Universidade Federal de Santa Catarina
Centro de Ciências Físicas e Matemáticas
Departamento de Matemática
Trabalho de Conclusão de Curso

Grupos Finitos

Marco Antônio da Silva

Orientador: Prof. Dr. Oscar Ricardo Janesch

Florianópolis
Maio de 2002.

200495

Esta Monografia foi julgada adequada como **TRABALHO DE CONCLUSÃO DE CURSO** *no Curso de Matemática – Habilitação Licenciatura*, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº 19/SCG/02.

Prof. Nereu Estanislau Burin
Professor da disciplina

Banca Examinadora:

Prof. Oscar Ricardo Janesch
Orientador

Prof. Rubens Starke

Prof. Roberto Corrêa da Silva

Ao meu pai que, embora não esteja mais neste plano, estará sempre presente em minhas lembranças. Minha referência de Homem em quem sempre me espelharei.

Agradecimentos

Agradeço aos meus pais por tudo que fizeram por mim.

Agradeço a minha namorada Danielle pela compreensão, carinho, apoio e incentivo dado em todos os momentos.

Aos colegas de graduação pelo convívio amigável de quatro anos de estudos e pelos momentos agradáveis de descontração.

Agradeço a colega Melissa Mendonça pelo suporte em LATEX, editor usado na compilação deste trabalho.

Agradeço aos professores e funcionários que contribuíram para a conclusão do curso de graduação. Em especial ao professor Elieser Batista, que sempre acreditou em meu potencial e que muito me incentivou em meus estudos, e as secretárias Silvia e Iara, pela paciência e apreço que tiveram comigo.

Meu profundo agradecimento ao professor *Oscar Ricardo Janesch* pelo apoio, dedicação e orientação do Trabalho de Conclusão de Curso.

À Deus, por tudo que sou e conquistei

Sumário

Resumo

Este trabalho é um estudo sobre a classificação, a menos de isomorfismo, de grupos finitos. Na classificação de um grupo abeliano G fazemos, primeiramente, a decomposição de G em soma direta de p-subgrupos de Sylow de G, em seguida decompomos cada p-grupo em soma direta de subgrupos cíclicos de G, obtendo assim a decomposição de G em soma direta de grupos cíclicos. Na classificação dos grupos não abelianos nós nos prendemos em ordens que seguissem padrões semelhantes. Classificamos grupos de ordens p, $2p$, p^2, p^3 e pq, onde p e q são números primos distintos e $p < q$. Para classificar esses grupos demonstramos alguns dos principais Teoremas de classificação.

Introdução

Neste trabalho faremos um estudo sobre a classificação, a menos de isomorfismo, de grupos finitos.

No capítulo 1 temos a teoria básica de grupos, apresentamos definições de grupos e subgrupos, falamos de classes laterais e demonstramos que para todo elemento x de um grupo G, a ordem da classe lateral à esquerda coincide com a ordem da classe lateral à direita. Demonstramos também o Teorema de Lagrange, que garante que a ordem e o índice de um subgrupo dividem a ordem do grupo. Apresentamos um sistema de afirmações equivalentes para identificarmos quando um subgrupo é normal e demonstramos o Teorema dos Homomorfismos, resultado que utilizamos com freqüência nesta monografia. Definimos grupos cíclicos e demonstramos que, a menos de isomorfismo, temos apenas dois grupos cíclicos, $(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$. Apresentamos os Teoremos de Sylow sem as demonstrações, pois deles nos interessa apenas o resultado para aplicá-los no desenvolvimento de algumas demonstrações de Teoremas de classificação. Definimos produto direto de grupos e vimos que todo grupo abeliano é o produto direto de seus subgrupos de Sylow.

No capítulo 2 classificamos todos os grupos abelianos finitos. Demonstramos o Teorema da Decomposição primária, que nos garante que todo grupo abeliano finito pode ser decomposto em soma direta de p-subgrupos de Sylow . Em seguida demonstramos um Teorema que nos assegura da unicidade de tal decomposição. Depois decompomos cada p-subgrupo em soma direta de subgrupos cíclicos demonstrando o Teorema da Decomposição dos p-Grupos Finitos e, como feito com o Teorema da Decomposição Primária, mostramos sua unicidade. Mostramos também que se dois grupos abelianos têm o mesmo tipo de decomposição então eles são isomorfos. Assim, a menos de um isomorfismo e a menos da ordem das parcelas das decomposições, classificamos todos os grupos abelianos finitos, e estes resultados estabelecem o Teorema Fundamental dos Grupos Abelianos Finitos.

No capítulo 3 trabalhamos com grupos não abelianos finitos de ordens que têm tratamentos semelhantes. Vimos que se a ordem de um grupo é um número primo então esse grupo é cíclico e portanto abeliano; se a ordem for $2p$ demonstramos uma proposição que nos assegura que temos apenas um grupo não abeliano, a menos de isomorfismo; para grupos de ordem quadrado de um primo demonstramos que não temos grupos não abelianos, e para isso demonstramos que se a ordem de um grupo é potência de um primo p então a ordem de seu centro tem pelo menos p elementos e que se o grupo quociente $\frac{G}{Z(G)}$ é cíclico então G é abeliano; para classificarmos os grupos de ordem potência cúbica de um primo dividimos em dois casos, quando $p = 2$ e quando p é ímpar. Vimos em ambos os casos que temos apenas, a menos de isomorfismo, dois grupos não abelianos com essa ordem; e se a ordem de um grupo é pq então temos, a menos de isomorfismo, dois grupos, um abeliano e outro não.

Temos então classificados todos os grupos não abelianos com essas ordens.

Capítulo 1

Teoria de Grupos e Homomorfismos

Neste capítulo apresentaremos toda a teoria que nos dará amparo para concluirmos o objetivo proposto do trabalho: *Classificar, a menos de isomorfismo, grupos finitos.* Daremos definições, evidenciaremos os principais teoremas e propriedades sobre cada tópico e fixaremos as notações que forem necessárias.

Nas duas primeiras seções definiremos Grupos e Subgrupos. Na terceira seção falaremos sobre Classes Laterais e demonstraremos o Teorema de Lagrange, principal resultado desta seção. A quarta seção trata de Grupos Quocientes e Homomorfismos de Grupos, um assunto que sempre estaremos usando nos capítulos subsequentes. Na quinta seção falaremos de Grupos Cíclicos e na sexta seção abordaremos, de forma sucinta, os p-Subgrupos de Sylow, os Teoremas de Sylow e os principais Corolários, sem nos atermos em suas formais demonstrações, com o propósito único de aplicá-los no desenvolvimento do trabalho. Na sétima e última seção definiremos Produto Direto de Grupos e mostraremos alguns resultados.

O leitor familiarizado com os resultados básicos sobre grupos pode ir diretamente a seção 1.6.

1.1 Grupo

Definição 1.1.1 *Seja G um conjunto não vazio e seja $\star : G \times G \longrightarrow G$ uma operação sobre G. Dizemos que esta operação define uma estrutura de grupo sobre o conjunto G, e denotamos por $(G, \star)$ se, e somente se, os seguintes axiomas estiverem verificados:*

G_1 : *Propriedade Associativa* - Quaisquer que sejam $x, y, z \in G$, temos

$$(x \star y) \star z = x \star (y \star z).$$

G_2 : Existência de elemento neutro - Existe em G um elemento e tal que para todo $x \in G$, temos

$$x \star e = e \star x = x.$$

G_3 : Existência de inverso - Para todo $x \in G$, existe $x' \in G$ tal que

$$x \star x' = x' \star x = e.$$

Se além disso a operação satisfizer o axioma

G_4 : Propriedade Comutativa - Quaisquer que sejam $x, y \in G$, temos

$$x \star y = y \star x,$$

dizemos que $(G, \star)$ é um grupo comutativo ou abeliano.

Ante a definição acima podemos tirar as seguintes conclusões:

1) O elemento neutro é único. De fato, se $e, e' \in G$ são elementos neutros de G, então

$$\begin{aligned} e &= e \star e' && \text{pois } e' \text{ é elemento neutro} \\ &= e' && \text{pois } e \text{ é elemento neutro} \end{aligned}$$

Logo, $e = e'$.

2) O elemento inverso é único. De fato, seja $a \in G$ e sejam $b, b' \in G$ dois elementos inversos de a, então

$$\begin{aligned} b &= b \star e = b \star (a \star b') && \text{, pois } b' \text{ é o inverso de } a \\ &= (b \star a) \star b' = e \star b' = b' && \text{, pois } b \text{ é o inverso de } a \end{aligned}$$

Logo, $b = b'$.

Denotamos por a^{-1} o inverso de a.

3) A partir da unicidade do inverso de um elemento $a \in G$, podemos provar um fato mais geral: Se $a, b \in G$, então $x \star a = b$ tem uma única solução em G, a

saber $b \star a^{-1}$. De fato, $b \star a^{-1}$ é uma solução; por outro lado, se c é uma solução de $x \star a = b$, então temos $c \star a = b$, logo $c \star a \star a^{-1} = b \star a^{-1}$, e portanto $c = b \star a^{-1}$. Analogamente, podemos provar que $a \star x = b$ tem uma única solução em G, a saber $a^{-1} \star b$. Logo, valem em G as leis do cancelamento à esquerda e à direita.

4) $(a \star b)^{-1} = b^{-1} \star a^{-1}$

De fato, $(a \star b) \star (b^{-1} \star a^{-1}) = a \star (b \star b^{-1}) \star a^{-1} = a \star (e) \star a^{-1} = a \star a^{-1} = e$.

Definição 1.1.2 *Dizemos que um grupo $(G, \star)$ é finito se o conjunto G for finito e, neste caso, o número de elementos de G, que denotaremos por $|G|$, será denominado ordem do grupo G, caso contrário dizemos que $(G, \star)$ é um grupo infinito e que $|G|$ é infinita.*

Teorema 1.1.1 *Seja $\star$ uma operação definida sobre um conjunto G e suponhamos que esta operação satisfaça o axioma G_1 e os seguintes:*

G_2': *Existe $e \in G$ tal que $a \star e = a$ para todo $a \in G$.*

G_3': *Para todo $a \in G$ existe $a' \in G$ tal que $a \star a' = e$.*

Nestas condições, a operação $\star$ define uma estrutura de grupo sobre o conjunto G.

Demonstração

Basta mostrar que $a' \star a = e$ e $e \star a = a$. Por hipótese, para todo elemento $a \in G$, existe $a' \in G$ tal que $a \star a' = e$ e também existe $a" \in G$ tal que $a' \star a" = e$. Portanto, temos:

$$\begin{aligned} a' \star a &= a' \star (a \star e) = a' \star [a \star (a' \star a")] = a' \star [(a \star a') \star a"] = \\ &= a' \star [(e) \star a"] = a' \star (e \star a") = a' \star a" = e \end{aligned}$$

e

$$e \star a = ((a \star a') \star a) = a \star (a' \star a) = a \star e = a$$

■

Proposição 1.1.1 *Seja G um grupo. Se para todo $x \in G$ temos $O(x) = 2$ então G é abeliano.*

Exemplo 1.1.6 O grupo D_n das simetrias espaciais de um polígono regular de n lados.

Seja $P_1P_2 \ldots P_n$ um polígono regular de n lados. Sejam $E_1, E_2, \ldots, E_n$ seus eixos. Considerando o conjunto das transformações espaciais que preservam o polígono com a operação de composição temos:

- id, $R_{\frac{2\pi}{n}}$, ..., $R_{\frac{2(n-1)\pi}{n}}$: as rotações no plano em torno do centro do polígono, no sentido anti-horário, de ângulos *zero*, $\frac{2\pi}{n}$,..., e $\frac{2(n-1)\pi}{n}$, respectivamente.
- R_1, R_2, ..., R_n: as rotações espaciais de ângulo π com os eixos E_1, E_2, ..., E_n respectivamente.

D_n munido com a operação de composição é um grupo não abeliano, pois quando compomos uma rotação plana com uma rotação espacial elas, em geral, não comutam.

Citaremos dois casos particulares e faremos detalhadamente suas tabelas de multiplicação, são eles o grupo D_3 das simetrias espaciais de um triângulo equilátero e o grupo D_4 das simetrias espaciais de um quadrado.

O Grupo D_3

Seja $P_1P_2P_3$ um triângulo equilátero e sejam E_1, E_2, E_3 seus eixos. Considerando o conjunto das transformações espaciais que preservam o triângulo com a operação de composição temos:

- id, $R_{\frac{2\pi}{3}}$, $R_{\frac{4\pi}{3}}$: as rotações no plano em torno do centro do triângulo, no sentido anti-horário, de ângulos *zero*, $\frac{2\pi}{3}$ e $\frac{4\pi}{3}$, respectivamente.
- R_1, R_2, R_3: as rotações espaciais de ângulo π com os eixos E_1, E_2, E_3 respectivamente.

Assim, $S_3 = \{\text{id}, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}, R_1, R_2, R_3\}$ e com a operação de composição de funções é um grupo, que não é abeliano pois

$R_1 \circ R_2 = R_{\frac{4\pi}{3}}$ e

$R_2 \circ R_1 = R_{\frac{2\pi}{3}}$.

O grupo D_3 pode ser gerado por dois elementos, por exemplo $R_{\frac{2\pi}{3}}$ e R_1.

TABELA DE MULTIPLICAÇÃO DE D_3:

	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
e	e	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e	R_3	R_1	R_2
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	e	$R_{\frac{2\pi}{3}}$	R_2	R_3	R_1
R_1	R_1	R_2	R_3	e	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$
R_2	R_2	R_3	R_1	$R_{\frac{2\pi}{3}}$	e	$R_{\frac{4\pi}{3}}$
R_3	R_3	R_1	R_2	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$	e

O Grupo D_4

Seja $P_1P_2P_3P_4$ um quadrado, sejam D_1, D_2, M e N os seus eixos. Considerando o conjunto das transformações espaciais que preservam o quadrado com a operação de composição temos:

- id, $R_{\frac{\pi}{2}}$, R_{π}, $R_{\frac{3\pi}{2}}$: as rotações no plano em torno do centro do quadrado, no sentido anti-horário, de ângulo zero, $\frac{\pi}{2}$, π e $\frac{3\pi}{2}$, respectivamente.
- R_M, R_N, R_1, R_2: as rotações espaciais de ângulo π com eixos M, N, D_1 e D_2, respectivamente.

Assim $D_4 = \{\text{id}, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}}, R_M, R_N, R_1, R_2\}$ e com aoperação de composição de funções é um grupo, que não é abeliano pois

$R_1 \circ R_M = R_{\frac{\pi}{2}}$ e

$R_M \circ R_1 = R_{\frac{3\pi}{2}}$.

O grupo D_4 pode ser gerado por dois elementos, por exemplo $R_{\frac{\pi}{2}}$ e R_M.

TABELA DE MULTIPLICAÇÃO DE D_4:

	e	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3\pi}{2}}$	R_M	R_N	R_1	R_2
e	e	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3\pi}{2}}$	R_M	R_N	R_1	R_2
$R_{\frac{\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3\pi}{2}}$	e	R_2	R_1	R_M	R_N
R_{π}	R_{π}	$R_{\frac{3\pi}{2}}$	e	$R_{\frac{\pi}{2}}$	R_N	R_M	R_2	R_1
$R_{\frac{3\pi}{2}}$	$R_{\frac{3\pi}{2}}$	e	$R_{\frac{\pi}{2}}$	R_{π}	R_1	R_2	R_N	R_M
R_M	R_M	R_1	R_N	R_2	e	R_{π}	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$
R_N	R_N	R_2	R_M	R_1	R_{π}	e	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$
R_1	R_1	R_N	R_2	R_M	$R_{\frac{\pi}{2}}$	$R_{\frac{3\pi}{2}}$	e	R_{π}
R_2	R_2	R_M	R_1	R_N	$R_{\frac{3\pi}{2}}$	$R_{\frac{\pi}{2}}$	R_{π}	e

Exemplo 1.1.7 Sejam $(A, \star)$ e $(B, \circ)$ dois grupos e seja $A \times B$ o produto cartesiano dos conjuntos A e B. Se (a, b) e (a', b') são dois elementos quaisquer de $A \times B$ então definimos a seguinte operação: $(a, b) \bullet (a', b') = (a \star a', b \circ b')$. Obtemos assim uma operação $\bullet$ sobre $A \times B$ e que $A \times B$ é um grupo, que é denominado grupo produto dos grupos $(A, \star)$ e $(B, \circ)$ ou produto direto dos grupos $(A, \star)$ e $(B, \circ)$, denotado $(A \times B, \bullet)$

Trataremos deste grupo em detalhes na seção 1.7.

1.2 Subgrupos

Definição 1.2.1 *Seja $(G, \star)$ um grupo. Um subconjunto não vazio H de G é um subgrupo de G, e denotamos por $H < G$, quando, com a operação de G, H é um grupo, isto é, quando as seguintes condições são satisfeitas:*

H_1- *Quaisquer h_1, h_2 em H, temos $h_1 \star h_2 \in H$.*

H_2- *Quaisquer h_1, h_2, h_3 em H, temos $h_1 \star (h_2 \star h_3) = (h_1 \star h_2) \star h_3$*

H_3- *Existe em H um elemento neutro e_H tal que $e_H \star h = h \star e_H = h$, qualquer que seja $h \in H$.*

H_4- *Para cada $h \in H$, existe $k \in H$ tal que $h \star k = k \star h = e_H$.*

Ante a definição acima podemos tirar as seguintes conclusões:

1) A condição H_2 é sempre satisfeita pois, a igualdade $h_1 \star (h_2 \star h_3) = (h_1 \star h_2) \star h_3$ é válida para todos os elementos de G.

2) O elemento neutro e_H de H é necessariamente igual ao elemento neutro e de G. De fato, tomando $a \in H \subset G$, temos $e_H \cdot a = a$ e portanto temos $e_H = e$.

3) Dado $h \in H$, o inverso de h em H é necessariamente igual ao inverso de h em G. De fato, se k é o inverso de h em H, então $hk = kh = e_H$, logo $hk = kh = e$, pois $e_H = e$, e portanto k é o inverso de h em G, e denotamos por h^{-1}.

Teorema 1.2.1 *Seja G um grupo e seja H um subconjunto não vazio de G. Então H é um subgrupo de G se, e somente se, as duas condições seguintes estiverem satisfeitas:*

I) $\forall h_1, h_2 \in H$, temos $h_1 \star h_2 \in H$

II) $\forall h \in H$, temos $h^{-1} \in H$.

Demonstração

Suponhamos que o subconjunto H satisfaça as condições I) e II) do Teorema acima, logo, em particular, está verificada a condição H_1 da definição 1.2.1. Basta mostrar que os axiomas H_2 , H_3 e H_4 são verdadeiros.

H_2 - Por hipótese, temos $(a \star b) \star c = a \star (b \star c)$, $\forall a, b, c \in G$, logo, esta igualdade também é verdadeira para todos os elementos $a, b, c \in H$.

H_3 - Como $H \neq \emptyset$ temos que existe um elemento a_0 em H, logo, de acordo com a condição II), $a_0^{-1} \in H$ e então, em virtude de I), $a_0 a_0^{-1} \in H$, ou seja, $e_H \in H$ e é imediato que $a \cdot e_H = a$, $\forall a \in H$.

H_4 - É verdadeiro em virtude da condição II).

Reciprocamente, suponhamos que H seja um subgrupo de G. Conforme a condição H_1 da definição 1.2.1 , H é fechado em relação à operação de G, logo, está satisfeita a condição I do Teorema. De acordo com o axioma H_3, existe em H o elemento e_H, portanto, $H \neq \emptyset$. Para verificarmos a condição II temos que $e_H \star e_H = e_H \star e$, logo, em virtude da lei do cancelamento aplicada a elementos de G temos que $e_H = e$. Se a é um elemento qualquer de H, então, de acordo com o axioma H_4, existe $a' \in H$ tal que $a \star a' = e_H = e$; esta igualdade mostra que a' também é o inverso de a em G. Portanto, conforme a unicidade do inverso, temos $a' = a^{-1}$ e então $a^{-1} \in H$.

■

O Teorema 1.2.1 mostra quando um subconjunto H de G é um subgrupo de G, no entanto, quando quisermos verificar se H é um subgrupo de G o Teorema seguinte nos dá uma forma mais prática de fazê-lo.

Teorema 1.2.2 *Seja $(G, \star)$ um grupo e seja H um subconjunto não vazio de G. Então H é subgrupo de G se, e somente se, quaisquer que sejam a e b em G, se $a \in H$ e $b \in H$ então $a^{-1}b \in H$.*

Demonstração

Sejam a e b dois elementos quaisquer de H; de acordo com a condição II do Teorema 1.2.1 , temos que $a^{-1} \in H$ e como $b \in H$ concluímos que $a^{-1}b \in H$. Reciprocamente, suponhamos que um subconjunto H de G satisfaça a condição de que quaisquer a, $b \in G$, se $a \in H$ e $b \in H$ então $a^{-1}b \in H$; logo, é de imediato que H não é vazio e portanto existe um elemento $a_0 \in H$, donde resulta que $e = a_0 \cdot a_0^{-1} \in H$.

Portanto, se a é um elemento qualquer de H, temos $a^{-1} = a^{-1} \cdot e \in H$, ou seja, vale a condição II do teorema 1.2.1. Finalmente, sejam a e b dois elementos quaisquer de H, conforme vimos acima temos $a^{-1} \in H$ e como $b \in H$ temos $(a^{-1})^{-1} \cdot b = a.b \in H$.

■

Teorema 1.2.3 *A intersecção de uma família não vazia $(H_i)_{i\in I}$ de subgrupos de um grupo G é um subgrupo de G.*

Demonstração

Suponhamos $H = \bigcap_{i\in I} H_i$. É de imediato que $H \neq \emptyset$ pois $e \in H_i$ para todo $i \in I$. Se a e b são dois elementos quaisquer de H temos que $a \in H_i$ e $b \in H_i$ para todo $i \in I$. Logo $a^{-1}b \in H_i$ para todo $i \in I$, donde $a^{-1}b \in H$.

