UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Antonio Diego Silva Farias

Classificação dos grupos finitos com um subgrupo cíclico maximal

Fortaleza
2011

Antonio Diego Silva Farias

Classificação dos grupos finitos com um subgrupo cíclico maximal

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Matemática da Universidade Federal do Ceará, como requisito parcial para obtenção do grau de Mestre em Matemática.

Área de Concentração: Álgebra.
Orientador: Prof. Dr. José Robério Rogério.

Fortaleza

2011

Farias, Antonio Diego Silva

F228c Classificação dos grupos finitos com um subgrupo cíclico maximal

Antonio Diego Silva Farias - Fortaleza: 2011.

90 f.

Orientador: Prof. Dr. José Robério Rogério

Área de Concentração: Matemática

Dissertação (Mestrado) - Universidade Federal do Ceará, Centro de Ciências, Fortaleza - CE

Departamento de Matemática, 2011.

1 - Teoria dos grupos. I - Rogério, José Robério (Orientador)

CDD 512.2

Agradecimentos

Primeiramente agradeço a todos os meus familiares especialmente a meus pais, que me apoiaram durante toda minha vida.

Agradeço ao professor José Robério Rogério, por ter aceito ser meu orientador e por ter sido de grande importância em minha formação acadêmica.

Agradeço também a todos os meus amigos da graduação e do mestrado, principalmente ao Raimundo Bastos (Bill), Jardênia, Kelvin, Alexandre, Emanuel Viana, Landerson, Gleison, Vanderson, Clodomir, César e Juliana.

Agradeço a todos Professores que contribuíram em minha formação, em especial a José Robério Rogério, Alexandre Fernades, José Afonso, Manuel Azevedo, Jorge Hebert, Plácido, Antonio Caminha, Silvano, Abdênago, Luquésio Jorge, José Oton, José Alberto e Lev Birbrair.

Agradeço aos professores José Alberto Duarte Maia e Antônio de Andrade e Silva por aceitarem participar da minha banca.

Ao CNPq pela ajuda financeira.

RESUMO

Durante toda a história da Matemática sempre se buscou classificar os objetos que estavam sendo estudados. A partir de um resultado clássico, que classificou os grupos de ordem p^n com um subgrupo cíclico maximal, V. V. Pylaev juntamente com N. F. Kuzennyi classificaram os grupos finitos com um subgrupo cíclico maximal. Utilizando este Teorema e um Lema de classificação dos grupos de ordem p^n com no máximo um subgrupo não cíclico maximal, classificaram também os grupos finitos com no máximo um subgrupo não cíclico maximal.

Palavras chave: Álgebra. Teoria dos grupos.

ABSTRACT

Throughout the history of mathematics has always sought to classify the objects that were being studied. From a classical result, which classified the groups of order p^n with a maximal cyclic subgroup, V. V. Pylaev with N. F. Kuzennyi classified the finite groups with a maximal cyclic subgroup. Using this Theorem and a Lemma for the classification of groups of order p^n with at most one non-cyclic maximal subgroup, also classified the finite groups with at most one non-cyclic maximal subgroup.

Keywords: Algebra. Group theory.

Conteúdo

NOTAÇÃO

$A \subseteq G$	A é subconjunto de G;
$A \subset G$	A é subconjunto de G com $A \neq G$;
$A \leq G$	A é subgrupo de G;
$A < G$	A é subgrupo de G com $A \neq G$;
$X \leq_G M$	X é G-submódulo;
$X <_G M$	X é G-submódulo com $X \neq M$;
$N \trianglelefteq G$	N é um subgrupo normal;
$N \triangleleft G$	N é um subgrupo normal com $N \neq G$;
$N \lessdot G$	N é um subgrupo maximal;
$N \cdot \triangleleft G$	N é um subgrupo normal minimal;
$N \underset{car}{\trianglelefteq} G$	N é um subgrupo característico de G;
$\frac{G}{N}$	Grupo quociente de G por N;
$H \simeq G$	H é isomorfo a G;
$\|H : G\|$	O índice de H em G;
$Z(G)$	O centro de G;
$C_G(H)$	O centralizador de H em G;
$N_G(H)$	O normalizador de H em G;
$G' = [G, G]$	O subgrupo derivado de G;
$\Phi(G)$	O subgrupo de Fratini de G;
$P \times Q$	Produto direto;
$P \rtimes Q$	Produto semidireto;
$S \oplus V$	Soma direta;
x^g	O conjugado de x por g.

S_X	Grupo das permutações do conjunto X;
$Aut\ G$	Grupo dos automorfismos de G;
$\bigcup\!\!\!\cdot$	União disjunta;
$\langle a \rangle$	Grupo gerado pelo elemento a;
$o(a)$	Ordem do elemento a;
$\|G\|$	Ordem do grupo G;
p	Um número primo;
p'	Um número primo diferente de p;
q	Um número primo;
q'	Um número primo diferente de q;
$Syl_p(G)$	O conjunto de todos os p-subgrupos de Sylow de G;
(m, n)	O mdc entre m e n;
$m \mid n$	m divide n;
$m \nmid n$	m não divide n;

Introdução

Um dos primeiros resultados sobre classificação de p-grupos com um subgrupo cíclico maximal pode ser estudado em nível de Graduação, visto que a demonstração do mesmo utiliza apenas feramentas elementares da teoria dos grupos, conforme segue:

Proposição 0.0.1. *Um grupo de ordem p^n contêm um subgrupo cíclico de índice p (Em outras palavras, um subgrupo cíclico maximal) se e somente se é um dos seguintes grupos:*

i) $G = \langle a;\ a^{p^n} = 1\rangle$, $n \geq 1$;

ii) $G = \langle a, b;\ a^{p^{n-1}} = 1,\ b^p = 1\rangle$, $n \geq 2$;

iii) $G = \langle a, b;\ a^{p^{n-1}} = 1,\ b^p = 1,\ bab^{-1} = a^{1+p^{n-2}}\rangle$, $n \geq 3$, p *é ímpar;*

iv) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}},\ bab^{-1} = a^{-1}\rangle$, $n \geq 3$;

v) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = 1,\ bab^{-1} = a^{-1}\rangle$, $n \geq 3$;

vi) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = 1,\ bab^{-1} = a^{1+2^{n-2}}\rangle$, $n \geq 4$;

vii) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = 1,\ bab^{-1} = a^{-1+2^{n-2}}\rangle$, $n \geq 4$.

Naturalmente tentou-se estender este resultado para grupos finitos em geral. Apenas em 1975 V. V. Pylaev em parceria com N. F. Kuzennyi conseguiram classificar os grupos finitos com um subgrupo cíclico maximal.

Teorema 0.0.1 (**Primeiro Teorema de Kuzennyi - Pylaev**). *Um grupo finito G contêm um subgrupo cíclico maximal se e somente se é de um dos seguintes tipos:*

i) $G = P \times \langle a_1\rangle$, *onde* $\langle a_1\rangle$ *é um grupo cíclico qualquer e* P *é um p-subgrupo de Sylow de* G *de um dos tipos indicados na Proposição 0.0.1;*

ii) $G = (\langle a_2 \rangle \rtimes P) \times \langle a_1 \rangle$, *onde* $\langle a_1 \rangle$ *é um grupo cíclico qualquer que é um subgrupo de Hall de* G, P *é um p-subgrupo de Sylow de* G *de um dos tipos indicados na Proposição 0.0.1,* $\langle a_2 \rangle \rtimes P$ *é não nilpotente, e* $C_P(\langle a_2 \rangle)$ *é um subgrupo cíclico de índice p em* P*;*

iii) $G = (P \rtimes \langle a_2 \rangle) \times \langle a_1 \rangle$, *onde* $\langle a_1 \rangle$ *é um grupo cíclico qualquer que é um subgrupo de Hall de* G, *e* $G_1 = P \rtimes \langle a_2 \rangle$ *é um grupo não nilpotente satisfazendo a seguinte condição:* P *é um p-subgrupo de Sylow de* G_1, $C_P(\langle a_2 \rangle) \geq \Phi(P)$, *e* $C_P(\langle a_2 \rangle)$ *é um subgrupo cíclico normal em* G_1 *tal que*

$$\frac{\langle a_2 \rangle C_P(\langle a_2 \rangle)}{C_P(\langle a_2 \rangle)} \lessdot \frac{G_1}{C_P(\langle a_1 \rangle)}.$$

Seria bastante interessante se conseguíssemos uma apresentação para os grupos com a propriedade acima, assim como faremos no caso em que G é p-grupo. Para demonstrar o Teorema presisaremos porvar o seguinte resultado:

Proposição 0.0.2. *Seja* G *um grupo finito, se existe um subgrupo* A *de* G *maximal abeliano, então* G *é solúvel.*

Feito isto, poderemos utilzar uma série de ferramentas que desenvolveremos nos Capítulos iniciais. Em seguida provaremos um Lema que nos ajudará a classificar os grupos finitos com no máximo um subgrupo não cíclico maximal.

Lema 0.0.1. *Um p-grupo contêm no máximo um subgrupo não cíclico maximal se e somente se é um dos seguintes grupos:*

i) $G = \langle a;\ a^{p^n} = 1 \rangle$, $n \geq 1$*;*

ii) $G = \langle a, b;\ a^{p^{n-1}} = 1,\ b^p = 1 \rangle$, $n \geq 2$*;*

iii) $G = \langle a, b;\ a^{p^{n-1}} = 1, b^p = 1, bab^{-1} = a^{1+p^{n-2}} \rangle$, $n \geq 3$, p *é ímpar;*

iv) $G = \langle a, b;\ a^4 = 1,\ b^2 = a^2,\ bab^{-1} = a^{-1} \rangle$*;*

v) $G = \langle a, b;\ a^{2^{n-1}} = 1, b^2 = 1,\ bab^{-1} = a^{1+2^{n-2}} \rangle$, $n \geq 4$.

Por fim, encerramos este trabalho classificando os grupos finitos com no máximo um subgrupo não cíclico maximal como uma aplicação não trivial do Primeiro Teorema de Kuzennyi - Pylaev.

Teorema 0.0.2 (**Segundo Teorema de Kuzennyi - Pylaev**)**.** *Um grupo finito* G *contêm no máximo um subgrupo cíclico maximal se e somente se é um dos seguintes grupos:*

i) G é um p-grupo de um dos tipos:

a) $\langle a;\ a^{p^n} = 1\rangle$, $n \geq 1$;

b) $\langle a, b;\ a^{p^{n-1}} = 1 = b^p,\ ba = ab\rangle$, $n \geq 2$;

c) $\langle a, b;\ a^{p^{n-1}} = 1 = b^p,\ bab^{-1} = a^{1+p^{n-2}}\rangle$, $n \geq 3$, *p ímpar;*

d) $\langle a, b;\ a^{2^{n-1}} = 1 = b^2,\ bab^{-1} = a^{1+2^{n-2}}\rangle$, $n \geq 4$;

e) Grupo Quaternio.

ii) $G = \langle a_1\rangle$ *é um grupo cíclico finito que não é p-grupo;*

iii) $G = P \times \langle a_1\rangle$, *onde* P *é o grupo quaternio ou abeliano elementar de ordem* p^2, *e* $\langle a_1\rangle$ *é um subgrupo de Sylow de* G;

iv) $G = (\langle a_2\rangle \rtimes \langle a\rangle) \times \langle a_1\rangle$, *onde* $\langle a\rangle$, $\langle a_1\rangle$ *e* $\langle a_2\rangle$ *são subgrupos de Sylow de* G, *e* $\langle a_2\rangle \rtimes \langle a\rangle$ *é não nilpotente tal que* $C_{\langle a\rangle}(\langle a_2\rangle) = \langle a^p\rangle$ *e* $C_{\langle a_2\rangle}(\langle a\rangle) = \langle a_2^{p_2}\rangle$;

v) $G = P \rtimes \langle a_2\rangle$, *onde* P *e* $\langle a_2\rangle$ *são subgrupos de Sylow de* G, $C_P(\langle a_2\rangle) = \Phi(P)$, $C_P(\langle a_2\rangle)$ *é cíclico normal de* G *tal que*

$$\frac{\langle a_2\rangle\Phi(P)}{\Phi(P)} \lessdot \frac{G}{\Phi(P)}.$$

Capítulo 1

Revisão de Teoria dos Grupos

Neste capítulo faremos uma revisão de alguns resultados básicos normalmente estudados em um curso de introdução a teoria dos grupos e que serão importantes na demonstração de nosso Teorema principal. Vamos supor que o leitor tem conhecimento das definições de grupo e de subgrupo. Começamos definido classes laterais, conforme segue.

1.1 Classes Laterais

Definição 1. *Dados $x, y \in G$. Dizemos que x está relacionado com y com respeito ao subgrupo H, ou simplesmente que $x \sim y$, se e somente se $x^{-1} * y \in H$.*

Proposição 1.1.1. *$\sim$ define uma relação de equivalência em G.*

Demonstração.

1. (Propriedade Reflexiva) $x \sim x$, pois H subgrupo e $x \in G$ implicam que $x^{-1} \in G$. Como $x * x^{-1} = 1 \in H$, temos $x \sim x$;

2. (Propriedade Simétrica) Suponha que $x \sim y$. Então $x^{-1} * y \in H$, como H é subgrupo temos que $(x^{-1} * y)^{-1} = y^{-1} * x \in H$. Portanto $x \sim y$ implica $y \sim x$;

3. (Propriedade Transitiva) Suponha que $x \sim y$ e que $y \sim z$, então $x^{-1} * y \in H$ e $y^{-1} * z \in H$. Logo, $(x^{-1} * y) * (y^{-1} * z) = x^{-1} * z \in H$, e portanto $x \sim z$.

□

Definição 2. *Dado $x \in G$, o conjunto $\overline{x} = \{y \in G;\ x \sim y\} = \{y \in G;\ y \in xH\} = xH$ é chamada classe lateral à esquerda de x.*

Observação 1. *$x \sim y \iff y * x^{-1} \in H$ também define uma relação de equivalência em G. Onde $\overline{x} = \{y \in G;\ x \sim y\} = \{y \in G;\ y \in Hx\} = Hx$ é chamada classe lateral à direita de x.*

Proposição 1.1.2. *Existe uma bijeção entre o conjunto A das classes laterais à direita e o conjunto B das classes laterais à esquerda.*

Demonstração. Basta definir $\phi :\ A \longrightarrow B$ pondo $\phi(Hx) = (x^{-1}H)$ e claramente ϕ é uma bijeção. □

Definição 3. *(**Transversal**) Seja $H \leq G$. Dizemos que $T \subseteq G$ é um transversal de H em G (à esquerda) se*

$$G = \bigcup_{t\ \in\ T} tH \text{ e } t \neq t' \Longrightarrow tH \neq t'H.$$

Exemplo 1. *Sejam $G = S_3 = \{(1, (123), (132), (12), (13), (23)\}$ e $H = \{1, (12)\}$*

Classes laterais (à esquerda)

$1H = H = (12)H$

$(13)H = \{(13), (123)\} = (123)H$

$(23)H = \{(23), (132)\} = (132)H$

Transversais

$T = \{1, (13), (23)\}, T = \{1, (13), (132)\}, \ldots$

Definição 4. *Se $|X|$ é o número de elementos do conjunto X (finito ou infinito), então:*

1. *$|X| = |Y|$ se existe uma aplicação bijetiva de X em Y*
2. *$|X| \leq |Y|$ se existe uma aplicação injetiva de X em Y*
3. *$|X||Y| = |X \times Y|$*

Proposição 1.1.3. *Se $|A_i| = |A|$ e para $i \neq j$ tem-se que $A_i \cap A_j = 1$, então*

$$|\bigcup_{i\ \in\ I} A_i| = |I||A|.$$

Demonstração. Defina $\phi : I \times A \longrightarrow \bigcup_{i \in I} A_i$ pondo $\phi(i,a) = \phi_i(a)$, onde ϕ_i é uma bijeção de A em A_i. Se $x \in \bigcup_{(x,i) \in T \times I} A_i$, então existe $i \in I$ tal que $x \in A_i$ e ϕ_i é bijeção, existe um único $a \in A$ tal que $\phi(a) = \phi_i(a) = x$ assim ϕ é **sobrejetiva**. Por outro lado se $\phi(i,a) = \phi(j,b) = x$, então existe um único $m \in I$ tal que $x \in A_i$, assim $i = j$ e $a = b$, tendo em vista que ϕ_i é bijetiva. Com isto provamos que ϕ é **bijetiva** □

Teorema 1.1.1 (**Teorema do Índice**). *Sejam G um grupo, $K \leq H$ e $H \leq G$ com K não vazio. Então $|G : K| = |G : H||H : K|$.*

Demonstração. Sejam T um transversal de H em G e U um transversal de K em H. Então $H = \bigcup_{u \in U} uK$ e $G = \bigcup_{t \in T} tH$. Vamos mostrar que $G = \bigcup_{(u,t) \in U \times T} tuK$. Com efeito, se $g \in G$ então $\exists^m\ t \in T$ e $h \in H$ tais que $g = th$. Como $h \in H$, $\exists\ u \in U$ e $k \in K$ tais que $h = uk$. Portanto, $g = tuk \in \bigcup_{(u,t) \in U \times T} tuK$. Logo $G \subseteq \bigcup_{(u,t) \in U \times T} tuK$. Tome $x \in \bigcup_{(u,t) \in U \times T} tuK$. Então $x = tuk$, onde $t \in T$, $u \in U$ e $k \in K$. Como $H = \bigcup_{u \in U} uK$ temos que $h = uk \in H$ e portanto $x = th$, mas como $G = \bigcup_{t \in T} tH$ temos que $x \in G$. Logo, $\bigcup_{(u,t) \in U \times T} tuK \subseteq G$ e portanto $\bigcup_{(u,t) \in U \times T} tuK = G$. Assim, o conjunto $\Omega = TU$ é um transversal de K em G, de modo que $|G : K| = |\Omega| = |TU| = |T||U| = |G : H||H : K|$ (Desde que $|TU| = |T||U|$). Falta mostrar que $|TU| = |T||U|$, para tanto defina $\phi :\ T \times U \to TU$ por $\phi(t,u) = tu$. Claramente ϕ está bem definida e é sobrejetiva. Se $tu = t'u'$, então $tuK = t'u'K$. Como $H = \bigcup_{u \in U} uK$ e $uK \neq u'K \subseteq H$, temos que $tH = t'H$ e assim $t = t'$ e ϕ é bijetiva. □

Corolário 1.1.1 (**Teorema de Lagrange**). *Sejam G um grupo e $H \leq G$, então*

$$|G| = |G : H||H|.$$

Demonstração. Basta toma $K = \{1\}$ no Teorema anterior e ver que

$$|G : K| = |G : H||H : K| \Longleftrightarrow |G| = |G : H||H|.$$

□

Corolário 1.1.2. *Se $|G| < \infty$ e $H \leq G$ então $|H| \mid |G|$.*

Demonstração. Basta ver que $|G| = |G : H||H|$, pelo Corolário anterior. □

Teorema 1.1.2 (**Teorema de Poincarré**). *Sejam G um grupo e $H, K \leq G$. Se $|G : H|$, $|G : K| < \infty$, então $|G : H \cap K| \leq |G : H||G : K| < \infty$.*

Demonstração. Defina

$$\phi : \ \{x(H \cap K);\ x \in G\} \longrightarrow \{xH; x \in G\} \times \{xK; x \in G\}$$

por $\phi(x(H \cap K)) = (xH, xK)$.
Dados $x, y \in G$. Se $\phi(x(H \cap K)) = \phi(y(H \cap K))$, então $(xH, xK) = (yH, yK)$. Assim, $xH = yH$ e $xK = yK$. Como por definição $y^{-1}x \in H \cap K$, temos que $x(H \cap K) = y(H \cap K)$. Portanto, ϕ é injetiva e vale a desigualdade do Teorema. □

Exemplo 2. *Sejam G um grupo e $H, K \leq G$. Se $(|G : H|, |G : K|) = 1$, então*

$$|G : H \cap K| = |G : H||G : K|.$$

Demonstração. Como $H \cap K \leq H \leq G$, pelo Teorema do índice temos que

$$|G : H \cap K| = |G : H||H : H \cap K| = |G : K||K : H \cap K|.$$

Logo, $|G : H| \mid |G : H \cap K|$ e $|G : K| \mid |G : H \cap K|$. Como $(|G : H|, |G : K|) = 1$, segue-se que $|G : H||G : K| \mid |G : H \cap K|$. Em particular $|G : H||G : K| \leq |G : H \cap K|$, mas pelo Teorema de Poincaré vale a desigualdade contrária e portanto temos a igualdade. (Observe que $(|G : H|, |G : K|) = 1$ só tem sentido se $|G : H|$,$|G : K| < \infty$). □

Proposição 1.1.4. *Sejam $H, K \leq G$. Então $|HK||H \cap K| = |H||K|$.*

Demonstração. Defina a seguinte relação de equivalência em $H \times K$.

$$(h, k) \sim (h', k') \Longleftrightarrow hk = h'k' \Longleftrightarrow h'^{-1}h = k'k^{-1} \in H \cap K.$$

Claramente $\sim$ é uma relação de equivalência em $H \times K$. Vejamos que

$$\overline{(h, k)} = \{(hx^{-1}, xk);\ x \in H \cap K\},$$

pois $h'^{-1}h = k'k^{-1} = x \iff hx^{-1} = h$ e $k' = xk$. Logo, $|\overline{(h,k)}| = |H \cap K|$. Para cada classe $\overline{(h,k)}$ podemos tomar um único representante (h', k') de forma que o conjunto $I = \{Representantes\}$ é tal que $H \times K = \bigcup\limits_{(h,k)\ \in\ I}^{\cdot} \overline{(h,k)}$. Pela Proposição 1.1.3 $|H \times K| = |I||\overline{(h,k)}| = |I||H \cap K|$. Falta mostrar que $|I| = |HK|$, feito isto a demonstração da Proposição acaba.

Afirmação: $|I| = |HK|$.

De fato, basta considerar $\phi : HK \to I$ por $\phi(hk) = \overline{(h,k)}$. Claramente ϕ é sobrejetiva e injetiva, e $hk = h'k' \implies \overline{(h,k)} = \overline{(h',k')}$. Portanto ϕ está bem definida e assim $|I| = |HK|$. □

1.2 Subrupos Normais e Grupos Cíclicos

Proposição 1.2.1. *Seja $N \leq G$. São equivalentes:*

i) $xN = Nx$, $\forall x \in G$;

ii) $x^{-1}Nx = N$, $\forall x \in G$;

iii) $x^{-1}Nx \subseteq N$, $\forall x \in G$;

Demonstração. $i) \implies ii)$

Dado $n \in N$ como $xN = Nx$, existe $m \in N$ tal que $nx = xm$. Assim, $x^{-1}nx = x^{-1}xm = m \in N$ e portanto, $x^{-1}Nx \subseteq N$. Se $n \in N$, então $nx \in Nx = xN$. Logo, $x^{-1}nx \in x^{-1}Nx$ e com isto $x^{-1}Nx = N$.

$ii) \implies iii)$ Trivial.

$iii) \implies i)$

Dado $n \in N$ temos que $x^{-1}nx \in x^{-1}Nx \subseteq N \implies Nx \subseteq xN$. Reciprocamente, $xnx^{-1} \in xNx^{-1} \subseteq N \implies xN \subseteq Nx \implies xN = Nx$. □

Definição 5. *Seja $N \leq G$. Se N satisfaz um dos itens da Proposição anterior, portanto todos, dizemos que N é um* ***Subgrupo Normal*** *de G, e denotamos $N \trianglelefteq G$.*

Proposição 1.2.2. *Seja $N \trianglelefteq G$, então o conjunto $\{xN;\ x \in G\}$ é um grupo com a seguinte operação: $(xN)(yN) = (xy)N$.*

Demonstração. Primeiro devemos mostrar que a operação está bem definida. Tome $xN = x'N$ e $yN = y'N$, para mostrar que $(xN)(yN) = (x'N)(y'N)$ é necessário e suficinte mostrar que $y'^{-1}x'^{-1}xy \in N$. Como $xN = x'N$, temos que $n = x'^{-1}x \in N$. Assim, $y'^{-1}x^{-1}xy = y'^{-1}ny \in N$ pela definição de grupo normal. Com isto fica provado que a operação é bem definida.

i) **Associatividade:** $(xN)[(yN)(zN)] = (xN)[(yz)N] = [x(yz)]N = [(xy)z]N$
$= [(xy)N](zN) = [(xN)(yN)](zN)$;

ii) **Elemento Neutro:** Dado $x \in G$, $(xN)(1N) = xN = (1N)(xN)$;

iii) **Elemento Inverso:** Dado $x \in G$, $(xN)(x^{-1}N) = 1N = (x^{-1}N)(xN)$. □

Denotamos por $\dfrac{G}{N} = \{xN;\ x \in G\}$, e o chamamos de grupo quociente.

Definição 6. *Seja $N \trianglelefteq G$, o índice de N sobre G é definido por $|G : N| = |G/N|$.*

Exemplo 3. *Seja $G = S_3$, e $N = \{1, (12)\}$. Então*
$(13)N = \{(13), (123)\}$;
$N(13) = \{(13), (132)\} \neq (13)N$.
Assim, N não é um subgrupo normal de G. As classes à direita de N são: $N, (13)N$ e $(23)N = \{(23), ((132)\}$. Veja que o produto de classes não está bem definido, pois $[(12)N][(23)N] = \{(13), (123)\}\{(23), (132)\} = \{(132), (23), (12), 1\}$ não é uma classe à direita de N.

Proposição 1.2.3. *Seja $N \leq G$ com $|G : N| = 2$, então $N \trianglelefteq G$.*

Demonstração. G é a união disjunta $N \cup Na = N \cup aN$, para todo $a \in G - N$. Se $aN \cap N \neq \emptyset$, então $ax = x'$, com x e x' elementos de N, isto é, $a = x'x^{-1} \in N$. Logo, $aN = Na$ e portanto N é um subgrupo normal de G. □

Proposição 1.2.4. *Sejam G um grupo e $H, K \leq G$, então:*

i) $HK \leq G$ se e somente se $HK = KH$;

ii) se $H \trianglelefteq G$ então $HK \leq G$.

Demonstração. i) Suponha que HK é subgrupo. Dado $kh \in KH$ temos que $kh = (h^{-1}k^{-1})^{-1} \in HK$, pois $HK \leq G$, então $KH \subseteq HK$. Agora, dado $hk \in HK$, temos

$(hk)^{-1} = k^{-1}h^{-1} \in KH$. Como HK é subgrupo, para $hk \in HK$ temos que $(hk)^{-1} \in HK$ e portanto $hk = ((hk)^{-1})^{-1} \in KH$. Assim, temos a igualdade.
ii) Seja $H \trianglelefteq G$, então dado $n \in N$ temos que $nH = Hn$. Portanto, $NH = HN$ e assim pelo item (i) $HN \leq G$ □

Definição 7. *Sejam G um grupo e $N \subseteq G$. Definimos o subgrupo gerado por N e denotamos por $\langle N \rangle$, o menor subgrupo de G que contêm N. Também podemos definir da seguinte forma:*

$$\langle N \rangle = \bigcap_{H \leq G,\ N \subseteq H} H.$$

Se $N = \{a\}$ denotamos $\langle \{a\} \rangle$ simplesmente por $\langle a \rangle$

Definição 8. *Seja G um grupo. Dado um elemento $a \in G$ definimos a ordem do elemento a como o menor número inteiro positivo n tal que $a^n = 1$ (se existir), se não existir tal número, dizemos que a ordem de a é zero. Denotamos a ordem de a por $o(a)$.*

Proposição 1.2.5. *Seja G um grupo e $a \in G$, então:*

i) $o(a) = |\langle a \rangle|$, se $o(a) \neq 0$;

ii) Se $a^n = 1$, então $o(a) \mid n$.

Demonstração. i) Basta ver que o conjunto $\{1, a, a^2, \ldots, a^{o(a)-1}\}$ é o menor grupo que contém a.
ii) Suponha que $a^n = 1$. Então pelo algorítmo da divisão existem inteiros p e r tais que $n = o(a).p + r$, com $0 \leq r < o(a)$. Portanto,

$$1 = a^n = a^{o(a).p+r} = a^{o(a).p}.a^r = (a^{o(a)})^p.a^r = a^r.$$

Como $o(a)$ tem a propriedade mínima, segue-se que $r = 0$ e $o(a) \mid n$. □

Definição 9. *Seja G um grupo, dizemos que G é um **grupo cíclico** se existe $a \in G$ tal que $G = \langle a \rangle$.*

Proposição 1.2.6. *Se G é um grupo cíclico, então todo subgrupo H de G também é ciclico.*

Demonstração. Seja $G = \langle a \rangle$. Se $H = \{1\}$, então H é cíclico gerado pelo elemento 1. Se $H \neq 1$, então existe um número inteiro d tal que $a^d \in H$ e como H é subgrupo temos que $a^{-d} \in H$. Assim existe um número inteiro positivo d tal que $a^d \in H$. Seja n o menor inteiro positvo tal que $a^n \in H$.

Afirmação: $\langle a^n \rangle = H$.

De fato, como $a^n \in H$, temos que $\langle a^n \rangle \subseteq H$. Para mostrar a outra inclusão tome $a^l \in H$, pelo algorítimo da divisão existem $m, p \in \mathbb{Z}$ tais que $l = n.m + p$ e $0 \leq p < n$. Portanto, $a^p = a^l.(a^{nm})^{-1} \in H$ e assim $p = 0$. Logo, $H = \langle a \rangle$ e H é cíclico. □

1.3 Subrupos Clássicos

Definição 10. *Sejam G um grupo e H um subgrupo de G definimos:*

i) O Núcleo Normal de H em G por $H_G = \bigcap_{y \in G} yHy^{-1}$

ii) O Fecho Normal de H em G por $H^G = \langle yHy^{-1}; y \in G \rangle$

iii) O Normalizador de H em G por $N_G(H) = \{x \in G; xHx^{-1} = H\}$

iv) O Centralizador de H em G por $C_G(H) = \{x \in G;\ xh = hx\ \forall h \in H\}$

v) O Centro de G por $Z(G) = \{x \in G;\ xy = yx\ \forall y \in G\} = C_G(G)$

Observação 2. *Se $H \trianglelefteq G$, então $H_G = H^G$.*

Demonstração. Basta ver que $H^y = H$, para todo $y \in G$. □

Observação 3. *Facilmente se verifica que H_G, H^G, $N_G(H)$ e $Z(G)$ são subgrupos de G e que H é um subgrupo normal de $N_G(H)$.*

Exemplo 4. *Seja $G = S_3$, $H = \{1, (12)\}$, encontremos H_G, H^G, $N_G(H)$, $C_G(H)$ e $Z(G)$.*
i) Seja $g = (13)$, então

$$H^g = g^{-1}Hg = (13)H(13) = \{(13)1(13), (13)(12)(13)\}$$

$$= \{1, (13)(123)\} = \{1, (23)\}.$$

Assim, $H_G = \bigcap_{y \in G} H^y \subseteq H \cap H^g = \{1\}$ *e portanto* $H_G = \{1\}$*;*

ii) $H^G \leq \langle H, H^g \rangle = \langle 1, (12), (13) \rangle$ *e* $H < H^G \leq G$. *Pelo Teorema de Lagrange* $|H^G| \mid |G|$ *e* $|H| \mid |H^G|$, *assim* $|H^G| = 6$ *e* $H^G = G$;
iii) $N_G(H)$ *é um subgrupo de* G *que contém* H *e pelo argumento anterior* $N_G(H) = H$ *ou* $N_G(H) = G$, *mas* $(13) \notin N_G(H)$. *Logo,* $N_G(H) = H$.
iv) $C_G(H) = H$.
v) $Z(G) = 1$

Proposição 1.3.1. *Sejam* G *um grupo e* $H \leq G$. *Então* H_G *é o maior subgrupo normal em* G *contido em* H *e* H^G *é o menor subgrupo normal em* G *que contém* H.

