REMat
ISSN 2177-5095
nº2 - 2010

REVISTA ELETRÔNICA DE MATEMÁTICA
www2.jatai.ufg.br/ojs/index.php/matematica
contato: remat.ufg@gmail.com

Estruturas de grupos finitos

Henrique Bernardes da Silva
Aluno do curso de Licenciatura em Matemática do CAJ/UFG
bernardes_henrique@yahoo.com.br

Esdras Teixeira Costa
Professor do Campus Jataí da Univesidade Federal de Goiás
esdras.ufg@gmail.com

Resumo

Nosso ponto de partida para este trabalho foi uma análise sobre as necessidades matemáticas que levaram à criação do conceito de grupo. A partir da definição de grupo e das implicações desta definição sobre um dado conjunto munido de uma operação $*$, nosso interesse foi estudar, a partir da tábua da operação $*$ quais as estruturas algébricas possíveis para um dado conjunto com n elementos. Esta estratégia foi eficiente para conjuntos finitos de ordem não superior a 6. Para conjuntos finitos de ordem maior, nossos esforços se concentraram em teoremas que, se não fornecem toda a estutura do grupo, fornecem a maior quantidade de informação possível. Seguindo esta linha de raciocínio, este artigo de revisão aborda determinados tópicos da teoria de grupos, chegando até os teoremas de Sylow.
Palavras-chave: Grupos finitos, estrutura, Sylow.

Finite groups structures

Abstract

We begin this work with an analysis of the mathematic motivations that have resulted in the creation of the concept of group. With the definition of group and the implications of this definition upon a given set with an operation $*$, we were concerned with studing, through the table of the operation $*$, which were the possible algebraic structures for a given set with n elements. This strategy was sufficient for finite groups of order less than 6. For finite sets of greater order, we concentrate on theorems that, if doesn't bring the whole structure of the groups, at least bring out the most of information about them. We present here some topics of groups theory, up to Sylow theorems.
Keywords: Finite groups, structure, Sylow.

1 Introdução

Suponha que sejam dados um conjunto X munido de uma operação binária $*$ e dois elementos $a, b \in X$. Vejamos quais seriam as condições necessárias sobre a, b, X e $*$ para que exista solução para uma equação do tipo

REMat
ISSN 2177-5095
nº2 - 2010
REVISTA ELETRÔNICA DE MATEMÁTICA
www2.jatai.ufg.br/ojs/index.php/matematica
contato: remat.ufg@gmail.com

$$a * x = b \tag{1}$$

A solução mais comum pede que existam dois elementos especiais dentro de X:

1. Um elemento $e \in X$ chamado de elemento neutro, que possui a capacidade de ser neutro em relação à operação $*$, o que se traduz em termos matemáticos por:

   "dado qualquer $y \in X$, $y * e = e * y = y$"

2. Um outro elemento y_a dependente de a com a propriedade de "transformar a no elemento neutro e através da operação $*$, o que se traduz em termos matemáticos por:

   "$a * y_a = y_a * a = e$"

Uma vez que assumimos a existência destes dois elementos e e y_a e ainda, por comodidade, denotemos y_a por a^{-1}, ao operarmos à esquerda ambos os lados da equação 1 por a^{-1}, temos:

$$\begin{aligned} a * x &= b \\ a^{-1} * (a * x) &= a^{-1} * b \end{aligned}$$

É necessário agora que a operação $*$ seja flexível o suficiente para permitir que façamos a escolha sobre quais elementos devem ser operados primeiro. Novamente, em linguagem matemática, a operação $*$ deve satisfazer, para quaisquer α, β, $\gamma \in X$:

$$\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma$$

Esta propriedade, chamada de associativa, permite que cheguemos então ao desfecho de nossa pequena investigação sobre a solução de 1:

$$\begin{aligned} a^{-1} * (a * x) &= a^{-1} * b \\ (a^{-1} * a) * x &= a^{-1} * b \\ e * x &= a^{-1} * b \\ x &= a^{-1} * b \end{aligned}$$

É razoável concluir então que, se quisermos resolver uma operação do tipo $a * x = b$ na qual a e b são elementos de um conjunto X que tem uma operação binária $*$, as seguintes três condições são imprecindíveis:

- Associatividade da operação $*$ em X;
- Existência de elemento neutro para a operação $*$ em X;

REMat
ISSN 2177-5095
nº2 - 2010
REVISTA ELETRÔNICA DE MATEMÁTICA
www2.jatai.ufg.br/ojs/index.php/matematica
contato: remat.ufg@gmail.com

*	e
e	e

Tabela 1: Um grupo com um único elemento

- Existência de um inverso a^{-1} com relação à operação $*$ para cada elemento $a \in X$.

