GRUPOS

Maria Lúcia Torres Villela
Instituto de Matemática
Universidade Federal Fluminense
Maio de 2008
Revisto em Dezembro de 2008

Sumário

Parte 2

Complementos da Teoria de Grupos

Nosso objetivo é apresentar, primeiramente, o conceito de subgrupo normal, que permitirá construir o grupo quociente. O grupo quociente é uma ferramenta muito importante nesse contexto e serão dados exemplos ilustrativos dessa teoria.

Complementaremos os resultados de homomorfismo de grupos, abordando o Teorema Fundamental dos homomorfismos de grupos e obtendo como aplicação o Teorema de Cauchy para grupos abelianos finitos.

Veremos a Equação de Classe de um grupo finito e, como uma aplicação classificaremos os grupos de ordem p^2, onde p é primo.

Apresentaremos uma demonstração do Teorema de Sylow, que utiliza diferentes relações de equivalência no grupo finito, realizando a contagem dos elementos do grupo finito de maneiras distintas.

Vamos apresentar condições necessárias e suficientes para um grupo ser isomorfo a um produto direto.

Classificaremos os p-grupos abelianos finitos e, finalmente, como uma aplicação do Teorema de Sylow e do conceito de produto direto, faremos a classificação dos grupos abelianos finitos.

Recomendamos consultar os seguintes textos:

- *Elements of Abstract Algebra* , R. A. Dean, Wiley Internacional, 1974.
- *A First Course in Abstract Algebra*, John B. Fraleigh, Addison-Wesley Publishing Company, 1967.

Referências:

Para a parte elementar da teoria de grupos: *Introdução à Álgebra*, Adilson Gonçalves, Projeto Euclides, IMPA, 2000.

(Esse texto tem uma abordagem ressaltando a importância da Teoria de Grupos a outras áreas.)

- *Elementos de Álgebra*, A. Garcia e Y. Lequain, IMPA, 4ª edição, 2006.
- *Topics in Algebra*, I. N. Herstein, John Wiley & Sons, 2nd edition, 1975.
- *Algebra*, Thomas W. Hungerford, Springer-Verlag, 1974.

Subgrupo normal e o grupo quociente

Sejam $(G, \cdot)$ um grupo e H um subgrupo de G.

Lembramos que podemos definir uma relação de equivalência em G, usando o subgrupo H, a saber, a *congruência módulo* H.

Sejam $a, b \in G$. Dizemos que a é *congruente* a b módulo H se, e somente se, $a \cdot b^{-1} \in H$. Nesse caso, escrevemos $a \equiv b \mod H$.

A classe de equivalência de $a \in G$ é

$$\begin{aligned} \overline{a} &= \{x \in G \mid x \equiv a \mod H\} \\ &= \{x \in G \mid x \cdot a^{-1} \in H\} \\ &= \{x \in G \mid x \cdot a^{-1} = h \in H\} \\ &= \{x \in G \mid x = h \cdot a \text{ com } h \in H\} \\ &= Ha \end{aligned}$$

Ha é chamada de *classe à direita de* H e a é um *representante* da classe Ha.

Das propriedades de uma relação de equivalência, temos que:

$G = \bigcup_{a \in G} Ha$ e esta união é disjunta nas classes distintas, pois

$Ha \cap Hb \neq \emptyset \iff a \equiv b \mod H \iff a \cdot b^{-1} \in H \iff Ha = Hb.$

De maneira análoga, definimos a *classe à esquerda* de H como

$$aH = \{a \cdot h \mid h \in H\}.$$

Nesse caso, $aH = bH \iff b^{-1}a \in H$.

As funções

$$\varphi : H \longrightarrow Ha,\ h \longmapsto ha \quad \text{e} \quad \psi : H \longrightarrow aH,\ h \longmapsto ah$$

são bijeções, mostrando que as classes à direita e as classes à esquerda têm a mesma cardinalidade de H.

Chamamos de *índice de* H em G à cardinalidade das classes laterais de H em G e denotamos por $i_G(H) = (G : H)$.

Para determinar o índice de H em G, tanto faz tomar classes à direita ou classes à esquerda.

Exemplo 1

$(\mathbb{Z}, +)$ é, a menos de isomorfismo, o único grupo cíclico infinito.

Os subgrupos de $\mathbb{Z}$ são $H_n = n\mathbb{Z}$, para $n \in \mathbb{N}$.

Seja $n \geq 1$. Então, $(\mathbb{Z} : n\mathbb{Z}) = n$.

De fato, para cada $a \in \mathbb{Z}$, pela divisão euclidiana de a por n, temos que $a = n \cdot q + r$, onde $0 \leq r \leq n - 1$, com $q, r \in \mathbb{Z}$ unicamente determinados. Assim, $\overline{a} = n\mathbb{Z} + a = n\mathbb{Z} + (n \cdot q + r) = n\mathbb{Z} + r = \overline{r}$. Como $r \neq s$ e $0 \leq r, s \leq n-1$ se, e somente se, $\overline{r} \neq \overline{s}$ portanto, o número de classes à direita de $n\mathbb{Z}$ em $\mathbb{Z}$ é o número de restos na divisão por n, isto é, $(\mathbb{Z} : n\mathbb{Z}) = n$.

Quando G é um grupo finito, temos que $i_G(H) = (G : H)$ é finito e

$$| G | = \sum_{a \in G} | Ha | = i_G(H) \cdot | H |,$$

onde a soma acima é feita nas classes distintas, isto é, nas classes disjuntas.

Nesse caso, $i_G(H) = (G : H) = \dfrac{| G |}{| H |}$.

Exemplo 2

Seja S_3 o grupo das bijeções de um conjunto com 3 elementos, com a operação de composição de funções, a saber,

S_3 também é conhecido como o grupo diedral 3, das simetrias espaciais do triângulo equilátero.

$$S_3 = \{I, \sigma, \tau, \tau^2, \sigma \circ \tau, \sigma \circ \tau^2 \,;\, \sigma^2 = I, \tau^3 = I, \tau \circ \sigma = \sigma \circ \tau^2\},$$

onde I é a identidade, $\sigma = (2,3)$ e $\tau = (1,2,3)$ são, respectivamente, as bijeções

$$\begin{array}{rcl} I : \{1,2,3\} & \longrightarrow & \{1,2,3\} \\ 1 & \longmapsto & 1 \\ 2 & \longmapsto & 2 \\ 3 & \longmapsto & 3 \end{array} \quad , \quad \begin{array}{rcl} \sigma : \{1,2,3\} & \longrightarrow & \{1,2,3\} \\ 1 & \longmapsto & 1 \\ 2 & \longmapsto & 3 \\ 3 & \longmapsto & 2 \end{array} \quad \text{e}$$

$$\begin{array}{rcl} \tau : \{1,2,3\} & \longrightarrow & \{1,2,3\} \\ 1 & \longmapsto & 2 \\ 2 & \longmapsto & 3 \\ 3 & \longmapsto & 1 \end{array}$$

Verifique que $\tau^2 = (1,3,2)$, $\sigma \circ \tau = (1,3)$ e $\sigma \circ \tau^2 = (1,2)$.

Consideremos os subgrupos $H = < \sigma > = \{I, \sigma\}$ e $K = < \tau > = \{I, \tau, \tau^2\}$.

Temos $i_{S_3}(H) = \frac{6}{2} = 3$ e $i_{S_3}(K) = \frac{6}{3} = 2$.

Classes à direita de H em G	Classes à esquerda de H em G
$H = \{I, \sigma\}$	$H = \{I, \sigma\}$
$H\tau = \{\tau, \sigma \circ \tau\}$	$\tau H = \{\tau, \tau \circ \sigma\} = \{\tau, \sigma \circ \tau^2\}$
$H\tau^2 = \{\tau^2, \sigma \circ \tau^2\}$	$\tau^2 H = \{\tau^2, \tau^2 \circ \sigma\} = \{\tau^2, \sigma \circ \tau\}$

Nesse caso, nem toda classe à direita de H em S_3 é uma classe à esquerda de H em S_3.

Classes à direita de K em G	Classes à esquerda de K em G
$K = \{I, \tau, \tau^2\}$	$K = \{I, \tau, \tau^2\}$
$K\sigma = \{\sigma, \tau \circ \sigma, \tau^2 \circ \sigma\} = \{\sigma, \sigma \circ \tau^2, \sigma \circ \tau\}$	$\sigma K = \{\sigma, \sigma \circ \tau, \sigma \circ \tau^2\}$

Nesse caso, cada classe à direita de K em S_3 é uma classe à esquerda de K em S_3.

Galois percebeu que os subgrupos, tais que toda classe à direita é uma classe à esquerda, deviam ser distinguidos dos demais subgrupos.

Definição 1 (Subgrupo normal)
Seja $(G, \cdot)$ um grupo. Um subgrupo N de G é um *subgrupo normal* de G se, e somente se, toda classe à direita de N em G é uma classe à esquerda de N em G. Escrevemos $N \lhd G$.

Exemplo 3
Seja $(G, \cdot)$ um grupo. Então, G e $\{e\}$ são subgrupos normais de G.

Quais são as classes do subgrupo $H = G$ no grupo G? Quais são as classes do subgrupo $H = \{e\}$ no grupo G?

Exemplo 4
O subgrupo $K = \{I, \tau, \tau^2\} = \langle\tau\rangle$ é um subgrupo normal de S_3.

O subgrupo $H = \{I, \sigma\} = \langle\sigma\rangle$ não é um subgrupo normal de S_3.

Exemplo 5
Se $(G, \cdot)$ é um grupo abeliano, então todo subgrupo é normal.

De fato, se H é um subgrupo de G e $a \in G$, então para qualquer $h \in H$ temos $ah = ha$, logo $aH = Ha$.

Exemplo 6
Seja $D_4 = \{S^i R^j \mid i = 0, 1;\ j = 0, 1, 2, 3;\ S^2 = I, R^4 = I, RS = SR^3\}$.

Seja $N = \langle R\rangle = \{I, R, R^2, R^3\}$. Então, N é um subgrupo normal de D_4.

Verifique!

Lema 1
Sejam $(G, \cdot)$ um grupo e N um subgrupo de G. N é um subgrupo normal de G se, e somente se, $aN = Na$, para cada $a \in G$.

Demonstração: Suponhamos que N seja um subgrupo normal de G e seja $a \in G$. Então, a classe à direita Na é uma classe à esquerda e como $a = a \cdot e \in aN$ temos que $Na = aN$. Reciprocamente, se $Na = aN$, para cada $a \in G$, então é óbvio que cada classe à direita de N em G é uma classe à esquerda. ■

Proposição 1
Sejam $(G, \cdot)$ um grupo e N um subgrupo de G. N é um subgrupo normal de G se, e somente se, $aNa^{-1} \subset N$, para cada $a \in G$.

Demonstração: Suponhamos que N seja um subgrupo normal de G. Pelo Lema anterior, temos que, para cada $a \in G$, $aN = Na$, logo $aNa^{-1} = N$, em particular, $aNa^{-1} \subset N$. Reciprocamente, suponhamos que, para cada $b \in G$, $bNb^{-1} \subset N$. Então,

Na primeira inclusão usamos que $a^{-1}Na \subset N$, fazendo $b = a^{-1}$.

$$N = (a \cdot a^{-1})N(a \cdot a^{-1}) = a(a^{-1}Na)a^{-1} \subset aNa^{-1} \subset N,$$

para cada $a \in G$.

Portanto, $aNa^{-1} = N$, para cada $a \in G$, isto é, $aN = Na$, para cada $a \in G$. Pelo Lema anterior, N é um subgrupo normal de G. ■

Com os subgrupos normais podemos dar ao conjunto quociente uma estrutura de grupo.

Proposição 2 (Grupo quociente)
Sejam $(G, \cdot)$ um grupo e N um subgrupo normal de G. O conjunto quociente $G/N = \{Na \,;\, a \in G\}$ é um grupo com a operação

$$Na \cdot Nb = Nab.$$

Mais ainda, $| G/N | = i_G(N)$ e se G é finito, então $| G/N | = \dfrac{| G |}{| N |}$.

Demonstração: Primeiramente, vamos mostrar que a operação independe dos representantes das classes.

De fato, se $Na = Nc$ e $Nb = Nd$, então $a \cdot c^{-1} = n_1 \in N$, assim como, $b \cdot d^{-1} = n_2 \in N$, logo

Na igualdade (1) usamos que $aN = Na$, assim, existe $n_3 \in N$ tal que $a \cdot n_2 = n_3 \cdot a$.

$$a \cdot b \cdot (c \cdot d)^{-1} = a \cdot (b \cdot d^{-1}) \cdot c^{-1} = (a \cdot n_2) \cdot c^{-1} \overset{(1)}{=} (n_3 \cdot a) \cdot c^{-1} = n_3 \cdot n_1 \in N,$$

mostrando que $Nab = Ncd$.

Agora vamos mostrar as propriedades da operação.

Sejam $a, b, c \in G$.

(i) (Associativa) $(Na \cdot Nb) \cdot Nc = Na \cdot (Nb \cdot Nc)$.

$$\begin{aligned}(Na \cdot Nb) \cdot Nc &= Nab \cdot Nc = N(ab)c \overset{(1)}{=} Na(bc) \\ &= Na \cdot Nbc = Na \cdot (Nb \cdot Nc)\end{aligned}.$$

Em todas as igualdades usamos a definição da operação em G/N, exceto em (1), onde usamos a associatividade da operação de G.

(ii) (Existência de elemento neutro) $N = Ne$ é o elemento neutro.

$$Ne \cdot Na = Na \cdot Ne = Na, \text{ para todo } Na \in G/N.$$

(iii) (Existência de inverso) O inverso de Na é Na^{-1}.

$$Na \cdot Na^{-1} = Na^{-1} \cdot Na = N. \qquad \blacksquare$$

Exemplo 7

Seja $K = \{I, \tau, \tau^2\}$. O grupo quociente $S_3/K = \{K, K\sigma\}$ é um grupo cíclico com 2 elementos gerado por $K\sigma$, pois $K\sigma \cdot K\sigma = K\sigma^2 = KI = K$.

$\sigma^2 = \sigma \circ \sigma = I$.

Exemplo 8

Seja $n \in \mathbb{N}$ tal que $n \geq 1$. Consideremos o subgrupo normal $n\mathbb{Z}$ de $\mathbb{Z}$. O grupo quociente é

$$\mathbb{Z}/n\mathbb{Z} = \{\, n\mathbb{Z}, n\mathbb{Z}+1, \ldots, n\mathbb{Z}+(n-1) \,\} = \{\, \overline{0}, \ldots, \overline{n-1} \,\},$$

onde $\overline{r} = n\mathbb{Z} + r$.

$\mathbb{Z}/n\mathbb{Z}$ também é denotado por $\mathbb{Z}_n$ e a operação do grupo quociente é a adição módulo n.

Nesse caso, apesar de $\mathbb{Z}$ ser um grupo infinito, o grupo quociente é finito, com $|\, \mathbb{Z}/n\mathbb{Z} \,| = n$.

Completamos agora os resultados sobre homomorfismos de grupos.

Sejam $(G, \cdot)$ e $(G', \star)$ grupos.

Lembramos que uma função $\varphi : G \longrightarrow G'$ é um homomorfismo de grupos se, e somente se, $\varphi(a \cdot b) = \varphi(a) \star \varphi(b)$, para quaisquer $a, b \in G$. Mais ainda, φ é injetor se, e somente se, $\text{Núcleo}(\varphi) = \{e_G\}$, onde

$$\text{Núcleo}(\varphi) = \{x \in G \,;\, \varphi(x) = e_{G'}\}.$$

Núcleo(φ) é um subgrupo de G.

Exemplo 9

Sejam $(G, \cdot)$ um grupo e N um subgrupo normal de G.

