UNIVERSIDADE ESTADUAL DA PARAÍBA - UEPB
CENTRO DE CIÊNCIAS HUMANAS E EXATAS - CCHE
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

Adriana Ribeiro Moura

Teoremas de Sylow e Aplicações

Monteiro - PB
2013

ADRIANA RIBEIRO MOURA

Teoremas de Sylow e Aplicações

Trabalho de Conclusão do Curso apresentado ao Centro de Ciências Humanas e Exatas - CCHE da Universidade Estadual da Paraíba - UEPB , em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática .

Orientação do Professor Ms. Marciel Medeiros de Oliveira .

Monteiro - PB
2013

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA SETORIAL – CAMPUS VI

M 924 t Moura, Adriana Ribeiro .

Teoremas de Sylow e Aplicações [Manuscrito] / por Adriana Ribeiro Moura. – 2013.

30 f.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Licenciatura Plena em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas, 2013.

"Orientação: Prof. Me. Marciel Medeiros de Oliveira, Departamento de Matemática".

1. Teoremas de Sylow. 2. Grupos. 3. Ação em um grupo I. . Título.

21.ed. CDD 512.2

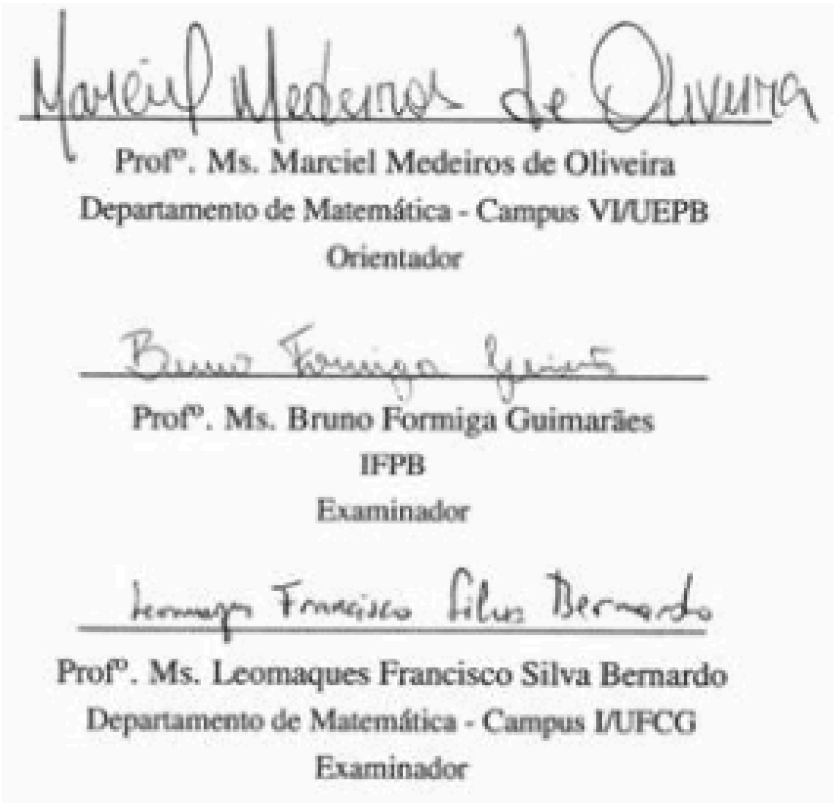
ADRIANA RIBEIRO MOURA

Teoremas de Sylow e Aplicações

Trabalho de Conclusão do Curso apresentado ao Centro de Ciências Humanas e Exatas - CCHE da Universidade Estadual da Paraíba - UEPB , em cumprimento às exigências legais para a obtenção do título de Graduado no Curso de Licenciatura Plena em Matemática .

Aprovado pela banca examinadora em 4 de setembro de 2013.

Banca Examinadora



Dedico esta conquista a minha mãe Josinete.

Agradecimentos

Agradeço primeiramente, a Deus, que me proporcionou força, saúde e coragem para conquistar uma meta na minha vida, me mostrou que era capaz de superar cada dificuldade encontrada no caminho. Aos meus pais: José Carlos e Josinete, principalmente a você mãe, exemplo de força e garra, energia viva das minhas motivações, que tantas vezes abriu mão de si para proporcionar não só a mim, mas aos meus irmãos uma vida feliz , de harmonia e união. Obrigada pela confiança depositada. Ao meu padrasto, Frutuoso, e meu tio, Joaquim, que sempre me incentivaram e acreditaram em mim. Aos meus irmãos, Fátima, Andréa e Adriano. Minha sobrinha Tessália. Bárbara (minha amiga) e sua família, nova casa pra mim em Monteiro. A UEPB que me proporcionou nesses quase cinco anos muitas vitórias e conquistas mostrando um novo mundo a ser alcançado, à todas as amizades encontradas um dia após o outro. Aos professores e também amigos, pessoas que fizeram parte da minha formação profissional, como também do meu crescimento pessoal. Sem deixar de agradecer as duas amigas que nos aproximamos quase no final do curso, mas que os momentos vividos juntos foram únicos, Ivone e Letícia, e ao restante da turma que levarei comigo um pedacinho de cada um de vocês. Em fim, agradeço a todos que de forma direta ou indiretamente fizeram parte dessa jornada. Percebo que os momentos de dificuldades foram necessários, mas vencemos, agora chega o fim e com ele muita saudade.

"A Matemática é a chave de ouro com que podemos abrir todas as ciências".
Victor Duruy

Resumo

Neste trabalho, de início, apresentamos a teoria sobre Ação de um Grupo num Conjunto, no qual foram fundamentados conceitos, tais como Órbita, Estabilizador, Ação por Conjugação, Classes de Conjugação de um Grupo, p-grupo, além de outros resultados, dando assim suporte teórico necessário à abordagem ao nosso foco, Teoremas de Sylow. Neste capítulo, foi necessário resultados como o Teorema da Correspondência e o Teorema de Cauchy para podermos enunciar os Teoremas de Sylow com suas respectivas demonstrações e, em seguida, exibirmos algumas aplicações.
Palavras-Chave: Grupos, Ação em um grupo e Teoremas de Sylow.

Abstract

In this work, initially, we present the theory of action of a Set in a group, which were based concepts, such as Orbit, stabilizer, action by conjugation, conjugation classes a Group, p-group, and other results, thereby supporting the necessary theoretical approach to our focus, Sylow Theorems. In this chapter, it was necessary as the results of Theorem Correspondence and Cauchy's theorem in order to outline the Sylow theorems with their respective statements and then exibirmos some applications.
Key words: *Groups, Action in a group and Sylow theorems.*

SUMÁRIO

1 Introdução

Sabemos que a ordem de qualquer subgrupo de um grupo finito divide a ordem do grupo. Este resultado é conhecido como o Teorema de Lagrange. Apesar da recíproca do Teorema de Lagrange não ser verdadeira, os Teoremas de Sylow nos fornecem uma "quase"recíproca para este último resultado. Além dessa quase recíproca, os Teoremas de Sylow nos dão outras informações importantes, como por exemplo sobre o número de subgrupos de uma determinada ordem e outras relações existentes entre eles.

Segundo Fraleigh (2002), os teoremas de Sylow são devido ao matemático norueguês Peter Ludvig Mejdell Sylow, que os publicou em um breve papel em 1872. Sylow declarou os teoremas em termos de grupos de permutação (porém a definição abstrata de um grupo ainda não havia sido dado). Georg Frobenius reprovou os teoremas para grupos abstratos em 1887, embora ele tenha observado que, de fato, cada grupo pode ser considerado como um grupo de permutação. Sylow aplicava imediatamente os teoremas para o problema da resolução de equações algébricas e mostrou que qualquer equação cujo Galois grupo tem ordem uma potência de um primo p é solúvel por radicais.

