$ temos que

$$\alpha(a_1^g, \ldots, a_d^g) = \sum_{i=1}^{d} \lambda_i(a_i^g) = \sum_{i=1}^{d} \lambda_i(a_i)^g = \alpha(a_1, \ldots, a_d)^g,$$

onde $\lambda_i(a_i^g) = \lambda_i(a_i)^g$ pois para todo $i = 1, \ldots, d$, λ_i é um G-endomorfismo. Assim α é um G-homomorfismo. Agora tomando um λ_i não nulo, a restrição de α para o i-ésimo fator de V coincide com λ_i, que é isomorfismo (como visto pelo lema de Schur) logo α é sobrejetiva (porque admite uma restrição sobrejetiva). Seja $M = \mathrm{Ker}(\alpha)$. Note que $V/M \cong_G A$. Como A é um G-módulo irredutível segue que M é um submódulo maximal de V.

Desta forma vimos que os submódulos maximais de V são do tipo $\mathrm{Ker}\,\alpha$, com $\alpha(a_1, \ldots, a_d) = \sum_{i=1}^{d} \lambda_i(a_i)$, onde os $\lambda_i \in F$ não são todos nulos.

Para cada $0 \neq \lambda \in F$, $(\lambda\lambda_1, \ldots, \lambda\lambda_d)$ define o mesmo submódulo maximal que $(\lambda_1, \ldots, \lambda_d)$. De fato, se $\beta : V \to A$ é definida por $\beta(a_1, \ldots, a_d) = \sum_{i=1}^{d} \lambda\lambda_i(a_i)$ então

$$\sum_{i=1}^{d} \lambda\lambda_i(a_i) = 0 \Leftrightarrow \lambda\lambda_1(a_1) + \ldots + \lambda\lambda_d(a_d) = 0 \Leftrightarrow \lambda(\sum_{i=1}^{d} \lambda_i(a_i)) = 0 \Leftrightarrow \sum_{i=1}^{d} \lambda_i(a_i) = 0,$$

isto é, $\operatorname{Ker}\beta = \operatorname{Ker}\alpha$.

Logo o número de submódulos maximais de V é

$$\frac{q^d - 1}{q - 1}.$$

Pelo Teorema da correspondência existe uma correspondência biunívoca entre os submódulos de V/H e os submódulos de V contendo H. Como H é minimal temos que $V/H \cong_G A^{d-1}$ e assim repetindo o que foi feito acima o número de submódulos maximais de V contendo H é

$$\frac{q^{d-1} - 1}{q - 1}.$$

Portanto o número de submódulos maximais de V não contendo H é

$$\frac{q^d - 1}{q - 1} - \frac{q^{d-1} - 1}{q - 1} = q^{d-1}.$$

Isso termina a demonstração. ■

Lema 3.14 *Sejam G um grupo solúvel finito e N um subgrupo normal minimal de G complementado. Se M é um complemento de N em G então número de conjugados de M é $|N|$ se $N \nleq Z(G)$ e 1 se $N \leq Z(G)$.*

Demonstração: Se $N \leq Z(G)$ então $M \trianglelefteq G$ e então o número de conjugados de M em G é 1. Agora suponha $N \nleq Z(G)$. Como N é um subgrupo normal minimal de um grupo solúvel temos que N é abeliano. Pelo item (b) da Proposição 3.4, tomando $H = N$ e $K = \{1\}$, temos que M é um subgrupo maximal de G. Como $M \leq N_G(M) \leq G$ e M é um subgrupo maximal de G segue que $M = N_G(M)$ ou $G = N_G(M)$. Suponha que $G = N_G(M)$. Temos então $M \trianglelefteq G$ e assim $[M, N] \leq M \cap N = \{1\}$, isto é, $M \leq C_G(N)$. Então para todo $g = mn \in G = MN$ e $n_1 \in N$ temos que

$$gn_1 = mnn_1 = mn_1n = n_1mn = n_1g,$$

isto é, $N \leq Z(G)$, contradição.

Logo $M = N_G(M)$ e temos portanto

$$\#\text{conjugados de } M = |G : N_G(M)| = |G : M| = |N|.$$

Isso termina a demonstração. ■

Proposição 3.15 (Gaschütz [6], Proposição 3) *Sejam G um grupo solúvel finito, H/K um fator principal de G complementado e G-isomorfo a A e C/R a coroa definida por H/K. O número de complementos de H/K em G/K é*

$$|A|^t \, |End_G(A)|^{m-1},$$

onde $t = 0$ se H/K é central, $t = 1$ se H/K não é central e m é o número de fatores G-isomorfos a A entre C e KR de uma série principal de G que passa por C e KR.

Demonstração: Seja M um complemento de H/K em G. Se $H/K \leq Z(G/K)$ temos que $G/K = H/K \times M/K$. Por outro lado se H/K não é central temos que $G/K = H/K \rtimes M/K$e M/K não é normal em G/K. Pelo Lema 3.14 o tamanho da classe de conjugação de M é $|H/K|^t$ onde $t = 0$ se H/K é central e $t = 1$ se H/K não é central.

Agora, no Lema 3.12 vimos que H/K tem uma classe de complementos para todo D/KR submódulo maximal de C/KR que complementa HR/KR. Este submódulo maximal D/KR de C/KR não contém HR/KR. Mais ainda, um submódulo maximal D/KR de C/KR complementa HR/KR se, e somente se, não contém HR/KR. No Lema 3.13 vimos que o número de submódulos maximais D/KR que não contêm HR/KR é $|F|^{m-1}$ onde $F = End_G(A)$ e $C/KR \cong A^m$. Desta forma o número de classes de complementos é $|F|^{m-1}$ e o resultado segue. ∎

Sejam agora $\mathcal{H}_1$ e $\mathcal{H}_2$ duas séries principais de um grupo finito solúvel G. Queremos construir uma bijeção entre os fatores principais dessas duas séries de tal forma que fatores complementados G-isomorfos a A em $\mathcal{H}_1$ sejam levados em fatores complementados G-isomorfos a A em $\mathcal{H}_2$.

Sejam G um grupo solúvel finito, A um G-módulo irredutível e C/R a coroa definida por A. Fixe H/K um fator principal G-isomorfo a A de $\mathcal{H}_1$. Vamos escrever a série $\mathcal{H}_1$ como

$$\mathcal{H}_1 : 1 = U_0 < U_1 < \ldots < U_r = G.$$

Como H/K é um fator principal de G da série $\mathcal{H}_1$, existe um j com $U_j = H$ e $U_{j-1} = K$. Além disso $H/K = U_j/U_{j-1} \cong_G A$ e como H/K é abeliano $U_j \leq C = C_G(A)$. Vamos agora multiplicar a série $\mathcal{H}_1$ por R, obtendo assim

$$R \leq U_1R \leq U_2R \leq \ldots \leq GR = G.$$

Como $U_j = H$ e $U_{j-1} = K$ temos que $U_jR = HR$ e $U_{j-1}R = KR$. Seja m o maior índice tal que $U_m/U_{m-1} \cong_G A$. Escrevemos então

$$R \leq U_1R \leq \ldots \leq U_mR \leq \ldots \leq G.$$

Novamente temos que $U_m \leq C$, e como $R \leq C$, $U_mR \leq C$. Escrevemos então

$$R \leq U_1R \leq \ldots \leq U_mR \leq C.$$

Agora completamos a sequência obtida acima à esquerda (de $\{1\}$ até R), completamos a sequência obtida acima à direita (de C até G) e depois refinamos para uma série principal. Chamaremos a série principal obtida de $\mathcal{S}_1$. Note que pelo Lema 3.12, SR/TR é um fator principal de $\mathcal{S}_1$ para todo fator principal S/T complementado de $\mathcal{H}_1$ que é G-isomorfo a A.

Sejam agora

$$X = \{\text{fatores principais de } \mathcal{H}_1 \text{ complementados e } G\text{-isomorfos a } A\},$$

$$Y = \{\text{fatores principais de } \mathcal{S}_1 \text{ complementados e } G\text{-isomorfos a } A\},$$

$$\delta : X \to Y,$$

onde δ é dada por $S/T \mapsto SR/TR$.

Vamos mostrar que δ é injetiva. Seja $S^*/T^* \in X$ tal que $\delta(S/T) = \delta(S^*/T^*)$, isto é, $SR/TR = S^*R/T^*R$, ou seja, $SR = S^*R$ e $TR = T^*R$. Vamos mostrar que $S = S^*$ e $T = T^*$. Pelo Lema 3.12, temos que $C \geq SR = S^*R > TR = T^*R$. Se $S^* \leq T$ temos $SR = S^*R \leq TR \leq SR$, isto é $SR = TR$, contradizendo o Lema 3.12. Então $S^* > T$. Se $S \leq T^*$ temos $S^*R = SR \leq T^*R \leq S^*R$, isto é $S^*R = T^*R$, contradizendo novamente o Lema 3.12. Então $S > T^*$. Como S/T e S^*/T^* estão na mesma série temos que $S \leq S^*$ ou $S^* \leq S$. Agora se $S > S^* > T$ então $S^*/T < S/T$ e como $\mathcal{H}_1$ é uma série principal, S^*/T é normal minimal em G/T, contradizendo que S/T é normal minimal em G/T. Se $S^* > S > T^*$ então $S/T^* < S^*/T^*$ e como $\mathcal{H}_1$ é uma série principal, S/T^* é normal minimal em G/T^*, contradizendo que S^*/T^* é normal minimal em G/T^*. Logo $S = S^*$. Analogamente obtemos que $T = T^*$. Portanto a aplicação δ é injetiva.

Como G é um grupo solúvel, um fator principal é não Frattini se, e somente se, é complementado. Segue então do Teorema 3.7 que $|X| = |Y|$. Desta forma δ é uma bijeção.

Analogamente, fixado um fator principal complementado G-isomorfo a A de $\mathcal{H}_2$, construimos uma série $\mathcal{S}_2$ e se

$$Z = \{\text{fatores principais de } \mathcal{H}_2 \text{ complementados e } G\text{-isomorfos a } A\},$$

$$W = \{\text{fatores principais de } \mathcal{S}_2 \text{ complementados e } G\text{-isomorfos a } A\},$$

podemos construir uma bijeção

$$\lambda : Z \to W.$$

Agora, sejam F_i, $i = 1, 2, \ldots, s$, os fatores principais complementados e G-isomorfos a A de $\mathcal{S}_1$ e L_i, $i = 1, 2, \ldots, s$, os fatores principais complementados G-isomorfos a A de $\mathcal{S}_2$. Pela construção das séries $\mathcal{S}_1$ e $\mathcal{S}_2$ temos $R \leq F_i, L_i \leq C$ para todo $i = 1, 2 \ldots, s$.

$$\begin{tikzcd}[arrows=dash]
 & F_1 \arrow[r] & F_2 \arrow[r] & \ldots \arrow[r] & F_s \arrow[dr] & \\
R \arrow[ur] \arrow[dr] & & & & & C \\
 & L_1 \arrow[r] & L_2 \arrow[r] & \ldots \arrow[r] & L_s \arrow[ur] &
\end{tikzcd}$$

Pela fórmula de Gaschütz, o número de complementos de F_i é $|A|^t \, |End_G(A)|^{s-i}$ e o número de complementos de L_i é $|A|^t \, |End_G(A)|^{s-i}$ para todo $i = 1, 2, \ldots, s$. Então contruimos uma bijeção θ entre os fatores principais complementados e G-isomorfos a A de $\mathcal{S}_1$ e os fatores principais complementados e G-isomorfos a A de $\mathcal{S}_2$ da seguinte maneira

$$\theta : F_i \mapsto L_i,$$

para todo $i = 1, 2, \ldots, s$. Portanto, compondo as aplicações δ, θ e λ obtemos uma bijeção entre X e Z de tal forma que fatores principais G-isomorfos a A e complementados de $\mathcal{H}_1$ são levados em fatores principais G-isomorfos a A e complementados de $\mathcal{H}_2$. Com isso provamos o seguinte teorema:

Teorema 3.16 *Sejam $G = U_0 > U_1 > \ldots > U_r = 1$ e $G = V_0 > V_1 > \ldots > V_r = 1$ duas séries principais de um grupo solúvel finito G. Então existe uma correspondência biunívoca entre os fatores das duas séries, tais que os fatores correspondentes são G-isomorfos e possuem o mesmo número de complementos.*

Capítulo 4

Complementos de fatores principais não abelianos de um grupo finito

4.1 G-grupos G-equivalentes

Esta e a próxima seção são baseadas no artigo *On Complemented Nonabelian Chief Factors of a Finite Group* [10] de P. Jiménez-Seral and J. Lafuente.

Dado um G-grupo A temos o produto semidireto $GA = G \ltimes A$, onde a multiplicação é dada por

$$g_1 a_1 \cdot g_2 a_2 = g_1 g_2 a_1^{g_2} a_2,$$

com $g_1, g_2 \in G$, $a_1, a_2 \in A$.