A função projeção $\pi : G \longrightarrow G/N$ definida, de maneira natural, por $\pi(a) = Na$ é um homomorfismo sobrejetor com $\text{Núcleo}(\pi) = N$.

Verifique!

Proposição 3 (Propriedade do núcleo)
Seja $\varphi : G \longrightarrow G'$ um homomorfismo do grupo $(G, \cdot)$ no grupo $(G', \star)$. Então, $N = \text{Núcleo}(\varphi)$ é um subgrupo normal de G.

Demonstração: Como $\varphi(e_G) = e_{G'}$, temos que $e_G \in N$. Além disso, se $a, b \in N$, então $\varphi(a \cdot b) = \varphi(a) \star \varphi(b) = e_{G'} \star e_{G'} = e_{G'}$ e $\varphi(a^{-1}) = (\varphi(a))^{-1} = e_{G'}^{-1} = e_{G'}$, logo $a \cdot b \in N$ e $a^{-1} \in N$, portanto N é um subgrupo de G. Agora precisamos mostrar que N é normal em G. De fato, se $a \in G$ e $n \in N$, então

$$\varphi(a \cdot n \cdot a^{-1}) = \varphi(a) \star \varphi(n) \star \varphi(a^{-1}) = \varphi(a) \star e_{G'} \star (\varphi(a))^{-1} = e_{G'},$$

mostrando que $a \cdot n \cdot a^{-1} \in N$, isto é, $aNa^{-1} \subset N$. Logo, $N \lhd G$. ■

Teorema 1 (Teorema Fundamental dos homomorfismos de grupos)
Sejam $(G, \cdot)$ e $(G', \star)$ grupos. Seja $\varphi : G \longrightarrow G'$ um homomorfismo de grupos sobrejetor com núcleo N. Então, existe um único isomorfismo de grupos $\overline{\varphi} : G/N \longrightarrow G'$, tal que $\varphi = \overline{\varphi} \circ \pi$, onde $\pi : G \longrightarrow G/N$ é o homomorfismo projeção definido por $\pi(a) = \overline{a} = Na$. Equivalentemente, dizemos que existe um único isomorfismo $\overline{\varphi} : G/N \longrightarrow G'$, tal que o seguinte diagrama é comutativo

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varphi}} & \\ G/N & & \end{array} \qquad\qquad \begin{array}{ccc} a & \xrightarrow{\varphi} & \varphi(a) \\ \downarrow & \nearrow_{\overline{\varphi}} & \\ \pi(a) = Na & & \end{array}$$

Demonstração: Devemos mostrar a existência e a unicidade do isomorfismo $\overline{\varphi}$. Primeiramente, vamos mostrar a unicidade. Suponhamos que exista um homomorfismo $\overline{\varphi} : G/N \longrightarrow G'$ tal que $\varphi = \overline{\varphi} \circ \pi$. Então,

$$\overline{\varphi}(Na) = \overline{\varphi}(\pi(a)) = (\overline{\varphi} \circ \pi)(a) = \varphi(a), \text{ para qualquer } Na \in G/N,$$

mostrando a unicidade do homomorfismo.

Definimos então $\overline{\varphi}(Na) = \varphi(a)$.

Primeiramente, precisamos mostrar que o valor de $\overline{\varphi}$ independe do representante da classe de G/N.

Vamos mostrar que $\overline{\varphi}$ é um isomorfismo de grupos. De fato, sejam $a, b \in G$ com $Na = Nb$. Então,

$$a \cdot b^{-1} \in N \text{ e } e_{G'} = \varphi(a \cdot b^{-1}) = \varphi(a) \star (\varphi(b))^{-1}.$$

Donde $\varphi(a) = \varphi(b)$, portanto $\overline{\varphi}(Na) = \overline{\varphi}(Nb)$ e $\overline{\varphi}$ está bem definida, isto é, $\overline{\varphi}$ é uma função. Além disso:

$$\overline{\varphi}(Na \cdot Nb) \overset{(1)}{=} \overline{\varphi}(Na \cdot b) \overset{(2)}{=} \varphi(a \cdot b) \overset{(3)}{=} \varphi(a) \star \varphi(b) \overset{(4)}{=} \overline{\varphi}(Na) \star \overline{\varphi}(Nb),$$

mostrando que $\overline{\varphi}$ é um homomorfismo de grupos.

Usamos em (1) a definição da operação em G/N; em (2) e (4), a definição de $\overline{\varphi}$ e em (3), o fato de φ ser homomorfismo.

Seja agora $Na \in G/N$ tal que $e_{G'} = \overline{\varphi}(Na) = \varphi(a)$. Então, $a \in N$, logo $Na = N$ e $\overline{\varphi}$ é injetor.

Como φ é sobrejetor, para cada $a' \in G'$ existe $a \in G$, tal que $a' = \varphi(a) = \overline{\varphi}(Na)$. Logo, existe $Na \in G/N$, tal que $a' = \overline{\varphi}(Na)$, mostrando que $\overline{\varphi}$ é sobrejetor. Portanto, $\overline{\varphi}$ é um isomorfismo de grupos.
■

Veremos agora uma aplicação muito interessante do grupo quociente.

Teorema 2 (Teorema de Cauchy para grupos abelianos)
Seja $(G, \cdot)$ um grupo abeliano finito. Se p é um natural primo que divide a ordem de G, então existe $a \in G$, $a \neq e$, tal que $a^p = e$.

Nesse caso, G tem elemento de ordem p.

Demonstração: A demonstração é por indução sobre a ordem de G.

Se $| G | = 1$, então $G = \{e\}$ e nada há a demonstrar.

Suponhamos o resultado válido para grupos T, com $1 \leq |T| < |G|$. Vamos mostrar que vale para G.

Se G não tem subgrupos diferentes de $\{e\}$ e G, então G é cíclico de ordem prima, o único divisor primo de $|G|$ é $|G|$ e G tem $|G| - 1$ elementos de ordem $|G|$.

Faça o Exercício 4 dessa Seção.

Podemos supor que G tenha subgrupo N, $N \neq \{e\}$ e $N \neq G$. Então, $1 < |N| < |G|$.

Seja p um natural primo tal que p divide $|G|$.

Se p divide $|N|$, como N é um grupo abeliano, por hipótese de indução, existe $a \in N \subset G$, tal que $a \neq e$ e $a^p = e$, e encontramos o elemento procurado.

N é subgrupo de G se, e somente se, N é um grupo com a operação de G.

Portanto, podemos supor que p não divida $|N|$. Consideremos o grupo quociente G/N. Como $|G/N| = \frac{|G|}{|N|}$, $p \mid |G|$ e $p \nmid |N|$, temos que p divide $|G/N|$ e $|G/N| < |G|$. Por hipótese de indução, existe $Nb \in G/N$, tal que $Nb \neq N$ e $(Nb)^p = N$.

Num grupo abeliano, todo subgrupo é normal. Também, se G é abeliano, então G/N é abeliano.

Assim, $b \notin N$. Entretanto, $N = (Nb)^p = Nb^p$, isto é, $b^p \in N$. Por Corolário do Teorema de Lagrange, $e = (b^p)^{|N|} = b^{p|N|} = (b^{|N|})^p$.

Seja $a = b^{|N|}$. Afirmamos que $a \neq e$.

De fato, suponhamos, por absurdo, que $b^{|N|} = e$. Como p é primo e não divide $|N|$, então $\text{mdc}(p, |N|) = 1$, logo existem $\alpha, \beta \in \mathbb{Z}$, tais que $1 = \alpha|N| + \beta p$. Então,

$$Nb = (Nb)^1 = (Nb)^{\alpha|N|+\beta p} = (Nb^{|N|})^\alpha \cdot (Nb^p)^\beta = N^\alpha \cdot N^\beta = N \cdot N = N,$$

contradizendo o fato de que $b \notin N$.

Concluímos então que $a = b^{|N|} \in G$ é o elemento procurado. ■

Exemplo 10

Todo grupo abeliano de ordem 6 é cíclico.

De fato, seja $(G, \cdot)$ um grupo abeliano com $|G| = 6 = 2 \cdot 3$. Pelo Teorema de Cauchy para grupos abelianos, existem $a, b \in G$, com $a \neq e$ e $b \neq e$, tais que $a^2 = e$ e $b^3 = e$. Afirmo que $c = a \cdot b$ tem ordem 6. É claro que $c^6 = (a \cdot b)^6 = a^6 \cdot b^6 = (a^2)^3 \cdot (b^3)^2 = e$. Por outro lado, seja $n \geq 1$, tal que $e = c^n = a^n \cdot b^n$. Então, $a^n = b^{-n} \in H \cap K$, onde $H = \langle a \rangle$ e $K = \langle b \rangle$. Pelo Teorema de Lagrange, $|H \cap K|$ divide $|H| = 2$ e $|H \cap K|$ divide $|K| = 3$, logo $|H \cap K| = 1$, que é equivalente a $H \cap K = \{e\}$. Portanto, $a^n = e$ e $b^n = e$. Logo, $2 = \circ(a)$ divide n e $3 = \circ(b)$ divide n, isto é, n é múltiplo do $\text{mmc}(2, 3) = 6$.

Quando $a \cdot b = b \cdot a$, temos que $(a \cdot b)^n = a^n \cdot b^n$, para todo $n \in \mathbb{Z}$.

Desse modo, o menor inteiro positivo tal que $c^n = e$ é 6, mostrando que $\circ(c) = 6$. Como $\langle c \rangle \subset G$ e $|\langle c \rangle| = |G| < \infty$, então $\langle c \rangle = G$ e G é cíclico.

Exercícios

1. Sejam a, b elementos do grupo abeliano $(G, \cdot)$.
   (a) Mostre que $(a \cdot b)^n = a^n \cdot b^n$, para todo $n \in \mathbb{Z}$.
   (b) Mostre que se $\circ(a) = m$, $\circ(b) = n$ e $\text{mdc}(n, m) = 1$, então $\circ(a \cdot b) = mn$.
   (c) Mostre que se $\circ(a) = m$ e $\circ(b) = n$, então existe $c \in G$ tal que $\circ(c) = \text{mmc}(m, n)$.

Escolha de modo conveniente $s, r > 0$ e tome $c = a^r \cdot b^s$.

2. Seja $(G, \cdot)$ um grupo com elemento neutro e.
   Mostre que se $x^2 = e$ para todo $x \in G$, então G é abeliano.

3. Seja $(G, \cdot)$ um grupo com $2n$ elementos, onde $n \geq 1$.
   Prove que existe $x \in G$, $x \neq e$, tal que $x^2 = e$, onde e é o elemento neutro.

4. Seja $G \neq \{e\}$ um grupo que só tem subgrupos triviais.

   Mostre que G é um grupo finito de ordem prima.

5. Seja H um subgrupo de um grupo $(G, \cdot)$. Definimos

$$C(H) = \{\, x \in G \;;\; x \cdot h = h \cdot x \;,\; \text{para todo } h \in H \,\}.$$

   Mostre que $C(H)$ é um subgrupo de G.

6. Mostre que se N e H são subgrupos normais de G, então $N \cap H$ é normal em G.

7. Mostre que se N e H são subgrupos de G e H é normal em G, então $H \cap N$ é um subgrupo normal de N.

   Dê um exemplo mostrando que $H \cap N$ pode não ser normal em G.

8. Mostre que se G é um grupo abeliano, então todo subgrupo de G é normal em G.

9. Seja G um grupo finito que tem um único subgrupo H com ordem de H elementos. Mostre que H é um subgrupo normal de G.

10. Se um subgrupo cíclico T de um grupo G é normal em G, então todo subgrupo de T é normal em G.

11. Seja $(G, \cdot)$ um grupo e H um subgrupo de G tal que $(G : H) = 2$. Mostre que H é normal em G.

12. Prove, usando um exemplo, que existem um grupo G e subgrupos E e F com $E \subset F \subset G$, onde E é normal em F, F é normal em G, mas E não é normal em G. Sugestão: Procure o exemplo em S_4.

13. Seja H um subgrupo de $(G, \cdot)$ e seja $N(H)$, o *normalizador* de H, definido por

$$N(H) = \{x \in G \;;\; xHx^{-1} = H\}.$$

    Mostre que:

    (a) $N(H)$ é um subgrupo de G, $H \subset N(H)$ e H é normal em $N(H)$.

    (b) Se H é um subgrupo normal de um subgrupo K de G, então $K \subset N(H)$. (Isto é, $N(H)$ é o maior subgrupo de G no qual H é normal.)

(c) H é um subgrupo normal de G se, e somente se, $N(H) = G$.

14. Seja $(G, \cdot)$ um grupo. O *centro* de G é o conjunto

$$Z(G) = \{x \in G \ ; \ gx = xg, \text{ para todo } g \in G\}.$$

Mostre que:

(a) $Z(G)$ é um subgrupo de G.

(b) $Z(G)$ é normal em G.

(c) Se H é um subgrupo de $Z(G)$, então H é um subgrupo normal de G.

15. Mostre que:

(a) $Z(S_3) = \{I\}$.

(b) $Z(D_4) = \{I, R^2\} = \langle R^2 \rangle$.

16. Seja K um corpo e $GL(n, K) = \{ A \in M_{n\times n}(K) \ ; \ A \text{ é invertível } \}$.

(a) Mostre que $GL(n, K)$ é um grupo com a operação de multiplicação de matrizes.

(b) Seja $SL(n, K) = \{ A \in GL(n, K) \ ; \ \det(A) = 1\}$.

Mostre que $SL(n, K)$ é um subgrupo normal de $GL(n, K)$.

17. Se N é um subgrupo normal de um grupo G e $a \in G$ tem ordem $\circ(a)$, mostre que $\circ(Na)$, a ordem de Na em G/N, divide $\circ(a)$.

18. Seja N um subgrupo normal de um grupo finito $(G, \cdot)$, tal que $|N|$ e $i_G(N) = (G : N)$ são primos entre si.

Mostre que se $x \in G$ e $x^{|N|} = e$, então $x \in N$.

19. Seja $(G, \cdot)$ um grupo tal que $(a \cdot b)^p = a^p \cdot b^p$, para quaisquer $a, b \in G$, onde p é um número natural primo.

Seja $S = \{ x \in G \ ; \ x^{p^m} = e \ , \text{ para algum } m \geq 1 \text{ dependendo de } x \}$.

(a) Mostre que S é um subgrupo normal de G.

(b) Mostre que se $\overline{G} = G/S$ e se $\overline{x} \in \overline{G}$ é tal que $\overline{x}^p = \overline{e}$, então $\overline{x} = \overline{e}$.

20. Seja $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} ; a, b, d \in \mathbb{R} \text{ e } ad \neq 0 \right\}$, com a operação de multiplicação de matrizes. Seja $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} ; b \in \mathbb{R} \right\}$.

    Mostre que N é um subgrupo normal de G e que G/N é abeliano.

21. Vendo $\mathbb{Z}$ como um subgrupo aditivo do grupo aditivo dos números racionais $\mathbb{Q}$, mostre que dado $\overline{x} \in \mathbb{Q}/\mathbb{Z}$ existe um inteiro $n \geq 1$, tal que $n\overline{x} = \overline{0}$.

22. Mostre que cada classe de $\mathbb{Z}$ em $\mathbb{R}$ tem um representante x, tal que $0 \leq x < 1$.

    Estamos olhando para o grupo aditivo $\mathbb{R}/\mathbb{Z}$.

23. Seja D o subgrupo de $\mathbb{R}$ gerado por 2π ($\mathbb{R}$ é um grupo aditivo). Seja $\mathbb{R}^+$ o grupo multiplicativo dos números reais positivos e seja $\mathbb{C}^*$ o grupo multiplicativo dos números complexos não-nulos.