Ainda, de acordo o autor acima, Sylow passou a maior parte de sua vida profissional como professor de ensino médio em Halden, na Noruega, e só foi nomeado para um cargo na Universidade de Cristiana em 1898. Ele dedicou oito anos de sua vida ao projeto de edição das obras matemáticas de seu compatriota Niels Henrik Abel.

Dessa forma, neste trabalho, fazemos uma apresentação dos Teoremas de Sylow e algumas de suas aplicações, o qual está organizado em três capítulos obedecendo à seguinte divisão: No primeiro capítulo alguns conceitos básicos, seguido de algumas definições e resultados necessários para a apresentação dos Teoremas de Sylow; no segundo capítulo estão apresentados os Teoremas de Sylow com suas respectivas demonstrações; no terceiro capítulo apresentamos algumas importantes aplicações dos Teoremas de Sylow.

2 Conceitos Básicos

Neste capitulo vamos apresentar alguns conceitos necessários para a compreensão dos próximos capítulos.

2.1 Grupos

Definição 2.1 *Seja G um conjunto não vazio e $*$ uma operação em G. Dizemos que $(G,*)$ é um **grupo** se valem:*
i) $(a*b)*c = a*(b*c)$, $\forall a,b,c \in G$
ii) Existe $e \in G$ *tal que* $a*e = e*a = a, \ \ \forall a \in G$
iii) Para cada $a \in G$*, existe* $a' \in G$ *tal que* $a*a' = a'*a = e$

Se, além disso, a operação $*$ for comutativa, ou seja, $a*b = b*a \ \ \forall a,b \in G$, dizemos que $(G,*)$ é um ***grupo comutativo*** (ou abeliano).

Observação 2.1 *1) Por simplicidade, usaremos apenas G ao invés de $(G,*)$. para denotar um grupo, ficando subentendido a operação. Também, usaremos ab, ao invés de $a*b$ para denotar a operado com b.*
2) O grupo G possui um único elemento neutro.
3) Para cada $a \in G$, existe um único $a' \in G$ tal que $a*a' = a'*a = e$. O elemento inverso de $a \in G$ é denotado por a^{-1}.
4) Operações em um grupo.

Multiplicativa: *Nesta notação a operação "$*$" é denotada por ".", o elemento neutro "e" é denotado por "1" e o elemento inverso de $a \in G$ por a^{-1}.*

Aditiva: *Nesta notação a operação "$*$" é denotada por "$+$", o elemento neutro é denotado por "0" e o elemento inverso $a \in G$ é denotado por "$-a$".*

Usaremos a notação multiplicativa. Todavia, tudo pode ser adaptada para a notação aditiva.

Exemplo 2.1 *São exemplos de grupos aditivos abelianos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$ e $\mathbb{C}$, com a adição usual.*

Exemplo 2.2 *São exemplos de grupos multiplicativos abelianos $\mathbb{Q}^*$, $\mathbb{C}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$, com a multiplicação usual.*

2.2 Subgrupos

Definição 2.2 *Seja G um grupo e H um subconjunto não vazio de G. Dizemos que H é um* ***subgrupo*** *de G, denotado por $H \leq G$, se valem:*
i) $x.y \in H, \forall x, y \in H$;
ii) $x^{-1} \in H, \forall x \in H$

Observação 2.2 *Se G é um grupo e $H \leq G$. Então valem:*
1) $e \in H$, onde e é o elemento neutro de G.
2) O subgrupo H com operação de G, é por si só um grupo.

Exemplo 2.3 *a) Dado um grupo G temos que $\{e\}$ e G são subgrupos de G. Esses subgrupos são chamados* ***subgrupos triviais*** *de G.*
b) Seja G um grupo. Definimos o centro de G denotado por $Z(G)$, com sendo

$$Z(G) = \{x \in G \mid xa = ax, \forall a \in G\}.$$

Temos que $Z(G)$ é subgrupo de G.
c) Seja G um grupo, H um subgrupo de G e $a \in G$. Definimos o ***conjugado*** *de H por a, denotado por H^a, como sendo $H^a = \{a^{-1}ha \mid h \in H\}$. Temos que H^a é subgrupo de G.*
d) Seja G um grupo, H um subgrupo de G. Definimos o ***normalizador*** *de H em G, denotado por $N_G(H)$, como sendo $N_G(H) = \{a \in G \mid H^a = H\}$. Temos que $N_G(H)$ é subgrupo de G.*
e) Sejam G um grupo, H um subgrupo de G e $a \in G$. Definimos:

i) O ***centralizador*** *de a em G, denotado por $C_G(a)$, com $C_G(a) = \{x \in G \mid xa = ax\}$.*

ii) O ***centralizador*** *de H em G, denotado por $C_G(H)$, com*

$$C_G(H) = \{x \in G \mid xh = hx, \forall h \in H\}.$$

Ademais, temos $C_G(a)$ e $C_G(H)$ são subgrupos de G.

2.3 Grupos Cíclicos

Sejam G e $a \in G$. Denotemos por $< a >$, o subconjunto de G dado por $< a >= \{a^n \mid n \in \mathbb{Z}\}$.

Proposição 2.1 *Se G é um grupo e $a \in G$. Então $< a >$ é um subgrupo de G.*

Demonstração: Sejam $x, y \in < a >$, então $x = a^r$ e $y = a^s$, onde r e s são inteiros. Daí, $x.y = a^r.a^s = a^{r+s} \in < a >$. E mais, se $x \in < a >$, então $x = a^r \Rightarrow x^{-1} = (a^r)^{-1} = a^{-r} \in < a >$. Logo, $< a >$ é subgrupo de G. ■

Observação 2.3 *O grupo $< a >$ de G é chamado de subgrupo de G* ***gerado por*** *$a \in G$.*

Definição 2.3 *Seja G um grupo. Dizemos que G é* ***cíclico*** *se existir $a \in G$ tal que $< a >= G$. Quando existir $a \in G$ tal que $< a >= G$ o elemento a é chamado um* ***gerador*** *de G.*

Exemplo 2.4 *1) O grupo $(\mathbb{Z}, +)$ é cíclico, pois*

$$< 1 >= \{n.1 \mid n \in \mathbb{Z}\} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\} = \mathbb{Z}.$$

2) O grupo $(\mathbb{Q}, +)$ não é cíclico.

Proposição 2.2 *Todo grupo cíclico é abeliano.*

Demonstração: Seja G um grupo cíclico, então existe $a \in G$ tal que $< a >= \{a^n \mid n \in \mathbb{Z}\} = G$. Sendo $x, y \in G$, temos que $x = a^r$ e $y = a^s$, $r, s \in \mathbb{Z}$. Dai $x.y = a^r.a^s = a^{r+s} = a^{s+r} = a^s.a^r = y.x$. Logo G é abeliano. ■

Observação 2.4 *Todo subgrupo H de um grupo cíclico G, é também cíclico.*

2.4 Ordem de um elemento em um grupo

Definição 2.4 *Seja G um grupo e $g \in G$. Definimos a* ***ordem*** *de g, denotada por $O(g)$ como sendo o menor inteiro positivo n tal que $g^n = e$ e, neste caso, $O(g) = n$. Se não existe n nestas condições, dizemos que a ordem de g é infinita e neste caso escrevemos $O(g) = \infty$.*

Observação 2.5 1) *O elemento $e \in G$ tem ordem 1,ou seja, $O(e) = 1$. De fato, $e^1 = e$.*
2) *Se G é finito, então todo elemento de G tem ordem finita.*

Proposição 2.3 *Seja G um grupo e $a \in G$ com ordem $O(a) = h$. Então $a^m = e \Leftrightarrow h|m$.*