Demonstração. A demonstração deste resultado segue diretamente da definição. □

Observação 4. *Se* $H \leq G$, *então ,* $N_G(H) \geq H$ *e* $|G : H| = |G : N_G(H)||N_G(H) : H|$.

Teorema 1.3.1 (**Identidade de Dedekind**). *Sejam* G *um grupo,* $A, B, C \leq G$ *com* $A \leq B$. *Então,*

$$A(B \cap C) = (AC) \cap B.$$

Demonstração. É claro que $A(C \cap B) \leq (AC) \cap B$. Seja $x \in (AC) \cap B$. Então $x = ac = b$, onde $a \in A$, $c \in C$ e $b \in B$. Assim, $c = a^{-1}b \in B$. Logo, $c \in C \cap B$ e portanto $ac \in A(C \cap B)$. □

1.4 Homomorfismos de Grupos

Definição 11. *Sejam* G *e* H *grupos. Uma aplicação* $\varphi : G \longrightarrow H$ *é um Homomorfismo se* $\varphi(ab) = \varphi(a)\varphi(b)$, *para* $a, b \in G$. *O Núcleo de* φ *será e definido por:*

$$Ker(\varphi) = \{g \in G;\ \varphi(g) = 1_H\}.$$

A Imagem de φ *é definida e denotada por* $Im(\varphi) = \varphi(G)$. *Um homomorfismo injetivo é chamado de* ***Monomorfismo****, um homomorfismo sobrejetivo é chamado de* ***Epimorfismo*** *e um homomorfismo bijetivo é chamado de* ***Isomorfismo****. Um isomorfismo de* G *em* G *é chamado* ***Automorfismo****. Se existe um isomorfismo entre* G *e* H *dizemos simplesmente que* $G \simeq H$.

Observação 5. *Facilmente se verifica que $\simeq$ é uma relação de equivalência no conjunto de todos os grupos.*

Proposição 1.4.1. *Seja $\varphi: G \longrightarrow H$ um homormorfismo entre grupos, então:*

i) $\varphi(1_G) = 1_H$;

ii) $\varphi(a^{-1}) = [\varphi(a)]^{-1}$;

iii) $Ker(\varphi) \trianglelefteq G$;

iv) $Im(\varphi) \leq H$.

Demonstração. A prova de *i*), *ii*) e *iv*) seguem diretamente da definição.
iii) Seja $N = Ker(\varphi)$ e tome $g \in G$, para provarmos que N é normal é suficiente mostrar que $g^{-1}Ng \subseteq N$. Dado $g^{-1}xg \in g^{-1}Ng$, temos que

$$\varphi(g^{-1}xg) = \varphi(g^{-1})\varphi(x)\varphi(g) = \varphi(x) = 1_H.$$

Assim, $g^{-1}Ng \subseteq N$ e portanto $Ker(\varphi) \trianglelefteq G$. □

Teorema 1.4.1 (**Primeiro Teorema do Isomorfismo**). *Sejam G, H grupos e $\varphi: G \longrightarrow H$ um homomorfismo de grupos. Então*

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

Demonstração. A prova deste Teorema se resume em definir um homormorfismo bijetivo entre $\dfrac{G}{Ker(\varphi)}$ e $Im(\varphi)$. Defina $\Psi: \dfrac{G}{Ker(\varphi)} \longrightarrow Im(\varphi)$ por:

$$\Psi(xKer(\varphi)) = \varphi(x).$$

Para simplificar a demonstração escreva $N = Ker(\varphi)$.

• Ψ é bem definida.

De fato, se $gN = hN$, então $gh^{-1} \in N$ e portanto $1 = \varphi(gh^{-1}) = \varphi(g)[\varphi(h)]^{-1}$. Logo,

$$\varphi(g) = \Psi(gN) = \Psi(hN) = \varphi(h).$$

• Claramente Ψ é homomorfismo sobrejetivo.

• Ψ é injetivo.

Suponha que $\Psi(gN) = \Psi(hN)$. Então $\varphi(g) = \varphi(h)$, asssim $\varphi(gh^{-1}) = \varphi(g)[\varphi(h)]^{-1} = 1$ e portanto $gh^{-1} \in N$. Com isto provamos que $gN = hN$. □

Corolário 1.4.1 (**Segundo Teorema do Isomorfismo**). *Sejam G um grupo, $H \leq G$ e $N \trianglelefteq G$, então $N \cap H \trianglelefteq H$, $N \trianglelefteq NH$ e* $\dfrac{HN}{N} \simeq \dfrac{H}{H \cap N}$.

Demonstração. Basta definir $\varphi : \ H \longrightarrow \dfrac{HN}{N}$ por $\varphi(h) = hN$ e observar que φ é um homomorfismo cujo núcleo é exatamente $H \cap N$. □

Corolário 1.4.2 (**Terceiro Teorema do Isomorfismo**). *Sejam G um grupo, $H \trianglelefteq G$, $N \trianglelefteq G$ e $H \leq N$. Então,*

$$\frac{G}{N} = \frac{G/H}{N/H}.$$

Demonstração. Basta definir $\varphi : \ \dfrac{G}{H} \longrightarrow \dfrac{G}{N}$ por $\varphi(gH) = gN$ e observar que φ é um homomorfismo cujo núcleo é $\dfrac{N}{H}$. □

Teorema 1.4.2 (**Teorema da Correspondência**). *Se G um grupo e $N \trianglelefteq G$, então existe uma correspondência biunívoca entre os subgrupos de G que contêm N e os subgrupos de $\dfrac{G}{N}$. Por esta correspondência, subgrupos normais de G que contêm N correspondem a subgrupos normais de $\dfrac{G}{N}$ e vale a recíproca.*

Demonstração. Sejam $\mathcal{A} = \{H;\ H \leq G,\ N \leq H\}$, $\mathcal{B} = \{\overline{H};\ \overline{H},\ \leq G/N\}$ e defina $\varphi : \ \mathcal{A} \longrightarrow \mathcal{B}$ e $\psi : \ \mathcal{B} \longrightarrow \mathcal{A}$ pondo $\varphi(H) = \{hN;\ h \in H\}$ e $\psi(\overline{H}) = \{h \in G;\ hN \in \overline{H}\}$.

Afirmação 1: Dado $H \in \mathcal{A}$ o conjunto $\varphi(H)$ pertence a $\mathcal{B}$.

i) Como $1 \in H$ temos que $N \in \varphi(H)$;

ii) Dados $h_1N, h_2N \in \varphi(H)$, $(h_1N)(h_2N)^{-1} = h_1h_1^{-1}N \in \varphi(H)$, pois $h_1h_1^{-1} \in H$.

Portanto φ está bem definida.

Afirmação 2: Dado $\overline{H} \in \mathcal{B}$ o conjunto $\psi(\overline{H})$ pertence a $\mathcal{A}$.

i) $N \subseteq \psi(\overline{H})$, pois $nN = N \in \overline{H}$ para todo $n \in N$. Em particular $1 \in \psi(\overline{H})$;

ii) Dados $h_1, h_2 \in \psi(\overline{H})$ temos

$$h_1h_2^{-1}N = (h_1N)(h_2N)^{-1} \in \overline{H}.$$

Portanto, $h_1h_2^{-1} \in \psi(\overline{H})$ e provamos que $\psi(\overline{H})$ é um subgrupo de G que contém N. É fácil ver que φ e ψ são uma inversa da outra e asssim φ e ψ são bijeções.

Obs: Todo subgrupo de $\dfrac{G}{N}$ é da forma $\dfrac{H}{N}$ onde H é um subgrupo de G que contêm N.

Se $H \trianglelefteq G$, $N \leq H$, então pelo Terceiro Teorema do Isomorfismo

$$\frac{H}{N} \trianglelefteq \frac{G}{N}.$$

Suponha agora que $\frac{H}{N} \trianglelefteq \frac{G}{N}$. Afirmamos que $H \trianglelefteq G$.
De fato, dado $x \in H$ temos que $(g^{-1}xg)N = (gN)^{-1}(xN)(gN) \in \frac{G}{N}$ e portanto $g^{-1}xg \in H$. Logo, $H \trianglelefteq G$. □

Lema 1.4.1 (**N/C Lema**). *Sejam G um grupo e $H \leq G$. Então $\frac{N_G(H)}{C_G(H)} \simeq L$, onde L é um subgrupo de Aut $H = \{Automorfismos\ de\ H\}$.*

Demonstração. Defina $\varphi :\ N_G(H) \longrightarrow AutH$

$$g \longmapsto \varphi_g :\ h \longmapsto ghg^{-1}$$

Claramente φ é homomorfismo e $Ker(\varphi) = C_G(H)$. Pelo Primeiro Teorema do Isomorfismo

$$\frac{N_G(H)}{C_G(H)} \simeq Im(\varphi) \leq AutH.$$

□

Definição 12. *Um subgrupo H de um grupo G é característico se para todo automorfismo $\gamma :\ G \longrightarrow G$ tem-se que $\gamma(H) = H$. Notação: $H \overset{\trianglelefteq}{_{car}} G$.*

Observação 6. *$\gamma_g :\ G \longrightarrow G$ dada por $\gamma_g(x) = g^{-1}xg$ é um automorfismo de G para todo $g \in G$ e desta forma todo subgrupo característico é normal.*

Proposição 1.4.2. *Se G é um grupo e existem $H, N \leq G$ tais que $H \overset{\trianglelefteq}{_{car}} N \trianglelefteq G$, então $H \trianglelefteq G$.*

Demonstração. Como $N \trianglelefteq G$ podemos definir para cada $g \in G$ o automorfisfo $\gamma :\ N \longrightarrow N$ dado por $\gamma_g(x) = g^{-1}xg \in N$. Assim, $\gamma_g(H) = H$ para todo $g \in G$ e com isto $H \trianglelefteq G$. □

Observação 7. *$N \trianglelefteq H \trianglelefteq G$ não implica a normalidade de N em G.*

Demonstração. Sejam $G = S_4$, $H = A_4$ e $N = \{1, (12)(34), (13)(24), (14)(23)\}$. Então, $N \trianglelefteq H \trianglelefteq G$, pois $|G : H| = |H : N| = 2$, mas $N \ntrianglelefteq G$. □

1.5 Ação de Grupos

Sejam G um grupo e X um conjunto qualquer. Definimos o conjunto das permutações de X por $S_X = \{f : X \longrightarrow X;\ f \text{ é bijetiva}\}$ e dizemos que G **age** sobre X se existe um homomorfismo $\varphi : G \longrightarrow S_X$ que a cada $g \in G$ associa um bijeção $\varphi_g : X \longrightarrow X$. Dizemos que φ é uma ação de G em X.

Neste caso, $x \sim y \Longleftrightarrow \varphi_g(x) = y$ define uma relação de equivalência. Definimos:

• A **Órbita** de $x \in X$ por $\mathcal{O}(x) = \{\varphi_g(x);\ g \in G\} = \overline{x}$;

• O **Estabilizador** de $x \in X$ por $E(x) = \{g \in G;\ \varphi_g(x) = x\}$;

• $Fix_X(G) = \{x \in X;\ \varphi_g(x) = x\ \forall g \in G\}$.

Proposição 1.5.1. *Se φ é uma ação de G sobre X. Então:*

i) $X = \bigcup\limits_{x \in T}^{\cdot} \mathcal{O}(x)$;

ii) $E(x) \leq G$;

iii) $|G : E(x)| = |\mathcal{O}(x)|$.

Demonstração. *i)* Basta ver que $\mathcal{O}(x)$ é a classe de equivalência de x.

ii) $1 \in E(x)$, pois $\varphi_1 = Id_X$ e $Id_X(x) = x$ para todo $x \in X$. Dados $g, h \in E(x)$ temos,

$$\varphi_{gh^{-1}}(x) = \varphi_g \circ (\varphi_h)^{-1}(x) = \varphi_g[(\varphi_h)^{-1}(x)] = \varphi_g(x) = x.$$

Logo, $E(x)$ é um subgrupo de G.

iii) Defina $\psi : \{gE(x);\ g \in G\} \longrightarrow \mathcal{O}(x)$ por $\psi(g) = \varphi_g(x)$.

• ψ é bem definida.

De fato, se $gE(x) = hE(x)$, então $h^{-1}g \in E(x)$, ou seja, $\varphi_{h^{-1}g}(x) = x$. Portanto,

$$x = \varphi_{h^{-1}}(\varphi_g(x)) = [\varphi_h]^{-1}(\varphi_g(x)).$$

Logo, $\varphi_h(x) = \varphi_g(x)$.

• ψ é injetiva.

Se $\varphi_h(x) = \varphi_g(x)$, então

$$x = [\varphi_h]^{-1}(\varphi_g(x)) = \varphi_{h^{-1}}(\varphi_g(x)) = \varphi_{h^{-1}g}(x).$$

Assim, $h^{-1}g \in E(x)$ e portanto $hE(x) = gE(x)$. Como φ é claramente sobrejetiva, concluímos que $|G : E(x)| = |\mathcal{O}(x)|$. □

Exemplo 5 (**Ação nas Classes**). *Seja $H \leq G$ com $|G : H| = n$. Defina $\varphi : G \longrightarrow S_X$, $X = \{xH;\ x \in G\}$ pondo $\varphi_g(xH) = gxH$.*

• $\varphi_g \in S_X$.

Suponha que $\varphi_g(xH) = \varphi_g(yH)$. Então $gxH = gyH$ e portanto $xH = yH$. Isto prova que φ_g é injetiva. Dado $yH \in X$, $\varphi_g(g^{-1}yH) = yH$, logo φ_g é sobrejetiva.

• $\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$, *ou seja φ é um homomorfismo.*

De fato, $\varphi(gg')(xH) = gg'xH = \varphi_g(g'xH) = \varphi_g \circ \varphi_{g'}(xH)$

• $Ker(\varphi) = \{g \in G;\ \varphi_g = Id_X\}$. *Assim,*

$$g \in Ker(\varphi) \Longleftrightarrow \varphi_g(xH) = gxH = xH \forall x \in G$$

$$\Longleftrightarrow x^{-1}gx \in H \forall x \in G \Longleftrightarrow g \in xHx^{-1} \forall x \in G$$

$$\Longleftrightarrow g \in H^{g^{-1}} \Longleftrightarrow g \in H_G.$$

Portanto, $Ker(\varphi) = H_G$. Logo,

$$\frac{G}{H_G} \simeq Im(\varphi) \leq S_X \simeq S_n.$$

Em particular, $|G : H_G| \mid n!$.

Corolário 1.5.1. *Seja $H \leq G$ com $|G : H| = p$, onde p é o menor primo que divide a ordem de G. Então, $H = H_G \trianglelefteq G$.*

Demonstração. Pelo exemplo anterior $\dfrac{G}{H_G} \simeq L \leq S_p$.

Afirmação: $|H : H_H| = 1$.

De fato, se $|H : H_G| \neq 1$, então existe um primo q tal que $q \mid |H : H_G|$. Mas como $|H : H_G| \mid |G|$ concluímos que $q \geq p$. Por outro lado, como $H_g \leq H \leq G$ e $q \mid |G : H_G| \mid p!$. Daí, $q \leq p$ e portanto $p = q$. Assim, $p^2 \mid |G : H_G|$, pois $p! = |G : H_G| = |G : H||H : H_G|$. Com isto obtemos que $p^2 \mid p!$, que é um absurdo. □

Teorema 1.5.1. *i) Seja G um p-grupo finito (isto é, $|G| = p^n$) e suponha que G age sobre X (ou seja, existe um homomorfismo $\varphi : G \longrightarrow S_X$). Então $|Fix(G)| \equiv |X| \pmod p$.*

ii) Sejam $H, J \leq G$ com $|J| = p^m$ e $|G : H| = r$, onde $p \nmid r$. Então existe $x \in G$ tal que $J \leq H^x$.

iii) Se $H \leq G$, $|H| = p^m$ e $p \mid |G : H|$, então $p \mid |N_G(H) : H|$. Em particular, se $|G| = p^n$ e $H < G$, então $H < N_G(H)$.

iv) Seja $H \trianglelefteq G$, G finito, e $J \leq G$ com $|J| = p^m$. Se $|H| \equiv 1 \ (mod\ p)$, então $H \cap C_G(J) \neq 1$. Em particular, se $|G| = p^n$ e H é normal próprio, então $H \cap Z(G) \neq 1$.

Demonstração. i) Como G é finito, temos que $X = \mathcal{O}_{x_1} \cup \mathcal{O}_{x_2} \cup \ldots \cup \mathcal{O}_{x_r}$. Logo,

$$|X| = |\mathcal{O}_{x_1}| + |\mathcal{O}_{x_2}| + \ldots + |\mathcal{O}_{x_r}| = |Fix_X(G)| + |\mathcal{O}_{x_s}| + \ldots + |\mathcal{O}_{x_r}|,$$

onde $Fix_X(G) = \{x_1, x_2, \ldots, x_{s-1}\}$ e $x_s, x_{s+1}, \ldots, x_r \notin Fix_X(G)$. Agora, pela Proposição 1.5.1, temos que $|\mathcal{O}_{x_i}| = |G : E(x_i)| = p^{\alpha_i}$. Como $|G : E(x_i)| = 1$ se e somente se $x_i \in Fix_X(G)$, concluímos que $p \mid (|X| - |Fix_X(G)|)$ e portanto $|Fix_X(G)| \equiv |X| \ (mod\, p)$.
ii) Considere J agindo nas classes de X, conforme fizemos no exemplo anterior. Por *i)* obtemos que $|Fix_X(G)| \equiv |X| = r \ (mod\ p)$. Como $p \nmid r$, temos que $p \nmid |Fix_X(G)|$ e portanto $Fix_X(G) \neq \emptyset$. Tome $xH \in Fix_X(G)$ então,

$$gxH = \varphi_g(xH) = xH \ \forall g \in J \Longleftrightarrow gxH = xH \ \forall g \in J$$

$$\Longleftrightarrow x^{-1}gx \in H \ \forall g \in J \Longleftrightarrow g \in H^{x^{-1}} \ \forall g \in J.$$

Logo, $J \leq H^{x^{-1}}$.
iii) Sejam $X = \{xH;\ x \in G\}$ e $\varphi : H \longrightarrow S_X$ dada por $\varphi_h(xH) = hxH$. Por (i) $|FIX_X(H)| \equiv |X| \ (mod\ p)$, onde $|X| = |G : H|$. Agora,

$$xH \in FIX_X(H) \Longleftrightarrow hxH = xH \ \forall h \in H \Longleftrightarrow x^{-1}hx \in H \ \forall h \in H$$

$$\Longleftrightarrow x^{-1}Hx \subseteq H \Longleftrightarrow x \in N_G(H).$$

Assim, $|FIX_X(H)| = |N_G(H) : H|$. Em particular, se $|G| = p^m$, $H < G$ e $p \mid |G : H|$, então $p \mid |N_G(H) : H|$ e portanto $H < N_G(H)$.
iv) Seja $\varphi : J \longrightarrow S_H$ dada por $\varphi_g(h) = ghg^{-1}$. É claro φ é uma ação bem definida, pois $H \trianglelefteq G$. Por (i) $|FIX_X(J)| \equiv |H| \ (mod\ p)$, mas como $|H| \not\equiv 1 \ (mod\ p)$ concluímos que $|FIX_X(J)| \not\equiv 1 \ (mod\ p)$. Por outro lado, $1 \in FIX_X(H)$ (isto é, $|FIX_X(H)| > p$) e

portanto existe $h \neq 1$ tal que $h \in FIX_X(H)$. Logo, para todo $g \in J$ temos $ghg^{-1} = h$ e daí, $h \in H \cap C_G(J)$. Em particular, se $|G| = p^k$ e $H \trianglelefteq G$, $H \neq 1$, tome $J = G$ e então

$$H \cap C_G(G) = H \cap Z(G) \neq 1.$$

□

Corolário 1.5.2. *Seja G um grupo com $|G| = p^m$, então:*

1) Existe uma cadeia $1 = G_0 < G_1 < \ldots < G_m = G$, com $G_i \trianglelefteq G$ e $|G_i| = p^i$ para $i \in \{0, 1, \ldots, m\}$.

2) Se $H < G$, então existe $K \leq G$ tal que $H < K$ e $|K : H| = p$.

Demonstração. 1) Seja H subgrupo maximal de G, pelo item (iii) do Teorema anterior $H \trianglelefteq G$, pois $H < N_G(H)$. Agora, pelo item (iv) do Teorema anterior $H \cap Z(G) \neq 1$ e portanto $Z(G) \neq 1$. Tome $z \in Z(G)$ e então $o(z) = p^k$.
Se $k = 1$ temos que $G_1 = \langle z \rangle$ é normal em G com $|\langle z \rangle| = p$.
Se $k \neq 1$, então $w = z^{p^{k-1}} \in Z(G)$ e $o(w) = p$, portanto $\langle w \rangle \trianglelefteq G$ com $|\langle w \rangle| = p$. Desta forma podemos trocar w por z de modo que $N = \langle z \rangle$ é normal com $|N| = p$. Portanto $\overline{G} = \dfrac{G}{N}$ tem ordem p^{m-1} e por indução existe uma cadeia $\overline{1} = \overline{G_0} < \overline{G_1} < \ldots < \overline{G_m} = \overline{G}$, com $\overline{G_i} \trianglelefteq G$ e $|G_i| = p^i$. Pelo Teorema da Correspondência $\overline{G_i} = \dfrac{G_{i+1}}{N}$, onde $G_{i+1} \trianglelefteq G$ e $|G_{i+1}| = |G_i||N| = p^{i+1}$.
2) Se $m = 1$, então $H = 1$ e $K = G$. Suponha $m > 1$, de modo análogo ao item (1) $Z(G) \neq 1$ e existe $z \in Z(G)$ tal que $o(z) = p$. Assim, temos duas possibilidades:
i) $z \in H$, então $\dfrac{H}{\langle z \rangle} < \dfrac{G}{\langle z \rangle}$, onde $\dfrac{H}{\langle z \rangle}$ tem ordem p^{m-1}. Por indução existe $\overline{K} \leq G$ tal que $\dfrac{H}{\langle z \rangle} < \overline{K}$ e $|\overline{K} : \overline{H}| = p$. Pelo Teorema da Correspondência $\overline{K} = \dfrac{K}{\langle z \rangle}$, onde $H \leq K$ e $|K : H| = p$.
ii) $z \in H$. Seja $K = \langle z \rangle H$. Então $K \leq G$, pois $\langle z \rangle \trianglelefteq G$, $H < K$ e

$$|K| = \frac{|H||\langle z \rangle|}{|H \cap \langle z \rangle|} = p|H|.$$

Portanto, $|K : H| = p$. □

1.6 Teoremas de Sylow

Seja G um grupo, um subgrupo H de G é dito ser um p-subgrupo de Sylow de G se existe um número primo p tal que todo elemento $x \in H$ tem ordem p^α, onde $\alpha \geq 0$ depende do elemento x. Escreveremos $H \in Syl_p(G)$ para dizer que H é um p-subgrupo de Sylow de G.

Teorema 1.6.1 (**Primeiro Teorema de Sylow**). *Seja G um grupo finito com $|G| = p^m r$, onde p é primo com $(p, r) = 1$ e $m \geq 1$. Então, existe $H \leq G$ tal que $|H| = p^m$.*

Demonstração. Sejam $X = \{U \subseteq G;\ |U| = p^m\}$ e $\varphi :\ G \longrightarrow S_X$ dada por $\varphi_g(U) = gU$. É fácil ver que φ é uma ação e

$$|X| = \binom{p^m r}{p^m} = \frac{p^m r!}{p^m!(p^m r - p^m)!} = \frac{p^m r}{p^m}\frac{p^m r - 1}{p^m - 1}\cdots\frac{p^m r - (p^m - 1)}{p^m - (p^m - 1)}.$$

Para cada $1 \leq j \leq p^m - 1$, escreva $j = p^k q$, onde $p \nmid q$. Então,

$$\frac{p^m r - j}{p^m - i} = \frac{p^m r - p^k q}{p^m - p^k q} = \frac{p^{m-k} r - q}{p^{m-k} - q},$$

onde $p \nmid p^{m-k} r - q$ e também não divide $p^{m-k} - q$. Portanto, p não divide $|X|$ e como $X = \mathcal{O}_{V_1} \cup \ldots \mathcal{O}_{V_s}$ seque que $p \nmid |\mathcal{O}_V|$ para algum V. Agora, $p \nmid |\mathcal{O}_V| = |G : E_V|$ e $p^m \mid |G| = |G : E_V||E_V|$. Portanto, $p^m \mid |E_V|$ e assim $p^m \leq |E_V|$, onde $E_V = \{g \in G;\ gV = V\}$. Tome $x \in V$ e defina $\theta :\ E_V \longrightarrow V$ por $\theta(w) = wx$. Então θ é bem definida, pois $hV = V$, e injetiva. Daí, $|E_V| \leq p^m$ e portanto $|E_V| = p^m$. □

Corolário 1.6.1. *Se G é um grupo finito com $|G| = p^m r$, onde p é primo com $(p, r) = 1$ e $m \geq 1$, então para cada $i \in \{1, 2, \ldots, m\}$ existe H_i tal que $|H_i| = p^i$.*

Demonstração. Pelo primeiro Teorema de Sylow, existe $H \leq G$ tal que $|H| = p^m$ e pelo Corolário 1.5.2 existe $H_i \leq H$ tal que $|H_i| = p^i$. □

Corolário 1.6.2 (**Segundo Teorema de Sylow**). *Nas condições do primeiro Teorema de Sylow, se H e J são subgrupos de G com $|H| = |J| = p^m$, então existe $g \in G$ tal que $H = J^g$.*

Demonstração. Segue diretamente do item (ii) do Teorema 1.5.1. □

Teorema 1.6.2 (**Terceiro Teorema de Sylow**). *Nas condições do primeiro Teorema de Sylow, se* $n_p = |\{H \leq G;\ |H| = p^m\}|$, *então* $n_p = |G : N_G(H)|$, *onde* $H \leq G$ *com* $|H| = p^m$, *e* $n_p \equiv 1\ (mod\ p)$. *Note que* $n_p = |G : N_G(H)|$ *implica que* $n_p \mid |G : H| = r$.

Corolário 1.6.3 (**Argumento de Fratini**). *Sejam* G *um grupo,* $N \trianglelefteq G$ *e* $P \in Syl_p(N)$. *Então,* $G = NN_G(P)$.

Demonstração. É claro que $G \supseteq NN_G(P)$. Se $g \in G$, então $P^g \subseteq N^g = N$. Logo, $P, P^g \in Syl_p(N)$ e assim, pelo segundo Teorema de Sylow P e P^g são conjugados em N, isto é, existe $x \in N$ tal que $P^x = P^g$. Logo, $P = P^{gx^{-1}}$ e portanto $gx^{-1} \in N_G(N) \Longrightarrow g = (gx^{-1})x \in N_G(P)N = NN_G(P)$. Assim, $G \subseteq NN_G(P)$ e daí temos a igualdade $G = NN_G(P)$. □

1.7 Produto Direto e Produto Semidireto

1.7.1 Produto Direto

Dados dois grupos H e K podemos contruir outro grupo chamado produto direto de H por K e denotado por $H \times K$ com o seguinte operação: $(h_1, k_1) \odot (h_2, k_2) = (h_1h_2, k_1k_2)$. É fácil verificar que $H \times K$ munido desta operação satisfaz os axiomas de grupo e claramente temos subgrupos $H^* = \{(h, 1);\ h \in H\}$ e $K^* = \{(1, k);\ k \in K\}$ que são respectivamente isomorfos aos grupo H e K.

Proposição 1.7.1. *Os subgrupos* H^* *e* K^* *são subgrupos normais de* $H \times K$ *com* $H \times K = H^*K^*$ *e* $H^* \cap K^* = 1$.

Demonstração. Dado $(h, k) \in H \times K$ temos que $(h, k)^{-1}H^*(h, k) = \{(h, k)^{-1}(h', 1)(h, k);\ h' \in H\} = \{(h^{-1}h'h, 1);\ h' \in H\} = H^*$. Logo, H^* é subgrupo normal de $H \times K$. De modo análogo, provamos que K^* é subgrupo normal de $H \times K$. É claro que $H \times K = H^*K^*$ e $H^* \cap K^* = 1$. □

Desta forma provamos que se $G = H \times K$, existem subgrupos normais H^* e K^* isomorfos a H e K respectivamente com $G = H^*K^*$ e $H^* \cap K^* = 1$. Provaremos agora que vale a recíproca conforme segue.

Proposição 1.7.2. *Seja G um grupo tal que H e K são subgrupos normais de G com $G = HK$ e $H \cap K = 1$. Então, $G \simeq H \times K$.*

Demonstração. Defina $\varphi : H \times K \longrightarrow G$ por $\varphi[(h,k)] = hk$. Como $h^{-1}k^{-1}hk \in H \cap K = 1$, temos que φ é uma aplicação bem definida.

• φ é homomorfismo. Primeiro vejamos que os elementos de H comutam com o elementos de K. De fato, como $G = HK = KH$, temos que $hk = k'h'$ e assim, $hkh^{-1} = k'h'h^{-1} \in K$. Portanto, $h = h'$ e consequentemente $k' = k$. Agora,

$$\varphi[(h_1,k_1)(h_2,k_2)] = \varphi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \varphi[(h_1,k_1)]\varphi(h_2,k_2)].$$

• É claro que φ é sobrejetiva.

• φ é injetiva.

$$\varphi[(h_1,k_1)] = \varphi[(h_2,k_2)] \Longleftrightarrow h_1k_1 = h_2k_2 \Longleftrightarrow h_2^{-1}h_1 = k_2k_1^{-1},$$

mas $h_2^{-1}h_1 \in H$ e $k_2k_1^{-1} \in K$. Portanto, $h_2^{-1}h_1$ e $k_2k_1^{-1}$ pertencem a $H \cap K$. Logo, $h_1 = h_2$ e $k_1 = k_2$.

Isto prova que φ é isomorfismo.