    Mostre que $\varphi : \mathbb{R}^+ \times \mathbb{R}/D \longrightarrow \mathbb{C}^*$ definida por $\varphi(r, \overline{\theta}) = re^{i\theta}$ é um isomorfismo de grupos.

24. Mostre que cada classe de $\mathbb{R}^+$ em $\mathbb{C}^*$ tem um único representante complexo de valor absoluto 1.

    Estamos olhando para o grupo multiplicativo $\mathbb{C}^*/\mathbb{R}^+$.

25. Sejam $\varphi : G \longrightarrow G'$ um homomorfismo sobrejetor de grupos e $N = \text{núcleo}(\varphi)$. Mostre que:

    Sejam $f : A \longrightarrow B$ uma função e $C \subset B$. A imagem inversa de C por f é o subconjunto de A $f^{-1}(C) = \{x \in A; f(x) \in C\}$.

    (a) Se H é um subgrupo de G e $H \supset N$, então $\varphi(H)$ é um subgrupo de G' e $\varphi^{-1}(\varphi(H)) = H$.

    (b) Se H' é um subgrupo de G', então $\varphi^{-1}(H')$ é um subgrupo de G contendo N e $\varphi(\varphi^{-1}(H')) = H'$.

    (c) As aplicações

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{subgrupos de } G \\ \text{que contém } N \end{array} \right\} & \longrightarrow & \left\{ \text{subgrupos de } G' \right\} \\ H & \longmapsto & \varphi(H) \end{array} \quad \text{e}$$

$$\begin{array}{ccc} \left\{ \text{subgrupos de } G' \right\} & \longrightarrow & \left\{ \begin{array}{c} \text{subgrupos de } G \\ \text{que contém } N \end{array} \right\} \\ H' & \mapsto & \varphi^{-1}(H') \end{array}$$

    são bijeções e inversas uma da outra. Além disso, essas bijeções levam subgrupos normais em subgrupos normais, isto é:

i. Se $H \lhd G$, então $\varphi(H) \lhd G'$.

ii. Se $H' \lhd G'$, então $\varphi^{-1}(H') \lhd G$.

26. Seja N um subgrupo normal do grupo $(G, \cdot)$.

Seja $\pi : G \longrightarrow G/N$ o homomorfismo definido por $\pi(x) = Nx$.

Mostre que:

(a) Se H é um subgrupo de G e $H \supset N$, então

$$\overline{H} := \pi(H) = \{Nx \ ; \ x \in H\}$$

Observamos que $\overline{H} = H/N$.

é um subgrupo de G/N.

Além disso, se $H \lhd G$, então $\overline{H} \lhd G/N$.

(b) Se $\overline{H}$ é um subgrupo de G/N, então

$$H := \{x \in G \ ; \ Nx \in \overline{H}\}$$

é um subgrupo de G, $H \supset N$ e $\pi(H) = \overline{H}$.

Além disso, se $\overline{H} \lhd G/N$, então $H \lhd G$.

27. Sejam $m \geq 2$ e $n \geq 2$ inteiros tais que $\text{mdc}(m, n) = 1$. Seja

$$\begin{array}{rcl} \varphi : \mathbb{Z} & \longrightarrow & \mathbb{Z}_m \times \mathbb{Z}_n \\ x & \longmapsto & (\overline{x}, \overline{\overline{x}}), \end{array}$$

onde $\overline{x} = x \mod m$ e $\overline{\overline{x}} = x \mod n$.

(a) Mostre que φ é um homomorfismo sobrejetor de grupos.

(b) Mostre que Núcleo$(\varphi) = mn\mathbb{Z}$.

(c) Mostre que $\mathbb{Z}_m \times \mathbb{Z}_n$ é um grupo isomorfo a $\mathbb{Z}_{mn}$.

Um princípio de contagem

Pretendemos tentar entender um grupo finito, estudando-o a partir de seus subgrupos.

Como operando com elementos de certos subgrupos de um grupo finito podemos obter todos os elementos do grupo?

Com esse objetivo, vamos estudar um tipo especial de subconjunto que pode ser construído dentro de um grupo, usando dois dos seus subgrupos.

Definição 2
Sejam H e K subgrupos de um grupo $(G, \cdot)$. Definimos o subconjunto HK de G por

$$HK = \{ h \cdot k \,;\, h \in H,\ k \in K\}.$$

Observação: Em virtude de $e \in K$, temos que $H \subset HK \subset G$. Analogamente, como $e \in H$, temos que $K \subset HK \subset G$.

Exemplo 11
Para qualquer subgrupo H de um grupo $(G, \cdot)$, temos que $H \subset HH \subset H$, isto é, $H = HH$.

Da definição acima, $HH = \{h_1 h_2 \,;\, h_1, h_2 \in H\}$.

Exemplo 12
Consideremos os subgrupos $H = \{I, \sigma\}$, $K = \{I, \tau, \tau^2\}$ e $L = \{I, \sigma\tau\}$ do grupo $S_3 = \{I, \sigma, \tau, \tau^2, \sigma\tau, \sigma\tau^2 \,;\, \sigma^2 = I, \tau^3 = I, \tau\sigma = \sigma\tau^2\}$. Temos que:

$HL = \{I, \sigma\tau, \sigma, \sigma(\sigma\tau) = \tau\}$,

$LH = \{I, \sigma, \sigma\tau, (\sigma\tau)\sigma = \sigma(\tau\sigma) = \sigma(\sigma\tau^2) = \tau^2\}$,

$HK = \{I, \tau, \tau^2, \sigma, \sigma\tau, \sigma\tau^2\}$ e

$KH = \{I, \sigma, \tau, \tau\sigma = \sigma\tau^2, \tau^2, \tau^2\sigma = \sigma\tau\}$, onde $\tau^2\sigma = \tau(\tau\sigma) = \tau(\sigma\tau^2) = (\tau\sigma)\tau^2 = (\sigma\tau^2)\tau^2 = \sigma\tau$

Observamos que $HL \neq LH$ e nenhum desses subconjuntos é um subgrupo de S_3. Enquanto, $HK = KH = S_3$.

Quais são os subgrupos não-triviais de S_3? São 4. Determine-os.

É possível determinar o número de elementos do conjunto HK, quando ambos os subgrupos são finitos.

Proposição 4 (Um princípio de contagem)
Sejam H e K subgrupos finitos de um grupo $(G, \cdot)$. Então,

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Lembre que ...
$H \cap K$ é um subgrupo de G.

Demonstração: Primeiramente, observamos que para cada $u \in H \cap K$, temos $u^{-1} \in H \cap K$ e

$$hk = \underbrace{(hu)}_{\in H}\underbrace{(u^{-1}k)}_{\in K}, \text{ para quaisquer } h \in H \text{ e } k \in K.$$

Por outro lado, para $h, h_1 \in H$ e $k, k_1 \in K$, temos:

$$\begin{aligned} h \cdot k = h_1 \cdot k_1 &\iff {h_1}^{-1} \cdot h = k_1 \cdot k^{-1} \in H \cap K \\ &\iff \text{existe } u \in H \cap K, \text{ tal que } {h_1}^{-1} \cdot h = u \text{ e } k_1 \cdot k^{-1} = u \\ &\iff \text{existe } u \in H \cap K, \text{ tal que } h = h_1 \cdot u \text{ e } k = u^{-1} \cdot k_1. \end{aligned}$$

Portanto, vale a fórmula proposta. ■

R pode ser, geometricamente, identificado com a rotação de $\frac{\pi}{4}$ ou com a bijeção $(1,2,3,4)$.
S pode ser, geometricamente, identificado à simetria com respeito a uma diagonal do quadrado ou à bijeção $(1,3)(2,4)$.

Exemplo 13
Consideremos o grupo D_4, subgrupo de S_4, a saber,

$$D_4 = \{\, S^i R^j \,;\, i = 0,1;\, j = 0,1,2,3;\, S^2 = I,\, R^4 = I,\, RS = SR^3 \,\}.$$

Sejam $H = \langle S \rangle = \{I, S\}$, $N = \langle R \rangle = \{I, R, R^2, R^3\}$, $K = \langle R^2 \rangle = \{I, R^2\}$, $L = \{I, SR, R^2, SR^3\}$ e $M = \{I, SR\}$.
Determine o número de elementos dos subconjuntos HK, KH, HN, NH, NL, LN, HM, MH, NM e MN. Determine os subconjuntos e compare-os. Quais são subgrupos de D_4?

Considerando que sabemos contar os elementos do conjunto HK, se ambos são finitos, o interessante é quando o conjunto HK é um subgrupo de G. A seguinte proposição responde a essa questão.

Proposição 5
Sejam H e K subgrupos do grupo $(G, \cdot)$.

Cuidado! A igualdade ao lado é de conjuntos.

HK é um subgrupo de G se, e somente se, $HK = KH$.

Demonstração: Suponhamos que HK seja um subgrupo de G. Seja $x \in HK$. Então, $x^{-1} \in HK$, isto é, $x^{-1} = h \cdot k$, com $h \in H$ e $k \in K$. Assim, $x = (x^{-1})^{-1} = (h \cdot k)^{-1} = k^{-1} \cdot h^{-1} \in KH$, mostrando que $HK \subset KH$. Para todo $h \in H$ e $k \in K$, temos que $h^{-1} \in H$ e $k^{-1} \in K$. Portanto, $k \cdot h = (h^{-1} \cdot k^{-1})^{-1} \in HK$, nos dá que $KH \subset HK$.

Reciprocamente, suponhamos que $HK = KH$. Como $e \in H$ e $e \in K$, então $e = e \cdot e \in HK$. Sejam $h, h_1 \in H$, $k, k_1 \in K$, $x = h \cdot k \in HK$ e $y = h_1 \cdot k_1 \in HK$. Como $HK = KH$, então existem $h_2 \in H$ e $k_2 \in K$, tais que $k \cdot h_1 = h_2 \cdot k_2$. Assim,

$x \cdot y = (h \cdot k) \cdot (h_1 \cdot k_1) \overset{(1)}{=} h \cdot (k \cdot h_1) \cdot k_1 \overset{(2)}{=} h \cdot (h_2 \cdot k_2) \cdot k_1 \overset{(3)}{=} (h \cdot h_2) \cdot (k_2 \cdot k_1) \in HK.$

Em (1) e (3) usamos a associatividade da operação de G e em (2), a igualdade acima.

Além disso, $x^{-1} = (h \cdot k)^{-1} = k^{-1} \cdot h^{-1} \in KH = HK.$ ■

Corolário 1
Se H e K são subgrupos de um grupo abeliano $(G, \cdot)$, então HK é um subgrupo de G.

Exercícios

1. Sejam H e K subgrupos de um grupo finito $(G, \cdot)$, tais que $|H| > \sqrt{|G|}$ e $|K| > \sqrt{|G|}$. Mostre que $H \cap K \neq \{e\}$.

2. Seja $(G, \cdot)$ um grupo de ordem pq, onde p e q são primos com $p > q$. Mostre que G tem no máximo um subgrupo de ordem p.

3. Sejam N e H subgrupos de um grupo $(G, \cdot)$.

   Esse Exercício é muito importante. Vamos utilizar os resultados na Seção 4.

   (a) Mostre que se N ou H é normal em G, então NH é um subgrupo de G.

   (b) Sejam N e H subgrupos normais de G.

      i. Mostre que NH é um subgrupo normal de G.

      ii. Mostre que se $H \cap N = \{e\}$, então $hn = nh$, para quaisquer $h \in H$ e $n \in N$.

   (c) Sejam N e H subgrupos normais de G, tais que $N \cap H = \{e\}$. Mostre que $\varphi : N \times H \longrightarrow NH$ definida por $\varphi(n, h) = n \cdot h$ é um isomorfismo de grupos.

4. Seja $\varphi : G \longrightarrow G'$ um homomorfismo de grupos. Mostre que:

   (a) Se H é um subgrupo de G, então $\varphi(H)$ é um subgrupo de G' e $\varphi^{-1}(\varphi(H)) = HN$, onde $N = \text{núcleo}(\varphi)$.

   Sejam $f : A \longrightarrow B$ uma função e $C \subset B$. A imagem inversa de C por f é o subconjunto de A $f^{-1}(C) = \{x \in A; f(x) \in C\}$.

   (b) Se H' é um subgrupo de G', então $\varphi^{-1}(H')$ é um subgrupo de G contendo $N = \text{núcleo}(\varphi)$ e $\varphi(\varphi^{-1}(H')) = H' \cap \text{Imagem}(\varphi)$.

5. Seja $(G, \cdot)$ um grupo e sejam H e K subgrupos de G.

   Dados $x, y \in G$ definimos

   $$x \sim y \iff y = hxk, \text{ para algum } h \in H \text{ e para algum } k \in K.$$

Mostre que:

(a) $\sim$ é uma relação de equivalência em G.

(b) A classe de equivalência de cada $x \in G$ é o conjunto
$$HxK = \{\, hxk \,;\, h \in H \text{ e } k \in K \,\}.$$

(c) A função $f : HxK \longrightarrow H(xKx^{-1})$ é uma bijeção.

(d) Se G é um grupo finito, então o número de elementos de HxK é
$$|HxK| = \frac{|H||K|}{|H \cap (xKx^{-1})|}.$$

A equação de classe e aplicações

A relação de equivalência módulo H, onde H é um subgrupo de um grupo $(G, \cdot)$ permite visualisar G por meio das classes à direita de H em G, a saber, os subconjuntos Ha, onde $a \in G$. Desse modo, obtivemos o belo Teorema de Lagrange para grupos finitos: $|H|$ divide $|G|$.

Agora, vamos usar uma outra relação de equivalência no grupo G, para fazer a contagem de seus elementos de maneira diferente.

Definição 3 (Conjugação)
Sejam $(G, \cdot)$ um grupo e $a, b \in G$. Dizemos que b é *conjugado* de a se, e somente se, existe $x \in G$ tal que $b = x^{-1}ax$. Escrevemos $b \sim a$ e chamamos $\sim$ de *conjugação*.

Proposição 6
A conjugação é uma relação de equivalência em $(G, \cdot)$.

Demonstração: Como $a = eae$, temos que $a \sim a$. Se $b \sim a$, então existe $x \in G$ tal que $b = x^{-1}ax$, logo $a = xbx^{-1} = (x^{-1})^{-1}bx^{-1}$, com $x^{-1} \in G$, mostrando que $a \sim b$. Finalmente, suponhamos que $a \sim b$ e $b \sim c$. Então, existem $x, y \in G$, tais que $a = x^{-1}bx$ e $b = y^{-1}cy$, logo $a = x^{-1}(y^{-1}cy)x = (yx)^{-1}c(yx)$, mostrando que $a \sim c$. ■

Definição 4 (Classe de conjugação)
Seja $(G, \cdot)$ um grupo e $\sim$ a conjugação. Para cada $a \in G$ definimos a *classe de conjugação de* a por

$$C(a) = \{b \in G \,;\, b \sim a\} = \{x^{-1}ax \,;\, x \in G\}.$$

Exemplo 14
Em qualquer grupo $(G, \cdot)$, temos que $C(e) = \{e\}$.

Exemplo 15
Se $(G, \cdot)$ é um grupo abeliano, então $C(a) = \{a\}$, para todo $a \in G$.

Observação: Como a conjugação é uma relação de equivalência em G, temos que:

(i) $C(a) \cap C(b) \neq \emptyset \iff C(a) = C(b) \iff a \sim b$;

(ii) $G = \bigcup C(a)$.

Portanto, esta união é disjunta nas classes distintas.

Corolário 2
Seja $(G, \cdot)$ um grupo finito e $\sim$ a conjugação. Seja $c_a = |C(a)|$. Então,

$$|G| = \sum c_a, \text{ onde a soma é feita nas classes distintas.}$$

Demonstração: É imediata, a partir da observação acima. ■

A conjugação desempenha um papel muito importante, quando o grupo é finito e, obviamente, não-abeliano.