Detalhes sobre tais propriedades são exaustivamente considerados em (DOMINGUES-2003). Estamos então a par da necessidade de se nomear de forma particular um conjunto X munido de uma operação $*$ de tal forma que sejam satisfeitas as três condições acima.

Definição 1. Um **grupo** é um conjunto X munido de uma operação $*$ que satisfaz as três condições acima. Considerações adicionais sobre esta definição podem ser encontradas em (HERSTEIN-1975) e (MONTEIRO-1971).

Existe uma outra propriedade que nem toda operação possui, mas que facilita muito o trabalho com grupos. A propriedade em questão se chama comutatividade; se a operação de um grupo possui esta propriedade, o grupo é chamado abeliano, em honra ao matemático norueguês Niels Henrik Abel (1802-1829).

Definição 2. Seja G um grupo e $*$ a operação deste grupo. Dizemos que $*$ é comutativa se para quaisquer elementos a, $b \in G$ temos a validade da igualdade abaixo:

$$a * b = b * a$$

É importante frisar novamente que nem toda operação possui tal propriedade. Uma boa fonte de exemplos de operações não comutativas é (DOMINGUES-2003).

2 Tábua de grupos com ordem menor ou igual a seis

Apresentaremos agora os exemplos mais simples de grupos finitos. Para isto, consideraremos grupos com apenas 2, 3, 4, 5 ou 6 elementos. Na análise que se segue das tábuas de operação destes grupos, consideraremos sempre o elemento e como sendo o elemento neutro.

Inicialmente, temos o caso óbvio de um grupo com apenas um elemento, ou grupo de ordem um, como em (FRALEIGH-2000). Como este grupo deve ter um elemento neutro, é evidente que este único elemento deve ser justamente o neutro. A única operação possível também tem resultado trivial. Isto quer dizer que um grupo de um único elemento só pode ter como tábua de sua operação esta dada a seguir:

Seja G um grupo de ordem dois, ou seja, com apenas dois elementos. Então necessariamente um deles deve ser o elemento neutro e; ao outro elemento, denotado por a, só resta a possibilidade que ele seja seu próprio elemento inverso, do contrário teríamos dois inversos para e, o que é absurdo. Podemos representar este grupo pela tábua a seguir.

$*$	e	a
e	e	a
a	a	e

Tabela 2: Um grupo com apenas dois elementos

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tabela 3: Um grupo com exatamente três elementos

A partir do que vimos acima, esta é a única estrutura possível para tal grupo, no sentido de que qualquer outro grupo com dois elementos terá uma tábua idêntica a esta.
Temos representado na 3 um grupo de ordem três. A multiplicação pelo elemento neutro tem sempre resultado óbvio. Já o produto $a * b$ tem três resultados possíveis:

1. $a * b = e$
2. $a * b = a$
3. $a * b = b$

É fácil ver que se $a * b = a$ então teríamos $b = e$, o que é absurdo pois nosso grupo tem três elementos distintos a, b, c.
Um argumento inteiramente análogo nos permite concluir que $a * b = b$ é igualmente absurdo; sendo assim podemos afirmar que $a * b = e$. Como visto em (FRALEIGH-2000), na área das respostas de uma tábua da operação de um grupo não podem haver repetições de elementos nem nas linhas e nem nas colunas; isto nos permite concluir a tabela abaixo, que, de acordo com o que vimos acima, é a única alternativa possível para um grupo de apenas três elementos.