■

Sejam G um grupo e S um subconjunto não vazio de G. Introduzimos a notação

$$< S > = \{a_1, a_2, \ldots, a_n \ ; \ n \in \mathbb{N}, a_i \in S \text{ ou } a_i^{-1} \in S\}.$$

Quando S é finito da forma $S = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ é comum denotar simplesmente,

$$< S > = < \alpha_1, \alpha_2, \ldots, \alpha_m >$$

ao invés de

$$< S > = < \{\alpha_1, \alpha_2, \ldots, \alpha_m\} > .$$

Nota que se $g \in G$ então

$$< g > = \{\ldots, (g^-)^2, g^{-1}, e, g, g^2, \ldots\}.$$

Usando a notação g^{-r} para $(g^{-1})^r$, $r \in \mathbb{N}$, vem que

$$< g > = \{g^t \ ; \ t \in \mathbb{Z}\}.$$

Proposição 1.2.1 *Seja S um subconjunto do grupo G. Então o conjunto $\langle S \rangle$ é um subgrupo de G.*

Demonstração

Sejam $x, y \in (S)$. Assim,

$$\begin{aligned} x &= a_1 a_2 \ldots a_n \text{ com } a_i \in S \text{ ou } a_i^{-1} \in S \\ y &= b_1 b_2 \ldots b_m \text{ com } b_i \in S \text{ ou } b_i^{-1} \in S \end{aligned}$$

Logo, $x \cdot y = a_1 a_2 \ldots a_n \cdot b_1 b_2 \ldots b_m$ e $x^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$ estão também em $< S >$.

■

Definição 1.2.2 *Se S é um subconjunto não vazio do grupo G, o grupo $< S >$ é chamado subgrupo gerado por S.*

Em particular, para todo elemento g do grupo G, o subgrupo gerado por g é $< g >= \{g^t \ ; \ t \in \mathbb{Z}\}$.

Vejamos alguns exemplos

Exemplo 1.2.1 Todo grupo G admite, pelo menos, dois subgrupos, a saber: $\{e\}$ e G.

Exemplo 1.2.2 O grupo aditivo $\mathbb{Z}$ dos números inteiros é um subgrupo do grupo aditivo $\mathbb{Q}$ dos números racionais que, por sua vez, é um subgrupo do grupo aditivo $\mathbb{R}$ dos números reais.

Exemplo 1.2.3 Para todo número inteiro n, seja $n\mathbb{Z}$ o conjunto de todos os inteiros que são múltiplos de n. A igualdade $qn - q'n = (q - q')n$ mostra que $n\mathbb{Z}$ é um subgrupo do grupo aditivo $\mathbb{Z}$.

Exemplo 1.2.4 O grupo multiplicativo $\mathbb{Q}^*$ dos números racionais não nulos é um subgrupo do grupo multiplicativo $\mathbb{R}^*$ dos números reais não nulos que, por sua vez, é um subgrupo do grupo multiplicativo $\mathbb{C}^*$ dos números complexos não nulos.

Exemplo 1.2.5 $\{\mathrm{id}, R_1\}$, $\{\mathrm{id}, R_2\}$, $\{\mathrm{id}, R_3\}$ e $\{\mathrm{id}, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}\}$ são subgrupos de D_3;

$\{\mathrm{id}, R_1\}$, $\{\mathrm{id}, R_2\}$, $\{\mathrm{id}, R_M\}$, $\{\mathrm{id}, R_N\}$, $\{\mathrm{id}, R_\pi\}$ e $\{\mathrm{id}, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}\}$ são subgrupos de D_4.

Exemplo 1.2.6 Se H e K são dois subgrupos de G, então $H \cap K$ é um subgrupo de G. De um modo geral, se $\{H_i\}_{i \in I}$ é uma família de subgrupos não vazios de G, então $\bigcap H_i$, $i \in I$ é um subgrupo de G *(conforme demonstrado no Teorema 1.2.3)*.

Exemplo 1.2.7 Seja G um grupo e $g \in G$. Então $< g >$ é um subgrupo de G.

Exemplo 1.2.8 Seja G um grupo e $x \in G$. Então $C_G(x) = \{y \in G; \ yx = xy\}$ é um subgrupo de G chamado de *centralizador de x em G*.

Proposição 1.2.2 *Os únicos subgrupos do grupo aditivo $\mathbb{Z}$ são da forma $n\mathbb{Z}$, com $n \in \mathbb{N}$.*

Demonstração

Seja H um subgrupo qualquer de $\mathbb{Z}$. Se $H = \{0\}$, então $H = 0.\mathbb{Z}$. Suponhamos que $H \neq \{0\}$. Seja $n = min\{x \in H;\ x > 0\}$. Como $n \in H$ e H é um subgrupo de $\mathbb{Z}$, temos $n\mathbb{Z} \subset H$. Reciprocamente, seja $h \in H$. Pelo algoritmo de Euclides, $h = qn + r$, com $0 \leq r < n$; como h e n pertencem a H, r pertence a H também; pela minimalidade de n temos

$$\left.\begin{array}{c} r \in H \\ 0 \leq r < n \end{array}\right\} \Rightarrow r = 0$$

e portanto $h = qn$, ou seja, $h \in n\mathbb{Z}$. Logo, $H \subseteq n\mathbb{Z}$ e portanto $H = n\mathbb{Z}$. Finalmente, se $H = n'\mathbb{Z}$, com $n' \geq 0$ segue evidentemente que $n' \neq 0$ e $n \leq n'$, mas de $n \in n'\mathbb{Z}$ vem $n = qn'$, com $q > 0$, logo $n \geq n'$ e então $n = n'$. Fica assim provado que o número inteiro $n > 0$ tal que $H = n\mathbb{Z}$ é único.

■

Definição 1.2.3 *Um grupo G é dito cíclico quando ele pode ser gerado por um elemento, isto é, quando $G = < g >$, para algum $g \in G$.*

$\mathbb{Z} = < 1 >$; $\mathbb{Z}/n\mathbb{Z} = < \overline{1} >$ são exemplos de grupos cíclicos.

Trataremos destes grupos em detalhes na seção 1.5.

Definição 1.2.4 *Seja G um grupo. O subgrupo $(\{xyx^{-1}y^{-1};\ x, y \in G\})$ chama-se subgrupo dos comutadores de G, e é denotado por G'.*

É de imediata conclusão que G é abeliano se, e somente se, $G' = \{e\}$.

Definição 1.2.5 *Seja G um grupo. O subgrupo $\{x \in G;\ xg = gx, \forall g \in G\}$ chama-se centro de G , e é denotado por $Z(G)$.*

É de imediata conclusão que G é abeliano se, e somente se, $G = Z(G)$.

Definição 1.2.6 *Seja $a \in G$. A ordem do elemento $a \in G$, que denotaremos por $O(a)$, é a ordem do subgrupo gerado por a, isto é, $O(a) = | < a > |$.*

Proposição 1.2.3 *Seja $x \in G$ tal que $O(x) = n < \infty$. Então $n = min\{N \in \mathbb{N}\backslash\{0\};\ x^N = e\}$ e $< x >= \{e, x, x^2, \ldots, x^{n-1}\}$.*

Demonstração

Como $< x >= \{x^m;\ m \in \mathbb{Z}\}$, e como por hipótese $< x >$ é finito, temos que existe $p, q \in \mathbb{Z}$, $p \neq q$, tais que $x^p = x^q$. Sem perda de generalidade, podemos supor que $p > q$.

De $x^p = x^q$ segue que $x^{p-q} = e$, isto é, existe um número $p - q = N > 0$ tal que $x^N = e$. Seja então o inteiro $r = min\{N \in \mathbb{N}\backslash\{0\};\ x^N = e\}$. Devemos provar que $r = n$. Para isso, basta mostrar que $< x >= \{e, x, x^2, \ldots, x^{r-1}\}$ e os elementos $e, x, x^2, \ldots, x^{r-1}$ são todos distintos.

Supondo que $x^p = x^q$ com $0 \leq p \leq r-1$, $0 \leq q \leq r-1$, $p \neq q$ e supondo $p > q$ então $x^{p-q} = e$, com $0 < p - q < r$. Isso contradiz a minimalidade de r. Segue que $e, x, x^2, \ldots, x^{r-1}$ são elementos distintos de G. Para mostrar que $< x > = \{e, x, x^2, \ldots, x^{r-1}\}$ devemos mostrar que para todo $m \in \mathbb{Z}$, $x^m = x^l$ para algum $0 \leq l < r$. Para isso, observemos que pelo algoritmo de Euclides, $m = qr + l$ com $r > l \geq 0$, e portanto $x^m = x^{qr+l} = (x^r)^q \cdot x^l = e^q \cdot x^l = x^l$.

■

Proposição 1.2.4 *Seja $m \in \mathbb{Z}$. Então $\overline{m}$ gera o grupo $(\mathbb{Z}_n, +)$ se, e somente se, $mdc\{m, n\} = 1$*

Demonstração

Suponhamos que $\overline{m}$ gera $(\mathbb{Z}_n, +)$, então $\overline{1} = \overline{mp}$, para algum $\overline{p} \in \mathbb{Z}_n$. Assim $1 - mp \in n\mathbb{Z}$. Logo existe $q \in \mathbb{Z}$ tal que $1 - mp = nq$, isto é, $1 = nq + mp$. Portanto $mdc\{m, n\} = 1$. Reciprocamente, suponhamos que $mdc\{m, n\} = 1$. Então, pela Identidade de Bezout, existem $p, q \in \mathbb{Z}$ tais que $mp + nq = 1$. Assim

$$\overline{mp + nq} = \overline{mp} + \overline{nq} = \overline{mp} = \overline{1}.$$

Logo se $\overline{a} \in \mathbb{Z}_n$, então

$$\overline{a} = \overline{a}.\overline{1} = \overline{a}.\overline{mp} = \overline{m}.(\overline{a}.\overline{p}) = \overline{m}.(\overline{ap})$$

Portanto, $\overline{m}$ gera $(\mathbb{Z}_n, +)$

■

1.3 Classes Laterais e Teorema de Lagrange

Seja G um grupo e seja H um subgrupo de G. Vamos definir sobre G a seguinte relação R_H :

$$xR_Hy \Leftrightarrow \exists h \in H \ \textit{tal que} \ x = yh.$$

Dessa forma, R_H é uma relação de equivalência. De fato,

Reflexiva : $xR_Hx \Leftrightarrow \exists h \in H$ tal que $x = xh$. Basta tomar $h = e$, onde e é o elemento neutro de H.

Simétrica : $xR_Hy \Leftrightarrow \exists h \in H$ tal que $x = yh \Leftrightarrow xh^{-1} = y \Leftrightarrow yR_Hx$.

Transitiva : xR_Hy e $yR_Hz \Leftrightarrow \exists h_1, h_2$ tais que $x = yh_1$ e $y = zh_2 \Leftrightarrow x = yh_1 = zh_2h_1 = z(h_2h_1) \Leftrightarrow xR_Hz$

Similarmente, podemos definir a seguinte relação R'_H :

$$xR'_Hy \Leftrightarrow \exists h \in H \ \textit{tal que} \ x = hy$$

e, como na relação R_H, concluímos que R'_H é uma relação de equivalência.

Definição 1.3.1 *A classe de equivalência, segundo a relação R_H, que contém o elemento x é o conjunto*

$$\overline{x} = \{y \in G;\ yR_Hx\} \ = \ \{xh;\ h \in H\}$$

e denominamos Classe Lateral à esquerda de H. De modo análogo, definimos

$$\overline{x} = \{y \in G;\ yR'_Hx\} \ = \ \{hx;\ h \in H\}$$

a Classe Lateral à direita de H.

Obtemos assim a classe lateral à esquerda de H em G de x, denotada por xH e a classe lateral à direita de H em G de x, denotada por Hx.

Lema 1.3.1 *Seja H um subgrupo de um grupo G e sejam x, y dois elementos quaisquer de G. Então, $xH = yH$ se, e somente se, $Hx^{-1} = Hy^{-1}$.*

Demonstração

De $xH = yH$ resulta que $x^{-1}y \in H$, logo, $y^{-1}(x^{-1})^{-1} = (x^{-1}y)^{-1} \in H$ e então $Hx^{-1} = Hy^{-1}$. Reciprocamente, suponhamos que esta última igualdade seja verdadeira, assim temos $y^{-1}x = y^{-1}(x^{-1})^{-1} \in H$. Logo, $x^{-1}y = (y^{-1}x)^{-1} \in H$ e então $xH = yH$.

■

Seja H um subgrupo de um grupo G e considere a relação R_H determinada por H. Denotamos todas as classes de equivalência segundo esta relação por G/R_H. Dizemos que H tem índice (à esquerda) finito se, e somente se, o conjunto quociente G/R_H é finito e, neste caso, o número de elementos desse conjunto é denominado índice à esquerda de H em G. Caso contrário, dizemos que H tem índice à esquerda infinito. Essas noções aplicam-se também com o qualitativo "à direita", e consideramos o conjunto quociente G/R'_H.

O Lema 1.3.1 nos mostra que a aplicação $xH \mapsto Hx^{-1}$ é uma bijeção de G/R_H em G/R'_H e daqui resulta, em particular, que G/R_H é finito se, e somente se, G/R'_H o for. Com isso, não há necessidade de distinguir o índice à esquerda ou à direita de H em G e dizemos simplesmente que H tem índice finito ou infinito em G, e denotaremos por $(G : H)$. Logo,

$$(G : H) = \sharp G/R_H = \sharp G/R'_H.$$

Lema 1.3.2 *Se H é um subgrupo finito de um grupo G, então para todo elemento $a \in G$ temos $|H| = |aH| = |Ha|$.*

Demonstração

Basta notar que as aplicações $x \mapsto ax$ e $x \mapsto xa$, são, respectivamente, bijeções de H em aH e de H em Ha.

■

Seja G um grupo finito. Se H é um subgrupo de G então G/R_H é evidentemente finito; além disso, G/R_H é a reunião de $(G : H)$ classes laterais disjuntas duas a duas, e como estas classes têm o mesmo número de elementos, que é igual a $|H|$ *(lema 1.3.2)*, temos que $|G| = (G : H).|H|$. Fica assim demonstrado o seguinte Teorema:

Teorema 1.3.1 *(Lagrange) Para todo subgrupo H de um grupo finito G, tem-se*

$$|G| = (G : H).|H|$$

Em particular, a ordem e o índice de todo subgrupo de G dividem a ordem de G.

1.4 Grupos Quocientes e Homomorfismos

Seja H um subgrupo de um grupo G e considere as relações de equivalência R_H e R'_H determinadas por H. Para todo $x \in G$, xH e Hx são, respectivamente, as classes de equivalência módulo R_H e módulo R'_H determinadas por x.

Note que $R_H = R'_H$ se, e somente se, $xH = Hx$, qualquer que seja $x \in G$. Um subgrupo que satisfaz esta condição é denominado *subgrupo normal*, segundo a Definição 1.4.2 abaixo.

Definição 1.4.1 *Seja H um subgrupo normal de um grupo G e considere o conjunto quociente G/H de G pela relação de equivalência H. Os elementos desse conjunto são as classes laterais $xH = Hx$, $x \in G$. Sejam xH e yH duas classes laterais quaisquer. Definamos em G/H a operação*

Logo, o produto de duas classes laterais módulo H é uma classe lateral módulo H. Fica assim definida uma operação sobre o conjunto G/H.

Definição 1.4.2 *Seja H um subgrupo de G. Dizemos que H é um subgrupo normal de G, e denotamos $H \lhd G$ se as afirmações da proposição seguinte são satisfeitas:*

Proposição 1.4.1 *Seja H um subgrupo de G. As afirmações abaixo são equivalentes:*

(I) A operação induzida sobre as classes laterais à esquerda em G é bem definida;

(II) $\forall g \in G$, vale $gHg^{-1} \subset H$

(III) $\forall g \in G$, vale $gHg^{-1} = H$

(IV) $\forall g \in G$, vale $gH = Hg$, isto é, $\forall g \in G$, a classe lateral à esquerda de H é igual à classe lateral à direita de H.

Demonstração

(I)$\Leftrightarrow$ (II) Sejam $x, y \in G$ e $h, k \in H$ arbitrários, assim, x e xh são representantes da mesma classe xH, y e yk são representantes da mesma classe yH. Assim, a operação induzida sobre as classes laterais é bem definida se e somente se

$$xyH = xhykH\ ,\ \forall x, y \in G, \forall h, k \in H.$$

Logo, se e somente se

$$H = y^{-1}x^{-1}xyH = y^{-1}x^{-1}xhykH = y^{-1}hyH\ ,\ \forall y \in G\ ,\ \forall h \in H$$

e portanto se e somente se

$$yhy^{-1} \in H\ ,\ \forall y \in G\ ,\ \forall h \in H.$$

(III)$\Rightarrow$ (II) (óbvio)

(II)$\Rightarrow$ (III) Suponhamos que $gHg^{-1} \subset H$, $\forall g \in G$; o objetivo é mostrar que $H \subset gHg^{-1}$, $\forall g \in G$. Sejam então $h \in H$ e $g \in G$, temos que:

$$h = g(g^{-1}hg)g^{-1} \in g(g^{-1}Hg)g^{-1} \subset gHg^{-1}$$

pois $g^{-1}Hg \subset H$, por hipótese.

(III)$\Rightarrow$(IV)

$$gHg^{-1} = H \Rightarrow gHg^{-1}g = Hg \Rightarrow gH = Hg\ ,\ \forall g \in G.$$

(IV)$\Rightarrow$ (III)

$$gH = Hg \Rightarrow gHg^{-1} = Hgg^{-1} = H$$

■

Proposição 1.4.2 *Seja H um subgrupo normal de um grupo G e considere o conjunto quociente G/H. A operação*

$$(xH, yH) \longrightarrow (xy)H$$

define uma estrutura de grupo sobre o conjunto G/H.

Demonstração

O axioma G_1 segue da associatividade de G e da definição da operação em G/H. Assim pelo Teorema 1.1.1 basta verificar os axiomas G_2' e G_3'.

G_2': Considerando o conjunto H temos que, para toda classe lateral xH de G/H:

$$(xH)H = (xH).(eH) = xeH = xH.$$

G_3': Seja xH uma classe lateral qualquer e considere a classe lateral $x^{-1}H \in G/H$. Logo

$$(xH)(x^{-1}H) = (xx^{-1})H = eH = H.$$

■

O grupo $(G/H, \cdot)$ passa a ser denominado *grupo quociente* de $(G, \cdot)$ pelo subgrupo normal H.

Com o Teorema acima concluímos que o elemento neutro do grupo quociente $(G/H, \cdot)$ é o subconjunto H e o inverso de cada elemento xH é a classe lateral $x^{-1}H$.

Vejamos alguns exemplos de subgrupos normais

Exemplo 1.4.1 Todo grupo G admite pelo menos dois subgrupos normais, a saber: $\{e\}$ e G.

Exemplo 1.4.2 Seja G um grupo e $Z(G)$ seu centro. então $Z(G)$ é um subgrupo normal de G

Exemplo 1.4.3 Seja G um grupo e H um subgrupo de G. Se o índice de H em G é 2 então H é um subgrupo normal de G.

Exemplo 1.4.4 Todo subgrupo de um grupo abeliano é normal.

Exemplo 1.4.5 Seja o grupo aditivo $\mathbb{Z}$ dos números inteiros e seja H um subgrupo de $\mathbb{Z}$. Conforme a Proposição 1.2.2 existe um único número natural n tal que $H = n\mathbb{Z}$ e note que H é normal em $\mathbb{Z}$. Se x e y são dois elementos quaisquer de $\mathbb{Z}$, então $x \equiv y(mod H)$ se, e somente se, $x - y \in H = n\mathbb{Z}$, ou seja, se e somente se, $x \equiv y(mod n)$, portanto, a relação de equivalência determinada por H coincide com a congruência módulo n, e mais, o conjunto quociente $\mathbb{Z}/n\mathbb{Z}$ tem exatamente n elementos.

Definição 1.4.3 *Sejam G e G' dois grupos e seja f uma aplicação do conjunto G no conjunto G'. Dizemos que f é um homomorfismo de $(G, \cdot)$ em $(G', \times)$ se, e somente se:*

$$f(a \cdot b) = f(a) \times f(b)$$

quaisquer que sejam a e b em G. Se o grupo G é aditivo e G' é multiplicativo então representaremos esta fórmula por

$$f(a + b) = f(a) \cdot f(b).$$

Definição 1.4.4 *Se f é um homomorfismo sobrejetor de G em G' então dizemos que f é um epimorfismo de G em G'.*

Se f é um homomorfismo injetivo de G em G' então dizemos que f é um monomorfismo de G em G'.

Finalmente, se f é um homomorfismo bijetivo de G em G' então dizemos que f é um isomorfismo de G em G' . Neste caso também dizemos que G é um grupo isomorfo ao grupo G' e denotamos por $G \simeq G'$.

Um homomorfismo de G em G é denominado endomorfismo de G e um isomorfismo de G em G é chamado automorfismo de G.

Indicamos por $Hom(G, G')$ o conjunto de todos os homomorfismos de G em G' e denotamos $End(G) = Hom(G, G)$. Além disso, indicamos por $Aut(G)$ o conjunto de todos os automorfismos do grupo G.

Teorema 1.4.1 *Para todo homomorfismo f de um grupo G num grupo G' valem as seguintes propriedades:*

(a) $f(e)$ é o elemento neutro de G';

(b) $f(a^{-1}) = (f(a))^{-1}$;

(c) Se H é um subgrupo de G, então $f(H)$ é um subgrupo de G'

(d) Se K' é um subgrupo de G', então $K = f^{-1}(K')$ é um subgrupo de G e, além disso, se $K' \lhd G'$ então $K \lhd G$.

Demonstração

(a) $f(e) = f(e \cdot e) = f(e) \cdot f(e)$ e daqui resulta que $f(e)$ é o elemento neutro de G'.

(b) $f(e) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$, logo, $f(a^{-1}) = (f(a))^{-1}$.

(c) É imediato que $f(H)$ é não vazio, pois $e \in H$ e portanto $f(e) \in f(H)$. Se a' e b' são dois elementos quaisquer de $f(H)$ então $a' = f(a)$ e $b' = f(b)$, com a e b em H, logo, $a^{-1}b \in H$ e como $a'^{-1}b' = (f(a))^{-1} \cdot f(b) = f(a^{-1}) \cdot f(b) = f(a^{-1}b)$ resulta que $a'^{-1}b' \in f(H)$.