O nosso objetivo será determinar c_a.

Definição 5 (Normalizador de um elemento)
Seja $(G, \cdot)$ um grupo. Seja $a \in G$. O *normalizador* de a é o conjunto

O normalizador de a é o conjunto dos elementos do grupo que comutam com a.

$$N(a) = \{x \in G \,;\, ax = xa\}.$$

Exemplo 16
Em qualquer grupo $(G, \cdot)$, temos que:
$N(e) = G$;
$\langle a \rangle \subset N(a)$.

Exemplo 17
Se $(G, \cdot)$ é um grupo abeliano, então $N(a) = G$, para todo $a \in G$.

Exemplo 18
Seja $(G, \cdot)$ um grupo não-abeliano.
Então, existem $a, b \in G$ tais que $ab \neq ba$. Logo, $b \notin N(a)$ e $N(a) \subsetneq G$.

Proposição 7
Seja $(G, \cdot)$ um grupo. $N(a)$ é um subgrupo de G, para todo $a \in G$.
Demonstração: É claro que $e \in N(a)$.

Para cada $x \in N(a)$, temos que $ax = xa$, logo

$$ax^{-1} = (x^{-1}x)(ax^{-1}) = x^{-1}(xa)x^{-1} = x^{-1}(ax)x^{-1} = (x^{-1}a)(xx^{-1}) = x^{-1}a,$$

mostrando que $x^{-1} \in N(a)$.

Sejam agora $x, y \in N(a)$. Então, $ax = xa$, $ay = ya$ e

$$a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a,$$

mostrando que $xy \in N(a)$. ■

Agora podemos determinar $c_a = |C(a)|$, para cada a em um grupo finito.

Teorema 3
Seja $(G, \cdot)$ um grupo finito. Então, para cada $a \in G$,

$$c_a = \frac{|G|}{|N(a)|} = (G : N(a)) = i_G(N(a)).$$

Demonstração: Vamos construir uma bijeção entre o conjunto das classes à direita de $N(a)$ em G e o conjunto $C(a)$, a classe de conjugação de a, mostrando que têm o mesmo número de elementos, isto é, $(G : N(a)) = c_a$.

Seja $f : \{N(a)x \ ; \ x \in G\} \longrightarrow C(a) = \{x^{-1}ax \ ; \ x \in G\}$ definida por $f(N(a)x) = x^{-1}ax$. Primeiramente, vamos verificar que f é uma função, isto é, f independe do representante da classe à direita. De fato, sejam $x, y \in G$:

$$\begin{array}{lll} N(a)x = N(a)y & \text{se, e somente se,} & xy^{-1} \in N(a) \\ & \text{se, e somente se,} & (xy^{-1})a = a(xy^{-1}) \\ & \text{se, e somente se,} & y^{-1}ay = x^{-1}ax, \end{array}$$

Multiplicamos à esquerda da igualdade por x^{-1} e à direita por y.

mostrando também que f é injetora.

Além disso, pela definição do contradomínio de f, temos que f é sobrejetora. Portanto, f é uma bijeção. ■

Corolário 3 (Equação de classe)
Seja $(G, \cdot)$ um grupo finito. Então,

$$|G| = \sum \frac{|G|}{|N(a)|},$$

onde a soma é feita nas classes de conjugação distintas.

Demonstração: Pelo Corolário 2 e pelo Teorema anterior, temos:

$$|G| = \sum c_a = \sum \frac{|G|}{|N(a)|},$$

onde a primeira soma é feita nas classes de conjugação distintas. ■

Com o objetivo de ver algumas aplicações belíssimas da Equação de classe, introduzimos o conceito de centro de um grupo.

Definição 6 (Centro de um grupo)
Seja $(G, \cdot)$ um grupo. O *centro* de G é o conjunto

$$Z(G) = \{x \in G \; ; \; xa = ax, \text{ para todo } a \in G\}.$$

Observação: $Z(G)$ é um subgrupo de G e é claro que, para qualquer $a \in G$, $Z(G) \subset N(a) \subset G$.

Veja Exercício 14 da Seção 1.

Proposição 8
Seja $(G, \cdot)$ um grupo e seja $a \in G$. Então, $a \in Z(G)$ se, e somente se, $N(a) = G$. Se G é um grupo finito, então $a \in Z(G)$ se, e somente se, $|N(a)| = |G|$.

Demonstração:

$$\begin{aligned} a \in Z(G) &\iff ax = xa, \text{ para todo } x \in G \\ &\iff \text{para todo } x \in G,\ x \in N(a) \\ &\iff G \subset N(a) \\ &\iff G = N(a). \end{aligned}$$

A última equivalência segue do fato de $N(a) \subset G$.

A última afirmação é óbvia. ■

No estudo dos grupos finitos, conforme veremos com o Teorema de Sylow, desempenham um papel muito importante os seus subgrupos cuja ordem são da forma p^n, para algum primo p que divide a ordem do grupo, motivando a seguinte definição.

Definição 7 (p-grupos finitos)
Seja p um natural primo. Um grupo finito $(G, \cdot)$ é chamado um p-*grupo* se, e somente se, $|G| = p^n$, para algum $n \in \mathbb{N}$.

Exemplo 19
Sabemos que os grupos de ordem 4, a menos de isomorfismo, são $\mathbb{Z}_4$ ou $\mathbb{Z}_2 \times \mathbb{Z}_2$, isto é, os grupos de ordem 4 são o cíclico de ordem 4 ou o grupo de Klein, ambos grupos abelianos.

Modelos multiplicativos para os grupos de ordem 4 são:

(i) As raízes complexas da unidade: $\{1, -1, i, -i\} = \langle i \rangle$.

(ii) Os invertíveis do anel $\mathbb{Z}_8$: $\mathbb{Z}_8^\star = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

Os grupos de ordem 2^2 são abelianos, conforme foi visto num Curso elementar de grupos. Como uma aplicação da Equação de classe, vamos generalizar esse resultado.

Teorema 4 (Centro de p-grupos)
Se $(G, \cdot)$ é um grupo tal que $|G| = p^n$, onde p é um natural primo e $n \geq 1$, então $Z(G) \neq \{e\}$.

Demonstração: Seja $a \in G$. Como $N(a)$ é um subgrupo de G, pelo Teorema de Lagrange, $|N(a)|$ divide $|G|$, logo $|N(a)| = p^{n_a}$, onde $0 \leq n_a \leq n$. Pela Proposição anterior, $a \in Z(G)$ se, e somente se, $n_a = n$. Seja $z = |Z(G)|$. Consideremos a Equação de classe de G.

$$\begin{aligned} |G| &= \sum \frac{|G|}{|N(a)|}, \text{ onde a soma é nas classes de conjugação distintas,} \\ p^n &= \sum_{n_a = n} \frac{|G|}{|N(a)|} + \sum_{n_a < n} \frac{|G|}{|N(a)|} \\ p^n &= z + \sum_{n_a < n} \underbrace{\frac{|G|}{|N(a)|}}_{\text{p divide}} \end{aligned}$$

A classe de conjugação de $a \in Z(G)$ é o conjunto unitário $\{a\}$. Então, há z elementos com $n_a = n$.

Como p divide p^n e divide cada parcela do tipo p^{n-n_a}, com $n_a < n$, obtemos que p divide z. Logo, $z \geq p$ e $Z(G) \neq \{e\}$. ■

Corolário 4 (Grupos de ordem p^2)
Se $(G, \cdot)$ é um grupo de ordem p^2, onde p é primo, então G é abeliano.

Demonstração: G é abeliano se, e somente se, $G = Z(G)$. Vamos mostrar que $|Z(G)| = p^2$.

Como $Z(G) \neq \{e\}$ é um subgrupo, pelo Teorema de Lagrange, $|Z(G)| = p$ ou $|Z(G)| = p^2$. Suponhamos, por absurdo, que $|Z(G)| = p$. Então, existe $a \in G$, tal que $a \notin Z(G)$. Logo, $Z(G) \subsetneq N(a)$. Pela Proposição 8, temos que $N(a) \subsetneq G$. Assim, $p = |Z(G)| < |N(a)| < |G| = p^2$, contradizendo o Teorema de Lagrange. ■

Faça agora os Exercícios 5 e 6 dessa Seção.

A seguir, a segunda aplicação da Equação de classe de um grupo finito.

Você vai classificar os grupos de ordem p^2.

Teorema 5 (Teorema de Cauchy)
Seja $(G, \cdot)$ um grupo finito. Se p é um natural primo e divide a ordem de G, então G tem um elemento de ordem p.

Demonstração: Procuramos um elemento $a \in G$, $a \neq e$, tal que $a^p = e$. A demonstração será feita por indução sobre a ordem de G.

Se $|G| = 1$, nada há a demonstrar. Suponhamos o resultado válido para os grupos G' com $1 \leq |G'| < |G|$. Vamos mostrar que vale para G.

Suponhamos que os únicos subgrupos de G sejam os triviais, isto é, G e $\{e\}$. Pelo Exercício 4 da Seção 1, G é cíclico de ordem prima e o primo tem que ser p. Nesse caso, qualquer $a \in G$, $a \neq e$, tem ordem p.

Podemos supor que G tem subgrupo não-trivial. Consideraremos dois casos.

Caso 1: Existe subgrupo não-trivial de G, digamos H, tal que p divide $|H|$.

Nesse caso, $1 < |H| < |G|$ e, pela hipótese de indução, existe $a \in H$, $a \neq e$, tal que $a^p = e$, e a é o elemento de G procurado.

Caso 2: Para qualquer subgrupo não-trivial H de G, p não divide $|H|$.

Se $a \neq e$, então $\{e\} \subsetneq N(a)$, pois $\{e, a\} \subset \langle a \rangle \subset N(a)$.

Nesse caso, sempre que $a \notin Z(G)$, temos $\{e\} \subsetneq N(a) \subsetneq G$ e p não divide $|N(a)|$. Escrevendo a Equação de classe de G, temos:

$$
\begin{aligned}
|G| &= \sum \frac{|G|}{|N(a)|}, \text{ onde a soma é nas classes de conjugação distintas,} \\
|G| &= \sum_{N(a)=G} \frac{|G|}{|N(a)|} + \sum_{N(a)\neq G} \frac{|G|}{|N(a)|} \\
\underbrace{|G|}_{p \text{ divide}} &= |Z(G)| + \underbrace{\sum_{N(a)\neq G} \underbrace{\frac{|G|}{|N(a)|}}_{p \text{ divide}}}_{p \text{ divide}}
\end{aligned}
$$

$N(a) = G \iff a \in Z(G)$. Há $|Z(G)|$ classes de conjugação distintas com $C(a) = \{a\}$.

Como p divide $|G|$ e p não divide $|N(a)|$, quando $\{e\} \subsetneq N(a) \subsetneq G$, então p divide cada parcela da direita do tipo $\dfrac{|G|}{|N(a)|}$. Logo, p divide $|Z(G)|$. Por hipótese, p não divide a ordem dos subgrupos próprios de G, então concluímos que $Z(G) = G$ e G é abeliano. Pelo Teorema de Cauchy para grupos abelianos, G tem elemento de ordem p. ■

Exercícios

1. Liste todas as classes de conjugação $C(a)$, para $a \in S_3$, determine $c_a = |\, C(a)\,|$ e verifique a equação de classe em S_3.

2. Liste todas as classes de conjugação $C(a)$ no grupo dos quatérnios, determine $c_a = |\, C(a)\,|$ e verifique a equação de classe.

3. Se em um grupo finito G a classe de conjugação de um elemento a tem exatamente 2 elementos, prove que G tem um subgrupo normal N, tal que $N \neq \{e\}$ e $N \neq G$.

4. Sejam $(G, \cdot)$ um grupo e $Z(G)$ seu centro. Mostre que se $G/Z(G)$ é cíclico, então G é abeliano.

5. Seja $(G, \cdot)$ um grupo não-cíclico de ordem p^2.

   (a) Mostre que existem subgrupos H e K de G, com $|H| = p$ e $|K| = p$, tais que $H \cap K = \{e\}$ e cada $a \in G$ se escreve de uma única maneira como $a = hk$.

   (b) Mostre que $\varphi : H \times K \longrightarrow G$ definida por $\varphi((h, k)) = hk$ é um isomorfismo de grupos.

   (c) Mostre que G é isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$.

6. Seja p um natural primo. Mostre que, a menos de isomorfismo, só há dois grupos de ordem p^2, a saber, $\mathbb{Z}_{p^2}$ e $\mathbb{Z}_p \times \mathbb{Z}_p$.

Neste Exercício você vai classificar os grupos de ordem p^2.

7. Seja $(G, \cdot)$ um grupo não-abeliano de ordem p^3, onde p é primo.

   Mostre que $| Z(G) | = p$ e $G/Z(G)$ é isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$.

8. Seja G um grupo de ordem p^m e seja H um subgrupo de G de ordem p^n, onde $n < m$.

   Mostre que existe um subgrupo K de G tal que $H \lhd K$ e $| K | = p^{n+1}$.

   Sugestão: Escolha $x \in Z(G)$, com $\circ(x) = p$. Considere $H < x >$ e os casos $x \in H$ ou $x \notin H$.

9. Seja G um grupo de ordem p^m, p primo. Mostre que existem subgrupos N_i, $i = 0, \ldots, r$, para algum r, tais que

$$G = N_0 \supset N_1 \supset \cdots \supset N_r = \{e\},$$

   onde $N_i \lhd N_{i-1}$ e N_{i-1}/N_i é cíclico de ordem p.

Neste Exercício, você vai continuar a aprender alguns resultados importantes sobre os p-grupos finitos.

10. Seja $(G, \cdot)$ um grupo com $|G| = p^n$, onde p é um primo e $n \geq 1$.

    (a) Mostre que G tem subgrupos de ordem p^α, para $0 \leq \alpha \leq n$.
    Sugestão: indução sobre n e passagem ao quociente para diminuir o número de elementos.

    (b) Seja $H \neq G$ um subgrupo de G. Mostre que existe $x \in G$, $x \notin H$, tal que $xHx^{-1} = H$.
    Sugestão: indução sobre n ($2^{\underline{a}}$ forma) e passagem ao quociente para diminuir o número de elementos, considerando os seguintes casos: $K \not\subset H$ e $K \subset H$, onde $K = \langle a \rangle$, $a \in Z(G)$ e $\circ(a) = p$.

Lembre que $Z(G) \neq \{e\}$ e, pelo Teorema de Cauchy, $Z(G)$ tem subgrupo K com $|K| = p$ e $K \lhd G$.

(c) Mostre que qualquer subgrupo de G de ordem p^{n-1} é normal em G.

Sugestão: use o item anterior, tomando o normalizador do subgrupo.

Teorema de Sylow

Vamos agora nos dedicar a demonstrar o Teorema de Sylow, que garante a existência de subgrupos de um grupo finito com ordens especiais.

Definição 8 (p-Sylow subgrupo)
Seja $(G,\cdot)$ um grupo finito. Seja p um natural primo. Um subgrupo H de G é chamado um p-*Sylow subgrupo de* G se, e somente se, $|H| = p^m$, onde p^m divide $|G|$, mas p^{m+1} não divide $|G|$.

p^m é a maior potência de p que divide $|G|$.

Exemplo 20
Em $(S_3,\circ)$, $H = \langle\sigma\rangle$ é um 2-Sylow subgrupo de S_3 e $K = \langle\tau\rangle$ é um 3-Sylow subgrupo de S_3.

Observamos que $\{I, \sigma\tau\}$ e $\{I, \sigma\tau^2\}$ são os outros 2-Sylow's subgrupos de S_3, enquanto K é o único 3-Sylow subgrupo de S_3.