□

Exemplo 6. *Sejam $\langle a \rangle$ e $\langle b \rangle$ grupos cíclico com ordens relativamente primas. Então $\langle a \rangle \times \langle b \rangle$ é cíclico.*

Demonstração. Podemos mostrar sem muita deficuldade que $|\langle a \rangle \times \langle b \rangle| = |\langle a \rangle||\langle b \rangle|$. Deste modo basta mostrar que o elemento $ab := (a,b) \in \langle a \rangle \times \langle b \rangle$ tem ordem igual a $|\langle a \rangle||\langle b \rangle| = o(a)o(b)$.

De fato, $(ab)^{o(a)o(b)} = (a^{o(a)o(b)}, b^{o(a)o(b)}) = 1$. Logo, $o(ab) \mid o(a)o(b)$ e como $(o(a), o(b)) = 1$ concluímos que $o(ab) = o(a)o(b)$ e portanto $\langle a \rangle \times \langle b \rangle = \langle ab \rangle$. □

1.7.2 Produto Semidireto

Suponha agora que $G = NH$, onde $N \trianglelefteq G$, $H \leq G$ e $N \cap H = \{1\}$. Neste caso dizemos que G é o produto semidireto de N por H e denotamos $G = N \rtimes H$.

Proposição 1.7.3. *Seja $G = N \rtimes H$, então:*

i) $\dfrac{G}{N} \simeq H$;

ii) $N \cap N_G(H) = C_N(H)$;

iii) Todo $g \in G$ tem uma única decomposição da forma $g = nh$, onde $n \in N$ e $h \in H$;

iv) $\theta : H \longrightarrow AutN$ *dada por* $\theta_h(n) = hnh^{-1}$ *é homomorfismo tal que* $nhn_1h_1 = n\theta_h(n_1)hh_1$.

Demonstração. i) Segue diretamente do segundo Teorema do Isomorfismo.

ii) É claro que $C_N(H) \leq N \cap N_G(H)$. Tome $g \in N \cap N_G(H)$ e $h \in H$, então $g^{-1}h^{-1}gh \in H \cap N = \{1\}$. Logo, $gh = hg$ e portanto $N \cap N_G(H) = C_N(H)$.

iii) Suponha que $g = nh = n_1h_1$. Então, $n_1^{-1}n = h_1h^{-1} \in N \cap H = \{1\}$. Portanto, $h = h_1$ e $n = n_1$.

iv) Basta verificar que a operação acima é bem definica e que G munido desta operação satisfaz os axiomas de grupo. Já a prova de que $N \simeq N^*$, $H \simeq H^*$, $H^* \cap N^* = \{1\}$ e claro que $G = N^*H^H$. □

A próxima Proposição nos garante que vale a recíproca, conforme segue.

Proposição 1.7.4. *Suponha que H e N são grupos e seja $\theta : H \longrightarrow AutN$ um homomorfismo. Então $G = \{(n,h);\ n \in N,\ h \in H\}$ munido da operação $(n,h)(n_1,h_1) = (n\theta(h)(n_1), hh_1)$ é um grupo com $N \simeq N^* \trianglelefteq G$, $H \simeq H^* \leq G$, $H^* \cap N^* = 1$ e $G = N^*H^*$. Neste caso, para explicitar o homomorfismo θ, denotamos $G = N \rtimes_\theta H$.*

Demonstração. É claro que a operação θ é bem definida.

Associatividade:

$$((n,h)(n_1,h_1))(n_2,h_2) = (n\theta(h)(n_1), hh_1)(n_2,h_2)$$

$$= (n\theta(h)(n_1)\theta(hh_1)(n_2), hh_1h_2)$$

e

$$(n,h)((n_1,h_1)(n_2,h_1)) = (n,h)(n_1\theta(h_1)(n_2),h_1h_2)$$

$$= (n\theta(h)(n_1)\theta(hh_1)(n_2),hh_1h_2).$$

Logo, $((n,h)(n_1,h_1))(n_2,h_2) = (n,h)((n_1,h_1)(n_2,h_1))$.

Elemento Neutro:

$$(1,1)(n,h) = (1\theta(1)(n),1h) = (n,h)$$

e

$$(n,h)(1,1) = (n\theta(h)(1),h1) = (n,h).$$

Elemento inverso: Dado $(n,h) \in G$ temos

$$(\theta(h^{-1)})n^{-1}),h^{-1})(n,h) = (\theta(h^{-1}(n^{-1})\theta(h)(n),h) = (1,1)$$

e

$$(n,h)(\theta(h^{-1})n^{-1},h^{-1}) = (n\theta(\theta(h^{-1})n^{-1},hh^{-1})$$

$$= (n\theta(1)(n^{-1}),1) = (nn^{-1},1) = (1,1).$$

Portanto G é um grupo. Para finalizar, mostraremos que $N^* \trianglelefteq G$, $H^* \leq G$, $G = N^*H^*$ e $N^* \cap H^* = 1$.

Afirmação: $N^* \trianglelefteq G$.

• É claro que $(1,1) \in N^*$;

• Dado $(n,1) \in N^*$ temos que $(n,1)^{-1} = (\theta(1)(n^{-1}),1) = (n^{-1},1) \in N^*$

• Dados $(n,1),(n_1,1) \in N^*$ temos que $(n,1)(n_1,1) = (n\theta(1)(n_1),1) = (nn_1,1) \in N^*$.

Com isto provamos que $N \leq G$.

• Dados $(n,1) \in N^*$ e $(m,h) \in G$ temos

$$(m,h)^{-1}(n,1)(m,h) = (\theta(h^{-1})(m^{-1}),h^{-1}(n,1)(m,h)$$

$$= (\theta(h^{-1})(m^{-1}),h^{-1})(n\theta(1)(m),h) = (\theta(h^{-1})(m^{-1}),h^{-1})(nm,h)$$

$$(\theta(h^{-1})(m^{-1})\theta(h^{-1})(nm),1) = (\theta(h^{-1})(m^{-1}nm),1) \in N^*,$$

visto que $\theta(h^{-1})(m^{-1}nm) \in N$.

De modo análogo provamos que $H^* \leq G$, claramente temos $G = N^*H^*$ e $N^* \cap H^* = 1$. $\square$

Capítulo 2

Preliminares

Neste capítulo estudaremos vários resultados que normalmente não são vistos em cursos introdutórios de teoria dos grupos.

2.1 Séries Normais e Subnormais

Uma **Série** (S) é uma sequência de subgrupos G_i de G tais que:

$$(S) : 1 = G_0 \leq G_1 \leq \cdots \leq G_n = G.$$

Dizemos que (S) é **Subnormal** se $G_i \trianglelefteq G_{i+1}$, (S) é **Normal** se $G_i \trianglelefteq G$. Observe que toda série normal é subnormal. Um **Refinamento** de uma série (S) é uma série (T): $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G.$, onde cada G_i é termo da série (S). Dizemos que (S) é uma **Série de Composição** se (S) não tem refinamento próprio. Um subgrupo N de um grupo G é dito ser **Normal Minimal** se: $1 \neq N \triangleleft G$, e não existe K com $1 < K \leq N$ e $K \trianglelefteq G$. Notação: $N \cdot\triangleleft G$. Uma série (S) é dita ser uma **Série Principal** se $\frac{G_{i+1}}{G_i} \cdot\triangleleft \frac{G}{G_i}$.

Exemplo 7. *Sejam* $G = A_4$, $H = \{1, (12)(34)\}$ *e* $V = \{1, (12)(34), (13)(24), (14)(23)\}$.

$$(S) : \ 1 \trianglelefteq V \trianglelefteq A_4;$$

$$(T) : \ 1 \trianglelefteq H \trianglelefteq V \trianglelefteq A_4.$$

Então (T) é uma série de composição que refina (S) : $V \cdot \lhd A_4$ e (S) é uma série pricipal que não é de composição.

Proposição 2.1.1. *i) (S) é serie de composição se e somente se $\frac{G_{i+1}}{G_i}$ é simples;*

ii) Todo grupo finito tem uma série de composição;

Demonstração. i) Suponha que $\frac{G_{i+1}}{G_i}$ é não simples. Então existe um subgrupo próprio $\overline{H} = \frac{H}{G_i} \trianglelefteq \frac{G_{i+1}}{G_i}$ e desta forma pelo Teorema da correspondência temos $G_i \trianglelefteq H \trianglelefteq G_{i+1}$ e portanto (S) tem um refinamento próprio, que é uma contradição. Logo, $\frac{G_{i+1}}{G_i}$ é simples. Suponha que $\frac{G_{i+1}}{G_i}$ é simples. Então é claro que (S) não tem refinamento próprio.
ii) Seja G um grupo finito. Se G é simples, então G tem uma série de composição dada por $1 \trianglelefteq G$. Suponha G não simples e seja $G_1 \cdot \lhd G$, se $\frac{G}{G_1}$ é simples o resultado está demonstrado, caso contrário por indução existe uma série de composição $(S) : \overline{1} \trianglelefteq \overline{G_2} \trianglelefteq \ldots \trianglelefteq \overline{G_n} = \overline{G}$ e pelo Teorema da Correnpondência obtemos uma série (S') dada por $1 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G$ que é de composição. □

2.2 Comutadores

Sejam G um grupo e $x_1, x_2, \ldots, x_n \in G$. Definimos e denotamos o comutador de x_1 por x_2 da seguinde forma:

$$[x_1, x_2] = x_1^{-1} x_2^{-1} x_1 x_2.$$

O comutador de n elementos , $n > 2$, é definido por $[x_1, x_2, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$. A próxima Proposição nos dará uma serie de propriedades sobre os comutadores.

Proposição 2.2.1. *Sejam $x, y, z, t \in G$. Então:*

i) $[x, y] = 1$ se e somente se $xy = yx$;

ii) $[x, y]^{-1} = [y, x]$;

iii) $[x, y]^z = [x^z, y^z]$;

iv) $[xy, z] = [x, z]^y [y, z]$;

v) $[x, yz] = [x, z][x, y]^z$;

vi) $[x, y^{-1}] = ([x, y]^{y^{-1}})^{-1}$ *e* $[x^{-1}, y] = ([x, y]^{x^{-1}})^{-1}$;

vii) Se $[x, y]$ *comuta com* x *e* y*, então* $[x^n, y] = [x, y^n] = [x, y]^n$ *para* $n \in \mathbb{Z}$;

viii) Nas condições de (vii) vale $(xy)^n = [x, y]^{\frac{n(n-1)}{2}} x^n y^n$ *para todo inteiro* $n \geq 1$;

ix) $[x, y]z = x[x^z, y^z]$;

x) $[x^y, z] = [x, z]^{[x,z]}[x, y, z]$;

xi) $[x^{yz}, t] = [x^y, t]^{[x^y,z]}[x^y, z, t]$;

xii) $[xy, z] = [x, z][x, z, y][y, z]$;

xiii) $[x, yz] = [x, z][x, y][x, y, z]$;

xiv) $[x, y, z] = [x, y]^{-1}[x, y]^z$;

xv) Se $\varphi : G \longrightarrow G$ *é um homomorfismo então,* $[\varphi(x), \varphi(y)] = \varphi([x, y])$;

*xvi) (**Identidade de Holl-Witt**)* $[x, y^{-1}, z][y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$.

Demonstração. A prova deste resultado segue diretamente da definição. □

Definição 13. *Sejam* $X \subseteq G$ *e* $Y \leq G$*, definimos os seguintes subgrupos:*

i) $X^Y = \langle x^y;\ x \in X,\ y \in Y \rangle$;

ii) $[X, Y] = \langle [x, y];\ x \in X,\ y \in Y \rangle$.

Proposição 2.2.2. *Seja* $X, Y, K \leq G$*. Então:*

i) $X^K \trianglelefteq \langle X, K \rangle$;

ii) $X^K = \langle X, [X, K] \rangle$;

iii) $[X, K]^K = [X, K]$;

iv) Se $K = \langle Y \rangle$*, então* $[X, K] = [X, Y]^K$.

Demonstração. i) Como $X \leq X^K$, temos que $X \leq N_G(X^K)$. Agora, dados $x^k \in X^K$ e $k_1 \in K$ temos: $(x^k)^{k_1} = x^{kk_1} \in X^K$. Logo, $K \leq N_G(X^K)$ e daí concluímos que $X^K \trianglelefteq \langle X, K \rangle$.

ii) Como $[x, k] = \ x_{-1}k^{-1}xk = x^{-1}x^k$ temos que $x^k \in \langle X, [X, K] \rangle$ e portanto $X^K \leq \langle X, [X, K] \rangle$. Reciprocamente, $X \leq X^K$ e $[x, k] = x^{-1}x^k \in X^K$. Daí, $X^K = \langle X, [X, K] \rangle$.

iii) É claro que $[X, K] \leq [X, K]^K$. Agora, pela propriedade (v) de comutadores temos que: $[x, kk_1] = [x, k_1][x, k]^{k_1}$ e portanto, $[x, k]^{k_1} = [x, k_1]^{-1}$

$[x, kk_1] \in [X, K]$. Logo, $[X, K]^K = [X, K]$.

iv) Como $Y \subseteq K$ temos que $[X,K] = [X,K]^K \supseteq [X,Y]^K$. Assim, basta mostrar a inclusão contrária. Sejam $x \in X$ e $k \in K$. Então $k = y_1^{e_1} y_2^{e_2} \dots y_l^{e_r}$, onde $y_j \in Y$ e $e_j = \pm 1$. Desta forma temos que

$$[x,k] = [x, y_1^{e_1} y_2^{e_2} \dots y_r^{e_r}] = [x, y_r^{e_r}][x, y_1^{e_1} y_2^{e_2} \dots y_r^{e_{r-1}}]^{y_r^{e_r}}.$$

• Se $l = 1$, então $[x,k] = [y, y^e] = [x,y]$ ou $[x,k] = [y,y^e] = [x, y^{-1}] = [x,y]^{y^{-1}}$. Com isto concluímos que $[x,y] \in [X,Y]^K$.

Agora, por indução $[x, [x, y_1^{e_1} y_2^{e_2} \dots y_r^{e_{r-1}}]] \in [X,Y]^K$ e também $[x, y_r^{e_r}] \in [X,Y]^K$. Portanto, $[x,k] \in [X,Y]^K$. Logo, $[X,K] = [X,Y]^K$. □

Proposição 2.2.3. *Sejam $H, K, N \leq G$. Então:*

i) $[H,K] = [K,H] \trianglelefteq \langle H,K \rangle$, em particular $[H,G] \trianglelefteq G$;

ii) Se $N \trianglelefteq G$, então $\dfrac{G}{N}$ é abeliano se e somente se $G' = [G,G] \leq N$;

iii) $[H,K] \leq H$ se e somente se $K \leq N_G(H)$. Em particular, se $H \trianglelefteq G$, então $[H,G] \leq H$;

iv) Se $H \trianglelefteq G$, $K \trianglelefteq G$ e $N \trianglelefteq G$, então $[HK, N] = [H,N][K,N]$;

v) Se $H \trianglelefteq G$, $K \trianglelefteq G$ e $H \leq K$, então $\dfrac{K}{H} \leq Z\left(\dfrac{G}{H}\right)$ se e somente se $[G,K] \leq H$;

vi) Se $N \trianglelefteq G$ e $N \leq H$, então $\left[\dfrac{G}{N}, \dfrac{H}{N}\right] = \dfrac{[G,H]N}{N}$.

Demonstração. i) $[H,K] = \langle [h,k];\ h \in H,\ k \in K \rangle = \langle [k,h]^{-1};\ k \in K,\ h \in H \rangle \leq [K,H]$. Analogamente, $[K,H] = \langle [k,h];\ k \in K,\ h \in H \rangle = \langle [h,k]^{-1};\ h \in H,\ k \in K \rangle \leq [H,K]$, portanto $[H,K] = [K,H]$. Como pelo item (*iii*) da Proposição anterior $[H,K]^K = [H,K]$ temos que $K \leq N_H([H,K])$ e também $[K,H]^H = [K,H]$. Logo $H \leq N_G([K,H]) = N_G([H,K])$. Assim, $[H,K] = [K,H] \trianglelefteq \langle H,K \rangle$.

ii) Suponha $\dfrac{G}{N}$ abeliano, então $[x,y]N = (x^{-1}y^{-1}xy)N = N$. Daí, $[x,y] \in N$ para todos $x, y \in G$. Logo, $G' \leq N$.

Reciprocamente, se $G' \leq N$ então $[x,y]N = N$ e portanto $xyN = yxN$. Logo, $\dfrac{G}{N}$ é abeliano.

iii) Suponha que $[H,K] \leq H$, então $[K,H] = [H,K] \leq H$. Portanto, $k^{-1}h^{-1}kh \leq H\ \forall k \in K$ e $h \in H$. Logo, $k^{-1}h^{-1}k \in H$ e assim, $K \leq N_G(H)$.

Reciprocamente, suponha que $K \leq N_G(H)$. Então $k^{-1}h^{-1}k \in H\ \forall k \in K$. Logo, $k^{-1}h^{-1}kh \in H$ e daí, $[K,H] = [H,K] \leq H$. Em particular, se $H \trianglelefteq G$, então $[H,G] \leq H$.

iv) Como $[H,N],[K,N] \leq [HK,N]$ temos que $[H,N][K,N] \leq [HK,N]$. Agora, $[hk,n] = [h,n]^k[k,n] = [h^k,n^k][k,n] = [h',n'][k,n] \in [H,N][K,N]$, pois $H, N \trianglelefteq G$. Logo, $[HK,N] = [H,N][K,N]$.

v) Suponha que $\dfrac{K}{H} \leq Z\left(\dfrac{G}{H}\right)$. Então, $[g,k] = g^{-1}k^{-1}gk \in K$, pois $K \trianglelefteq G$, e $(g^{-1}k^{-1}gk)H = (g^{-1}H)(k^{-1}H)(gH)(kH) = H$, pois $kH, k^{-1}H \in \dfrac{K}{H} \leq Z\left(\dfrac{G}{H}\right)$. Logo, $[g,k] \leq H$ e com isto provamos que $[G,K] \leq H$.

Suponha agora que $[G,H] \leq H$, então

$$(g^{-1}k^{-1}gk)H = (g^{-1}H)(k^{-1}H)(gH)(kH) = H.$$

Logo, $(gH)(kH) = (kH)(gH)\ \forall k \in K$ e $g \in G$. Portanto $\dfrac{K}{H} \leq Z\left(\dfrac{G}{H}\right)$.

vi) $\left[\dfrac{G}{N}, \dfrac{H}{N}\right] = \langle [gN,hN];\ g \in G,\ h \in H\rangle$, mas

$$[gN,hN] = g^{-1}Nh^{-1}NgNhN = (g^{-1}h^{-1}gh)N = [g,h]N.$$

Por outro lado, $\dfrac{[G,H]N}{N} = \{xN;\ x \in [G,H]\}$. Assim, $\left[\dfrac{G}{N}, \dfrac{H}{N}\right] \leq \dfrac{[G,H]N}{N}$. Agora, se $xN \in \dfrac{[G,H]N}{N}$, então $x = [g_1,h_1]^{e_1} \ldots [g_n,h_n]^{e_n}$ e portanto

$$xN = ([g_1,h_1]N)^{e_1} \ldots ([g_n,h_n]N)^{e_n} \in \langle [g,h]N\rangle = \left[\frac{G}{N}, \frac{H}{N}\right].$$

□

2.3 Solubilidade e Nilpotência

Um grupo G é dito ser **Solúvel** se existe uma série subnormal

$$(S):\ 1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$$

com $\dfrac{G_{i+1}}{G_i}$ abeliano. Dizemos que G é **Supersolúvel** se existe uma série (S) com $G_i \trianglelefteq G$ e $\dfrac{G_{i+1}}{G_i}$ cíclico. G é **Nilpotente** se existe uma série central (S), isto é, $G_i \trianglelefteq G$ e $\dfrac{G_{i+1}}{G_i} \leq Z\left(\dfrac{G}{G_i}\right)$, ou seja $[G_{i+1},G] \leq G_i$.

Observação 8. • *Todo grupo nilpotente é solúvel;*

• *Todo grupo supersolúvel é solúvel;*

• S_3 *é supersolúvel e não é nilpotente, pois*

$$1 \trianglelefteq \langle(123)\rangle \trianglelefteq S_3$$

é tal que $\frac{\langle(123)\rangle}{1}$ *e* $\frac{S_3}{\langle(123)\rangle}$ *são cíclicos. Portanto* S_3 *é supersolúvel e consequentemente* S_3 *é solúvel. Agora, como* $Z(S_3) = 1$ *não existe uma série central para* S_3 *e assim,* S_3 *é não nilpotente.*

Proposição 2.3.1. *G é solúvel se e somente se existe $n \geq 0$ tal que $G^{(n)} = 1$, onde $G^{(0)} = G$, $G^{(1)} = G'$ e $G^{(n)} = (G^{(n-1)})'$.*

Demonstração. Suponha que G é Solúvel. Então existe uma série

$$(S) : = 1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$$

com $\frac{G_{i+1}}{G_i}$ abeliano.
Afirmação: $G^{(i)} \leq G_{n-i}$ $\forall 0 \leq i \leq n$.

Para $i = 0$ temos $G^{(0)} = G = G_n = G_{n-0}$. Suponha que $G^{(i)} \leq G^{(n-i)}$. Então como $\frac{G_{n-i}}{G_{n-(i+1)}}$ é abeliano, pelo item (ii) da Proposição 2.2.3, $(G_{n-i})' \leq G_{n-(i+1)}$. Agora, como $G^{(i)} \leq G_{n-i}$ temos que $G^{(i+1)} = (G^{(i)})' \leq (G_{n-i})' \leq G_{n-(i+1)}$. Assim como $G_0 = 1$ concluímos que $G^{(n)} = G_{n-n} = 1$.

Suponha agora que existe $n \geq 0$ tal que $G^{(n)} = 1$. Então como $G^{(n+1)} \trianglelefteq G^{(n)}$ temos a série $1 = G^{(n)} \trianglelefteq \ldots \trianglelefteq G^{(0)} = G$ subnormal com $\frac{G^{(i-1)}}{G^{(i)}}$ abeliano, tendo em vista que fazendo $N = G'$ no item (ii) da Proposição 2.2.3 obtemos que $\frac{G}{G'}$ é abeliano. Portanto, G é solúvel. □

Corolário 2.3.1. *Seja G um grupo solúvel. Então todo subgrupo de G é solúvel.*

Demonstração. Suponha que $H \leq G$. Então $H^{(n)} \leq G^{(n)}$, deste modo H é solúvel. □

Corolário 2.3.2. *Se G é um grupo solúvel e $N \trianglelefteq G$, então $\frac{G}{N}$ é solúvel.*

Demonstração. Pelo item (vi) da Proposição 2.2.3 temos:

$$\left(\frac{G}{N}\right)' = \left[\frac{G}{N}, \frac{G}{N}\right] = \frac{[G,G]N}{N} = \frac{G'N}{N}.$$

Suponha por indução que que $\left(\frac{G}{N}\right)^{(n)} = \frac{G^{(n)}N}{N}$. Novamente, pelo item (vi) da Proposição 2.2.3, obtemos

$$\left(\frac{G}{N}\right)^{(n+1)} = \left[\frac{G^{(n)}N}{N}, \frac{G^{(n)}N}{N}\right] = \frac{[G^{(n)}N, G^{(n)}N]N}{N}$$

$$= \frac{[G^{(n)}, G^{(n)}][G^{(n)}, N][N, G^{(n)}][N, N]N}{N},$$

mas como $[G^{(n)}, N], [N, G^{(n)}], [N, N] \leq N$ concluímos que

$$\left(\frac{G}{N}\right)^{(n+1)} = \frac{G^{(n+1)}N}{N}.$$

Daí, como existe $n \geq 0$ tal que $G^{(n)} = 1$ temos,

$$\left(\frac{G}{N}\right)^{(n)} = \frac{G^{(n)}N}{N} = \frac{N}{N}.$$

Portanto $\frac{G}{N}$ é solúvel. □

Corolário 2.3.3. *Seja $N \trianglelefteq G$ com N, $\frac{G}{N}$ solúveis, então G é solúvel.*

Demonstração. Sabemos que existem $n, m \geq 0$ tais que $N^{(n)} = 1$ e $\left(\frac{G}{N}\right)^{(m)} = \frac{N}{N}$. Mas como feito no Corolário anterior, $\left(\frac{G}{N}\right)^{(m)} = \frac{G^{(m)}N}{N} = \frac{N}{N}$. Logo, $G^m \leq N$ e assim $(G^{(m)})^{(n)} \leq N^{(n)} = 1$. Portanto, G é solúvel. □

Definição 14 (Série Central Inferior). *Seja G um grupo e considere $\Gamma_1(G) = G$ definimos*

$$\Gamma_n(G) = [\Gamma_{n-1}(G), G], \quad n \geq 2.$$

Observação 9. • *$\Gamma_n(G) \trianglelefteq G$ para $n \geq 1$;*
• *$\frac{\Gamma_n(G)}{\Gamma_{n+1}(G)} \leq Z\left(\frac{G}{\Gamma_{n+1}(G)}\right)$, tendo em vista que $\Gamma_{n+1}(G) = [\Gamma_n(G), G] \trianglelefteq \Gamma_n(G)$, pois $\Gamma_{n+1} \trianglelefteq G$.*

Definição 15. *Considere $Z_0(G) = 1$, o Teorema da Correpondência nos permite definir $Z_n(G)$ como o subgrupo que satisfaz a seguinte igualdade:*

$$Z\left(\frac{G}{Z_{n-1}(G)}\right) = \frac{Z_n(G)}{Z_{n-1}(G)}.$$

Observação 10. *$Z_n \leq Z_{n+1}$ e como $Z\left(\frac{G}{Z_{n-1}(G)}\right) \trianglelefteq \frac{G}{Z_{n-1}(G)}$, então $Z_n \trianglelefteq G$*

Proposição 2.3.2. *Seja G nilpotente e $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ uma série central, isto é, $\frac{G_{i+1}}{G_i} \leq Z\left(\frac{G}{G_i}\right)$. Então,*

i) $\Gamma_i(G) \leq G_{n-i+1},\ \forall i \in \{1, 2, \ldots, n\}$;

ii) $G_i \leq Z_i(G),\ \forall i \in \{0, 1, \ldots, n\}$;

Demonstração. Confira 5.19 de [8]. □

Definimos a **Classe de Nilpotência** de um grupo G como o comprimento da série central inferior que é igual ao comprimento da série central superior e denotamos este comprimento por $Cl(G)$. Denotaremos por N_c o conjunto de todos os grupos com $Cl(G) \leq c$.

Observação 11. *Se G é um grupo abeliano, então $Cl(G) = 1$.*

Proposição 2.3.3. *Seja G um grupo. Então valem:*

i) Se $N \trianglelefteq G$ e $\frac{G}{N}$ é nilpotente, então G é nilpotente;

ii) $G \in N_c$ se e somente se $\frac{G}{Z(G)} \in N_{c-1}$;

iii) Se G é nilpotente e $N \trianglelefteq G$, então $N \cap Z(G) \neq 1$;

iv) Se $|G| = p^n$, então G é nilpotente;

v) Se G é nilpotente e $H \leq G$, então H é subnormal, isto é, existem $H_1, H_2, \ldots, H_n \leq G$ tais que $H \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$;

vi) Se G é finito, então G é nilpotente se e somente se todo fator pricipal é central.

Demonstração. i) Como $\frac{G}{N}$ é nilpotente existe uma série central

$$\frac{N}{N} \trianglelefteq \frac{H_1}{N} \trianglelefteq \ldots \trianglelefteq \frac{G}{N}.$$

Isto é, $\left[\frac{H_{i+1}}{N}, \frac{G}{N}\right] \leq \frac{H_i}{N}$. Portanto $\frac{[H_{i+1}, G]N}{N} \leq \frac{H_i}{N}$ e daí, $[H_{i+1}, G] \leq H_i$. Logo, a série

$$1 \trianglelefteq N \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq G$$

é central e com isto G é nilpotente.

ii) ($\Longrightarrow$) Como $G \in N_c$ temos que $Z_c(G) = G$ e assim,

$$Z_{c-1}\left(\frac{G}{Z_c(G)}\right) = \frac{Z_{c-1+1}(G)}{Z(G)} = \frac{Z_c(G)}{Z(G)} = \frac{G}{Z(G)}.$$

Portanto, $\frac{G}{Z(G)} \in N_{c-1}$.