(d) É imediato que $K = f^{-1}(K')$ é não vazio, pois $f(e) \in K'$ e portanto $e \in f^{-1}(K')$. Se a e b são dois elementos quaisquer de K, então $f(a) \in K'$ e $f(b) \in K'$, logo $f(a^{-1}b) = f(a^{-1})f(b) = (f(a))^{-1}f(b) \in K'$, donde $a^{-1}b \in K$ e fica assim demonstrado que K é um subgrupo de G. Finalmente, seja x um elemento qualquer de G e considere um elemento y de xKx^{-1}. Logo $y = xax^{-1}$ com $a \in K$, donde resulta que $f(y) = f(x)f(a)f(x)^{-1}$ e como $f(a) \in K'$ e K' é normal em G' temos que $f(y) \in K'$, isto é, $y \in K$ e fica assim demonstrado que $xKx^{-1} \subset K$.

■

Definição 1.4.5 *Para todo homomorfismo $f : G \to G'$, a imagem da aplicação f, indicada por $Im(f)$, passa a ser denominada imagem do homomorfismo f. O conjunto de todos os elementos $a \in G$ tais que $f(a) = e'$, onde e' indica o elemento neutro de G' é denominado núcleo ou Kernel do homomorfismo f e será indicado por $Ker(f)$. Assim, concluímos que $Ker(f) = f^{-1}(e')$, logo $Ker(f)$ é um subgrupo normal de G, e ainda, todo subgrupo normal H de G é o núcleo de algum homomorfismo, pois a aplicação*

$$\phi : G \to G/H$$

é um homomorfismo cujo núcleo é H.

Teorema 1.4.2 *Se $f : G \to G'$ é um isomorfismo, então a aplicação inversa $f^{-1} : G' \to G$ é um isomorfismo.*

Demonstração

É óbvio que f^{-1} é uma bijeção de G' em G. Por outro lado, se a' e b' são dois elementos quaisquer de G', então existem a e b em G tais que $f(a) = a'$ e $f(b) = b'$. Logo $a'b' = f(a)f(b) = f(ab)$, donde $f^{-1}(a'b') = ab = f^{-1}(a')f^{-1}(b')$. Portanto f^{-1} é um homomorfismo bijetivo.

■

Teorema 1.4.3 *(Teorema dos homomorfismos) Seja $f : G \to G'$ um homomorfismo de grupos. Então:*

1) A função

$$\begin{array}{rcl} \overline{f} : G/Ker(f) & \longrightarrow & f(G) \\ g(Ker(f)) & \longmapsto & f(g) \end{array} \quad \textit{é um isomorfismo.}$$

2) Temos ainda as seguintes bijeções:

$$\left\{ \begin{array}{c} \textit{Subgrupos de } G \\ \textit{que contém} Ker(f) \end{array} \right\} \Leftrightarrow \{\textit{Subgrupos de } f(G)\}$$

$$H \longmapsto f(H)$$

$$f^{-1}(H') \longmapsto H'$$

Além disso, estas bijeções levam subgrupos normais em subgrupos normais, ou seja:

(a) $H \lhd G \Rightarrow f(H) \lhd f(G)$

(b) $H' \lhd f(G) \Rightarrow f^{-1}(H') \lhd G$

Demonstração

1) Primeiramente devemos verificar que $\overline{f}$ é um função bem definida, isto é, se $g(Ker(f)) = \bar{g}(Ker(f))$ então $f(g) = f(\bar{g})$. Mas, $g(Ker(f)) = \bar{g}(Ker(f))$ implica que $g = \bar{g}k$, para algum $k \in Ker(f)$ e portanto $f(g) = f(\bar{g}k) = f(\bar{g})f(k) = = f(\bar{g})e_{G'} = f(\bar{g})$.

É de imediato que $\overline{f}$ é uma função sobrejetora. Para g, g' em G, temos:

$$\overline{f}(g(Ker(f)) \cdot g'(Ker(f)) = \overline{f}(g \cdot g'(Ker(f)) = f(gg') = f(g) \times f(g') =$$

$$= \overline{f}(g(Ker(f))) \times \overline{f}(g'(Ker(f)))$$

assim, $\overline{f}$ é um homomorfismo.

$$Ker(\overline{f}) = \{g(Ker(f));\ f(g) = e_{G'}\} = \{g(Ker(f));\ g \in Ker(f)\}$$

assim, $Ker(\overline{f}) = \{e.Ker(f)\}$ ou seja, $\overline{f}$ é injetiva.

Portanto, $\overline{f}$ é um isomorfismo.

Para provarmos o segundo item do teorema provaremos inicialmente os seguintes Lemas:

Lema 1.4.1 *Se H é um subgrupo de G então $f(H)$ é um subgrupo de G' e $f^{-1}(f(H)) =$ $= H(Ker(f))$.*

Demonstração

Seja $hk \in H(Ker(f))$, isto é, $h \in H$ e $k \in Ker(f)$. Temos $f(hk) =$ $= f(h) \times f(k) = f(h) \cdot e_{G'} = f(h) \in f(H)$, fica provado que $H(Ker(f)) \subset f^{-1}(f(H))$. Para provar a inclusão contrária, tomemos $y \in f^{-1}(f(H))$. Por definição, temos $f(y) \in f(H)$, então existe $h \in H$ tal que $f(y) = f(h)$, logo $f(h^{-1}y) = f(h)^{-1} \times f(y) =$ $= e_{G'}$, isto é, $h^{-1}y \in Ker(f)$. Assim, $y = h(h^{-1}y) \in HKer(f)$. Logo $f^{-1}(f(H)) \subseteq$ $Hker(f)$.

■

Lema 1.4.2 *Se H' é um subgrupo de G' então $f(f^{-1}(H') = H' \cap f(G)$.*

Demonstração

É óbvio que $f(f^{-1}(H')) \subset H' \cap f(G)$. Para provar a inclusão oposta, tomemos $y \in H' \cap f(G)$, como $y \in f(G)$, existe $g \in G$ tal que $f(g) = y$. De $y \in H'$, obtemos
$g \in f^{-1}(H')$ e assim $y = f(g) \in f(f^{-1}(H'))$.

■

Demonstração do item 2):

Se $H \supseteq Ker(f)$ então $f^{-1}(f(H)) = H$ e se $H' \subseteq f(G)$ então $f(f^{-1}(H')) = H'$. Obtemos assim que as duas funções definidas em 2) são uma a inversa da outra. Falta mostrar que essas funções levam subgrupos normais em subgrupos normais.

(a) Dados $y \in f(G)$ e $x \in f(H)$ quaisquer, devemos mostrar que $yxy^{-1} \in f(H)$. Mas $y = f(g)$ e $x = f(h)$ com $g \in G$ e $h \in H$ e logo $yxy^{-1} = f(g)f(h)f(g)^{-1} =$ $= f(ghg^{-1})$. Como por hipótese $H \lhd G$, segue que $ghg^{-1} \in H$ e portanto $yxy^{-1} \in f(H)$.

(b) Dados $g \in G$ e $\alpha \in f^{-1}(H')$ quaisquer, devemos mostrar que $g\alpha g^{-1} \in f^{-1}(H')$. Mas $f(g\alpha g^{-1}) = f(g)f(\alpha)f(g)^{-1}$ e $f(\alpha) \in H'$. Como por hipótese $H' \lhd f(G)$ segue que $f(g\alpha g^{-1}) \in H'$ e portanto $g\alpha g^{-1} \in f^{-1}(H')$.

■

Note que se

$$\begin{array}{rccc} \varphi: & (G,\cdot) & \longrightarrow & (G',\star) \\ & g & \longmapsto & \varphi(g) \end{array}$$

é um isomorfismo, então para todo elemento x de G temos $O(x) = O(\varphi(x))$. De fato, basta notar que φ sendo uma bijeção leva cada elemento de $< x >$ em apenas um elemento de $< \varphi(x) >$ e portanto $O(x) = O(\varphi(x))$.

Vejamos alguns exemplos de homomorfismos e isomorfismos de grupos

Exemplo 1.4.6 $\begin{array}{rccc} Id: & (G,\cdot) & \longrightarrow & (G,\cdot) \\ & g & \longmapsto & Id(g) = g \end{array}$

é um homomorfismo chamado *identidade.*

Exemplo 1.4.7 $\begin{array}{rccc} e: & (G,\cdot) & \longrightarrow & (G,\cdot) \\ & g & \longmapsto & e(g) = e_G \end{array}$

é um homomorfismo chamado *trivial.*

Exemplo 1.4.8 Seja $n \in \mathbb{Z}$ fixo. Então $\begin{array}{rccc} \varphi_n: & (\mathbb{Z},+) & \longrightarrow & (\mathbb{Z},+) \\ & z & \longmapsto & \varphi_n(z) = n\mathbb{Z} \end{array}$

é um homomorfismo. Mais geralmente, se $(G,\cdot)$ é um grupo abeliano então

$$\begin{array}{rccc} \varphi_n: & (G,\cdot) & \longrightarrow & (G,\cdot) \\ & g & \longmapsto & \varphi_n(g) = g^n \end{array}$$

é um homomorfismo.

Exemplo 1.4.9 Seja $H \lhd G$ e considere o grupo quociente G/H. A aplicação

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & G/H \\ & g & \longmapsto & \varphi(g) = gH \end{array}$$

é um homomorfismo chamado de *projeção canônica ou homomorfismo canônico.*

Exemplo 1.4.10 Seja $(\mathbb{R},+)$ o grupo aditivo dos números reais e $(\mathbb{R}_+^*,\cdot)$ o grupo multiplicativo dos números reais estritamente positivos. Se $a \neq 1$ é um número real estritamente positivo então a aplicação

$$\begin{array}{rccc} \varphi: & (\mathbb{R},+) & \longrightarrow & (\mathbb{R}_+^*,\cdot) \\ & x & \longmapsto & \varphi(x) = a^x \end{array}$$

é um isomorfismo. Analogamente, a aplicação

$$\begin{array}{rccl} \phi: & (\mathbb{R}_+^*, \cdot) & \longrightarrow & (\mathbb{R}, +) \\ & x & \longmapsto & \phi(x) = log_a x \end{array}$$

é um isomorfismo.

Exemplo 1.4.11 Os grupos S_3 e D_3 são isomorfos. De fato, considerando a aplicação φ abaixo:

$$\begin{array}{rccl} \varphi: & S_3 & & \longrightarrow D_3 \\ & id & & \longmapsto id \\ & \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha \right. & & \longmapsto R_{\frac{2\pi}{3}} \\ & \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \alpha^2 \right. & & \longmapsto R_{\frac{4\pi}{3}} \\ & \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \beta \right. & & \longmapsto R_3 \\ & \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \alpha\beta \right. & & \longmapsto R_2 \\ & \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \alpha^2\beta \right. & & \longmapsto R_1 \end{array}$$

É fácil verificar que φ é um homomorfismo, e conforme a definimos, φ é uma bijeção. Portanto, φ é um isomorfismo.

Exemplo 1.4.12 Seja o seguinte subconjunto H de S_4:

$$\mathrm{H}= \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \right\}$$

Temos que os grupos H e D_4 são isomorfos. De fato, considerando a aplicação ϕ abaixo:

$$
\begin{array}{rlll}
\phi: & H & & \longrightarrow D_4 \\
& id & & \longmapsto id \\
& \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{array}\right) = \alpha & & \longmapsto R_{\frac{\pi}{2}} \\
& \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{array}\right) = \alpha^2 & & \longmapsto R_{\pi} \\
& \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{array}\right) = \alpha^3 & & \longmapsto R_{\frac{3\pi}{2}} \\
& \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{array}\right) = \beta & & \longmapsto R_N \\
& \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{array}\right) = \alpha\beta & & \longmapsto R_1 \\
& \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{array}\right) = \alpha^2\beta & & \longmapsto R_M \\
& \left(\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{array}\right) = \alpha^3\beta & & \longmapsto R_2
\end{array}
$$

É fácil verificar que ϕ é um homomorfismo, e conforme a definimos, ϕ é uma bijeção. Portanto, ϕ é um isomorfismo.

1.5 Grupos Cíclicos

Definição 1.5.1 *Dizemos que um grupo G é cíclico se, e somente se, existe um elemento $a \in G$ tal que $G = < a >$. Todo elemento a que satisfaz esta condição é denominado gerador do grupo cíclico G.*

Proposição 1.5.1 *Seja $G = \{\ldots, a^{-1}, e, a, a^2, \ldots\}$ um grupo cíclico de ordem infinita. Então:*

(a) A função $\varphi: \begin{array}{ll} (\mathbb{Z}, +) & \longrightarrow (G, \cdot) \\ z & \longmapsto \varphi(z) = a^z \end{array}$

é um isomorfismo

(b) O elemento a^z gera G se e somente se $z = 1$ ou $z = -1$.

Demonstração

(a) φ é um homomorfismo, pois para quaisquer $z_1, z_2 \in \mathbb{Z}$

$$\varphi(z_1 + z_2) = a^{z_1+z_2} = a^{z_1} \cdot a^{z_2} = \varphi(z_1) \cdot \varphi(z_2).$$

Se $\varphi(z_1) = \varphi(z_2) \Rightarrow a^{z_1} = a^{z_2} \Rightarrow a^{z_1 - z_2} = e \Rightarrow z_1 - z_2 = 0 \Rightarrow z_1 = z_2$. Provando que φ é injetiva. Como a sobrejetividade é evidente, temos que φ é um isomorfismo.

(b) A função $\varphi : z \mapsto a^z$ sendo um isomorfismo, a^z gera G se e somente se z gera $\mathbb{Z}$, e os únicos elementos que geram $\mathbb{Z}$ são $z = 1$ e $z = -1$.

■

Proposição 1.5.2 *Seja $G = \{e, a, a^2, \ldots, a^{n-1}\}$ um grupo cíclico de ordem finita igual a n. Então*

(a) A função $\psi : \begin{array}{lll} (\mathbb{Z}/n\mathbb{Z}, +) & \longrightarrow (G, \cdot) & \\ \overline{m} & \longmapsto \psi(\overline{m}) = a^m & \end{array}$ *é um isomorfismo.*

(b) O elemento a^m gera G se e somente se $mdc\{m, n\} = 1$.

Demonstração

(a) Pela proposição anterior, φ de $\mathbb{Z}$ em G dada por $z \mapsto a^z$ é um homomorfismo sobrejetor. Logo $\mathbb{Z}/Ker(\varphi)$ é isomorfo a G. Como G tem n elementos vem que $Ker(\varphi) = n\mathbb{Z}$. Portanto, $\varphi = \overline{\varphi}$ obtido do teorema dos homomorfismos é um isomorfismo.

(b) A função $\overline{m} \mapsto a^m$ sendo um isomorfismo, a^m gera G se, e somente se, $\overline{m}$ gera $(\mathbb{Z}/n\mathbb{Z}, +)$, e pela proposição 1.2.4, $\overline{m}$ gera $(\mathbb{Z}/n\mathbb{Z}, +)$ se, e somente se, $mdc\{m, n\} = 1$.

■

Proposição 1.5.3 *Seja $G = \{e, a, a^2, \cdots, a^{n-1}\}$ um grupo cíclico finito de ordem n.*

(a) Se $H \neq \{e\}$ é um subgrupo de G, então H é cíclico. De maneira precisa, $H = < a^m >$, onde m é o menor inteiro positivo tal que $a^m \in H$. H tem ordem igual a n/m.

(b) Se d é um divisor de n, então existe um único subgrupo H de G de ordem igual a d. Este subgrupo é $H = < a^{n/d} >$

Demonstração

(a) Seja m o menor inteiro positivo tal que $a^m \in H$. Segue que $< a^m > \subseteq H$. Reciprocamente, $a^u \in H$, fazendo a divisão de u por m temos:

$$u = qm + r \qquad \text{com} \qquad 0 \leq r < m.$$

Então $a^u = (a^m)^q . a^r$. Como $a^u \in H$ e $a^m \in H$; segue que $a^r = a^{u-mq} \in H$ e portanto, pela minimalidade de m, temos $r = 0$. Logo $m|u$ e portanto $a^u \in < a^m >$. Agora, $|G| = |H|.(G : H) \Rightarrow n = |H|.m \Rightarrow |H| = n/m$.

(b) Seja d um divisor de n. O subgrupo $< a^{n/d} >$ tem ordem d. Para provarmos a unicidade, seja então H um subgrupo de ordem d. Pela parte (a), $H =< a^m >$ com m inteiro tal que n/m , isto é, $n/m = d$. Portanto $m = n/d$ e $H =< a^{n/d} >$.

■

Proposição 1.5.4 *Seja G um grupo. Se $|G| = p$, p primo, então G é cíclico.*

Demonstração

Seja $\alpha \in G\backslash\{e\}$ e considere $< \alpha >$ o subgrupo gerado por α. Pelo Teorema de Lagrange, temos $| < \alpha > |$ divide $|G|$ e portanto que $| < \alpha > | = |G|$, pois $|G|$ é primo. Logo $G =< \alpha >$.

■

Vejamos dois exemplos de Grupos Cíclicos

Exemplo 1.5.1 O grupo aditivo $\mathbb{Z}$ dos Inteiro é cíclico, pois $\mathbb{Z} =< 1 >$.

Exemplo 1.5.2 Para todo número inteiro n, o Grupo aditivo $\mathbb{Z}_n$ dos Inteiros módulo n é cíclico, pois $\mathbb{Z}_n =< \overline{1} >$.

Através das proposições 1.5.1 e 1.5.2 concluímos que estes dois exemplos acima incluem, a menos de isomorfismo, todos os grupos cíclicos.

1.6 Teoremas de Sylow

Teorema 1.6.1 *(1o. Teorema de Sylow) Seja G um grupo finito de ordem $p^m b$ com p primo e $mdc\ \{p, b\} = 1$. Então, para cada n, $0 \leq n \leq m$, existe um subgrupo H de G tal que $|H| = p^n$.*

Embora não demonstraremos os Teoremas de Sylow, conforme dito na descrição deste capítulo, demonstraremos o teorema abaixo, que nos será bastante útil para o desenvolvimento dos capítulos seguintes. As demonstrações dos Teoremas de Sylow podem ser encontradas no livro *Garcia A. & Lequain, Y, Álgebra: Um Curso de Introdução - IMPA - Rio de Janeiro, 1988. Capítulo IV.2*

Teorema 1.6.2 *(Cauchy) Seja G um grupo abeliano finito. Seja p um primo que divide $|G|$. Então existe $x \in G$ de ordem p.*

Demonstração

Faremos a demonstração usando o segundo pricípio de indução finita sobre $|G|$.

Se $|G| = 1$, não há nada para fazer.

Se $|G| > 1$, suponhamos, como hipótese de indução, que o Teorema vale para todos os grupos abelianos de ordem menor que $|G|$, queremos mostrar que o Teorema vale também para o grupo G.

Se $p = |G|$, então G é cíclico e qualquer gerador de G tem ordem p e, neste caso, não precisamos usar a hipótese de indução.

Se $p \neq |G|$, afirmamos primeiro que existe um subgrupo H tal que $1 < |H| < |G|$. De fato, tome $y \in G$, $y \neq e$, se $< y > \neq G$ então $H = < y >$ serve. Se $< y > = G$, então $y^p \neq e$ e $H = < y^p >$ serve, pois $|H| = O(y^p) = \frac{|G|}{p} < |G|$.

Agora, se p divide $|H|$ então, pela hipótese de indução, existe $x \in H \subseteq G$ de ordem p, e acabou.

Se p não divide $|H|$ então, pela igualdade $|G| = |H| \cdot |G/H|$, vemos que p divide $|G/H|$ e que $|G/H| < |G|$. Logo, pela hipótese de indução, existe $\overline{z} \in G/H$ de ordem p. Considere o homomorfismo canônico $\varphi : G \to G/H$, tome $z \in G$ tal que $\varphi(z) = \overline{z}$. Seja r a ordem de z. De $z^r = e$, temos $\varphi(z^r) = \varphi(e)$ ou seja $\overline{z}^r = \overline{e}$, portanto, r é um múltiplo da ordem de $\overline{z}$, isto é, um múltiplo de p, digamos $r = kp$ com $k \geq 1$; então z^k é um elemento de G de ordem p.

■

Corolário 1.6.1 *(Generalização do Teorema de Cauchy para grupos não necessariamente abelianos) Sejam G um grupo finito e p um primo que divide $|G|$. Então existe*

$x \in G$ *de ordem* p.

Corolário 1.6.2 *Sejam G um grupo finito e p um primo. Seja p^m a maior potência de p que divide $|G|$. Então existe um subgrupo de G de ordem p^m.*

Definição 1.6.1 *Sejam G um grupo finito, p um primo e p^m a maior potência de p que divide $|G|$. Os subgrupos de G que têm ordem p^m, cuja existência está garantida pelo Corolário 1.6.2, são chamados p-subgrupos de Sylow de G.*

Observe que se p é um primo que não divide $|G|$, então $\{e\}$ é o único p-subgrupo de Sylow de G.

Corolário 1.6.3 *Sejam G um grupo finito e p um número primo. Então $|G|$ é igual a uma potência de p se e só se cada elemento de G tem ordem igual a uma potência de p.*

Definição 1.6.2 *Seja p um primo. Um grupo G , não necessariamente finito, no qual todo elemento tem ordem igual a uma potência de p é chamado um p-grupo.*

Vejamos alguns exemplos de p-grupos.

1) $D_4, Q_3, \mathbb{Z}/8\mathbb{Z}, \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}, \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ são 2-grupos de ordem $8 = 2^3$.

2) $(\mathbb{Z}/p^n\mathbb{Z}, +)$ é um p-grupo de ordem p^n.

3) $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \ldots$ é um 2-grupo infinito.

O Corolário anterior diz que os p-grupos finitos são exatamente os grupos cuja ordem é uma potência do primo p.

Teorema 1.6.3 *(2o. Teorema de Sylow) Sejam G um grupo finito e p um primo. Então:*

i) Todos os p-subgrupos de Sylow de G são conjugados entre si. Em particular, um p-subgrupo de Sylow S de G é normal em G se, e somente se, S é o único p-subgrupo de Sylow de G. Neste caso, S é um subgrupo característico de G.

ii) Se P é um p-subgrupo de G, então existe um p-subgrupo de Sylow S de G tal que $P \subseteq S$.