Ao estudarmos o caso de um grupo de ordem quatro, notamos que desta vez existem duas possibilidades para a tábua da operação:

A primeira estrutura guarda similaridades com aquelas apresentadas anteriores; tal estrutura é chamada de grupo cíclico finito – detalhes em (FRALEIGH-2000) – e para o caso

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

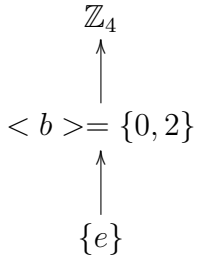
Tabela 4: Grupo cíclico com quatro elementos

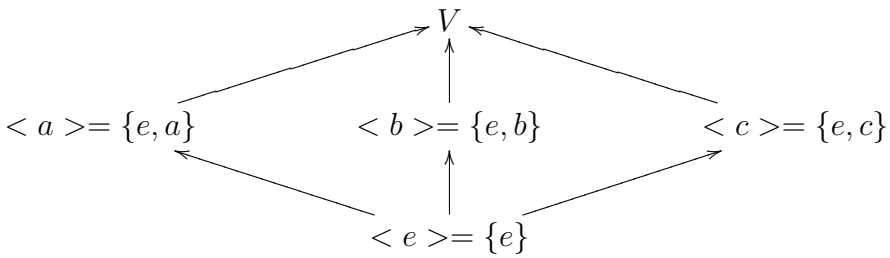
$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Tabela 5: Klein Viergruppe

dos grupos já apresentados, podemos agora denotá-los respectivamente por $\mathbb{Z}_2$, $\mathbb{Z}_3$ e o atual grupo $\mathbb{Z}_4$. Já a segunda estrutura apresentada acima tem particularidades como, por exemplo, o fato de que $a * a = b * b = c * c = e$. Este grupo é chamado de grupo-4 de Klein, ou simplesmente grupo de Klein. A notação mais comum para esta estrutura é V, por conta da palavra alemã *Viergruppe*.

É interessante notar que para o caso dos grupos de ordem quatro, existem outros grupos dentro destes; neste caso, estes grupos são cíclicos e obviamente de ordem menor que quatro, como podemos observar nos diagramas abaixo:





Tais grupos contidos em outros "maiores" são chamados subgrupos. É através deles que estudamos os grupos de ordens superiores. Se para o caso de ordens pequenas como as que vimos até agora a análise da estrutura é fácil e praticamente imediata, para grupos de ordem um pouco maior a necessidade de ferramentas um pouco mais poderosas se faz presente. Para grupos de ordem 16, por exemplo, existem 14 tipos diferentes de estruturas sendo 5 abelianos (apenas um cíclico) e 9 não abelianos.

Para o caso dos grupos cíclicos finitos, como visto em (GARCIA-2002) e (GONÇALVES-1999),

é possível estabelecer uma estrutura geral devido à simplicidade dos mesmos; assim, todo grupo cíclico tem uma estrutura com as seguintes propriedades:

1. Comutatividade; ou seja, todo grupo cíclico é abeliano;
2. Todos os seus subgrupos são também cíclicos.
3. Se a ordem de um grupo cíclico G é n então este grupo é sempre da forma $G = \{e, a, a^2, \cdots, a^{n-1}\}$;

Vale ainda, o teorema a seguir, retirado de (FRALEIGH-2000):

Teorema 3. *Se $G = \{e, a, a^2, \cdots, a^{n-1}\}$ é um grupo cíclico com n elementos, então qualquer elemento $b = a^s \in G$ gera um subgrupo cíclico H de G contendo exatamente $\dfrac{n}{mdc(n,s)}$ elementos.*

Na seção seguinte veremos a estrutura dos grupos abelianos finitamente gerados.

3 Estrutura dos grupos abelianos finitamente gerados

Para entendermos a estrutura dos grupos abelianos finitamente gerados, precisamos revisar as seguintes definições e teoremas, vistos em (FRALEIGH-2000). Esta mesma fonte deve ser consultada caso haja dúvidas quanto a grupos finitamente gerados.

Definição 4. O produto cartesiano dos conjuntos S_1, S_2, S_3, ..., S_n é o conjunto de todas as n-uplas ordenadas $(a_1, a_2, a_3, \ldots, a_n)$ onde $a_i \in S_i\, i = 1, 2, 3, \ldots, n$.

O produto cartesiano é denotado por

$$S_1 \times S_2 \times S_3 \times \ldots \times S_n \text{ ou por } \prod_{i=1}^{n} S_i$$

Teorema 5. Seja G_1, G_2, ..., G_n, grupos. Para $(a_1\, a_2, a_3, \ldots, a_n)$ e $(b_1, b_2, b_3, \ldots, b_n)$ em $\prod_{i=1}^{n} G_i$, defina $(a_1\, a_2, a_3, \ldots, a_n)\cdot(b_1, b_2, b_3, \ldots, b_n)$ sendo o elemento $(a_1b_1, a_2b_2, a_3b_3, \ldots, a_3b_n)$. Então $\prod_{i=1}^{n} G_i$ é um grupo, produto direto dos grupos G_i, sobre esta operação binária.