Exemplo 21
Seja $(G,\cdot)$ um grupo cíclico de ordem 10 gerado por a. Então, $H = \langle a^5\rangle$ é o único 2-Sylow subgrupo de G e $N = \langle a^2\rangle$ é o único 5-Sylow subgrupo.

Porque há um único 2-Sylow subgrupo e um único 5-Sylow subgrupo?

Teorema 6 (Teorema de Sylow)
Seja $(G,\cdot)$ um grupo finito. Seja p um natural primo, tal que $p^m \mid |G|$ e $p^{m+1} \nmid |G|$. Então,

(i) G tem subgrupo de ordem p^m.

(ii) Os p-Sylow subgrupos de G são conjugados, isto é, se H e K são p-Sylow subgrupos de G, então existe $a \in G$ tal que $K = a^{-1}Ha$.

Além disso, o número n_p de p-Sylow subgrupos de G é $n_p = \dfrac{|G|}{|N(P)|}$, onde P é qualquer p-Sylow subgrupo. Em particular, n_p divide $|G|$.

(iii) $n_p \equiv 1 \mod p$.

Para o melhor entendimento dividimos a demonstração do Teorema de Sylow em três etapas, uma para cada item.

Teorema 7 (Teorema de Sylow-1ª Parte)
Seja $(G,\cdot)$ um grupo finito.
Seja p um natural primo tal que $p^m \mid |G|$ e $p^{m+1} \nmid |G|$. Então, G tem subgrupo de ordem p^m.

Demonstração: A demonstração será feita por indução sobre $|G|$.

Se $|G| = 1$, então o resultado é trivialmente verdadeiro.

Suponhamos o resultado válido para os grupos com ordem menor do que $|G|$, com $|G| > 1$. Vamos mostrar que vale para G.

Se G tem algum subgrupo $H \subsetneq G$ tal que p^m divide $|H|$ e $p^{m+1} \nmid |H|$, por hipótese de indução, H tem subgrupo de ordem p^m e esse subgrupo é o subgrupo de G procurado.

Portanto, podemos supor que p^m não divide a ordem dos subgrupos próprios de G. Note que, nesse caso, $m \geq 1$.

Lembre que ...
$N(a) \neq G$ sempre que $a \in G$ e $a \notin Z(G)$.

Pela Equação de classe de G, temos que:

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} \frac{|G|}{|N(a)|},$$

onde a soma é nas classes de conjugação distintas.

Como, para todo $a \notin Z(G)$, $p^m \mid |G|$ e $p^m \nmid |N(a)|$, então p divide $\dfrac{|G|}{|N(a)|}$ e logo, p divide $|Z(G)|$.

Pelo Teorema de Cauchy, existe $b \in Z(G)$, tal que $b \neq e$ e $b^p = e$. Seja $N = \langle b \rangle$, o subgrupo de G gerado por b. Temos que:

(1) $|N| = p$;

(2) N é subgrupo normal de G pois, $b \in Z(G)$ e para todo $g \in G$,

$$g^{-1}bg = g^{-1}gb = b,$$

nos dá que

$$g^{-1}b^r g = \underbrace{(g^{-1}bg)(g^{-1}bg)\cdots(g^{-1}bg)}_{r \text{ fatores}} = b^r \subset N, \text{ para todo } r \in \mathbb{N}.$$

Podemos, então, considerar o grupo quociente G/N, com $|G/N| = \dfrac{|G|}{|N|} = \dfrac{|G|}{p} < |G|$.

Como $p^m \mid |G|$ e $p^{m+1} \nmid |G|$, temos que $p^{m-1} \mid |G/N|$ e $p^m \nmid |G/N|$. Por hipótese de indução, G/N tem um subgrupo $\overline{H}$ com $|\overline{H}| = p^{m-1}$.

$G/N = \{Nx\,;\, x \in G\}$, N é o elemento neutro de G/N e $\pi : G \longrightarrow G/N$, $x \longmapsto Nx$. é homomorfismo sobrejetor de grupos.
Fez o Exercício 26 da Seção 1?

Seja $H = \{x \in G\,;\, Nx \in \overline{H}\}$. Afirmamos que H é um subgrupo de G, $N \subset H$ e $\pi(H) = \overline{H}$, isto é, $\overline{H} = \{Nx\,;\, x \in H\} = H/N$, onde $\pi : G \longrightarrow G/N$ é definida por $\pi(x) = Nx$.

De fato, se $x \in N$, então $Nx = N \in \overline{H}$ logo, pela definição de H, temos que $x \in H$, mostrando que $N \subset H$.

Sejam $x, y \in H$. Por definição de H, temos que $Nx, Ny \in \overline{H}$. Como $\overline{H}$ é um subgrupo de G/N, então $N(xy) = NxNy \in \overline{H}$ e $Nx^{-1} = (Nx)^{-1} \in \overline{H}$, mostrando que $xy \in H$ e $x^{-1} \in H$.

Assim, $p^{m-1} = |\overline{H}| = |H/N| = \dfrac{|H|}{p}$, isto é, $|H| = p^m$.

Logo, H é o p-Sylow subgrupo de G procurado. ■

Para demonstrar a 2ª e 3ª partes do Teorema de Sylow, precisamos da relação de equivalência no grupo $(G, \cdot)$ do Exercício 5 da Seção 2, além do conceito de normalizador de um subgrupo.

Definição 9 (Relação dupla de H e K em $(G, \cdot)$)
Sejam H e K subgrupos de um grupo $(G, \cdot)$. Sejam $x, y \in G$. Dizemos que $x \sim y$ se, e somente se, existem $h \in H$ e $k \in K$ tais que $y = hxk$.

Lema 2
A relação $\sim$ é uma relação de equivalência em G.
Demonstração: Faça o Exercício 5 da Seção 2.

Definição 10 (Classe dupla de H e K no grupo $(G, \cdot)$)
Para cada $x \in G$, a classe de equivalência de x na relação $\sim$ acima é chamada de *classe dupla de* H e K em G e é o subconjunto de G

$$HxK = \{hxk\ ;\ h \in H \text{ e } k \in K\}.$$

Observação: Se H e K são subgrupos finitos de $(G, \cdot)$, então

$$|HxK| = \frac{|H||K|}{|H \cap (xKx^{-1})|}.$$

De fato, $|HxK| = |H(xKx^{-1})|$, pois a função $f : HxK \longrightarrow H(xKx^{-1})$ definida por $f(hxk) = hxkx^{-1}$ é uma bijeção . Além disso, xKx^{-1} é um subgrupo de G, subgrupo conjugado de K, com $|xKx^{-1}| = |K|$ e

$$|H(xKx^{-1})| \overset{(1)}{=} \frac{|H||xKx^{-1}|}{|H \cap (xKx^{-1})|} = \frac{|H||K|}{|H \cap (xKx^{-1})|}.$$

A igualdade (1) segue da Proposição 4 da Seção 2.

Teorema 8 (Teorema de Sylow-2ª Parte)
Seja $(G, \cdot)$ um grupo finito. Seja p um natural primo, tal que $p^m \mid |G|$ e $p^{m+1} \nmid |G|$. Então, quaisquer dois p-Sylow subgrupos de G são conjugados em G.

Demonstração: Sejam H e K dois p-Sylow subgrupos de G, isto é, de ordens p^m. Queremos mostrar que existe $a \in G$, tal que $H = aKa^{-1}$. Decompondo G nas classes duplas HxK temos:

(1) $G = \bigcup HxK$, onde a união é feita nas classes duplas distintas (disjuntas);

(2) $|G| = \sum |HxK|$, onde a soma é feita nas classes duplas distintas.

$H \cap (xKx^{-1}) \subsetneq H$, pois $|H| = |K| = |xKx^{-1}|$ e $H \neq xKx^{-1}$. $H \cap (xKx^{-1})$ é subgrupo próprio de H e, pelo Teorema de Lagrange, $|H \cap (xKx^{-1})|$ divide $|H|$.

Suponhamos, por absurdo, que $H \neq xKx^{-1}$, para todo $x \in G$. Então, $|H \cap (xKx^{-1})| = p^n$, para algum n, tal que $0 \leq n < m$; assim,

$$|HxK| = \frac{|H| \cdot |K|}{|H \cap (xKx^{-1})|} = \frac{p^m \cdot p^m}{p^n} = p^{2m-n} \text{ e } 2m-n = m+(m-n) \geq m+1,$$

logo, p^{m+1} divide $|HxK|$, para todo $x \in G$. De (2), obtemos que p^{m+1} divide $|G|$, uma contradição com a hipótese.

Portanto, existe $a \in G$ tal que $H = aKa^{-1}$. ■

Definição 11 (Normalizador de H)
Seja H um subgrupo de $(G, \cdot)$. O *normalizador* de H é o conjunto

$$N(H) = \{x \in G; x^{-1}Hx = H\}.$$

Proposição 9 (Propriedades do normalizador de H)
Seja H um subgrupo de $(G, \cdot)$. Então,

(i) $N(H)$ é um subgrupo de G;
(ii) $H \subset N(H)$ e $H \lhd N(H)$;
(iii) se K é um subgrupo de G e H é normal em K, então $K \subset N(H)$.

Demonstração: Você já devia ter feito o Exercício 13 da Seção 1.

Observação:

(1) H é um subgrupo normal de G se, e somente se, $N(H) = G$.

(2) A condição (iii) da Proposição acima significa que $N(H)$ é o maior subgrupo de G, tal que H é normal.

Exemplo 22
Se $(G, \cdot)$ for um grupo abeliano, então $N(H) = G$, para qualquer subgrupo H de G.

Teorema 9 (Teorema de Sylow-2ª Parte, continuação)
Seja $(G, \cdot)$ um grupo finito. Seja p um natural primo, tal que $p^m \mid |G|$ e $p^{m+1} \nmid |G|$. Então, o número n_p de p-Sylow subgrupos de G é

$$n_p = \frac{|G|}{|N(P)|} = (G : N(P)), \text{ onde P é qualquer } p\text{-Sylow subgrupo de G.}$$

Em particular, n_p divide $|G|$.

Demonstração: Seja P um p-Sylow subgrupo de G. Como qualquer p-Sylow subgrupo de G é conjugado de P, então o número n_p de p-Sylow subgrupos é dado pelo número de subgrupos conjugados de P em G distintos, a saber, $x^{-1}Px$, com $x \in G$. Sejam $x, y \in G$. Temos que:

$$\begin{aligned} x^{-1}Px = y^{-1}Py &\iff yx^{-1}Pxy^{-1} = P \\ &\iff (xy^{-1})^{-1}P(xy^{-1}) = P \\ &\iff xy^{-1} \in N(P) \\ &\iff N(P)x = N(P)y \\ &\iff x \text{ e } y \text{ estão na mesma classe à direita de } N(P) \text{ em } G. \end{aligned}$$

Logo, n_p é o número de classes à direita distintas de $N(P)$ em G, isto é, o índice de $N(P)$ em G, seguindo o resultado. ■

Teorema 10 (Teorema de Sylow-3ª Parte)
Seja $(G, \cdot)$ um grupo finito. Seja p um natural primo, tal que $p^m \mid |G|$ e $p^{m+1} \nmid |G|$. Então, o número n_p de p-Sylow subgrupos de G é da forma $n_p = 1 + sp$, para algum $s \in \mathbb{N}$.

Demonstração: Seja P um p-Sylow subgrupo de G. Decompondo G nas classes duplas de P e P, temos:

(1) $G = \bigcup PxP$, onde a união é nas classes duplas distintas (disjuntas);

(2) $|PxP| = \dfrac{|P|^2}{|P \cap (xPx^{-1})|}$.

Para contar o número de elementos de PxP, consideramos dois casos:

Caso 1: $x \notin N(P)$

Suponhamos que $x \notin N(P)$. Então, $xPx^{-1} \neq P$ e $P \cap (xPx^{-1}) \neq P$. Logo, $P \cap (xPx^{-1}) \subsetneq P$ e $|P \cap (xPx^{-1})| = p^n$, para algum n, tal que $0 \leq n < m$. De (2) temos que $|PxP| = \dfrac{p^{2m}}{p^n} = p^{2m-n}$, com $2m - n = m + (m - n) \geq m + 1$. Portanto, p^{m+1} divide $|PxP|$.

Caso 2: $x \in N(P)$

Suponhamos que $x \in N(P)$. Então, $xPx^{-1} = P$, que é equivalente a $xP = Px$. Logo,

$$PxP = P(xP) = P(Px) = (PP)x = Px.$$

Então, $|PxP| = |Px| = |P| = p^m$.

Agora podemos concluir a demonstração. De (1) temos que:

Lembre que ...
$PP = \{a \cdot b \,;\, a, b \in P\}$.
É claro que $PP \subset P$. Além disso, se $a \in P$, então $a = a \cdot e \in PP$, mostrando que $P \subset PP$. Portanto, $PP = P$.

$$|G| = \sum |PxP| = \underbrace{\sum_{x \in N(P)} |PxP|}_{\text{Soma 1}} + \underbrace{\sum_{x \notin N(P)} |PxP|}_{\text{Soma 2}},$$

onde a soma é feita tomando um único elemento em cada classe dupla.

Soma 1: Se $x \in N(P)$, então $PxP = Px$ e as classes duplas distintas são as classes distintas de P em $N(P)$, isto é, o índice de P em $N(P)$, dado por $i_{N(P)}(P) = \dfrac{|N(P)|}{|P|}$. Logo,

$$\text{Soma 1} = \sum_{x \in N(P)} |Px| = |P| \cdot \frac{|N(P)|}{|P|} = |N(P)|.$$

Soma 2: Se $x \notin N(P)$, então p^{m+1} divide cada parcela da Soma 2, logo p^{m+1} divide a Soma 2. Portanto,

$$\text{Soma 2} = \sum_{x \notin N(P)} |PxP| = rp^{m+1}, \text{ para algum } r \in \mathbb{N}.$$

Portanto, $|G| = |N(P)| + rp^{m+1}$.

Como $|N(P)|$ divide $|G|$, temos que $\dfrac{rp^{m+1}}{|N(P)|} \in \mathbb{N}$ e

$$n_p = \frac{|G|}{|N(P)|} = 1 + \frac{rp^{m+1}}{|N(P)|}.$$

Além disso, como p^m divide $|G|$ e rp^{m+1}, então p^m divide $|N(P)|$. Entretanto, p^{m+1} não divide $|N(P)|$, pois não divide $|G|$, logo p divide $\dfrac{rp^{m+1}}{|N(P)|}$. Portanto,

$$n_p = \frac{|G|}{|N(P)|} = 1 + sp, \text{ para algum } s \in \mathbb{N}. \qquad \blacksquare$$

Observação: Em um grupo finito G, como conseqüência do Teorema anterior, temos que $\text{mdc}(n_p, p) = 1$.

Nos seguintes exemplos você vai ver como aplicar o Teorema de Sylow e, de diferentes maneiras, obter informações importantes sobre o grupo finito, olhando apenas para o seu número de elementos.

Exemplo 23

Seja $(G, \cdot)$ um grupo com $|G| = 11^2 \cdot 13^2$. Vamos mostrar que G é um grupo abeliano.

Primeiramente, quantos 11-Sylow e 13-Sylow subgrupos há?

Como $\text{mdc}(n_{11}, 11) = 1$ e n_{11} divide $11^2 \cdot 13^2$, temos que n_{11} divide 13^2. Assim, $n_{11} \in \{1, 13, 13^2\}$, mas $n_{11} \equiv 1 \mod 11$, $13 \equiv 2 \mod 11$ e $13^2 \equiv 2^2 = 4 \mod 11$, logo $n_{11} = 1$. Portanto, existe um único 11-Sylow subgrupo H e, forçosamente, H é normal em G.