Demonstração: Usaremos o algoritmo da divisão, $m = hq + r$ $(0 \leq r < h)$ Com efeito, $e = a^m = a^{hq+r} = a^{hq}.a^r = (a^h)^q.a^r = (e)^q.a^r = e^q.a^r = e.a^r = a^r \Rightarrow a^r = e$. Logo, $r = 0$. Do contrário teríamos uma contradição com a minimalidade de h. Logo, $m = hq \Rightarrow h|m$. Reciprocamente, suponha que $h|m$, então $m = hq$, com $q \in \mathbb{Z}$. Daí, $a^m = a^{hq} = (a^h)^q = e^q = e$.
■

2.5 Classes Laterais e Teorema de Lagrange

Definição 2.5 *Sejam G um grupo, H um subgrupo de G e $g \in G$. Definimos:*
i) A ***classe lateral à esquerda*** *de H contendo g, como sendo o conjunto $gH = \{gh \mid h \in H\}$.*
ii) A ***classe lateral à direita*** *de H contendo g, como sendo o conjunto $Hg = \{hg \mid h \in H\}$.*

Exemplo 2.5 *Considere o grupo aditivo $\mathbb{Z}_6$ e seja o subgrupo $H = \{\overline{0}, \overline{3}\}$. Então as classes laterais a esquerda são $\overline{0}+H$, $\overline{1}+H$ e $\overline{2}+H$.*

Observação 2.6 1) *Claramente $g \in Hg$ e $g \in gH$. Pois, $g = eg \in Hg$ e $g = ge \in gH$. Dessa forma, $Hg \neq \emptyset$ e $gH \neq \emptyset$.*
2)*As aplicações*

$$\varphi_1 : \begin{array}{ccc} H & \longrightarrow & Hg \\ h & \longmapsto & \varphi_1(h) = hg \end{array} \quad e \quad \varphi_2 : \begin{array}{ccc} H & \longrightarrow & gH \\ h & \longmapsto & \varphi_1(h) = gh \end{array}$$

são claramente bijetivas. Logo, H, Hg e gH tem mesma cardinalidade (ou quantidade de elementos). Ou seja, $|Hg| = |H| = |gH|$.
3) *Sendo $H \leq G$ e $a, b \in G$, então:*
i) ou $Ha = Hb$, ou $Ha \cap Hb = \emptyset$.
ii) ou $aH = bH$, ou $aH \cap bH = \emptyset$
4) *A união das classes laterais à esquerda ou à direita distintas forma o grupo todo.*
5) *É indiferente usar na prática classe lateral à esquerda ou à direita.*
6) *A quantidade de classes laterais à direita ou à esquerda distintas de H em G é chamada* ***índice*** *de H em G e denotada por $|G : H|$.*

2.6 Teorema de Lagrange

Teorema 2.1 *(Teorema de Lagrange) Sejam G um grupo finito e H um subgrupo de G. Então a ordem de H divide a ordem de G.*

Demonstração: Sejam $a_1H, a_2H, ..., a_nH$ as n classes laterais distintas de H em G, onde $a_iH \cap b_jH = \emptyset$. Então o índice de H em G é $|G : H| = n$. Desde que a união é disjunta segue que $a_1H \cup a_2H \cup ... \cup a_nH = G$. Daí, $|a_1H \cup a_2H \cup ... \cup a_nH| = |G|$. Donde $\underbrace{|a_1H| + |a_2H| + ... + |a_nH|}_{n-parcelas} = |G|$. Desde que $|a_1H| = |H|, |a_2H| = |H|, ..., |a_nH| = |H|$. Obtemos que $\underbrace{|H| + |H| + ... + |H|}_{n-parcelas} = |G| \Rightarrow n.|H| = |G|$, ou seja, ordem de H divide ordem de G. ■

2.7 Subgrupo Normal

Definição 2.6 *Sejam G um grupo e H um subgrupo de G. Dizemos que H é um subgrupo normal em G, denotado $H \trianglelefteq G$, se $aH = Ha, \forall a \in G$.*

Observação 2.7 1) *Sejam G um grupo e $H \leq G$, temos que $H \trianglelefteq G$ se, e somente se, $N_G(H) = G$.*
2) *Se $H^a \subset H$, para todo $a \in G$, então $H \trianglelefteq G$.*

Exemplo 2.6 1 *Se G é um grupo abeliano e H é um subgrupo de G, então H é normal.*
2) Se G é um grupo, então $\{e\} \trianglelefteq G$ e $G \trianglelefteq G$.
3) Se G é um grupo e $H \trianglelefteq G$, então $C_G(H) \trianglelefteq N_G(H)$ e $H \trianglelefteq N_G(H)$.
4) Se G é um grupo, então $Z(G) \trianglelefteq G$.

Definição 2.7 *Dizemos que um grupo G é **simples** se os únicos subgrupos normais de G são $\{e\}$ e G.*

Proposição 2.4 *Seja G um grupo e N e H são subgrupos de G então:*
a) $HN \leq G$ se, e somente se, $HN = NH$.
b) Se $H \subseteq N_G(N)$ ou $N \subseteq N_G(H)$, então $NH \leq G$.
c) Se $H, N \trianglelefteq G$, então $NH \trianglelefteq G$.

2.8 Grupos Quocientes

Sejam G um grupo e $N \trianglelefteq G$. Tomemos $G/N = \{aN \mid a \in G\}$ é chamado de conjunto quociente de G por N. Dados aN, bN em G/N defina $(aN)(bN) = (ab)N$. É possivel mostrar que essa operação é bem definida e que G/N munido dessa operação é um grupo, chamado de ***grupo quociente de G por N***. Observe que $eN = N$ é o elemento neutro de G/N. Dado $a \in G$, temos que $(aN)^{-1} = a^{-1}N$. Por indução é possível mostrar que $(aN)^n = a^nN$, para todo $a \in G$ e $n \in \mathbb{Z}$. Ademais, denotamos $aN = \overline{a}$.

Exemplo 2.7 *Se G é um grupo, então $G/G = \{\overline{e}\}$ e $G/\{\overline{e}\} = G$.*

Proposição 2.5 *Sejam G um grupo e $N \trianglelefteq G$. Então:*
1- Se G abeliano, então $\overline{G} = G/N$ é abeliano.
2- Se G é cíclico, então $\overline{G} = G/N$ é cíclico.

Demonstração: 1) Seja $\overline{x}, \overline{y} \in \overline{G} = G/N$. Então, $\overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{y \cdot x} = \overline{y} \cdot \overline{x}$.
2) Se $G = < x > = \{x^m \ ; \ m \in \mathbb{Z}\}$ então para todo $\overline{y} = Ny \in \overline{G} = G/N$ temos que $y \in G = < x >$ e assim $y = x^m$ para algum $m \in \mathbb{Z}$ e daí segue que $\overline{y} = \overline{x^m} = \overline{x}^m \in < \overline{x} > = \{\overline{x}^r / r \in \mathbb{Z}\}$ e assim $\overline{G} = < \overline{x} >$ como queríamos demonstrar. ■

2.9 Homomorfismo de Grupos

Definição 2.8 *Sejam $(G_1,*)$ e $(G_2,\cdot)$ grupos. Definimos um* ***homomorfismo*** *de G_1 em G_2, como sendo uma função que satisfaz:*

$\varphi(x*y) = \varphi(x)\cdot\varphi(y)$

para quaisquer $x,y \in G_1$.

Quando $\varphi : G_1 \to G_2$ for injetora, dizemos que φ é um homomorfismo injetor(ou monomorfismo).

Quando $\varphi : G_1 \to G_2$ for sobrejetivo, dizemos que φ é um homomorfismo sobrejetor (ou epimorfismo).

Quando $\varphi : G_1 \to G_2$ for um homomorfismo bijetor, dizemos que φ é um isomorfismo. Nesse caso dizemos que G_1 e G_2 são isomorfos e denotamos por $G_1 \simeq G_2$.