($\Longleftarrow$) Agora temos que

$$Z_{c-1}\left(\frac{G}{Z(G)}\right) = \frac{G}{Z(G)}.$$

Logo,

$$Z_{c-1}\left(\frac{G}{Z(G)}\right) = \frac{Z_c(G)}{Z(G)} = \frac{G}{Z(G)}.$$

Portanto, $G \in N_c$.

iii) Considere a série $1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \ldots \trianglelefteq Z_n(G) = G$. Então existe $r \in \{1, 2, \ldots, n\}$ tal que $N \cap Z_r(G) \neq 1$ e $N \cap Z_{r-1}(G) = 1$. Deste modo $[N \cap Z_r(G), G] \leq Z_{r-1}(G) \cap N$, pois $N \trianglelefteq G$ e $[Z_r(G), G] \leq Z_{r-1}(G)$ por definição. Portanto, $[N \cap Z_r(G), G] = 1$ e daí, $1 \neq N \cap Z_r(G) \leq Z(G)$.

iv) Pelo item (1) do Corolário 1.5.2, para cada $i \in \{1, 2, \ldots, n\}$ existe $H \trianglelefteq G$ e $|H_i| = p^i$ e pelo item (iv) do Teorema 1.5.1, $H \cap Z(G) \neq 1$. Em particular, $Z(G) \neq 1$ e desta forma por indução $\frac{G}{Z(G)}$ é nilpotente. Logo, pelo item (ii) G é nilpotente .

v) Seja $1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \ldots \trianglelefteq G_n = G$. Temos,

$$\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\frac{G}{Z_i(G)}\right).$$

Logo,

$$\frac{Z_{i+1}(G)}{Z_i(G)} \leq N_{\frac{G}{Z_i(G)}}\left(\frac{HZ_i(G)}{Z_i(G)}\right).$$

Portanto,

$$\frac{HZ_i(G)}{Z_i(G)} \trianglelefteq \frac{Z_{i+1}(G)}{Z_i(G)} . \frac{HZ_i(G)}{Z_i(G)} = \frac{Z_{i+1}(G)H}{Z_i(G)}.$$

Assim, $HZ_i(G) \trianglelefteq HZ_{i+1}(G)$ e com isto concluímos que

$$H = Z_0(G)H \trianglelefteq Z_1(G)H \trianglelefteq \ldots \trianglelefteq Z_n(G)H = G.$$

vi) ($\Longrightarrow$) Suponha que G é um grupo finito nilpotente e seja

$$1 = G_0 \trianglelefteq \ldots \trianglelefteq G_n = G$$

uma série principal, isto é, $\frac{G_{i+1}}{G_i} \cdot\triangleleft \frac{G}{G_i}$. Basta ver que todo normal minimal de um grupo nilpotente é central. Dados G nilpotente e $N \cdot\triangleleft G$ pelo item (*iii*) $N \cap Z(G) \neq 1$, mas $N \cap Z(G) \trianglelefteq G$ e $N \cap Z(G) \leq N$ assim, $N \leq Z(G)$.
Se toda série pricipal é central é óbvio que G é nilpotente. □

Teorema 2.3.1 (**Teorema de Fitting**). *Sejam G um grupo e $A, B \trianglelefteq G$ com $Cl(A) = a$ e $Cl(B) = b$. Então $Cl(AB) \leq a + b$.*

Demonstração. Se $A = 1$ ou $B = 1$, então $a = 1$ ou $b = 1$ e portanto vale o Teorema. Suponha $A \neq 1$ e $B \neq 1$. Sejam $N = Z(A) \neq 1$ e $M = Z(B) \neq 1$. Observe que $Z(A) \overset{\triangleleft}{car} A \trianglelefteq G$, portanto $N = Z(A) \trianglelefteq G$ e de modo análogo $M = Z(B) \trianglelefteq G$. Logo,

$$\frac{AB}{N} = \frac{A}{N}\frac{BN}{N} \quad e \quad \frac{AB}{M} = \frac{AM}{M}\frac{B}{M}.$$

Pelo Segundo Teorema do Isomorfismo $\frac{BN}{N} \simeq \frac{B}{B \cap N}$ e $\frac{AM}{M} \simeq \frac{A}{A \cap M}$. Assim, $Cl\left(\frac{BN}{N}\right)$ $\leq Cl(B) = b$ e $Cl\left(\frac{AM}{M}\right) \leq Cl(A) = a$ e também $Cl\left(\frac{A}{N}\right) = a - 1$ e $Cl\left(\frac{B}{M}\right) = b - 1$. Por indução $\left(\frac{AB}{N}\right) \leq \left(\frac{A}{N}\right) + \left(\frac{BN}{N}\right) \leq a-1+b$ e $\left(\frac{AB}{M}\right) \leq \left(\frac{AM}{M}\right) + \left(\frac{B}{M}\right) \leq a+b-1$. Agora $\theta : AB \longrightarrow \frac{AB}{N} \times \frac{AB}{M}$ dada por $\theta(x) = (xN, xM)$ é um homomorfismo com $Nuc\,\theta = N \cap M$. Assim, $\frac{AB}{N \cap M} \simeq H \leq \frac{AB}{N} \times \frac{AB}{M}$. Logo, como $Cl\left(\frac{AB}{N \cap M}\right) \leq a+b-1$ e $N \cap M \leq Z(AB)$ temos que

$$\frac{AB}{Z(AB)} \simeq \frac{\frac{AB}{N \cap M}}{\frac{Z(AB)}{N \cap M}}.$$

Portanto, $Cl\left(\frac{AB}{Z(AB)}\right) \leq a + b - 1$ e daí, $Cl(AB) \leq a + b$. □

Definição 16. *Seja G um grupo. O subgrupo de Fitting de G é definido por $F(G) = \langle N \trianglelefteq G;\ N$ é nilpotente$\rangle$.*

Pelo Teorema de Fitting se G é um grupo finito, então $F(G) = \prod_{N \trianglelefteq\ G\ nilp} N$ é nilpotente.

Definição 17. *Um grupo G é dito ser p-Abeliano Elementar se G é abeliano e para todo $x \in G$ tem-se que $x^p = 1$.*

Observação 12. *Se G é p-abeliano elementar, então G é um espaço vetorial sobre $\mathbb{Z}_p$*

Teorema 2.3.2. *i) Seja G solúvel não trivial, então G é simples se e somente se $|G| = p$, onde p é um número primo;*

ii) Seja G finito, então são equivalentes:

a) G é solúvel;

b) Todo fator de composição tem ordem prima;

c) Todo fator principal é p-abeliano elementar.

Demonstração. *i*) Como $G' \trianglelefteq G$ temos que $G' = 1$ ou $G' = G$. Como G é solúvel, temos que $G' = 1$ e portanto G é abelino simples. Logo, $|G| = p$.
ii) $(a \Longrightarrow b)$ Seja $\frac{G_{i+1}}{G_i}$ fator de composião, então $\frac{G_{i+1}}{G_i}$ é solúvel e simples. Logo, pelo item (i) $\left|\frac{G_{i+1}}{G_i}\right| = p$.
$(b \Longrightarrow a)$ e $(c \Longrightarrow a)$ seguem diretamente da definição.
$(a \Longrightarrow c)$ Seja $N \cdot \triangleleft G$, então $N' \overset{\trianglelefteq}{car} N \trianglelefteq G$. Portanto $N' = 1$ ou $N' = N$, mas como N é solúvel e $N \neq 1$ segue-se que $N' = 1$ e assim, N é abeliano. Seja $A = \{x \in N;\ x^p = 1\}$, então $\forall x, y \in A$ temos que $(xy^{-1})^p = x^p y^{-1} = 1$. Logo, $A \trianglelefteq N$. Além disso, se $g \in G$ e $x \in A$ temos que $(g^{-1}xg)^p = g^{-1}x^p g = 1$. Portanto $A \trianglelefteq G$ e com isto $A = 1$ ou $A = N$. Agora, se p divide $|N|$, existe $x \in N$ tal que $x^p = 1$ com isto $A = N$ e portanto N é p-abeliano elementar. Como $N \neq 1$, existe um pripo p que divide $|N|$. Mostramos que todo subgrupo normal minimal em um grupo solúvel é p-abeliano elementar, mas isto é suficiente para para provar que todo fator princial é p-abeliano elementar. □

Definição 18. *Seja G um grupo, o subgrupo de Fratini de G é definido e denotador por*

$$\Phi(G) = \bigcap_{M\ \lneq\ G} M.$$

Um elemento $g \in G$ é dito ser não gerador de G se $G = \langle X, g\rangle$ implica que $G = \langle X\rangle$.

Lema 2.3.1. *Seja G um grupo finito. Então $\Phi(G)$ é o conjunto dos não geradores de G. Além disso, se $K \trianglelefteq G$, então $K \leq \Phi(G)$ se e somente se não existe $H \leq G$ tal que $KH = G$.*

Demonstração. Seja $g \in G$ um elemento não gerador de G. Se $g \notin \Phi(G)$ existe $M \lessdot G$ tal que $g \notin M$. Portanto, $G = \langle M, g\rangle$. Logo, $G = \langle M\rangle$ (Absurdo!). Assim, $g \in \Phi(G)$ e portanto $\{\text{Não geradores de G}\} \subseteq \Phi(G)$. Tome agora $g \in \Phi(G)$ e um subconjunto X de G tal que $G = \langle X, g\rangle$, se $G \neq \langle X\rangle$, então existe $M \lessdot G$ tal que $X \subseteq M$. Como $g \in \Phi(G)$ temos que $g \in M$ e daí, $\langle X, g\rangle \leq \langle M, g\rangle = M \neq G$, que é uma contradição. Logo, $G = \langle X\rangle$ e g é não gerador de G.
Seja $K \trianglelefteq G$, se $K \leq \Phi(G)$ e $H \leq G$ com $KH = G$, então $H = G$, pois se $H < G$ existiria um subgrupo maximal M de G contendo H. Portanto, $G = KH \leq M$ e assim $G = M$, que é um absurdo. Desta forma provamos que $\nexists H \leq G$ tal que $G = HK$.
Suponha agora que $K \trianglelefteq G$ e $K \not\leq \Phi(G)$, então existe $M \lessdot G$ tal que $K \not\leq M$ e portanto $G = HM$. □

Corolário 2.3.4. *Sejam G um grupo finito e $K \trianglelefteq G$, se $K \leq \Phi(G)$ e existe $H \leq G$ com $G = KH$, então $G = H$.*

Demonstração. Segue do Lema anterior. □

Teorema 2.3.3 (**Caracterização dos Grupos Nilpotentes Finitos**). *Seja G um grupo finito, então são equivalentes:*

i) G é nilpotente;

ii) Todo subgrupo de G é subnormal;

iii) Se $H < G$, então $H < N_G(H)$;

iv) Se $M \lessdot G$, então $M \trianglelefteq G$;

v) $G' \leq \Phi(G)$;

vi) Se $P \in Syl_p(G)$, então $P \trianglelefteq G$;

vii) $G = P_1 \times P_2 \times \ldots \times P_n$, onde $P_i \in Syl_{p_i}(G)$.

Demonstração. *i)* $\Longrightarrow$ *ii)* Já foi provado em geral no item (v) da Proposição 2.3.3.

ii) $\Longrightarrow$ *iii)* Dado $H < G$ existem por hipótese $H_i \leq G$ tais que $H \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G$. Então existe $i \in \{1, 2, \ldots, n\}$ tal que $H \triangleleft H_i$ e assim $H < N_G(H)$.

iii) $\Longrightarrow$ *iv)* Seja $M \lessdot G$ então como $M < N_G(M)$ temos que $M \trianglelefteq G$.

iv) $\Longrightarrow$ *v)* Seja MG. Então por hipótese $M \triangleleft G$ e daí, $\left|\dfrac{G}{M}\right| = p$. Assim, $\dfrac{G}{M}$ é abeliano e portanto $G' \leq M$. Logo $G' \leq \Phi(G)$.

v) $\Longrightarrow$ *iv)* Seja $M \lessdot G$. Então $\dfrac{M}{G'} < \dfrac{G}{G'}$, como $\dfrac{G}{G'}$ é abeliano temos que $\dfrac{M}{G'} \trianglelefteq \dfrac{G}{G'}$ e pelo Teorema da correspondência $M \trianglelefteq G$.

iv) $\Longrightarrow$ *vi)* Suponha que existe $P \in Syl_p(G)$ tal que $P \ntrianglelefteq G$, isto é $N_G(P) \neq G$. Seja $M \lessdot G$ tal que $N_G(P) \leq M$.

Afirmação: $M = N_G(M)$.

De fato, é claro que $M \leq N_G(M)$ e para $g \in N_G(M)$ temos que $P, P^g \leq M^g = M$. Pelo segundo Teorema de Sylow, existe $x \in M$ tal que $P^x = P^g$, logo $P = P^{gx^{-1}}$ e portanto $gx^{-1} \in N_G(P) \leq M$. Assim, $g \in M$ e com isto provamos que $M = N_G(M)$ o que é um absurdo já que por hipótese $M \trianglelefteq G$. Logo, $P \trianglelefteq G$.

vi) $\Longrightarrow$ *vii)* Segue diretamente da Proposição 1.7.2.

vii) $\Longrightarrow$ *i)* Pelo Teorema de Fitting o produto direto de grupos nilpotentes é nilpotente e pelo item *(iv)* da Proposição 2.3.3 todo p-grupo é nilpotente. Portanto, $G = P_1 \times P_2 \times \ldots \times P_n$ é nilpotente. □

Proposição 2.3.4. *Seja G um grupo finito. Então:*

i) Se $N \trianglelefteq G$, $H \leq G$ e $N \leq \Phi(H)$, então $N \leq \Phi(G)$;

ii) Se $M \trianglelefteq G$, então $\Phi(M) \leq \Phi(G)$;

iii) Se $N \trianglelefteq G$, então $\Phi\left(\dfrac{G}{N}\right) \geq \dfrac{\Phi(G)N}{N}$. Agora, se $N \leq \Phi(G)$ vale a igualdade.

iv) Seja $A \trianglelefteq G$, A abeliano e $\Phi(G) \cap A \neq 1$, então existe $H \leq G$ tal que $G = AH$ e $H \cap A = 1$, ou seja $G = A \rtimes H$.

Demonstração. i) Suponha que $N \not\leq \Phi(G)$. Então existe um subgrupo maximal M tal que $N \not\leq M$ e portanto $G = NM$ e $H = G \cap H = MN \cap H = N(M \cap H)$ pela identidade de Dedekind. Como $N \leq \Phi(H)$ temos que $H = H \cap M$, logo $H \leq M$, mas $N \leq H$ e assim concluímos que $N \leq M$ (Contradição).

ii) É fácil ver que $\Phi(M) \overset{\trianglelefteq}{car} M \trianglelefteq G$, logo $\Phi(M) \trianglelefteq G$. Fazendo $N = \Phi(M)$ e $H = M$ em (i) obtemos o resultado desejado.

(*iii*) Dado $\frac{M}{N} \lessdot \frac{G}{N}$ temos que $M \lessdot G$ e portanto $\frac{\Phi(G)N}{N} \leq \frac{M}{N}$. Logo,

$$\Phi\left(\frac{G}{N}\right) = \bigcap_{\frac{M}{N} < \frac{G}{N}} \frac{M}{N} \geq \frac{\Phi(G)N}{N}.$$

Suponha agora que $N \leq \Phi(G)$ e seja $\frac{H}{N} = \Phi\left(\frac{G}{N}\right)$, onde $N \trianglelefteq H \leq G$. Então, $\frac{H}{N} = \Phi\left(\frac{G}{N}\right) \geq \frac{\Phi(G)N}{N} = \frac{\Phi(G)}{N}$ e $H \geq \Phi(G)$. Seja $M \lessdot G$, então $N \leq \Phi(G) \leq M$ e $\frac{M}{N} \lessdot \frac{G}{N}$. Logo, $\frac{H}{N} = \Phi\left(\frac{G}{N}\right) \leq \frac{M}{N}$ e $H \leq M$, para todo $M \lessdot G$. Assim, $H \leq \Phi(G) \Longrightarrow H = \Phi(G)$.
iv) É claro que existe $H \leq G$ tal que $G = HA$. Seja H um grupo de ordem mínima tal que $G = HA$.

Se $H \cap A \leq \Phi(H)$, então $H \cap A \trianglelefteq H$ e como A é abeliano temos que $H \cap A \trianglelefteq A \Longrightarrow H \cap A \trianglelefteq HA = G$. Pelo item (i) $H \cap A \leq \Phi(G)$, mas $H \cap A \leq \Phi(G) \cap A = 1$. Logo, $H \cap A = 1$.

Suponha agora que $H \cap A \not\leq \Phi(H)$. Então existe $M \lessdot H$ tal que $H \cap A \not\leq M < H$. Logo, $(H \cap A)M = H$ e portanto $G = HA = (H \cap A)MA = (H \cap A)AM = AM < G$, pois $M < H$ e H tem a propriedade mínima, que é um absurdo. □

Definição 19. *Um grupo G é dito ser característicamente simples se os únicos subgrupos característicos de G são 1 e G.*

Proposição 2.3.5. *Se G é um grupo p-abeliano elementar finito, então G é característicamente simples.*

Demonstração. Seja $H \overset{\trianglelefteq}{car} G$, $H \neq 1$ e tome $v \in H - \{0\}$, $w \in G - \{0\}$. Sejam $B = \{v_1 = v, v_2, \ldots, v_r\}$ e $B' = \{v'_1 = w, v'_2, \ldots, v'_r\}$ duas bases de G. Defina $\theta : G \longrightarrow G$ por $\theta(\sum_{i=1}^{r} \overline{n_i} v_i) = \sum_{i=1}^{r} \overline{n_i} v'_i$. Então θ é um automorfismo de G com $\theta(v) = w$, como $H \overset{\trianglelefteq}{car} G$ temos que $w \in H$ e assim $H = G$. Com isto provamos que G é característicamente simples. □

Proposição 2.3.6. *Seja G um p-grupo finito. Então $\Phi(G) = 1$ se e somente se G é p-abeliano elementar.*

Demonstração. ($\Longrightarrow$) Seja $M \lessdot G$, então $M \trianglelefteq G$, pois todo p-grupo finito é nilpotente, e portanto $\left|\frac{G}{M}\right| = p$, daí $G' \leq M$ e $(xM)^p = x^pM = M$, logo $x^p \in M\ \forall x \in G$. Portanto $G' \leq \Phi(G)$ e $M \lessdot G$, com isto $G' = 1$. Assim, G é abeliano. Agora, como $x^p \in M\ \forall x \in G$ temos que $x^p \in \Phi(G)\ \forall x \in G$ e daí $x^p = 1\ \forall x \in G$. Logo, G é p-abeliano elementar.
($\Longleftarrow$) Temos que $\Phi(G) \overset{\triangleleft}{car} G$ e $\Phi(G) \neq G$. Como G é p-abeliano elementar temos que G é característicamente simples e portanto $\Phi(G) = 1$. □

Corolário 2.3.5. *Seja G um p-grupo finito, então $\frac{G}{\Phi(G)}$ é p-abeliano elementar.*

Demonstração. Seja $N = \Phi(G)$, então pelo item (iii) da Proposição 2.3.4

$$\Phi\left(\frac{G}{N}\right) = \frac{\Phi(G)N}{N} = 1.$$

Portanto, pela Proposição anteior segue o resultado. □

Proposição 2.3.7. *Seja G um grupo supersolúvel.*

i) Se $N \cdot \triangleleft\, G$, então $|N| = p$;

ii) Se $M \lessdot G$, então $|G : M| = p$.

Demonstração. i) Sejam $1 = G_o \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G$ uma série normal com $\frac{G_{i+1}}{G_i}$ cíclico, $N \cdot \triangleleft\, G$ e $i = min\{1, \ldots, n;\ N \cap G_j \neq 1\}$. Então, $N \cap G_i = N$ pois $N \cap G_i \leq N$, $N \cap G_i \trianglelefteq G$ e $N \cap G_i \neq 1$. Agora, no Teorema 2.3.2 mostramos que se G é solúvel e $N \cdot \triangleleft\, G$, então N é p-abeliano elementar e portanto $N \simeq C_p \times C_p \times \ldots \times C_p$ Por outro lado,

$$N \simeq \frac{N \cap G_i}{N \cap G_{i-1}} = \frac{N \cap G_i}{(N \cap G_i) \cap G_{i-1}} \simeq \frac{(N \cap G_i)G_{i-1}}{G_{i-1}} \leq \frac{G_i}{G_{i-1}}.$$

Portanto N é cíclico e daí $N \simeq C_p$. Logo, $|N| = p$.

ii) Sejam $M \lessdot G$ e $N \cdot \triangleleft\, G$, temos duas possibilidade:

a) $N \leq M$.

Neste caso, $\frac{M}{N} \lessdot \frac{G}{N}$ e por indução $\left|\frac{G}{N} : \frac{M}{N}\right| = p$. Portanto, $|G : M| = p$.

b) $N \not\leq M$.

Neste outro caso temos que $G = MN$ e

$$\frac{G}{N} = \frac{MN}{N} \simeq \frac{M}{M \cap N} \simeq M,$$

pois $N \cap M \neq N$ e $|N| = p$. Assim,

$$|G : M| = \frac{|G|}{|M|} = \frac{|G|}{\left|\frac{G}{N}\right|} = |N| = p$$

. □

2.4 Teorema de Schur-Zassenhaus e Aplicações

Teorema 2.4.1 (**Schur-Zassenhaus**). *Seja G um grupo finito e $N \trianglelefteq G$ com $(|N|, |G : N|) = 1$. Então existe $H \leq G$ tal que $|H| = |G : N|$. Em particular $G = HN$ e $H \cap N = 1$, pois $(|N|, |H|) = 1$. Além disso dois quaisquer subgrupos de ordem $|G : N|$ são conjugados em G.*

Demonstração. Veja 9.1.2 de [8]. □

Embora o Teorema acima seja de grande relevância não o demonstraremos, pois acredito que será mais interessente apresentarmos algumas aplicações conforme segue.

Proposição 2.4.1 (**P. Hall**). *Seja G um grupo finito e sulúvel com $|G| = mn$, $(m, n) = 1$. Então existe $H \leq G$ com $|H| = m$ e dois quaisquer subgrupos de ordem m são conjugados.*

Demonstração. **(Existência)** Seja $N \cdot \lhd G$, então pelo Teorema 2.3.2 N é p-abeliano elementar, isto é, $|N| = p^k$ e N é abeliano.
Caso 1: $p \mid m$. Então $\left|\frac{G}{N}\right| = \left(\frac{m}{p^k}\right) n$, por indução, existe $\frac{H}{N} \leq \frac{G}{N}$ tal que $\left|\frac{H}{N}\right| = \frac{m}{p^k}$ e portanto $|H| = m$.
Caso 2: $p \nmid m$. Então $\frac{G}{N} = m\left(\frac{n}{p^k}\right)$, por indução existe $\frac{K}{N} \leq \frac{G}{N}$ tal que $\left|\frac{K}{N}\right| = m$. Observe agora que $N \trianglelefteq K$ e que $(|N|, |K : N|) = 1$, pois $p \nmid m$. Pelo Teorema de Schur-Zassenhaus existe $H \leq K$ tal que $K = NH$ e $H \cap N = 1$. Logo, $H \leq G$ com $|H| = m$
(Conjugação) Sejam H e H' subgrupos de G com $|H| = |H'| = m$ e tome $N \cdot \lhd G$, então como N é p-abeliano elementar ($|N| = p^k$ e N é abeliano).
Caso 1: $p \mid m$ e portanto $p^k \mid m$. Agora como

$$|NH : H| = \frac{|NH|}{|H|} = \frac{|N||H|}{|H||N \cap H|} = \frac{|N|}{|N \cap H|} = |N : N \cap H| = p^\alpha$$

e $p \nmid n = |G:H| = |G:NH||NH:H|$ temos que $\alpha = 0$, assim $|NH:H| = 1$ e portanto $NH = H$. Logo, $N \leq H$ e analogamente $N \leq H'$. Mas $\dfrac{G}{N}$ é um grupo solúvel com $\left|\dfrac{G}{N}\right| = \left(\dfrac{m}{p^k}\right) n$, onde $\left(\dfrac{m}{p^k}, n\right) = 1$ e $\left|\dfrac{H}{N}\right| = \left|\dfrac{H'}{N}\right| = \dfrac{M}{p^k}$. Por indução, existe $g \in G$ tal que

$$\frac{H'}{N} = \left(\frac{H}{N}\right)^{gN} = \frac{(gN)H(g^{-1}N)}{N} = \frac{gHg^{-1}}{N}.$$

Portanto, $H' \leq H^g$ e assim $H' = H^g$.

Caso 2: $p \nmid m$ (isto é, $p \mid n$ e com isto $p^k \mid n$). Neste caso, $N \cap H = 1 = N \cap H'$ e então pelo Segundo Teorema do Isomorfismo $\dfrac{HN}{N} \simeq H$ e $\dfrac{H'N}{N} \simeq H'$. Desta forma temos que $\dfrac{G}{N}$ é solúvel com $\left|\dfrac{G}{N}\right| = m\left(\dfrac{n}{p^k}\right)$, onde $\left(m, \dfrac{n}{p^k}\right) = 1$ e $\left|\dfrac{HN}{N}\right| = \left|\dfrac{H'N}{N}\right| = m$. Por indução, existe $g \in G$ tal que

$$\frac{H'N}{N} = \left(\frac{HN}{N}\right)^{gN} = \frac{(gN)HN(g^{-1}N)}{N} = \frac{H^gN}{N}.$$

Assim, $H'N = H^gN = K$ e $(|K:N|, |N|) = (m, p^k) = 1$, pois $p \nmid m$. Pelo Teorema de Schur-Zassenhaus, existe $x \in K$ tal que $H' = (H^g)^x = H^{gx}$. □

Proposição 2.4.2. *Seja G um grupo finito tal que todo subgrupo maximal tem indice primo, se p é o maior primo que divide a ordem de G, então $|Syl_p(G)| = 1$. Em particular, se G é supersolúvel vale a Proposição.*

Demonstração. Suponha que $n_p = |Syl_p(G)| > 1$. Então $N_G(P) < G$ e assim existe M tal que $N_G(P) \leq M \lneq G$. Observe que $P \leq N_G(P) \leq M$ e portanto $N_G(P) \leq N_M(P)$, e também $P \in Syl_p(M)$. Mas $|M:N_M(P)| = n'_p = |Syl_p(M)| \equiv 1 \ (mod\ p)$, $|G:N_G(P)| = n_p \equiv 1 \ (mod\ p)$, $|G:N_G(P)| = |G:M||M:N_G(P)|$ e $|G:M| = q$, onde q é um primo diferente de p $(q < p)$. Daí,

$$n_p = qn'_p \implies q \equiv 1 \ (mod\ p).$$

Logo,

$$p \mid q-1 \implies p \leq q-1 \implies p < q.$$

Absurdo! □

2.5 O Homomorfismo Transfer

Sejam $H < G$ com $|G : H| = n$ e $\theta : H \longrightarrow A$ um homomorfismo, onde A é um grupo abeliano. Fixado um transversal $T = \{t_1, t_2, \ldots, t_n\}$ e dado $x \in G$ definimos $t_{(i)x}$ pela equação $H(t_i x) = Ht_{(i)x}$ e portanto $t_i x t_{(i)x}^{-1} \in H$. Defina $\theta^* : G \longrightarrow A$ por

$$\theta^*(x) = \prod_{i=1}^{n} \theta(t_i x t_{(i)x}).$$

Observação 13. *$x : i \longrightarrow (i)x$ é uma permutação em $I_n = \{1, 2, \ldots, n\}$.*

Demonstração. Se $(i)x = (j)x$, então

$$Ht_i x = Ht_j x \Longleftrightarrow Ht_i = Ht_j \Longleftrightarrow t_i = t_j \iff i = j.$$

□

Lema 2.5.1. *i) θ^* é um homomorfismo;*

ii) θ^* independe do transversal escolhido.

Demonstração. i) Devemos mostrar que $\theta^*(xy) = \theta^*(x)\theta^*(y)$. Temos,

$$Ht_{(i)xy} = Ht_i xy = (Ht_i x)y = Ht_{(i)x}y = Ht_{((i)x)y},$$

Portanto $t_{(i)xy} = t_{((i)x)y}$. Por definição

$$\theta^*(xy) = \prod_{i=1}^{n} \theta(t_i xy t_{(i)xy}^{-1}) = \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1} t_{(i)x} y t_{(i)xy}^{-1}) = \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1})(t_{(i)x} y t_{(i)xy}^{-1}).$$

Agora, como A é abeliano e $x : i \longrightarrow (i)x$ é uma permutação em I_n concluímos que

$$\theta^*(xy) = \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1}) \prod_{i=1}^{n} \theta(t_{(i)x} y t_{(i)xy}^{-1}) = \theta^*(x)\theta^*(y).$$

ii) Seja $T' = \{t'_1, t'_2, \ldots, t'_n\}$ outro transversal de H em G. A menos de uma permutação vale a igualdade $Ht_i = Ht'_i$ e desta forma podemos supor que $Ht_i = Ht'_i$. Assim, $t'_i = h_i t_i$, onde $h_i \in H$. Agora dado $x \in G$ temos que

$$Ht'_i x = Ht_i x \Longrightarrow Ht'_{(i)x} = Ht(i)x \Longrightarrow t'(i)x = h_{(i)x} t_{(i)x},$$

onde $h_{(i)x} \in H$. Portanto,

$$\theta^*_{T'}(x) = \prod_{i=1}^{n} \theta(t'_{(i)x} t'^{-1}_{(i)x}) = \prod_{i=1}^{n} \theta(h_i t_i x t^{-1}_{(i)x} h^{-1}_{(i)x})$$

$$= \prod_{i=1}^{n} \theta(h_i)\theta(t_i x t_{(i)x})\theta(h^{-1}_{(i)x}) = \prod_{i=1}^{n} \theta(t_i x t_{(i)x})\theta(h_i)\theta(h^{-1}_{(i)x})$$

$$= \theta^*_T(x) \prod_{i=1}^{n} \theta(h_i)\theta(h^{-1}_{(i)x}).$$

Mas como $x : \ i \longrightarrow (i)x$ é uma permutação e A é abeliano concluímos que $\prod_{i=1}^{n} \theta(h_i)\theta(h^{-1}_{(i)x}) = 1$ e assim $\theta^*_{T'}(x) = \theta^*_T(x)$. □

Lema 2.5.2 (**Calculo de θ^***). *Sejam $H < G$ e $\theta : \ H \longrightarrow A$ um homomorfismo com A abeliano e $|G : H| = n$. Então para cada $x \in G$ existem $l_1, l_2, \ldots, l_k \in N$ e $s_1, s_2, \ldots, s_k \in \mathbb{N}$ tais que $\theta^*(x) = \prod_{i=1}^{k} \theta(s_i x^{l_i} s_i^{-1})$ e $\sum_{i=1}^{k} l_i = n$.*

Demonstração. Fixe $x \in G$, tome $s_1 \in G$ e seja $l_1 = min\{l \in \mathbb{N}^*; \ Hs_1x^{l_1} = Hs_1\}$, observe que existe l_1, pois $|G : H| = n$.

Se $l_1 = n$, então $T = \{s_1, s_1x, \ldots, s_1x^{l_1-1}\}$ é um transversal de H em G. Caso contrário existe $s_2 \in G$ tal que $Hs_2 \neq Hs_1x^j$, para $0 \leq j \leq l_1 - 1$. Seja $l_2 = min\{l \in \mathbb{N}^*; \ Hs_2x^{l_2} = Hs_2\}$.