Como $\text{mdc}(n_{13}, 13) = 1$ e n_{13} divide $11^2 \cdot 13^2$, temos que n_{13} divide 11^2. Assim, $n_{13} \in \{1, 11, 11^2\}$, mas $n_{13} \equiv 1 \mod 13$, $11 \equiv -2 \mod 13$ e $11^2 \equiv (-2)^2 = 4 \mod 13$, logo $n_{13} = 1$. Portanto, existe um único 13-Sylow subgrupo K e, forçosamente, K é normal em G.

Temos $|H| = 11^2$ e $|K| = 13^2$. Pelo Corolário 4 da Seção anterior, H e K são grupos abelianos.

$H \cap K$ é subgrupo de H e K, logo $|H \cap K|$ divide $|H|$ e $|H \cap K|$ divide $|K|$, isto é, $|H \cap K|$ divide $\text{mdc}(|H|, |K|) = \text{mdc}(11^2, 13^2) = 1$. Portanto, $|H \cap K| = 1$ e $H \cap K = \{e\}$.

Além disso, pelo Exercício 3, item (a), da Seção 2, HK é um subgrupo de G.

Como $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K| = |G|$, obtemos que $HK = G$.

Sejam $a \in H$ e $b \in K$. Então,

$$aba^{-1}b^{-1} = \begin{cases} \underbrace{a}_{\in H}\underbrace{(ba^{-1}b^{-1})}_{\in H} \in H \\ \underbrace{(aba^{-1})}_{\in K}\underbrace{b^{-1}}_{\in K} \in K \end{cases} \Longrightarrow aba^{-1}b^{-1} \in H \cap K = \{e\}$$

$bHb^{-1} = H$
e
$aKa^{-1} = K$.

Logo, $aba^{-1}b^{-1} = e$, isto é, $ab = ba$. Com isso, concluímos que G é um grupo abeliano.

Com os resultados que veremos na próxima Seção, você vai saber, mais ainda, que G é isomorfo ao produto direto interno de H e K.

Exemplo 24

Seja $(G, \cdot)$ um grupo de ordem $380 = 2^2 \cdot 5 \cdot 19$. Vamos mostrar que o 5-Sylow e o 19-Sylow subgrupos de G são normais em G.

Como $\text{mdc}(n_5, 5) = 1$ e n_5 divide $2^2 \cdot 5 \cdot 19$, temos que n_5 divide $2^2 \cdot 19$.

Logo, $n_5 \in \{1, 2, 2^2 = 4, 19, 2 \cdot 19 = 38, 2^2 \cdot 19 = 76\}$.

Além disso, $n_5 \equiv 1 \mod 5$. Então, $n_5 = 1$ ou $n_5 = 76$.

Como $\text{mdc}(n_{19}, 19) = 1$ e n_{19} divide $2^2 \cdot 5 \cdot 19$, temos que n_{19} divide $2^2 \cdot 5$.

Logo, $n_{19} \in \{1, 2, 2^2 = 4, 5, 2 \cdot 5 = 10, 2^2 \cdot 5 = 20\}$.

Além disso, $n_{19} \equiv 1 \mod 19$. Então, $n_{19} = 1$ ou $n_{19} = 20$.

Agora podemos mostrar que $n_5 = 1$ ou $n_{19} = 1$.

Suponhamos, por absurdo, que $n_5 = 76$ e $n_{19} = 20$. Os 19-Sylow subgrupos de G têm 19 elementos, logo são cíclicos de ordem prima e só se intersectam no elemento neutro. Os 5-Sylow subgrupos têm 5 elementos, são cíclicos de ordem prima e só se intersectam no elemento neutro. Contando os elementos de G, obtemos:

elementos de G cuja ordem é $19 \longmapsto 18 \times 20 = 360$

elementos de G cuja ordem é $5 \longmapsto 4 \times 76 = 304$

Assim, $360 + 304 = 664 > 380 = |G|$, obtemos uma contradição.

Concluímos, então que um 19-Sylow subgrupo ou um 5-Sylow subgrupo de G é normal.

Sejam H um 19-Sylow subgrupo, com $|H| = 19$, e K um 5-Sylow subgrupo, com $|K| = 5$. Temos que $H \cap K = \{e\}$, pois $\text{mdc}(|H|, |K|) = 1$. Como um desses subgrupos é normal, pelo Exercício 3, item (a), da Seção 2, HK é um subgrupo de G. Contando os elementos de HK, temos:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = 19 \cdot 5 = 95.$$

Seja $L = HK$. Sejam n'_5 e n'_{19} o número, respectivamente, de 5-Sylow e de 19-Sylow subgrupos de L. Aplicando o Teorema de Sylow a L, temos:

$$\begin{cases} n'_5 \equiv 1 \mod 5 \\ n'_5 \mid 5 \cdot 19 \end{cases} \Longrightarrow \begin{cases} n'_5 \equiv 1 \mod 5 \\ n'_5 \mid 19 \end{cases} \Longrightarrow \begin{cases} n'_5 \equiv 1 \mod 5 \\ n'_5 \in \{1, 19\} \end{cases}$$

logo, $n'_5 = 1$ e

$$\begin{cases} n'_{19} \equiv 1 \mod 19 \\ n'_{19} \mid 5 \cdot 19 \end{cases} \Longrightarrow \begin{cases} n'_{19} \equiv 1 \mod 19 \\ n'_{19} \mid 5 \end{cases} \Longrightarrow \begin{cases} n'_{19} \equiv 1 \mod 19 \\ n'_{19} \in \{1, 5\} \end{cases}$$

logo, $n'_{19} = 1$.

Como H e K são subgrupos de $HK = L$, então H é o 19-Sylow subgrupo de L, com H normal em HK, e K é o 5-Sylow subgrupo de HK, com K normal em HK.

Já fez o Exercício 13 da Seção 1?

$N(H)$ é o maior subgrupo de G, tal que H é normal, portanto $HK \subset N(H)$ e HK é subgrupo de $N(H)$. Por outro lado,

$$n_{19} = (G : N(H)) = \frac{|G|}{|N(H)|} \leq \frac{|G|}{|HK|} = \frac{2^2 \cdot 5 \cdot 19}{5 \cdot 19} = 4.$$

Como $n_{19} \in \{1, 20\}$, temos que $n_{19} = 1$.

Analogamente, $N(K)$ é o maior subgrupo de G, tal que K é normal, portanto $HK \subset N(K)$ e HK é subgrupo de $N(K)$. Por outro lado,

$$n_5 = (G : N(K)) = \frac{|G|}{|N(K)|} \leq \frac{|G|}{|HK|} = \frac{2^2 \cdot 5 \cdot 19}{5 \cdot 19} = 4.$$

Como $n_5 \in \{1, 76\}$, temos que $n_5 = 1$.

Exemplo 25

Seja $(G, \cdot)$ um grupo de ordem $56 = 2^3 \cdot 7$. Afirmamos que G tem um subgrupo normal de ordem 7 ou um subgrupo normal de ordem 8.

De fato, temos:

$$\begin{cases} n_7 \equiv 1 \mod 7 \\ n_7 \mid 2^3 \cdot 7 \end{cases} \Longrightarrow \begin{cases} n_7 \equiv 1 \mod 7 \\ n_7 \mid 8 \end{cases} \Longrightarrow \begin{cases} n_7 \equiv 1 \mod 7 \\ n_7 \in \{1, 2, 2^2, 2^3\} \end{cases}$$

logo, $n_7 = 1$ ou $n_7 = 8$.

Se $n_7 = 1$, então o 7-Sylow subgrupo, que tem 7 elementos, é normal.

Suponhamos que $n_7 = 8$. Vamos mostrar que $n_2 = 1$ e assim, o 2-Sylow subgrupo, que tem 8 elementos, é normal.

Os 7-Sylow subgrupos de G têm 7 elementos, logo são cíclicos de ordem prima e só se intersectam no elemento neutro.

G tem $6 \times 8 = 48$ elementos de ordem 7. Restam em G, exatamente, $56 - 48 = 8$ elementos.

Sabemos que G tem pelo menos um subgrupo H com 8 elementos, nenhum dos 48 elementos de ordem 7 está em H, portanto H se constitui dos 8 elementos restantes e é o único subgrupo de G com 8 elementos. Logo, H é normal em G.

Exercícios

1. Mostre que se G é um grupo de ordem $2^2 \cdot 7 \cdot 13$, então G tem um subgrupo normal de ordem 13.

2. Seja p um primo, $p \neq 2$. Prove que todo grupo de ordem $2p$ tem um subgrupo normal.

3. Discuta o número e a natureza de um 3-Sylow subgrupo e de um 5-Sylow subgrupo de um grupo de ordem $3^2 \times 5^2$.

4. Mostre que todo grupo de ordem 33, 35 ou 65 é cíclico.

5. Seja G um grupo com $|G| = pq$, $p < q$ números primos. Mostre que se p não divide $q - 1$, então G é cíclico.

6. Seja G um grupo com ordem p^2q, p, q primos distintos. Prove que G tem um subgrupo normal não-trivial, isto é diferente de $\{e\}$ e de G.

7. Seja G um grupo de ordem 30.

   (a) Mostre que um 3-Sylow ou um 5-Sylow subgrupo de G tem que ser normal em G.

   (b) Mostre que cada 3-Sylow e cada 5-Sylow subgrupo de G é normal em G.

   (c) Mostre que G tem um subgrupo normal de ordem 15.

   (d) Classifique os grupos de ordem 30.

   (e) Quantos grupos de ordem 30 há?

Esses dois últimos itens não podem ser resolvidos com a teoria apresentada até aqui.

8. Prove que se um grupo de ordem 28 tem um subgrupo normal de ordem 4, então é abeliano.

9. Determine os possíveis números de 11-Sylow, 7-Sylow e 5-Sylow subgrupos de um grupo com $5^2 \times 7 \times 11$ elementos.

10. Seja G um grupo de ordem 231. Mostre que o 11-Sylow subgrupo está contido no centro de G.

11. Seja G um grupo de ordem 385. Mostre que seu 11-Sylow subgrupo é normal em G e seu 7-Sylow subgrupo está contido no centro de G.

Produto direto

Nosso objetivo é expressar um grupo, quando possível, em termos de grupos menos complexos. Com esse objetivo introduzimos o conceito de produto direto.

Definição 12 (Produto direto)
Sejam $G_1, \ldots, G_n$ grupos. O *produto direto* de $G_1, \ldots, G_n$ é

$$G_1 \times \cdots \times G_n = \{(x_1, \ldots, x_n) \; ; \; x_j \in G_j, \text{ para todo } j = 1, \ldots, n\}.$$

com a operação $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 \cdot y_1, \ldots, x_n \cdot y_n)$, onde na j-ésima coordenada a operação é do grupo G_j, para cada $j = 1, \ldots, n$.

Vamos determinar condições para um grupo G ser isomorfo a um produto direto (interno) $H_1 \cdot \ldots \cdot H_n$, onde $H_1, \ldots, H_n$ são subgrupos de G.

Teorema 11 (Produto direto)
Sejam $G, G_1, \ldots, G_n$ grupos. G é isomorfo a $G_1 \times \cdots \times G_n$ se, e somente se, G tem subgrupos $H_1 \simeq G_1, \ldots, H_n \simeq G_n$, tais que:

$\simeq$ significa isomorfo.

(i) $G = H_1 \cdot \ldots \cdot H_n$;
(ii) $H_j \lhd G$, para todo $j = 1, \ldots, n$;
(iii) $H_j \cap (H_1 \cdot \ldots \cdot \widehat{H_j} \cdot \ldots \cdot H_n) = \{e\}$, para todo $j = 1, \ldots, n$.

$H_1 \cdot \ldots \cdot \widehat{H_j} \cdot \ldots \cdot H_n$ significa que H_j não ocorre no produto, é omitido.

Antes de demonstrarmos o Teorema, damos duas condições equivalentes às três condições acima.

Lema 3
Sejam G um grupo e $H_1, \ldots, H_n$ subgrupos de G. Valem as condições (i), (ii) e (iii) do Teorema anterior se, e somente se, valem as condições (iv) e (v) descritas a seguir:

(iv) Para cada $a \in G$, existem elementos $x_1 \in H_1, \ldots, x_n \in H_n$, unicamente determinados, tais que $a = x_1 \cdot \ldots \cdot x_n$.
(v) Para todo $x \in H_i$ e para todo $y \in H_j$, com $1 \leq i \neq j \leq n$, temos $x \cdot y = y \cdot x$.

Cuidado! Podemos trocar a ordem dos fatores apenas quando operamos elementos de H_i e H_j, com $i \neq j$.

Demonstração:

($\Longrightarrow$:) Suponhamos que valham as propriedades (i), (ii) e (iii) do Teorema anterior. Sejam $x \in H_i$ e $y \in H_j$ com $i \neq j$. Consideremos o elemento $xyx^{-1}y^{-1}$. Então,

$$xyx^{-1}y^{-1} = \begin{cases} (xyx^{-1})y^{-1} \in H_j, & \text{pois } H_j \lhd G \\ x(yx^{-1}y^{-1}) \in H_i, & \text{pois } H_i \lhd G. \end{cases}$$

Logo, $xyx^{-1}y^{-1} \in H_i \cap H_j \subset H_i \cap (H_1 \cdot \ldots \cdot \widehat{H_i} \cdot \ldots \cdot H_n) = \{e\}$, pela propriedade (iii). Portanto, $xyx^{-1}y^{-1} = e$, que é equivalente a $xy = yx$, mostrando a propriedade (v).

Para cada $a \in G$, pela condição (i), existe $x_j \in H_j$, com $j = 1, \ldots, n$, tal que $a = x_1 \cdot \ldots \cdot x_n$. Suponhamos agora que

$$x_1 \cdot \ldots \cdot x_n = y_1 \cdot \ldots \cdot y_n, \qquad (\star)$$

com $x_j, y_j \in H_j$, para cada $j = 1, \ldots, n$.

Multiplicando ambos os lados da igualdade $(\star)$ por ${y_1}^{-1}$ à esquerda e por ${x_n}^{-1} \cdot \ldots \cdot {x_2}^{-1}$ à direita , obtemos

$$ {y_1}^{-1}x_1 = y_2 \cdots y_{n-1} \underbrace{y_n {x_n}^{-1}}_{\in H_n} {x_{n-1}}^{-1} \cdots {x_2}^{-1}. $$

Começamos com ${x_{n-1}}^{-1}$, que comuta com $y_n {x_n}^{-1}$. Ao encontrarmos y_{n-1} temos que parar. Depois tomamos ${x_{n-2}}^{-1}$, que comuta com $(y_{n-1}{x_{n-1}}^{-1})(y_n {x_n}^{-1})$.

Usando a condição (v), sucessivamente, para ${x_{n-1}}^{-1}, \ldots, {x_2}^{-1}$, obtemos que

$$ \underbrace{{y_1}^{-1}x_1}_{\in H_1} = \underbrace{(y_2{x_2}^{-1})}_{\in H_2} \cdots \underbrace{(y_{n-1}{x_{n-1}}^{-1})}_{\in H_{n-1}} \underbrace{(y_n{x_n}^{-1})}_{\in H_n} $$

Assim, ${y_1}^{-1}x_1 \in H_1 \cap (H_2 \cdots H_n) = \{e\}$, pela condição (iii). Logo, ${y_1}^{-1}x_1 = e$ e $x_1 = y_1$. Cancelando em $(\star)$, obtemos

$$x_2 \cdot \ldots \cdot x_n = y_2 \cdot \ldots \cdot y_n.$$

Procedendo de modo similar, obtemos

$$ \underbrace{{y_2}^{-1}x_2}_{\in H_2} = \underbrace{(y_3{x_3}^{-1})}_{\in H_3} \cdots \underbrace{(y_n{x_n}^{-1})}_{\in H_n}. $$

Logo, ${y_2}^{-1}x_2 \in H_2 \cap (H_3 \cdots H_n) \subset H_2 \cap (H_1 H_3 \cdots H_n) = \{e\}$.