A noção de G-isomorfismo não é boa para fatores principais não abelianos. Por exemplo, considere G um grupo primitivo do tipo 3 com subgrupos normais minimais A e B. Vimos que A e B são não abelianos e que A e B não saõ G-isomorfos.

Definição 4.1 *Sejam A e B dois G-grupos. Dizemos que A e B são G-equivalentes e denotamos por $A \sim_G B$ se existem um isomorfismo $\varphi : A \to B$ e um isomorfismo $\phi : GA \to GB$ tal que o diagrama abaixo comuta:*

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r, "i"] \arrow[d, "\varphi"] & GA \arrow[r, "\pi"] \arrow[d, "\phi"] & G \arrow[r] \arrow[d, "1_G"] & 1 \\
1 \arrow[r] & B \arrow[r, "j"] & GB \arrow[r, "\rho"] & G \arrow[r] & 1
\end{tikzcd} \tag{1}$$

No diagrama acima, $i : A \to GA$ é dado por $a^i = 1a = a$, $j : B \to GB$ é dado por $b^j = 1b = b$, $\pi : GA \to G$ é dado por $(ga)^\pi = g$ e $\rho : GB \to G$ é dado por $(gb)^\rho = g$, para quaisquer $a \in A$, $b \in B$ e $g \in G$.

Vamos mostrar que $\sim_G$ é uma relação de equivalência. Temos que $A \sim_G A$ tomando $\varphi = 1_A : A \to A$ e $\phi = 1_{GA} : GA \to GA$. Se $A \sim_G B$ por $\varphi : A \to B$ e $\phi : GA \to GB$, então $B \sim_G A$ por $\varphi^{-1} : B \to A$ e $\phi^{-1} : GB \to GA$. Se $A \sim_G B$ por $\varphi_1 : A \to B$ e $\phi_1 : GA \to GB$ e se $B \sim_G$ por $\varphi_2 : B \to C$ e $\phi_2 : GB \to GC$ então $A \sim_G C$ por $\varphi_1\varphi_2 : A \to C$ e $\phi_1\phi_2 : GA \to GC$.

Se $\varphi : A \to B$ é um G-isomorfismo então $(ga)^\phi = ga^\varphi$, $g \in G$, $a \in A$, define um isomorfismo $\phi : GA \to GB$ que faz o diagrama (1) comutar. De fato, ϕ é homomorfismo porque

$$\phi(g_1a_1g_2a_2) = \phi(g_1g_2a_1^{g_2}a_2) = g_1g_2(a_1^{g_2}a_2)^\varphi = g_1g_2(a_1^{g_2})^\varphi a_2^\varphi = g_1g_2(a_1^\varphi)^{g_2}a_2^\varphi,$$
$$\phi(g_1a_1)\phi(g_2a_2) = g_1a_1^\varphi g_2a_2^\varphi = g_1g_2(a_1^\varphi)^{g_2}a_2^\varphi,$$

e o diagrama (1) comuta pois

$$a^{i\phi} = (1a)^\phi = 1a^\varphi = a^\varphi,$$
$$a^{\varphi j} = (a^\varphi)^j = 1a^\varphi = a^\varphi.$$
$$(ga)^{\pi 1_G} = g^{1_G} = g,$$
$$(ga)^{\phi\rho} = (ga^\varphi)^\rho = g.$$

Desta forma se A e B são G-grupos G-isomorfos temos que A e B são G-equivalentes. A recíproca não é verdadeira. Sejam S um grupo simples não abeliano, $G = S \times S$ e $A = S \times \{1\}$ e $B = \{1\} \times S$ os subgrupos normais minimais de G. Veremos na próxima seção que A e B são G-equivalentes. Por outro lado, vimos que G é um grupo primitivo do tipo 3 com $C_G(A) = B$ e $C_G(B) = A$. Assim $C_G(A) \neq C_G(B)$ e portanto A e B não são G-isomorfos.

Definição 4.2 *Seja B um G-grupo, um 1-cociclo de G em B é uma aplicação $\beta : G \to B$ tal que $(g_1g_2)^\beta = (g_1^\beta)^{g_2}g_2^\beta$. Denotamos por $Z^1(G,B)$ o conjunto dos 1-cociclos de G em B.*

O núcleo de β é definido por $\operatorname{Ker}\beta = \{g \in G : g^\beta = 1\}$. Temos que $\operatorname{Ker}\beta \leq G$. De fato, dados $g, h \in \operatorname{Ker}\beta$, temos que $(gh)^\beta = (g^\beta)^h h^\beta = 1^h 1 = 1$ e $1 = 1^\beta = (gg^{-1})^\beta = (g^\beta)^{g^{-1}}(g^{-1})^\beta = (g^{-1})^\beta$. Por outro lado, $\operatorname{Ker}\beta$ não é necessariamente um subgrupo normal de G.

Dado um G-grupo B e um 1-cociclo $\beta \in Z^1(G,B)$, então $b^{\eta(g)} = b^{gg^\beta} = (g^\beta)^{-1}b^g g^\beta$ define um homomorfismo $\eta : G \to AutB$. De fato, sejam $g_1, g_2 \in G$ e $b \in B$, temos por uma lado

$$b^{\eta(g_1g_2)} = (b^{g_1g_2})^{(g_1g_2)^\beta} = (b^{g_1g_2})^{(g_1^\beta)^{g_2}g_2^\beta} = (g_2^\beta)^{-1}((g_1^\beta)^{g_2})^{-1}b^{g_1g_2}(g_1^\beta)^{g_2}g_2^\beta,$$

e por outro lado

$$b^{\eta(g_1)\eta(g_2)} = (b^{g_1g_1^\beta})^{g_2g_2^\beta} = (g_2^\beta)^{-1}((g_1^\beta)^{-1}b^{g_1}g_1^\beta)^{g_2}g_2^\beta = (g_2^\beta)^{-1}((g_1^\beta)^{-1})^{g_2}b^{g_1g_2}(g_1^\beta)^{g_2}g_2^\beta,$$

isto é, η é um homomorfismo. O G-grupo correspondente é denotado B_β e chamado o G-grupo obtido de B por torção via β.

Proposição 4.3 *Sejam A e B dois G-grupos. A e B são G-equivalentes se, e somente se, existe um 1-cociclo $\beta \in Z^1(G,B)$ tal que $A \cong_G B_\beta$, isto é, existe um isomorfismo $\varphi : A \to B$ tal que $a^{g\varphi} = a^{\varphi g g^\beta}$, $a \in A$, $g \in G$.*

Demonstração: Suponha que A e B são G-equivalentes. Então o diagrama (1) comuta. Dessa forma dado $a \in A$, por um lado $a^{i\phi} = (1a)^\phi = a^\phi$, por outro lado, $a^{\varphi j} = (a^\varphi)^j = 1a^\varphi = a^\varphi$. Logo, como $a^{i\phi} = a^{\varphi j}$, temos que $a^\phi = a^\varphi$, para todo $a \in A$.

Defina $\beta : G \to B$ por $g^\beta = g^{-1}g^\phi$. Vamos mostrar que $g^\beta \in B$. Seja $g^\phi = xb$ com $x \in G$ e $b \in B$. Temos $(g1)^{\pi 1_G} = g$ e $(g1)^{\phi\rho} = (xb)^\rho = x$. Como o diagrama (1) comuta obtemos que $x = g$ e assim $g^\beta = g^{-1}g^\phi = g^{-1}gb = b \in B$. Agora vamos mostrar que β é um 1-cociclo. Temos que

$$(g_1g_2)^\beta = (g_1g_2)^{-1}(g_1g_2)^\phi = g_2^{-1}g_1^{-1}g_1^\phi g_2^\phi = g_2^{-1}g_1^{-1}g_1^\phi g_2 g_2^{-1}g_2^\phi = g_2^{-1}g_1^\beta g_2 g_2^\beta = (g_1^\beta)^{g_2}g_2^\beta,$$

isto é, β é um 1-cociclo.

Temos então que $a^{\varphi g g^\beta} = a^{\phi g g^{-1} g^\phi} = a^{\varphi g^\phi}$. Como a ação de um elemento de G no produto semi-direto é a ação de conjugação obtemos que

$$a^{\varphi g g^\beta} = a^{\varphi g^\phi} = (g^\phi)^{-1}a^\varphi g^\phi = (g^\phi)^{-1}a^\phi g^\phi = (a^g)^\phi = (a^g)^\varphi.$$

Reciprocamente, suponha que existe um 1-cociclo $\beta \in Z^1(G,B)$ tal que $A \cong_G B_\beta$, isto é, $a^{g\varphi} = a^{\varphi g g^\beta}$, onde $\varphi : A \to B$ é um isomorfismo. Defina $\phi : GA \to GB$ por $(ga)^\phi = gg^\beta a^\varphi$, com $a \in A$ e $g \in G$.

Dados $a \in A$, $b \in B$ e $g \in G$, temos que

$$a^{i\phi} = (1a)^\phi = 11^\beta a^\varphi = a^\varphi,$$

$$a^{\varphi j} = (a^\varphi)^j = 1a^\varphi = a^\varphi,$$

$$(ga)^{\pi 1_G} = g^{1_G} = g,$$

$$(ga)^{\phi\rho} = (gg^\beta a^\varphi)^\rho = g,$$

onde na última igualdade usamos que $g^\beta a^\varphi \in B$. Desta forma o diagrama (1) comuta e ϕ é homomorfismo porque

$$(g_1a_1g_2a_2)^\phi = (g_1g_2a_1^{g_2}a_2)^\phi = g_1g_2(g_1g_2)^\beta(a_1^{g_2}a_2)^\varphi = g_1g_2(g_1^\beta)^{g_2}g_2^\beta(a_1^{g_2})^\varphi a_2^\varphi =$$
$$g_1g_2g_2^{-1}g_1^\beta g_2g_2^\beta a_1^{\varphi g_2 g_2^\beta}a_2^\varphi = g_1g_2g_2^{-1}g_1^\beta g_2g_2^\beta(g_2^\beta)^{-1}g_2^{-1}a_1^\varphi g_2g_2^\beta a_2^\varphi =$$
$$= g_1g_1^\beta a_1^\varphi g_2g_2^\beta a_2^\varphi = (g_1a_1)^\phi(g_2a_2)^\phi.$$

Isso termina a demonstração. ■

Corolário 4.4 *Sejam A e B dois G-grupos abelianos. Então $A \cong_G B$ se, e somente se, A é G-equivalente a B.*

Demonstração: Como B é abeliano temos que $b^{gg^\beta} = b^g$ pois $g^\beta \in B$. Assim, para todo 1-cociclo β, $B \cong_G B_\beta$ e temos então pela proposição anterior que $A \cong_G B_\beta \cong_G B$ se, e somente se, A e B são G-equivalentes. ∎

Lembre que um fator principal H/K de G é dito Frattini se $H/K \leq \Phi(G/K)$ e é complementado se existe um subgrupo M de G tal que $MH = G$ e $M \cap H = K$ (assim M é um complemento de H/K em G). Vimos na Proposição 3.4 que um fator principal abeliano ou é complementado ou é Frattini. Por outro lado, vimos que os fatores principais não abelianos são sempre não Frattini. Além disso veremos no apêndice deste trabalho um exemplo de um fator principal não abeliano não complementado.

Proposição 4.5 *Seja H/K um fator principal não abeliano de G. Então H/K é complementado em G se, e somente se, existe um G-grupo B, $B \sim_G H/K$, tal que $H \leq C_G(B)$.*

Demonstração: Suponha que M é um complemento de H/K em G, onde H/K é um G-grupo com a ação de G sendo a ação de conjugação por $g \in G$. Considere o G-grupo $B = H/K$ com a ação de G definida por

$$\theta : G \to AutB$$

dada por $b^{\theta(g)} = b^m$, com b^m sendo uma conjugação, e o 1-cociclo

$$\beta : G \to B$$

dado por $g^\beta = hK$, se $g \in G$, $g = mh$, $m \in M$, $h \in H$. Note que θ e β são bem definidas (pela unicidade módulo K de $g \in G = MH$), vamos então mostrar que θ é um homomorfismo e β é um 1-cociclo. Sejam $g_1 = m_1h_1$, $g_2 = m_2h_2 \in G$. Temos que $g_1g_2 = m_1h_1m_2h_2 = m_1m_2m_2^{-1}h_1m_2h_2$. Note que $m_1m_2 \in M$ e como H é normal em G, $m_2^{-1}h_1m_2h_2 \in H$. Desta forma $b^{\theta(g_1g_2)} = b^{m_1m_2}$ e $b^{\theta(g_1)\theta(g_2)} = (b^{m_1})^{\theta(g_2)} = (b^{m_1})^{m_2}$, isto é, θ é um homomorfismo. Por outro lado, $(g_1g_2)^\beta = m_2^{-1}h_1m_2h_2K$ e

$$(g_1^\beta)^{\theta(g_2)}g_2^\beta = (h_1K)^{\theta(g_2)}(h_2K) = (h_1K)^{m_2}(h_2K) = m_2^{-1}(h_1K)m_2(h_2K) = m_2^{-1}h_1m_2h_2K,$$

isto é, $(g_1g_2)^\beta = ((g_1)^\beta)^{\theta(g_2)}g_2^\beta$.