Exemplo 2.8 *Sejam*

$$\begin{array}{rccc} \varphi : & G & \longrightarrow & G \\ & x & \longmapsto & \varphi(x) = x \end{array}$$

Note que dados $a,b \in G$, temos $\varphi(a) = a$ e $\varphi(b) = b$. Agora, $\varphi(a*b) = a.b = \varphi(a).\varphi(b)$

Definição 2.9 *Seja $\varphi : G_1 \to G_2$ um homomorfismo. Definimos:*
i) O ***núcleo*** *de φ, denotado por $Ker\,\varphi$, como sendo $Ker\,\varphi = \{x \in G_1 \mid \varphi(x) = e_2\}$*
ii) A ***imagem*** *de φ, denotada por $Im\varphi$, como sendo $Im\varphi = \{\varphi(x) \mid x \in G_1\}$.*

Proposição 2.6 *Sejam $\varphi : G_1 \to G_2$ um homomorfismo. Então:*
a) $Im\varphi \leq G_2$.
b) $Ker\varphi \trianglelefteq G_1$.
c) Se $H \leq G_1$, então $\varphi(H) \leq G_2$.
d) φ é um homomorfismo injetor se e somente se, $Ker\varphi = \{e\}$.

Teorema 2.2 *(Primeiro Teorema dos Isomorfismos) Seja $\varphi : G_1 \to G_2$ um homomorfismo e seja $N = Ker\varphi$. Então $\frac{G_1}{Ker\varphi} \backsimeq Im\varphi$*

Demonstração: Considere a aplicação $\psi : \frac{G_1}{N} \to Im\varphi$ dada por $\psi(\overline{g}) = \varphi(g)$ onde $\overline{g} = gN$. Sendo $\overline{a},\overline{b} \in G_1/N$, então

$$\psi(\overline{a}.\overline{b}) = \psi(\overline{ab}) = \overline{a}.\overline{b} = aN.bN = \overline{ab} = \varphi(ab) = \varphi(a).\varphi(b) = \psi(\overline{a}).\psi(\overline{b})$$

Logo, ψ é homomorfismo de G_1/N em $Im\varphi$. Mostremos que ψ é injetora. De fato suponha $a \in G_1$ tal que $\overline{a} \in Ker\psi$. Então $\psi(\overline{a}) = e_2 = \varphi(a)$. E daí,

$$\varphi(a) = e_2 \Rightarrow a \in Ker\varphi \Rightarrow a \in N.$$

Logo, $\overline{a} = \overline{e_1}$. Portanto, $Ker\psi = \{\overline{e_1}\}$. Portanto, ψ injetora. Pela construção de ψ, concluímos que ela é sobrejetora. Logo, ψ é um isomorfismo. ■

Teorema 2.3 *Sejam G_1 e G_2 grupos e $\varphi : G_1 \to G_2$ um homomorfismo injetivo. Então $G_1 \backsimeq Im\varphi$.*

Teorema 2.4 *(Segundo Teorema dos Isomorfismos) Seja G um grupo e $N, H \leq G$ com $N \trianglelefteq G$. Então $\frac{HN}{N} \backsimeq \frac{H}{H \cap N}$.*

Demonstração: Dica da demonstração: defina $\varphi : H \longrightarrow \frac{HN}{N}$ dada por $\varphi(h) = \overline{h}$. Mostre que φ é homomorfismo sobrejetivo e que $Ker\ \varphi = H \cap N$. Conclua que $H \cap N \trianglelefteq H$ e que $\frac{HN}{N} \backsimeq \frac{H}{H \cap N}$. ■

Teorema 2.5 *(Terceiro Teorema dos Isomorfismos) Sejam G um grupo e $N, H \trianglelefteq G$ com $N \subseteq H$ Então*

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

Demonstração: Dica da demonstração: defina

$$\begin{array}{rccc} \varphi : & G/N & \longrightarrow & G/H \\ & Ng & \longmapsto & \varphi(Ng) = Hg \end{array}$$

Mostre que φ está definida e é um homomorfismo sobrejetivo e $Ker\varphi = H/N$. ■

Teorema 2.6 *(Teorema da Representação) Sejam G um grupo finito $H \leq G$ com índice de H finito, digamos $|G : H| = n$. Então, existe $N \trianglelefteq G$, com $N \subseteq H$, tal que $\frac{G}{N}$ é um grupo finito e $|\frac{G}{N}|$ divide $n!$.*

Demonstração: Considere o conjunto $E = \{xH \mid x \in G\}$. Temos que E é um conjunto finito com n elementos. Para cada $g \in G$, considere a aplicação $\varphi_g : E \to E$ dada por $\varphi_g(xH) = gxH$. Temos que φ_g é uma bijeção e assim $\varphi_g \in S_E = \{f : E \to E \mid f \ \ bijetora\}$. Defina então $\varphi : G \to S_E$ dada por $\varphi(g) = \varphi_g$. Note que φ é um homomorfismo de grupos, onde $Ker\varphi = N$ e claro que $N \trianglelefteq G$. Suponha agora $g \in N$, temos que $\varphi_g = Id_E$ e daí $\varphi_g(H) = H$. Logo, $gH = H$, ou seja, $g \in H$. Daí, $N \subseteq H$. Além disso, $\frac{G}{N} \backsimeq Im\varphi$ e $|\frac{G}{N}| = |Im\varphi|$. Pelo Teorema de Lagrange temos que $|\frac{G}{N}|$ divide $n!$. ■

3 Teoremas de Sylow

Neste capítulo apresentamos os teoremas de Sylow com suas respectivas demonstrações.

3.1 Ação de um grupo em um conjunto

Definição 3.1 *Sejam G um grupo e X um conjunto não vazio. Definimos uma* ***ação de*** *G* ***em*** *X como sendo uma aplicação*

$$\begin{array}{rccc} \rho & : & G\times X & \longrightarrow X \\ & & (g,x) & \longmapsto \quad \rho(g,x)=g\cdot x \end{array}$$

que satisfaz:
i) $e\cdot x = x$ *para todo* $x\in \mathrm{X}$.
ii) $g_1\cdot(g_2\cdot x)=(g_1\cdot g_2)\cdot x$ *para quaisquer* $g_1,g_2\in G$ *e* $x\in \mathrm{X}$.

Observação 3.1 *Sendo*

$$\begin{array}{rccc} \rho & : & G\times X & \longrightarrow X \\ & & (g,x) & \longmapsto \quad g\cdot x \end{array}$$

uma ação de G em X. *Considere* $g\in G$ *e* $x_1,x_2\in \mathrm{X}$, *temos* $x_1 = g\cdot x_2$ *se, e somente se,* $x_2 = g^{-1}\cdot x_1$.