Teorema 1.6.4 *(3o. Teorema de Sylow) Seja G um grupo finito de ordem $p^m b$ com p primo e $mdc\{p, b\} = 1$. Seja S um p-subgrupo de Sylow de G e seja n_p o número de p-subgrupos de Sylow de G. Então*

$$\begin{cases} n_p \text{ divide } b \\ n_p \equiv 1 \,(mod\, p) \end{cases}$$

1.7 Produto Direto

Seja $\{G_i\}_{1\leq i\leq n}$ uma família não vazia de grupos multiplicativos e seja $G = G_1 \times G_2 \times \ldots \times G_n$ o produto cartesiano dos conjuntos $G_1, G_2, \ldots, G_n$. Sejam $(g_1, g_2, \ldots, g_n)$ e $(h_1, h_2, \ldots, h_n)$ dois elementos quaiquer de G e definamos em G a seguinte operação:

$$(g_1, g_2, \ldots, g_n).(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n)$$

Desta forma, G munido desta operação é um grupo chamado *Grupo produto direto da família* $\{G_i\}_{1\leq i\leq n}$. De fato, para todo $g_i \in G_i$ existe $g_i^{-1} \in G_i$, para todo $i \in \{1, 2, \ldots, n\}$, pois G_i é um grupo. Logo, se $(g_1, g_2, \ldots, g_n)$ é um elemento qualquer de G, o seu inverso é um elemento de G e é dado por:

$$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}) \in G$$

Da mesma forma, se g_i e h_i são dois elementos quaisquer de G_i então $g_ih_i^{-1} \in G_i$, $\forall i \in \{1, 2, \ldots, n\}$. Logo, se $(g_1, g_2, \ldots, g_n)$ e $(h_1, h_2, \ldots, h_n)$ são dois elementos quaisquer de G então

$$(g_1, g_2, \ldots, g_n).(h_1, h_2, \ldots, h_n)^{-1} = (g_1, g_2, \ldots, g_n).(h_1^{-1}, h_2^{-1}, \ldots, h_n^{-1}) =$$

$$= (g_1h_1^{-1}, g_2h_2^{-1}, \ldots g_nh_n^{-1}) \in G.$$

A propriedade associativa é evidente em G. Portanto, G é um grupo. É fácil ver que o elemento neutro de G é $(e_1, e_2, \ldots e_n)$ onde e_i é o elemento neutro de G_i , $\forall i \in \{1, 2, \ldots, n\}$.

Afirmamos que $G = G_1 \times G_2 \times \ldots \times G_n$ é abeliano se, e somente se, G_i é abeliano, $\forall i \in \{1, 2, \ldots, n\}$. De fato, se G é abeliano então para quaisquer dois elementos $(g_1, g_2, \ldots, g_n), (h_1, h_2, \ldots, h_n)$ de G temos

$$(g_1, g_2, \ldots, g_n).(h_1, h_2, \ldots, h_n) = (h_1, h_2, \ldots, h_n).(g_1, g_2, \ldots, g_n) ,$$

ou seja,

$$(g_1h_1, g_2h_2, \ldots, g_nh_n) = (h_1g_1, h_2g_2, \ldots, h_ng_n) \ , \ \forall i \in \{1, 2, \ldots, n\}.$$

Logo, G_i é abeliano, $\forall i \in \{1, 2, \ldots, n\}$. Por outro lado, se G_i é abeliano $\forall i \in$

$\{1, 2, \ldots, n\}$ então $g_i h_i = h_i g_i$. Logo,

$$(g_1\,,\, g_2\,,\, \ldots\,,\, g_n).(h_1\,,\, h_2\,,\, \ldots\,,\, h_n) = (g_1h_1\,,\, g_2h_2\,,\, \ldots\,,\, g_nh_n) =$$

$$= (h_1g_1\,,\, h_2g_2\,,\, \ldots\,,\, h_ng_n) = (h_1\,,\, h_2\,,\, \ldots\,,\, h_n).(g_1\,,\, g_2\,,\, \ldots\,,\, g_n).$$

Portanto G é abeliano e fica assim demonstrada a afirmação acima.

No caso em que G_i , $\forall i \in \{1, 2, \ldots, n\}$ é um grupo aditivo é natural substituirmos a frase *Produto Direto* por *Soma Direta* e substituimos a operação de multiplicação pela operação de adição, ou seja, dados $(g_1\,,\, g_2\,,\, \ldots\,,\, g_n), (h_1\,,\, h_2\,,\, \ldots\,,\, h_n)$ dois elementos quaisquer de G, temos

$$(g_1\,,\, g_2\,,\, \ldots\,,\, g_n).(h_1\,,\, h_2\,,\, \ldots\,,\, h_n) = (g_1 + h_1\,,\, g_2 + h_2\,,\, \ldots\,,\, g_n + h_n).$$

Feitas as considerações acima, podemos apresentar a definição formal de Produto Direto Interno.

Definição 1.7.1 *Sejam G um grupo e $G_1, G_2, \ldots, G_n$ subgrupos de G. Dizemos que G é produto direto interno de $G_1, G_2, \ldots, G_n$, e denotaremos por $G = G_1 \odot G_2 \odot \ldots \odot G_n$, se as condições seguintes são satisfeitas:*

1) Para todo $z \in G$ existem únicos $x_1 \in G_1, \ldots, x_n \in G_n$ tais que $z = x_1x_2 \ldots x_n$.

2) Para $i \neq j$, $x \in G_i$ e $y \in G_j$, temos $xy = yx$.

Vamos apresentar um sistema de condições que é equivalente ao da definição acima e que é melhor para cálculos.

Proposição 1.7.1 *Sejam G um grupo e $G_1, G_2, \ldots, G_n$ subgrupos de G. Então, G é o produto direto interno de $G_1, G_2, \ldots, G_n$ se e somente se as condições seguintes são satisfeitas:*

3) $G_i \lhd G$, $\forall i = 1, 2, \ldots, n$.

4) $G = G_1G_2 \ldots G_n$.

5) $G_i \cap G_1 \ldots G_{i-1}G_{i+1} \ldots G_n = \{e\}$, $\forall i \in \{1, 2, \ldots, n\}$.

Demonstração

Suponhamos que as condições 3), 4) e 5) estão satisfeitas. Sejam $x \in G_i$ e $y \in G_j$, com $i \neq j$ e considere o elemento $xyx^{-1}y^{-1}$. Temos $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in$

G_j, pois $G_j \lhd G$, e $xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in G_i$, pois $G_i \lhd G$, assim $xyx^{-1}y^{-1} \in G_i \cap G_j \subseteq G_i \cap G_1 \dots G_{i-1}G_{i+1} \dots G_n = \{e\}$. Logo $xyx^{-1}y^{-1} = e$ e portanto $xy = yx$, isto é, a condição 2) está satisfeita. Seja agora $z \in G$. Pela condição 4), existem $x_i \in G_i$, $i \in \{1, 2, \dots, n\}$ tais que $z = x_1x_2 \dots x_n$. Queremos mostrar que os x_i's são únicos. Suponhamos então que $x_1 \dots x_n = y_1 \dots y_n$ com $y_i \in G_i$; multiplicando ambos os lados por y_1^{-1} à esquerda e por $x_n^{-1}x_{n-1}^{-1} \dots x_2^{-1}$ à direita obtemos que $y_1^{-1}x_1 = y_2y_3 \dots y_{n-1}y_nx_n^{-1}x_{n-1}^{-1} \dots x_2^{-1}$. Usando repetidas vezes a condição 2), que já sabemos ser satisfeita, obtemos que

$$y_1^{-1}x_1 = y_2x_2^{-1}y_3x_3^{-1} \dots y_nx_n^{-1}$$

e então $y_1^{-1}x_1 \in G_1 \cap G_2 \dots G_n = \{e\}$ ou seja $x_1 = y_1$. De $x_1x_2 \dots x_n = y_1y_2 \dots y_n$ e $x_1 = y_1$, tiramos que $x_2 \dots x_n = y_2 \dots y_n$. Procedendo como acima, obtemos que

$$y_2^{-1}x_2 = y_3x_3^{-1} \dots y_nx_n^{-1}$$

e então $y_2^{-1}x_2 \in G_2 \cap G_3 \dots G_n \subseteq G_2 \cap G_1G_3 \dots G_n = \{e\}$ ou seja $x_2 = y_2$. Continuando desta maneira obtemos que a condição 1) está satisfeita. Reciprocamente, suponhamos que as condições 1) e 2) são satisfeitas. Sejam então $y \in G_i$ e $z \in G$; queremos mostrar que $zyz^{-1} \in G_i$. Pela condição 1), temos $z = x_1x_2 \dots x_n$ com $x_j \in G_j$ e portanto

$$zyz^{-1} = x_1 \dots x_ix_{i+1} \dots x_nyx_n^{-1} \dots x_{i+1}^{-1}x_i^{-1}x_{i-1}^{-1} \dots x_1^{-1}.$$

Aplicando repetidamente a condição 2) ao elemento y com os elementos x_j, $j = i+1, \dots, n$, obtemos

$$zyz^{-1} = x_1 \dots x_iyx_i^{-1} \dots x_1^{-1}.$$

Agora, aplicando repetidamente a condição 2) ao elemento $x_iyx_i^{-1}$, que pertence a G_i, com os elementos x_j, $j = 1, \dots, i-1$, obtemos

$$zyz^{-1} = x_iyx_i^{-1}.$$

Logo zyz^{-1} pertence a G_i. Isto prova que a condição 3) é satisfeita.

A condição 4) é claramente satisfeita pois ela é mais fraca que a condição 1). Provaremos agora que a condição 5) é satisfeita. Seja $z \in G_i \cap G_1 \dots G_{i-1}G_{i+1} \dots G_n$;

como $z \in G_i$, podemos escrever

$$z = x_1 x_2 \ldots x_n, \text{ com } x_j \in G_j \ \forall j = 1, \ldots, i-1, i+1, \ldots, n \text{ e } x_i = e.$$

Da unicidade dada pela condição 1), concluímos que $z = e$, e isto termina a prova.

■

Proposição 1.7.2 *Sejam G um grupo e $G_1, G_2, \ldots, G_n$ subgrupos de G. Se G é o produto direto interno de $G_1, G_2, \ldots, G_n$, então G é isomorfo ao produto direto $G_1 \times G_2 \times \ldots \times G_n$.*

Demonstração

Considere $\varphi : G \to G_1 \times G_2 \times \ldots \times G_n$ a função definida da seguinte maneira: para um elemento $g \in G$, $\varphi(g) = (x_1, x_2, \ldots, x_n)$ onde $x_i \in G_i$, $i \in \{1, 2, \ldots, n\}$, são os únicos elementos tais que $g = x_1 x_2 \ldots x_n$. Esta função φ é claramente uma bijeção e provaremos agora que φ é um homomorfismo de grupos. Sejam $g = x_1 x_2 \ldots x_n$ e $g' = y_1 y_2 \ldots y_n$ dois elementos de G. Então

$$gg' = x_1 x_2 \ldots x_n y_1 y_2 \ldots y_n = x_1 y_1 x_2 y_2 \ldots x_n y_n$$

onde a última igualdade foi obtida por aplicações sucessivas da condição 2). Deste modo obtemos que $\varphi(gg') = (x_1 y_1, x_2 y_2, \ldots, x_n y_n) = \varphi(g)\varphi(g')$ e portanto que φ é um homomorfismo.

■

Proposição 1.7.3 *Se G é um grupo abeliano finito, então G é o produto direto interno de seus subgrupos de Sylow e portanto, G é isomorfo ao produto direto de seus subgrupos de Sylow.*

Demonstração

Escreva $|G| = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$, onde $p_1, p_2, \ldots, p_r$ são primos distintos. Naturalmente, G sendo abeliano, todos os subgrupos de G são normais em G. Conseqüentemente, pelo 2o. Teorema de Sylow, obtemos que, para cada p_i, existe um único p_i-subgrupo de Sylow de G, que denotamos por H_i, assim $|H_i| = p_i^{s_i}$. Queremos mostrar que $G = H_1 \odot H_2 \odot \cdots \odot H_r$. Mostraremos que as condições 3), 4) e 5) são satisfeitas. A condição 3) é satisfeita, pois G é abeliano. Agora, pela propriedade de produto de grupos, temos que $H_1 H_2$ é um subgrupo de G, pois $H_2 \triangleleft G$,

e $|H_1H_2| = |H_1| \cdot |H_2| = p_1^{s_1}p_2^{s_2}$, pois $H_1 \cap H_2 = \{e\}$. De fato, se $k \in H_1 \cap H_2$ então $O(x)$ divide $p_1^{s_1}$ e $p_2^{s_2}$, donde $O(k) = 1$. Novamente, $(H_1H_2)H_3$ é um subgrupo de G, pois $H_3 \lhd G$, e $|H_1H_2H_3| = |H_1H_2| \cdot |H_3| = p_1^{s_1}p_2^{s_2}p_3^{s_3}$, pois $(H_1H_2) \cap H_3 = \{e\}$; continuando desta maneira, obtemos que $H_1H_2 \ldots H_r$ é um subgrupo de G e que $|H_1H_2 \ldots H_r| = p_1^{s_1}p_2^{s_2} \ldots p_r^{s_r}$; logo $G = H_1H_2 \ldots H_r$ e portanto a condição 4) é satisfeita. Agora, para todo $i \in \{1, 2, \ldots, r\}$, temos $H_i \cap H_1 \ldots H_{i-1}H_{i+1} \ldots H_r = \{e\}$, pois $|H_i| = p_i^{s_i}$ e $|H_i \ldots H_{i-1}H_{i+1} \ldots H_r| = p_1^{s_1} \ldots p_{i-1}^{s_i-1}p_{i+1}^{s_i+1} \ldots p_r^{s_r}$ são números primos entre si, e então a condição 5) é satisfeita.

■

Capítulo 2

Os Grupos Abelianos Finitos

Neste capítulo usaremos a notação aditiva, pois todos os grupos que consideraremos serão abelianos. Nosso objetivo é classificar, a menos de isomorfismo, todos os grupos abelianos finitos. Faremos isso decompondo cada grupo abeliano finito como soma direta de p-subgrupos. Depois faremos a decomposição de cada p-grupo abeliano finito como soma direta de subgrupos cíclicos. Estas duas decomposições estabelecem o *Teorema Fundamental dos Grupos Abelianos Finitos*.

2.1 Decomposição em p-Grupos

Nesta seção mostraremos como decompor um grupo abeliano finito em p-subgrupos de G e mostraremos que, a menos de uma ordenação dos números primos, essa decomposição é única.

Seja G um grupo abeliano finito. Para cada número n, associamos o conjunto G_n formado pelos elementos de G cuja ordem é uma potência de n, isto é,

$$G_n = \{x \in G\,;\, O(x) = n^r, \text{ para algum } r \in \mathbb{N}\}$$

e trocando n por um número primo p, afirmamos que

$$G_p = \{x \in G\,;\, p^r \cdot x = 0, \text{ para algum } r \in \mathbb{N}\}$$

De fato, seja $x \in G_p$, então $O(x) = p^r$, para algum $r \in \mathbb{N}$, logo $p^r.x = 0$ e portanto x pertence ao conjunto $\{x \in G\,;\, p^r \cdot x = 0, \text{ para algum } r \in \mathbb{N}\}$. Por outro lado, seja x um elemento do conjunto $\{x \in G\,;\, p^r.x = 0, \text{ para algum } r \in \mathbb{N}\}$. Então existe $r \in \mathbb{N}$ tal que $p^r.x = 0$, ou seja, $O(x)$ divide p^r. Então $O(x)$ é potência de p, e termina assim a demontração da afirmação acima.

Em alguns casos, notadamente naqueles onde G denota um grupo com índice numérico ($\mathbb{Z}_n$, D_n, etc) é conveniente usar parênteses na notação acima. Assim escreveremos, quando for necessário, $G_p = (G)_p$.

Veremos agora que G_p é um p-subgrupo de G.

Proposição 2.1.1 *Se G é um grupo abeliano finito e p é um número primo então $G_p < G$ e $|G_p| = p^t$, para algum $t \in \mathbb{N}$.*

Demonstração

Desde que $O(0) = 1 = p^0$ segue que $0 \in G_p$. Dados $x, y \in G_p$ temos $O(x) = p^r$ e $O(y) = p^s$, com $r, s \in \mathbb{N}$. Tomando $u = r + s$, vem que, $p^u(x - y) = p^s(p^r x) - p^r(p^s y) = 0$. Logo G_p é um subgrupo de G. Suponhamos por absurdo que a ordem de G_p não seja potência de p. Então existe um primo q, $q \neq p$, tal que q divide a ordem de G_p. Pelo Teorema de Cauchy existe $x \in G_p$ com $O(x) = q$. Isso leva a contradição $q = p^r$ para algum $r \in \mathbb{N}$.

■

As hipóteses de G ser abeliano e p ser primo são essenciais para a proposição 2.1.1. De fato, para $D_3 = \{e, a, a^2, b, ab, a^2b\}$ temos $(D_3)_2 = \{e, b, ab, a^2b\}$, que não é grupo pois $b \cdot ab = a^2 \notin (D_3)_2$. E para $\mathbb{Z}_4$ temos $(\mathbb{Z}_4)_4 = \{\overline{0}, \overline{1}, \overline{3}\}$, que não é grupo pois $\overline{1} + \overline{1} = \overline{2} \notin (\mathbb{Z}_4)_4$.

Para facilitar a apresentação de exemplos, provaremos primeiro um lema tratando de propriedades dos p-subgrupos G_p.

Lema 2.1.1 *Sejam G um grupo abeliano finito e p, q números primos.*

a) $G_p \neq \{0\} \Leftrightarrow p \mid |G|$;

b) $p \neq q \Rightarrow G_p \cap G_q = \{0\}$;

c) $|G| = p^n$, $n \in \mathbb{N} \Rightarrow G_p = G$;

d) $G \simeq G' \Rightarrow G_p \simeq G'_p$;

e) $G = H \times K \Rightarrow G_p = H_p \times K_p$.

Demonstração

a) ($\Rightarrow$) Seja $x \in G_p$, $x \neq 0$. Então $O(x) = p^n$, $n \neq 0$. Sabemos que $|<x>| = O(x) = p^n$ e $|<x>| \mid |G|$. Como $n \neq 0$, vem que $p \mid |G|$.

($\Leftarrow$) Se $p \mid |G|$ então pelo Teorema de Cauchy, existe $x \in G$ tal que $O(x) = p$. Logo $0 \neq x \in G_p$ e portanto $G_p \neq \{0\}$.

b) Se $x \in G_p \cap G_q$ devemos ter $O(x) = p^n = q^m$ com $p \neq q$. A única solução possível é $n = m = 0$, isto é, $G_p \cap G_q = \{0\}$.

c) Para cada $x \in G$, o Teorema de Lagrange assegura que $|<x>| \mid |G|$. Mas $O(x) = |<x>|$ e $|G| = p^n$. Portanto $O(x)$ é potência de p, e conseqüentemente $G = G_p$.

d) Por hipótese, existe um isomorfismo $\varphi : G \longrightarrow G'$, do qual obtemos o isomorfismo $\varphi|_{G_p} : G_p \longrightarrow \varphi(G_p)$. Assim basta provar que $\varphi(G_p) = G'_p$. Se $y \in \varphi(G_p)$, então $y = \varphi(x)$, para algum $x \in G_p$. Desde que $O(y) = O(x)$ temos que $y \in G'_p$, isto é, $\varphi(G_p) \subseteq G'_p$. Por outro lado, se $y \in G'_p$ então $y \in G'$ e $O(y) = p^n$, para algum $n \in \mathbb{N}$. Assim existe $x \in G$ tal que $y = \varphi(x)$. Mas $O(x) = O(\varphi(x))$ e portanto $O(x) = p^n$, ou seja, $x \in G_p$. Portanto $y \in \varphi(G_p)$ provando que $G'_p \subseteq \varphi(G_p)$. Logo, $G'_p = \varphi(G_p)$ e portanto, $G_p \simeq G'_p$.

e) Seja $x = (u, v) \in G_p$, onde $u \in H$ e $v \in K$. Como $O(x) = p^n$, $n \in \mathbb{N}$, temos $(0,0) = p^n \cdot x = (p^n \cdot u, p^n \cdot v)$, implicando em $u \in H_p$ e $v \in K_p$. Logo $x \in H_p \times K_p$. Tomando agora $(u, v) \in H_p \times K_p$, existem $m, n \in \mathbb{N}$ tais que $p^n \cdot u = p^m \cdot v = 0$. Segue que $p^{n+m}(u, v) = (p^m(p^n u), p^n(p^m v)) = (0, 0)$, isto é, $(u, v) \in G_p$.

■

Corolário 2.1.1 *Seja G um grupo abeliano finito. Se $G \simeq H_1 \times H_2 \times \ldots \times H_n$ então $G_p \simeq (H_1)_p \times (H_2)_p \times \ldots \times (H_n)_p$, para cada número primo p.*

Demonstração

Aplicando o item (d) do Lema 2.1.1 em $G \simeq H_1 \times H_2 \times \ldots \times H_n$, vem que $G_p \simeq (H_1 \times H_2 \times \ldots \times H_n)_p$. Sucessivas aplicações do item (e) do Lema 2.1.1 provam que $(H_1 \times H_2 \times \ldots \times H_n)_p = (H_1)_p \times (H_2)_p \times \ldots \times (H_n)_p$.

■

Exemplo 2.1.1 Se p é um número primo e $n \in \mathbb{N}$ então $(\mathbb{Z}_{p^n})_p = \mathbb{Z}_{p^n}$ *(lema 2.1.1 (c)).*

Exemplo 2.1.2 $(\mathbb{Z}_{p^n})_q = \{\overline{0}\}$ para todo número primo $q \neq p$. *(lema 2.1.1 (a)).*

Exemplo 2.1.3 Calculando a ordem de cada elemento de $\mathbb{Z}_6$ concluimos que $(\mathbb{Z}_6)_2 = \{\overline{0}, \overline{3}\} \simeq \mathbb{Z}_2$ e $(\mathbb{Z}_6)_3 = \{\overline{0}, \overline{2}, \overline{4}\} \simeq \mathbb{Z}_3$. Por outro lado, sabemos que $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$ e aplicando o Corolário 2.1.1 temos $(\mathbb{Z}_6)_2 \simeq (\mathbb{Z}_2)_2 \times (\mathbb{Z}_3)_2 = \mathbb{Z}_2 \times \{\overline{\overline{0}}\} \simeq$ $\simeq \mathbb{Z}_2$ e $(\mathbb{Z}_6)_3 \simeq (\mathbb{Z}_2)_3 \times (\mathbb{Z}_3)_3 = \{\overline{0}\} \times \mathbb{Z}_3 \simeq \mathbb{Z}_3$.