Se $l_1 + l_2 = n$ temos que $T = \{s_1, s_1x, \ldots, s_1x^{l_1-1}, s_2, \ldots, s_sx^{l_2-1}\}$ é transversal de H em G. Caso contrário procedemos indutivamente até que tenhamos $s_1, s_2, \ldots, s_k \in G$ e $l_1, l_2, \ldots, l_k \in \mathbb{N}^*$ com $l_1 + l_2 + \ldots + l_k = n$ e $T = \{s_1, \ldots, s_1x^{l_1-1}, s_2, \ldots, s_kx^{l_k-1}\}$ transversal de H em G (Observe que como $|G : H| = n$ repetiremos este processo um número finito de vezes até obtermos o transversal T). Assim,

$$\theta^*(x) = \prod_{i=1}^{l_1} \theta(t_i x t^{-1}_{(i)x}) \ldots \prod_{i=l_{k-1}}^{l_k} \theta(t_i x t^{-1}_{(i)x}).$$

Observe que

$$Ht_{(1)x} = Ht_1x = Hs_1x \Longrightarrow t_{(i)x} = t_2;$$

$$\vdots$$

$$Ht_{(l_1-1)x} = Hs_1x^{l_1-2}x = Hs_1x^{l_1-1} = Ht_{l_1} \Longrightarrow t_{(l_1-1)} = t_{l_1}$$

$$Ht_{(l_1)x} = Hs_1x^{l_1-1}x = Hs_1 = Ht_1 \Longrightarrow t_{(l_1)x} = t_1.$$

Logo,

$$\prod_{i=1}^{l_1} \theta(t_i x t_{(i)x}) = \theta(t_1 x t_2^{-1})\theta(t_2 x t_3^{-1}) \dots \theta(t_l x t_1^{-1})$$

$$= \theta(t_1 x t_2^{-1} t_2 x t_3^{-1} \dots t_{l-1} x t_l^{-1} t_l^{-1} x t_1^{-1}) = \theta(t_1 x^{l_1} t_1^{-1}) = \theta(s_1 x^{l_1} s_1^{-1}).$$

De modo análogo, temos que

$$\prod_{i=l_j+1}^{l_{j+1}} \theta(t_i x y_{(i)x} = \theta(s_{j+1} x^{l_{j+1}} s_{j+1}^{-1})).$$

Portanto,

$$\theta^*(x) = \prod_{i=1}^{k} (\theta(s_i) x^{l_i} s_i^{-1}).$$

□

Lema 2.5.3 (Schur). *Seja G um grupo com $H \leq Z(G)$ e $|G : H| = n$. Então $\theta^*(x) = x^n$, onde $\theta : H \longrightarrow H$ é a identidade. Em particular $(xy)^n = x^n y^n$.*

Demonstração. Pelo Lema anterior existem $s_1, s_2, \dots, s_k \in G$ e $l_1, l_2, \dots, l_k \in \mathbb{N}$ tais que $\sum_{i=1}^{k} l_i = n$ e

$$\theta^*(x) = \prod_{i=1}^{k} \theta(s_i x^{l_i} s_i^{-1}) = \prod_{i=1}^{k} s_i x^{l_i} s_i^{-1}.$$

Mas como $s_i x^{l_i} s_i^{-1} = z_i \in H \leq Z(G)$ temos que $x^{l_1} \in H \leq Z(G)$. Assim

$$\theta^*(x) = \prod_{i=1}^{k} x^{l_1} = x^n.$$

□

2.5.1 O Transfer de um p-Subgrupo de Sylow

Definição 20. *Sejam G um grupo finito e $P \in Syl_p(G)$, definimos*

$$G'(P) = \bigcap \left\{ N \trianglelefteq G;\ \frac{G}{N} \text{ é } p - abeliano \right\}.$$

• Sejam $N_1, \ldots, N_r$ todos os subgrupos normais de G tais que $\frac{G}{N}$ é p-abeliano. Então, $\varphi : G \longrightarrow \frac{G}{N_1} \times \frac{G}{N_2} \times \ldots \times \frac{G}{N_r}$ dada por $\varphi(x) = (xN_1, \ldots, xN_r)$ é um homomorfismo com $Nuc\ \varphi = \bigcap_{i=1}^{r} N_r = G'(P)$, desta forma $\frac{G}{G'(P)} \overset{\leq}{\sim} \frac{G}{N_1} \times \frac{G}{N_2} \times \ldots \times \frac{G}{N_r}$. Assim, $\frac{G}{G'(P)}$ é um p-grupo abeliano e portanto $G' \leq G'(P)$.

• $p \nmid \left|\frac{G'(P)}{G'}\right|$.

De fato, $\left|\frac{G'(P)}{G'}\right| \leq \frac{G}{G'}$ e $\frac{G}{G'}$ é abeliano. Assim $\frac{G'(P)}{G'} = \frac{K}{G'} \times \frac{H}{G'}$, onde $\frac{H}{G'} \in Syl_p\left(\frac{G}{G'}\right)$ e $p \nmid \left|\frac{K}{G'}\right|$. Agora,

$$\frac{\frac{G'(P)}{G'}}{\frac{K}{G'}} \simeq \frac{H}{G'},$$

onde $\frac{H}{G'}$ é p-grupo, logo $\frac{G'(P)}{K} \simeq \frac{H}{K}$ é p-grupo. Por outro lado, $\frac{G}{G'(P)} \overset{\leq}{\sim} \frac{G}{N_1} \times \frac{G}{N_2} \times \ldots \times \frac{G}{N_r}$ é p-abeliano, daí $\frac{G}{K}$ é p-grupo abeliano. Portanto $G'(P) \leq K$, assim $G'(P) = K$ e daí concluímos que $p \nmid \left|\frac{G'(P)}{G'}\right|$.

Lema 2.5.4. *Sejam G um grupo finito, $P \in Syl_p(G)$ e $\theta : P \longrightarrow \frac{P}{P'}$ homomorfismo definido por $\theta(x) = P'x$. Então $Nuc\ \theta^* = G'(P)$, $P \cap G' = P \cap G'(P)$ e*

$$Im\ \theta^* \simeq \frac{G}{Nuc\ \theta*} = \frac{PG'(P)}{G'(P)} = \frac{P}{P \cap G'(P)} = \frac{P}{P \cap G'} = \frac{PG'}{G'}.$$

Demonstração. Como $P \in Syl_p(G)$ temos que $p \nmid |G : P| = |G : PG'(P)||PG'(P) : P|$ e daí $p \nmid |G : PG'(P)|$. Por outro lado, $\frac{G}{G'(P)}$ é p-grupo, isto é, $p^\alpha = |G : G'(P)| = |G : PG'(P)||PG'(P) : G'(P)|$. Como $p \nmid |G : PG'(P)|$ concluímos que $|G : PG'(P)| = 1$ e com isto $G = PG'(P)$. Logo, $Im\ \theta^* \simeq \frac{PG'(P)}{G'(P)}$ e como $\frac{G}{Nuc\ \theta^*} \simeq Im\ \theta^* \leq \frac{P}{P'}$ temos que $\frac{G}{Nuc\ \theta^*}$ é p-abeliano. Assim $G'(P) \leq Nuc\ \theta^*$.
Agora, o Lema 2.5.2 nos diz que dado $x \in G$ existem $s_1, \ldots s_k \in G$ e $l_1, \ldots, l_k \in \mathbb{N}$, com $\sum_{i=1}^{k} l_i = n = |G : P|$ tais que $\theta^*(x) = \prod_{i=1}^{k} \theta(s_i x^{l_i} s_i^{-1}) = P'(\prod_{i=1}^{k}(s_i x^{l_i} s_i^{-1}))$. Mas como $G = PG'(P)$ temos que $s_i = a_i b_i$, onde $a_i \in P$ e $b_i \in G'(P)$, assim $Ps_i = Pb_i$ de modo que

$$P'(s_i x^{l_i} s_i^{-1}) = P'(a_i b_i x^{l_i} b_i^{-1} a_i^{-1}) = (P'a_i)(P'(b_i x^{l_i} b_i^{-1}))(P'a_i^{-1}) = P'(b_i x^{l_i} b_i^{-1})$$

(Observe que $b_i x^{l_i} b_i^{-1} \in P$, pois por construção $s_i x^{l_1} s_i^{-1} \in P$). Desta forma podemos supor que $s_i \in G'(P)$. Como $G'(P) \trianglelefteq G$ temos que $G'(P)x^{l_i} = x^{l_i}G'(P)$, ou seja, existe $s_i' \in G'(P)$ tal que $s_i x = x s_i'$ deste modo obetemos que

$$\theta^*(x) = P'(\prod_{i=1}^{k}(x^{l_i} s_i' s_i^{-1})) = P'(x^{l_1} s_i' s_i^{-1} x^{l_2} s_2' s_2^{-1} \dots x^{l_k} s_k' s_k^{-1}) = P'(x^n s).$$

Logo, se $x \in Nuc\ \theta^*$ concluímos que $P' = P' x^n s)$ e portanto $x^n \in P' s^{-1} \subseteq G'(P)$. Assim, $(xG'(P))^n = 1 \Longrightarrow o(xG'(P)) \mid n$, mas também temos que $o(xG'(P)) \mid |G : G'(P)| = p^\alpha$ e $(n, p) = 1$. Portanto, $o(xG'(P)) = 1$ e daí obtemos $x \in G'(P)$. Com isto provamos que $G'(P) = Nuc\ \theta^*$.
Finalmente, $\dfrac{G'(G'(P) \cap P)}{G'} \leq \dfrac{G'(P)}{G'}$, onde p não divide $\left|\dfrac{G'}{G'(P)}\right|$. Por outro lado, usando o Segundo Teorema do Isomorfismo e o fato de que $G' \leq G'(P)$, obtemos

$$\frac{G'(G'(P) \cap P)}{G'} \simeq \frac{G'(P) \cap P}{G' \cap (G'(P) \cap P)} = \frac{G'(P) \cap P}{G' \cap P} \leq \frac{P}{G' \cap P}.$$

Portanto $\dfrac{G'(G'(P) \cap P)}{G'} = 1$ já que p não divide divide $\left|\dfrac{G'(G'(P) \cap P)}{G'}\right|$. Logo, $G' \cap P = G'(P) \cap P$ e assim temos,

$$Im\ \theta^* \simeq \frac{G}{Nuc\ \theta*} = \frac{PG'(P)}{G'(P)} = \frac{P}{P \cap G'(P)} = \frac{P}{P \cap G'} = \frac{PG'}{G'}.$$

□

Teorema 2.5.1 (**Burnside**). *Sejam G um grupo finito, $P \in Syl_p(G)$, P abeliano e $N = N_G(P)$. Então $P = C_P(N) \times [N, P]$.*

Demonstração. Seja $\theta :\ P \longrightarrow P$ dada por $\theta(x) = x$, temos:

- $G = G'(P)P$;
- $Nuc\ \theta^* = G'(P) > G'$;
- $G'(P) \cap P = G' \cap P$;
- $Im\ \theta^* \simeq \dfrac{G}{Nuc\ \theta^*} = \dfrac{PG'(P)}{G'(P)} = \dfrac{P}{P \cap G'(P)} = \dfrac{P}{P \cap G'} = \dfrac{PG'}{G'}$;
- $\theta^*(G) = \theta^*(G'(P)P) = \theta^*(P)$, pois $G'(P) = Nuc\ \theta^*$.
- Dado $x \in G$ existem $s_1, \dots, s_k \in G$ e $l_1, \dots, l_k \in \mathbb{N}$, $\sum_{i=1}^{k} l_i = n = |G : P|$, tais que

$\theta^*(x) = \prod_{i=1}^{k}(s_i x^{l_i} s_i^{-1})$

Sejam $x \in P$ e $y = x^{l_i} \in P$. Então $y^{s_i^{-1}} = s_i y s_i^{-1} \in P$ por construção e $y^{s_i^{-1}} \in P^{s_i^{-1}}$, como P e $P^{s_i^{-1}}$ são abelianos concluímos que $P, P^{s_i^{-1}} \leq C_G(y^{s_i^{-1}}) \Longrightarrow P, P^{s_i^{-1}} \in Syl_p(C_G(y^{s_i^{-1}}))$. Pelo Segundo Teorema de Sylow existe $c_i \in C_G(y^{s_i^{-1}})$ tal que $P = P^{s_i^{-1}c_i^{-1}}$. Daí, $r_i = s_i^{-1}c_i^{-1} \in N_G(P)$ e assim temos

$$\theta^*(x) = \prod_{i=1}^{k} y^{s_i^{-1}} = \prod_{i=1}^{k} y^{s_i^{-1}c_i^{-1}} = \prod_{i=1}^{k} y^{r_i} = \prod_{i=1}^{k} (x^{l_i})^{r_i} = \prod_{i=1}^{k} x^{l_i}[x^{l_i}, r_i]$$

$$= \prod_{i=1}^{k} x^{l_i} \prod_{i=1}^{k} [x^{l_i}, r_i] = x^n a,$$

onde $a \in [P, N]$. Portanto, $x^n = \theta^*(x)d^{-1} \in \theta^*(P)[P, N] \leq P$. Mas como $x \in P$ temos que $(o(x), n) = 1$ e com isto existem $l, s \in \mathbb{Z}$ tais que $o(x)l + sn = 1$. Logo, $x = x^{o(x)l+sn} = x^{sn} = (x^n)^s \in \theta^*(P)[P, N]$. Assim, $P \leq \theta^*(P)[P, N] \leq P$ e portanto $P = \theta^*(P)[P, N]$.

Afirmação 1: $\theta^*(P) \cap Nuc\ \theta^* = Im\ \theta^* \cap Nuc\ \theta^* = 1$.

De fato, seja $\theta^*(y) \in Im\ \theta^* \cap Nuc\ \theta^* \leq G = G'(P)P$. Então existem $y' \in G'(P) = Nuc\ \theta^*$ e $x \in P$ tais que $x = y'x$. Assim, $\theta^*(y) = \theta^*(x) = x^n a$, $a \in [P, N] \leq G' \leq G'(P) \leq Nuc\,\theta^*$, e então $1 = \theta^*(\theta^*(x)) = \theta^*(x^n a) = (\theta^*(x))^n$. Portanto, $o(\theta^*(x)) \mid n$, mas $\theta^*(x) \in P$ e $(n, p) = 1$. Logo, $\theta^*(x) = 1$. Agora $[P, N] \leq G' \leq G'(P) = Nuc\,\theta^*$, então $\theta^*(P) \cap [P, N] = 1$ e com isto obtemos

$$P = \theta^*(P) \times [P, N] = Im\ \theta^* \times [P, N].$$

Afirmação 2: $Im\ \theta^* = \theta^*(P) \trianglelefteq N$.

De fato, sejam $x \in P$, $T = \{t_1, \ldots t_n\}$ um transversal e $\theta^*(x) = \prod_{i=1}^{n} t_i x t_{(i)x}^{-1}$. Dado $y \in N$, $\{t_1^y, \ldots, t_n^y\}$ também é um transversal, pois $Pt_i^y = Pt_j^y \Longrightarrow P^{y^{-1}}t_i = P^{y^{-1}}t_j \Longrightarrow Pt_i = Pt_j \Longrightarrow i = j$. Vajamos também que $Pt_i^y x^y = Pt_{(i)x^y}^y$,mas

$$Pt_i^y x^y = (Pt_i x)^y = (Pt_{(i)x})^y = Pt_{(i)x}^y.$$

Portanto, $Pt_{(i)x^y}^y = Pt_{(i)x}^y$ e

$$(\theta^*(x))^y = (\prod_{i=1}^{n} t_i x t_{(i)x}^{-1})^y = \prod_{i=1}^{n} t_i^y x^y t_{(i)x}^{-y} = \prod_{i=1}^{n} t_i^y x^y t_{(i)x^y}^{-y} = \theta^*(x^y).$$

Assim $(\theta^*(x))^y \in \theta^*(P)$, $\forall x \in P$ e $\forall y \in N$. Logo, $\theta^*(P) = Im\ \theta^* \trianglelefteq N$ e portanto $[\theta^*(P), N] \leq \theta^*(P) \cap [P, N] = 1$. Desta forma provamos que $\theta^*(P) \leq C_P(N)$.
Agora, se $x \in C_P(N)$, então

$$\theta^*(x) = x^n \prod_{i=1}^{k} [x^{l_i}, r_i] = x^n,$$

pois $x^{l_1} \in C_P(N)$ e $r_i \in N$. Daí como $(n, p) = 1$ existem $l, s \in \mathbb{Z}$ tais que $ln + sp = 1$. Assim,

$$x = x^{ln} = (x^n)^l = (\theta^*(x))^l \in \theta^*(P).$$

Portanto, $C_P(N) = \theta^*(P)$ e daí concluímos que

$$P = C_P(N) \times [P, N].$$

□

Observação 14. *Ainda no contexto do Teorema acima temos* $[P, N] \leq G' \cap P = G'(P) \cap P$. *Como* $P = C_P(N) \times [P, N]$ *temos que*

$$\theta^*(P) = C_P(N) \simeq \frac{P}{[P, N]}$$

e ainda

$$Im\ \theta^* = \theta^*(P) \simeq \frac{G}{G'(P)} = \frac{PG'(P)}{G'(P)} \simeq \frac{P}{P \cap G'(P)}.$$

Portanto,

$$\left|\frac{P}{[P, N]}\right| = \left|\frac{P}{G'(P) \cap P}\right|$$

e daí $|[P, N]| = |G'(P) \cap P| \Longrightarrow [P, N] = G'(P) \cap P$.

Corolário 2.5.1 (**Teorema de Burnside-Transfer**). *Se* G *é um grupo finito e existe* $P \in Syl_p(G)$ *tal que* $P \leq Z(N)$, $N = N_G(P)$, *então existe* $H \trianglelefteq G$ *tal que* $G = HP$, $H \cap P = 1$. *Em particular, se* $C_G(P) = N_G(P)$, *então existe* $H \trianglelefteq G$ *tal que* $G = HP$ *com* $H \cap P = 1$.

Demonstração. Como $P \leq Z(N)$ temos que P é abelino e $[P, N] = 1$. O Teorema de Burnside nos diz que $P = C_P(N)$, mas como $1 = [P, N] = G'(P) \cap P$ e $G = G'(P)P$. Logo $H = G'(P) \trianglelefteq G$ é tal que $G = HP$ e $H \cap P = 1$. Em particular, se $C_G(P) = N_G(P) = N$, então $1 = [P, N] \Longrightarrow P \leq Z(N)$, portanto existe $H \trianglelefteq G$ tal que $G = HP$ e $H \cap P = 1$. □

Proposição 2.5.1. *Seja G um grupo finito. Se existe um subgrupo A de G maximal e abeliano, então G é solúvel.*

Demonstração. Suponha que a afirmação acima seja falsa e seja G um contra-exemplo mínimo. Neste caso, se existir um grupo H é satisfazendo as hipóteses do Lema com $|H| < |G|$, então H é solúvel.

Caso 1: $A_G \neq 1$. Então $\dfrac{A}{A_G}$ é um subgrupo maximal abeliano de $\dfrac{G}{A_G}$ com $\left|\dfrac{G}{A_G}\right| < |G|$. Portanto $\dfrac{G}{A_G}$ é solúvel e A_G é solúvel, pois $A_G \leq A$ é abeliano. Logo G é solúvel, que é uma contradição.

Caso 2: $A_G = 1$. Sejam $\pi = \{$ Primos que dividem $|A|\}$, $\pi' = \{$ Primos que não dividem $|A|\}$ e $p \in \pi$. Como A é abeliano temos que $Syl_pA = \{P_0\}$ e $A \leq N_G(P_0)$. Seja $P \in Syl_pG$ com $P_0 \leq P$. Então $P_0 = P \cap A$. Agora, como $A_G = 1$ e $P_0 \leq A$ temos que $P_0 \not\trianglelefteq G$, assim $N_G(P_0) \neq G$. Sendo A maximal concluímos que $N_G(P_0) = A$. Portanto,

$$P_0 \;=\; P \cap A \;=\; P \cap N_G(P_0) \;=\; N_P(P_0),$$

anteriormente mostramos que todo p-grupo é nilpotente, mostramos também que se G é nilpotente e $H < G$, então $H < N_G(H)$. Assim, se $P_0 < P$ teíamos que $P_0 < N_P(P_0) = P_0$, portanto $P_0 = P$ e $p \nmid |G : A|$. Logo $(|A|, |G : A|) = 1$. Por outro lado,

$$A \leq C_G(P) \leq N_G(P) = A, \quad \forall P \in Syl_P(A).$$

Pelo Teorema de Burnside-Transfer, existe $N_P \trianglelefteq G$ tal que $G = PN_P$ e $P \cap N_P = 1$.
Seja $L = \bigcap_{p\in\pi} N_P$. Claro que $L \trianglelefteq G$, então $\dfrac{G}{L} \simeq \overline{H}$, onde $\overline{H}$ é um subgrupo de $\dfrac{G}{N_{P_1}} \times \ldots \times \dfrac{G}{N_{P_r}} \simeq P_1 \times \ldots \times P_r$ e P_i é abeliano, assim $\dfrac{G}{L}$ é um π-grupo abeliano e portanto $\dfrac{G}{L}$ é solúvel. Mas como p não divide $|N_P| = |G : P|$, temos que L é π'-grupo.

Se $L = 1$, então G é abeliano e portanto solúvel. Desta forma podemos supor que $L \neq 1$ e com isto $L \not\subseteq A$ (pois $L \trianglelefteq G$ e $A_G = 1$) e $G = AL$, $A \cap L = 1$, já que A é π-grupo e L é π'-grupo.

Seja $Q \in Syl_q(L)$, onde $L \trianglelefteq G$. Pelo Argumento de Fratini temos que $G = LN_G(Q)$

Observe que $L = 1$ implica G solúvel e portanto podemos supor que

$L \neq 1$. Deste modo $L \cap A = 1$, pois L é π'-grupo e A é π-grupo, assim como A é

maximal concluímos que $G = AL$. Seja $Q \in Syl_q L$ $(L \trianglelefteq G)$, pelo Argumento de Fratini $G = N_G(Q)L$.

Mas pelo Segundo Teorema do Isomorfismo $\frac{G}{L} \simeq \frac{N_G(Q)}{N_G(Q) \cap L} = \frac{N_G(Q)}{N_L(Q)}$ e com isto concluímos que $(|L|, |N_G(Q) : N_L(Q)|) = 1$.

Observe também que $N_L(Q) \trianglelefteq N_G(Q)$ com $(|N_L(Q)| : |N_L(Q) : Q|) = 1$. Assim, pelo Teorema de Schur-Zassenhaus existe $X \leq N_G(Q)$ tal que $N_G(Q) = N_L(Q)X$ e $X \cap N_L(Q) = 1$. Deste modo $G = LN_G(Q) = L(N_L(Q)X) = LX = LA$ com $X \cap L = 1$, pois $|X| = |N_G(Q) : N_L(Q)| = |G : L|$ e $(|L||G : L|) = 1$. Novamente, pelo Teorema de Schur-Zassenhaus, existe $g \in G$ tal que $X = A^g$ e assim X é maximal abeliano.

Agora temos que $Q \trianglelefteq N_G(Q)$, $X \leq N_G(Q)$, $X < \cdot G$ e $X \cap Q = 1$. De modo que $X < QX \leq N_G(Q) \leq G$. Portanto $G = QX = N_G(Q)$ e com isto provamos que $Q \trianglelefteq G$, consequentemente $Q \trianglelefteq L$. Então mostramos que todo subgrupo de Sylow de L é normal, com isto L é nilpotente e em particular L é solúvel.

Como mostramos que $\frac{G}{L}$ e L são solúveis o Corolário 2.3.2 nos garante que G é solúvel, mas G foi escolhido como o menor grupo não solúvel com um subgrupo maximal e abeliano (Absurdo!). Logo todo grupo finito com um subgrupo maximal abelina é solúvel. □

2.6 O Teorema de Maschke

Definição 21. *Sejam G um grupo e $\mathbb{K}$ um corpo. Um espaço vetorial M sobre $\mathbb{K}$ é dito ser um G-módulo ou um G-espaço (à direita) sobre $\mathbb{K}$, se podemos definir uma operação*

$$\alpha : \ M \times G \longrightarrow M$$

$$(m, g) \longrightarrow mg$$

com as seguintes propriedades:

- $(\alpha m + \beta n)g = \alpha(mg) + \beta(ng)$;
- $m(gg') = (mg)g'$;
- $m1 = m$

Para quaisquer $\alpha, \beta \in \mathbb{K}$, $m, n \in M$ e $g, g' \in G$.

Definição 22. *Sejam G um grupo, $\mathbb{K}$ um corpo e M um G-módulo sobre $\mathbb{K}$. Um subespaço vetorial X de M é dito ser G-invariante (G-subespaço ou G-submódulo), se para todos $x \in X$, $g \in G$ temos $xg \in X$. Notação: $X \leq_G M$.*
Denotamos por $\mathbb{S}_G(M)$ o conjunto de todos os G-submódulos de M, ou seja,

$$\mathbb{S}_G(M) = \{X;\ X \leq_G M\}.$$

Definição 23. *Seja M um G-módulo sobre $\mathbb{K}$.*

i) M é um G-módulo irredutível, se $M \neq 0$ e se M e 0 são os únicos G-submódulos de M, isto é, $|\mathbb{S}_G(M)| = 2$.

ii) M é um G-módulo completamente redutível, se para todo $X \in \mathbb{S}_G(M)$ existe $Y \in \mathbb{S}_G(M)$ tal que $M = X \oplus Y$.

Teorema 2.6.1 (**Maschke**). *Sejam G um grupo finito e $\mathbb{K}$ um corpo cuja característica $p \geq 0$ não divide $|G|$. Se M é um G-módulo sobre $\mathbb{K}$, então M é completamente redutível.*

Demonstração. Tome $X \in \mathbb{S}_G(M)$. Como X é um subespaço vetorial de M, sabemos da Álgebra Linear que existe um subespaço Y de M tal que $M = X \otimes Y$. Vamos construir $Y^* \in \mathbb{S}_G(M)$ tal que $M = X \oplus Y^*$ e para isto consideremos a projeção de M sobre X, isto é,

$$\pi : M \longrightarrow X$$

$$m \longrightarrow \pi(m)$$

onde $\pi(m) = x$, visto que, dado $m \in M$ existem únicos $x \in X$ e $y \in Y$ tais que $m = x + y$. Definimos a aplicação

$$\tau : M \longrightarrow M$$

por $\tau(m) = m - \dfrac{1}{|G|}\displaystyle\sum_{g \in G} \pi(mg^{-1})g$, $\forall m \in M$. Note que $0 \neq 1 + 1 + 1 + \ldots + = |G| \in \mathbb{K}$ (soma de $|G|$ vezes o elemeno $1 \in \mathbb{K}$) já que a característica p de $\mathbb{K}$ não divide $|G|$. Observe que τ goza das seguintes propriedades:
i) τ é linear, pois é uma combinação de aplicações lineares;
ii) $\tau(mg) = \tau(m)g$, para todos $m \in M$ e $g \in G$;

De fato,

$$\begin{aligned}\tau(mg) &= mg - \frac{1}{|G|}\sum_{g'\in G}\pi(mgg'^{-1})g' \\ &= mg - \frac{1}{|G|}\sum_{g'\in G}\pi(m(g'g^{-1})^{-1}g'g^{-1})g \\ &= (m - \frac{1}{|G|}\sum_{g'\in G}\pi(mg'^{-1})g')g \\ &= \tau(m)g.\end{aligned}$$

iii) $X \subseteq Ker\tau$

Para $m = x \in X$ temos $\tau(x) = x - \frac{1}{|G|}\sum_{g\in G}\pi(mg^{-1})g = x - \frac{1}{|G|}|G|x = x - x = 0$, já que $xg^{-1} \in X$ e consequentemente $\pi(xg^{-1})g = xg^{-1}g = x$.

iv) $\tau^2 = \tau$.

Veja que

$$\begin{aligned}\tau^2(m) &= \tau(\tau(m)) \\ &= \tau(m) - \frac{1}{|G|}\sum_{g\in G}\tau(\pi(xg^{-1})g) \\ &= \tau(m)\end{aligned}$$

visto que $\pi(mg^{-1})g \in X \subseteq Ker\tau$.

Definamos agora $Y^* = Im\tau = \{\tau(m);\ m \in M\}$. Claramente Y^* é um subespaço de M. Além disso, para todo $y \in Y^*$ existe $m \in M$ tal que $\tau(m) = y$. Também, para todo $g \in G$ segue por (ii) que $yg = \tau(m)g = \tau(mg)$ e $m - \tau(m) \in X$, para $\tau(m) \in Y^*$. Logo, $M = X + Y^*$. Seja $x = \tau(m) \in X \cap Y^*$, $m \in M$. Segue por (iii) e (iv) que $0 = \tau(x) = \tau(\tau(m)) = x$. Portanto, $X \cap Y = 0$ e daí concluímos que $M = X \oplus Y^*$.

□

Capítulo 3

Teoremas de Kuzennyi - Pylaev

Neste capítulo provaprovaremos os Teoremas de Kuzennyi - Pylaev sobre classificação dos grupos finitos com um subgrupo cíclico maximal e sobre classificação dos grupos finitos com no máximo um subgrupo não cíclico maximal. Antes de provamos estes Teoremas precisaremos classificar os grupos de ordem p^n satisfazendo as mesmas propriedades.

3.1 Grupos Finitos com um Subgrupo Cíclico Maximal

3.1.1 Classificação dos $p-$grupos com um subgrupo cíclico maximal

Antes de classificar os p-grupos com um subgrupo cíclico maximal, precisaremos provar o Lema abaixo que nos ajudará na demonstração do Teorema de classificação.

Lema 3.1.1. *Se G é nilpotente de classe menor ou igual a 2, então* $(xy)^m = x^m y^m [y,x]^{\binom{m}{2}}$.

Demonstração. Como Cl(G) ≤ 2 temos que $1 = \gamma_3(\mathrm{G}) = [G', G]$, assim $G' \leq \mathrm{Z(G)}$. Precisaremos provar primeiramente a seguinte afirmação.
Afirmação: $[y^m, x] = [y,x]^m$.

O caso $m = 1$ é trivial. Suponha que $[y^m, x] = [y, x]^m$. Então, $[y^{m+1}, x] = [y^m y, x] = [y^m, x]^y [y, x]$ e como $G' \in Z(G)$ temos que $[y^m, x]^y = [y^m, x]$. Portanto, $[y^{m+1}, x] = [y^m, x][y, x] = [y, x]^m [y, x] = [y, x]^{m+1}$.

Prova do Lema $(m = 2)$. Usando o fato de que $G' \leq Z(G)$ obtemos

$$1 = [x, y^{-1}y] = [x, y][x, y^{-1}]^y = [x, y][x, y^{-1}]$$

e portanto $[y, x] = [x, y]^{-1} = [x, y^{-1}]$.
Novamente, como $G' \leq Z(G)$ vemos que

$$x^2y^2[y, x] = x^2[y, x]y^2 = x^2[x, y^{-1}]y^2 = x^2x^{-1}yxy^{-1}y^2$$

$$= xyxy = (xy)^2.$$

Suponha agora que tenhamos $(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}$ para algum $n \geq 2$. Então,

$$(xy)^{n+1} = (xy)^n(xy) = x^n y^n [x, y]^{\binom{n}{2}} xy.$$

Mas pela afirmação $[y^n, x] = [y, x]^n \implies (y^n)^{-1}x^{-1}y^n x = [y, x]^n$. Assim

$$y^n x = xy^n [y, x]^n.$$

Daí,

$$(xy)^{n+1} = x^n xy^n [y, x]^n y[y, x]^{\binom{n}{2}} = x^{n+1}y^{n+1}[y, x]^{n+\binom{n}{2}}$$
$$= x^{n+1}y^{n+1}[y, x]^{\binom{n+1}{2}}$$

□

Proposição 3.1.1 (**Classificação dos p-Grupos Finitos com um Subgrupo Cíclico Maximal**). *Um grupo de ordem p^n contêm um subgrupo cíclico de índice p (Em outras palavras, um subgrupo cíclico maximal) se e somente se é um dos seguintes grupos:*

i) $G = \langle a;\ a^{p^n} = 1 \rangle$, $n \geq 1$;

ii) $G = \langle a, b;\ a^{p^{n-1}} = 1,\ b^p = 1 \rangle$, $n \geq 2$;

iii) $G = \langle a, b;\ a^{p^{n-1}} = 1,\ b^p = 1,\ bab^{-1} = a^{1+p^{n-2}} \rangle$, $n \geq 3$, p *é ímpar;*

iv) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}},\ bab^{-1} = a^{-1} \rangle$, $n \geq 3$;

v) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = 1,\ bab^{-1} = a^{-1}\rangle$, $n \geq 3$;

vi) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = 1,\ bab^{-1} = a^{1+2^{n-2}}\rangle$, $n \geq 4$;

vii) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = 1,\ bab^{-1} = a^{-1+2^{n-2}}\rangle$, $n \geq 4$.