Exemplo 3.1 1) *Se G é um grupo e* X *é um conjunto não vazio. Defina a aplicação*

$$\begin{array}{rccc} \rho_0 & : & G\times X & \longrightarrow X \\ & & (g,x) & \longmapsto \quad \rho_0(g,x)=x \end{array}$$

ρ_0 *é uma ação de G em* X*, chamada de* ação trivial.
2) *Considere um conjunto A não vazio e o grupo simétrico* S_A*. A aplicação*

$$\begin{array}{rccl} \theta & : & S_A \times A & \longrightarrow A \\ & & (f,a) & \longmapsto \quad f \cdot a = f(a) \end{array}$$

é uma ação de S_A *em A.*

Definição 3.2 *Sejam G um grupo,* X *um conjunto não vazio e*

$$\begin{array}{rccl} \rho & : & G \times X & \longrightarrow X \\ & & (g,x) & \longmapsto \quad \rho(g,x) = g \cdot x \end{array}$$

uma ação de G em X*. Dado* $x \in$ X*, definimos:*
i) A ***órbita de*** *x por* ρ *(ou* ρ-***órbita de*** *x), denotado por* O_x*, como sendo*

$$O_x = \{g \cdot x \mid g \in G\}.$$

ii) O ***estabilizador de*** *x com respeito a* ρ*, denotada por*

$$E_x = \{g \in G \mid g \cdot x = x\},$$

note que O_x *é um subconjunto de* X *e* E_x *um subconjunto de G.*

Observação 3.2 *Para* $x \in$ X*, temos que* $O_x \subseteq$ X*. Temos também que* E_x *é um subgrupo de G.*

Exemplo 3.2 1)*Considere a ação trivial*

$$\begin{array}{rccl} \rho_0 & : & G \times X & \longrightarrow X \\ & & (g,x) & \longmapsto \quad g \cdot x = x \end{array}$$

Dado $x \in$ X*, temos que o estabilizador e a órbita de x com respeito à ação trivial são dados, respectivamente, por* $E_x = \{g \in G \mid g \cdot x = x\} = G$ *e* $O_x = \{g \cdot x \mid g \in G\} = \{x\}$.
2) *Considere G um grupo e* S_G *o conjunto de todos os subgrupos de G. A aplicação*

$$\begin{array}{rccl} \rho & : & G \times S_G & \longrightarrow S_G \\ & & (g,H) & \longmapsto \quad \rho(g,H) = g \cdot H = gHg^{-1} \end{array}$$

onde $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$*, é uma ação de G em* S_G*, chamada de* ***ação por conjugação.*** *Observe que dado H subgrupo de G, temos que a órbita e o estabilizador de H com relação à ação por conjugação são, respectivamente,*

$$O_H = \{gHg^{-1} \mid g \in G\} \quad e \quad E_H = \{g \in G \mid gHg^{-1} = H\}.$$

Ademais, note que $E_H = N_G(H)$.
3) *Considere um grupo G e a aplicação*

$$\begin{array}{rccc} \theta & : & G \times G & \longrightarrow G \\ & & (g,x) & \longmapsto \quad g \cdot x = gxg^{-1} \end{array}$$

Esta aplicação é uma ação de G em G, chamada de ***ação por conjugação.*** *Dado* $x \in G$*, temos* $O_x = \{g \cdot x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$*. Este conjunto é chamado de* ***classe de conjugação de*** *x* ***em*** *G e denotado por* $Cl_G(x)$*. Ademais, observe que* $E_x = \{g \in G \mid g \cdot x = x\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$*. Note também que* $E_x = \mathrm{C}_G(x)$.
4- *Sejam H um subgrupo de um grupo G, X um conjunto não vazio e* $\rho : G \ x \ X \to X$ *uma ação de G em X. Definimos a restrição de* ρ *a H como sendo a ação*

$$\begin{array}{rccc} \rho_H & : & H \times X & \longrightarrow X \\ & & (h,x) & \longmapsto \quad \rho_H(h,x) = \rho(h,x) \end{array}$$

Observe que, dado $x \in X$, $\mathrm{O}_x = \{h \cdot x \mid h \in H\}$ *e* $\mathrm{E}_x = \{h \in H \mid h \cdot x = x\} = H \cap \mathrm{E}_x$.

Proposição 3.1 *Sejam G um grupo finito e*

$$\rho \ : \ G \times X \ \longrightarrow X$$

uma ação de G em X. Para todo $x \in X$*, tem-se* O_x *é finita e* $|\mathrm{O}_x|||G|$.

Demonstração: Fixemos $x \in X$, arbitrário. Claramente $\mathrm{O}_x = \{g \cdot x \mid g \in G\}$ é finito. Considere $E_{G:E_x} = \{gE_x \mid g \in G\}$ o conjunto das todas as classes laterais à esquerda de E_x em G. Defina a aplicação

$$\begin{array}{rccc} \rho & : & E_{G:E_x} & \longrightarrow O_x \\ & & gE_x & \longmapsto \quad \rho(gE_x) = g \cdot x \end{array}$$

Supondo $g_1, g_2 \in G$ tais que $g_1E_x = g_2E_x$, então $g_2^{-1}g_1 \in E_x$ e dai $(g_2^{-1}g_1) \cdot x = x$. Logo, $g_2 \cdot [(g_2^{-1}g_1) \cdot x] = g_2 \cdot x$, ou seja, $g_1 \cdot x = g_2 \cdot x$ e assim ρ é bem definida. Além disso, ρ é sobrejetiva. Suponha $g_1E_x, g_2E_x \in E_{G:E_x}$ tais que $\rho(g_1E_x) = \rho(g_2E_x)$, então $g_1 \cdot x = g_2 \cdot x$ e dai $(g_2^{-1}g_1) \cdot x = x$, ou seja, $g_2^{-1}g_1 \in E_x$, isto é, $g_1E_x = g_2Ex$. Temos então que ρ é injetora. Sendo assim, ρ é bijetora. Logo, $|O_x| = |E_{G:E_x}| = |G : E_x|$.

■

Sejam G um grupo e

$$\begin{array}{rccc} \rho & : & G\times X & \longrightarrow X \\ & & (g,x) & \longmapsto \quad g\cdot x \end{array}$$

uma ação de G em X. Definimos em X a relação $\sim_\rho$ da seguinte forma:

$$x_1 \sim_\rho x_2 \text{ se existe } g\in G, \text{ tal que } x_1 = g\cdot x_2$$

para $x_1, x_2 \in X$.

É fácil ver que $\sim_\rho$ é uma relação de equivalência. Além disso, dado $x \in X$, a classe de equivalência de x com relação à $\sim_\rho$ é exatamente O_x.

Temos então:

- $\mathrm{X} = \bigcup_{x\in \mathrm{X}} \mathrm{O}_x$.
- Se $x_1, x_2 \in X$ e $\mathrm{O}_{x_1} \neq \mathrm{O}_{x_2}$, então. $\mathrm{O}_{x_1} \cap \mathrm{O}_{x_2} = \emptyset$.
- Para $x_1, x_2 \in X$, valem: $x_1 \sim_\rho x_2 \Leftrightarrow x_2 \in \mathrm{O}_{x_1} \Leftrightarrow x_1 \in \mathrm{O}_{x_2} \Leftrightarrow \mathrm{O}_{x_1} = \mathrm{O}_{x_2}$.

Definição 3.3 *Dizemos que uma ação*

$$\begin{array}{rccc} \rho & : & G\times X & \longrightarrow X \\ & & (g,x) & \longmapsto \quad g\cdot x \end{array}$$

é ***transitiva*** *se ela determina uma única órbita em X. Ou seja, se dados $x_1, x_2 \in X$, existe $g \in G$ tal que $g\cdot x_1 = x_2$.*

Sendo

$$\begin{array}{rccc} \rho & : & G\times X & \longrightarrow X \\ & & (g,x) & \longmapsto \quad g\cdot x \end{array}$$

uma ação de um grupo G em um conjunto X e $g \in G$. Definimos

$$Fix\,(g) = \{x \in \mathrm{X}\,;\; g\cdot x = x\}.$$

Definimos também

$$Fix\,(G) = \{x \in X\,;\; g\cdot x = x \;\; \forall g \in G\}.$$

Observação 3.3 *Observe que dados $g \in G$ e $x_0 \in \mathrm{X}$ vale $x_0 \in Fix\,(g)$ se, e somente se, $g \in E_{x_0}$.*

Além disso, observe que $Fix(G) = \bigcap_{g\in G} Fix(g)$. Dado $x_0 \in X$, valem:

$$x_0 \in Fix(G) \Leftrightarrow E(x_0) = G \Leftrightarrow \mathrm{O}_\rho(x_0) = \{x_0\}.$$