Demonstração.
Note que se $a_i, b_i \in G_i$ e G_i é um grupo temos que $a_i \cdot b_i \in G_i$. Então pela definição de operação binária em $\prod_{i=1}^{n} G_i$, temos que este conjunto é fechado em relação a esta operação.

Se e_i é o elemento identidade em G_i, então, $(e_1, e_{2,\ldots,} e_n)$ é o elemento identidade em $\prod_{i=1}^{n} G_i$. Claramente notamos que a lei associativa é válida neste conjunto. Finalmente, o inverso de $(a_1\, a_2,\, a_3,\, \ldots, a_n)$ é $\left(a_1^{-1},\, a_2^{-1},\, a_3^{-1},\, \ldots, a_n^{-1}\right)$. Desta forma $\prod_{i=1}^{n} G_i$ é um grupo. □

As provas do teorema e do corolário a seguir podem ser encontradas em (FRALEIGH-2000):

Teorema 6. O grupo $\mathbb{Z}_m \times \mathbb{Z}_n$ é cíclico e tem a mesma estrutura de $\mathbb{Z}_{mn}$ se, e somente se, m e n são primos entre si, ou seja, $mdc\,(m, n) = 1$.

Corolário 7. O grupo $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ é cíclico tem a mesma estrutura de $\mathbb{Z}_{m_1 m_2 m_3, \ldots m_n}$se, e só se, quaisquer dos m_i distintos, $i = 1, 2, 3, \ldots, n$ são relativamente primos.

3.1 A estrutura dos grupos abelianos finitamente gerados

O teorema a seguir tem importância evidente, uma vez que o mesmo fornece a estrutura de qualquer grupo abeliano finitamente gerado. Uma prova completa pode ser encontrada na seção 4.4 de (FRALEIGH-2000).

Teorema 8. (*Teorema Fundamental dos grupos abelianos finitamente gerados*) Todo grupo abeliando finitamente gerado tem a estrutura de um produto direto de grupos cíclicos da forma

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \ldots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$$

onde p_i são números primos, não necessáriamente distintos, e r_i são inteiros positivos. O produto direto é único, exceto unicamente por uma possível reorganização de seus fatores, isto é, o número de seus fatores $\mathbb{Z}$ é único e as potências de primos $(p_i)^{r_i}$são únicas.

Definição 9. Um grupo é decomponível se tem uma estrutura igual ao produto direto de dois grupos próprios não triviais. Se isto não ocorre dizemos que tal grupo é indecomponível.

Teorema 10. Os grupos abelianos finitos indecomponíveis são exatamente os grupos cíclicos em que a ordem é a potência de um número primo.

Demonstração.

Seja e G um grupo abeliano finito indecomponível. Então, pelo Teorema 8, G tem a estrutura de um produto direto de grupos cíclicos em que a ordem é uma potência de um número primo. Já que G é indecomponível, este produto direto consiste apenas de um grupo cíclico em que a ordem é uma potência de um número primo.

Considere agora um número primo p qualquer. Então $\mathbb{Z}_{p^r}$ é indecomponível pois, se $\mathbb{Z}_{p^r}$ fosse isomorfo a $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$, onde $i + j = r$, então todo elemento teria que possuir ordem no máximo igual a $p^{max(i,\,j)} < p^r$. □

Teorema 11. Se m divide a ordem de um grupo abeliano finito G, então G possui um subgrupo de ordem m.