Demonstração. ($\Longleftarrow$) Trivial.

($\Longrightarrow$) Seja G um grupo abeliano com $|G| = p^n$ contendo um subgrupo cíclico maximal N. Como G é nilpotente temos que todo subgrupo maximal é normal, desta forma concluímos que $N = \langle a\rangle$, onde $o(a) = p^{n-1}$ e então $\left|\frac{G}{N}\right| = p$. Assim, como $\frac{G}{N}$ é cíclico existe $x \in G$ tal que

$$\frac{G}{N} = \langle xN\rangle.$$

Então,

$$G = \langle x, N\rangle = \langle x\rangle\langle N\rangle = \langle x\rangle\langle a\rangle.$$

Agora, como $\left|\frac{G}{N}\right| = p$ temos que $(xN)^p = x^pN = N$. Portanto $x^p \in N = \langle a\rangle$. Escreva $x^p = a^i$, temos duas possibilidades:

1) Se $p \not| i$, então $(p^{n-1}, i) = 1$ e com isto existem $r, s \in \mathbb{Z}$ tais que $rp^{n-1} + si = 1$. Assim

$$a = a^{rp^{n-1}+si} = a^{si} = (a^i)^s = x^s.$$

Portanto $a \in \langle x\rangle$ e daí obtemos que $G = \langle x;\ x^{p^n} = 1\rangle$, ou seja G é do tipo (i).

2) Se $p \mid i$, $x^p = a^i = a^{jp} = (a^j)^p = b^p$, onde $b = a^j \in \langle a\rangle$.

• Como G é abeliano temos que $(xb^{-1})^p = x^p(b^{-1})^p = x^px^{-p} = 1$ e portanto $o(xb^{-1}) \mid p$ já que $o(xb^{-1}) = p$, mas se $o(xb^{-1}) = 1$ então necessariamente $x = b$ e daí $G = \langle a\rangle$, que não é verdade.

• $G = \langle xb^{-1}, a\rangle$, pois $x = xb^{-1}a^j \in \langle xb^{-1}, a\rangle$ e assim $G = \langle x, a\rangle \leq \langle xb^{-1}, a\rangle$ e obviamente $\langle xb^{-1}, a\rangle \leq G$.

• $\langle xb^{-1}\rangle \cap \langle a\rangle = 1$.

De fato, $\langle xb^{-1}\rangle \cap \langle a\rangle = 1$ ou $\langle xb^{-1}\rangle \cap \langle a\rangle = \langle xb^{-1}\rangle$, mas se $\langle xb^{-1}\rangle \cap \langle a\rangle = \langle xb^{-1}\rangle$, então $\langle xb^{-1}\rangle \leq \langle a\rangle$ e com isto teríamos que $G = \langle a\rangle$.

Deste modo concluímos que $G = \langle a, xb^{-a};\ a^{p^{n-1}} = 1,\ (xb^{-1})^p = 1\rangle$, tipo (ii).

Suponha agora que G é não abeliano ($n \geq 3$). Assim como no caso anterior $\frac{G}{N} = \langle xN\rangle$, onde $N = \langle a\rangle$, $o(a) = p^{n-1}$ e $x \in G$. Portanto $G = \langle x, N\rangle = \langle x\rangle\langle a\rangle$

Afirmação: $a^x = a^m$, onde $1 < m < p^{n-1}$.

De fato, como $|G : \langle a\rangle| = p$ temos que $\langle a\rangle \trianglelefteq G$ e com isto $a^x \in \langle a\rangle$. Daí $a^x = a^m$, $1 \leq m \leq p^{n-1}$, mas

$$m = 1 \Longrightarrow a^x = a \Longrightarrow ax = xa \Longrightarrow G' = 1,$$

e

$$m = p^{n-1} \Longrightarrow a^x = 1 \Longrightarrow x^{-1}ax = 1 \Longrightarrow ax = x \Longrightarrow a = 1.$$

Agora

$$a^{x^2} = (a^x)^x = (a^m)^x = (a^x)^m = a^{m^2}$$

$$a^{x^3} = (a^{x^2})^x = (a^{m^2})^x = (a^x)^{m^2} = a^{m^3}$$

$$\vdots$$

$$a = a^{x^p} = a^{m^p} \Longrightarrow a^{m^p-1} = 1 \Longrightarrow p^{n-1} \nmid (m^p - 1).$$

Logo, $m^p \equiv 1\ (mod\ p^{n-1})$ e em particular $m^p \equiv 1\ (mod\ p)$. Pelo Teorema de Fermat $m^p \equiv m\ (mod\ p) \Longrightarrow m \equiv 1\ (mod\ p)$, portanto $p \mid (m-1)$ e daí $p \nmid m$

Caso 1: $p > 2$.

Seja $m = 1 + kp^i$ com $0 < i < n-1$ e $p \nmid k$ (Observe que $i = n-1 \Longrightarrow a^x = a^m = a \Longrightarrow ax = xa \Longrightarrow G' = 1$). Assim

$$m^p = (1+kp^i)^p = 1 + \binom{p}{1}kp^i + \binom{p}{2}(kp^i)^2 + \ldots + \binom{p}{p-1}(kp^i)^{p-1} + (kp^i)^p$$

$$= 1 + kp^{i+1} + lp^{i+2}.$$

Portanto, $m^p - 1 = kp^{i+1} + lp^{i+2}$, mas $m^p \equiv 1 (mod\ p^{n-1})$ nos diz que $kp^{i+1} + lp^{i+2} = l'p^{n-1}$. Daí

$$k = l'p^{n-1-(i+1)} - lp^{i+2-(i+1)} = l'p^{n-i-2} - lp.$$

Como, $p \nmid k$ temos que $n - i - 2 = 0$, com isto obtemos $i = n-2$ e $m = 1 + kp^{n-2}$, onde $p \nmid k$. Agora como $p \nmid k$ temos que $(p,k) = 1$, logo existem $r, s \in \mathbb{Z}$ tais que $rk + sp = 1$. Assim,

$$a^{x^r} = a^{m^r} = a^{(1+kp^{n-2})^r} = a^{1+krp^{n-2}+\binom{r}{2}(kp^{n-2})^2+\ldots+(kp^{n-2})^r}$$

$$= a^{1+(1-sp)p^{n-2}+p^{n-1}} = a^{1+p^{n-2}-sp^{n-1}} = a^{1+p^{n-2}}.$$

Observe agora que $x^r \notin N \Longrightarrow x^{rk} = x^{1-sp} = x.x^{-sp} = x \Longrightarrow x \in N \Longrightarrow G = N$.
Portanto, $x^r \notin N$ e $G = \langle x^r, N\rangle$. Assim substituindo x^r por x podemos supor que $a^x = a^{1+p^{n-2}}$. Portanto,

$$(a^p)^x = (a^x)^p = (a^{1+p^{n-1}})^p = a^{p+p^{n-1}} = a^p.$$

Logo, $a^p \in Z(G)$ e com isto temos que $|Z(G)| \geq p^{n-2}$. Assim, $|Z(G)| = p^{n-2}$, p^{n-1} ou p^n, mas $|Z(G)| = p^n$ ou p^{n-1} implica G abeliano. Logo, $|Z(G)| = p^{n-2}$ e deste modo $Z(G) = \langle a^p\rangle$. Agora como $x^p \in \langle a\rangle$ temos

$$(x^p)^a = (a^j)^a = a^j = x,$$

assim $x^p \in Z(G) = \langle a\rangle$ e portanto $o(x^p) \mid p^{n-2}$ e $x^p = (a^p)^l = (a^l)^p = b^l$, $b = a^l \in N$. Além disso, $\left|\dfrac{G}{Z(G)}\right| = p^2$ e com isto $Cl(G) \leq 2$. Pelo Lema 3.1.1 temos que

$$(xb^{-1})^p = x^p b^{-p}[b^{-1}, x]^{\binom{p}{2}} = x^p b^{-1}[b^{-1}, x]^{\frac{p(p-1)}{2}}$$

$$= x^p b^{-p}[b^{-1}x^p]^{\frac{p-1}{2}} = b^p b^{-1}[b^{-1}, b^p]^{\frac{p-1}{2}} = 1.$$

Como $xb^{-1} = 1 \Longrightarrow x = b \in N \Longrightarrow G = N$, temos $o(xb^{-1}) = p$. Observe também que

$$a^{xb^{-1}} = (a^x)^{b^{-1}} = a^x = a^{1+p^{n-2}}.$$

Substituindo xb^{-1} por x obtemos G = $\langle a, x;\ a^{p^{n-1}} = 1 = x^p, a^x = a^{1+p^{n-2}}\rangle$, $n \geq 3$. Ou seja, G é do tipo (iii).

Caso 2: $p = 2$.

Temos $G = \langle a, x;\ a^{2^{n-1}} = 1,\ a^x = a^m\rangle$, onde $m^2 \equiv 1\ (mod\ 2^{n-1})$ e $m \equiv 1\ (mod\ 2)$. Assim, $m = 1 + 2k$ e então $m^2 - 1 = (1 + 2k)^2 - 1 = 4k + 4k^2 = 4k(k + 1)$. Por outro lado, $m^2 - 1 = 2^{n-1}k'$, de modo que

$$4k(k + 1) = 2^{n-1}k' \Longrightarrow k(k + 1) = 2^{n-3}k'.$$

Desta forma $2^{n-3} \mid k$ ou $2^{n-3} \mid (k + 1)$ e portanto $k = 2^{n-3}l$ ou $k = 2^{n-3}l - 1$. Mas se $k = 2^{n-3}l$ e $l = 2l'$, então $m = 1 + 2k = 1 + 2^{n-1}l' \Longrightarrow a^x = a^m = a \Longrightarrow xa = ax \Rightarrow G' = 1$. Portanto restam duas possibilidades:

Caso A: $m = 1 + 2^{n-2}l$, com $l = 2l' + 1$.

Neste caso temos que

$$a^x = a^m = a^{1+2^{n-2}l} = a^{1+2^{n-2}(2l'+1)} = a^{1+2^{n-2}}.$$

Se $n = 3$, então $o(a) = 2^{3-1} = 4$, $a^x = a^{1+2} = a^3 = a^{-1}$ e $x^2 \in \langle a \rangle$, pois $\left|\frac{G}{\langle a \rangle}\right| = 2$. Assim $x^2 \in \{1, a, a^2, a^3\}$.

• $x^2 = a \Longrightarrow G = \langle x, x^2 \rangle = \langle x \rangle$, que é um absurdo.

• $x^2 = a^3 = a^{-1} \Longrightarrow G = \langle x, a \rangle = \langle x, a^{-1} \rangle = \langle x, x^2 \rangle = \langle x \rangle$, que nos leva a outro absurdo.

• $x^2 = 1 \Longrightarrow G = \langle a, x;\ a^{2^{3-1}} = 1 = x^2,\ a^x = a^{-1} \rangle$, com isto G é do tipo (v).

• $x^2 = a^2 \Longrightarrow G = \langle a, x;\ a^{2^{3-1}} = a^4 = x^4 = 1,\ a^x = a^{-1} \rangle$, desta forma concluímos que G é do tipo (iv).

Agora se $n \geq 4$, então também temos $x^2 \in \langle a \rangle$, $o(a) = 2^{n-1}$ e $x^2 = a^{2r}$, pois se $x^2 = a^{2r+1}$ teríamos que $\langle x^2 \rangle = \langle a^{2r+1} \rangle = \langle a \rangle$ visto que $(2^{n-1}, 2r + 1) = 1$ e daí G $= \langle x \rangle$. Seja $b = a^{r(2^{n-3}-1)}$. Então pelo Lema anterior temos que

$$(xb)^2 = x^2b^2[b, x] = a^{2r}a^{2r(2^{n-3}-1)}b^{-1}x^{-1}bx = a^{r2^{n-2}}b^{-1}b^x$$

$$= a^{r2^{n-3}}a^{-r(2^{n-3}-1)}(a^{r(2^{n-3}-1)})^x = a^{r2^{n-2}-rs^{n-3}+r}(a^x)^{r(2^{n-3}-1)}$$

$$= a^{r2^{n-2}-rs^{n-3}+r}(a^m)^{r(2^{n-3}-1)} = a^{r2^{n-2}-r2^{n-3}+r+(1+2^{n-2})(r2^{n-3}-r)}$$

$$= a^{2^{n-5}} = 1,$$

pois $2n - 5 \geq n - 1$ uma vez que $n \geq 4$. Portanto,

$$G = \langle a, xb;\ a^{2^{n-1}} = 1 = (xb)^2,\ a^{xb} = (a^b)^x = a^x = a^{1+2^{n-2}} \rangle,$$

com isto temos que G é do tipo (vi).

Caso B: $m = 2^{n-2}l - 1$.

Subcaso B.1: Se $l = 2t$, então $m = 2^{n-1}t - 1$ e $a^x = a^m = a^{2^{n-1}t-1} = a^{-1}$.

Afirmação: $Z(G) = \langle a^{2^{n-2}} \rangle$.

De fato, $(a^{2^{n-2}})^x = (a^x)^{2^{n-2}} = (a^{-1})^{2^{n-2}} = (a^{2^{n-2}})^{-1} = a^{2^{n-2}}$. Portanto, $a^{2^{n-2}} \in Z(G)$ e com isto temos que $\langle a^{2^{n-2}} \rangle \leq Z(G)$. Reciprocamente, dado $g \in Z(G) < G = \langle a, x \rangle$ temos que $g = a^i x^j$, onde $i, j \in \mathbb{Z}$, e também $g^x = g = g^a$. Deste modo

$$(a^i x^j)^x = a^i x^j \Longrightarrow (a^i)^x x^j = a^i x^j \Longrightarrow (a^x)^i$$

$$= a^i \Longrightarrow a^{-i} = a^i \Longrightarrow a^{2i} = 1$$

e

$$(a^i x^j)^a = a^i x^j \Longrightarrow a^i (x^a)^j = a^i x^j \Longrightarrow a^{-1} x^j a = x^j,$$

mas $j = 2q$ ou $j = 2q + 1$.

• Se $j = 2q$, então $g = a^i x^j = a^i a^r = a^s$, pois $x^2 \in \langle a \rangle$.

• Se $j = 2q + 1$, então $g = a^i x^j = a^i x^{2q+1} = a^i a^r x = a^s x$ e com isto

$$g^a = g \Longrightarrow a^s x^a = a^s x \Longrightarrow x^a = x \Longrightarrow G' = 1.$$

Logo $j = 2q$, $g = a^s$ com $a^{2s} = 1$. Assim $2^{n-1} \mid 2s \Longrightarrow 2^{n-2} \mid s \Longrightarrow s = 2^{n-1}t \Longrightarrow g \in \langle a^{2^{n-2}} \rangle$.

Observe agora que $a^{x^2} = (a^x)^x = (a^{-1})^x = a \Longrightarrow x^2 \in Z(G)$. Portanto, $x^2 = 1$ ou $x^2 = a^{2^{n-2}}$, de modo que

$$G = \langle a, x;\ a^{2^{n-1}} = 1 = x^2;\ a^x = a^{-1} \rangle \ tipo\ (v)$$

ou

$$G = \langle a, x;\ a^{2^{n-1}} = 1,\ x^2 = a^{2^{n-2}};\ a^x = a^{-1} \rangle \ tipo\ (iv)$$

Subcaso B.2: Se $l = 2t + 1$, então $m = l2^{n-2} - 1 = t2^{n-1} - 1$. Como $x^2 \in \langle a \rangle$ temos que $x^2 = a^s$, mas se $2 \nmid s$ temos que $\langle a \rangle = \langle a^s \rangle \Longrightarrow a \in \langle x \rangle \Longrightarrow G = \langle x \rangle$, desta forma $s = 2r$ e $x^2 = a^s = a^{2r}$. Portanto,

$$x^2 = (x^2)^x = (a^{2r})^x = (a^x)^{2r} = (a^m)^{2r} = (a^{2^{n-2}-1})^{2r}$$

$$= a^{r2^{n-1}-2r} = a^{-2r}.$$

Assim

$$a^{2r} = x^2 = a^{-2r} \Longrightarrow a^{4r} = 1.$$

Logo, $o(a) = 2^{n-1} \mid 4r \Longrightarrow 2^{2^{n-2}} \mid 2r \Longrightarrow x^2 = a^{2r} = a^{2^{n-2}q} \in \langle a^{2^{n-2}} \rangle = \{1, a^{2^{n-2}}\}$. Se $x^2 = a^{2^{n-2}}$, então

$$(xa^{-1})^2 = xa^{-1}xa^{-1} = x^2x^{-1}a^{-1}xa^{-1} = x^2(a^{-1})^x a^{-1} = x^2(a^x)^{-1}a^{-1}$$

$$= x^2(a^m)^{-1}a^{-1} = a^{2^{n-2}}a^{-2^{n-2}+1}a^{-1} = 1.$$

Portanto $G = \langle a, xa^{-1};\ a^{2^{n-2}} = 1 = (xa^{-1})^2,\ a^{xa^{-1}} = (a^{2^{n-2}-1})^{a^{-1}} = a^{2^{n-2}-1}\rangle$, tipo (vii). Finalmente, se $x^2 = 1$ temos $G = \langle a, x;\ a^{2^{n-2}} = 1 = x^2,\ a^x = a^{2^{n-2}-1}\rangle$, tipo (vii). □

3.1.2 O Primeiro Teorema de Kuzennyi - Pylaev

Agora utilizaremos os resultado estudados anteriormente para demonstrar o Primeiro Teorema de Kuzennyi - Pylaev. Começamos definindo o conceito de base de Sylow.

Definição 24. *Seja G um grupo finito, com $|G| = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$. Dados $P_i \in Syl_{p_i}G$, dizemos que o conjunto $\{P_1, P_2, \dots, P_n\}$ é uma **Base de Sylow** para G se $P_iP_j = P_jP_i$ para todos $i, j \in \{1, 2, \dots, n\}$. Observe que $P_iP_j = P_jP_i$ se e somente se P_iP_j é um subgrupo de G.*

Lema 3.1.2. *Seja G um grupo finito e solúvel, então G possui uma Base de Sylow.*

Demonstração. Escreva $|G| = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$, fixe p_i e defina $p_i' = \prod_{j\neq i} p_j^{\alpha_j}$. Então, $|G| = p_i'p_i^{\alpha_1}$ e $(p_i', p_i^{\alpha_1}) = 1$, pelo Teorema de P. Hall, existe $Q_i \leq G$ tal que $|Q_i| = p_i'$. Seja $P_j = \bigcap_{i\neq j} Q_i$. Então como $|G : Q_i| = \prod_{i\neq j} p_i^{\alpha_i}$ obtemos que $|G : P_j| = \prod_{i\neq j} p_i^{\alpha_i}$ e portanto $|P_j| = p_j^{\alpha_j}$, assim $P_j \in Syl_{p_j}G$. Seja $K = \bigcap_{i,j\neq k} Q_k$. Então P_i,$P_j \subseteq K$ e $|K| = p_i^{\alpha_i}p_j^{\alpha_j}$, pois $|G : K| = \prod_{i,j\neq k} p_k^{\alpha_k}$. Por outro lado, $|P_iP_j| = \frac{|P_i||P_j|}{|P_i \cap P_j|} = |P_i||P_j| = p_i^{\alpha_i}p_j^{\alpha_j} = |K|$. Logo, $P_iP_j = K = P_jP_i$. □

Teorema 3.1.1 (**Primeiro Teorema de Kuzennyi - Pylaev**). *Um grupo finito G contêm um subgrupo cíclico maximal se e somente se é um dos seguintes tipos:*

i) $G = P \times \langle a_1\rangle$, onde $\langle a_1\rangle$ é um grupo cíclico qualquer e P é um p-subgrupo de Sylow de G de um dos tipos indicados na Proposição 3.1.1;

ii) $G = (\langle a_2\rangle \rtimes P) \times \langle a_1\rangle$, onde $\langle a_1\rangle$ é um grupo cíclico qualquer que é um subgrupo de Hall de G. P é um p-subgrupo de Sylow de G de um dos tipos indicados na Proposição 3.1.1, $\langle a_2\rangle \rtimes P$ não é nilpotente, e $C_P(\langle a_2\rangle)$ é um subgrupo cíclico de índice p em P;

iii) $G = (P \rtimes \langle a_2 \rangle) \times \langle a_1 \rangle$*, onde* $\langle a_1 \rangle$ *é um grupo cíclico qualquer que é um subgrupo de Hall de* G*, e* $G_1 = P \rtimes \langle a_2 \rangle$ *é um grupo não-nilpotente satisfazendo a seguinte condição:* P *é um p-subgrupo de Sylow de* G_1*,* $C_P(\langle a_2 \rangle) \geq \Phi(P)$*, e* $C_P(\langle a_2 \rangle)$ *é um subgrupo cíclico normal em* G_1 *tal que*

$$\frac{\langle a_2 \rangle C_P(\langle a_2 \rangle)}{C_P(\langle a_2 \rangle)} \ll \frac{G_1}{C_P(\langle a_1 \rangle)}$$

.

Demonstração. ($\Longrightarrow$) Seja G um grupo finito e $A \ll G$ cíclico, então pela Proposição 2.5.1 G é solúvel. Portanto, $|G : A| = p^\alpha$ e existe uma base de Sylow $P_1, P_2, \ldots, P_n, P$ para G com $p_i \neq p$ e $p_i \neq p_j$ para $i \neq j$.

Afirmação 1: Podemos supor que $P_1, P_2, \ldots, P_n \leq A$.

De fato, para cada p_i existe um único p_i-subgrupo de Sylow de A, digamos que $Syl_{p_i}A = \{P_i^*\}$. Agora, como $|G : A| = p^\alpha$, p_i não divide $|A : P_i^*|$ e

$$|G : P_i^*| = |G : A||A : P_i^*|,$$

temos que p_i não divide $|G : P_i^*|$ e assim $P_i^* \in Syl_{p_i}G$. Claramente temos que $P_i^*P_j^* = P_j^*P_i^*$, pois A é abeliano e P_i^*, $P_j^* \leq A$ e como $P_i^* \in Syl_{p_i}G$ existem $g_i \in G$ tais que $P_i^* = P_i^{g_i}$.

Como $P_i^* \trianglelefteq A$ e $P_i^* \cap P_j^* = 1$ temos $H = P_1^*P_2^* \ldots P_n^* \leq A$ com $|H| = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, onde $p_i^{\alpha_i}$ é a maior poetência de p_i que divide $|G|$. Agora, $|P| = p^\beta$, onde p^β é a maior potência de p que divide $|G|$ e $P \cap H = 1$, pois $(|H|, |P|) = 1$. Logo

$$|PH| = \frac{|P||H|}{|H \cap P|} = |P||H| = |G|.$$

Portanto, $G = PH = PA$, já que $PH \subseteq G$ e $H \leq A$.

Já sabemos que $P_i^*P_j^* = P_j^*P_i^*$ e que $P_i^* = P_i^{g_i}$, como $G = AP$ existem $a_i \in A$ e $x_i \in P$ tais que $g_i = x_ia_i$. Observe que $P_i^* = P_i^{x_ia_i} \iff (P_i^*)^{a_i^{-1}} = P_i^{x_i} \iff P_i^* = P_i^{x_i}$. Daí,

$$P_i^*P = P_i^{x_i}P = (P_iP)^{x_i} = (PP_i)^{x_i} = PP_i^{x_i} = PP_i^*.$$

Logo, $P_1^*, P_2^*, \ldots, P_n^*, P$ é uma base de Sylow para G com $P_i \leq A$, $i = 1, 2, \ldots, n$.

Defina $\langle a_1\rangle$ como o produto direto de todos os subgrupos de Sylow de G contidos em A que são fatores diretos de G, isto é, $\langle a_1\rangle = P_{i_1} \times P_{i_2} \times \ldots \times P_{i_s}$, onde para cada P_{i_j} existe $N_{i_j} \trianglelefteq G$ tal que $N_{i_j} \cap P_{i_j} = 1$ e $G = P_{i_j} \times N_{i_j}$. Observe que isto só faz sentido se P_{i_j} for normal em G, $\langle a_1\rangle$ é um subrupo cíclico normal de G e que $\langle a_1\rangle$ pode ser trivial. Seja

$$G_1 = \bigcap_j N_{i_j}.$$

Então G_1 é subgrupo normal de G. Como $(|G : N_{i_j}|, |G : N_{i_k}|) = 1$ pelo Teorema de Poincarré,

$$|G : G_1| = |G : N_{i_1}||G : N_{i_2}| \ldots |G : N_{i_s}| = p_{i_1}^{\alpha_{i_1}} p_{i_2}^{\alpha_{i_2}} \ldots p_{i_s}^{\alpha_{i_s}} = |\langle a_1\rangle|,$$

e como $p_{i_j}^{\alpha_{i_j}}$ é a maior potência de p_{i_j} que divide $|G|$ temos que $(|G_1|, |\langle a_1\rangle|) = 1$ e portanto $G_1 \cap \langle a_1\rangle = 1$. Assim, como $G_1\langle a_1\rangle \subseteq$ G e

$$|G_1\langle a_1\rangle| = \frac{|G_1||\langle a_1\rangle|}{|G_1 \cap \langle a_1\rangle|} = |G_1||\langle a_1\rangle| = |G|,$$

concluímos que $G = G_1\langle a_1\rangle$, $\langle a_1\rangle \trianglelefteq G$, $G_1 \trianglelefteq G$ e $\langle a_1\rangle \cap G_1 = 1$. Assim $G = G_1 \times \langle a_1\rangle$. Agora, $A = G_1\langle a_1\rangle \cap A$ e pela Identidade de Dedekind

$$A = (G_1\langle a_1\rangle) \cap A = (G_1 \cap A)\langle a_1\rangle = A_1\langle a_1\rangle,$$

onde $A_1 \trianglelefteq A$, $\langle a_1\rangle \trianglelefteq A$ e $A_1 \cap \langle a_1\rangle = 1$. Logo,

$$A = A_1 \times \langle a_1\rangle,$$

onde $A_1 = G_1 \cap A$ é cíclico, pois $A_1 \leq A$ e A é cíclico.

Afirmação 2: P $\leq G_1$ e $A_1 \lessdot G_1$.
De fato, como $G_1 \trianglelefteq G$, $|G : G_1| = |\langle a_1\rangle| = p_{i_1}^{\alpha_{i_1}} p_{i_2}^{\alpha_{i_2}} \ldots p_{i_s}^{\alpha_{i_s}}$ e dado $\widetilde{P} \in Syl_pG_1$ temos que $\widetilde{P} \in Syl_pG$ e daí existe $g \in G$ tal que $P = \widetilde{P}^g \leq G_1$ já que $\widetilde{P} \subseteq G_1 \trianglelefteq G$. Agora, se existir $\widetilde{A_1}$ tal que $A_1 < \widetilde{A_1} < G_1$, então

$$A = A_1 \times \langle a_1\rangle < \widetilde{A_1} \times \langle a_1\rangle < G_1 \times \langle a_1\rangle = G.$$

O que contradiz o fato de $A \lessdot G$. Logo, a Afirmação é verdadeira.

Seja $\langle a_2\rangle$ um subgrupo de Hall de A_1 com ordem relativamente prima com p. Observe que se $Q \in Syl_q A_1$ com $q \neq p$, então $q \nmid |G_1 : A_1| = p^\beta$ e $q \nmid |G : G_1| = p_{i_1}^{\alpha_{i_1}} p_{i_2}^{\alpha_{i_2}} \dots p_{i_s}^{\alpha_{i_s}}$, pois cada p_{i_j} aparece no produto com sua maior potência que divide a ordem de G. Portanto, $Q \in Syl_q\, G$, como é óbvio que dados primos q, $\overline{q}$ distintos $Q \cap \overline{Q} = 1$, $Q \trianglelefteq A_1$ e $\overline{Q} \trianglelefteq A_1$, concluímos que $\langle a_2\rangle$ é o produto direto de todos os subgrupos de Sylow de G contidos em A_1 para primos diferentes de p.

Caso 1: $\langle a_2\rangle = 1$.

Se $\langle a_2\rangle = 1$, então G_1 é um p-grupo, pois $|G_1| = |G_1 : A_1||A_1| = p^\beta p^\gamma$ e pela Afirmação 2, $P \leq G_1$. Portanto, $P = G_1$ e $A_1 \ll G_1 = P$, onde A_1 é cíclico. Assim, temos que $G_1 = P$, onde P é um grupo de um dos tipos da Proposição 3.1.1. Logo, $G = G_1 \times \langle a_1\rangle = P \times \langle a_1\rangle$ é do tipo (i) do Teorema.

Caso 2: $\langle a_2\rangle \neq 1$.

Afirmação 3: $G_1 = \langle a_2\rangle P = A_1 P$.

De fato, $A_1 = G_1 \cap A$ e $(|G : G_1|, |G : A|) = 1$, então pelo Exemplo 2,

$$|G : G_1||G_1 : A_1| = |G : A_1| = |G : G_1||G : A|.$$

Portanto $|G : G_1| = |G : A| = p^\alpha$, daí, $|G_1 : \langle a_2\rangle| = p^{\alpha+\beta}$. Por outro lado, $(|\langle a_2\rangle|, |P|) = 1$, e deste modo $|G_1| = |\langle a_2\rangle||P| = |\langle a_2\rangle P|$. Logo $G_1 = \langle a_2\rangle P = A_1 P$.

Escreva $\langle a_2\rangle = \langle a_2^*\rangle \times \langle a_2^0\rangle$, onde $\langle a_2^*\rangle$ é o produto direto de todos os subgrupos $Q \in Syl_q G$ contidos em A_1, $q \neq p$, com $Q \trianglelefteq G_1$ (característico) e portanto $Q \trianglelefteq G$, e $\langle a_2^0\rangle$ é o produto direto de todos os subgrupos $\overline{Q} \in Syl_{\overline{q}}\, G$ contidos em A_1, $\overline{q} \neq p$, com $\overline{Q} \ntrianglelefteq G_1$.

Dado um fator Q de $\langle a_2^0\rangle$ sabemos que $Q \trianglelefteq A_1$, pois A_1 é cíclico. Assim, $N_{G_1}(Q) \supseteq A_1$ e como $A_1 \ll G_1$, $Q \ntrianglelefteq G_1$, concluímos que $N_{G_1}(Q) = A_1$. Por outro lado, temos que

$$A_1 \subseteq C_{G_1}(Q) \subseteq N_{G_1}(Q) = A_1.$$

Portanto, $N_{G_1}(Q) = C_{G_1}(Q)$, pelo Teorema de Burnside-Transfer existe $H_Q \trianglelefteq G_1$ tal que $H_Q \cap Q = 1$ e $G_1 = QH_Q$. Observe que P, $\langle a_2^*\rangle \leq H_Q$ para todo fator Q de $\langle a_2^0\rangle$ e portanto $\langle a_2^*\rangle P \leq N$, onde $N = \bigcap_Q H_Q \trianglelefteq G$.