Logo, $Fix(G)$ é a união das ρ-órbitas unitárias. Suponha agora X finito e $O_1, O_2, ..., O_n$ as distintas ρ-órbitas. Temos:

$$|X| = |O_1| + |O_2| + ... + |O_n|$$

Suponha que $O_1, ..., O_n$ são as ρ-órbitas unitárias temos que $|Fix(G)| = r$. Daí,

$$|X| = |O_1| + ... + |O_r| + |O_{r+1}| + ... + |O_n| = |Fix(\mathbb{G})| + \sum_{J=r+1}^{n} |O_j|.$$

Exemplo 3.3 *1) Considere a ação trivial*

$$\begin{array}{rccc} \rho_0 \ : & G \times X & \longrightarrow & X \\ & (g,x) & \longmapsto & g \cdot x = x \end{array}$$

Temos, $Fix(g) = X, \forall g \in G$ *e* $Fix(G) = X$. *Assim* $O(x) = \{x\}$ *e* $E(x) = G, \forall x \in X$.
2) Considere o conjunto $\mathbb{R}^2$ *e o grupo aditivo dos reais* $(\mathbb{R}, +)$. *Considere também a ação*

$$\begin{array}{rccc} \varphi \ : & \mathbb{R} \times \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ & (t,(x,y)) & \longmapsto & t \cdot (x,y) = (t+x, t+y) \end{array}$$

Dado $(x,y) \in \mathbb{R}^2$, *temos*

$$E(x,y) = \{0\}$$

e

$$O(x,y) = \{t \cdot (x,y); t \in \mathbb{R}\} = \{(t+x, t+y); t \in \mathbb{R}\}.$$

3) Seja G um grupo finito e considere a ação por conjugação

$$\begin{array}{rccc} \rho \ : & G \times G & \longrightarrow & G \\ & (g,x) & \longmapsto & g \cdot x = gxg^{-1} \end{array}$$

Dado $x \in G$ *temos* $E_x = C_G(x)$ *e* $O_x = \{gxg^{-1} \mid g \in G\} = Cl_G(x)$. *Além disso* $|Cl_G(x)| = |G \ : \ C_G(x)|$ *e assim* $|Cl_G(x)|$ *divide* $|G|$. *Temos também*

$$Fix(G) = \{x \in G \ ; \ g \cdot x = x, \forall g \in G\} = \{x \in G \ ; \ gxg^{-1} = x; \forall g \in G\}$$

$$= \{x \in G \ ; \ gx = xg; \forall g \in G\} = Z(G)$$

.

Observação 3.4 *Sendo* $\mathrm{Cl}_1,...,\mathrm{Cl}_n$ *as distintas classes de conjugação de* G *e* $\mathrm{Cl}_1,...,\mathrm{Cl}_r$ *classes unitárias, temos*

$$|G| = |Z(G)| + \sum_{i=r+1}^{n} |\mathrm{Cl}_i|$$

a qual é chamada de ***equação das classes de conjugação do grupo*** *G.*

Definição 3.4 *Seja* $p \in \mathbb{Z}$ *um número primo . Definimos um* p-***grupo*** *finito como sendo um grupo finito cuja ordem é uma potência de* p*.*

Proposição 3.2 *Sejam* G *um grupo finito de ordem* p^n*, com* p *primo e* $n \geq 1$ *e* X *um conjunto finito e*

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

uma ação em X*. Então* $|\mathrm{X}| \equiv |Fix(G)| \pmod{p}$.

Demonstração: Sendo $\mathrm{O}_1,...,\mathrm{O}_r,\mathrm{O}_{r+1},...,\mathrm{O}_n$ as distintas ρ-órbitas, com $\mathrm{O}_1,...,\mathrm{O}_r$ unitárias e $\mathrm{O}_{r+1},...,\mathrm{O}_n$ não unitárias, temos

$$|\mathrm{X}| = |Fix(G)| + \sum_{J=r+1}^{n} |\mathrm{O}_J|,$$

ou seja

$$|\mathrm{X}| - |Fix(G)| = \sum_{J=r+1}^{n} |\mathrm{O}_J|$$

como $|\mathrm{O}_J| > 1$ e $|\mathrm{O}_J|$ divide p^n, para $J = r+1,...,n$. Temos que p divide $|\mathrm{O}_J|$. Daí $|\mathrm{X}| \equiv |Fix(G)| \pmod{p}$. ■

Corolário 3.1 *Se* G *é um grupo finito de ordem* p^n *com* p *primo e* $n \geq 1$*, então* $|Z(G)| > 1$.

Demonstração: Considere a ação por conjugação:

$$\begin{aligned} \rho \ : \ G \times G \ &\longrightarrow G \\ (g,x) \ &\longmapsto \ g \cdot x = gxg^{-1} \end{aligned}$$

Note que $Fix(G) = Z(G)$. Sendo assim, pelo resultado anterior temos $|G| \equiv |Z(G)| \pmod{p}$ e daí p divide $|Z(G)|$. ■

Corolário 3.2 *Se* G *é um grupo de ordem* p^2 *com* p *primo. Então* G *é abeliano.*

Demonstração: Pelo corolário anterior, temos $|Z(G)| > 1$, logo $|Z(G)| = p$ ou $|Z(G)| = p^2$. Suponha por contradição que seja $p = |Z(G)|$. Então $|\frac{G}{Z(G)}| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$. E daí $\frac{G}{Z(G)}$ é cíclico. Logo G é abeliano, daí $|Z(G)| = p^2$. ■

Teorema 3.1 *(Teorema da correspondência) Sejam G e G' grupos e $\psi : G \to G'$ um homomorfismo sobrejetivo tal que $N = Ker(\psi)$. Então:*
a) Se $H \leq G$, então $H' = \psi(H) = \{\psi(h) : h \in H\} \leq G'$. Mais ainda, se $H \trianglelefteq G$, então $H' \trianglelefteq G'$.
b) Se $H' \leq G'$, então existe único $H = \psi^{-1}(H') = \{g \in G \,;\, \psi(g) \in H'\} \supseteq N, H \leq G$ tal que $\psi(H) = H'$.

Demonstração: a) Dado K subgrupo de G_1, temos $H = \psi^{-1}(K)$. Claramente, H é subgrupo de G e $Ker\,\psi \leq H$. Além disso, $\psi(H) = \psi(\psi^{-1}(K)) = K$. Suponha agora H_1 e H_2 subgrupos de G, ambos contendo $Ker\,\psi$, com $\psi(H_1) = \psi(H_2)$. Suponha $h \in H_1$, existe então $h' \in H_2$ tal que $\psi(h) = \psi(h')$ e assim $h^{-1}h' \in Ker\,\varphi \subseteq H_2$. Logo, $h \in H_2$ e portanto $H_1 \subseteq H_2$. Analogamente,$H_2 \subseteq H_1$.
b) Suponha $\psi H \trianglelefteq G_1$, como $H = \psi^{-1}(\psi(H))$, temos $H \trianglelefteq G$. Supondo $H \trianglelefteq G$, temos $\psi(H) \trianglelefteq Im\psi = G_1$. ■

Corolário 3.3 *Sejam G um grupo e N um subgrupo normal de G. Então valem:*
a) Todo subgrupo de $\frac{G}{N}$ é da forma $\frac{H}{N}$, onde H é subgrupo de G contendo N (onde $\frac{H}{N} = \{hN \mid h \in H\}$). Ademais, se H_1 e H_2 são subgrupos de G, ambos contendo N, tais que $\frac{H_1}{N} = \frac{H_2}{N}$, então $H_1 = H_2$.
b) Se H é subgrupo de G, com $N \subseteq H$, valem $H \trianglelefteq G$ se, e somente se, $\frac{H}{N} \trianglelefteq \frac{G}{N}$.