Note ainda que

$$\mathbb{Z}_6 = (\mathbb{Z}_6)_2 \oplus (\mathbb{Z}_6)_3.$$

Exemplo 2.1.4 $(\mathbb{Z}_9)_3 = \mathbb{Z}_9$ e $(\mathbb{Z}_3 \times \mathbb{Z}_3)_3 = \mathbb{Z}_3 \times \mathbb{Z}_3$ *(lema 2.1.1 (c) e (e)).*

Desde que $(\mathbb{Z}_9)_3$ e $(\mathbb{Z}_3 \times \mathbb{Z}_3)_3$ não são isomorfos, pois $\mathbb{Z}_3 \times \mathbb{Z}_3$ não tem elemento de ordem 9, concluímos do exemplo 2.1.4 que o p-subgrupo G_p não depende apenas da ordem do grupo G, mas sim da ordem dos elementos de G.

Vejamos mais um exemplo:

Exemplo 2.1.5 Sejam $G = \mathbb{Z}_{12}$ e $G' = \mathbb{Z}_2 \times \mathbb{Z}_6$. Através do cálculo da ordem dos elementos de G e G' obtemos

$$G_2 = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \simeq \mathbb{Z}_4 \text{ e } G_3 = \{\overline{0}, \overline{4}, \overline{8}\} \simeq \mathbb{Z}_3$$

$$G'_2 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{3}), (\overline{1}, \overline{0}), (\overline{1}, \overline{3})\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ e } G'_3 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{2}), (\overline{0}, \overline{4})\} \simeq \mathbb{Z}_3.$$

Utilizando o Lema 2.1.1 e seu Corolário obtemos

$$G_2 = (\mathbb{Z}_{12})_2 \simeq (\mathbb{Z}_4 \times \mathbb{Z}_3)_2 = (\mathbb{Z}_4)_2 \times (\mathbb{Z}_3)_2 = \mathbb{Z}_4 \times \{\overline{0}\} \simeq \mathbb{Z}_4$$

$$G_3 = (\mathbb{Z}_{12})_3 \simeq (\mathbb{Z}_4 \times \mathbb{Z}_3)_3 = (\mathbb{Z}_4)_3 \times (\mathbb{Z}_3)_3 = \{\overline{0}\} \times \mathbb{Z}_3 \simeq \mathbb{Z}_3$$

$$G'_2 = (\mathbb{Z}_2 \times \mathbb{Z}_6)_2 = (\mathbb{Z}_2)_2 \times (\mathbb{Z}_6)_2 \simeq (\mathbb{Z}_2)_2 \times (\mathbb{Z}_2)_2 \times (\mathbb{Z}_3)_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \{\overline{0}\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$G'_3 = (\mathbb{Z}_2 \times \mathbb{Z}_6)_3 = (\mathbb{Z}_2)_3 \times (\mathbb{Z}_6)_3 \simeq (\mathbb{Z}_2)_3 \times (\mathbb{Z}_2)_3 \times (\mathbb{Z}_3)_3 = \{\overline{0}\} \times \{\overline{0}\} \times \mathbb{Z}_3 \simeq \mathbb{Z}_3$$

Novamente observamos que apesar de $|G| = |G'|$ temos G_2 não é isomorfo a G'_2, e também

$$G = G_2 \oplus G_3$$

$$G' = G'_2 \oplus G'_3$$

Nosso objetivo agora será mostrar que a segunda parte da observação acima é um resultado geral, ou seja, todo grupo abeliano finito G é soma direta dos seus

p-subgrupos G_p.

Já vimos no lema 2.1.1 que se p não divide $|G|$ então $G_p = \{0\}$. Assim nosso interesse é estudar G_p, para p divisor de $|G|$.

Seja $n = |G|$. Pelo Teorema Fundamental da Aritmética podemos escrever

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$$

onde $\{p_1, p_2, \ldots, p_s\}$ é o conjunto de primos distintos que dividem n e $e_i \in \mathbb{N}$ para $i \in \{1, 2, \ldots, s\}$.

Da decomposição $|G| = n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$ segue, para $i \in \{1, 2, \ldots, s\}$, que G não possui elemento de ordem p_i^{α} com $\alpha > e_i$. De fato, se existisse um elemento $x \in G$ com $O(x) = |< x >| = p_i^{\alpha}$, $\alpha > e_i$, teríamos pelo Teorema de Lagrange que $p_i^{\alpha} \mid n$, implicando em $p_i | p_j$ para algum $j \neq i$, $j \in \{1, 2, \ldots, s\}$, que é impossível. Isso mostra que

$$G_{p_i} \subseteq \{x \in G;\ p_i^{e_i} \cdot x = 0\}$$

e como a inclusão inversa é evidente, concluímos que

$$G_{p_i} = \{x \in G;\ p_i^{e_i} \cdot x = 0\},\ \text{para cada } i \in \{1, 2, \ldots, s\}$$

Provaremos agora o principal teorema desta seção, conhecido como *Teorema da Decomposição Primária*. Este nome deve-se ao fato de que, para cada primo p que divide a ordem de G, o p-subgrupo G_p é chamado de *Componente p-Primário de G*.

Teorema 2.1.1 *(Teorema da Decomposição Primária) Seja G um grupo abeliano de ordem $n = p_1^{e_1} \cdot p_2^{e_2} \ldots \cdot p_s^{e_s}$, onde $p_1, p_2, \ldots, p_s$ são primos distintos e $e_i \in \mathbb{N}$ para $i \in \{1, 2, \ldots, s\}$. Então*

$$G = G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{p_s}.$$

Demonstração

É claro que $G_{p_1} + G_{p_2} + \ldots + G_{p_s} \subseteq G$. Para verificar a outra inclusão iniciamos escrevendo $n_i = \frac{n}{p_i^{e_i}}$. Afirmamos que $\text{mdc}\,(n_1, n_2, \ldots, n_s) = 1$. De fato, se não fosse assim existiria um número primo q tal que $q \mid n_i$, $\forall i \in \{1, 2, \ldots, s\}$. Mas $n_1 = p_2^{e_2} \cdot \ldots \cdot p_t^{e_t}$ e $q \mid n_1$ implica em $q = p_j$, para algum $j \in \{2, \ldots, s\}$. Da mesma forma, $n_j = p_1^{e_1} \cdot \ldots \cdot p_{j-1}^{e_{j-1}} \cdot p_{j+1}^{e_{j+1}} \cdot \ldots \cdot p_s^{e_s}$ e $q \mid n_j$ implica em $q = p_k$ com

$k \neq j$ e $k \in \{1, 2, \ldots, s\}$. Isso leva à contradição $p_j = q = p_k$, $k \neq j$. Logo $\text{mdc}\,(n_1, n_2, \ldots, n_s) = 1$ e pela Identidade de Bezout,

$$1 = h_1 n_1 + h_2 n_2 + \ldots + h_s n_s\,,\ h_i \in \mathbb{Z}.$$

Dado $x \in G$ temos $x = h_1 n_1 x + h_2 n_2 x + \ldots + h_s n_s x$. Mas

$$p_i^{e_i}(h_i n_i x) = h_i(p_i^{e_i} n_i)x = h_i(nx) = h_i \cdot 0 = 0$$

isto é, $h_i n_i x \in G_{p_i}$. Portanto $x \in G_{p_1} + G_{p_2} + \ldots + G_{p_s}$ e concluímos que $G = G_{p_1} + {+}G_{p_2} + \ldots + G_{p_s}$. Para ver que a soma é direta, tomamos $x \in G_{p_i} \cap (G_{p_1} + {+}G_{p_2} + \ldots + G_{p_{i-1}} + G_{p_{i+1}} + \ldots + G_{p_s})$. Segue que $p_i^{e_i}.x = 0$ e $x = y_1 + y_2 + {+}\ldots + y_{i-1} + y_{i+1} + \ldots + y_s$ com $y_j \in G_{p_j}$. Note que $p_j^{e_j} \mid n_i$, para $j \neq i$. Como $p_j^{e_j}.y_j = 0$, temos que $n_i.y_j = 0$, e portanto temos a igualdade $n_i \cdot x = n_i y_1 + n_i y_2 + \ldots + n_i y_{i-1} + n_i y_{i+1} + \ldots + n_i y_s = 0$. Agora temos $p_i^{e_i}.x = 0 = n_i.x$, assim $O(x) \mid p_i^{e_i}$ e $O(x) \mid n_i$, mas pela escolha de n_i temos $\text{mdc}\,(n_i, p_i^{e_i}) = 1$. Logo $O(x) = 1$, isto é, $x = 0$ e portanto $G = G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{p_s}$.

■

Já sabemos, pela Proposição 2.1.1, que $|G_p|$ é uma potência de p. Agora, podemos ser mais precisos.

Corolário 2.1.2 *Seja G um grupo abeliano de ordem $n = p_1^{e_1}.p_2^{e_2}.\ \ldots\ .p_s^{e_s}$ onde $p_1, p_2, \ldots, p_s$ são primos distintos e $e_i \in \mathbb{N}$ para $i \in \{1, 2, \ldots, s\}$. Então $|G_{p_i}| = p_i^{e_i}$.*

Demonstração

Pelo Teorema acima sabemos que $G = G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{p_s}$. Pela Proposição 1.7.1 sabemos que $G_{p_1} \oplus G_{p_2} \ldots \oplus G_{p_s} \simeq G_{p_1} \times G_{p_2} \times \ldots \times G_{p_s}$. Além disso, vimos na Proposição 2.1.1 que $|G_{p_i}| = p_i^{t_i}$. Assim $p_1^{e_1}.p_2^{e_2}.\ \ldots\ .p_s^{e_s} = n = |G| = |G_{p_1} \times G_{p_2} \times \ldots \times G_{p_s}| = |G_{p_1}|.|G_{p_2}|.\ \ldots\ .|G_{p_s}| = p_1^{t_1}.p_2^{t_2}.\ \ldots\ .p_s^{t_s}$. Pela unicidade da decomposição obtida do Teorema Fundamental da Álgebra, concluímos que $e_i = t_i$, $i \in \{1, 2, \ldots, s\}$. Logo $|G_{p_i}| = p_i^{e_i}$.

■

Podemos ilustrar o resultado do Corolário anterior, retomando os exemplos.

No exemplo 2.1.1, tínhamos $G = \mathbb{Z}_{p^n}$ e $G_p = \mathbb{Z}_{p^n}$. Como $|G| = p^n$, pelo Corolário 2.1.2 deveríamos ter $|G_p| = p^n$.

No exemplo 2.1.4, tínhamos $G = \mathbb{Z}_9$ e $G_3 = \mathbb{Z}_9$. Como $|G| = 9 = 3^2$, pelo Corolário 2.1.2 deveríamos ter $|G_3| = 9$.

No exemplo 2.1.5, tínhamos $G = \mathbb{Z}_{12}$, $G_2 \simeq \mathbb{Z}_4$ e $G_3 \simeq \mathbb{Z}_3$. Como $|G| = 12 = 2^2 \cdot 3$, pelo Corolário 2.1.2 deveríamos ter $|G_2| = 4$ e $|G_3| = 3$.

O próximo Teorema é um importante complemento para o Teorema 2.1.1. Ele garante que qualquer outra decomposição de um grupo abeliano finito em soma direta de subgrupos de ordem potência de número primo coincide com a decomposição primária.

Teorema 2.1.2 *(Unicidade da Decomposição Primária) Seja G um grupo abeliano de ordem $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s}$, onde $p_1, p_2, \ldots, p_s$ são primos distintos e $e_i \in \mathbb{N}$ para $i \in \{1, 2, \ldots, s\}$. Se $\{q_j\}_{j=1}^t$ é uma família de números primos distintos e H_j é um q_j-subgrupo de G, para cada $j \in \{1, 2, \ldots, t\}$, satisfazendo $G = H_1 \oplus H_2 \oplus \ldots \oplus H_t$, então $s = t$ e $G_{p_i} = H_i$, para $i \in \{1, 2, \ldots, s\}$, a menos de uma possível reordenação dos primos $\{q_j\}_{j=1}^t$.*

Demonstração

Fixemos a ordem de H_j escrevendo $|H_j| = q_j^{a_j}$ para $j \in \{1, 2, \ldots, t\}$. Por hipótese, $G = H_1 \oplus H_2 \oplus \ldots \oplus H_t$ e procedendo como na demonstração do Corolário 2.1.2 temos

$$p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_s^{e_s} = n = q_1^{a_1} \cdot q_2^{a_2} \cdot \ldots \cdot q_t^{a_t}.$$

A unicidade da decomposição obtida do Teorema Fundamental da Álgebra assegura que $s = t$, e que a menos de reordenação do conjunto de primos $\{q_1, q_2 \ldots, q_s\}$ vale $p_i^{e_i} = q_i^{a_i}$. Assim, se $x \in H_i$ então $p_i^{e_i} \cdot x = q_i^{a_i} \cdot x = 0$, mostrando que $H_i \subseteq G_{p_i}$. Mas além disso, $|H_i| = |G_{p_i}|$. Portanto $H_i = G_{p_i}$.

■

2.2 Decomposição dos p-Grupos

Os Teoremas 2.1.1 e 2.1.2 mostram que todo grupo abeliano finito e não nulo G pode ser representado de modo único, a menos da ordem das parcelas, como soma direta da família finita de p-subgrupos não nulos G_p. Para completar este resultado faremos a decomposição dos p-subgrupos G_p em soma direta finita de grupos cíclicos.

A decomposição em soma direta finita de grupos cíclicos é possível para todo p-grupo abeliano finito não nulo. Provaremos este resultado geral e então o

utilizaremos para os p-subgrupos G_p.

Iniciamos com o seguinte Lema.

Lema 2.2.1 *Se $G \neq \{0\}$ é um p-grupo abeliano finito e se d é um elemento de G de ordem máxima p^k, então G é a soma direta do subgrupo cíclico $< d >$ e de um subgrupo N de G.*

Demonstração

Consideremos o conjunto Γ de todos os subgrupos H de G tais que $H \cap < d >= \{0\}$ e ordenemos Γ por inclusão. É imediato que $\Gamma \neq \emptyset$, pois $\{0\} \cap < d >= \{0\}$. Como G é finito segue que Γ também é finito, logo, existe em Γ um elemento maximal N. Note que se N' é um subgrupo qualquer de G e se $N \subsetneqq N'$ então $N' \cap < d > \neq \{0\}$, pois N é elemento maximal de Γ. Tomando $G' = N + < d >$ e usando o fato de $N \cap < d >= \{0\}$ temos que $G' = N \oplus < d >$. Se mostrarmos que $G' = G$ obteremos a tese do Lema. Suponhamos, por absurdo, que $G' \neq G$. Afirmamos, nesse caso, que existe um $x \in G$ tal que $x \notin G'$ e $p.x \in G'$. De fato, existe, por hipotese, um elemento x' em G que não pertence a G'. Como $x' \in G$ e G é um p-grupo finito temos $O(x') = p^i$, com $i \geq 1$, logo existe um menor número natural não nulo j tal que $p^j x' \in G'$. Se $j = 1$ basta escolher $x = x'$ e se $j > 1$ escolheremos $x = p^{j-1} \cdot x'$. Assim $x \in G$, $p.x = p^j x' \in G'$ e $x \notin G'$ pela minimalidade de j.

De $p.x \in G' = < d > \oplus N$ resulta que $px = md + h$, com m inteiro e $h \in N$. Desde que p^k é a maior ordem dos elementos de G,

$$0 = p^k.x = p^{k-1}(px) = p^{k-1}md + p^{k-1}h,$$

de onde vem $p^{k-1}md = -p^{k-1}h \in < d > \cap N = 0$. Logo $p^{k-1}md = 0$ e daqui concluímos que $p^k | (p^{k-1}m)$, logo $m = pm'$. Por outro lado, temos

$$h = px - md = p(x - m'd).$$

Como $m'd \in < d >$, se admitirmos que $x - m'd \in N$ teremos $x = x - m'd + m'd \in N + < d > = G'$. Mas $x \notin G'$ e portanto $x - m'd \notin N$. Logo

$$N' = N + < x - m'd > \supset N \text{ e } N' \neq N$$

e daqui resulta que $N' \cap < d > \neq \{0\}$, ou seja, existe $rd \in N'$, com $r \in \mathbb{Z}$ e $rd \neq 0$.

Para este elemento rd temos $rd = h_0 + s(x - m'd)$, com $h_0 \in N$ e $s \in \mathbb{Z}$, logo, $sx = rd - sm'd - h_0 \in N + < d >= G'$. Admitindo que $p|s$, escrevemos $p\alpha = s$ e de $rd = h_0 + s(x - m'd)$ vem que $rd = h_0 + \alpha p(x - m'd)$. Sabemos que $p(x - m'd) = h \in N$, logo $\alpha p(x - m'd) \in N$. Também $h_0 \in N$ e então $rd = h_0 + \alpha p(x - m'd) \in N$. Mas isso não é possível pois $rd \in < d >$, $rd \neq 0$ e $< d > \cap N = \{0\}$. Portanto $p \nmid s$. Fica assim provado que $sx \in G'$ e $px \in G'$ com s e p primos entre si. Pela Identidade de Bezout existem números inteiros u e v tais que $us + vp = 1$. Concluímos que $x = u(sx) + v(px)$ e então $x \in G'$ pois $sx, px \in G'$, contradizendo a escolha do elemento $x \notin G'$.

■

Com o auxílio deste Lema podemos ser mais precisos na decomposição de um p-grupo $G \neq \{0\}$ demonstrando o Teorema seguinte.

Teorema 2.2.1 *(Teorema da Decomposição dos p-Grupos Finitos) Todo p-grupo abeliano finito $G \neq \{0\}$ é a soma direta de uma família finita de subgrupos cíclicos.*

Demonstração

Seja p^s a ordem de G e façamos a demonstração usando o segundo princípio de indução finita sobre $s \geq 1$.

Se $s = 1$ então G é cíclico e não há nada a demonstrar. Suponhamos então que $s > 1$ e que o Teorema seja verdadeiro para todo p-grupo abeliano finito de ordem p^t, com $1 \leq t < s$. Seja d um elemento de G de ordem máxima p^k. Se $k = s$ então G é cíclico e, neste caso, nada há para demonstrar. Se $k < s$, então o Lema 2.2.1 nos garante que G é a soma direta de $N_1 =< d >$ com um subgrupo N de G. Se $N = \{0\}$ então $< d >= N_1 = G$ e $O(d) = p^k = p^s$ implicando em $k = s$. Absurdo pois $k < s$. Se $N = G$ então $N_1 =< d >= \{0\}$. Absurdo pois d é elemento de ordem máxima de $G \neq \{0\}$. Logo $N \neq \{0\}$, $N \neq G$ e $|N| = p^t$ com $1 \leq t < s$, de onde vem, conforme a hipótese de indução, que N é a soma direta da família $\{N_i\}_{2 \leq i \leq m}$ de subgrupos cíclicos e é imediato que G é a soma direta da família $\{N_i\}_{1 \leq i \leq m}$, onde cada N_i é um grupo cíclico.

■

Na seção anterior provamos o Teorema 2.1.1 que garante que todo grupo finito tem uma decomposição primária, e em seguida provamos o Teorema 2.1.2 que dá a unicidade desta decomposição. Agora, no Teorema 2.2.1, verificamos que todo p-grupo abeliano finito tem uma decomposição em soma direta de subgrupos cíclicos.

No entanto a decomposição obtida no Teorema 2.2.1 não é única em geral. Vejamos alguns exemplos.

Exemplo 2.2.1 Seja $G = \mathbb{Z}_3 \times \mathbb{Z}_3$. Tomando

$$H_1 = < (\overline{1}, \overline{0}) >= \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0}), (\overline{2}, \overline{0})\} \ < \ G$$

$$H_2 = < (\overline{0}, \overline{1}) >= \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2})\} \ < \ G$$

é fácil ver que $G = H_1 \oplus H_2$, com H_1 e H_2 cíclicos.

Também podemos escolher

$$H_1' = < (\overline{1}, \overline{2}) >= \{(\overline{0}, \overline{0}), (\overline{1}, \overline{2}), (\overline{2}, \overline{1})\} \ < \ G$$

$$H_2' = < (\overline{1}, \overline{1}) >= \{(\overline{0}, \overline{0}), (\overline{1}, \overline{1}), (\overline{2}, \overline{2})\} \ < \ G$$

e novamente temos $G = H_1' \oplus H_2'$, com H_1' e H_2' cíclicos.

Como H_1, H_2, H_1' e H_2' são dois a dois distintos, obtivemos a decomposição de G como soma direta de subgrupos cíclicos de duas formas diferentes.

Observemos no exemplo acima que apesar de não termos a unicidade da decomposição, o número de somandos diretos bem como suas ordens , coincidem nas duas decomposições. Vejamos mais um exemplo.

Exemplo 2.2.2 Seja $G = \mathbb{Z}_8 \times \mathbb{Z}_4$. Tomando

$$H_1 = < (\overline{1}, \overline{\overline{0}}) >= \{(\overline{0}, \overline{\overline{0}}), (\overline{1}, \overline{\overline{0}}), (\overline{2}, \overline{\overline{0}}), (\overline{3}, \overline{\overline{0}}), (\overline{4}, \overline{\overline{0}}), (\overline{5}, \overline{\overline{0}}), (\overline{6}, \overline{\overline{0}}), (\overline{7}, \overline{\overline{0}})\} \ < \ G$$

$$H_2 = < (\overline{0}, \overline{\overline{1}}) >= \{(\overline{0}, \overline{\overline{0}}), (\overline{0}, \overline{\overline{1}}), (\overline{0}, \overline{\overline{2}}), (\overline{0}, \overline{\overline{3}})\} \ < \ G$$

é claro que $G = H_1 \oplus H_2$, com H_1 e H_2 cíclicos.