Então, ${y_2}^{-1}x_2 = e$, isto é, $x_2 = y_2$.

Continuando o processo, temos $x_1 = y_1$, $\ldots$, $x_n = y_n$, mostrando a unicidade.

($:\Longleftarrow$) Reciprocamente, suponhamos que valham as propriedades (iv) e (v).

De (iv) segue que $G = H_1 \cdots H_n$, mostrando (i).

Agora vamos mostrar a condição (ii), isto é, $H_j \lhd G$. Sejam $y \in H_j$ e $a \in G$, com j fixo. Mostraremos que $aya^{-1} \in H_j$.

Pela condição (iv), $a = x_1 \cdots x_n$, com $x_i \in H_i$ e

$$\begin{aligned} aya^{-1} &= (x_1 \cdots x_n)y(x_n^{-1} \cdots x_1^{-1}) \\ &= x_1 \cdots x_j x_{j+1} \cdots x_n y x_n^{-1} \cdots x_{j+1}^{-1} x_j^{-1} \cdots x_1^{-1}. \end{aligned}$$

Aplicando a condição (v), repetidamente, ao elemento x_i, com $i = j+1, \ldots, n$, obtemos:

x_i comuta com os elementos à sua direita até encontrar x_i^{-1} e aí $x_i x_i^{-1} = e$.

$$aya^{-1} = x_1 \cdots x_{j-1} \underbrace{x_j y x_j^{-1}}_{\in H_j} x_{j-1}^{-1} \cdots x_1^{-1}.$$

Aplicando a condição (v) ao elemento $x_j y x_j^{-1}$, obtemos

$x_j y x_j^{-1}$ comuta com o elemento à sua esquerda.

$aya^{-1} = x_j y x_j^{-1} \in H_j$, mostrando a propriedade (ii).

Mostraremos agora a condição (iii). Seja $a \in H_j \cap (H_1 \cdots \widehat{H_j} \cdots H_n)$.

Como $a \in H_j$, podemos escrever $a = x_1 \cdots x_n$, com $x_j = a$ e $x_i = e$, para todo $i \neq j$.

Como $a \in H_1 \cdots \widehat{H_j} \cdots H_n$, podemos escrever $a = x_1 \cdots x_n$ com $x_i \in H_i$, para $i \neq j$ e $x_j = e$.

Da unicidade da condição (iv), obtemos que $a = e$. ■

Demonstração do Teorema (Produto direto):

($\Longrightarrow$:) Seja $\varphi : G \longrightarrow G_1 \times \cdots \times G_n$ um isomorfismo de grupos.

e_i é o elmento neutro de G_i.

Seja $H_j = \varphi^{-1}(K_j)$, onde $K_j = \{e_1\} \times \cdots \times \{e_{j-1}\} \times G_j \times \{e_{j+1}\} \times \cdots \times \{e_n\}$.

Então, K_1, ..., K_n são subgrupos de $G_1 \times \cdots \times G_n$, tendo as condições (i), (ii) e (iii). Logo, H_1, ..., H_n são subgrupos de G tendo essas mesmas condições.

Fez os Exercícios 25 e 26 da Seção 1?

($:\Longleftarrow$) Suponhamos que G tenha subgrupos $H_1, \ldots, H_n$, com $H_j \simeq G_j$ satisfazendo as condições (i), (ii) e (iii). Consideremos

$$\begin{aligned} \varphi : G = H_1 \cdots H_n &\longrightarrow H_1 \times \cdots \times H_n \\ h_1 \cdots h_n &\longmapsto (h_1, \ldots, h_n) \end{aligned}$$

φ é uma função, em virtude da condição (iv). É óbvio que φ é uma bijeção. Vamos mostrar que φ é um homomorfismo de grupos.

Sejam $a = x_1 \cdots x_n$ e $b = y_1 \cdots y_n$. Então,

$$\begin{aligned} ab &= (x_1 \cdots x_n)(y_1 \cdots y_n) \\ &\overset{(1)}{=} (x_1 y_1)(x_2 y_2) \cdots (x_n y_n) \end{aligned}$$

Em (1) usamos a condição (v).

e

$$\begin{aligned}\varphi(ab) &= \varphi((x_1y_1)(x_2y_2)\cdots(x_ny_n)) \\ &= (x_1y_1,\ldots,x_ny_n) \\ &= (x_1,\ldots,x_n)(y_1,\ldots,y_n) \\ &= \varphi(a)\varphi(b)\end{aligned}$$

Tome $\psi_j : H_j \longrightarrow G_j$ um isomorfismo de grupos e construa

$$\begin{aligned}\psi : H_1 \times \cdots \times H_n &\longrightarrow G_1 \times \cdots \times G_n \\ (h_1,\ldots,h_n) &\longmapsto (\psi_1(h_1),\ldots,\psi_n(h_n)).\end{aligned}$$

Então, ψ é um isomorfismo de grupos e $\psi\circ\varphi$ é o isomorfismo procurado de G em $G_1 \times \cdots \times G_n$. ■

Esse Teorema, junto com o Teorema de Sylow, tem uma importante aplicação aos grupos abelianos finitos diferentes de $\{e\}$.

Nosso objetivo será obter a classificação dos grupos abelianos finitos diferentes de $\{e\}$. Podemos descrever todos esses grupos, olhando apenas para $|G| > 1$ e escrevendo $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, onde $p_1 < \cdots < p_r$ são primos e $\alpha_1 > 0, \ldots, \alpha_r > 0$.

Veremos que só precisamos entender os p-grupos abelianos finitos.

Proposição 10 (Estrutura dos grupos abelianos finitos)
Seja $(G,\cdot)$ um grupo abeliano finito, $G \neq \{e\}$, com $|G| = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, onde $p_1 < \cdots < p_r$ são primos e $\alpha_1 > 0, \ldots, \alpha_r > 0$. Seja S_j o p_j-Sylow subgrupo de G, para $j = 1,\ldots,r$. Então,

$$G = S_1 \cdot \ldots \cdot S_r \simeq S_1 \times \cdots \times S_r.$$

Lembramos que se G é abeliano e H e K são subgrupos de G, então HK sempre é subgrupo de G.

Demonstração: Primeiramente, observamos que $|S_j| = {p_j}^{\alpha_j}$.

Como G é abeliano, todo subgrupo é normal, em particular, $S_j \lhd G$, para cada $j = 1,\ldots,r$. Assim, $S_1 \cdot \ldots \cdot S_r$ é um subgrupo de G.

Além disso, $S_j \cap (S_1 \cdots \widehat{S_j} \cdots S_r) = \{e\}$.

De fato, seja $x \in S_j$ e $x = x_1 \cdots x_{j-1}x_{j+1} \cdots x_r$. Então, $\circ(x)$ divide $p_j^{\alpha_j}$ e $\circ(x_i)$ divide $p_i^{\alpha_i}$, para $i \neq j$. Tomamos $n = \prod_{i\neq j} {p_i}^{\alpha_i} = \lambda_i {p_i}^{\alpha_i}$. Logo,

$$x^n = \left(\prod_{i\neq j} x_i\right)^n = \prod_{i\neq j}({x_i}^n) = \prod_{i\neq j}\left({x_i}^{{p_i}^{\alpha_i}}\right)^{\lambda_i} = \prod_{i\neq j} e^{\lambda_i} = e.$$

Portanto, $\circ(x)$ divide n. Então, $\circ(x)$ divide $\text{mdc}(p_j^{\alpha_j}, n) = 1$.

Logo, $\circ(x) = 1$, isto é, $x = e$.

Portanto,

$$\begin{aligned} |S_1 \cdots S_r| &= \frac{|S_1||S_2 \cdots S_r|}{|S_1 \cap (S_2 \cdots S_r)|} = |S_1||S_2 \cdots S_r| \\ &= |S_1|\frac{|S_2||S_3 \cdots S_r|}{|S_2 \cap (S_3 \cdots S_r)|} = |S_1||S_2||S_3 \cdots S_r| \\ &= \cdots = |S_1||S_2| \cdots |S_r| = |G|, \end{aligned}$$

mostrando que $G = S_1 \cdot \ldots \cdot S_r$.

Pelo Teorema 11, $G = S_1 \cdots S_r \simeq S_1 \times \cdots \times S_r$ é o produto direto interno dos seus p_i-Sylow subgrupos. ■

Para entender os grupos abelianos finitos diferentes de $\{e\}$ precisamos apenas saber quem são os grupos abelianos de ordem p^n, onde p é primo e $n \geq 1$.

Teorema 12 (Estrutura dos grupos abelianos de ordem p^n)
Seja $(G, \cdot)$ um grupo abeliano de ordem p^n, onde p é primo e $n \geq 1$. Então, existem $n_1 \geq \cdots \geq n_k \geq 1$ e subgrupos cíclicos $H_1, \ldots, H_k$ com $|H_i| = p^{n_i}$, tais que

$$G = H_1 \cdots H_k \simeq H_1 \times \cdots \times H_k, \text{ com } n = n_1 + \cdots + n_k$$

e os números naturais $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$ são chamados de *invariantes de* G.

Nos Exercícios 5 e 6 da Seção 3 você classificou os grupos de ordem p^2.

Adiante vamos justificar essa terminologia.

Demonstração: Nosso objetivo é encontrar $a_1, \ldots, a_k \in G$, com $\circ(a_j) = p^{n_j}$, $j = 1, \ldots, k$, $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$, e cada $x \in G$ se escreva de modo único como $x = {a_1}^{\alpha_1} \cdots {a_k}^{\alpha_k}$.

Nesse caso, observamos que $\max\{\circ(x) \ ; \ x \in G\} = p^{n_1}$. Essa é a inspiração para a demonstração do Teorema.

Escolhemos $a_1 \in G$ tal que $\circ(a_1)$ é máxima, digamos $\circ(a_1) = p^{n_1}$.

Seja $H_1 = \langle a_1 \rangle$. Se $H_1 = G$, então $n_1 = n$ e terminamos. Nesse caso, G é cíclico de ordem p^n.

Caso contrário, $H_1 \subsetneq G$, $1 \leq n_1 < n$. Podemos considerar $\overline{G} = G/H_1$. Esse grupo quociente também é abeliano e $|\overline{G}| = p^{n-n_1}$.

Seja $b_2 \in G$ com $\circ(\overline{b_2}) = p^{n_2} = \max\{\circ(H_1 x) \ ; \ x \in G\}$, onde $\overline{b_2} = H_1 b_2$.

Afirmamos que $n_2 \leq n_1$. De fato,

$$\overline{b_2}^{\circ(b_2)} = (H_1 b_2)^{\circ(b_2)} = H_1 {b_2}^{\circ(b_2)} = H_1 e = H_1.$$

Logo, $\circ(\overline{b_2}) = p^{n_2}$ divide $\circ(b_2) = p^l \leq p^{n_1}$. Assim, $n_2 \leq l \leq n_1$, isto é, $n_2 \leq n_1$.

Para termos um produto direto precisamos que $H_1 \cap \langle b_2 \rangle = \{e\}$.

Digamos que $H_1 \cap \langle b_2 \rangle \neq \{e\}$.

Como p^{n_2} é a menor potência de p, tal que $b_2^{p^{n_2}} \in H_1$, então $b_2^{p^{n_2}} = a_1^i$ e assim,

$$a_1^{ip^{n_1-n_2}} = \left(a_1^i\right)^{p^{n_1-n_2}} = \left(b_2^{p^{n_2}}\right)^{p^{n_1-n_2}} = b_2^{p^{n_1}} \overset{(1)}{=} e,$$

A igualdade (1) segue do fato $\circ(b_2)$ divide p^{n_1}.

logo $p^{n_1} = \circ(a_1)$ divide $ip^{n_1-n_2}$, portanto p^{n_2} divide i.

Escrevendo $i = jp^{n_2}$, temos $b_2^{p^{n_2}} = a_1^i = a_1^{jp^{n_2}}$. Logo, $\left(a_1^{-j} b_2\right)^{p^{n_2}} = e$.

Tomando $a_2 = a_1^{-j} b_2$, obtemos $\circ(a_2) = p^{n_2}$.

Seja $H_2 = \langle a_2 \rangle$. Afirmamos que $H_1 \cap H_2 = \{e\}$.

De fato, seja $x = a_2^t \in H_1$. Então,

$$x = a_2^t = \left(a_1^{-j} b_2\right)^t = \underbrace{\left(a_1^{-j}\right)^t}_{\in H_1} b_2^t \in H_1,$$

logo $b_2^t \in H_1$, portanto p^{n_2} divide t. Como $\circ(a_2) = p^{n_2}$, concluímos que $x = e$.

Caso $n = n_1 + n_2$, então $G = H_1 H_2$ com $H_1 \cap H_2 = \{e\}$ e terminamos.

Caso contrário, $H_1 H_2$ é um subgrupo próprio de G, $n_1 + n_2 < n$ e consideramos $\overline{G} = G/H_1 H_2$. Esse grupo é abeliano com $|\overline{G}| = p^{n-(n_1+n_2)}$.

Seja $b_3 \in G$ um elemento, tal que $\overline{b_3} = (H_1 H_2) b_3$ tem ordem máxima p^{n_3} em $\overline{G}$.

Afirmamos que $n_3 \leq n_2 \leq n_1$.

De fato, pela escolha de n_2, temos $b_3^{p^{n_2}} \in H_1 \subset H_1 H_2$. Logo, $\overline{b_3}^{p^{n_2}} = \overline{e}$, então p^{n_3} divide p^{n_2}, isto é, $n_3 \leq n_2$.

Como ${b_3}^{p^{n_3}} \in H_1 H_2$, então ${b_3}^{p^{n_3}} = {a_1}^{i_1} {a_2}^{i_2}$.

Afirmamos que p^{n_3} divide i_1 e p^{n_3} divide i_2.

$$\left({a_1}^{i_1} {a_2}^{i_2}\right)^{p^{n_2-n_3}} = \left({b_3}^{p^{n_3}}\right)^{p^{n_2-n_3}} = {b_3}^{p^{n_2}} \in H_1$$

Por outro lado, $\left(a_1{}^{i_1}a_2{}^{i_2}\right)^{p^{n_2-n_3}} = \underbrace{\left(a_1{}^{i_1}\right)^{p^{n_2-n_3}}}_{\in H_1}\left(a_2{}^{i_2}\right)^{p^{n_2-n_3}}$. Então, $\left(a_2{}^{i_2}\right)^{p^{n_2-n_3}} \in H_1$ e, pela escolha de n_2, p^{n_2} divide $i_2p^{n_2-n_3}$, isto é, p^{n_3} divide i_2.

$$\left(a_1{}^{i_1}a_2{}^{i_2}\right)^{p^{n_1-n_3}} = \left(b_3{}^{p^{n_3}}\right)^{p^{n_1-n_3}} = b_3{}^{p^{n_1}} = e \in H_2$$

Por outro lado, $\left(a_1{}^{i_1}a_2{}^{i_2}\right)^{p^{n_1-n_3}} = \left(a_1{}^{i_1}\right)^{p^{n_1-n_3}}\underbrace{\left(a_2{}^{i_2}\right)^{p^{n_1-n_3}}}_{\in H_2}$. Então, $\left(a_1{}^{i_1}\right)^{p^{n_1-n_3}} \in H_1 \cap H_2 = \{e\}$. Logo, $\left(a_1{}^{i_1}\right)^{p^{n_1-n_3}} = e$ e p^{n_1} divide $i_1p^{n_1-n_3}$, isto é, p^{n_3} divide i_1.

Escrevendo $i_1 = j_1p^{n_3}$ e $i_2 = j_2p^{n_3}$, então $b_3{}^{p^{n_3}} = a_1{}^{j_1p^{n_3}}a_2{}^{j_2p^{n_3}}$. Tomando $a_3 = a_1{}^{-j_1}a_2{}^{-j_2}b_3$, temos $\circ(a_3) = p^{n_3}$.