Lema 3.2 *Sejam G um grupo abeliano finito e p um divisor primo de $|G|$. Então, G possui algum elemento de ordem p.*

Demonstração: Indução em $|G|$. Se $|G| = p$, é imediato!

Suponha então $|G| > p$ e suponha que o resultado vale para os grupos de ordem menor que $|G|$. Considere N um subgrupo de G, com $\{e\} \neq N \neq G$. Observe que $|N|$, $|\frac{G}{N}| < |G|$ e que $|G| = |N|\,|\frac{G}{N}|$. Logo, p divide $|N|$ ou p divide $|\frac{G}{N}|$. Se $p \mid |N|$, então existe $x \in N$, com $O(x) = p$ e acabou. Se $p \,||\, \frac{G}{N}|$, então $\frac{G}{N}$ possui algum elemento de ordem p, digamos gN. Logo $(gN)^p = g^pN = N$, então $g^p \in N$, daí $(g^p)^{|N|} = e \Rightarrow g^{p|N|} = e$. Daí, $O(g^k) = p$, o que conclui a demonstração. ■

Teorema 3.3 *(Teorema de Cauchy) Se G é um grupo finito e p é um divisor primo de $|G|$, então G possui algum elemento de ordem p.*

Demonstração: Indução em $|G|$. É imediato!

Suponha $|G| > p$ e suponha que esse resultado vale para todo grupo de ordem menor $|G|$. Se $p \mid |Z(G)|$, temos que existe $x \in Z(G)$ tal que $O(x) = p$(lema).
Suponha então que p não divide $|Z(G)|$. Sejam $Cl_1, ..., Cl_n$ as classes de conjugação não unitárias de G. Como $|G| = |Z(G)| + \sum_{i=1}^{n} |Cl_i|$ e p não divide $|Z(G)|$, existe $i \in \{1, ..., n\}$ tal que p não divide $|Cl_i|$. Tomando $g \in G$ tal que $Cl_i = Cl_G(g)$, temos $|Cl_i| = |Cl_G(g)| = \frac{|G|}{|C_G(g)|}$

e daí $|G| = |Cl_i||C_G(g)|$ e $|C_G(g)| < |G|$.
Como p divide $|C_G(g)| < |G|$, existe $x \in C_G(g)$ tal que $O(x) = p$. ■

Lema 3.4 *Seja G um grupo finito, p um divisor primo de $|G|$ e H um p-subgrupo de G. Então $|G:H| \equiv |N_G(H):H| \pmod{p}$.*

Demonstração: Considere a ação

$$\begin{array}{rccc} \rho : & H \times E_{G:H} & \longrightarrow & E_{G:H} \\ & (h, gH) & \longmapsto & h \cdot (gH) = hgH \end{array}$$

Observe que $|E_{G:H}| = |G:H|$. Vamos agora analisar o conjunto

$$Fix(H) = \{gH \in E_{G:H} \mid h \cdot (gH) = gH \ , \forall h \in H\}.$$

Temos que

$$Fix(H) = \{gH \in E_{G:H} / |\ hgH = gH,\ \forall h \in H\}$$

$$= \{gH \in E_{G:H} \mid g^{-1}hg \in H,\ \forall h \in H\} = \{gH \in E_{g:h} \mid H^g \subseteq H\}$$

$$= \{gH \in E_{G:H} \mid H^g = H\} = \{gH \in E_{G:H} \mid g \in N_G(H)\} = \frac{N_G(H)}{H}$$

e daí $|Fix(H)| = |N_G(H):H|$. Logo, $|G:H| \equiv |N_G(H):H| \pmod{p}$. ■

3.2 Primeiro Teorema de Sylow

Sejam G um grupo finito e p um divisor primo de $|G|$, sendo p^n a maior potência de p que divide $|G|$.
a) Se $1 \leq i \leq n$, então G possui subgrupo de ordem p^i.
b) Se $1 \leq i < n$ e H é um subgrupo de G de ordem p^i, então existe algum subgrupo K de G, de ordem p^{i+1}, tal que $H \trianglelefteq K$.
Demonstração: Pelo teorema de Cauchy, G possui subgrupo de ordem p. Suponha agora H um subgrupo de G de ordem p^i, com $1 \leq i \leq n-1$. Temos que $|G| = |H||G:H| = p^i|G:H|$ e daí p divide $|G:H|$. Logo, p divide $|N_G(H):H|$, ou seja pelo Lema 2.4 p divide $|\frac{N_G(H)}{H}|$. Daí $\frac{N_G(H)}{H}$ possui subgrupos de ordem p, ou seja, existe K subgrupo de $N_G(H)$, com $H \subseteq K$, tal que $|\frac{K}{H}| = p$. Logo $|K| = |H|p = p^i p = p^{i+1}$ e $H \trianglelefteq K$. ■

Sejam G um grupo finito, p um divisor primo de $|G|$ e p^n a maior potência de p que divide $|G|$, ou seja, $|G| = p^n \cdot m$, onde $mdc(p,m) = 1$. Definimos ***S_p-subgrupos*** (ou p-subgrupo de Sylow) de G como sendo um subgrupo de ordem p^n.

Se H é um p-subgrupo de G, então H está contido em algum S_p-subgrupo de G. Denotamos por $Syl_p(G)$ o conjunto de todos os S_p-subgrupos de G.

3.3 Segundo Teorema de Sylow

Sejam G um grupo finito e p um divisor primo de $|G|$. Então quaisquer dois S_p-subgrupos de G são conjugados.

Demonstração: Se P_1 e P_2 são S_p-subgrupos de G. Defina

$$\begin{array}{rccc} \rho & : & P_1 \times E_{G:P_2} & \longrightarrow E_{G:P_2} \\ & & (x, gP_2) & \longmapsto \quad x \cdot (gP_2) = xgP_2 \end{array}$$

Temos que ρ é uma ação de P_1 em $E_{G:P_2}$ e que $|E_{G:P_2}| = |G : P_2| = \frac{|G|}{|P_2|}$. Assim, p não divide $|E_{G:P_2}|$. Ou seja, G é p-grupo finito e p primo e X conjunto finito. Sendo $\rho : P_1 \times E_{G:P_2} \longrightarrow E_{G:P_2}$ ação, segue que $|X| \equiv |Fix(P_1)| \pmod{p}$ X é um conjunto finito e p não divide $|X|$. Temos

$$\begin{aligned} Fix(P_1) &= \{gP_2 \in E_{G:P_2} \mid x \cdot (gP_2) = gP_2, \forall x \in P_1\} \\ &= \{gP_2 \in E_{G:P_2} \mid xgP_2 = gP_2, \forall x \in P_1\} \\ &= \{gP_2 \in E_{G:P_2} \mid g^{-1}xg \in P_2, \forall x \in P_1\} \\ &= \{gP_2 \in E_{G:P_2} \mid P_1^g \subseteq P_2\} \\ &= \{gP_2 \in E_{G:P_2} \mid P_1^g = P_2\} \end{aligned}$$

Como $|P_1| = |P_2|$, observe que $|G : P_2| \equiv |Fix(P_1)| \pmod{p}$ e daí $Fix(P_1) \neq \emptyset$. Logo, existe $g \in G$ tal que $P_1^g = P_2$. ■

3.4 Terceiro Teorema de Sylow

Sejam G um grupo finito e p um divisor primo de $|G|$. Sendo n_p o número de S_p-subgrupos de G, temos n_p divide $|G : P|$ onde $P \in Syl_pG$ e $n_p \equiv 1 \pmod{p}$.