Seja agora $\varphi : H/K \to B$ dada por $(xK)^\varphi = xK$, se $x \in H$. Com isto temos

$$(xK)^{g\varphi} = (x^gK)^\varphi = x^gK,$$

onde x^g é conjugação por g, e

$$[(xK)^{\varphi\theta(g)}]^{g^\beta} = [(xK)^{\theta(g)}]^{g^\beta} = [(xK)^m]^{g^\beta} =$$
$$(x^mK)^{hK} = x^{mh}K = x^gK = (x^gK)^\varphi = (xK)^{g\varphi}.$$

Logo pela Proposição 4.3 temos que $H/K \cong_G B_\beta$ e $H/K \sim_G B$. Por outro lado, $C_G(B) = \{mh, m \in M, h \in H : (xK)^m = xK, \forall x \in H\} = C_M(H/K)H$.

Reciprocamente, se existe um G-grupo B tal que $B \sim_G H/K$ e $H \leq C_G(B)$ temos por 4.3 um G-isomorfismo $\varphi : B \to (H/K)_\alpha$ onde $\alpha \in Z^1(G, H/K)$. Se $b \in B$, $h \in H$ temos $b^\varphi = (b^h)^\varphi = b^{\varphi h h^\alpha}$ e $h \in H \leq C_G(B)$. Portanto $hKh^\alpha \in C_{H/K}(H/K) = 1$, pois H/K é um fator principal não abeliano de G. Logo $h^\alpha = h^{-1}K$. Tome $M = \operatorname{Ker}\alpha$. Seja $g \in G$ e $g^\alpha = hK$, $h \in H$. Temos que $(gh)^\alpha = (g^\alpha)^h h^\alpha = (hK)^h(h^{-1}K) = (hK)(h^{-1}K) = 1K$. Com isto $gh \in \operatorname{Ker}\alpha$, segue que $G = HM$. Se $m \in M \cap H$ então $m^\alpha = K$ e $m^\alpha = m^{-1}K$, assim $m^{-1}K = K$, isto é, $m \in K$ e portanto $M \cap H \leq K$. Agora se $x \in K$ temos $x^\alpha = x^{-1}K = K$, isto é, $x \in M$. Como $K \leq H$ temos então $K \leq M \cap H$. Logo $K = M \cap H$. ■

Observe que o resultado é falso para fatores principais abelianos. Se H/K um fator principal abeliano Frattini de G, tomando $B \cong_G H/K$ temos $B \sim_G H/K$, $H \leq C_G(H/K) = C_G(B)$ mas H/K não é complementado.

4.2 Fatores principais G-relacionados

Definição 4.6 *Dois fatores principais de um grupo G são ditos G-relacionados se eles são G-isomorfos ou se existe um quociente primitivo do tipo 3 de G onde cada subgrupo normal minimal do quociente é G-isomorfo, respectivamente, a um dos fatores principais.*

Desta forma dados dois fatores principais H_1/K_1 e H_2/K_2 de G, H_1/K_1 e H_2/K_2 são G-relacionados se $H_1/K_1 \cong_G H_2/K_2$ ou se existe $N \trianglelefteq G$ tal que G/N é um grupo primitivo do tipo 3, $Soc(G/N) = A \times B$, $H_1/K_1 \cong_G A$ e $H_2/K_2 \cong_G B$. Se dois fatores principais de G são G-relacionados e não são G-isomorfos então os fatores principais são não abelianos, já que os subgrupos normais minimais de um grupo primitivo do tipo 3 são não abelianos. Nesta seção iremos mostrar que dois fatores principais são G-relacionados se, e somente se, são G-equivalentes. Desta forma seguirá que a relação de ser G-relacionado é uma relação de equivalência.

Considere

$$\mathcal{CF}(G) = \{H/K : H, K \trianglelefteq G, H/K \text{ é fator principal de } G\}$$

e defina para um G-grupo A

$$I_G(A) = \{g \in G : g \text{ induz um automorfismo interno em } A\}.$$

Proposição 4.7 *Sejam A e B dois G-grupos. Se $A \sim_G B$ então $I_G(A) = I_G(B)$.*

Demonstração: Suponha $A \sim_G B$. Pela Proposição 4.3 existe $\varphi : A \to B$ tal que $a^{g\varphi} = a^{\varphi g g^\beta}$, onde $a \in A$, $g \in G$ e $g^\beta \in B$.

Seja $g \in I_G(A)$, existe $x \in A$ tal que $a^g = a^x$, para todo $a \in A$. Temos

$$(a^x)^\varphi = (x^{-1}ax)^\varphi = (x^{-1})^\varphi a^\varphi x^\varphi = (x^\varphi)^{-1} a^\varphi x^\varphi = (a^\varphi)^{x^\varphi} \qquad (*)$$

Então
$$a^{\varphi g g^{\beta}} = a^{g\varphi} = a^{x\varphi},$$
assim
$$a^{\varphi g} = a^{x\varphi(g^{\beta})^{-1}} \overset{(*)}{=} (a^{\varphi})^{x^{\varphi}(g^{\beta})^{-1}},$$

onde $a^{\varphi}, x^{\varphi}(g^{\beta})^{-1} \in B$. Desta forma $g \in I_G(B)$, sendo $x^{\varphi}(g^{\beta})^{-1}$ um elemento de B. Portanto $I_G(A) \subseteq I_G(B)$. Sendo $\sim_G$ uma relação de equivalência, a inclusão $I_G(B) \subseteq I_G(A)$ segue de $B \sim_G A$. ∎

Lema 4.8 *Sejam G um grupo finito e H/K é um fator principal de G, então $I_G(H/K) = HC_G(H/K)$. Em particular, $I_G(H/K) = C_G(H/K)$ se H/K é um fator principal abeliano.*

Demonstração: Seja $g \in I_G(H/K)$, existe $aK \in H/K$ tal que $g^{-1}nKg = a^{-1}naK$, $\forall\, nK \in H/K$. Assim $ag^{-1}nK = nag^{-1}K$, $\forall\, nK \in H/K$, isto é $ag^{-1} \in C_G(H/K)$ e logo $g^{-1} \in a^{-1}C_G(H/K) \subseteq HC_G(H/K)$. Com isso $I_G(H/K) \subseteq HC_G(H/K)$.

Seja agora $hg \in HC_G(H/K)$, com $h \in H$ e $g \in C_G(H/K)$. Desta forma $\forall\, nK \in H/K$ temos $(hg)^{-1}nK(hg) = (hg)^{-1}n(hg)K = g^{-1}(h^{-1}nh)gK = g^{-1}g(h^{-1}nh)K = h^{-1}nhK$, isto é, $hg \in I_G(H/K)$. Com isso $HC_G(H/K) \subseteq I_G(H/K)$.

Em particular, no caso em que H/K é um fator principal abeliano temos $H \leq C_G(H/K)$ e assim $I_G(H/K) = C_G(H/K)$. ∎

Lema 4.9 *Sejam G um grupo e H_1/K_1 e H_2/K_2 dois fatores principais não abelianos de G. Então H_1/K_1 e H_2/K_2 são G-isomorfos se, e somente se, $C_G(H_1/K_1) = C_G(H_2/K_2)$.*

Demonstração: Suponha que $H_1/K_1 \cong_G H_2/K_2$. Pelo Lema 2.1 temos que $C_G(H_1/K_1) = C_G(H_2/K_2)$.

Reciprocamente suponha que H_1/K_1 e H_2/K_2 são fatores principais não abelianos de G tais que $C = C_G(H_1/K_1) = C_G(H_2/K_2)$. Temos que $K_i \leq C \cap H_i \leq H_i$, $i = 1, 2$. Como H_i/K_i é um fator principal de G, $C \cap H_i = K_i$ ou $C \cap H_i = H_i$, $i = 1, 2$. Se $C \cap H_i = H_i$ temos que $H_i \leq C$, o que implica que H_i/K_i é abeliano, $i = 1, 2$, contradição. Logo $K_i = C \cap H_i$, $i = 1, 2$. Assim $H_i/K_i = H_i/C \cap H_i \cong_G H_iC/C$, $i = 1, 2$. Pelo Lema 2.1, como $H_1/K_1 \cong_G H_1C/C$, temos que $C_G(H_1/K_1) = C_G(H_1C/C) = C$. Desta forma $C_{G/C}(H_1C/C) = C/C$, isto é, H_1C/C é um subgrupo normal minimal de G/C com centralizador trivial. Pelo item (b) da Proposição 2.14, G/C é um grupo primitivo do tipo 2. Como H_2C/C também é um subgrupo normal minimal de G/C temos que $H_1C = H_2C$. Portanto H_1/K_1 e H_2/K_2 são G-isomorfos. ∎

Proposição 4.10 *Sejam $F_1, F_2 \in \mathcal{CF}(G)$. Então as seguintes afirmações são equivalentes:*

1. *$F_1 \sim_G F_2$.*

2. *F_1 e F_2 são G-relacionados.*

3. *Ou $F_1 \cong_G F_2$ ou existe $E_i \in \mathcal{CF}(G)$ tal que $F_i \cong_G E_i$, $i = 1, 2$, e E_1 e E_2 possuem um complemento em comum em G que é um subgrupo maximal em G.*

4. *Ou $F_1 \cong_G F_2$ ou existe $E_i \in \mathcal{CF}(G)$ tal que $F_i \cong_G E_i$, $i = 1, 2$, e E_1 e E_2 possuem um complemento em comum em G.*

Demonstração: Iremos dividir nosso problema em três casos, o caso em que F_1 e F_2 são fatores principais abelianos, o caso em que assumimos que F_1 é um fator principal abeliano e o caso em que F_1 e F_2 são fatores principais não abelianos.

Note que se $F_1 \cong_G F_2$ então seguem todas as afirmações, isto é $F_1 \sim_G F_2$, F_1 e F_2 são G-relacionados e valem 3 e 4.

Caso 1: F_1 e F_2 são fatores principais abelianos.

Para este caso temos as equivalências F_1 e F_2 são G-isomorfos se, e somente se, F_1 e F_2 são G-equivalentes, se, e somente se, F_1 e F_2 são G-relacionados, isto é, todas as afirmações são válidas.

Caso 2: F_1 é um fator principal abeliano.

$1 \Rightarrow$ todos. Suponha que $F_1 \sim_G F_2$ então por definição temos $F_1 \cong F_2$ e segue que F_2 é abeliano, reduzindo o problema ao caso anterior.

$2 \Rightarrow$ todos. Suponha que F_1 e F_2 são G-relacionados, então $F_1 \cong_G F_2$ ou existe um quociente primitivo do tipo 3 de G com F_1 isomorfo a um dos subgrupos normais minimais desse quociente. Como os subgrupos normais minimais de um grupo primitivo do tipo 3 são não abelianos e F_1 é abeliano, não pode existir tal quociente. Logo $F_1 \cong_G F_2$.

$3 \Rightarrow$ todos. Vamos mostrar que F_2 é abeliano. Suponha que existam $E_i = H_i/K_i \in \mathcal{CF}(G)$ tal que $F_i \cong_G E_i$, $i = 1, 2$, e E_1 e E_2 possuem um complemento em comum em G que é um subgrupo maximal M de G. Desta forma $MH_i = G$ e $M \cap H_i = K_i$, $i = 1, 2$. Considere $N = M_G$. Note que $N \subseteq K_iN \subseteq M$, como $K_i, N \trianglelefteq G$ temos que $K_iN \trianglelefteq G$. Como N é o coração normal de M, isto é, N é o maior subgrupo normal de G contido em M, temos que $N = K_iN$, $i = 1, 2$. Então $M \cap H_iN = N(M \cap H_i) = NK_i = N$, $i = 1, 2$. Por outro lado, $N \cap H_i \subseteq M \cap H_i = K_i$ e $K_i \subseteq K_i(N \cap H_i) = K_iN \cap H_i = N \cap H_i$, para $i = 1, 2$. Desta forma

$$H_iN/N \cong_G H_i/N \cap H_i = H_i/K_i.$$

Temos então H_iN/N é um subgrupo normal minimal de G/N, $i = 1, 2$. Pelo Teorema 2.7, G/N é um grupo primitivo. Como estamos supondo H_1/K_1 abeliano e $H_1N/N \cong_G H_1/K_1$, temos então que G/N é um grupo primitivo do tipo 1. Como G/N possui apenas um subgrupo normal minimal, segue então que $H_1N/N = H_2N/N$. Desta forma $H_1/K_1 \cong_G H_1N/N = H_2N/N \cong_G H_2/K_2$. Portanto $F_1 \cong_G E_1 \cong_G E_2 \cong_G F_2$.

$4 \Rightarrow 3$. Suponha que existam $E_i = H_i/K_i \in \mathcal{CF}(G)$ tal que $F_i \cong_G E_i$, $i = 1, 2$, e E_1 e E_2 possuem um complemento M em comum em G. Para concluir basta mostrar que M é um subgrupo maximal de G.