Como $(|G_1 : H_Q|, |G_1 : H_{\overline{Q}}|) = (|Q|, |\overline{Q}|) = 1$, pelo Teorema de Poincaré obtemos

$$|G_1 : N| = \prod_Q |G_1 : H_Q| = |\langle a_2^0 \rangle|.$$

Portanto, $|G_1| = |N||\langle a_2^0 \rangle| = |N\langle a_2^0 \rangle|$, pois $N \cap \langle a_2^0 \rangle = 1$. Logo $G_1 = N\langle a_2^0 \rangle$

Afirmação 4: $N = \langle a_2^* \rangle P$.

De fato, mostramos na Afirmação 3 que $G_1 = \langle a_2 \rangle P$. Portanto,

$$G_1 = \langle a_2 \rangle P = P\langle a_2 \rangle = P\langle a_2^* \rangle \langle a_2^0 \rangle = \langle a_2^* \rangle P \langle a_2^0 \rangle,$$

pois $\langle a_2^* \rangle \trianglelefteq G_1$, e $|G_1 : \langle a_2^* \rangle P| = |\langle a_2^0 \rangle| = |G_1 : N|$, daí como $\langle a_2^* \rangle P \leq N$ concluímos que $N = \langle a_2^* \rangle P$.

Pela Afirmação 3

$$G_1 = \langle a_2 \rangle P = P\langle a_2 \rangle = P\langle a_2^* \rangle \langle a_2^0 \rangle = \langle a_2^* \rangle P \langle a_2^0 \rangle,$$

onde $N = \langle a_2^* \rangle P \trianglelefteq G_1$ e $\langle a_2^* \rangle P \cap \langle a_2^0 \rangle = 1$. Logo $G_1 = (\langle a_2^* \rangle P) \rtimes \langle a_2^0 \rangle$.

Vamos considerar dois subcasos:

Subcaso 2.1: $\langle a_2^* \rangle$ é fator direto de G_1.

Neste caso todos os subgrupos de Sylow de $\langle a_2^* \rangle$ são subgrupos de Sylow de G que são fatores diretos de G. Portanto, $\langle a_2^* \rangle \leq \langle a_1 \rangle$ mas $\langle a_2^* \rangle \leq G_1$. Assim, $\langle a_2^* \rangle = 1$, pois $G_1 \cap \langle a_1 \rangle = 1$ e $\langle a_2^* \rangle \leq G_1$. Logo, $P = N \trianglelefteq G_1$ e

$$G_1 = P \rtimes \langle a_2^0 \rangle = P \rtimes \langle a_2 \rangle.$$

Subcaso 2.2: $\langle a_2^* \rangle$ não é fator direto de G_1.

Neste caso, $\langle a_2^* \rangle \neq 1$ e $C_{G_1}(\langle a_2^* \rangle) = A_1$, pois $\langle a_2^* \rangle \leq A_1$ e A_1 é cíclico maximal em G_1. Portanto, $C_{G_1}(\langle a_2^* \rangle) = A_1$ ou $C_{G_1}(\langle a_2^* \rangle) = G_1$. Suponha que $C_{G_1}(\langle a_2^* \rangle) = G_1$. Então $\langle a_2^* \rangle \leq Z(G_1)$ e como $\langle a_2^* \rangle \trianglelefteq G_1$ com $(|\langle a_2^* \rangle|, |G_1 : \langle a_2^* \rangle|) = 1$ o Teorema de Schur-Zassenhaus garante que existe $L \leq G_1$ tal que $G_1 = \langle a_2^* \rangle L$ com $\langle a_2^* \rangle \cap L = 1$. Como $\langle a_2^* \rangle \leq Z(G_1)$ temos que $L \trianglelefteq G_1$ e daí $\langle a_2^* \rangle$ é fator direto de G_1 (Absurdo!). Logo, $C_{G_1}(\langle a_2^* \rangle) = A_1$.

Vejamos agora que $A_1 \trianglelefteq G_1$, pois $C_{G_1}(\langle a_2^* \rangle) \trianglelefteq G_1$ e

$$A_1 = C_{G_1}(\langle a_2^* \rangle) \leq N_{G_1}(\langle a_2^* \rangle) = G_1.$$

Observe que todo subgrupo de Sylow de A_1 é normal (característico), portanto normal em G_1 (característico) e desta forma normal em G. Logo $\langle a_2^* \rangle = \langle a_2 \rangle$, $\langle a_2^0 \rangle = 1$, $\langle a_2 \rangle \trianglelefteq G_1$ e

$$G_1 = \langle a_2 \rangle \rtimes P.$$

Daí,

$$G_1 = P \rtimes \langle a_2 \rangle \quad ou \quad G_1 = \langle a_2 \rangle \rtimes P.$$

Afirmação 5: Em qualquer um dos casos acima G_1 é não-nilpotente.
Se G_1 for nilpotente, pelo Teorema de Caracterização dos Grupos Nilpotentes Finitos $G_1 = P \times Q_1 \times \ldots \times Q_r$, onde $r \geq 1$ já que estamos no caso em que $\langle a_2 \rangle \neq 1$. Assim, $G = P \times Q_1 \times \ldots \times Q_r \times \langle a_1 \rangle$ e portanto $Q_i \leq A$, $Q_i \in Syl_{q_i} G$ e Q_i é fator direto de G. Absurdo, pois todos os subgrupos de Sylow de G contidos em A que são fatores diretos de G estão contidos em $\langle a_1 \rangle$.

Afirmação 6: $C_{G_1}(\langle a_2 \rangle) = A_1 = \langle a_2 \rangle \times C_P(\langle a_2 \rangle)$.
Já sabemos que A_1 é cíclico, $\langle a_2 \rangle \leq A_1$ e $C_{G_1}(\langle a_2 \rangle) \geq A_1$, onde $A_1 \trianglelefteq G_1$. Portanto, $C_{G_1}(\langle a_2 \rangle) = A_1$ ou $C_{G_1}(\langle a_2 \rangle) = G_1$. Suponha que $C_{G_1}(\langle a_2 \rangle) = G_1$. Então $\langle a_2 \rangle \leq Z(G_1)$ e como $G_1 = \langle a_2 \rangle P$, concluímos que $P \trianglelefteq G_1$. Portanto, $G_1 = \langle a_2 \rangle \times P$ é o produto direto de seus subgrupos de Sylow, que é um absurdo. Logo, $C_{G_1}(\langle a_2 \rangle) = A_1$.
Observe que $\langle a_2 \rangle \trianglelefteq A_1$, $C_P(\langle a_2 \rangle) = C_{G_1}(\langle a_2 \rangle) \cap P$ é cíclico e normal em A_1, pois A_1 é cíclico, $\langle a_2 \rangle \cap C_P(\langle a_2 \rangle) \leq \langle a_2 \rangle \cap P = 1$ e

$$C_{G_1}(\langle a_2 \rangle) = A_1 = A_1 \cap G_1 = A_1 \cap (\langle a_2 \rangle P) = \langle a_2 \rangle (A_1 \cap P)$$

$$= \langle a_2 \rangle (C_{G_1}(\langle a_2 \rangle) \cap P) = \langle a_2 \rangle C_P(\langle a_2 \rangle) = \langle a_2 \rangle \times C_P(\langle a_2 \rangle)$$

Agora vamos considerar o caso em que G $= (\langle a_2\rangle \rtimes P) \times \langle a_1\rangle$, por construção $\langle a_1\rangle$ é subgrupo cíclico que é subgrupo de Hall de G, $P \in Syl_pG$, $\langle a_2\rangle \rtimes P$ é não-nilpotente e $C_P(\langle a_2\rangle)$ é cíclico. Falta mostrar que $C_P(\langle a_2\rangle) \lessdot P$.

Afirmação 7: $C_P(\langle a_2\rangle) \lessdot P$.
De fato, $C_P(\langle a_2\rangle) = C_{G_1}(\langle a_2\rangle) \cap P = A_1 \cap P \neq P$, pois se $A_1 \cap P = P$, então $P \leq A_1 \leq A$, mas $|G : A| = p^\alpha$ implica $P \not\leq A$, que é um absurdo. Seja $M \lessdot P$ tal que $C_P(\langle a_2\rangle) \leq M$, devemos mostrar que $C_P(\langle a_2\rangle) = M$. Como $C_P(\langle a_2\rangle) \leq M$, pela Afirmação 6 temos

$$A_1 = \langle a_2\rangle C_P(\langle a_2\rangle) \leq \langle a_2\rangle M \leq \langle a_2\rangle P = G_1.$$

Se $\langle a_2\rangle M = \langle a_2\rangle P$, então $P \leq \langle a_2\rangle M$ e para todo $x \in P$ existem $a \in \langle a_2\rangle$ e $m \in M < P$ tais que $x = am$. Daí $a \in P \cap \langle a_2\rangle$ e portanto $a = 1$. Logo, $x \in M$ e $M = P$ (Absurdo!). Como $A_1 \lessdot G_1$ concluímos que $\langle a_2\rangle C_P(\langle a_2\rangle) = A_1 = \langle a_2\rangle M$. Logo $M \leq A_1$ e como $M < P$ temos que

$$M \leq A_1 \cap P = C_P(\langle a_2\rangle).$$

Daí, $M = C_P(\langle a_2\rangle)$, $C_P(\langle a_2\rangle) <\cdot\, P$ e G é do tipo (ii) do Teorema.

Consideremos agora o caso em que $G = (P \rtimes \langle a_2\rangle) \times \langle a_1\rangle$. Temos que P é normal em G_1 e portanto normal em G, $A_1 = \langle a_2\rangle \times C_P(\langle a_2\rangle)$ e $C_P(\langle a_2\rangle) \neq P$, pois $P \not\leq A_1$.

Afirmação 8: $\Phi(P)C_P(\langle a_2\rangle) < P$.
É claro que $\Phi(P)C_P(\langle a_2\rangle) \leq P$. Suponha que $\Phi(P)C_P(\langle a_2\rangle) = P$. Então

$$P = \Phi(P)C_P(\langle a_2\rangle) \leq \langle \Phi(P), C_P(\langle a_2\rangle)\rangle \leq P$$

e portanto $P = \langle \Phi(P), C_P(\langle a_2\rangle)\rangle = \langle C_P(\langle a_2\rangle)\rangle = C_P(\langle a_2\rangle)$ (Absurdo!).
De modo análogo $\Phi(G_1)C_{G_1}(\langle a_2\rangle) < G_1$. Como $P \trianglelefteq G_1$ temos que $\Phi(P) \leq \Phi(G_1)$ e portanto $\Phi(P)C_{G_1}(\langle a_2\rangle) \leq \Phi(G_1)C_{G_1}(\langle a_2\rangle) < G_1$. Logo,

$$\Phi(G_1)C_{G_1}(\langle a_2\rangle) = A_1 = C_{G_1}(\langle a_2\rangle).$$

Com isto provamos que $\Phi(P) \leq C_P(\langle a_2\rangle) = C_{G_1}(\langle a_2\rangle) \cap P$. Como $\dfrac{P}{\Phi(P)}$ é p-abeliano elementar, concluímos que

$$\frac{C_P(\langle a_2\rangle)}{\Phi(P)} \trianglelefteq \frac{P}{\Phi(P)}.$$

Assim, pelo Teorema da Correspondência, $C_P(\langle a_1\rangle) \trianglelefteq P$ e portanto

$$N_{G_1}(C_P(\langle a_2\rangle)) \geq P.$$

Por outro lado, A_1 cíclico implica que $N_{G_1}(C_P(\langle a_2\rangle)) \geq A_1$, já que $C_P(\langle a_2\rangle) \leq A_1$ e então

$$G_1 = PA_1 = N_{G_1}(C_P(\langle a_2\rangle)).$$

Logo $C_P(\langle a_2\rangle) \trianglelefteq G_1$.
Finalmente, vamos mostrar que $\dfrac{\langle a_2\rangle C_P(\langle a_2\rangle)}{C_P(\langle a_2\rangle)} \lessdot \dfrac{G_1}{C_P(\langle a_2\rangle)}$. Claro que

$$\frac{A_1}{C_P(\langle a_2\rangle)} = \frac{\langle a_2\rangle C_P(\langle a_2\rangle)}{C_P(\langle a_2\rangle)} < \frac{G_1}{C_P(\langle a_2\rangle)}.$$

Seja $\overline{H} \lessdot \dfrac{G_1}{C_P(\langle a_2\rangle)}$ tal que $\dfrac{A_1}{C_P(\langle a_2\rangle)} \leq \overline{H}$. Pelo Teorema da Correspondência existe $H < G_1$ tal que $A_1 \leq H$ e $\overline{H} = \dfrac{H}{C_P(\langle a_2\rangle)}$, como A_1 é maximal em G_1 concluímos que $A_1 = H$ e portanto $\dfrac{\langle a_2\rangle C_P(\langle a_2\rangle)}{C_P(\langle a_2\rangle)} < \lessdot \dfrac{G_1}{C_P(\langle a_2\rangle)}$.

($\Longleftarrow$) Suponha que G é do tipo (i), isto é, $G = P \times \langle a_1\rangle$, onde P é um p-Subgrupo de Sylow de G de um dos tipos da Proposição 3.1.1 e $\langle a_1\rangle$ é um subgrupo cíclico qualquer. Seja $\langle a\rangle$ cíclico maximal em P. Então $A = \langle a\rangle \times \langle a_1\rangle$ é cíclico. Se $A \leq H \leq G$, então

$$\langle a\rangle = \langle a\rangle(P \cap \langle a_1\rangle) = P \cap (\langle a\rangle\langle a_1\rangle) = P \cap A \leq P \cap H \leq P.$$

Logo, $P \cap H = P$ ou $P \cap H = \langle a\rangle$.
Se $P \cap H = P$, então $P \leq H$ e portanto $G = \langle a\rangle P \leq H \leq G$. Assim, $H = G$.
Se $P \cap H = \langle a\rangle$, então

$$H = G \cap H = (\langle a_1\rangle P) \cap H = \langle a_1\rangle(P \cap H)$$

$$= (\langle a_1\rangle\langle a\rangle) = A.$$

Logo, A é cíclico maximal em G.

Suponha agora que G é do tipo (ii), ou seja, $G = (\langle a_2\rangle \rtimes P) \times \langle a_1\rangle$, onde $\langle a_1\rangle$ é um grupo cíclico que é subgrupo de Hall de G, P é um p-Subgrupo de Sylow de G de um dos tipos da Proposição 3.1.1, $\langle a_2\rangle \rtimes P$ é não-nilpotente e $C_P(\langle a_2\rangle)$ é cíclico maximal em P.
Seja $A = \langle a_2\rangle \times C_P(\langle a_2\rangle) \times \langle a_1\rangle$. Observe que $(|\langle a_2\rangle|, |C_P(\langle a_2\rangle)|) = 1 = (|\langle a_2\rangle C_P(\langle a_2\rangle)|, |\langle a_1\rangle|)$. Logo A é cíclico em G. Mostraremos agora que A é maximal em G e para isto seja $A \leq H \leq G$. Então

$$A \cap P = (\langle a_2\rangle C_P(\langle a_2\rangle)\langle a_1\rangle) \cap P = C_P(\langle a_2\rangle)((\langle a_2\rangle\langle a_1\rangle) \cap P)$$

$$= C_P(\langle a_2\rangle) \leq H \cap P \leq P$$

Assim, $H \cap P = C_P(\langle a_2\rangle)$ ou $H \cap P = P$. Se $H \cap P = P$, então $P \leq H$ e portanto $H = G$, pois

$$G = \langle a_2\rangle P\langle a_1\rangle \leq H.$$

Se $H \cap P = C_P(\langle a_2\rangle)$, então

$$A = \langle a_2\rangle C_P(\langle a_2\rangle)\langle a_1\rangle = \langle a_2\rangle(H \cap P)\langle a_1\rangle = (\langle a_2\rangle P\langle a_1\rangle) \cap H = H.$$

Logo, A é cíclico maximal em G.
Finalmente, considere G do tipo (iii), isto é, $G = (P \rtimes \langle a_2\rangle) \times \langle a_1\rangle$, onde $\langle a_1\rangle$ é um grupo cíclico que é um subgrupo de Hall de G, $P \rtimes \langle a_2\rangle$ é não-nilpotente satisfazendo a seguinte condição: P é um p-subgrupo de Sylow de G_1, $C_P(\langle a_2\rangle) \geq \Phi(P)$ e $C_P(\langle a_2\rangle)$ é um subgrupo cíclico normal de G_1 tal que

$$\frac{\langle a_2\rangle C_P(\langle a_2\rangle)}{C_P(\langle a_2\rangle)} \lessdot \frac{G_1}{C_P(\langle a_1\rangle)}.$$

Seja $A = C_P(\langle a_2\rangle) \times \langle a_2\rangle \times \langle a_1\rangle$. Então A é cíclico, pois $(|\langle a_2\rangle|, |C_P(\langle a_2\rangle)|) = 1 = (|\langle a_2\rangle C_P(\langle a_2\rangle)|, |\langle a_1\rangle|)$. Vamos mostrar agora que A é maximal, para tanto tome $A \leq H \leq G$, então definindo $G_1 = (P \rtimes \langle a_2\rangle)$ obtemos

$$\frac{\langle a_2\rangle C_P(\langle a_2\rangle)}{C_P(\langle a_2\rangle)} \leq \frac{H \cap G_1}{C_P(\langle a_2\rangle)} \leq \frac{G_1}{C_P(\langle a_2\rangle)}.$$

Portanto, $H \cap G_1 = \langle a_2\rangle C_P(\langle a_2\rangle)$ ou $H \cap G_1 = G_1$.
Se $H \cap G_1 = G_1$, então $G_1 \leq H$ e como $A \leq H$ temos que $PA \leq H$. Assim $H = G$, pois

$$G = P\langle a_2\rangle\langle a_1\rangle = PC_P(\langle a_2\rangle)\langle a_2\rangle\langle a_1\rangle = PA \leq H \leq G.$$

Se $H \cap G_1 = \langle a_2 \rangle C_P(\langle a_2 \rangle)$ então $H \cap G_1 = A \cap G_1$, pois

$$H \cap G_1 = \langle a_2 \rangle C_P(\langle a_2 \rangle) \leq A \cap G_1 \leq H \cap G_1.$$

Agora,

$$H = G \cap H = (G_1\langle a_1 \rangle) \cap H = (G_1 \cap H)\langle a_1 \rangle = (G_1 \cap A)\langle a_1 \rangle = (G_1\langle a_1 \rangle) \cap A = A.$$

Com isto provamos que A é maximal.

□

3.2 Grupos Finitos com no Máximo um Subgrupo não Cíclico Maximal

3.2.1 Classificação dos p-grupos com no máximo um subgrupo não cíclico maximal

Assim como fizemos anteriormente, começamos demonstrando um lema de classificação dos p-grupos com no máximo um subgrupo não cíclio maximal.

Lema 3.2.1. *Um p-grupo contêm no máximo um subgrupo não cíclico maximal se e somente se é um dos seguintes grupos:*

i) $G = \langle a;\ a^{p^n} = 1 \rangle$, $n \geq 1$;

ii) $G = \langle a, b;\ a^{p^{n-1}} = 1,\ b^p = 1,\ bab^{-1} = a \rangle$, $n \geq 2$;

iii) $G = \langle a, b;\ a^{p^{n-1}} = 1,\ b^p = 1,\ bab^{-1} = a^{1+p^{n-2}} \rangle$, $n \geq 3$, p *é ímpar;*

iv) $G = \langle a, b;\ a^4 = 1,\ b^2 = a^2,\ bab^{-1} = a^{-1} \rangle$;

v) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = 1,\ bab^{-1} = a^{1+2^{n-2}} \rangle$, $n \geq 4$.

Demonstração. Se G é um p-grupo cíclico, então G é do tipo (i). Sejam G um grupo não cíclico não trivial e $M_1 \lessdot G$. Considere $x \in G - M_1$, como G é não cíclico temos que $\langle x \rangle < G$ e com isto existe $M_2 \lessdot G$ tal que $x \in M_2$. Assim, se G é um p-Grupo com no máximo um subgrupo não cíclico maximal, então G contém um subgrupo cíclico maximal

e portanto G é um dos grupos da Proposição 3.1.1. Logo, é suficiente determinar quais dos grupos da Proposição 3.1.1 que contêm no máximo um subgrupo não cíclico maximal.

($\Longrightarrow$) Basta mostrar que os seguintes grupos contém pelo menos dois subgrupos não cíclicos maximais:

1) $G = \langle a, b;\ a^{2^{n-1}} = 1 = b^2,\ a^b = a^{-1}\rangle$, $n \geq 3$;

2) $G = \langle a, b;\ a^{2^{n-1}} = 1 = b^2,\ a^b = a^{-1+2^{n-2}}\rangle$, $n \geq 4$;

3) $G = \langle a, b;\ a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}},\ a^b = a^{-1}\rangle$, $n > 3$.

Para tanto, provaremos que $M_1 = \langle a^2\rangle\langle b\rangle$ e $M_2 = \langle a^2\rangle\langle ab\rangle$ são maximais e não cíclicos. Observe que $|G : \langle a^2\rangle| = 4$, $b \notin \langle a^2\rangle$ e $ab \notin \langle a^2\rangle$. Assim, $|G : M_1| = |G : M_2| = 2$ e portanto M_1 e M_2 são maximais.

Caso 1) $G = \langle a, b;\ a^{2^{n-1}} = 1 = b^2,\ a^b = a^{-1}\rangle$, $n \geq 3$.

Suponha que M_1 é cíclico. Então,

$$a^2b = ba^2 = a^{-2}b \qquad \therefore a^4 = 1.$$

Logo, $o(a) \mid 4$ e assim $n = 3$. Agora, basta observar que $M_1 = \{1, a^2, b, a^2b\}$ é não cíclico, feito isto chegamos em um absurdo. Suponha agora que M_2 é cíclico e então,

$$a^2ab = aba^2 = a^{-1}b \qquad \therefore a^4 = 1.$$

Portanto, $o(a) \mid 4$ e assim $n = 3$. Assim como no caso anterior, basta observar que $M_2 = \{1, a^2, ab, a^3b\}$ é não cíclico.

Caso 2) $G = \langle a, b;\ a^{2^{n-1}} = 1 = b^2,\ a^b = a^{-1+2^{n-2}}\rangle$, $n \geq 4$.

Suponha que M_1 é cíclico. Então,

$$a^2b = ba^2 = a^{-2+2^{2-1}}b \qquad \therefore a^{-4+2^{n-1}} = 1.$$

Logo, $o(a) = 2^{n-1} \mid (2^{n-1} - 4)$ e assim $n = 3$, que é um absurdo. Suponha que M_2 é cíclico e então,

$$a^2ab = aba^2 = aa^{-2+2^{n-1}}b \qquad \therefore a^{-4+2^{n-1}} = 1.$$

Portanto, $o(a) = 2^{n-1} \mid (2^{n-1} - 4)$ e assim $n = 3$ (Contradição).

Caso 3) $G = \langle a, b;\ a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}},\ a^b = a^{-1}\rangle$, $n > 3$.

Suponha que M_1 é cíclico. Então,

$$a^2b = ba^2 = a^{-2}b \qquad \therefore a^4 = 1.$$

Logo, $o(a) \mid 4$ e assim $n = 3$, que não ocorre já que $n > 3$. Suponha que M_2 é cíclico. Então,

$$a^2ab = aba^2 = a^{-1}b \qquad \therefore a^4 = 1.$$

Portanto, $o(a) \mid 4$ e assim $n = 3$ (Absurdo!).

($\Longleftarrow$) Devemos mostrar que todos os grupos listados no Lema contêm no máximo um subgrupo maximal não cíclico . É claro grupos do tipo (i) ou do tipo (ii) com $n = 2$ satisfazem as hipóteses do Lema.

Seja $G = \langle a, b;\ a^4 = 1,\ b^2 = a^2,\ bab^{-1} = a^{-1}\rangle$, tipo (iv). Tome H subgrupo próprio de G, então $|H| = 1$, 2 ou 4. Se $|H| = 1$ ou 2, então H é cíclico. Suponha $|H| = 4$:

1) Se $a \in H$, então $H = \langle a\rangle$;

2) Se $a^3 \in H$, então $H = \langle a^3\rangle = \langle a\rangle$;

3)Se $b \in H$, então $H = \langle b\rangle$;

4)Se $b^3 \in H$, então $H = \langle b^3\rangle = \langle b\rangle$.

Como $G = \{1,\ a,\ a^2,\ a^3,\ b,\ b^3,\ ab,\ a^3b\}$ temos que se $a \neq H$ e $b \neq H$, então $H = \{1, a^2, ab, a^3b\} = \langle ab\rangle$. Assim, todo subgrupo próprio de G é cíclico e, em particular, todo subgrupo maximal de G é cíclico.

Suponha agora que G é do tipo (ii) com $n \geq 3$, do tipo (iii) ou do tipo (v). Então, $M_1 = \langle a^p\rangle\langle b\rangle$ é não cíclico maximal e $M_2 = \langle a\rangle$ é cíclico maximal. Seja M um subgrupo maximal de G diferente de M_1 e de M_2, é claro que todo elemento de M pode ser escrito da forma $a^\alpha b^\beta$, onde $\alpha \geq 0$ e $\beta \geq 0$.

Afirmação: Existe $d \in M$ tal que $d = a^\alpha b$, com $(\alpha, p) = 1$.

De fato, observe que $\langle a^p\rangle \overset{\lhd}{_{car}} M_2 \lhd G$, pois M_2 é maximal em um p-grupo (nilpotente) e $\langle a^p\rangle = \Phi(M_2)$. Assim, $\langle a^p\rangle \lhd G$, onde $\langle a^p\rangle = \Phi(M_2) \leq \Phi(G)$ e portanto $\langle a^p\rangle \leq M$ ($\langle a^p\rangle \lhd M$, pois $\langle a^p\rangle \lhd$ G). É claro que $\dfrac{G}{\langle a^p\rangle}$ tem ordem p^2, $\dfrac{G}{\langle a^p\rangle} = \langle \overline{a}, \overline{b}\rangle = \langle \overline{a}\rangle\langle \overline{b}\rangle$ e $\langle \overline{a}\rangle \cap \langle \overline{b}\rangle = 1$ (ou seja, $\dfrac{G}{\langle a^p\rangle} = \langle \overline{a}\rangle \times \langle \overline{b}\rangle$). Seja $\overline{M} = \dfrac{M}{\langle a^p\rangle}$. Então $\overline{M}$ é um subgrupo não

trivial e próprio de $\dfrac{G}{\langle a^p\rangle} = \overline{G}$. Portanto, todo elemento $d \in M - \langle a^p\rangle$ tem imagem da forma $\overline{a}^{\alpha}\overline{b}^{\beta}$, $0 \leq \alpha < p$ e $0 \leq \beta < p$, em $\overline{G}$.
Observe que se $\alpha = 0$, então $\overline{d} = \overline{b}^{\beta}$ com $0 \leq \beta < p$ e desse modo temos que

$$\beta = 0 \Longrightarrow \overline{d} = \overline{1} \Longrightarrow d \in \langle a^p\rangle.$$

Portanto, $\alpha \neq 0$. De modo análogo, se $\beta = 0$ então $\overline{d} = \overline{a}^{\alpha}$, onde $0 \leq \alpha < p$ e desta forma concluímos que

$$\alpha = 0 \Longrightarrow \overline{d} = \overline{1} \Longrightarrow d \in \langle a^p\rangle$$

Com isto mostramos que todo elemento $d \in M - \langle a^p\rangle$ tem imagem da forma $\overline{a}^{\alpha}\overline{b}^{\beta}$, $0 < \alpha < p$ e $0 < \beta < p$. Como $(p, \beta) = 1$ existem $r, s \in \mathbb{Z}$ tais que

$$rp + s\beta = 1 \Longrightarrow \alpha rp + \alpha s\beta = \alpha.$$

Assim, $x = \alpha s$ é solução da equação $\beta x \equiv \alpha \ (mod\ p)$. Pelo algoritmo da divisão existem $q, x_0 \in \mathbb{Z}$ tais que $x = qp + x_0$, $0 < x_0 < p$, e deste modo x_0 é solução da equação $\beta x \equiv \alpha \ (mod\ p)$ com $0 < x_0 < p$. Então $\overline{d} = \overline{d_0}^{\beta}$, onde $\overline{d_0} = \overline{a}^{x_0}\overline{b}$. Portanto, sem perda de generalidade, podemos escolher $d \in M - \langle a^p\rangle$ de modo que a imagem em $\overline{M}$ de d seja $\overline{d_0}$. Isto mosta que $\langle a^p\rangle\langle d\rangle = \langle a^p\rangle\langle a^{x_0}\rangle\langle b\rangle$.
Note que $(x_0, p) = 1$, pois $0 < x_0 < p$. Então $d = a^{sp}a^{x_0}b = a^{sp+x_0}b$, onde $(sp + x_0, p) = 1$. Trocando $sp + x_0$ por α obtemos o resultado desejado.

Vamos mostrar agora que $\langle d\rangle$ é maximal em G, isto é, $M = \langle d\rangle$. Primeiro mostraremos que para grupos do tipo (ii) com $n \geq 3$, tipo (iii) e tipo (v) temos que $a^p \in \langle d\rangle$.
Suponha G do tipo (ii) com $n \geq 3$. Como $ab = ba$ e $b^p = 1$ temos que

$$(a^{\alpha}b)^p = a^{\alpha p}b^p = (a^p)^{\alpha}.$$

Como $(\alpha, p) = 1$, então $(\alpha, o(a^p)) = 1$ e assim, existem $r, s \in \mathbb{Z}$ tais que $r\alpha + so(a^p) = 1$. Logo,

$$a^p = (a^p)^{r\alpha + so(a^p)} = (a^p)^{r\alpha} = (a^{\alpha}b)^{pr} \in \langle a^{\alpha}b\rangle = \langle d\rangle.$$

Suponha $G = \langle a, b;\ a^{p^{n-1}} = 1,\ b^p = 1,\ bab^{-1} = a^{1+p^{n-2}}\rangle$, $n \geq 3$, p é ímpar, tipo (iii). Então:

$$ba^pb^{-1} = (bab^{-1})^p = (a^{1+p^{n-2}})^p = a^{p+p^{n-1}} = a^p.$$

Assim, $\langle a^p \rangle \leq Z(G)$ e portanto $Cl(G) \leq 2$, pois $|G : Z(G)| = 1$, p ou p^2. Logo, pelo Lema 3.1.1

$$(a^\alpha b)^p = a^{\alpha p} b^p [b,a]^{\binom{p}{2}} = a^{\alpha p}[b^p, a]^{\frac{p-1}{2}} = a^{\alpha p}.$$

Novamente, como $(\alpha, p) = 1$ temos que $a^p \in \langle a^\alpha b \rangle$.