Demonstração: Consideremos $P \in Syl_pG$. Temos que $P \in Syl_pG = \{P^x / x \in G\}$. Denotemos por S_G conjunto dos subgrupos de G,

$$\begin{array}{rccc} \theta & : & G \times S_G & \longrightarrow S_G \\ & & (g,h) & \longmapsto \quad g \cdot H = gHg^{-1} = H^{g^{-1}} \end{array}$$

$E(H_0) = \{g \in G \mid gH_0g^{-1} = H_0\} = \{g \in G \mid H_0^{g^{-1}} = H_0\} = N_G(H_0)$. Temos que $\mathrm{O}(H_0) = \{gHg^{-1} \mid g \in G\} =$ conjunto dos conjugados de H_o em G. Mas,

$$|G| = |\mathrm{E}(H_0)|\,|\mathrm{O}(H_0)| = |G : N_G(H_0)|$$

e assim $|Syl_pG| = |G : N_G(P)|$. Sabemos que $|G : P| = |G : N_G(P)|\ |N_G(P) : P| \Rightarrow |G : P| = n_p|N_G(P) : P|$ e que $|G : P| \equiv |N_G(P) : P| \pmod{p}$. Logo, $n_p|N_G(P) : P| \equiv |N_G(P) : P| \pmod{p}$. como p não divide $|N_G(P) : P|$, temos $n_p \equiv 1 \pmod{p}$. ■

4 Aplicações dos Teoremas de Sylow

Neste capítulo apresentamos algumas aplicações dos teoremas de Sylow, as quais são muito importantes para o estudo mais aprofundado de álgebra abstrata.

Aplicação 1. Sejam G um grupo abeliano finito e $n \in \mathbb{N}$ um divisor de $|G|$. Então G possui, subgrupo de ordem n.
Demonstração: Seja $n = p_1^{l_1}\ p_2^{l_2}...p_k^{l_k}$, onde $p_1, p_2, ..., p_k$, são primos distintos e $l_i \geq 1$. Pelo 1^o teorema de Sylow, existe H_i subgrupo de G, com $|H_i| = p_i^{l_i}$, para todo $i = 1, ..., k$. Como G é abeliano, temos que $H = H_1 \cdot H_2...H_k$ é um subgrupo de G. Ademais, $|H| = |H_1||H_2|...|H_k| = n$.

■

Aplicação 2. Se G é um grupo de ordem 100, então G possui um único subgrupo de ordem 25.
Demonstração: Se G é um grupo de ordem 100, então o(s) seu(s) S_5-subgrupo(s) tem ordem 25. Seja n_5 o número de S_5-subgrupos de G. Pelo 3^o teorema de Sylow, temos
$n_5 \equiv 1 \pmod 5$
$n_5|4$. Logo, $n_5 = 1$. ■

Aplicação 3. Sejam $p, q \in \mathbb{N}$ primos tais que $p < q$ e p não divide $q - 1$. Então, todo grupo de ordem pq é cíclico.
Demonstração: Seja $|G| = pq$. Tomando n_p= número de S_p-subgrupo e n_q= número de S_q-subgrupo, temos
$n_p \equiv 1 \pmod p$
$n_p|q$
e
$n_q \equiv 1 \pmod q$
$n_q|p$
Logo $n_p = 1$ ou q. Mas por hipótese temos que $p \nmid q - 1$ daí q não é congruente a $1 \pmod p$ e assim $n_p = 1$. Da mesma maneira temos $n_q = 1$ ou p. Note $p < q$ e assim $p - 1 < q$. Daí

$q \nmid p-1$ o que implica p não é congruente $1 \pmod{q}$, logo $n_q = 1$. E assim $n_p = n_q = 1$. Seja H o único subgrupo de ordem p e N o único subgrupo de ordem q de G. Logo $H, N \trianglelefteq G$. Além disso, $G = HN$ e $H \cap N = \{e\}$. Logo $G \simeq H \times N$. E assim, G é cíclico. ■

Aplicação 4. Se G é um grupo de ordem 24, então G não é simples.

Demonstração: Seja $|G| = 2^3 \cdot 3$. Pelo 1º teorema de Sylow temos que G possui um subgrupo H de ordem 8.
Como $|G:H| = \frac{|G|}{|H|} = \frac{2^3 \cdot 3}{8} = 3$ então pelo teorema da representação temos que existe $N \trianglelefteq G$ com $N \subseteq H$ tal que $|\ \frac{G}{N}\ |$ divide 3! .
Possibilidades para $|N|$
Se $|N| = 8$ temos $|\ \frac{G}{N}\ | = 3$ e $3|3!$
Se $|N| = 4$ temos $|\ \frac{G}{N}\ | = 6$ e $6|3!$
Se $|N| = 2$ temos $|\ \frac{G}{N}\ | = 12$ e $12 \nmid 3!$
Logo, as possibildades para $|N|$ é $|N| = 8$ ou $|N| = 4$ e assim G não é simples. ■

Aplicação 5. Seja G um grupo abeliano finito, com $|G| = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ com $p_1, p_2, ..., p_k$ números primos dois a dois distintos. Para cada $i = 1, 2, ..., k$ tome H_i um S_p-subgrupo de G. Então,

$$G \simeq H_1 \times H_2 \times ... \times H_k.$$

Demonstração: De fato, para cada $i = 1, 2, ..., k$ sejam H_{i_1} e H_{i_2} S_{p_i}-subgrupo de G. Pelo Segundo Teorema de Sylow temos que existe $g_i \in G$ tal que $H_{i_1}^{g_i} = H_{i_2}$. Portanto, para cada $i = 1, ..., k$, temos que existe um único S_{p_i}-subgrupo de G. Logo, para cada $i = 1, ..., k$, temos

$$H_i \cap (H_1 ... H_{i-1} H_{i+1} ... H_k) = \{e\}$$

e $G = H_1 H_2 ... H_k$. Portanto, $G \simeq H_1 \times H_2 \times ... \times H_k$. ■

Aplicação 6. Um grupo de ordem 182 possui no máximo 91 elementos de ordem 2.

Demonstração: $|G| = 2 \cdot 91 = 2 \cdot 7 \cdot 13$
$n_2 = n^{\text{o}}$ de subgrupos de ordem 2
$n_2 \equiv 1 \pmod{2}$
$n_2 | 91$
$n_2 = 91$ ou $n_2 = 1$. Daí só tem no máximo 91 elementos de ordem 2. ■

Aplicação 7. Sejam G um grupo finito e p um divisor primo de $|G|$. Suponha $N \trianglelefteq G$ e P um S_p-subgrupo. Mostre que:
a) Se p divide $|N|$, então $N \cap P$ é um S_p- subgrupo de N.
b) $\frac{PN}{N}$ é um S_p-subgrupo de $\frac{G}{N}$

Demonstração: Temos que $|P \cap N|$ divide $|P|$ e assim $|P \cap N|$ é potência de p. Como $N \trianglelefteq G$, temos que PN é subgrupo de G. Daí, segue que p não divide $|PN : P|$, pois se p dividisse $|PN : P|$,teríamos que $p|P|$ dividiria $|PN|$ e daí $p|P|$ dividiria $|G|$, o que é um absurdo. Mas, $\frac{|N|}{|N \cap P|} = \frac{|PN|}{|P|}$ e assim p não divide $|N : N \cap P|$.
Logo, $|N \cap P|$ é a maior potência de p que divide $|N|$.

■

Referências

BRANDAO, A. P. J. **Notas de aula,** disciplina Álgebra I, Campus-I/UFCG.

FRALEIGH, J. B. **A First Course in Abstract Algebra ,** 7th Edition, Seventh Edition, 2002.

HYGINO, D.; GELSON, I. **Álgebra Moderna,** São Paulo: editora atual, 2003.

GARCIA, A.; YVES, L. **Álgebra: um curso de introdução,** Rio de Janeiro: IMPA, 1988.

GONÇALVES, A. **Introdução à Algebra,** 5^{o}. Rio de Janeiro: IMPA, 2011.