Seja L um subgrupo maximal de G tal que $M \subseteq L$. Temos que $MH_1 = LH_1 = G$ e $M \cap H_1 = K_1$. Agora, como $H_1 \trianglelefteq G$, $L \cap H_1 \trianglelefteq L$ e como H_1/K_1 é abeliano, $L \cap H_1/K_1 \trianglelefteq H_1/K_1$, assim $L \cap H_1 \trianglelefteq H_1$ e portanto $L \cap H_1 \trianglelefteq LH_1 = G$. Temos então

$$G \geq H_1 \geq H_1 \cap L \geq K_1.$$

Como H_1/K_1 é um fator principal de G temos que $H_1 \cap L = H_1$ ou $H_1 \cap L = K_1$. Se $H_1 \cap L = H_1$ então $H_1 \leq L$ e $H_1L = L \neq G$. Então $H_1 \cap L = K_1$. Desta forma

$$M/K_1 \cong M/M \cap H_1 \cong MH_1/H_1 = G/H_1 = LH_1/H_1 \cong L/L \cap H_1 \cong L/K_1,$$

logo $|M| = |L|$ o que nos dá $M = L$ e assim provando que M é um subgrupo maximal de G.

Caso 3: F_1 e F_2 são fatores principais não abelianos.

Iremos assumir neste caso que os fatores principais não são G-isomorfos, pois, como vimos anteriormente, todas as afirmações seguem no caso em que eles são G-isomorfos.

$1 \Rightarrow 2$. Sejam $F_1 = H_1/K_1$ e $F_2 = H_2/K_2$ e suponha que $F_1 \sim_G F_2$. Sejam $A = C_G(H_1/K_1)$ e $B = C_G(H_2/K_2)$. Como H_1/K_1 e H_2/K_2 não são G-isomorfos segue do Lema 4.9 que $A \neq B$. Agora como $H_1/K_1 \sim_G H_2/K_2$, pela Proposição 4.7, temos que $I_G(H_1/K_1) = I_G(H_2/K_2) = I$.

Vamos mostrar que $AB = I$. Pelo Lema 4.8 temos que $I_G(H_1/K_1) = H_1C_G(H_1/K_1) = H_1A$ e $I_G(H_2/K_2) = H_2C_G(H_2/K_2) = H_2B$. Desta forma $A \subseteq I_G(H_1/K_1) = I$ e $B \subseteq I_G(H_2/K_2) = I$, logo $AB \subseteq I$. Por outro lado, H_1/K_1 e H_2/K_2 são fatores principais de G, assim pelo teorema de Jordan-Hölder $H_1/K_1 \cong_G S/T$ com S/T fator principal na série de composição de G em que H_2/K_2 aparece. Note que, como $H_1/K_1 \cong_G S/T$ temos $A = C_G(H_1/K_1) = C_G(S/T)$ e, em particular, $H_1/K_1 \sim_G S/T$, ou seja, $I = I_G(H_1/K_1) = I_G(S/T) = SA$. Como S/T e H_2/K_2 são fatores principais distintos de uma mesma série temos então $H_2 \subseteq T$ ou $S \subseteq K_2$. No primeiro caso temos que $H_2 \subseteq T \subseteq C_G(S/T) = C_G(H_1/K_1) = A$ o que nos dá $I = H_2B \subseteq AB$. No segundo caso temos que $S \subseteq K_2 \subseteq C_G(H_2/K_2) = B$ o que nos dá $I = SA \subseteq BA = AB$. Em ambos os casos, $I \subseteq AB$. Segue então que $AB = I$.

Vamos agora mostrar que $K_2 = H_2 \cap B$. Temos que $K_2 \subseteq B = C_G(H_2/K_2)$ e assim $K_2 \leq H_2 \cap B \leq H_2$. Como H_2/K_2 é um fator principal, temos que $H_2 \cap B = H_2$ ou

$H_2 \cap B = K_2$. Se $H_2 \cap B = H_2$ temos $H_2 \subseteq B = C_G(H_2/K_2)$ o que implica H_2/K_2 abeliano, contradição. Assim $B \cap H_2 = K_2$. Analogamente, $A \cap H_1 = K_1$. Desta forma

$$A/A \cap B \cong_G AB/B = I/B = H_2B/B \cong_G H_2/H_2 \cap B = H_2/K_2.$$

Analogamente,

$$B/A \cap B \cong_G AB/A = I/A = H_1A/A \cong_G H_1/H_1 \cap A = H_1/K_1.$$

Mostraremos que $G/A\cap B$ é um grupo primitivo do tipo 3 terminando assim a demonstração. Podemos, sem perda de generalidade, assumir que $A \cap B = \{1\}$. Segue das igualdades acima que $A \cong_G H_2/K_2$, $B \cong_G H_1/K_1$. Pelo Lema 2.1, $C_G(A) = C_G(H_2/K_2) = B$ e $C_G(B) = C_G(H_1/K_1) = A$. Por hipótese $H_1/K_1 \sim_G H_2/K_2$, como $\sim_G$ é uma relação de equivalência, $B \sim_G A$. Logo existem $\alpha \in Z^1(G, A)$ e um G-isomorfismo $\varphi : B \to A_\alpha$. Seja

$$M = \operatorname{Ker} \alpha = \{g \in G : g^\alpha = 1\},$$

vamos mostrar que M complementa A em G. Temos $B \sim_G A$ e $A = C_G(B)$, assim $\forall\ a \in A$ e $\forall\ b \in B$, $b^\varphi = (b^a)^\varphi = b^{\varphi a a^\alpha}$, isto é, $aa^\alpha \in C_A(A)$. Agora, $C_A(A) = A \cap C_G(A) = A \cap B = \{1\}$. Assim $aa^\alpha = 1$, isto é, $a^\alpha = a^{-1}$, $\forall\ a \in A$. Seja $g \in G$ e $g^\alpha = a$. Temos $(ga)^\alpha = (g^\alpha)^a a^\alpha = a^a a^\alpha = a^{-1}aaa^\alpha = 1$, isto é, $ga \in \operatorname{Ker} \alpha$ e logo $G = AM$. Se $m \in M \cap A$ então $m^\alpha = 1$ e $m^\alpha = m^{-1}$, assim $m = 1$ e então $M \cap A = \{1\}$. Logo M é um complemento para A em G.

Vamos agora mostrar que M também complementa B em G. Sejam $b \in B$ e $m \in B \cap M$, desta forma $m \in C_G(A)$ e $m^\alpha = 1$. Temos então que

$$b^\varphi = b^{\varphi m} = b^{\varphi m m^\alpha} = b^{m\varphi}.$$

Logo $b = b^m$, $\forall\ b \in B$ e então $m \in C_G(B) = A$. Assim $m \in M \cap A = \{1\}$, obtemos $m = 1$ e então $B \cap M = \{1\}$. Além disso $A \sim_G B$ implica que $A \cong B$ como grupos e assim $|G| = |AM| = |A|\,|M| = |B|\,|M| = |BM|$ e portanto $G = BM$, isto é, M é um complemento para B em G.

Como M complementa os subgrupos normais minimais $A = C_G(B)$ e $B = C_G(A)$ de G, segue do item (b) da Proposição 2.13 que G é um grupo primitivo do tipo 1 ou 3. Como A e B são não abelianos temos que G é um grupo primitivo do tipo 3.

$2 \Rightarrow 3$. Se F_1 e F_2 são G-relacionados então ou $F_1 \cong_G F_2$ ou existe $N \trianglelefteq G$ tal que A/N e B/N são subgrupos normais minimais de G/N, G/N é um grupo primitivo do tipo 3 e $A/N \cong_G F_1$ e $B/N \cong_G F_2$. Como G/N é um grupo primitivo do tipo 3, existe $M/N \in G/N$ que complementa A/N e B/N e M/N é maximal em G/N. Tome então $E_1 = A/N$ e $E_2 = B/N$. Temos que M é um subgrupo maximal de G, $MA = MB = G$ e $M \cap A = M \cap B = N$.

$3 \Rightarrow 4$. Imediato.

$4 \Rightarrow 1$. Observe que para mostrar que 4 implica 1 podemos substituir os fatores principais $F_1 = H_1/K_1$, $F_2 = H_2/K_2$ por fatores principais G-isomorfos a eles. Suponha que um subgrupo M de G complementa H_1/K_1 e H_2/K_2, ou seja, $MH_i = G$, $M \cap H_i = K_i$, $i = 1, 2$. Seja $N = M_G$. Note que M complementa NH_1/N e NH_2/N. De fato, $MNH_i = MH_i = G$ e $M \cap NH_i = N(M \cap H_i) = NK_i = N$, $i = 1, 2$. Temos que $N \cap H_i = K_i$. De fato, $H_i \geq N \cap H_i \geq K_i$, $N \cap H_i \trianglelefteq G$ e H_i/K_i é um fator principal, então $N \cap H_i = H_i$ ou $N \cap H_i = K_i$. Se $N \cap H_i = H_i$ teríamos $H_i \leq N \leq M$ o que daria $MH_i = M \neq G$ para $i = 1, 2$. Então $N \cap H_i = K_i$, $i = 1, 2$. Desta forma temos os G-isomorfismos

$$H_1N/N \cong_G H_1/N \cap H_1 = H_1/K_1,$$

$$H_2N/N \cong_G H_2/N \cap H_2 = H_2/K_2.$$

Logo podemos substituir H_1/K_1 por H_1N/N e H_2/K_2 por H_2N/N.

Em outras palavras podemos supor que $N \leq H_i$ para $i = 1, 2$. Mas como N contem K_i e H_i/K_i é um fator principal de G, segue que $K_1 = N = K_2$, logo H_1/N e H_2/N são dois subgrupos normais minimais distintos de G/N (distintos porque se fossem iguais então H_1/K_1 e H_2/K_2 seriam G-isomorfos), logo $(H_1/N) \cap (H_2/N) = N/N$, ou seja $H_1 \cap H_2 = N$.

Vamos mostrar que $H_1/N \sim_G H_2/N$. Para isto vamos construir um 1-cociclo $\beta \in Z^1(G, H_1/N)$ e um isomorfismo $\varphi : H_2/N \to H_1/N$ tal que $(xN)^{g\varphi} = (xN)^{\varphi g g^\beta}$, para quaisquer $x \in H_1$ e $g \in G$. Assim teremos $H_2/N \cong_G (H_1/N)_\beta$ e pela Proposição 4.3, $H_1/N \sim_G H_2/N$. Para isto podemos supor, sem perda de generalidade, que $N = M_G = \{1\}$. Assim $K_1 = K_2 = \{1\}$ e H_1, H_2 são normais minimais em G. Mostraremos que H_1 e H_2 são G-equivalentes.

Considere

$$\beta : G \to H_1$$

dada por $g^\beta = y$, para $g \in G$, $y \in H_1$ e $gy \in M$, pois $G = H_1M$.

Como $G = H_1 \rtimes M$, pela unicidade da escrita do produto semi-direto temos que β é bem definida. Agora vamos mostrar que β é um 1-cociclo. Sejam $m_1 = g_1y_1$ e $m_2 = g_2y_2$ com $m_1, m_2 \in M$, $g_1, g_2 \in G$ e $y_1, y_2 \in H_1$. Temos $g_1 = m_1y_1^{-1}$ e $g_2 = m_2y_2^{-1}$, assim $g_1g_2 = m_1y_1^{-1}m_2y_2^{-1} = m_1m_2m_2^{-1}y_1^{-1}m_2y_2^{-1} = m_1m_2(y_2m_2^{-1}y_1m_2)^{-1}$, onde $m_2^{-1}y_1^{-1}m_2y_2^{-1} \in H_1$ pois $H_1 \trianglelefteq G$. Assim $m_1m_2 = g_1g_2(y_2m_2^{-1}y_1m_2)$ e então $(g_1g_2)^\beta = y_2m_2^{-1}y_1m_2$. Por outro lado

$$(g_1^\beta)^{g_2}g_2^\beta = y_1^{g_2}y_2 = g_2^{-1}y_1g_2y_2 = y_2m_2^{-1}y_1m_2y_2^{-1}y_2 = y_2m_2^{-1}y_1m_2.$$

Então $(g_1g_2)^\beta = (g_1^\beta)^{g_2}g_2^\beta$, isto é β é um 1-cociclo.

Considere agora

$$\varphi : H_2 \to H_1$$

dada por $x^{\varphi} = y$, se $x \in H_2$, $y \in H_1$ e $xy \in M$.

Vamos mostrar que φ é bem definida. Sejam $x \in H_2$, $y, y' \in H_1$ com $xy \in M$ e $xy' \in M$. Temos que $xy = m \in M$ e $xy' = m' \in M$ o que nos dá $x = my^{-1} = m'y'^{-1}$. Desta forma

$$(my^{-1}m^{-1})m = (m'y'^{-1}m'^{-1})m',$$

como $G = H_1 \rtimes M$, pela unicidade da escrita do produto semi-direto, obtemos que $my^{-1}m^{-1} = m'y'^{-1}m'^{-1}$ e $m = m'$. Desta forma $y^{-1} = y'^{-1}$ e portanto $y = y'$.