Demonstração.
Pelo Teorema 8, podemos escrever G da forma $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \ldots \times \mathbb{Z}_{(p_n)^{r_n}}$, em que os primos p_i não são necessariamente distintos. Se $(p_1)^{r_1} \cdot (p_2)^{r_2} \cdot \ldots \cdot (p_n)^{r_n}$ é a ordem de G, então m deve ser da forma $(p_1)^{s_1} \cdot (p_2)^{s_2} \cdot \ldots \cdot (p_n)^{s_n}$, onde $0 \leq s_i \leq r_i$. Pelo Teorema 3, $(p_i)^{r_i - s_i}$ gera um subgrupo cíclico de $\mathbb{Z}_{(p_i)^{r_i}}$ de ordem igual ao quociente de $(p_i)^{r_i}$ pelo mdc de $(p_i)^{r_i}$ e $(p_i)^{r_i - s_i}$. Como $mdc((p_i)^{r_i},\ (p_i)^{r_i - s_i}) = (p_i)^{r_i - s_i}$, então $(p_i)^{r_i - s_i}$ gera um subgrupo cíclico de $\mathbb{Z}_{(p_i)^{r_i}}$, de ordem $\frac{(p_i)^{r_i}}{(p_i)^{r_i - s_i}} = (p_i)^{s_i}$. Temos então que $\langle (p_1)^{r_1 - s_1} \rangle \times \langle (p_2)^{r_2 - s_2} \rangle \times \ldots \times \langle (p_n)^{r_n - s_n} \rangle$ é o subgrupo de ordem m desejado. □

Teorema 12. Se m não é divisivel por nenhum quadrado de algum número primo, então todo grupo abeliano de ordem m é cíclico.

Demonstração.
Seja G um grupo abeliano de ordem m, tal que m não é divisível pelo quadrado de nenhum número primo. Então pelo Teorema 8, G é isomorfo a $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \ldots \times \mathbb{Z}_{(p_n)^{r_n}}$, onde $m = (p_1)^{r_1} \cdot (p_2)^{r_2} \cdot \ldots \cdot (p_n)^{r_n}$. Já que m é "livre de quadrados" , temos para todo índice i que $r_i = 1$ e que todos p_i são primos distintos. O corolário 7 mostra-nos que G é isomorfo a $\mathbb{Z}_{p_1 p_2, \ldots p_n}$, então G é cíclico. □

4 Teoremas de isomorfismo

O leitor atento certamente já observou a esta altura que utilizamos até aqui a expressão "ter a mesma estrutura de" como sinônimo de isomorfismo. Esta é uma noção central em álgebra, uma vez que duas estruturas algébricas isomorfas são indistinguíveis do ponto de vista da álgebra. De maneira informal, podemos dizer que um isomorfismo entre dois grupos é uma bijeção que preserva completamente a operação entre os elementos destes grupos. Descreveremos abaixo os teoremas de isomorfismo mais comuns, retirados de (FRALEIGH-2000) mas também presentes em (LANG-1972).

Proposição 13. Seja G um grupo, N um subgrupo normal de G e G/N o grupo quociente de G por N. Então o homomorfismo canônico $f : G \to G/N$ é uma função sobrejetora tal que:

a) $f(x,\, y) = f(x)f(y),\ \forall\, x, y \in G$
b) $N = \{x \in G;\ f(x) = e\}$, onde e é a identidade de G e $\bar{e}$ é a identidade de G/N.

Teorema 14. (*Primeiro Teorema de Isomorfismo*) Seja $f : G \to G'$ um homomorfismo de núcleo K, e seja $h : G \to G/K$ o homomorfismo canônico. Existe um único isomorfismo $g : G/K \to f(G)$ tal que $f(x) = g(h(x))$ para cada $x \in G$.

REMat
ISSN 2177-5095
nº2 - 2010
REVISTA ELETRÔNICA DE MATEMÁTICA
www2.jatai.ufg.br/ojs/index.php/matematica
contato: remat.ufg@gmail.com

Teorema 15. (*Segundo Teorema de Isomorfismo*) Seja H um subgrupo de G e seja N um subgrupo normal de G. Então $(HN)/N \cong H/(H \cap N)$.

Teorema 16. (*Terceiro Teorema de Isomorfismo*) Seja H e K subgrupos normais de um grupo G com $K \leq H$. Então $G/H \cong (G/K)(H/K)$.

5 Classes de conjugação e Teoremas de Sylow

Quando a ordem de um grupo é grande o suficiente para tornar cansativo e enfadonho o trabalho de análise de seus subgrupos um a um, são necessárias técnicas mais avançadas para proceder com tal análise. A melhor destas técnicas tem sido a coleção de resultados conhecidos coletivamente por Teoremas de Sylow. Antes de introduzirmos os teoremas de Sylow, veremos algumas preliminares que podem ser vistas também em (FRALEIGH-2000).