Escolhendo agora

$$H_1' = < (\overline{1}, \overline{\overline{1}}) >= \{(\overline{0}, \overline{\overline{0}}), (\overline{1}, \overline{\overline{1}}), (\overline{2}, \overline{\overline{2}}), (\overline{3}, \overline{\overline{3}}), (\overline{4}, \overline{\overline{0}}), (\overline{5}, \overline{\overline{1}}), (\overline{6}, \overline{\overline{2}}), (\overline{7}, \overline{\overline{3}})\} \ < \ G$$

$$H_2' = < (\overline{4}, \overline{\overline{1}}) >= \{(\overline{0}, \overline{\overline{0}}), (\overline{4}, \overline{\overline{1}}), (\overline{0}, \overline{\overline{2}}), (\overline{4}, \overline{\overline{3}})\} \ < \ G$$

temos $G = H_1' \oplus H_2'$, com H_1' e H_2' subgrupos cíclicos.

O próximo Teorema mostra que o ocorrido nos exemplos acima é um caso geral, isto é, todas as decomposições de um p-grupo abeliano finito em soma direta de subgrupos cíclicos têm o mesmo número de subgrupos, e a menos de uma reordenação, os subgrupos cíclicos correspondentes em cada decomposição têm a mesma ordem. Logo são isomorfos.

Precisamos do seguinte Lema.

Lema 2.2.2 *Se $H = < a > \neq \{0\}$ é um p-grupo cíclico de ordem p^s então o conjunto*

$$H_1 = \{x \in H \ ; \ px = 0\}$$

é um subgrupo de ordem p.

Demonstração

É claro que H_1 é subgrupo de H. Os elementos $i.p^{s-1}a$ com $i = 1, 2, \ldots, p$ pertencem a H_1, pois $p.i.p^{s-1}a = i.p^s a = i.0 = 0$, e os elementos $i.p^{s-1}a$, com $i = 1, 2, \ldots, p$ são todos distintos. Por outro lado, seja $x = ja$, com $1 \leq j \leq p^s - 1$, um elemento qualquer de H e suponhamos que $x \in H_1$. Então $pja = 0$, de onde vem que $p^s|(pj)$ ou $p^{s-1}|j$ e então $j = ip^{s-1}$, onde $1 \leq i \leq p - 1$.

■

Teorema 2.2.2 *(Unicidade da Decomposição dos p-Grupos) Se um p-grupo abeliano finito $G \neq \{0\}$ é a soma direta de duas famílias $\{H_i\}_{1 \leq i \leq r}$ e $\{H'_j\}_{1 \leq j \leq s}$ de subgrupos cíclicos de G e se $H_i \neq \{0\}$, $i = 1, 2, \ldots, r$ e $H_j \neq \{0\}$, $j = 1, 2, \ldots, s$ então $r = s$ e, usando-se uma notação conveniente, temos $|H_i| = |H'i|$ para $i = 1, 2, \ldots, r$.*

Demonstração

Seja p^d a ordem de G. Vamos fazer a demonstração usando o segundo princípio de indução finita sobre d. Se $d = 1$ então G é cíclico e neste caso temos $r = s = 1$ e $H_1 = H'_1 = G$. Suponhamos agora, como hipótese de indução, que o teorema seja válido para todo p-grupo de ordem, $p^{d'}$, com $1 \leq d' \leq d$. Fixemos as notações seguintes:

$$H_i = < a_i > \ , \ |H_i| = p^{e_i} \ , e_1 \geq e_2 \geq \ldots \geq e_r \geq 1$$

$$H'_j = < b_j > \ , \ |H'_j| = p^{f_j} \ , f_1 \geq f_2 \geq \ldots \geq f_r \geq 1$$

Note que as relações de ordem entre os expoentes e_i e f_j são possíveis pois podemos reordenar, caso seja necessário, os conjuntos $\{H_i\}_{1\leq i\leq r}$ e $\{H'_j\}_{1\leq j\leq s}$.

É fácil ver que

$$G_{(p)} = \{x \in G \mid px = 0\} \quad e$$

$$G^{(p)} = \{py \mid y \in G\}.$$

são subgrupos de G. Afirmamos que $|G_{(p)}| = p^r$. De fato, dado $x \in G$, podemos escrevê-lo como $x = x_1 + x_2 + \ldots + x_r$, com $x_i \in H_i$ para $i \in \{1, 2, \ldots, r\}$. Assim $x \in G_{(p)}$ se, e somente se, $px = 0$, que equivale a $px_1 + px_2 + \ldots + px_r = 0$. Desde que $px_i \in H_i$ e $G = H_1 \oplus H_2 \oplus \ldots \oplus H_r$, temos que $px_1 + px_2 + \ldots + px_r = 0$ se, e somente se, $px_i = 0\ \forall i \in \{1, 2, \ldots, r\}$. Assim $x \in G_{(p)}$ se, e somente se, $x_i \in \{x \in H_i;\ px = 0\}$ que é um grupo de ordem p, pelo Lema anterior. Logo $|G_{(p)}| = p^r$.

De maneira análoga, trocando a família $\{H_i\}_{1\leq i\leq r}$ pela família $\{H'_j\}_{1\leq j\leq s}$, chegamos a conclusão que $|G_{(p)}| = p^s$. Portanto $r = s$. Olhemos agora para os expoentes $e_1, e_2, \ldots, e_r$ e separemos a demonstração em dois casos.

1º Caso

$\forall i \in \{1, 2, \ldots, r\}$ temos $e_i = 1$. Nesta situação temos $|H_i| = p$, $\forall i \in \{1, 2, \ldots, r\}$. Como $G = H_1 \oplus H_2 \oplus \ldots \oplus H_r$, vem que todo elemento de G tem ordem p, isto é, $G = G_{(p)}$. Por outro lado, $|H'_j| = p^{f_j}$, $\forall j \in \{1, 2, \ldots, s\}$ e então, supondo que exista um $f_j > 1$ teremos, pelo Teorema de Cauchy, um elemento neste $H'_j \subseteq G$ de ordem superior a p. Contradição. Logo devemos ter $f_j = 1, \forall j \in \{1, 2, \ldots, s\}$ e portanto $e_i = f_i$, $\forall i \in \{1, 2, \ldots, r\}$.

2º Caso

Existe um $i \in \{1, 2, \ldots, r\}$ tal que $e_i > 1$. Seja m o maior índice de e tal que $e_m > 1$. Temos $1 \leq m \leq r$, $e_m > 1$ e $e_\alpha = 1$ para $m < \alpha \leq r$.

Se $f_1 = 1$ então $f_j = 1$, $\forall j \in \{1, 2, \ldots, s\}$ e usando o primeiro caso com f_j no lugar de e_i, vem que $e_i = 1$, $\forall i \in \{1, 2, \ldots, r\}$. Contradição. Logo $f_1 > 1$ e então existe um maior índice n para f tal que $f_n > 1$. Temos $1 \leq n \leq s = r$, $f_n > 1$ e $f_\beta = 1$ para $n < \beta \leq s = r$.

Afirmação 1

pH_i e pH'_j são subgrupos cíclicos de $G^{(p)}$, para todo $i, j \in \{1, 2, \ldots, r\}$.

Basta provar para pH_i com um i fixado. Como $H_i < G$ temos $pH_i = \{px;\ x \in H_i\} \subseteq \{py;\ y \in G\} = G^{(p)}$. Além disso, é imediato que pH_i é fechado por diferenças. Logo $pH_i < G^{(p)}$.

Para ver que pH_i é cíclico, provemos que $pH_i = < pa_i >$ já que $H_i = < a_i >$. Para a primeira inclusão, tomamos $pu \in pH_i$, $u = \lambda a_i$ e então $pu = p(\lambda a_i) = \lambda(pa_i) \in < pa_i >$. Para a outra inclusão, tomamos $\lambda pa_i \in < pa_i >$ e escrevemos $\lambda pa_i = p(\lambda a_i) \in pH_i$, pois $\lambda a_i \in H_i$.

Afirmação 2:

$$G^{(p)} = pH_1 \oplus pH_2 \oplus \ldots \oplus pH_m \text{ e } G^{(p)} = pH'_1 \oplus pH'_2 \oplus \ldots \oplus pH'_n.$$

Basta provar que $G^{(p)} = pH_1 \oplus pH_2 \oplus \ldots \oplus pH_m$, pois a outra parte da afirmação é demonstrada de forma análoga a esta. Pela Afirmação 1, para cada $i \in \{1, 2, \ldots m\}$ temos que $pH_i < G^{(p)}$. Logo $pH_1 + pH_2 + \ldots + pH_m \subseteq G^{(p)}$. Seja agora $x \in G^{(p)}$. Então $x = py$ para algum $y \in G$. Escrevemos $y = y_1 + y_2 + \ldots + y_r$, com $y_i \in H_i$. Lembre que $|H_i| = p^{e_i}$, $|H_m| = p^{e_m} > p$, pois $e_m > 1$ e $|H_\alpha| = p^{e_\alpha} = p$, pois $e_\alpha = 1$ para $m < \alpha \leq r$. Segue que $x = py = py_1 + py_2 + \ldots + py_r$ com $py_\alpha = 0$ para $m < \alpha \leq r$. Assim $x = py_1 + py_2 + \ldots + py_m \in pH_1 + pH_2 + \ldots + pH_m$ provando que $G^{(p)} = pH_1 + pH_2 + \ldots + pH_m$. Além disso, como $pH_i \subseteq H_i$ e a soma da família $\{H_i\}_{1 \leq i \leq r}$ é direta, temos que

$$G^{(p)} = pH_1 \oplus pH_2 \oplus \ldots \oplus pH_m.$$

Da afirmação 2 concluímos que

$$|G^{(p)}| = |pH_1|.|pH_2|. \ldots .|pH_m| = |pH'_1|.|pH'_2|. \ldots .|pH'_n|.$$

Sabemos que H_i é um grupo cíclico de ordem p^{e_i}, e então $H_i \simeq \mathbb{Z}_{p^{e_i}}$. A restrição deste isomorfismo ao subgrupo cíclico pH_i de H_i possibilita provar que $pH_i \simeq p\mathbb{Z}_{p^{e_i}} = p(\frac{\mathbb{Z}}{p^{e_i}.\mathbb{Z}}) \simeq \frac{p\mathbb{Z}}{p^{e_i}.\mathbb{Z}} \simeq \frac{\mathbb{Z}}{p^{e_i-1}.\mathbb{Z}}$. Assim, $|pH_i| = p^{e_i-1}, \forall i \in \{1, 2, \ldots, r\}$. Analogamente $|pH'_j| = p^{e_j-1}$, $\forall j \in \{1, 2, \ldots, r\}$. Donde concluímos que se $p^{d'} = |G^{(p)}|$

então

$$d' = (e_1 - 1) + (e_2 - 1) + \ldots + (e_m - 1) = (f_1 - 1) + (f_2 - 1) + \ldots + (f_n - 1) < d.$$

Aplicando a hipótese de indução ao grupo $G^{(p)} = H_1 \oplus H_2 \oplus \ldots \oplus H_m = H'_1 \oplus H'_2 \oplus \ldots \oplus H'_n$ temos que $m = n$ e $|H_i| = |H'_i|$ para $i = 1, 2, \ldots, m$. Mas já vimos que para $m < \alpha \leq r$ temos $e_\alpha = 1$ e para $m = n < \beta \leq s = r$ temos $f_\beta = 1$. Logo $|H_\alpha| = p^{e_\alpha} = 1 = p^{f_\beta} = |H'_\beta|$, provando que $|H_i| = |H'_i|$ para i=1,2,...,r. ■

Temos provado que todo p-grupo abeliano finito não nulo pode ser decomposto em soma direta de subgrupos cíclicos. Além disso, o comprimento de quaisquer duas destas decomposições é o mesmo e os fatores cíclicos correspondentes têm a mesma ordem.

2.3 Teorema Fundamental dos Grupos Abelianos Finitos

Nesta seção apresentaremos o *Teorema Fundamental dos Grupos Abelianos Finitos* , que decompõe todo grupo abeliano finito não nulo G em soma direta de uma família de p-subgrupos cíclicos não nulos. A unicidade desta decomposição é obtida a menos de isomorfismo. Além disso, provaremos um Teorema que dá exatamente o número de grupos abelianos, dois a dois não isomorfos, de cada ordem fixada.

Teorema 2.3.1 *(Teorema Fundamental dos Grupos Abelianos Finitos) Todo grupo abeliano finito $G \neq \{0\}$ é a soma direta de uma família $\{G_i\}_{1 \leq i \leq r}$ de p-subgrupos cíclicos não nulos. Além disso, o número destes grupos cíclicos e suas ordens são determinados de modo único pelo grupo G.*

O Teorema 2.1.1 mostra que G é soma direta de p-subgrupos abelianos G_p. Mas G_p é um p-grupo, e então pelo Teorema 2.2.1 temos que cada grupo G_p é soma direta de subgrupos cíclicos. Segue então que G é soma direta de uma família $\{G_i\}_{1 \leq i \leq r}$ de p-subgrupos cíclicos não nulos. Além disso, o Teorema 2.1.2 assegura que a primeira decomposição é feita de modo único. Também o Teorema 2.2.2 assegura que a segunda decomposição sempre tem o mesmo número de parcelas, e as ordens destas parcelas que são os subgrupos cíclicos, é preservada. Assim, a ordem de G, determina de forma única o número de p-subgrupos cíclicos desta decomposição, bem como suas ordens.

O Teorema acima não é prático para determinar as classes de isomorfismos de grupos abelianos de uma ordem fixada. Nem ao menos deixa claro a quantidade de tais classes.

Para resolver este problema, vamos olhar as duas decomposições feitas no Teorema 2.3.1, para um grupo abeliano G de ordem $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_t^{\alpha_t}$.

Pelo Teorema 2.1.1 temos

$$G = G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{p_t}$$

O corolário 2.1.2 diz que $|G_{p_i}| = p_i^{\alpha_i}$, e então estes p-grupos podem ser decompostos através dos Teoremas 2.2.1 e 2.2.2 como

$$G_{p_i} \simeq \mathbb{Z}_{p_i^{r_{i1}}} \oplus \mathbb{Z}_{p_i^{r_{i2}}} \oplus \ldots \oplus \mathbb{Z}_{p_i^{r_{it_i}}}.$$

Pela igualdade das ordens, vem que

$$p_i^{\alpha_i} = p_i^{r_{i1}}.p_i^{r_{i2}}.\ldots.p_i^{r_{it_i}},$$

isto é, $\alpha_i = r_{i1} + r_{i2} + \ldots + r_{it_i}$. Segue que $\{r_{i1}, r_{i2}, \ldots, r_{it_i}\}$ é uma partição de α_i, conforme a próxima definição.

Definição 2.3.1 *Seja $n \in \mathbb{N}, n \geq 1$. Chamamos de partição de n a todo conjunto de inteiros positivos $\{n_1, n_2, \ldots, n_s\}$ tal que:*

(i) $n = n_1 + n_2 + \ldots + n_s$

(ii) $n_1 \geq n_2 \geq \ldots \geq n_s \geq 1$

Notação:
$P(n)$ é o conjunto das partições de n.
$P^*(n)$ é o número de partições de n, isto é, $P^*(n) = \sharp P(n)$

Exemplo 2.3.1 $P(3) = \{\{3\}, \{2,1\}, \{1,1,1\}\}$ e $P^*(3) = 3$
$P(4) = \{\{4\}, \{3,1\}, \{2,2\}, \{2,1,1\}, \{1,1,1,1\}\}$ e $P^*(4) = 5$

Agora podemos provar o seguinte Teorema.

Teorema 2.3.2 *O número de grupos abelianos de ordem $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_t^{\alpha_t}$, dois a dois não isomorfos é $\prod_{i=1}^{n} p^*(\alpha_i)$.*

Demonstração

Seja G um grupo abeliano. Pelo Teorema 2.1.1 temos

$$G = G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{p_t}$$

e esta decomposição é única pelo Teorema 2.1.2. Para cada $i \in \{1, 2, \ldots, t\}$ temos que G_{p_i} é um p-grupo abeliano finito, então pelos Teoremas 2.2.1 e 2.2.2 podemos escrever de maneira única, a menos de isomorfismo

$$G_{p_i} \simeq \mathbb{Z}_{p_i{}^{r_{i1}}} \oplus \mathbb{Z}_{p_i{}^{r_{i2}}} \oplus \ldots \oplus \mathbb{Z}_{p_i{}^{r_{i\lambda_i}}}.$$

onde $\{r_{i1}, r_{i2}, \ldots, r_{i\lambda_i}\} = \alpha_i{}^G$ é uma partição de α_i. Desta forma, podemos associar ao grupo G de ordem n um único elemento $(\alpha_1{}^G, \alpha_2{}^G, \ldots, \alpha_t{}^G)$, que é uma t-upla correspondente as partições dos expoentes dos primos da fatoração de n. Seja T_n o conjunto dos grupos abelianos finitos de ordem n, dois a dois não isomorfos. Pela unicidade do elemento $(\alpha_1{}^G, \alpha_2{}^G, \ldots, \alpha_t{}^G)$ vem que a aplicação

$$\begin{array}{rccl} \Psi: & T_n & \longrightarrow & P(\alpha_1) \times P(\alpha_2) \times \ldots \times P(\alpha_t) \\ & G & \longmapsto & (\alpha_1{}^G, \alpha_2{}^G, \ldots, \alpha_t{}^G) \end{array}$$

está bem definida.

É claro que o número de elementos de $P(\alpha_1) \times P(\alpha_2) \times \ldots \times P(\alpha_t)$ é $(\sharp P(\alpha_1)) . (\sharp P(\alpha_2)) . \ldots . (\sharp P(\alpha_t)) = \prod_{i=1}^{n} P^*(\alpha_i)$. Assim basta provar que Ψ é bijetora. Para ver que é sobrejetora, tomamos $(\widetilde{\alpha_1}, \widetilde{\alpha_2}, \ldots, \widetilde{\alpha_t}) \in P(\alpha_1) \times P(\alpha_2) \times \times \ldots \times P(\alpha_t)$, com $\widetilde{\alpha_i} = \{r_{i1}, r_{i2}, \ldots r_{i\lambda_i}\}$ uma partição de $\widetilde{\alpha_i}$, isto é, $r_{i1} + r_{i2} + + \ldots + r_{i\lambda_i} = \widetilde{\alpha_1}$. Vamos escolher $G_i = \mathbb{Z}_{p_i{}^{r_{i1}}} \times \mathbb{Z}_{p_i{}^{r_{i2}}} \times \ldots \times \mathbb{Z}_{p_i{}^{r_{i\lambda_i}}}$. É óbvio que $|G_i| = p_i{}^{r_{i1}} . p_i{}^{r_{i2}} . \ldots . p_i{}^{r_{i\lambda_i}} = p_i{}^{\alpha_i}$. Tomando agora $G = G_1 \times G_2 \times \ldots \times G_t$ temos $|G| = |G_1| . |G_2| . \ldots . |G_t| = p_1{}^{\alpha_1} . p_2{}^{\alpha_2} . \ldots . p_t{}^{\alpha_t} = n$. Logo $G \in T_n$ e vamos provar que $\Psi(G) = (\widetilde{\alpha_1}, \widetilde{\alpha_2}, \ldots \widetilde{\alpha_t})$.

De fato, $G = G_{p_1} \oplus Gp_2 \oplus \ldots \oplus Gp_t$ e $G_{p_i} = \mathbb{Z}_{p_i{}^{s_{i1}}} \oplus \mathbb{Z}_{p_i{}^{s_{i2}}} \oplus \ldots \oplus \mathbb{Z}_{p_i{}^{s_{i\beta_i}}}$. Pela definição de Ψ, vem que,

$$\Psi(G) = (\alpha_1{}^G, \alpha_2{}^G, \ldots, \alpha_t{}^G) \quad , \quad \alpha_i{}^G = \{s_{i1}, s_{i2}, \ldots s_{i\beta_i}\}$$

Agora

$$G \simeq \mathbb{Z}_{p_1{}^{s_{11}}} \oplus \ldots \mathbb{Z}_{p_1{}^{s_{1\beta_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_t{}^{s_{t1}}} \oplus \ldots \oplus \mathbb{Z}_{p_t{}^{s_{t\beta_t}}}$$

e

$$G = G_1 \times G_2 \times \ldots \times G_t \simeq \mathbb{Z}_{p_1{}^{r_{11}}} \oplus \ldots \oplus \mathbb{Z}_{p_1{}^{r_{1\lambda_1}}} \oplus \ldots \oplus \mathbb{Z}_{p_t{}^{r_{t1}}} \oplus \ldots \oplus \mathbb{Z}_{p_t{}^{r_{t\lambda_t}}}.$$

Desde que o número destes fatores e suas ordens são determinados de modo único pelo grupo G, conforme o Teorema 2.3.1, devemos ter $\{s_{i1}, s_{i2}, \ldots, s_{i\beta_i}\} = \{r_{i1}, r_{i2}, \ldots, r_{i\lambda_i}\}$, ou seja, ${\alpha_i}^G = \widetilde{\alpha_i}$. Isso prova que $\Psi(G) = ({\alpha_1}^G, {\alpha_2}^G, \ldots, {\alpha_t}^G) = (\widetilde{\alpha_1}, \widetilde{\alpha_2}, \ldots, \widetilde{\alpha_t})$.

Falta provar a injetividade de Ψ. Suponhamos que $G, H \in T_n$ e $G \neq H$. Devemos verificar que $\Psi(G) \neq \Psi(H)$. Equivalentemente, admitindo que $\Psi(G) = \Psi(H)$ com $G, H \in T_n$, devemos provar que $G = H$ em T_n, isto é, $G \simeq H$. Mas

$$\Psi(G) = \Psi(H) \Rightarrow$$

$$\Rightarrow {\alpha_i}^G = {\alpha_i}^H \qquad , \forall i \in \{1, 2, \ldots, t\}$$

$$\Rightarrow \{r_{i1}^G, r_{i2}^G, \ldots, r_{it_i}^G\} = \{r_{i1}^H, r_{i2}^H, \ldots, r_{it_i}^H\} \qquad , \forall i \in \{1, 2, \ldots, t\}$$

$$\Rightarrow G_{p_i} \simeq \mathbb{Z}_{p_i{}^{r_{i1}^G}} \oplus \mathbb{Z}_{p_i{}^{r_{i2}^G}} \oplus \ldots \oplus \mathbb{Z}_{p_i{}^{r_{it_i}^G}} \simeq \mathbb{Z}_{p_i{}^{r_{i1}^H}} \oplus \mathbb{Z}_{p_i{}^{r_{i2}^H}} \ldots \oplus \mathbb{Z}_{p_i{}^{r_{it_i}^H}} \simeq H_{p_i}$$

Desde que

$$G = G_{p_1} \oplus G_{p_2} \oplus \ldots \oplus G_{pt}$$

$$H = H_{p_1} \oplus H_{p_2} \oplus \ldots \oplus H_{pt}$$

temos que $G \simeq H$

■

O último Teorema não só apresenta o número de grupos abelianos, dois a dois não isomorfos, de ordem n, mas também fornece um algoritmo para descrevê-los. Este algoritmo está justamente na parte da demonstração que verifica que Ψ é bijetora.