Vamos mostrar que φ é injetiva. Sejam $y = y'$ com $xy = m$ e $x'y' = m'$ para $x, x' \in H_2$, $y, y' \in H_1$ e $m, m' \in M$. Temos que $y^{-1} = y'^{-1}$ e então $m^{-1}x = m'^{-1}x'$. Assim

$$(m^{-1}xm)m^{-1} = (m'^{-1}x'm')m'^{-1},$$

como $G = H_2 \rtimes M$, pela unicidade da escrita do produto semi-direto, obtemos que $m^{-1}xm = m'^{-1}x'm'$ e $m^{-1} = m'^{-1}$. Desta forma $m = m'$ e portanto $x = x'$.

Vamos mostrar que φ é sobrejetiva. Dado $y \in H_1$, $y \in G = H_2 \rtimes M$, assim $y = h_2m$, com $h_2 \in H_2$ e $m \in M$. Desta forma $h_2^{-1}y = m$ e portanto $(h_2^{-1})^{\varphi} = y$.

Com isso $\varphi : H_2 \to H_1$ é um isomorfismo. Vamos mostrar agora que $x^{g\varphi} = x^{\varphi g g^{\beta}}$, para todos $x \in H_2$ e $g \in G$, pois desta forma $H_2 \cong_G (H_1)_{\beta}$. Sejam $x^{g\varphi} = (x^g)^{\varphi} = y$, $x^{\varphi} = y_1$ e $g^{\beta} = z$, com $x \in H_2$, $y, y_1, z \in H_1$ e $g \in G$. Pelas definições de φ e β temos $x^g y = m \in M$, $xy_1 = m_1 \in M$ e $gz = m_2 \in M$. Queremos mostrar que $y = y_1^{gz}$. Por um lado temos,

$$y^{-1}y_1^{gz} = m^{-1}x^g z^{-1}g^{-1}x^{-1}m_1gz = m^{-1}g^{-1}xgz^{-1}g^{-1}x^{-1}m_1gz =$$
$$(m^{-1}g^{-1}xgm)(m^{-1}z^{-1}g^{-1}x^{-1}gzm)(m^{-1}z^{-1}g^{-1}m_1gz) = x^{gm}(x^{-1})^{m_2m}(m^{-1}m_2^{-1}m_1m_2),$$

isto é,

$$y^{-1}y_1^{gz}(m^{-1}m_2^{-1}m_1m_2)^{-1} = x^{gm}(x^{-1})^{m_2m} \in H_2$$

Por outro lado temos,

$$y^{-1}y_1^{gz} = m^{-1}x^g z^{-1}g^{-1}x^{-1}m_1gz = m^{-1}g^{-1}xgz^{-1}g^{-1}x^{-1}m_1gz =$$
$$m^{-1}g^{-1}m_1y_1^{-1}gm_2^{-1}y_1m_2 = m^{-1}zm_2^{-1}m_1y_1^{-1}m_2z^{-1}m_2^{-1}y_1m_2 =$$
$$(m^{-1}zm)(m^{-1}m_2^{-1}m_1y_1^{-1}m_1^{-1}m_2m)$$
$$(m^{-1}m_2^{-1}m_1m_2z^{-1}m_2^{-1}m_1^{-1}m_2m)(m^{-1}m_2^{-1}m_1y_1m_1^{-1}m_2m)(m^{-1}m_2^{-1}m_1m_2) =$$
$$(z^m)[(y_1^{-1})^{m_1^{-1}m_2m}]((z^{-1})^{m_2^{-1}m_1^{-1}m_2m})(y_1^{m_1^{-1}m_2m})(m^{-1}m_2^{-1}m_1m_2),$$

isto é,

$$y^{-1}y_1^{gz}(m^{-1}m_2^{-1}m_1m_2)^{-1} = (z^m)[(y_1^{-1})^{m_1^{-1}m_2m}]((z^{-1})^{m_2^{-1}m_1^{-1}m_2m})(y_1^{m_1^{-1}m_2m}) \in H_1.$$

Assim $y^{-1}y_1^{gz}(m^{-1}m_2^{-1}m_1m_2)^{-1} \in H_1 \cap H_2$. Como $H_1 \cap H_2 = M_G = \{1\}$ temos que $y^{-1}y_1^{gz}(m^{-1}m_2^{-1}m_1m_2)^{-1} = 1$. Pela unicidade da escrita na produto semidireto H_1M seque que $y^{-1}y_1^{gz} = 1$. Portanto $y = y_1^{gz}$. Com isso temos que $H_2 \sim_G H_1$. ■

Corolário 4.11 *Sejam G um grupo, H/K é um fator principal de G, $A, B \trianglelefteq G$ com $B \leq A$. Se $A/B \sim_G H/K$ então A/B é um fator principal de G.*

Demonstração: Suponha que H/K é um fator principal abeliano. Temos $A/B \cong_G H/K$ e então A/B é um fator principal de G. Suponha agora que H/K é um fator principal não abeliano. Se $A/B \cong_G H/K$ então A/B é um fator principal de G. Se eles não são G-isomorfos, existe um quociente primitivo do tipo 3 de G tal que A/B e H/K são G-isomorfos, respectivamente, a um dos 2 subgrupos normais minimais desse quociente. Desta forma H/K e A/B são G-isomorfos a fatores principais de G e assim A/B é um fator principal de G. ■

4.3 A coroa de um grupo finito associada a um fator principal

Esta seção é majoritariamente baseada no artigo *Nonabelian crowns and schunck classes of finite groups* [11] de J. Lafuente. Nesta seção usaremos as notações $M <_{max} G$ para indicar que M é um subgrupo maximal de G, $N \trianglelefteq_{min} G$ para indicar que N é um subgrupo normal minimal de G e $G \in P_3$ para indicar que G é um grupo primitivo do tipo 3.

Proposição 4.12 *Sejam H/K um fator principal não abeliano de G e $C = C_G(H/K)$. Então G/C é um grupo primitivo do tipo 2 com subgrupo normal minimal R/C tal que $R/C \cong_G H/K$.*

Demonstração: Seja $R = HC \trianglelefteq G$. Temos que $H \cap C = K$. De fato, $H \geq H \cap C \geq K$, e como H/K é um fator principal de G temos $H \cap C = H$ ou $H \cap C = K$. Se $H = H \cap C$ temos $H \subseteq C = C_G(H/K)$ o que implica H/K abeliano, contradição. Logo $H \cap C = K$. Temos que $R/C = HC/C \cong_G H/H \cap C = H/K$ e portanto $C_G(R/C) = C_G(H/K) = C$. Então $C_{G/C}(R/C) = C/C$, isto é, R/C é um subgrupo normal minimal de G/C com centralizador trivial. Pelo Item (b) da Proposição 2.14, G é um grupo primitivo do tipo 2. ■

Note que $R = HC_G(H/K)$, então pelo Lema 4.8 temos que $R = I_G(H/K)$.

Proposição 4.13 *Sejam G um grupo finito, H/K um fator principal não abeliano de G e $C = C_G(H/K)$. Seja*

$$\mathbb{E} = \{C\} \cup \{M_G \mid M <_{max} G, MH_1 = G, K_1 \leq H_1 \cap M, H/K \cong_G H_1/K_1\}.$$

Então se

$$\mathbb{F} = \{C\} \cup \{E \trianglelefteq G \mid G/E \in P_3, C/E \trianglelefteq_{min} G/E\},$$

temos que $\mathbb{E} = \mathbb{F}$.

Demonstração: Vamos primeiro mostrar que $\mathbb{E} \subseteq \mathbb{F}$. Seja M um subgrupo maximal de G, $E = M_G \in \mathbb{E}$, $E \neq C$. Temos $MH_1 = G$ e $K_1 \leq M \cap H_1$, onde $H/K \cong_G H_1/K_1$. Seja $D = EH_1$. Temos que $H_1 \cap E = K_1$. De fato, $K_1 \leq M$ e $K_1 \trianglelefteq G$ o que nos dá $K_1 \leq M_G = E$, assim $K_1 \leq H_1 \cap E \leq H_1$. Como H_1/K_1 é um fator principal de G temos $H_1 \cap E = K_1$ ou $H_1 \cap E = H_1$. Se $H_1 \cap E = H_1$ obtemos que $H_1 \subseteq E = M_G \subseteq M$ e assim $H_1M = M \neq G$, contradição. Desta forma $D/E = EH_1/H_1 \cong_G H_1/H_1 \cap E = H_1/K_1$. Então $E \leq C_G(D/E) = C_G(H_1/K_1) = C_G(H/K) = C$, isto é, $E < C$. Assim D/E é um subgrupo normal minimal de G/E e temos que $C_{G/E}(D/E) = C/E \neq E/E$. Sabemos que $G/E = G/M_G$ é um grupo primitivo, então só podemos ter G/E primitivo do tipo 3, já que $C_{G/E}(D/E) \neq E/E$ (o que exclui o caso primitivo do tipo 2) e $D/E \cong_G H_1/K_1 \cong_G H/K$ que é não abeliano (o que exclui o caso primitivo do tipo 1). Desta forma $\mathbb{E} \subseteq \mathbb{F}$.

Vamos agora mostrar que $\mathbb{F} \subseteq \mathbb{E}$. Seja $C \neq E \in \mathbb{F}$, assim G/E é um grupo primitivo do tipo 3 com subgrupos normais minimais C/E e D/E. Temos que $(D/E)\cap(C/E) = E/E$, desta forma $DC/C \cong_G D/C \cap D = D/E$, isto é, DC/C é um subgrupo normal minimal de G/C. Além disso, $G/C \cong (G/E)/(C/E)$ e então pelo ítem (c) da Proposição 2.14, G/C é um grupo primitivo do tipo 2. Pela Proposição 4.12 temos $DC/C \cong_G H/K$, assim $D/E \cong_G H/K$. Como G/E é um grupo primitivo do tipo 3, existe um subgrupo M/E maximal em G/E tal que $MD = G$ e $(M/E)_{G/E} = E/E$. Como $(M/E)_{G/E} = M_G/E$ temos que $M_G = E \in \mathbb{E}$ e então $\mathbb{F} \subseteq \mathbb{E}$. ■

Definição 4.14 *Sejam G um grupo finito e H/K um fator principal não abeliano de G. Considere $S = \cap\mathbb{E}$. Dizemos que R/S é a H/K-coroa de G, onde $R = I_G(H/K)$.*

Também nos referimos a R/S como a coroa definida por H/K.

Proposição 4.15 *Sejam G um grupo finito, H/K um fator principal não abeliano de G e $S = \cap\mathbb{E}$. Se $|\mathbb{E}| = 1$, seja*

$$\mathbb{D} = \mathbb{E} = \{C\}.$$

Se $|\mathbb{E}| > 1$, seja

$$\mathbb{D} = \{C\} \cup \{D \mid D/E \trianglelefteq_{min} G/E, C \neq E \in \mathbb{E}\}.$$

Então $S = \cap\mathbb{D}$.

Demonstração: Se $|\mathbb{E}| = 1$ temos $\mathbb{D} = \mathbb{E} = \{C\}$ e assim $S = \cap\mathbb{D}$.

Se $|\mathbb{E}| > 1$, temos $\mathbb{D} = \{D \mid D/E \trianglelefteq_{min} G/E, C \neq E \in \mathbb{E}\}$. Assim se $C \neq D \in \mathbb{D}$ obtemos que C/E e D/E são os dois subgrupos normais minimais de G/E, onde G/E é um grupo primitivo do tipo 3, sendo $\mathbb{E} = \mathbb{F}$. Temos então que $E = C \cap D$. Desta forma $C/E = C/C \cap D$ e $D/E = D/C \cap D$. Então

$$\cap\mathbb{D} = \cap\{C \cap D = E \mid D \in \mathbb{D}\} = \cap\mathbb{E} = S.$$

Isso termina a demonstração. ■

Lema 4.16 *Sejam G um grupo e $N \trianglelefteq G$. Se $C_G(N) = 1$ então $Soc(G) \subseteq N$.*

Demonstração: Suponha que A é um subgrupo normal minimal não trivial de G e A não está contido em N. Temos então $A \cap N = \{1\}$. Como $A, N \trianglelefteq G$ temos $[A, N] \leq A \cap N = \{1\}$ o que implica que $A \subseteq C_G(N) = \{1\}$, contradição. Logo A está contido em N. Como $Soc(G)$ é o produto dos subgrupos normais minimais de G obtemos que $Soc(G) \subseteq N$. ■

Proposição 4.17 *Sejam G um grupo finito, H/K um fator principal não abeliano de G e R/S a H/K-coroa de G. Então $R/S = Soc(G/S)$.*

Demonstração: Vamos primeiro mostrar que $Soc(G/S) \subseteq R/S$. Lembre que $R = I_G(H/K) = HC$, com $C = C_G(H/K)$ e $R/C \cong_G H/K$. Seja $D \in \mathbb{D}$ com $D \neq C$, vamos mostrar que $R \supseteq D$, onde D/E, C/E são os subgrupos normais minimais de G/E e G/E é um grupo primitivo do tipo 3. Note que como $C_{G/E}(D/E) = C/E$, temos que $C_G(D/E) = C$ logo $E \leq C \leq R$, e então $E \leq R$. Note que $CD/C \cong_G D/C \cap D = C/E$. Desta forma CD/C é um subgrupo normal minimal de G/C. Como G/C é um grupo primitivo do tipo 2 e R/C é um subgrupo normal minimal de G/C obtemos que $R = CD$. Assim $D \subseteq R$.