Definição 17. Se G é um grupo, definiremos uma relação em G como segue:

$$x, y \in G, x \sim y \Longleftrightarrow \exists\, g \in G \text{ tal que } y = g^{-1}xg \tag{2}$$

Esta é uma relação de equivalência, pois:
i) $x \sim x$, $\forall\, x \in G$,pois, $x = e^{-1}xe$, $\forall\, x \in G$.
ii) se $x \sim y$ então $y \sim x$. Basta observar que se $x \sim y$ existe $g \in G$ tal que $y = g^{-1}xg$. Assim se $u = g^{-1}$temos $x = u^{-1}yu$, ou seja $y \sim x$.
iii) se $x \sim y$ e $y \sim z$ então $x \sim z$. De fato se $y = g^{-1}xg$ e $z = h^{-1}yh$ onde g, $h \in G$ temos $z = u^{-1}xu$, onde $u = gh$, portanto temos que $x \sim z$.

Definição 18. Se $x \sim y$ dizemos que x e y são elementos **conjugados**. Se denotarmos $g^{-1}xg = x^g$, são válidas as seguintes propriedades:

a) $x^e = x, \forall\, x \in G$
b) $y = x^g \Rightarrow x = y^{g-1}$, $\forall\, x \in G$
c) $(x^g)^h = x^{(gh)}$, $\forall\, x,\, y,\, g \in G$

Definição 19. Seja X um conjunto e G um grupo. Uma ação de G em X é a aplicação $* : G \times X \to X$ tal que:

1. $ex = e$ para todo $x \in X$.
2. $(g_1g_2)(x) = g_1(g_2x)$ para todo $x \in X$ e todo g_1, $g_2 \in G$. Nestas condições, X é um *G-conjunto ou $G-set$.*

Sejam X um G-set, $x \in X$ e $g \in G$. Quando $gx = x$ definimos os conjuntos auxiliares

$$X_g = \{x \in X / gx = x\} \text{ e } G_x = \{g \in G / gx = x\}$$

notemos que se X é um $G-set$ então para cada $x \in G$, G_x é um subgrupo de G chamado de subgrupo de isotropia de x.

Definição 20. Seja X um $G-set$. Cada "célula" na partição da relação de equivalência descrita na definição 17 é chamada de ***órbita*** *em X sobre G.* Se $x \in X$, a célula contendo x é a *órbita de x*. Denotaremos esta célula por Gx.

Os teoremas a seguir têm suas demonstrações disponíveis em (FRALEIGH-2000).

Teorema 21. Seja X um $G-set$ e $x \in X$. Então $|Gx| = (G : G_x)$. Se $|G|$é finita, então $|Gx|$é um divisor de $|G|$.

Teorema 22. Seja G um grupo de ordem p^ne seja X um $G-set$ finito. Então $|X| \equiv |X_G| \, (mod\, p)$.

Definição 23. A classe $C_x = \{y : x \sim y\} = \{x^g : g \in G\}$ para a relação definida em 2 é chamada de *classe de conjugação* em G, determinada pelo elemento $x \in G$.

Se G é um grupo finito e existem n classes de conjugação em G, com representantes $x_1, x_2, \ldots, x_n$, então

$$G = C_{x_1} \cup C_{x_2} \cup \ldots \cup C_{x_n}$$

de onde temos que $|G| = |C_{x_1}| + |C_{x_2}| + \ldots + |C_{x_n}|$. Notemos que $x \in Z(G)$, o centro do grupo G, se e somente se $C_x = \{x\}$ e a equação de classes torna-se

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |C_{x_i}|$$

Teorema 24. (*Teorema de Cauchy*) Seja p um primo divisor da ordem de um grupo finito G. Então $\exists\, a \in G$ tal que a ordem de a é igual a p.

Demonstração.
Utilizaremos indução sobre a ordem de G. Se $|G| = 1$ o teorema é verdadeiro, pois, não existe primo dividindo $|G| = 1$.

Suponhamos que o teorema seja válido para todos os grupos L tais que $1 \leq |L| \leq |G|$.

Caso 1 G é um grupo cíclico.
Seja $G = \langle x \rangle$ e seja p um divisor primo de $|G|$. Neste caso sabemos que $\mathcal{O}(x) = p^r \cdot m$ onde $r \geq 1$ e $a = x^{p^{r-1} \cdot m}$ é tal que $a^p = e$, $a \neq e$ como queríamos demonstrar.