Olhando atentamente a demonstração, observamos que

$$\begin{array}{rccc} \Psi^{-1}: & P(\alpha_1) \times P(\alpha_2) \times \ldots \times P(\alpha_t) & \longrightarrow & T_n \\ & ({\alpha_1}^G, {\alpha_2}^G, \ldots, {\alpha_t}^G) & \longmapsto & G \end{array}$$

onde $G_i = \mathbb{Z}_{p_i{}^{r_{i1}}} \oplus \mathbb{Z}_{p_i{}^{r_{i2}}} \oplus \ldots \oplus \mathbb{Z}_{p_i{}^{r_{i\lambda_i}}}$ quando $\alpha_i = \{r_{i1}, r_{i2}, \ldots, r_{i\lambda_i}\}$ é uma partição de α_i.

Vejamos alguns exemplos.

Exemplo 2.3.2 Seja G um grupo tal que $|G| = 15 = 3^1.5^1$, assim temos $P(1) = 1$ e portanto existe um único grupo abeliano de ordem 15, a menos de isomorfismo.

Exemplo 2.3.3 Determinar o número de classes de isomorfismos de grupos abelianos de ordem 16200.

$$16200 = 2^3 . 3^4 . 5^2$$
$$P^*(3) = 3 \quad , \quad P^*(4) = 5 \quad e \quad P^*(2) = 2.$$

Logo temos 30 grupos dois a dois não isomorfos de ordem 16200.

Exemplo 2.3.4 Determinar a menos de isomorfismo, todos os grupos abelianos de ordem 360.

$$360 = 2^3 . 3^2 . 5$$
$$P^*(3) = 3 \quad , \quad P^*(2) = 2 \quad e \quad P^*(1) = 1.$$

Logo temos 6 grupos abelianos não isomorfos de ordem 360. São eles:

$G_1 = \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{360}$
$G_2 = \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
$G_3 = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
$G_4 = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
$G_5 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
$G_6 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

Exemplo 2.3.5 Determinar a menos de isomorfismo, todos os grupos abelianos de ordem 1200.

$$1200 = 2^4 . 3 . 5^2$$
$$P^*(4) = 5 \quad , \quad P^*(1) = 1 \quad e \quad P^*(2) = 2.$$

Logo temos 10 grupos abelianos não isomorfos de ordem 1200. São eles:

$G_1 = \mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \simeq \mathbb{Z}_{1200}$
$G_2 = \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
$G_3 = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
$G_4 = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
$G_5 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
$G_6 = \mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$G_7 = \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$G_8 = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$G_9 = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$G_{10} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

Temos então classificados todos os grupos abelianos finitos.

Capítulo 3

Grupos Finitos não Abelianos

Neste capítulo pretendemos descrever, a menos de isomorfismo, alguns grupos *finitos não abelianos*. Não abordaremos uma ordem específica, mas sim categorias de ordem que têm tratamento semelhante. Dessa forma, nosso interesse é por grupos de ordem p, $2p$, p^2, p^3 e pq, onde p e q são primos distintos com $p < q$.

3.1 Grupos de ordem p, $2p$, p^2 e p^3

Nesta seção inicial trataremos de grupos cuja classificação é relativamente simples, com exceção dos grupos de ordem p^3, onde p é um número primo ímpar.

Vimos no capítulo 1 que se a ordem de G é um número primo, então G é cíclico com p elementos e portanto $G \simeq \mathbb{Z}_p$ é abeliano. Assim não temos grupos não abelianos cuja ordem é um número primo.

Um outro caso bastante simples, é quando $|G| = 2p$, onde p é um número primo ímpar. De fato, sabemos que o grupo Diedral D_p é não abeliano de ordem $2p$, e a proposição abaixo mostra que ele é único com tais propriedades.

Proposição 3.1.1 *Seja G é um grupo de ordem $2p$, onde p é um número primo ímpar. Então $G \simeq \mathbb{Z}_{2p}$ ou $G \simeq D_p$.*

Demonstração

Se $|G| = 2p$ o Teorema de Cauchy garante que existem $s, t \in G$ tais que $O(s) = p$ e $O(t) = 2$. Seja $H = < s >$. Pelo Teorema de Lagrange temos

$$|G| = |H| \cdot (G : H).$$

Como $|G| = 2p$ e $|H| = p$ segue que $(G : H) = 2$ e portanto $H \lhd G$. Logo $\forall g \in G$, $gHg^{-1} = H$. Em particular, $tst^{-1} \in H$. Mas $O(t) = 2$ implica em $t^{-1} = t$, logo $tst \in H$ e H é cíclico, assim $tst = s^i$, $0 \leq i < p$.

$$t^2 = e \Rightarrow s = t^2st^2 = t(tst)t = ts^it.$$

Por outro lado

$$ts^it = \underbrace{tst \,.\, tst \,.\, \ldots \,.\, tst}_{i \text{ vezes}}$$

ou seja,

$$\overbrace{s^{i+i+\cdots+i}}^{i \text{ vezes}} = s^{i^2}.$$

Logo $ts^it = s^{i^2}$

Afirmação 1: $i^2 \equiv 1 (mod\, p)$.

$s = s^\alpha$, para algum $\alpha \in \mathbb{Z}$, então $s^{\alpha-1} = e$. Logo $p|\alpha - 1$, ou seja, $\alpha \equiv 1\,(mod\, p)$.

Fazendo $\alpha = i^2$ a afirmação está demonstrada. Desta forma temos $i^2 \equiv 1\,(mod\, p)$ e então $p|i^2-1$. Como $i^2-1 = (i+1)(i-1)$ segue que $p|i+1$ ou $p|i-1$.

Se $p|i + 1 \Rightarrow i \equiv -1\,(mod\, p)$

Se $p|i - 1 \Rightarrow i \equiv 1\,(mod\, p)$

Logo $i \equiv 1\,(mod\, p)$ ou $i \equiv -1\,(mod\, p)$. Com isso temos duas possibilidades: $tst = s$ ou $tst = s^{-1}$.

- Se $tst = s \Rightarrow ts = st^{-1} = st$, conseqüentemente G é abeliano e portanto $G \simeq \mathbb{Z}_{2p}$.
- Se $tst = s^{-1} \Rightarrow ts = s^{-1}t = s^{p-1}t$ e temos $G \simeq D_p$.

■

Assim D_p constitui a única família de grupos não abelianos de ordem $2p$, para p um número primo ímpar. Note que quando $p = 2$ estamos no caso p^2. Logo conhecemos todos os grupos não abelianos de ordem $2p$.

O próximo caso trata de grupos cuja ordem é p^2. Embora este seja menos simples que o caso anterior, concluiremos que se $|G| = p^2$ então G é abeliano.

Lema 3.1.1 *Sejam p um número primo e G um grupo tal que $|G| = p^n$ com $n \geq 1$. Então $|Z(G)| \geq p$.*

Demonstração

A equação das classes de conjugação garante que

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)|.$$

Para $x_\alpha \notin Z(G)$ temos $|Cl(x_\alpha)| > 1$ e afirmamos que $|Cl(x_\alpha)|$ divide $|G|$. De fato, seja $H = C_G(x) = \{g \in G;\ gx = xg\} = \{g \in G;\ x^g = x\}$ e seja $G/H = \{Hg;\ g \in G\}$ o conjunto de todas as classes laterais à esquerda de H em G.

Pelo Teorema de Lagrange temos $|G| = |G/H|.|H|$. Consideremos a aplicação abaixo definida por

$$\begin{array}{rccc} \phi: & G/H & \longrightarrow & Cl(x) \\ & Hg & \longmapsto & x^g \end{array}$$

É fácil ver que ϕ é sobrejetiva. Note que se $\phi(Hg_1) = \phi(Hg_2)$ então

$$x^{g_1} = x^{g_2} \Rightarrow x^{g_1 g_2^{\ -1}} = x \Rightarrow g_1 g_2^{-1} \in Cl(x) = H \Rightarrow Hg_1 = Hg_2.$$

Assim ϕ é bijetiva e $|G/H| = |Cl(x)| = \frac{|G|}{|H|}$ e portanto $|Cl(x)|$ divide $|G|$, ou seja, divide p^n. Logo $|Cl(x_\alpha)|$ é uma potência de p. Em particular, $|Cl(x_\alpha)|$ é múltiplo de p e portanto $\sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)|$ é um múltiplo de p.

Da equação das classes de conjugação, temos

$$|Z(G)| = |G| - \sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)|$$

e o elemento neutro de G pertence a $Z(G)$, ou seja, $Z(G) \neq \emptyset$ e $|Z(G)|$ é um múltiplo de p, uma vez que $|G| = p^n$ e $\sum_{x_\alpha \notin Z(G)} |Cl(x_\alpha)|$ é múltiplo de p. Logo $|Z(G)|$ tem pelo menos p elementos. Portanto $|Z(G)| \geq p$.

■

O Lema acima afirma que se $|G| = p^n$, $n \geq 1$, então $|Z(G)| \geq p$. Em

particular, se $|G| = p^2$ então $|Z(G)| = p$ ou $|Z(G)| = p^2$. A proposição abaixo mostrará que, neste caso particular, $|Z(G)|$ não pode ser p.

Proposição 3.1.2 *Seja G um grupo e seja $Z(G)$ seu centro. Se $\frac{G}{Z(G)}$ é cíclico então G é abeliano.*

Demonstração

Sejam $x, y \in G$. Então $\overline{x} = xZ(G)$ e $\overline{y} = yZ(G)$ estão em $\frac{G}{Z(G)}$, isto é

$$x.Z(G) = \alpha^n Z(G) \Rightarrow x = \alpha^n g_1 \ , \ g_1 \in Z(G)$$

$$y.Z(G) = \alpha^m Z(G) \Rightarrow y = \alpha^m g_2 \ , \ g_2 \in Z(G),$$

e portanto temos

$$\overline{x}.\overline{y} = \alpha^n g_1 \alpha^m g_2 = \alpha^{n+m} g_1 g_2 = \alpha^{m+n} g_2 g_1 = \alpha^m \alpha^n g_2 g_1 = \alpha^m g_2 . \alpha^n g_1 = \overline{y}.\overline{x}$$

■

Teorema 3.1.1 *Seja p um número primo. Então todo grupo de ordem p^2 é abeliano.*

Demonstração

Pelo lema anterior, as possibilidades para $|Z(G)|$ são p ou p^2.

Se $|Z(G)| = p$ então $\left|\frac{G}{Z(G)}\right| = p$, logo $\frac{G}{Z(G)}$ é cíclico. Então, pela proposição 3.1.2, G é abeliano e portanto $G = Z(G)$. Mas $G = Z(G)$ implica em $\left|\frac{G}{Z(G)}\right| = 1$, contradizendo o fato de que $\left|\frac{G}{Z(G)}\right| = p$ quando $|Z(G)| = p$. Assim, o índice de $Z(G)$ em G não pode ser um número primo. Então, só podemos ter $|Z(G)| = p^2$.

Se $|Z(G)| = p^2 \Rightarrow Z(G) = G \Rightarrow G$ é abeliano.

■

Portanto, não temos grupos não abelianos de ordem p^2.

Abordaremos agora os grupos de ordem p^3, onde p é um número primo. Primeiro trataremos do caso $p = 2$ e depois do caso p ímpar.

Lembre que já conhecemos dois grupos não abelianos e não isomorfos de ordem 8. A saber D_4 e Q_3. Eles não são isomorfos pois D_4 tem apenas os elementos

a e a^3 de ordem 4 enquanto que Q_3 tem $+i, -i, +j, -j, +k, -k$ como elementos de ordem 4.

Esses grupos são classificados segundo as relações abaixo:

$$D_4 =< a, b; a^4 = b^2 = e \text{ e } b^{-1}ab = a^3 >$$

$$Q_3 =< a, b; a^4 = e, a^2 = b^2 \text{ e } b^{-1}ab = a^3 >$$

onde o grupo dos Quatérnios Q_3 foi apresentado como o conjunto

$$Q_3 = \{+1, -1, +i, -i, +j, -j, +k, -k\}$$

munido do produto

$ij = -ji = k$
$jk = -kj = i$
$ki = -ik = j$

Escolhendo $a = i$ e $b = j$ o grupo dos Quatérnios está classificado como na relação acima.

Os grupos não abelianos de ordem 2^3 ficam completamente determinados com o teorema abaixo.

Teorema 3.1.2 *Os únicos grupos não abelianos de ordem 8 são D_4 e Q_3.*

Demonstração

Seja G um grupo não abeliano de ordem 8. Então G não possui elemento de ordem 8. Também pela proposição 1.1.1 G possui pelo menos um elemento de ordem diferente de 2. Assim G possui um elemento a de ordem 4. Chamando $H =< a >$ temos que $H \lhd G$ por ter índice 2. Seja $b \in G$ tal que $b \notin H$. Afirmamos que $b^2 \in H$. De fato, como temos exatamente duas classes laterais e $b \notin H$ essas classes são exatamente H e Hb. Assim temos que o grupo G é gerado por a e b. Se $b^2 \in Hb$ então $b^2 = a^i b$, $i \in \{0, 1, 2, 3\}$, implicando em $b = a^i \in H$ o que contradiz nossa escolha de $b \notin H$. Portanto $b^2 \in H$. Vamos analisar as possibilidades para b^2. Note que $b^2 = a$ ou $b^2 = a^3$ leva a $O(b) = 8$ que não pode ocorrer pois G não é abeliano. Assim restam as possibilidades $b^2 = e$ e $b^2 = a^2$. Além disso como $H \lhd G$ devemos ter $b^{-1}ab \in H$, isto é, $b^{-1}ab = e$, $b^{-1}ab = a$, $b^{-1}ab = a^2$ ou $b^{-1}ab = a^3$. Se $b^{-1}ab = e$ leva a $a = e$ e se $b^{-1}ab = a$ leva a $ab = ba$, que não pode ocorrer pois $O(a) = 4$ e G não é

comutativo. Supondo $b^{-1}ab = a^2$ e lembrando que $O(a^2) = 2$ vem que

$$e = a^2 \cdot a^2 = b^{-1}abb^{-1}ab = b^{-1}a^2b$$

daí $b = a^2b$ e chegamos à contradição $a^2 = e$. Portanto devemos ter $b^{-1}ab = a^3$.

Temos apenas as seguintes possibilidades para os geradores de G:

- $a^4 = e$, $b^2 = a^2$ e $b^{-1}ab = a^3$
- $a^4 = e$, $b^2 = e$ e $b^{-1}ab = a^3$

que correspondem respectivamente a Q_3 e D_4.

■

Teorema 3.1.3 *Seja G um grupo não abeliano de ordem p^3, onde p é um número primo ímpar. Então temos exatamente duas possibilidades não isomorfas.*

1) $G = G_1 =< a, b\,;\, a^{p^2} = b^p = e,\, b^{-1}ab = a^{p+1} >$

2) $G = G_2 =< a, b, c\,;\, a^p = b^p = c^p = e, ab = bac, ca = ac, cb = bc >$

Demonstração

Como G é não abeliano, não temos elemento de ordem p^3. Logo, a ordem dos elementos diferentes do elemento neutro só pode ser p ou p^2. Vamos inicialmente supor que G tem um elemento a tal que $O(a) = p^2$. Assim, $H =< a >$ é um subgrupo de ordem p^2. Desde que H é um subgrupo maximal do p-grupo G temos que $H \lhd G$ pelo Teorema 1.6.2 *(2o. Teorema de Sylow)*. Desde que $\left|\frac{G}{H}\right| = p$ devemos ter classes laterais definidas a partir de H que formam uma partição de G da forma

$$G = H_1 + H_2 + \ldots + H_p.$$

Claro que podemos tomar $H_1 = H$, a classe do elemento neutro. Dado $b_2 \in G$ tal que $b_2 \notin H$, afirmamos que $G = H + Hb_2 + \ldots + Hb_2^{p-1}$ é uma partição de G. De fato, para $i \in \{0, 1, \ldots, p-1\}$ temos que Hb_2^i é uma classe lateral segundo H, então precisamos apenas provar que são distintas e teremos que são disjuntos. Suponha que $Hb_2^i = Hb_2^j$, com $i \neq j$, $i, j \in \{0, 1, \ldots, p-1\}$. Sem perda de generalidade vamos considerar $i > j$. Desde que $b_2^i \in Hb_2^i = Hb_2^j$, existe $\alpha \in \{0, 1, \ldots, p^2\}$ tal que $b_2^i = a^\alpha b_2^j$, isto é, $b_2^{i-j} = a^\alpha$. Chamando $\beta = i - j$ e observando que $\beta \in \{0, 1, \ldots, p-1\}$ vemos que $\text{mdc}(\beta, p^2) = 1$. Agora, pela identidade de Bezout existem $x, y \in \mathbb{Z}$ tais que $x\beta + yp^2 = 1$ e portanto $b_2 = (b_2^\beta)^x \cdot (b_2^{p^2})^y = (b_2^\beta)^x = (b_2^{i-j})^x = (a^\alpha)^x$, que leva à

contradição $b_2 \in H$. Assim $Hb_2^i \neq Hb_2^j$ para $i \neq j$, $i, j \in \{0, 1, \ldots, p-1\}$ e temos a partição de G dada por $G = H + Hb_2 + \ldots + Hb^{p-1}$.

Como $b_2^p \in G$ devemos ter $b_2^p \in Hb_2^i$, para algum $i \in \{0, 1, \ldots, p-1\}$, isto é, $b_2^p = a^\alpha b_2^i$ donde $b_2^{p-i} = a^\alpha \in H \cap Hb_2^{p-i} = \emptyset$. Logo deve ser $i = 0$, ou seja, $b_2^p = a^\alpha \in H$. A normalidade de H em G também garante que $b_2^{-1}ab_2 = a^r$ para algum $r \in \{2, 3, \ldots, p^2\}$. Excluímos $r = 1$ pois neste caso teríamos que $ab_2 = b_2a$, e como G é gerado por a e b_2 teríamos que G é abeliano, contradizendo nossa hipótese.

Afirmação 2 Para todo $j \in \mathbb{N}$ temos $b_2^{-j}ab_2^j = a^{r^j}$.

Faremos por indução sobre j. O caso $j = 1$ já vimos acima. Suponha que a igualdade valha para j e considere

$$b_2^{-(j+1)}ab_2^{j+1} = b_2^{-1}b_2^{-j}ab_2^jb_2 = b_2^{-1}a^{r^j}b_2 =$$

$$= \underbrace{(b_2^{-1}ab_2)(b_2^{-1}ab_2)\ldots(b_2^{-1}ab_2)}_{r^j \ - \ fatores} = \underbrace{a^r \ldots . a^r}_{r^j \ - \ fatores} = a^{r \cdot r^j} = a^{r^{j+1}}$$

Como $b_2^p \in H$ temos que b_2^p comuta com a e então $a = b_2^{-p}ab_2^p = a^{r^p}$ implicando em $r^p \equiv 1\,(mod\,p^2)$ e em $r^p \equiv 1\,(mod\,p)$. Sabemos que o Pequeno Teorema de Fermat assegura que $r^p \equiv r\,(mod\,p)$. Segue que $r \equiv 1\,(mod\,p)$ e escrevemos $r = 1 + sp$.

Afirmação 3 $0 < s < p$ e $\exists j \in \mathbb{N}$ tal que $js \equiv 1\,(mod\,p)$.

Como $r = 1 + sp$ e $1 < r < p^2$ vemos que $s > 0$. Também $0 < r - 1 < p^2 - 1$, temos $sp < p^2 - 1 < p^2$ e então $s < p$. Olhando $\overline{s}$ como elemento do corpo $\mathbb{Z}_p$ obtemos um inverso $\overline{j} \in \mathbb{Z}_p$, isto é, $\overline{s}\overline{j} = \overline{1}$ e portanto $js \equiv 1\,(mod\,p)$.

Para o elemento j obtido na afirmação anterior calculamos

$$b_2^{-j}ab_2^j = (a^r)^j = a^{(1+sp)^j}.$$

Como $O(a) = p^2$, nos interessa conhecer o expoente de a feita a congruência módulo p^2.

$$(1 + sp)^j = 1 + jsp + \frac{j(j-1)}{2}(sp)^2 + \frac{j(j-1)(j-2)}{3!}(sp)^3 + \ldots + (sp)^j$$

Note que a partir da segunda parcela todos os somandos são divisíveis por p^2, e então $(1+sp)^j \equiv (1+jsp)\,(mod\,p^2)$. Além disso, $js \equiv 1\,(mod\,p)$ implica em $jsp \equiv p\,(mod\,p^2)$, e então $(1+sp)^j \equiv (1+p)\,(mod\,p^2)$. Agora podemos concluir que

$$b_2^{-j}ab_2^j = (a^r)^j = a^{(1+sp)^j} = a^{1+p}.$$

Recapitulando as propriedades obtidas para o elemento $b_2 \in G$

$$b_2 \notin H,\ b_2^p \in H,\ b_2^{-j}ab_2^j = a^{1+p}, \qquad \text{para algum } j,\ 1 \leq j \leq p-1.$$

Então $G = H + Hb_2 + Hb_2^2 + \ldots + Hb_2^{p-1}$ é uma partição de G e G é gerado por a e b_2, já que $H =< a >$ é subgrupo maximal e $b_2 \notin A$.

Vamos tomar agora $b_1 = b_2^j \in G$.

Afirmação 4 $b_1 \notin H$.

Vimos que j é inversível em $\mathbb{Z}_p$, logo $mdc\,\{j,p\} = 1$ e então existem $x, y \in \mathbb{Z}$ tais que $1 = xj + yp$. Também como $b_2^p \in H$, temos que $b_2^p = a^\alpha$ para algum $\alpha \in \{0,1,\ldots,p^2\}$.

$$b_2 = (b_2^j)^x(b_2^p)^y = b_1^x(a^\alpha)^y.$$

Supondo que $b_1 \in H$ segue da igualdade acima que $b_2 \in H$, que é uma contradição.