Agora como D/E é um subgrupo normal minimal de G/E e G/E é um grupo primitivo do tipo 3, pela Proposição 2.14, $G/D \cong (G/E)/(D/E)$ é um grupo primitivo do tipo 2. Agora, $R/D = CD/D \cong_G C/C \cap D = C/E$, e desta forma R/D é o subgrupo normal minimal de G/D. Com isso $C_{G/D}(R/D) = D/D$ o que implica que $C_G(R/D) = D$. Da mesma forma, $C_G(R/C) = C$. Assim $C_G(R/S) = C_G(R/\cap \mathbb{D}) = \cap \mathbb{D} = S$, e então $C_{G/S}(R/S) = S/S$. Logo pelo Lema 4.16 temos que $Soc(G/S) \subseteq R/S$.

Vamos agora mostrar que $R/S \subseteq Soc(G/S)$. Seja $S = \bigcap_{i=1}^{r} D_i$, com $D_i \in \mathbb{D}$ e r o menor possível. Considere a aplicação injetiva

$$\varphi : R/S \hookrightarrow \prod_{i=1}^{r} R/D_i.$$

Desta forma R/S é isomorfo a um subgrupo de $\prod_{i=1}^{r} R/D_i$. Sejam então $D_1/S, D_2/S, \ldots, D_r/S$ distintos (pela minimalidade de r) em R/S. Considere $L_j = \bigcap_{i \neq j}^{r} D_i$. Como r foi escolhido para ser o menor possível temos que L_j contém S propriamente, isto é L_j não é igual a S. Seja $xS \in L_j/S$, temos que

$$\varphi(xS) = (xD_1, \ldots, xD_{j-1}, xD_j, xD_{j+1}, \ldots, xD_r) = (D_1, \ldots, D_{j-1}, xD_j, D_{j+1}, \ldots, D_r),$$

desta forma

$$\varphi(L_j/S) \subseteq D_1/D_1 \times \ldots D_{j-1}/D_{j-1} \times R/D_j \times D_{j+1}/D_{j+1} \times \ldots \times D_r/D_r \cong R/D_j.$$

Como φ é injetiva temos que $1 \neq \varphi(L_j/S)$. Por outro lado, como φ é G-homomorfismo, $\varphi(L_j/S) \trianglelefteq G/D_j$. Assim $1 \neq \varphi(L_j/S) \trianglelefteq G/D_j$. Como R/D_j é normal minimal em G/D_j temos então que $\varphi(L_j/S) = R/D_j$. Desta forma $L_j/S \cong_G R/D_j$ logo L_j/S é subgrupo normal minimal de G/S e φ é um G-isomorfismo tal que

$$R/S \cong_G \prod_{i=1}^{r} R/D_i.$$

Seja agora $X = \langle L_j \mid j = 1, \ldots, r\rangle = L_1 \ldots L_r$. Para todo j temos

$$R/D_j = \varphi(L_j/S) \subseteq \varphi(X/S) = \prod_{i=1}^{r} R/D_i.$$

Desta forma

$$R/S = \varphi^{\leftarrow}\left(\prod_{i=1}^{r} R/D_i\right) = \varphi^{\leftarrow}(\varphi(X/S)) = X/S.$$

Assim $R = X$. Então $R/S = X/S = L_1/S \ldots L_r/S \subseteq Soc(G/S)$. ∎

Corolário 4.18 *Sejam G um grupo finito, H/K um fator principal não abeliano de G, $C = C_G(H/K)$ e $R = I_G(H/K)$. Se $C \neq D \in \mathbb{D}$ então $R/D \sim_G H/K$ e $R/C \cong_G H/K$.*

Demonstração: Vimos na Proposição 4.17 que $R = CD$,

$$R/C = CD/C \cong_G D/C \cap D = D/E,$$

$$R/D = CD/D \cong_G C/C \cap D = C/E.$$

Como G/E é um grupo primitivo do tipo 3 com $Soc(G/E) = (C/E)(D/E)$ temos que R/C e R/D são G-relacionados. Então pela Proposição 4.10, $R/C \sim_G R/D$. Como $R/C \cong_G H/K$ temos, em particular, $R/C \sim_G H/K$. Como $\sim_G$ é uma relação de equivalência obtemos que $R/D \sim_G H/K$. ∎

Lema 4.19 *Sejam G um grupo finito, H/K um fator principal não abeliano de G e R/S a H/K-coroa de G. Então cada fator que aparece na H/K-coroa de G é G-equivalente a H/K. Mais ainda, seja F/T um fator principal de uma série principal de G que passa por R e S tal que $H/K \sim_G F/T$, então $S \leq T \leq F \leq R$.*

Demonstração: Pela Proposição 4.17 temos que $R/S \cong_G \prod_{i=1}^{r} R/D_i$, onde $D_1, \ldots, D_r \in \mathbb{D}$. Temos que $C_G(H/K) = C \in \mathbb{D}$ e $R/C \cong_G H/K$, então $R/C \sim_G H/K$. Agora se $C \neq D \in \mathbb{D}$, pelo Corolário 4.18 temos $R/D \sim_G H/K$. Desta forma para cada $D_i \in \mathbb{D}$, $i = 1, \ldots, r$, temos $R/D_i \sim_G H/K$. Então cada fator que aparece na H/K-coroa de G é G-equivalente a H/K.

Vamos agora mostrar que cada fator principal F/T de uma série de G que passa por R e S com $F/T \sim_G H/K$, é tal que $S \leq T \leq F \leq R$. Como $F/T \sim_G H/K$ temos que

$I_G(F/T) = I_G(H/K)$. Desta forma $F \leq I_G(F/T) = I_G(H/K) = R$. Como $F/T \sim_G H/K$, pela Proposição 4.10, F/T e H/K são G-relacionados. Assim existe $N \trianglelefteq G$ tal que G/N é um grupo primitivo do tipo 3 e $A/N \cong_G F/T$ e $B/N \cong_G H/K$ são os subgrupos normais minimais de G/N. Então existe M um subgrupo maximal de G tal que M complementa A/N e B/N, isto é, $MA = MB = G$ e $M \cap A = M \cap B = N$. Como $B/N \cong_G H/K$, pela definição de $\mathbb{E}$ obtemos que $M_G \in \mathbb{E}$. Desta forma $S = \cap\mathbb{E} \leq M_G \leq M$. Agora $F \nleq N$, pois se $F \leq N$ teríamos $F \leq N \leq B = C_G(A/N) = C_G(F/T)$, ou seja F/T é abeliano e então $H/K \cong F/T$ é abeliano, contradição. Assim $N/N \neq FN/N \trianglelefteq G/N$, isto é, FN/N contém um subgrupo normal minimal de G/N. Então $FN \supseteq A$ ou $FN \supseteq B$, em quaisquer dos casos, como $MA = MB = G$, temos $MF = MNF \supseteq G$, logo $MF = G$. Desta forma, se $S \geq F$ obtemos que $M \geq S \geq F$, e assim $MF = M \neq G$ Como S e F estão na mesma série, $S \ngeq F$ implica que $S < F$. Agora $S \leq T$ pois se $T < S$ então S/T seria normal em F/T e logo F/T não seria um fator principal. Desta forma $S \leq T \leq F \leq R$. Logo todos os fatores principais G-equivalentes a H/K estão entre R e S. ∎

Como cada fator que aparece na coroa definida por H/K é G-equivalente a H/K e H/K é um fator principal de G temos então que cada fator que aparece na coroa definida por H/K é um fator principal de G.

A seguir daremos a generalização do conceito de coroa apresentada em [10]. Veremos que esta generalização engoba as Definições 3.8 e 4.14 de coroa para um fator principal.

Definição 4.20 *Sejam H/K um fator principal de G e $I = I_G(H/K)$. Definimos*

$$D_G(H/K) = \bigcap\{T \trianglelefteq G : T \leq I, I/T \sim_G H/K, I/T \nsubseteq \Phi(G/T)\}.$$

O quociente $I/D_G(H/K)$ é dito a H/K-coroa de G.

Note que se o grupo G é solúvel e H/K é um fator principal de G então H/K é abeliano, $I = C_G(H/K) = C$ e $D_G(H/K) = \bigcap\{T \trianglelefteq G : T < C, C/T \cong_G H/K, C/T \nsubseteq \Phi(G/T)\}$. Logo a definição acima coincide com a Definição 3.8.

Vamos agora mostrar que as Definições 4.14 e 4.20 de H/K-coroa de G são equivalentes quando H/K é um fator principal não abeliano. Já vimos que $I_G(H/K) = HC_G(H/K) = R$. Desta forma $I = R$. Para concluirmos a equivalência vamos mostrar que $D_G(H/K) = S$.

$D_G(H/K) \subseteq S$. Sabemos que se H/K é um fator principal não abeliano então $H/K \nleq \Phi(G/K)$, porque o subgrupo de Frattini é nilpotente. Desta forma $D_G(H/K) = \bigcap\{T \trianglelefteq G : T \leq R, R/T \sim_G H/K\}$. Seja R/S a coroa de H/K. Vimos na Proposição 4.17 que $R/S = Soc(G/S) = N_1/S \times \ldots \times N_t/S$, ou seja, $R = N_1 \ldots N_t$ e $S = N_i \cap (N_1 N_2 \ldots N_{i-1} N_{i+1} \ldots N_t)$, para todo $i = 1, \ldots, t$. Pelo Lema 4.19 temos que

$N_i/S \sim_G H/K$, para todo $i = 1, \ldots, t$. Defina $T_i = N_1N_2 \ldots N_{i-1}N_{i+1} \ldots N_t$. Temos que $\bigcap_i T_i = S$, $N_i \cap T_i = S$ e $T_iN_i = R$. Por outro lado,

$$R/T_i = T_iN_i/T_i \cong_G N_i/N_i \cap T_i = N_i/S.$$

Então $R/T_i \sim_G H/K$. Desta forma $D_G(H/K) \subseteq \bigcap_i T_i = S$.

$S \subseteq D_G(H/K)$. Queremos mostrar que $R/T \sim_G H/K$ implica que $T \supseteq S$. Suponha que $S \nsubseteq T$. Então $S \cap T \neq S$ e assim $S/S \cap T \neq 1$. Desta forma $S/S \cap T \cong_G ST/T \leq R/T$. Como R/T é um fator principal de G e $S, T \trianglelefteq G$, temos que $ST/T = R/T$ e assim $S/S \cap T \cong_G R/T$. Como $R/T \sim_G H/K$ obtemos então que $S/S \cap T \sim_G H/K$. Temos então que $S/S \cap T$ é um fator principal de G que é G-equivalente a H/K mas $S \cap T < S \leq R$, contradizendo o Lema 4.19. Logo $T \supseteq S$ e assim $S \subseteq D_G(H/K)$.

Agora podemos provar o seguinte Teorema:

Teorema 4.21 *Sejam H/K e H_0/K_0 dois fatores principais não abelianos de G. Então H/K e H_0/K_0 definem a mesma coroa se, e somente se, H/K e H_0/K_0 são G-relacionados, se e somente se, são G-equivalentes.*

Demonstração: Suponha que H/K e H_0/K_0 definem a mesma coroa. Pelo Lema 4.19, cada fator direto A da coroa é tal que $H/K \sim_G A \sim_G H_0/K_0$. Como $\sim_G$ é uma relação de equivalência obtemos que $H/K \sim_G H_0/K_0$.

Reciprocamente, suponha que $H/K \sim_G H_0/K_0$ e sejam R/S a coroa definida por H/K e R_0/S_0 a coroa definida por H_0/K_0. Vamos mostrar que $R = R_0$ e $S = S_0$. Como $H/K \sim_G H_0/K_0$ temos que $R = I_G(H/K) = I_G(H_0/K_0) = R_0$. Por outro lado, como $\sim_G$ é uma relação de equivalência, usando a equivalência das definições de coroa apresentadas acima obtemos que

$$S = D_G(H/K) = \bigcap \{T \trianglelefteq G : T \leq R, R/T \sim_G H/K\} =$$
$$\bigcap \{T \trianglelefteq G : T \leq R, R/T \sim_G H_0/K_0\} = D_G(H_0/K_0) = S_0.$$

Logo H/K e H_0/K_0 definem a mesma coroa. ■

4.4 Exemplos e aplicação de Coroa

Se $A = H/K$ é um fator principal não abeliano de G e $I/D = Soc(G/D)$ é a coroa de A temos que I/D é um produto direto de $\delta_G(A)$ subgrupos normais minimais G-equivalentes a A. Se $\delta_G(H/K) = 1$ então H/K pode ser complementado ou não. Como exemplo temos os casos $A_n < S_n$, $n \geq 3$, que é complementado, por exemplo pelo subgrupo $\langle(12)\rangle$ e

$A_6 < Aut(A_6)$ que como veremos no apêndice desse trabalho não é complementado.