Caso 2 G é um grupo abeliano não cíclico.
Seja p um divisor primo de $|G|$e seja $x \in G$, $x \neq e$. Se p divide $|\langle x \rangle|$então pelo caso anterior $\exists\, a \in \langle x \rangle$ tal que $\mathcal{O}(a) = p$ e o terorema está provado para este caso. Suponhamos entao que p não divide $|N|$onde $N = \langle x \rangle$. Pelo Teorema de Lagrange temos que p divide a ordem do grupo quociente $L = G/N$ (observe que $N \trianglelefteq G$ pois G é abeliano). Como $|L| < |G|$ temos pela hipótese de indução que $\exists\, g \in L$ tal que $\overline{g} \neq \overline{e}$ e $\overline{g}^p = \overline{e}$, ou seja, $\overline{g}^p = \overline{e}$, ou ainda, $g \notin N$, $g^p \in N$. Agora se $|N| = n$temos então que $(g^p)^n = g^{pn}$ e, portanto, p divide $|\langle g \rangle|$ e novamente pelo caso 1 $\exists\, a \in \langle g \rangle$ tal que $\mathcal{O}(a) = p$ e o teorema está provado para mais este caso.

Caso 3 G é um grupo não abeliano. Assim $Z = Z(G) \neq G$. Se p divide $|N|$segue que $\exists\, x_i \notin Z(G)$ tal que p não divide $[G : C_G(x_i)]$. Portanto p divide $|H|$ onde $H = C_G(x_i) \neq G$. Como $|H| < |G|$ pela hipótese de indução temos que $\exists\, a \in H$ tal que $\mathcal{O}(a) = p$ e o teorema está provado.

□

O teorema a seguir, mais uma vez, tem uma prova bastante detalhada em (FRALEIGH-2000).

Teorema 25. Seja H um subgrupo de ordem prima de um grupo finito G. Então $(N[H] : H) = (G : H)\,(mod\, p)$.

Finalmente, estamos agora em condições de apresentar os teoremas de Sylow, que são, como já dito anteriormente, as melhores ferramentas para se avaliar a estrutura de grupos de ordem alta. Os resultados são bem conhecidos e podem ser conferidos em (LANG-1972), (HERSTEIN-1975) ou ainda (FRALEIGH-2000).

Teorema 26. (*Primeiro Teorema de Sylow)* Seja G um grupo finito de ordem $|G| = mp^n$ com $n \geq 1$e p não divide m. Então:

i) G contém um subgrupo de ordem p^i para cada i onde $1 \leq i \leq n$

ii) Todo subgrupo H de G de ordem p^i é um sugrupo normal de m subgrupo de ordem p^{i+1}para $1 \leq i \leq n$.

Demonstração.
i) Sabemos que G contém um subgrupo de ordem p pelo Teorema de Cauchy. Utilizando indução mostraremos a existência de um subgrupo de ordem p^i para $i < n$, implicando na existência de um subgrupo de ordem p^{i+1}.

Seja H um subgrupo de ordem p^i. Se $i < n$, temos que p divide $(G : H)$. Pelo Teorema 25 temos que p divide $(N[H] : H)$. Como H é um subgrupo normal de $N[H]$, podemos formar $N[H]/H$, notando que p divide $|N[H]/H|$. Pelo Teorema de Cauchy o grupo quociente $N[H]/H$ possui um subrupo K que é de ordem p. Se $\gamma : N[H] \to N[H]/H$ é o isomorfismo canônico, então $\gamma^{-1}[K] = \{x \in N[H]/\gamma(x) \in K\}$ é um subgrupo de $N[H]$e consequentemente de G. Este subgrupo contém H e é de ordem p^{i+1}.
ii) Repetindo a construção do item anterior notemos que $H < \gamma^{-1}[K] \leq N[H]$ onde $|\gamma^{-1}[K] = p^{i+1}|$. Como H é normal em $N[H]$, □

Definição 27. Um Sylow p-subgrupo P de G é o máximo p-subrupo de G, isto é, um p-subgrupo que não está contido em nenhum p-subgrupo maior.

Seja G um grupor finito em que $|G| = mp^n$como no Teorema 26 . O teorem nos mostra que os Sylow p-subgrupos de G são exatamente aqueles de ordem p^n. Se P é um p-subgrupo, todo conjugado gPg^{-1}de P também é um p-subgrupo.