Finalmente, se G é do tipo (v), temos:

$$(a^\alpha b)^2 = a^\alpha b a^\alpha b = a^\alpha a^{\alpha(1+2^{n-2})} b^2 = a^{2\alpha(1+2^{n-3})} = (a^2)^{\alpha(1+2^{n-3})}.$$

Como $(\alpha, 2) = 1$ e $(2, 1 + 2^{n-3}) = 1$, concluímos que $a^2 \in \langle a^\alpha b \rangle$. Assim, $\langle a^p \rangle \leq \langle a^\alpha b \rangle$ e claramente $\langle a^\alpha b \rangle \neq \langle a^p \rangle$. Portanto $M = \langle a^\alpha b \rangle$, já que $|G : \langle a^p \rangle| = p^2$. Isto prova que M é cíclico.

□

Corolário 3.2.1. *Todo subgrupo maximal de um p-grupo finito G é cíclico se e somente se é G um dos seguintes grupos:*

i) Cíclico;

ii) Grupo quatérnio;

iii) Abeliano elementar de ordem p^2.

Demonstração. ($\Longrightarrow$) Seja G um p-Grupo finito tal que todo subgrupo próprio de G é cíclico. Então, Todo subgrupo maximal de G é cíclico e portanto G é um dos grupos do Lema 3.2.1, mas provamos que se grupos do tipo (ii) com $n > 2$, tipo (iii) ou do tipo (v) do mesmo Lema contêm um subgrupo maximal não cíclico. Logo, G é um dos grupos listados acima.

($\Longleftarrow$) Imediato. □

3.2.2 O Segundo Teorema de Kuzennyi - Pylaev

Finalmente, encerramos este trabalho classificando os grupos finitos com no máximo um subgrupo não cíclio maximal.

Teorema 3.2.1 (**Segundo Teorema de Kuzennyi - Pylaev**). *Um grupo finito G contêm no máximo um subgrupo não cíclico maximal se e somente se é um dos seguintes grupos:*

i) G é um p-grupo de um dos tipos:

a) $\langle a; a^{p^n} = 1\rangle$, $n \geq 1$;

b) $\langle a, b;\ a^{p^{n-1}} = 1 = b^p,\ ba = ab\rangle$, $n \geq 2$;

c) $\langle a, b;\ a^{p^{n-1}} = 1 = b^p,\ bab^{-1} = a^{1+p^{n-2}}\rangle$, $n \geq 3$, p *impar*;

d) $\langle a, b;\ a^{2^{n-1}} = 1 = b^2,\ bab^{-1} = a^{1+2^{n-2}}\rangle$, $n \geq 4$;

e) Grupo quaternio;

ii) $G = \langle a_1\rangle$ *é um grupo cíclico finito que não é p-grupo;*

iii) $G = P \times \langle a_1\rangle$, *onde P é o grupo quaternio ou abeliano elementar de ordem p^2, e $\langle a_1\rangle$ é um subgrupo de Sylow de G;*

iv) $G = (\langle a_2\rangle \rtimes \langle a\rangle) \times \langle a_1\rangle$, *onde $\langle a\rangle$, $\langle a_1\rangle$ e $\langle a_2\rangle$ são subgrupos de Sylow de G, e $\langle a_2\rangle \rtimes \langle a\rangle$ é não-nilpotente tal que $C_{\langle a\rangle}(\langle a_2\rangle) = \langle a^p\rangle$ e $C_{\langle a_2\rangle}(\langle a\rangle) = \langle a_2^{p_2}\rangle$;*

v) $G = P \rtimes \langle a_2\rangle$, *onde P e $\langle a_2\rangle$ são subgrupos de Sylow de G, $C_P(\langle a_2\rangle) = \Phi(P)$, $C_P(\langle a_2\rangle)$ é cíclico normal de G tal que*

$$\frac{\langle a_2\rangle\Phi(P)}{\Phi(P)} \lessdot \frac{G}{\Phi(P)}.$$

Demonstração. ($\Longrightarrow$) Seja G um grupo finito com no máximo um subgrupo não cíclico maximal. Assim como feito no Lema anterior, G contém um subgrupo cíclico maximal e portanto G é um dos grupos do Teorema 3.1.1.

Caso 1: $G = P \times \langle a_1\rangle$, onde $\langle a_1\rangle$ é um subgrupo cíclico de G e P é um subgrupo de Sylow de G de um dos tipos da Proposição 3.1.1.

Se $\langle a_1\rangle = 1$, então G é um p-grupo com no máximo um subgrupo não cíclico maximal e assim, pelo Lema 3.2.1, G é do tipo (i) do Teorema.

Se $\langle a_1\rangle \neq 1$ e P é cíclico, então G é um grupo cíclico que não é p-grupo, isto é, G é do tipo (ii) do Teorema.

Se $\langle a_1\rangle \neq 1$ e P é não cilcio, então todo subgrupo maximal de P é cíclico, pois P está contido em um subgrupo maximal M_1 que é não cíclico e se $H \lessdot P$ é não cíclico, então $M_2 = H \times \langle a_1\rangle$ também é não cíclico. Logo, pelo Corolário 3.2.1, G é o grupo quatérnio

ou abeliano elementar de ordem p^2. Para que tenhamos G do tipo (iii) falta mostar que $\langle a_1\rangle$ é subgrupo de Sylow de G.

Suponha que $\langle a_1\rangle$ não é q-grupo e decomponha $\langle a_1\rangle = \langle a_1^0\rangle \times \langle a_1^*\rangle$, onde $\langle a_1^0\rangle$ e $\langle a_1^*\rangle$ são subgrupos de Hall de $\langle a_1\rangle$. Assim, $P\langle a_1^0\rangle$, $P\langle a_1^*\rangle$ estão contidos em maximais não cíclicos distintos, pois P é não cíclico. Logo G, é do tipo (iii) do Teorema.

Caso 2: $G = (\langle a_2\rangle \rtimes P) \times \langle a_1\rangle$, onde $\langle a_1\rangle$ é um subgrupo cíclico que é subgrupo de Hall de G, P é um subgrupo de Sylow de G de um dos tipos da Proposição 3.1.1, $\langle a_2\rangle \rtimes P$ é não nilpotente e $C_P(\langle a_2\rangle)$ é cíclico de índice p em P.

Observe que neste caso $\langle a_2\rangle \neq 1$, pois P é nilpotente e $\langle a_2\rangle \rtimes P$ é não nilpotente. Suponha que P é não cíclico. Então existe um subgupo maximal não cíclico M_1 que contém P. Como $|P : C_P(\langle a_2\rangle)| = p$, existe $b \notin C_P(\langle a_2\rangle)$. Então $(\langle a_2\rangle \rtimes \langle b\rangle) \times \langle a_1\rangle$ está contido em um subgrupo maximal não cíclico M_2 diferente de M_1, pois não contém P, pois $P \leq M_2 \Longrightarrow G = M_2$, fato este que nos leva a uma contradição visto de G contém no máximo um subgrupo não cíclico maximal.

Assim, $P = \langle a\rangle$ e portanto $G = (\langle a_2\rangle \rtimes \langle a\rangle) \times \langle a_1\rangle$, onde $\langle a\rangle$ é um subgrupo de Sylow de G, $C_{\langle a\rangle}(\langle a_2\rangle) = \langle a^p\rangle$, pois $|P : C_{\langle a\rangle}(\langle a_2\rangle)| = p$, e $\langle a_2\rangle \rtimes \langle a\rangle$ é não nilpotente. Vamos agora considerar dois subcasos conforme segue.

Subcaso 2.1: $\langle a_1\rangle \neq 1$.

Suponha que $\langle a_1\rangle$ não é um q-grupo. Então podemos decompor $\langle a_1\rangle = \langle a_1^0\rangle \times \langle a_1^*\rangle$, onde $\langle a_1^0\rangle$ e $\langle a_1^*\rangle)$ são subrupos de Hall não triais de $\langle a_1\rangle$. Deste modo existem subgrupos maximais M_1 e M_2 tais que $(\langle a_2\rangle \rtimes \langle a\rangle) \times \langle a_1^0\rangle \leq M_1$ e $(\langle a_2\rangle \rtimes \langle a\rangle) \times \langle a_1^*\rangle \leq M_2$, como $(\langle a_2\rangle \rtimes \langle a\rangle)$ é não abeliano concluímos que M_1 e M_2 são não cíclicos maximais. Logo $\langle a_1\rangle$ é um q-grupo que é subgrupo de Hall de G, portanto $\langle a_1\rangle$ é subgrupo de Sylow de G.

Suponha agora que $\langle a_2\rangle$ não é q'-grupo e decomponha $\langle a_2\rangle = \langle a_2^0\rangle \times \langle a_2^*\rangle$, onde $\langle a_2^0\rangle$ e $\langle a_2^*\rangle$ são subgrupos de Hall não triviais de $\langle a_2\rangle$.

Afirmação: $[a_2^0, a] \neq 1$ e $[a_2^*, a] \neq 1$.

De fato, se $[a_2^0, a] = 1$, então

$$G = (\langle a_2\rangle \rtimes \langle a\rangle) \times \langle a_1\rangle = ((\langle a_2^0\rangle \times \langle a_2^*\rangle) \rtimes \langle a\rangle) \times \langle a_1\rangle = (\langle a_2^*\rangle \rtimes \langle a\rangle) \times (\langle a_2^0\rangle \times \langle a_1\rangle)$$

Neste caso sendo $(\langle a_2^*\rangle \rtimes P)$ não abeliano existem maximais não cíclicos contendo cada um $(\langle a_2^*\rangle \rtimes P) \times \langle a_2^0\rangle$ e $(\langle a_2^*\rangle \rtimes P) \times \langle a_1\rangle$. Logo, $[a_2^0, a] \neq 1$ e de modo análogo $[a_2^*, a] \neq 1$.

Agora como $[a_2^0, a] \neq 1$ e $[a_2^*, a] \neq 1$, concluímos que $(\langle a_2^0\rangle \rtimes P) \times \langle a_1\rangle$ e $(\langle a_2^*\rangle \rtimes P) \times \langle a_1\rangle$ são não abelianos e assim existem maximais M_1 e M_2 que os contém separadamente e então M_1 e M_2 são maximais não cíclicos.

Com isto provamos que $\langle a_1\rangle$ e $\langle a_2\rangle$ são subgrupos de Sylow de G, $C_{\langle a\rangle}(\langle a_2\rangle) = \langle a^p\rangle$ e $C_{\langle a_2\rangle}(\langle a\rangle) = \langle a_2^{p_2}\rangle$, pois $[a_2, a] \neq 1$ e se $[a_2^{p_2}, a] \neq 1$ teríamos $\langle a\rangle \rtimes \langle a_2\rangle$ e $(\langle a\rangle \rtimes \langle a_2^{p_2}\rangle) \times \langle a_1\rangle$ contidos em maximais distintos M_1 e M_2 . Logo, G é do tipo (iv).

Subcaso 2.2: $\langle a_1\rangle = 1$.

Suponha que $\langle a_2\rangle$ não é q-grupo e decomponha $\langle a_2\rangle = \langle a_2^0\rangle \times \langle a_2^*\rangle$, onde $\langle a_2^0\rangle$ e $\langle a_2^*\rangle$ são subgrupos de Hall não triviais de $\langle a_2\rangle$. Se $[a_2^0, a] = 1$, então $G = (\langle a_2\rangle \rtimes \langle a\rangle) = (\langle a_2^0\rangle \times \langle a_2^*\rangle) \rtimes \langle a\rangle = (\langle a_2^*\rangle \rtimes \langle a\rangle) \times (\langle a_2^0\rangle$, com isto voltamos ao Subcaso 2.1 e neste caso $\langle a_2^*\rangle$ e $\langle a_2^0\rangle$ são subgrupos de Sylow. O mesmo vale se $[a_2^*, a] = 1$. Logo, $\langle a\rangle$ e $\langle a_2\rangle$ são subgrupos de Sylow de G.

Afirmação: $C_{\langle a_2\rangle}(\langle a\rangle) = \langle a_2^{p_2}\rangle$.

De fato, suponha que $[a_2^{p_2}, a] \neq 1$. Então como nete caso G é não nilpotente, o item (iv) do Teorema 2.3.3 nos garante que existe $M < G$ maximal e não normal. Observe que $G = \langle a_2\rangle \rtimes \langle a\rangle$ é supersolúvel e portanto $|G : M| = p$ ou p_2. Mas se $|G : M| = p$ teríamos que $\langle a_2\rangle \leq M$, pois $\langle a_2\rangle \trianglelefteq G$ e assim

$$\frac{M}{\langle a_2\rangle} \trianglelefteq \frac{G}{\langle a_2\rangle} \simeq \langle a\rangle.$$

Daí, $M \trianglelefteq G$, mas M foi escolhido de modo que $M \not\trianglelefteq G$. Portanto, $|G : M| = p_2$ e deste modo podemos supor que $\langle a\rangle \leq M$, pois caso isto não ocorra existe $g \in G$ tal que $\langle a\rangle^g \leq M$ e assim basta definir $M_1 = M^{g^{-1}}$. Agora, pelo Segundo Teorema do Isomorfismo

$$|M : M \cap \langle a_2\rangle| = |G : \langle a_2\rangle| \; e \; M \cap \langle a_2\rangle \trianglelefteq M.$$

Daí,

$$p_2 = |G : M| = |\langle a\rangle : M \cap \langle a_2\rangle| \Longrightarrow M \cap \langle a_2\rangle = \langle a_2^{p_2}\rangle.$$

Portanto $M = \langle a_2^{p_2}\rangle\langle a\rangle$, que é não cíclico visto que por hipótese $[a_2^{p_2}, a] \neq 1$.

Observe agora que $\dfrac{M}{\langle a_2^{p_2}\rangle} \in Syl_{p_2}\dfrac{G}{\langle a_2^{p_2}\rangle}$ e $\dfrac{M}{\langle a_2^{p_2}\rangle} \not\trianglelefteq \dfrac{G}{\langle a_2^{p_2}\rangle}$. Assim existe $\dfrac{M_1}{\langle a_2^{p^2}\rangle} \in Syl_{p_2}\dfrac{G}{\langle a_2^{p_2}\rangle}$,

com $\frac{M_1}{\langle a_2^{p^2}\rangle} \neq \frac{M}{\langle a_2^{p^2}\rangle}$. Pelo segundo Teorema de Sylow existe $g \in G$ tal que

$$\frac{M_1}{\langle a_2^{p^2}\rangle} = \left(\frac{M}{\langle a_2^{p^2}\rangle}\right)^{g\langle a_2^{p_2}\rangle} = \frac{M^g}{\langle a_2^{p^2}\rangle}.$$

Logo, $M_1 = M^g$ é não cíclico, com $M_1 \neq M$. Assim, $[a_2^{p_2}, a] = 1$ e com isto fica provado que $C_{\langle a_2\rangle}(\langle a\rangle) = \langle a_2^{p_2}\rangle$.

Caso 3: $G = (P \rtimes \langle a_2\rangle) \times \langle a_1\rangle$, onde $\langle a_1\rangle$ é um subgrupo cíclico que é subgrupo de Hall de G, $G_1 = P \rtimes \langle a_2\rangle$ é não nilpotente satisfazendo a seguinte condição: P é um p-Subgrupo de Sylow de G_1, $C_P(\langle a_2\rangle) \geq \Phi(P)$ e $C_P(\langle a_2\rangle)$ é um subgrupo normal de G_1 tal que

$$\frac{\langle a_2\rangle C_P(\langle a_2\rangle)}{C_P(\langle a_2\rangle)} \lessdot \frac{G_1}{C_P(\langle a_2\rangle)}.$$

Subcaso 3.1: $\langle a_1\rangle \neq 1$. De modo análogo ao caso 2, podemos mostrar que $\langle a_1\rangle$ e $\langle a_2\rangle$ são subgrupos de Sylow de G. Se $P = \langle a\rangle$ com $o(a) = p$, então $[a_2^{p_2}, a] = 1$, pois se $[a_2^{p_2}, a] \neq 1$ existiria um subgrupo maximal não cíclico M_1 contendo $(P \rtimes \langle a_2^{p_2}\rangle) \times \langle a_1\rangle$. Mas como $P \rtimes \langle a_2\rangle$ é não abeliano, existe um maximal não cíclico M que o contêm. Logo $C_{\langle a_2\rangle}(\langle a\rangle) = \langle a_2^{p_2}\rangle$, se $P = \langle a\rangle$ com $o(a) > p$ e $C_{\langle a^2\rangle}(\langle a\rangle) = \langle a_2^{p_2}\rangle$, então G é do tipo (iv) do Teorema. Se P não é cíclico, então existem maximais não cíclicos distintos M_1 e M_2 que contêm respectivamente, $P \rtimes \langle a_2\rangle$ e $P \times \langle a_1\rangle$ (Absurdo!).

Subcaso 3.2: $\langle a_1\rangle = 1$. Se $\langle a_2\rangle$ não é p_2-grupo decomponha $\langle a_2\rangle = \langle a_2^0\rangle \times \langle a_2^*\rangle$. Assim se $[a_2^0, a] = 1$, então $G = (P \rtimes \langle a_2^*\rangle) \times \langle a_2^0\rangle$, onde $\langle a_2^0\rangle \neq 1$, isto é, voltamos ao Subcaso 3.1. De modo análogo, se $[a_2^*, a] = 1$ voltamos para o Subcaso 3.1. Assim, $[a_2^0, a] \neq 1$, $[a_2^*, a] \neq 1$ e existem subgrupos maximais não cíclicos contendo $P \rtimes \langle a_2^0\rangle$ e $P \rtimes \langle a_2^*\rangle$. Podemos supor agora que $\langle a_2\rangle$ é um p_2-grupo. Se $P = \langle a\rangle$, então $\Phi(P) = \langle a^p\rangle \leq C_P(\langle a_2\rangle)$. Portanto, $C_P(\langle a_2\rangle = \langle a^p\rangle$ ou $C_P(\langle a_2\rangle) = P$, mas $C_P(\langle a_2\rangle) = P$ implica que $P \rtimes \langle a_2\rangle$ abeliano, que é uma contradição. Logo, $C_P(\langle a_2\rangle) = \langle a^p\rangle = \Phi(P)$.

Finalmente, suponha que P é não cíclico. Por hipótese $\Phi(P) \leq C_P(\langle a_2\rangle)$, vamos mostrar que é impossível acontecer $\Phi(P) < C_P(\langle a_2\rangle)$.

Observe que $\overline{P} = \frac{P}{\Phi(P)}$ é um Espaço Vetorial sobre $\mathbb{Z}_p$, $Car(\mathbb{Z}_p) = p$ não divide a ordem de $\overline{G} = \frac{G}{P}$.

Defina $\gamma : \overline{P} \times \overline{G} \longrightarrow \overline{P}$ por $\gamma(\overline{x}, \overline{g}) = \overline{gxg^{-1}} = (gxg^{-1})\Phi(P)$.

• γ é bem definida. Suponha que $\overline{g} = \overline{g_1}$ e $\overline{x} = \overline{x_1}$. Então,

$$\overline{(gxg^{-1})}.\overline{(g_1x_1g_1^{-1})^{-1}} \;=\; \overline{(gxg^{-1})(g_1x_1^{-1}g_1^{-1})}.$$

Como $gg_1^{-1} \in P$, $xx_1^{-1} \in \Phi(P)$ e $\overline{P}$ é abeliano temos que

$$\overline{(gxg^{-1})(g_1x_1g_1^{-1})} = \overline{gxg^{-1}g_1x_1g_1^{-1}}$$

$$= \overline{gg^{-1}g_1xx_1^{-1}g_1^{-1}} = \overline{g_1g_1^{-1}} = \overline{1},$$

pois $\Phi(P) \trianglelefteq G$ e $x_1^{-1}x \in \Phi(P)$.

• É fácil ver que $\overline{P}$ é um $\overline{G}$ - Módulo.

• $\overline{P_1} = \overline{C_P(\langle a_2\rangle)}$ é $\overline{G}$ - submódulo que é próprio e não trivial, pois $C_P(\langle a_2\rangle) \neq 1$ já que $1 \leq \Phi(p) < C_P(\langle a_2\rangle)$ e $C_P(\langle a_2\rangle) \neq P$ pois G é não abeliano.

Dados $g \in G$ e $x \in C_P(\langle a_2\rangle)$ temos que $gxg^{-1} \in C_P(\langle a_2\rangle)$, pois $C_P(\langle a_2\rangle) \trianglelefteq G$ por hipótese. Assim, $\overline{gxg^{-1}} \in \overline{C_P(\langle a_2\rangle)}$ e portanto $\overline{P_1} <_{\overline{G}} \overline{P}$.

Assim, pelo Teorema de Maschke existe $\overline{P_2} <_{\overline{G}} \overline{P}$ não trivial tal que $\overline{P} = \overline{P_1} \oplus \overline{P_2} = \overline{P_1} \times \overline{P_2}$.

Observe agora que $P_2 \trianglelefteq G$, pois dados $g \in G$ e $x \in P$ pela definição de submódulo $\overline{gxg^{-1}} \in \overline{P_2}$. Logo, $\overline{P_2} \triangleleft \overline{G}$ e pelo Teorema da Correspondência $P_2 \trianglelefteq G$.

Considere agora o subgrupo $H = P_2 \rtimes \langle a_2\rangle$. Suponha que H é cíclico. Então $P_2 \leq N_G(\langle a_2\rangle)$ e como $P_1 \leq C_P(\langle a_2\rangle) \leq N_G(\langle a_2\rangle)$ temos que $P \leq N_G(\langle a_2\rangle)$ e é claro que $\langle a_2\rangle \leq N_G(\langle a_2\rangle)$. Daí, $\langle a_2\rangle \trianglelefteq G$ e portanto $G = P \times \langle a_2\rangle$, que é um absurdo. Logo, H é não cíclico e portanto existem um subgrupo maximal L não cíclico que o contém. Por outro lado, P é não cíclico e portanto existe um maximal M não cíclico que o contém (pois $\langle a_2\rangle \neq 1$). Observe que $L \neq M$, pois se $L = M$, então $G = P \rtimes \langle a_2\rangle = L$. Assim, $\Phi(P) = C_P(\langle a_2\rangle)$.

($\Longleftarrow$) Se G é to tipo (i) o Lema 3.2.1 nos garante que G contém no máximo um subgrupo não cíclico maximal e claramente se G é tipo (ii) ou (iii) todo subgrupo maximal é cíclico. Seja G do tipo (iv), isto é, $G = (\langle a_2\rangle \rtimes \langle a\rangle) \times \langle a_1\rangle$, onde $\langle a\rangle$, $\langle a_1\rangle$ e $\langle a_2\rangle$ são subgrupos de Sylow de G, e $\langle a_2\rangle \rtimes \langle a\rangle$ é não-nilpotente tal que $C_{\langle a\rangle}(\langle a_2\rangle) = \langle a^p\rangle$ e $C_{\langle a_2\rangle}(\langle a\rangle) = \langle a_2^{p_2}\rangle$. Observe que neste caso G é supersolúvel, pois

$$1 \trianglelefteq \langle a_2\rangle \times \langle a_1\rangle \trianglelefteq G,$$

onde $\langle a_2\rangle \times \langle a_1\rangle$ e $\dfrac{G}{\langle a_2\rangle \times \langle a_1\rangle}$ são cíclicos e assim, todo subgrupo maximal de G tem índice primo. Portanto, temos três casos a considerar:

Caso 1: $|G : M| = p$.

Como $\langle a_2\rangle$ e $\langle a_1\rangle$ são subgrupos de Sylow normais em G e $M \trianglelefteq G$, pois

$$\frac{M}{\langle a_2\rangle \times \langle a_1\rangle} \trianglelefteq \frac{G}{\langle a_2\rangle \times \langle a_1\rangle} \simeq \langle a\rangle,$$

temos que $\langle a_2\rangle \times \langle a_1\rangle le$ M e também $\langle a\rangle \not\subseteq M$. Assim, $G = M\langle a\rangle$ e $\dfrac{G}{M} \simeq \dfrac{\langle a\rangle}{M \cap \langle a\rangle}$. Logo $|\langle a\rangle : M \cap \langle a\rangle| = p$, como $\langle a\rangle$ é cíclico de ordem p^α temos que $M \cap \langle a\rangle = \langle a^p\rangle$. Daí, $M = \langle a_2\rangle \times \langle a^p\rangle \times \langle a_1\rangle$ que é cíclico.

Caso 2: $|G : M| = p_2$.

De modo análogo ao Caso 1, $\langle a_1\rangle$ é um subgrupo de Sylow normal em G. Portanto, $\langle a_1\rangle \leq M$. Como $p \nmid |M$ existe $g \in G$ tal que $\langle a\rangle^g \leq M \Longrightarrow \langle a\rangle \leq M^{g^{-1}} = M_1$. Observe que

$$\langle a_2^{p_2}\rangle \underset{car}{\trianglelefteq} \langle a_2\rangle \trianglelefteq G \Longrightarrow \langle a_2^{p_2}\rangle \trianglelefteq G.$$

Logo, pelo Segundo Teorema do Isomorfismo

$$\frac{G}{\langle a_2\rangle} = \frac{\langle a_2\rangle M_1}{\langle a_2\rangle} \simeq \frac{M_1}{\langle a_2\rangle \cap M_1}.$$

Daí, $|\langle a_2\rangle : M_1 \cap \langle a_2\rangle| = p_2$ e portanto $M_1 \cap \langle a_2\rangle = \langle a_2^{p_2}\rangle$ e $M_1 = H \times \langle a_2^{p_2}\rangle$, onde $H = \langle a\rangle \times \langle a_1\rangle$, que é cíclico e portanto $M = M_1^g$ também é cíclico (por hipótese $C_{\langle a_2\rangle}(\langle a\rangle) = \langle a_2^{p_2}\rangle$ se $\langle a_1\rangle \neq 1$ e $[a, a_2] = 1$), onde $H = \langle a\rangle \times \langle a_1\rangle$.

Caso 3: $|G : M| = p_1$.

Novamente, $\langle a_2\rangle$ é um subgrupo de Sylow normal em G e portanto $\langle a_2\rangle \leq M$. Como

$$\frac{M}{\langle a_2\rangle} \trianglelefteq \frac{G}{\langle a_2\rangle} \simeq \langle a\rangle \times \langle a_1\rangle$$

temos que $M \trianglelefteq G$ e assim, definindo $H = \langle a\rangle \times \langle a_1\rangle$ e aplicando o segundo Teorema do isomorfismo obtemos

$$\frac{G}{M} \simeq \frac{H}{M \cap H}.$$

Logo, $M \cap H = \langle a\rangle \times \langle a_1^{p_1}\rangle$ e com isto concluímos que $M = \langle a_2\rangle \rtimes (\langle a\rangle \times \langle a_1^{p_1}\rangle)$ que possivelmente é não cíclico.

Finalmente, suponha G do tipo (v), isto é, $G = P \rtimes \langle a_2 \rangle$, onde P e $\langle a_2 \rangle$ são subgrupos de Sylow de G, $C_P(\langle a_2 \rangle) = \Phi(P)$ é cíclico normal em G tal que $\frac{\langle a_2 \rangle \Phi(P)}{\Phi(P)} \lessdot \frac{G}{\Phi(P)}$.
Seja M maximal em G. Então $P \leq M$ ou $P \not\leq M$.
• Suponha que $P \leq M$. Como M é maximal em G e $P \triangleleft G$ temos que $P \triangleleft M$ e $\frac{M}{P} \lessdot \frac{G}{P} \simeq \langle a_2 \rangle$. Portanto, $|G : M| = |\overline{G} : \overline{M}| = p_2$ e deste modo $|\langle a_2 \rangle : M \cap \langle a_2 \rangle| = p_2$. Logo, $M \cap \langle a_2 \rangle = \langle a_2^{p_2} \rangle$ e $M = P\langle a_2^{p_2} \rangle = P \rtimes \langle a_2^{p_2} \rangle$, pois $P \cap \langle a_2 \rangle = 1$, $P \trianglelefteq M$ e $C_P(\langle a_2 \rangle) = \langle a_2^{p_2} \rangle$.
• Suponha que $P \not\leq M$, como $P \trianglelefteq G$ e $M \lessdot G$ temos que $G = MP$ e daí, pelo Segundo Teorema do Isomorfismo temos

$$\langle a_2 \rangle \simeq \frac{G}{P} = \frac{MP}{P} \simeq \frac{M}{M \cap P}.$$

Deste modo $|M| = |M \cap P||M : (M \cap P)| = |M \cap P||\langle a_2 \rangle|$. Portanto existe $g \in G$ tal que $M_1 = M^g$, mas como P $\trianglelefteq$ G temos que $\Phi(P) \leq \Phi(G) \leq M_1$ e $\Phi(P) \trianglelefteq$ G, com isto concluímos que $\Phi(P) \trianglelefteq M_1$. Observe agora que $M_1 = (M_1 \cap P)\langle a_2 \rangle$ e $\Phi(P) \leq M_1 \cap P$. Suponha que $\Phi(P) < M_1 \cap P$. Então $\Phi(P)\langle a_2 \rangle < M_1$ e portanto

$$\frac{\Phi(P)\langle a_2 \rangle}{\Phi(P)} < \frac{M_1}{\Phi(P)} < \frac{G}{\Phi(P)}$$

o que é uma contradição, pois por hipótese $\frac{\Phi(P)\langle a_2 \rangle}{\Phi(P)} \lessdot \frac{G}{\Phi(P)}$. Com isto provamos que $M_1 = \Phi(P)\langle a_2 \rangle$, mas como $C_P(\langle a_2 \rangle) = \Phi(P)$ é cíclico, concluímos que $M_1 = \Phi(P) \times \langle a_2 \rangle$ é cíclico e portanto $M = M_1^{g^{-1}}$ também é cíclico. Logo, G contém no máximo um subgrupo não cíclico maximal. □

Bibliografia

[1] BASTOS, Gervasio Gurgel. *Notas de álgebra*. 2^a ed., 2001 Fortaleza: Livro Técnico.

[2] BURNSIDE, W. *Theory of groups of finite order.* Cambridge, Cambridge University Press, 1911.

[3] DIXON, J.D. *Problems in group theory.* New York: Dover, 2007.

[4] GARCIA, Arnaldo: LEQUAIN, Yves. *Elementos de álgebra*. 5^a. ed. Rio de Janeiro: IMPA, 2008.

[5] HUNGERFORD, Thomas W. *Algebra*. New York: Springer-Verlag, 1974. (Graduate texts in mathematics ;73).

[6] MAIER, R. R., *Introdução à teoria das representações dos grupos finitos* , Brasília, 2002. 70 p. (Texto de aula)

[7] PYLAEV, V. V.: KUZENNVI, N. F. Finite groups with a cyclic maximal subgroup, *Ukrainskii Matematicheskii Zhurnal*, v. 28, n° 5, p. 646-654, 1976.

[8] ROBINSON, Derek J. S. *A Course in the theory of groups*, 2nd. ed New York: Springer-Verlag, 1996.