Lembre que se X é um grupo primitivo do tipo 2 e $Soc(X) = L$ definimos

$$\delta_n(X) = \{(x_1, x_2, \ldots, x_n) \in X^n : x_1L = x_2L = \ldots = x_nL\}.$$

Vimos que $\delta_2(X)$ é um grupo primitivo do tipo 3 com subgrupos normais minimais $L \times \{1\}$ e $\{1\} \times L$. Neste caso, os subgrupos normais minimais de $\delta_2(X)$ são $\delta_2(X)$-equivalentes. De maneira geral, se $G = \delta_n(X)$ então o quociente $G/\{1\} \times \{1\} \times L \times \ldots \times L$ é um grupo primitivo do tipo 3 e os subgrupos normais minimais $L_1 = L \times \{1\} \times \ldots \times \{1\}$ e $L_2 = \{1\} \times L \times \{1\} \times \ldots \times \{1\}$ de G são G-equivalentes. Procedendo desta forma obtemos que os n subgrupos normais minimais L_i, $i = 1, 2, \ldots, n$, de G são G-equivalentes.

Exemplo 4.1 *(a) Sejam* $G = \delta_n(X) = \{(x_1, x_2, \ldots, x_n) \in X^n : x_1L = x_2L = \ldots = x_nL\}$*,* X *um grupo primitivo do tipo 2 e* $Soc(X) = L$*. Se* $H/K = L_1 = L \times 1 \times \ldots \times 1$ *então*

$$C_G(H/K) = 1 \times L_2 \times \ldots \times L_n,$$
$$I_G(H/K) = HC_G(H/K) = L_1 \times L_2 \times \ldots \times L_n = Soc(G).$$

Tomando $T = L_1 \times \ldots \times \hat{L_i} \times \ldots \times L_n$*, isto é, o produto de* $L_1, \ldots, L_n$ *menos* L_i *temos* $I/T \sim_G H/K$*. Logo*

$$D_G(H/K) \subseteq \bigcap_{i=1}^{n} L_1 \times \ldots \times \hat{L_i} \times \ldots \times L_n = 1.$$

Portanto a coroa de H/K *é* $Soc(G)$ *e* $\delta_G(H/K) = n$*. Para qualquer outro subgrupo* L_i*,* $i = 1, 2, \ldots, n$*, normal minimal de* G*, a coroa de* L_i *é* $Soc(G)$*.*

(b) Sejam $G = \delta_n(X) = \{(x_1, x_2, \ldots, x_n) \in X^n : x_1L = x_2L = \ldots = x_nL\}$*,* X *um grupo primitivo do tipo 1 e* $Soc(X) = L$*. Se* $H/K = L_1 = L \times 1 \times \ldots \times 1$ *então, como* L_1 *é abeliano,*

$$I_G(H/K) = C_G(H/K) = L_1 \times L_2 \times \ldots \times L_n = Soc(G).$$

Agora, $L_1 \cong_G L_i$ *para todo* $i = 1, 2, \ldots, n$*. De fato, tome o isomorfismo canônico*

$$\begin{aligned} \varphi \colon L_1 &\longrightarrow L_i \\ (a, 1, \ldots, 1) &\longmapsto (1, \ldots, 1, a, 1, \ldots, 1). \end{aligned}$$

Dado $g = (x_1, x_2, \ldots, x_n) \in G$ *temos que*

$$((a, 1, \ldots, 1)^g)^\varphi = (a^{x_1}, 1, \ldots, 1)^\varphi = (1, \ldots, 1, a^{x_1}, 1, \ldots, 1)$$

$$((a, 1, \ldots, 1)^\varphi)^g = (1, \ldots, 1, a, 1, \ldots, 1)^g = (1, \ldots, 1, a^{x_i}, 1, \ldots, 1).$$

Como $x_1x_i^{-1} \in L$ *e* L *é abeliano temos* $x_1x_i^{-1}a = ax_1x_i^{-1}$*, isto é,* $a^{x_i} = a^{x_1}$ *e logo* $((a, 1, \ldots, 1)^g)^\varphi = ((a, 1, \ldots, 1)^\varphi)^g$*. Assim todos os* L_i*'s são* G*-isomorfos e* *consequentemente G-equivalentes. Portanto tomando $T = L_1 \times \ldots \times \hat{L}_i \times \ldots \times L_n$, isto é, o produto de $L_1, \ldots, L_n$ menos L_i temos $I/T \sim_G H/K$. Logo*

$$D_G(H/K) \subseteq \bigcap_{i=1}^{n} L_1 \times \ldots \times \hat{L}_i \times \ldots \times L_n = 1.$$

Portanto a coroa de H/K é $Soc(G)$ e $\delta_G(H/K) = n$. Para qualquer outro subgrupo L_i, $i = 1, 2, \ldots, n$, normal minimal de G, a coroa de L_i é $Soc(G)$.

Considere agora $G = X \times X \times X = X^3$, onde X é um grupo primitivo do tipo 2 com $Soc(X) = L$ e $X \neq L$. Vamos mostrar que os subgrupos normais minimais de G não são G-relacionados. Lembre que os subgrupos normais minimais de G são $L_1 = L \times \{1\} \times \{1\}$, $L_2 = \{1\} \times L \times \{1\}$ e $L_3 = \{1\} \times \{1\} \times L$. Note que L_1, L_2 e L_3 são dois a dois não G-isomorfos pois $C_G(L_1) = 1 \times X \times X$, $C_G(L_2) = X \times 1 \times X$ e $C_G(L_3) = X \times X \times 1$. Suponha que existe $N \trianglelefteq G$ com G/N um grupo primitivo do tipo 3, $Soc(G/N) = A \times B$, onde $A \cong_G L_1$ e $B \cong_G L_2$. Temos que N não contém L_1. De fato, se $L_1 \subseteq N$ então $L_1 \subseteq N \subseteq C_G(A) = C_G(L_1)$, contradição pois L_1 é um fator principal não abeliano. Analogamente, N não contém L_2. Além disso temos que N não pode conter $L \times L \times \{1\}$, $L \times \{1\} \times L$ e $1 \times L \times L$ pois estes contém L_1 ou L_2. Por outro lado, N contém L_3. De fato, se $N \not\supseteq L_3$ então $NL_i/N \cong_G L_i/L_i \cap N \cong_G L_i$, para $i = 1, 2, 3$. Desta forma G/N contém 3 subgrupos normais minimais distintos (porque não são G-isomorfos), mas G/N é um grupo primitivo do tipo 3, contradição. Logo $N \supseteq L_3$. Então G/N é um quociente de $X \times X \times X/L$. Vamos agora mostrar que $N = X_3 = \{1\} \times \{1\} \times X$, isso termina a demonstração porque segue que G/N é isomorfo a $X \times X$ que não é um grupo primitivo do tipo 3. Primeiro vejamos que $N \supseteq X_3$. Se $N \not\supseteq X_3$ então existe $(1, 1, x) = y \in X_3 - N$. Assim se $l = (\alpha, 1, 1) \in L_1$, temos $ly = yl$. Então $lNyN = yNlN$, ou seja, $N \neq yN \in C_G(L_1N/N)$, contradição porque $C_G(L_1N/N)$ é trivial. Agora vejamos que $X_3 \supseteq N$. Temos que $N \subseteq C_G(A) = C_G(L_1) = \{1\} \times X \times X$ e $N \subseteq C_G(B) = C_G(L_2) = X \times \{1\} \times X$. Logo $N \subseteq (\{1\} \times X \times X) \cap (X \times \{1\} \times X) = \{1\} \times \{1\} \times X = X_3$. Portanto L_1 e L_2 não são G-equivalentes. Podemos generalizar esse caso, definindo $G = X^n$, os subgrupos L_i, L_j normais minimais de G não são G-equivalentes se $i \neq j$.

Exemplo 4.2 *Sejam $G = X^n$, X um grupo primitivo do tipo 2 e $Soc(X) = L$. Se $H/K = L_1 = L \times 1 \times \ldots \times 1$, então*

$$C_G(H/K) = 1 \times X \times \ldots \times X,$$

$$I_G(H/K) = HC_G(H/K) = L_1 \times X \times \ldots \times X.$$

Se $I/T \sim_G H/K$, então $T = 1 \times X \ldots \times X$ e logo

$$D_G(H/K) = 1 \times X \ldots \times X.$$

Portanto a coroa de H/K é L_1 e $\delta_G(H/K) = 1$. Para qualquer outro subgrupo L_i, $i = 1, 2, \ldots, n$, normal minimal de G, a coroa de L_i é L_i.

Lembre que se $A = H/K$ é um fator principal não abeliano de G então $X = G/C_G(A)$ é um grupo primitivo do tipo 2 com $Soc(X) = HC/C \cong_G H/K$, onde $C = C_G(A)$.

Proposição 4.22 ([3], Proposição 9) *Sejam G um grupo finito, A um fator principal de G não Frattini e I/D a coroa de A. Então $G/D \cong \delta_d(X)$, onde $d = \delta_G(A)$, e $X = G/C_G(A)$.*

O grupo $\delta_d(X)$, com $d = \delta_G(A)$ e $X = G/C_G(A)$, é chamado de *crown-based power* de comprimento d.

Um fator principal de G é dito m-complementado se é complementado por um subgrupo maximal de G.

Proposição 4.23 *Seja G um grupo finito. Fixado A um fator principal não abeliano de G, se $\delta_G(A) > 1$ então todos os subgrupo normais minimais de G/S são m-complementados, onde $S = D_G(A)$.*

Demonstração: Indicando com H/S um fator da coroa, como $\delta_G(A) > 1$ temos que H/S é G-equivalente a um outro fator da coroa e não é G-isomorfo a ele pois seus centralizadores são diferentes. Desta forma existe um quociente G/N que é um grupo primitivo do tipo 3 e os dois subgrupos normais minimais são C/N e D/N onde $C = C_G(H/S)$ e $D/N \cong_G H/S$. Assim pelas propriedades de um grupo primitivo do tipo 3, existe um subgrupo M maximal de G tal que M complementa C/N e D/N em G, isto é, $MC = MD = G$ e $M \cap C = M \cap D = N$.

Vamos mostrar que $S \subseteq N$. Suponha que $S \nsubseteq N$. Então $N/N \neq SN/N \trianglelefteq G/N$. Como SN/N é normal em G/N, SN/N contém um subgrupo normal minimal de G/N. Então $SN \supseteq C$ ou $SN \supseteq D$. Agora, se $D \subseteq SN$, como $S, N \subseteq C$ teríamos $D \subseteq SN \subseteq C$, absurdo. Então $C \subseteq SN$ e desta forma $SN = C$. Agora $H/S \sim_G C/N = SN/N \cong_G S/S \cap N$, isto é, obtemos um fator principal G-equivalente a H/S com $S \cap N < S$, contradizendo o Lema 4.19. Logo $S \subseteq N$.

Vamos agora mostrar que M complementa H/S. Temos que $N \subseteq C$, assim se $H \subseteq N$ teríamos $H \subseteq C = C_G(H/S)$ e assim H/S é um fator principal abeliano, contradição. Então $H \nsubseteq N$ e assim $N/N \neq HN/N \trianglelefteq G/N$. Novamente, como HN/N é um subgrupo normal de G/N, HN/N contém um subgrupo normal minimal de G/N. Então $HN \supseteq C$ ou $HN \supseteq D$. Em ambos os casos, como $MC = MD = G$ temos $HM = HNM = G$. Agora, como $S \leq H, N$, temos que $S \leq H \cap N \leq H$. Como H/S é um fator principal de G temos que $H \cap N = H$ ou $H \cap N = S$. Se $H \cap N = H$ então $H \subseteq N$, contradição. Logo $H \cap N = S$. Assim $H/S = H/H \cap N \cong_G HN/N$, ou seja, HN/N é um subgrupo normal minimal de G/N. Então $HN = C$ ou $HN = D$, mas como $H \nsubseteq C$, não podemos ter $HN = C$. Assim $HN = D$, e logo $H \leq D$. Então $S = H \cap N = H \cap (M \cap D) = H \cap M$. Desta forma M complementa H/S. ∎

Apêndice

Neste apêndice mostraremos que A_6 é o único subgrupo normal minimal de $Aut(A_6)$, A_6 não é complementado em $Aut(A_6)$ e $A_6 \nleq \Phi(Aut(A_6))$.