Teorema 28. (*Segunto Teorema de Sylow*) Sejam P_1e P_2 Sylow p-subgrupos de um grupo finito G. Então P_1e P_2 são grupos conjugados de G.

Demonstração.
Seja $\mathcal{L}$uma coleção de classes laterais de P_1, e a ação de P_2 em $\mathcal{L}$ dada por $y(xP_1) = (yx)P_1$ para $y \in P_2$. Então $\mathcal{L}$é um P_2-set. Pelo Teorema 22, $\left|\mathcal{L}_{P_2}\right| \equiv |\mathcal{L}|\,(mod\,p)$, e $|\mathcal{L}| = (G : P_1)$ não é divisível por p, logo $\left|\mathcal{L}_{P_2}\right| \neq 0$. Seja $xP_1 \in \mathcal{L}_{P_2}$. Então $yxP_1 = xP_1$ para todo $y \in P_2$, assim $x^{-1}yxP_1 = P_1$ para todo $y \in P_2$. Desta forma $x^{-1}yx \in P_1$ para todo $y \in P_2$ e $x^{-1}P_2x \leq P_1$. Como $|P_1| = |P_2|$, temos que $P_1 = x^{-1}P_2x$, portanto P_1e P_2são de fato subgrupos conjugados. □

Teorema 29. (*Terceiro Teorema de Sylow*) Se G é um grupo fiinito e p divide $|G|$, então o número de Sylow p-subgrupos é congruente a 1 módulo p e divide $|G|$.

Demonstração.
Seja P um Sylow p-subgrupo de G. Seja $\mathcal{S}$ o conjunto de todos os Sylow p-subgrupo e a ação de P em $\mathcal{S}$ definida pela conjugação, tal que $x \in P$ e $T \in \mathcal{S}$ implica em xTx^{-1}. Pelo Teorema 22, $|\mathcal{S}| \equiv |\mathcal{S}_P|\,(mod\,p)$. Temos assim S_P. Se $T \in \mathcal{S}_P$, então $xTx^{-1} = T$ para todo $x \in P$. Assim $P \leq N[T]$ e $T \leq N[T]$. Como P e T são Sylow p-subgrupos de G, são também p-subgrupos de $N[T]$. Mas então eles são conjugados em $N[T]$ pelo Teorema 28. Já que T é um subgrupo normal de $N[T]$, este é o único conjugado em $N[T]$. Logo $T = P$. Então $\mathcal{S}_P = \{P\}$. Como $|\mathcal{S}| \equiv |\mathcal{S}_P| = 1(mod\,p)$, temos que o número de Sylow p-subgrupos é congruente a 1 modulo p.
Agora consideremos a ação de G sobre $\mathcal{S}$ pela conjugação. Sabendo que todo Sylow p-subgrupos são conjugados, há somente uma órbita em $\mathcal{S}$ sobre G. Se $P \in \mathcal{S}$, então $|\mathcal{S}| = (G : G_P)$ pelo Teorema 21. (G_P é de fato, o normalizador de P). Mas $(G : G_P)$ é um divisor de$|G|$, logo o número de Sylow p-subgrupos divide $|G|$. □

Referências

[FRALEIGH-2000] FRALEIGH, John B. A First Course in Abstract Algebra. 6^{th} Edition, New York: Addison Wesley, 2000.

[DOMINGUES-2003] DOMINGUES, H.H.; IEZZI, G. **Álgebra Moderna.** 4ª edição – Atual Editora - 2003.

[GONÇALVES-1999] GONÇALVES, Adilson. **Introdução à Álgebra.** 5ª edição. Rio de Janeiro: Projeto Euclides/IMPA, 1999.

[HERSTEIN-1975] HERSTEIN, I. N. **Tópicos de Álgebra.** 2ª edição, New York: John Wiley & Sons, Inc., 1975.

[GARCIA-2002] GARCIA, A.; LEQUAIN, Y. **Elementos de álgebra.** Rio de Janeiro: Projeto Euclides/ IMPA, 2002.

[LANG-1972] LANG, Serge. **Estruturas Algébricas.** Rio de Janeiro: Livros Técnicos e Cientificos, 1972.

[MONTEIRO-1971] MONTEIRO, L.H. **Elementos de Álgebra.** Rio de Janeiro: Livro Técnicos Cientificos, 1971.