Como $H =< a >$ é subgrupo maximal de G e $b_1 \notin H$, temos que G é gerado por a e b_1. Também vale $b_1^{-1}ab_1 = a^{1+p}$.

Desde que $b_2^p \in H$ e $b_1^p = (b_2^j)^p = (b_2^p)^j$ temos que $b_1^p \in H$, isto é, existe $t \in \{0,1,\ldots,p^2\}$ tal que $b_1^p = a^t$.

Afirmação 5 t é um múltiplo de p.

Pelo fato de G ser não abeliano, não podemos ter $O(b_1) = p^3$. Logo $(b_1^p)^p = e$, e então $e = a^{pt}$. Mas $O(a) = p^2$ e assim $p^2|pt$, isto é, t é múltiplo de p.

Vamos escrever $t = pu$.

Afirmação 6 Para todo $i \in \mathbb{Z}$ vale a relação $a^ib_1 = b_1a^{i(1+p)}$.

Para o caso $i > 0$, segue da igualdade $b_1^{-1}ab_1 = a^{1+p}$ que

$$b_1^{-1}a^ib_1 = \underbrace{(b_1^{-1}ab_1)(b_1^{-1}ab_1)\ldots(b_1^{-1}ab_1)}_{i\ -\ fatores} = \underbrace{a^{1+p}a^{1+p}\ldots a^{1+p}}_{i\ -\ fatores} = a^{i(1+p)}$$

e daí, $a^ib_1 = b_1a^{i(1+p)}$. Tiramos de $(a^ib_1)^{-1} = (b_1a^{i(1+p)})^{-1}$ que $b_1^{-1}a^{-i} = a^{-i(1+p)}b_1^{-1}$ e então $a^{-i}b_1 = b_1a^{-i(1+p)}$.

Nosso objetivo agora é mostrar que $(ba^{-u})^p = 1$, usando a afirmação anterior.

Provaremos primeiro, por indução sobre $n \in \mathbb{N}$, que

$$(b_1a^{-u})^n = b_1^n a^{-u[1+(1+p)+(1+p)^2+\ldots+(1+p)^{n\ -\ 1}]}$$

Para o caso $n = 1$, o lado direito da igualdade se reduz a $b_1a^{-u[1]}$ e não temos nada a fazer. Admitindo que a igualdade vale para n, calculamos:

$$(b_1a^{-u})^{n+1} = (b_1a^{-u})^n \cdot b_1a^{-u} = b_1^n(a^{-u[1+(1+p)+(1+p)^2+\cdots+(1+p)^{n-1}]}) \cdot (b_1a^{-u}) =$$

$$= b_1^nb_1a^{-u[1+(1+p)+(1+p)^2+\cdots+(1+p)^{n\ -\ 1}](1+p)} \cdot a^{-u} = b_1^{n+1} \cdot a^{-u(1+(1+p)+(1+p)^2+\cdots+(1+p)^n]}$$

Em particular, fazendo $n = p$, vemos que $(b_1a^{-u})^p = b_1^pa^{-u[1+(1+p)+(1+p)^2+\cdots+(1+p)^{p-1}]}$. Desde que $O(a) = p^2$, vamos olhar para $[1 + (1 + p) + (1 + p)^2 + \ldots + (1 + p)^{p-1}]$ módulo p^2:

$$\begin{aligned}
1 = 1 \Rightarrow \quad & 1 \equiv 1\,(mod\,p^2) \\
1 + p = 1 + p \Rightarrow \quad & 1 + p \equiv 1 + p\,(mod\,p^2) \\
(1 + p)^2 = 1 + 2p + p^2 \Rightarrow \quad & (1 + p)^2 \equiv 1 + 2p\,(mod\,p^2) \\
(1 + p)^3 = 1 + 3p + 3p^2 + p^3 \Rightarrow \quad & (1 + p)^3 \equiv 1 + 3p\,(mod\,p^2) \\
\vdots & \\
(1 + p)^{p-1} = 1 + (p - 1)p + \ldots + p^{p-1} \Rightarrow \quad & (1 + p)^{p-1} \equiv 1 + (p - 1)p\,(mod\,p^2)
\end{aligned}$$

Logo $[1+(1+p)+(1+p)^2+\ldots+(1+p)^{p-1}] \equiv p+p(1+2+3+\ldots+p-1)\,(mod\,p^2)$. Além disso, $1 + 2 + 3 + \ldots + p - 1 = \frac{p(p-1)}{2}$ é um múltiplo de p, pois por hipótese p é

um primo ímpar. Daí, $p(1+2+\ldots+p-1) = \frac{p^2(p-1)}{2} \equiv 0\,(mod\,p^2)$. Segue que

$$[1+(1+p)+(1+p)^2+\ldots+(1+p)^{p-1}] \equiv p\,(mod\,p^2)$$

e então $(b_1a^{-u})^p = b_1^p a^{-up} = 1$, já que $b_1^p = a^{up}$.

Escolhemos agora $b = b_1a^{-u}$ e como visto acima, $b^p = 1$. Note que $b \notin H$, pois caso contrário teríamos $b_1 \in H$ que sabemos não ser possível. Como H é subgrupo maximal gerado por a e $b \notin H$ temos que:

- G é gerado por a e b;
- $O(a) = p^2$;
- $O(b) = p$;

  Só resta mostrar que

- $b^{-1}ab = a^{p+1}$

  Mas isso vale pois

$$b^{-1}ab = a^u b_1^{-1} a b_1 a^{-u} = a^u a^{p+1} a^{-u} = a^{p+1}.$$

Fica provado que se G contém um elemento de ordem p^2 então

$$G = G_1 =< a, b; a^{p^2} = b^p = e \text{ e } b^{-1}ab = a^{p+1} >$$

Vamos agora provar o caso em que G não possui elemento de ordem p^2. Assim todo elemento diferente de e tem ordem p.

Sabemos pelo Lema 3.1.1 que o centro de G tem pelo menos p elementos. Mas não podemos ter $|Z(G)| = p^2$ pois então teríamos $\frac{G}{Z(G)}$ cíclico e pela proposição 3.1.2 concluiríamos que G é abeliano. Portanto $|Z(G)| = p$ e $\left|\frac{G}{Z(G)}\right| = p^2$. Pelo Teorema 3.1.1 $\frac{G}{Z(G)}$ é abeliano, mas sabemos que não é cíclico, logo $\frac{G}{Z(G)} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Assim, existem $x, y \in \frac{G}{Z(G)}$ tais que $x^p = y^p = e$ e $yx = xy$. Através da imagem inversa do homomorfismo canônico $\varphi : G \to \frac{G}{Z(G)}$ obtemos $a, b \in G$ tais que $\varphi(a) = x$ e $\varphi(b) = y$. Note que $a, b \notin Z(G) = \text{Ker}\varphi$, pois caso contrário teríamos $\varphi(a) = \varphi(b) = \overline{e}$, onde $\overline{e}$ é o elemento neutro de $\frac{G}{Z(G)}$. Como $O(\varphi(\alpha))|O(\alpha)$, devemos ter $O(x)|O(a)$ e $O(y)|O(b)$, isto é, $O(a) = O(b) = p$. Como $\frac{G}{Z(G)}$ é abeliano,

$$\varphi(a^{-1}b^{-1}ab) = \varphi(a^{-1})\varphi(b^{-1})\varphi(a)\varphi(b) = x^{-1}y^{-1}xy = \overline{e}$$

Segue que $a^{-1}b^{-1}ab \in \text{Ker}\varphi = Z(G)$.

Afirmação 7 a, b e $Z(G)$ geram G.

Seja $n \in \{1, 2, \ldots, p-1\}$ e suponha que $a^n \in Z(G)$. Então $\overline{e} = \varphi(a^n) = x^n$ que contradiz o fato de $O(x) = p$. Assim $a^n \notin Z(G)$ para $n \in \{1, 2, \ldots, p-1\}$ e analogamente $b^n \notin Z(G)$ para $n \in \{1, 2, \ldots, p-1\}$.

Supondo que $Z(G)a^n = Z(G)a^m$ com $n, m \in \{1, 2, \ldots, p-1\}$ e $n > m$ vem que $a^{n-m} \in Z(G)$ com $n - m \in \{1, 2, \ldots, p-1\}$, que já vimos que não pode ocorrer. Analogamente, $Z(G)b^n \neq Z(G)b^m$ para $n, m \in \{1, 2, \ldots, p-1\}$ e $n > m$.

Suponha agora que $Z(G)a^n = Z(G)b^m$ com $n, m \in \{1, 2, \ldots, p-1\}$. Então $a^n b^{-m} \in Z(G)$ e aplicando φ temos $\overline{e} = x^n y^{-m}$, isto é, $x^n = y^m$ que não pode ocorrer pois x e y são os geradores de $\frac{G}{Z(G)}$ com $O(x) = O(y) = p$ e $\left|\frac{G}{Z(G)}\right| = p^2$.

Concluímos que as classes laterais $Z(G), Z(G)a, \ldots, Z(G)a^{p-1}, Z(G)b, \ldots$ $\ldots, Z(G)b^{p-1}$ são todas distintas com p elementos. Assim, a partir de $Z(G)$, a e b geramos um subgrupo de G com $p + (p-1)p + (p-1)p = p^2 + p^2 - p > p^2$ elementos. Portanto, a, b e $Z(G)$ geram G.

Sabemos que $a^{-1}b^{-1}ab \in Z(G)$ e não podemos ter $a^{-1}b^{-1}ab = e$, pois neste caso $ab = ba$, e pela afirmação anterior a, b e $Z(G)$ geram G, logo teríamos que G é abeliano. Segue que $a^{-1}b^{-1}ab = c \in Z(G)$ e $o(c) = p$, isto é, c é um gerador de $Z(G)$. Portanto a, b e c geram G e valem as relações $a^p = b^p = c^p = e$ e $ab = bac$. Claro que c comuta com a e b e obtemos

$$G = G_2 = < a, b, c; a^p = b^p = c^p = e, ab = bac, ac = ca \text{ e } bc = cb >$$

É imediato que G_1 e G_2 não são isomorfos pois G_1 possui elementos de ordem p^2 e G_2 não.

■

3.2 Grupos de ordem pq

Nesta seção consideraremos p e q primos distintos com $p < q$ e estudaremos os grupos de ordem pq. Provaremos que se G é um grupo de ordem pq e se p não divide $q-1$ então $G \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$. Veremos ainda que quando p divide $q-1$ então

existe um único grupo não abeliano de ordem pq, que é gerado por dois elementos.

Teorema 3.2.1 *Seja G um grupo não abeliano de ordem pq, onde p e q são números primos e $p < q$. Então*

(i) $p|(q-1)$

(ii) $G =< a, b\,;\, a^p = b^q = e, a^{-1}ba = b^r >$

onde $r \not\equiv 1\,(mod\,q)$ *e* $r^p \equiv 1\,(mod\,q)$.

Demonstração

Pelo 1^0. Teorema de Sylow temos em G um elemento b de ordem q. Seja $H =< b >$, então H é um q-subgrupo de Sylow de G. O 3^0. Teorema de Sylow garante que o número de q-subgrupos de Sylow é $nq \equiv 1\,(mod\,q)$ e $nq|p$, isto é, $nq = 1 + uq$ para algum $u \in \mathbb{N}$ e $nq = 1$ ou $nq = p$. O caso $p = nq = 1 + uq$ contradiz a hipótese $p < q$. Logo $nq = 1$ e H é o único q-subgrupo de Sylow de G, e portanto $H \lhd G$ pelo 2^0 Teorema de Sylow. Analogamente, G tem um elemento a de ordem p. Chamando $S =< a >$ temos que S é um p-subgrupo de Sylow de G, e o número de tais subgrupos é da forma $n_p = 1 + vp$, $v \in \mathbb{N}$, e $n_p = 1$ ou $n_p = q$.

1^o **Caso:** $n_p = 1$

Como vimos acima, neste caso, $S \lhd G$. Podemos escrever $a^{-1}b^{-1}ab = = a^{-1}(b^{-1}ab) = (a^{-1}b^{-1}a)b$. Então

$$S \lhd G \text{ e } a \in S \Rightarrow b^{-1}ab \in b^{-1}Sb \subseteq S \Rightarrow a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) \in S$$

$$H \lhd G \text{ e } b \in H \Rightarrow a^{-1}ba \in a^{-1}Ha \subseteq H \Rightarrow a^{-1}b^{-1}ab = (a^{-1}b^{-1}a)b \in H$$

Assim, $a^{-1}b^{-1}ab \in S \cap H$, mas como S e H são grupos cíclicos cujas ordens são números primos distintos, temos que $S \cap H = \{e\}$. Segue que $ab = ba$. Como $O(a) = p$, $O(b) = q$ e $|G| = pq$ temos que G é gerado por a e b, e portanto G deve ser abeliano. Contradição!

2^o **Caso:** $n_p = q$

Como o caso anterior não é possível já temos provado que p divide $q - 1$ pois $n_p = q = 1 + vp$.

Como $H =< b > \lhd G$, vale $a^{-1}ba = b^r$ para algum r, e claramente $r \neq 1$ pois G é não abeliano. Além disso, como $O(b) = q$ temos que $b^r = b$ quando $r \equiv 1\,(mod\,q)$, e então concluímos que $r \not\equiv 1\,(mod\,q)$.

Afirmação 1 Para todo $j \in \mathbb{N}$ vale $a^{-j}ba^j = b^{r^j}$.

Faremos por indução sobre j. O caso $j = 1$ já está garantido. Admitamos que a igualdade valha para j, e considere

$$a^{-(j+1)}ba^{j+1} = a^{-1}(a^{-j}ba^j)a = a^{-1}b^{r^j}a =$$

$$= \underbrace{(a^{-1}ba)(a^{-1}ba)\ldots(a^{-1}ba)}_{r^j \text{ - vezes}} = \underbrace{b^r.b^r.\ldots.b^r}_{r^j \text{- vezes}} = b^{r\cdot r^j} = b^{r^{j+1}}$$

Desde que $a^p = e$, fazemos $j = p$ na igualdade da afirmação anterior, obtendo $b = a^{-p}ba^p = b^{r^p}$, donde $r^p \equiv 1\,(mod\,q)$ pois $O(b) = q$.

■

Quando estudamos a classificação de grupos finitos, é útil ter em mente uma formulação um pouco diferente do teorema anterior.

Proposição 3.2.1 *Seja G um grupo abeliano de ordem pq, onde p e q são primos distintos e $p < q$. Se p não divide $q - 1$ então G é cíclico.*

Demonstração

Seguindo a demonstração do Teorema anterior, vemos que não podemos entrar no segundo caso, pois lá teríamos $n_p = q = 1 + vp$, isto é, p divide $q - 1$. Logo estamos no primeiro caso que leva a G abeliano de ordem pq. Vimos no capítulo 2 que $G \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$ e portanto G é cíclico.

■

Vejamos alguns exemplos.

Exemplo 3.2.1 Seja G um grupo com $|G| = 15 = 3.5$. Desde que $p = 3$ e $q = 5$ temos que $p \nmid (q-1)$ então pela proposição 3.2.1 G é cíclico, isto é, $G \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$.

Exemplo 3.2.2 Analogamente se

$|G| = 33 = 3.11$

$|G| = 51 = 3 \cdot 17$
$|G| = 35 = 5 \cdot 7$
$|G| = 65 = 5 \cdot 13$

então G é cíclico.

Exemplo 3.2.3 Seja G um grupo tal que $|G| = 21 = 3 \cdot 7$. Claro que uma possibilidade é $G \simeq \mathbb{Z}_3 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{21}$ que é abeliano. Como 3 divide (7-1) podemos ter G não abeliano. Vamos admitir que exista G não abeliano *(veja próxima proposição)*. Pelo Teorema 3.2.1

$$G =< a, b;\ a^3 = b^7 = e,\ a^{-1}ba = b^r >$$

onde $r \not\equiv 1\,(mod\,7)$ e $r^3 \equiv 1\,(mod\,7)$. Vamos determinar os possíveis valores para r.

Note que:
$r = 0 \Rightarrow a^{-1}ba = e \Rightarrow ba = a = b = e$. Absurdo. Logo $r \neq 0$.

Podemos ter $r = 1, 2, 3, 4, 5, 6$.
Fazendo $r = 7$, obtemos novamente o absurdo acima pois $b^7 = b^0 = e$.
Fazendo $r = 8$, obtemos novamente a relação que tínhamos com $r = 1$.

Seguindo este raciocínio vemos que só nos interessa $r = 1, 2, 3, 4, 5, 6$. Mas $r = 1$ não satisfaz $r \not\equiv 1\,(mod\,7)$, e $r = 3, 5, 6$ não satisfaz a relação $r^3 \equiv 1\,(mod\,7)$. Portanto os possíveis valores para r são 2 e 4.

Aparentemente isso indica que podemos ter dois grupos não abelianos de ordem 21. A saber:

$$G =< a, b;\ a^3 = b^7 = e,\ a^{-1}ba = b^2 >$$

$$G' =< a, b;\ a^3 = b^7 = e,\ a^{-1}ba = b^4 > .$$

No entanto, sabemos da literatura de grupos finitos *(Garcia A. & Lequain, Y, Álgebra: Um Curso de Introdução - Proposição IV.21)* que existe apenas um grupo não abeliano de ordem 21. Isso significa que devemos ser capazes de provar que G e G' são isomorfos.

Em G vamos trocar o gerador a de ordem 3 por $\alpha^2 = a$, que também tem ordem 3.

Desde que $a^{-1}ba = b^2$, isto é, $ba = ab^2$ e $\alpha^2 = a$ temos

$$b\alpha = baa = ab^2a = abab^2 = a^2b^2b^2 = a^2b^4 = \alpha b^4.$$

Logo $G =< \alpha, b\,;\ \alpha^3 = b^7 = e\ ,\ \alpha^{-1}b\alpha = b^4 >$, ou seja, as relações de G e G' são as mesmas e $G \simeq G'$.

No desenvolvimento do exemplo acima, admitimos que existia um único grupo G de ordem $3.7 = 21$ não abeliano. Fizemos isso baseado na Proposição abaixo. *Garcia A. & Lequain, Y, Álgebra: Um Curso de Introdução - IMPA - Rio de Janeiro, 1988. Capítulo IV.7.*

Proposição 3.2.2 *Sejam $m, n, r \in \mathbb{N}$ tais que $r^m \equiv 1\,(mod\, n)$. Então existe um, e somente um, grupo G de ordem $m.n$ satisfazendo as relações*

$$G =< a, b\,;\ a^n = b^m = e\,,\ ba = a^r b >\,.$$

Fazendo $n = 7$, $m = 3$ e $r = 2$ produzimos um grupo não abeliano de ordem 21.

Temos ainda um outro resultado relacionado com o Teorema 3.2.1, que aparece no livro de *Marshall Hall Jr, The Theory of groups, Página 51.* Vamos apresentá-lo na forma de Lema.

Lema 3.2.1 *Sejam p e q primos distintos com $p < q$ tais que p não divide $(q-1)$. O sistema*

$$\begin{cases} z^p \equiv 1\,(mod\, q) \\ z \not\equiv 1\,(mod\, q) \end{cases}$$

sempre tem solução em $\mathbb{N}$. Além disso, se r é uma solução então o conjunto solução é $\{r, r^2, \ldots, r^{p-1}\}$.

De volta ao exemplo 3.2.3 onde tínhamos$|G| = 21 = 3.7$ com $p = 3$ e $q = 7$, vemos que as soluções para o sistema acima são exatamente 2 e 4.

A unicidade do grupo não abeliano de ordem 21 agora pode ser reobtida da próxima proposição.

Proposição 3.2.3 *Todas as soluções do sistema apresentado acima produzem o mesmo grupo não abeliano de ordem pq.*

Demonstração

Basta provar que para $u = 2, 3, \ldots, p-1$ os grupos

$$G_u = < a, b;\ a^p = b^q = e,\ a^{-1}ba = b^{r^u} >$$

e

$$G = < a, b;\ a^p = b^q = e,\ a^{-1}ba = b^r >$$

coincidem.

Em G vamos trocar o gerador a de ordem p por $\alpha = a^u$ que também tem ordem p.

Desde que $ba = ab^r$, segue por analogia ao que foi feito na demonstração do Teorema 3.1.3 que $b\alpha = \alpha b^{r^u}$. Assim

$$G = < \alpha, b;\ \alpha^p = b^q = e,\ \alpha^{-1}b\alpha = b^{r^u} >$$

que coincide com G_u.

■

Exemplo 3.2.4 Seja G um grupo tal que $|G| = 39 = 3.13$. Desde que para $r = 3, p = 3$ e $q = 13$ temos $r^p \equiv 1\,(mod\,q)$ existe, pela proposição 3.2.2 um grupo não abeliano de ordem 39. Além disso, $r = 3$ também é solução do sistema

$$\begin{cases} z^p \equiv 1\,(mod\,q) \\ z \not\equiv 1\,(mod\,q) \end{cases}$$

e então seu conjunto solução é {3,9}. Assim o único grupo não abeliano de ordem 39 é

$$G = < a, b;\ a^3 = b^{13} = 3,\ a^{-1}ba = b^3 > .$$

Com o que vimos neste trabalho, conseguimos classificar grupos finitos de várias ordens. No entanto, mesmo para ordens pequenas, por exemplo 12, 16, 18 e 20, não fizemos a classificação dos grupos não abelianos. A classificação de grupos não abelianos de ordens p^n para $n > 3$, p^2q e pqr, com p, q e r primos distintos requer muito trabalho, apesar de existir, em alguns casos, um procedimento geral. Isso foge do objetivo deste trabalho, que buscou apresentar apenas alguns dos Teoremas gerais de classificação.

Referências Bibliográficas

[1] Hall Jr, Marshall - The Theory of Groups - Chelsea Publishing Company - New York, 1968.

[2] Rotman, Joseph J., The Theory of Groups: An Introduction - Allyn and Bacon - Boston,1968.

[3] Burniside, W., Theory of Groups of Finite order - Dover Publication, Inc. - New York, 1955.

[4] Gonçalves, A, Introdução à Álgebra - IMPA - Rio de Janeiro, 1999.

[5] Garcia A. & Lequain, Y, Álgebra: Um Curso de Introdução - IMPA - Rio de Janeiro, 1988.

[6] Jacy Monteiro, L.H., Elementos de Álgebra - IMPA - Rio de Janeiro, 1969.