Seja F um corpo finito. Consideremos

$$GL(n,F) = \left\{ A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} : a_{ij} \in F, 1 \leq i,j \leq n, det(A) \neq 0 \right\},$$

o grupo das matrizes de tamanho $n \times n$ com entradas em um corpo F e

$$SL(n,F) = \{A \in GL(n,F) : det(A) = 1\},$$

o subgrupo das matrizes $n \times n$ com entradas em F e determinante igual a 1. É possível mostrar que o centro de $GL(n,F)$ é da forma

$$Z(GL(n,F)) = \left\{ \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix} : 0 \neq a \in F \right\},$$

onde as matrizes de $Z(GL(n,F))$ são chamadas de matrizes escalares. Assim o centro de $SL(n,F)$ é da forma

$$Z(SL(n,F)) = \left\{ \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix} : 0 \neq a \in F, a^n = 1 \right\}.$$

Considere também

$$PGL(n,F) := GL(n,F)/Z(GL(n,F))$$
$$PSL(n,F) := SL(n,F)/Z(GL(n,F)).$$

Note que $Z(GL(n, F)) \cong F^*$. É possível mostrar que $F^* = F - \{0\}$ é um grupo cíclico de ordem $|F| - 1$ ([9], Teorema 2.18). Contando as possibilidades para cada coluna é fácil ver que a ordem do grupo $GL(n, F)$ é dada por

$$|GL(n, F)| = (|F|^n - 1)(|F|^n - |F|) \dots (|F|^n - |F|^{n-1}).$$

É conhecido que os grupos $PSL(n, F)$ são em geral grupos simples não abelianos com as exceções $n = 1$, $(n, q) = (2, 2)$ e $(n, q) = (2, 3)$ ([17]).

Considere agora o corpo finito

$$F = \mathbb{F}_3[X]/(x^2 + 1),$$

onde denotaremos $\mathbb{F}_3$ por $\mathbb{F}_3 = \{-1, 0, 1\}$. Temos que

$$F = \{P(x) + (x^2 + 1) : P(x) \in \mathbb{F}_3[X]\} = \{ax + b + (x^2 + 1) : a, b \in \mathbb{F}_3\} =$$
$$\{-1, 0, 1, -i, i, -i - 1, -i + 1, i - 1, i + 1\},$$

onde $-1, 0, 1 \in \mathbb{F}_3$ e $i = \overline{x} = x + (x^2 + 1)$. Temos que $i^2 = x^2 + (x^2 + 1) = -1 + x^2 + 1 + (x^2 + 1) = -1 + (x^2 + 1) = -1$. É possível mostrar que dois corpos finitos de mesmo tamanho são isomorfos e um corpo finito de tamanho q é geralmente indicado por $\mathbb{F}_q$. Desta forma, como $|F| = 9$ temos que $F \cong \mathbb{F}_9$. Note que $\mathbb{F}_9 \supseteq \mathbb{F}_3$ e assim, na nossa notação, $3 = 0$.

Vamos estudar o grupo $PSL(2, 9)$, onde $F = \mathbb{F}_9$. Primeiro vamos calcular $|PSL(2, 9)|$. Temos que $|GL(2, 9)| = (9^2 - 1)(9^2 - 9) = 80 \cdot 72$. Agora considerando o epimorfismo

$$det : GL(2, 9) \to (\mathbb{F}_9)^*,$$

temos que $\text{Ker}(det) = SL(2, 9)$ e assim $|SL(2, 9)| = |GL(2, 9)| \,/\, |(\mathbb{F}_9)^*| = 80 \cdot 72/8 = 80 \cdot 9$. Seja agora $a \in \mathbb{F}_9$. Temos que se $a^2 = 1$ então $a = 1$ ou $a = -1$. Desta forma $|Z(SL(2, 9))| = 2$. Com isso

$$|PSL(2, 9)| = |SL(2, 9)| \,/\, |Z(SL(2, 9))| = 80 \cdot 9/2 = 360 = |A_6| \,.$$

Vamos agora mostrar que $PSL(2, 9) \cong A_6$. Note que se G é um grupo simples tal que $|G| = 360$ e G possui um subgrupo H com $[G : H] = 6$ então $G \cong A_6$. De fato, considere a ação de G no conjunto $\Omega = \{xH : x \in G\}$ dada por $(g, xH) \mapsto gxH$. Essa ação é transitiva e define um homomorfismo $\gamma : G \to Sym(\Omega) \cong S_6$. Como G é um grupo simples temos que $\text{Ker}(\gamma) = \{1\}$ ou $\text{Ker}(\gamma) = G$. Mas $\text{Ker}(\gamma) \neq G$ porque a ação é não trivial, sendo transitiva. Logo $\text{Ker}(\gamma) = \{1\}$. Desta forma G é isomorfo a um subgrupo de S_6. Temos que $[S_6 : G] = 2$ o que implica que $G \cong A_6$. Para mostrarmos então que $PSL(2, 9) \cong A_6$ vamos procurar um subgrupo H de $PSL(2, 9)$ de tal forma que $H \cong A_5$ e $[PSL(2, 9) : H] = 6$.

Podemos considerar (a menos de isomorfismo) $\mathbb{F}_9 = \{-1, 0, 1, -i, i, -i-1, -i+1, i-1, i+1\}$ e que $(\mathbb{F}_9)^*$ é um grupo cíclico de ordem 8. Note que $\lambda = i-1$ é tal que $\lambda^2 = -2i = i$, $\lambda^4 = i^2 = -1$ e $\lambda^8 = 1$, então $o(\lambda) = 8$ e podemos escrever $(\mathbb{F}_9)^* = \langle \lambda \rangle$.

Sejam agora

$$\alpha = \begin{pmatrix} 1 & \lambda \\ \lambda^2 & \lambda^6 \end{pmatrix} = \begin{pmatrix} 1 & i-1 \\ i & -i \end{pmatrix},$$

$$\beta = \begin{pmatrix} -1 & \lambda^3 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -i-1 \\ 0 & -1 \end{pmatrix}.$$

Observe que $det(\alpha) = -i - (i^2 - i) = -i + 1 + i = 1$ e $det(\beta) = 1 - 0 = 1$, ou seja, $\alpha, \beta \in SL(2,9)$. Denotamos, respectivamente, por $\overline{\alpha}$ e $\overline{\beta}$, os elementos $\alpha Z(SL(2,9))$ e $\beta Z(SL(2,9))$ de $PSL(2,9)$. Vamos mostrar que $\langle \overline{\alpha}, \overline{\beta} \rangle \cong A_5$. Para isso vamos calcular as ordens de $\overline{\alpha}$, $\overline{\beta}$ e $\overline{\alpha}\overline{\beta}$. Temos que

$$\alpha^2 = \begin{pmatrix} -i & -i \\ i+1 & 1-i \end{pmatrix}, \alpha^3 = \begin{pmatrix} 1-i & i \\ -i-1 & -i \end{pmatrix}, \alpha^5 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\beta^2 = \begin{pmatrix} 1 & -i-1 \\ 0 & 1 \end{pmatrix}, \beta^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \beta^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\alpha\beta = \begin{pmatrix} -1 & i \\ -i & 1 \end{pmatrix}, (\alpha\beta)^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, (\alpha\beta)^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Desta forma $o(\alpha) = 5$, $o(\beta) = 6$ e $o(\alpha\beta) = 4$. Por outro lado $\beta^3, (\alpha\beta)^2 \in Z(SL(2,9))$. Desta forma $o(\overline{\alpha}) = 5$, $o(\overline{\beta}) = 3$ e $o(\overline{\alpha}\overline{\beta}) = 2$. Seja então $H = \langle x, y | x^5 = y^3 = (xy)^2 = 1 \rangle \leq PSL(2,9)$, onde $x = \overline{\alpha}$ e $y = \overline{\beta}$. É conhecido que a apresentação de H se trata de uma apresentação de A_5 ([5]). Logo $H \cong A_5$. Com isso $PSL(2,9) \cong A_6$.

Observe que $|PGL(2,9)| = |S_6| = 720$, mas $PGL(2,9) \ncong S_6$. De fato, dado

$$\rho = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \in GL(2,9),$$

temos que

$$\rho^n = \begin{pmatrix} 1 & 0 \\ 0 & \lambda^n \end{pmatrix},$$

assim $\bar{\rho} \in PGL(2,9)$, dado por $\bar{\rho} = \rho Z(GL(2,9))$, é tal que $o(\bar{\rho}) = o(\rho) = o(\lambda) = 8$. Ou seja, $PGL(2,9)$ possui um elemento de ordem 8, enquanto S_6 não possui nenhum elemento de ordem 8.

Seja ϕ o automorfismo Frobenius de $\mathbb{F}_9 = \mathbb{F}_{3^2}$ definido por $a^\phi = a^3$ para $a \in \mathbb{F}_9$. Então ϕ induz um automorfismo em $GL(2,9)$, que também será denotado por ϕ, dado por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\phi = \begin{pmatrix} a^3 & b^3 \\ c^3 & d^3 \end{pmatrix},$$

para quaisquer $a, b, c, d \in \mathbb{F}_9$. Observe que ϕ se trata de um automorfismo pois se $a, b \in \mathbb{F}_9$ temos que $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3$, onde em $\mathbb{F}_9$ temos que $3 = 0$.

Seja então $P\Gamma L(2,9) = \langle PGL(2,9), \phi \rangle$. É conhecido que $P\Gamma L(2,9) \cong Aut(A_6)$ ([17], Teorema 3.2). $PSL(2,9)$ não possui complemento em $P\Gamma L(2,9)$. Para isso considere o seguinte lema.

Lema 4.24 ([13], Lema 1.2) *Se $PSL(n,q)$ tem complemento em $P\Gamma L(n,q)$ então*

$$mdc(m, d, (q-1)/d) = 1,$$

onde $q = p^m$, p primo e $d = mdc(n, q-1)$.

Então para $PSL(2,9)$ temos que $q = 9 = 3^2$, $m = 2$, $d = mdc(2,8) = 2$, $(q-1)/d = (9-1)/2 = 4$. Então $mdc(m, d, (q-1)/d) = mdc(2,2,4) = 2 \neq 1$. Desta forma $PSL(2,9)$ não possui complemento em $P\Gamma L(2,9)$.

Além disso, $PSL(2,9) \nleq \Phi(P\Gamma L(2,9))$ pois se $PSL(2,9) \leq \Phi(P\Gamma L(2,9))$, como o subgrupo de Frattini é nilpotente, teríamos $A_6 \cong PSL(2,9)$ nilpotente, absurdo.

Lembre que se S é um grupo simples não abeliano então $Aut(S)$ um grupo primitivo do tipo 2 com $Soc(Aut(S)) = S$. Desta forma temos que A_6 é o único subgrupo normal minimal de $Aut(A_6)$, A_6 não é complementado e $A_6 \nleq \Phi(Aut(A_6))$. Além disso, $Out(A_6) = Aut(A_6)/A_6 \cong C_2 \times C_2$.

Referências Bibliográficas

[1] A. Ballester-Bollinches and L. M. Ezquerro, *Classes of Finite Groups*, 1. ed. Springer Netherlands, 2006.

[2] D. W. Barnes, On complemented chief factors of finite soluble groups. *Bull. Austral. Math. Soc.*, **7** (1972), 101-104.

[3] E. Detomi and A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group. *Journal of Algebra*, **256** (2003), 615-668.

[4] K. Doerk and T. Hawkes, *Finite Soluble Groups.* Walter de Gruyter & Co., Berlin, 1992.

[5] Dune (https://math.stackexchange.com/users/39281/dune), *Group presentation of A_5 with two generators.* Disponível em: <https://math.stackexchange.com/a/1999793>. Acesso em: 20 de fev. de 2020.

[6] W. Gaschütz Die Eulersche Funktion endlicher auflösbarer Gruppen. *Illinois Journal of Mathematics*, **3** (1959), 469-476.

[7] W. Gaschütz Praefrattinigruppen, *Arch. Math.*, **13** (1962), 418-426.

[8] B. Huppert *Endlich Gruppen*, Springer-Verlag Berlin, 1967.

[9] N. Jacobson *Basic Algebra I*, Second edition, Dover Publications, 2009.

[10] P. Jiménez-Seral and J. Lafuente, On Complemented Nonabelian Chief Factors of a Finite Group. *Israel Journal of Mathematics*, **106** (1998), 177-188.

[11] J. Lafuente, Nonabelian crowns and schunck classes of finite groups. *Arch. Math.*, **42** (1984), 32-39.

[12] J. Lafuente, Maximal subgroups and the Jordan-Hölder Theorem, *Journal of the Australian Mathematical Society*, **46** (1989), 356-364.

[13] A. Lucchini, F. Menegazzo and M. Morigi, On the existence of a complement for a finite simple group in its automorphism group. *Illinois Journal of Mathematics*, **47** (2003), 395-418.

[14] D. J. S. Robinson, *A Course in the Theory of Groups*, Second Edition, Springer-Verlag New York, 1996.

[15] D. J. S. Robinson and J. S. Wilson, Soluble groups with many polycyclic quotients. *Proc. London Math. Soc (3)*, **48** (1984), 193-229.

[16] J. S. Rose, *A Course in the Theory of Groups*, Second Edition, Cambridge University Press, 1978.

[17] R. A. Wilson *The Finite Simple Groups*, Springer, 2009.