Seja $H_3 = \langle a_3\rangle$.

Afirmamos que $H_3 \cap (H_1H_2) = \{e\}$.

De fato, digamos que $a_3{}^t \in H_1H_2$. Então,

$$a_3{}^t = \left(a_1{}^{-j_1}a_2{}^{-j_2}b_3\right)^t = \underbrace{\left(a_1{}^{-tj_1}a_2{}^{-tj_2}\right)}_{\in H_1H_2}b_3{}^t,$$

logo $b_3{}^t \in H_1H_2$, portanto $\overline{b_3}^t = \overline{e}$ e p^{n_3} divide t. Como $\circ(a_3) = p^{n_3}$, concluímos que $a_3{}^t = e$.

Continuando o processo, obtemos subgrupos $H_1 = \langle a_1\rangle$, $H_2 = \langle a_2\rangle$, $\ldots$, $H_k = \langle a_k\rangle$ com ordens $p^{n_1} \geq p^{n_2} \geq \cdots \geq p^{n_k}$, respectivamente, tais que $G = H_1H_2\cdots H_k$ e, para cada $j = 2, \ldots, k$, $H_j \cap (H_1\cdots H_{j-1}) = \{e\}$. Assim, cada $x \in G$ tem uma única representação como $x = x_1\cdots x_k$, com $x_j \in H_j$ e $G = H_1\cdots H_k \simeq H_1 \times \cdots \times H_k$. ■

Veremos que os invariantes de um p-grupo abeliano finito descrevem completamente o grupo. Os grupos $H_1, \ldots, H_k$ não são únicos.

Exemplo 26

Seja $G = \{e, a, b, ab = ba; a^2 = e, b^2 = e\}$ o grupo de Klein.

Temos

$H_1 = \langle a\rangle$, $H_2 = \langle b\rangle$, $G = H_1H_2 \simeq H_1 \times H_2$ e

com $c = ab$, $H_3 = \langle c\rangle$, $G = H_1H_3 \simeq H_1 \times H_3$.

Mostraremos que, apesar dos grupos cíclicos não serem únicos, suas ordens são unicamente determinadas. Para isto definimos:

Definição 13
Seja $(G,\cdot)$ um grupo abeliano e s um inteiro.

$$G(s) = \{x \in G \ ; \ x^s = e\}.$$

É claro que $G(s)$ é um subgrupo de G.

Lema 4
Se $(G,\cdot)$ e $(G',\star)$ são grupos abelianos isomorfos então, para cada inteiro s, $G(s)$ e $G'(s)$ são isomorfos.

Demonstração: Seja $\varphi : G \longrightarrow G'$ um isomorfismo de grupos abelianos. Seja $x \in G(s)$. Então, $e = x^s$ e $e' = \varphi(e) = \varphi(x^s) = (\varphi(x))^s$, logo $\varphi(x) \in G'(s)$.

Por outro lado, para cada $y \in G'(s)$, existe um único $x \in G$ tal que $y = \varphi(x)$ e $e' = y^s = (\varphi(x))^s = \varphi(x^s)$. Logo, $x^s \in \text{Núcleo}(\varphi) = \{e\}$, isto é, $x^s = e$, portanto, $x \in G(s)$.

Então, φ induz um isomorfismo de $G(s)$ em $G'(s)$. ■

Lema 5
Seja $(G,\cdot)$ um grupo abeliano de ordem p^n, onde p é primo e $n \geq 1$. Suponhamos que $G = H_1 \cdots H_k$, onde $H_j = \langle a_j \rangle$ tem ordem p^{n_j}, $j = 1, \ldots, k$, e $n = n_1 + \cdots + n_k$. Se m é um inteiro tal que $n_t > m \geq n_{t+1}$, então

$$G(p^m) = K_1 \cdots K_t \cdot H_{t+1} \cdots H_k,$$

onde K_i é cíclico de ordem p^m e é gerado por ${a_i}^{p^{n_i - m}}$, para $i \leq t$.

A ordem de $G(p^m)$ é p^u, onde

$$u = mt + \sum_{i=t+1}^{k} n_i.$$

Demonstração: Primeiramente, afirmamos que $H_{t+1}, \ldots, H_k$ estão contidos em $G(p^m)$.

De fato, como $m \geq n_{t+1} \geq \cdots \geq n_k \geq 1$, então para todo j, tal que $t+1 \leq j \leq k$, temos que ${a_j}^{p^m} = \left({a_j}^{p^{n_j}}\right)^{p^{m-n_j}} = e$ logo, $a_j \in G(p^m)$ e $H_j = \langle a_j \rangle \subset G(p^m)$.

Lembre que ...
$o(a_j) = p^{n_j}$.

Consideremos $j \leq t$. Então $n_j \geq n_t > m$ e $\left({a_j}^{p^{n_j - m}}\right)^{p^m} = {a_j}^{p^{n_j}} = e$, logo ${a_j}^{p^{n_j - m}} \in G(p^m)$, assim $K_j = \langle {a_j}^{p^{n_j - m}} \rangle \subset G(p^m)$ e $|K_j| = p^m$.

Portanto, $K_1 \cdots K_t \cdot H_{t+1} \cdots H_k$ é subgrupo de G contido em $G(p^m)$. Esse produto é direto porque $H_1 \cdots H_k$ é produto direto. Vamos mostrar que esses elementos esgotam $G(p^m)$.

Seja $x = {a_1}^{i_1} \cdots {a_k}^{i_k} \in G(p^m)$. Então,

$$\begin{aligned} e = x^{p^m} &= a_1^{i_1 p^m} \cdots a_t^{i_t p^m} \cdots a_k^{i_k p^m} \\ &= a_1^{i_1 p^m} \cdots a_t^{i_t p^m}, \end{aligned}$$

onde a última igualdade segue do fato de que para $j \geq t+1$, independentemente do valor de i_j, $p^{n_j} = o(a_j)$ divide $i_j p^m$, porque $m \geq n_{t+1} \geq n_j$.

Agora, seja $1 \leq j \leq t$.

Devemos ter que p^{n_j} divide $i_j p^m$, com $n_j \geq n_t > m \geq n_{t+1}$, que é equivalente a $p^{n_j - m}$ divide i_j, se e somente se, $i_j = \lambda_j p^{n_j - m}$, com $\lambda_j \in \mathbb{Z}$.

Portanto,

$$x = a_1^{\lambda_1 p^{n_1 - m}} \cdots a_t^{\lambda_t p^{n_t - m}} \cdot a_{t+1}^{i_{t+1}} \cdots a_k^{i_k},$$

com $\lambda_1, \ldots, \lambda_t, i_{t+1}, \ldots, i_k \in \mathbb{Z}$.

Logo, $x \in K_1 \cdots K_t \cdot H_{t+1} \cdots H_k$.

A afirmação sobre o número de elementos de $G(p^m)$ é óbvia. ■

Corolário 5

Seja $(G, \cdot)$ um grupo abeliano com p^n elementos. Então, $|G(p)| = p^k$, onde k é o número de invariantes de G.

Demonstração: Temos $n_1 \geq \cdots \geq n_k \geq 1$. Tomamos $K_j = \langle a_j^{p^{n_j - 1}} \rangle$, para $j = 1, \ldots, k$. Então, $|K_j| = o(a_j^{p^{n_j - 1}}) = p$ e $|K_1 \cdots K_k| = p^k$. ■

Finalmente, podemos mostrar que os invariantes determinam um grupo abeliano com p^n elementos.

Justificativa da terminologia!

Teorema 13 (Classificação dos grupos abelianos de ordem p^n)

Dois grupos abelianos de ordem p^n, onde p é primo e $n \geq 1$ são isomorfos se, e somente se, têm os mesmos invariantes.

Demonstração: Sejam G e G' dois grupos abelianos com p^n elementos, onde

$G = H_1 \cdots H_k$, $H_i = \langle a_i \rangle$, $o(a_i) = p^{n_i}$, $n_1 \geq \cdots \geq n_k \geq 1$ e

$G' = N_1 \cdots N_s$, $N_j = \langle b_j \rangle$, $o(b_j) = p^{m_j}$, $m_1 \geq \cdots \geq m_s \geq 1$.

Vamos mostrar que G e G' são isomorfos se, e somente se, $k = s$ e $n_j = m_j$, para todo $j = 1, \ldots, k$.

($\Longleftarrow$:) Suponhamos que G e G' tenham os mesmos invariantes. Então,

$G = H_1 \cdots H_k$, $H_i = \langle a_i \rangle$, $o(a_i) = p^{n_i}$, $n_1 \geq \cdots \geq n_k \geq 1$ e

$G' = N_1 \cdots N_k$, $N_j = \langle b_j \rangle$, $o(b_j) = p^{n_j}$, $n_1 \geq \cdots \geq n_k \geq 1$.

Seja $\varphi : G \longrightarrow G'$ o único homomorfismo de grupos tal que $\varphi(a_i) = b_i$, para todo $i = 1, \ldots, k$. Como cada $x \in G$ se escreve na forma $x =$

Verifique!

$a_1^{i_1} \cdots a_k^{i_k}$, temos que $\varphi(x) = \varphi(a_1)^{i_1} \cdots \varphi(a_k)^{i_k} = b_1^{i_1} \cdots b_k^{i_k}$ e φ é um isomorfismo de grupos.

($\Longrightarrow$:) Suponhamos que G e G' sejam grupos isomorfos descritos com as notações do enunciado no início da demonstração. Pelo Lema 4, $G(p)$ e $G'(p)$ são isomorfos. Pelo Corolário anterior, $|G(p)| = p^k$ e $|G'(p)| = p^s$. Logo, $p^k = p^s$, donde $k = s$, isto é, o número de invariantes de G e G' é o mesmo.

Suponhamos, por absurdo, que $n_i \neq m_i$, para algum i, $1 \leq i \leq k$.

Seja t o menor i, com a propriedade acima, isto é, $n_t \neq m_t$, digamos que $n_t > m_t$ e $n_1 = m_1 \geq n_2 = m_2 \geq \cdots \geq n_t > m_t \geq m_{t+1}$.

Tomamos $m = m_t$.

Consideremos $H = \{x^{p^m} \ ; \ x \in G\}$ e $N = \{y^{p^m} \ ; \ y \in G'\}$.

Como G e G' são isomorfos, obtemos que H e N são isomorfos.

Vamos analisar os invariantes de N e H.

Como $m_1 = n_1 \geq \cdots \geq m_{t-1} = n_{t-1} > m_t = m$, então $N = D_1 \cdots D_{t-1}$, com $D_i = \langle {b_i}^{p^m} \rangle$, $|D_i| = p^{m_i - m}$. Logo, os invariantes de N são $m_1 - m = n_1 - m$, ..., $m_{t-1} - m = n_{t-1} - m$ e o número de invariantes é $t - 1$.

Antes de analisarmos os invariantes de H, escolhemos r de modo que $n_t \geq n_r > m = m_t \geq n_{r+1}$. Assim, para todo $i \geq r + 1$, temos $m = m_t \geq n_{r+1} \geq n_i$ e ${a_i}^{p^m} = e$.

Como $n_1 \geq \cdots \geq n_t \geq n_r > m = m_t \geq n_{r+1} \geq \cdots \geq n_k \geq 1$, então $H = C_1 \cdots C_t \cdots C_r$, com $C_i = \langle {a_i}^{p^m} \rangle$, $|C_i| = p^{n_i - m}$, para todo i tal que $1 \leq i \leq r$. Logo, os invariantes de H são $n_1 - m$, ..., $n_r - m$ e o número de invariantes é $r \geq t$.

Como H e N são isomorfos, têm o mesmo número de invariantes, contradizendo o fato que $r \geq t > t - 1$.

Portanto, concluímos que $m_i = n_i$, para todo $i = 1, \ldots, k$. ■

Pelo Teorema anterior, um grupo abeliano de ordem p^n, com p primo e $n \geq 1$, pode ser decomposto como um produto direto (interno) de subgrupos cíclicos, onde o número de elementos dos subgrupos cíclicos é único, considerando

$$p^{n_1} \geq \cdots \geq p^{n_k} \geq p \text{ e } n = n_1 + \cdots + n_k.$$

Definição 14 (Partição)
Seja $n \in \mathbb{N}$, $n \geq 1$. Dizemos que $n_1, \ldots, n_k \in \mathbb{N}$ é uma *partição* de n se, e somente se, $n = n_1 + \cdots + n_k$ com $n_1 \geq \cdots \geq n_k \geq 1$.

Exemplo 27
Se $n = 1$, então há uma única partição de n, a saber, $n = 1 = n_1$
As partições de $n = 2$ são duas:

$$\begin{array}{ll} 2, & n_1 = 2 \\ 2 = 1 + 1, & n_1 = n_2 = 1 \end{array}$$

As partições de $n = 3$ são:

$$\begin{array}{ll} 3, & n_1 = 3 \\ 3 = 2 + 1, & n_1 = 2 > n_2 = 1 \\ 3 = 1 + 1 + 1, & n_1 = n_2 = n_3 = 1 \end{array}$$

As partições de $n = 4$ são:

$$\begin{array}{ll} 4, & n_1 = 4 \\ 4 = 3 + 1, & n_1 = 3 > n_2 = 1 \\ 4 = 2 + 1 + 1, & n_1 = 2 > n_2 = n_1 = 1 \\ 4 = 1 + 1 + 1 + 1, & n_1 = n_2 = n_3 = n_4 = 1 \\ 4 = 2 + 2, & n_1 = n_2 = 2 \end{array}$$

Observamos que se $n_1 \geq \cdots \geq n_k \geq 1$ é uma partição de n, isto é, $n = n_1 + \cdots + n_k$, então podemos construir um grupo abeliano com p^n elementos, cujos invariantes são $n_1 \geq \cdots \geq n_k \geq 1$, a saber, $G = \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_k}}$.

Pelo Teorema anterior, duas partições de n distintas dão grupos abelianos com p^n elementos não-isomorfos.

Teorema 14
O número de grupos abelianos não-isomorfos de ordem p^n, p primo e $n \geq 1$ é $p(n)$, o número de partições de n.

Exemplo 28
$p(2) = 2$. Logo, há, a menos de isomorfismo, dois grupos abelianos com p^2 elementos, $\mathbb{Z}_{p^2}$ ou $\mathbb{Z}_p \times \mathbb{Z}_p$.
$p(3) = 3$. Logo, há, a menos de isomorfismo, três grupos abelianos com p^3 elementos, $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ ou $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.

Exemplo 29
Agora é a sua vez. Descreva os cinco grupos abelianos não-isomorfos de ordem p^4.

Corolário 6
O número de grupos abelianos não-isomorfos com ${p_1}^{\alpha_1} \cdot \ldots \cdot {p_s}^{\alpha_s}$ elementos, tais que $p_1 < \cdots < p_s$ são primos e $\alpha_i > 0$, é $p(\alpha_1) \cdot \ldots \cdot p(\alpha_s)$, onde $p(\alpha_i)$ é o número de partições de α_i, $i = 1, \ldots, s$.

Exemplo 30
Vamos descrever, a menos de isomorfismo, os grupos abelianos com 200 elementos.

Primeiramente, escrevemos $200 = 2^3 \times 5^2$.

Temos $\alpha_1 = 3$, $p(3) = 3$ e os grupos abelianos não-isomorfos com $2^3 = 8$ elementos são $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ e $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, olhando para as partições de 3 no Exemplo 27.

Temos $\alpha_2 = 2$, $p(2) = 2$ e os grupos abelianos não-isomorfos com $5^2 = 25$ elementos são $\mathbb{Z}_{25}$ e $\mathbb{Z}_5 \times \mathbb{Z}_5$. Logo, há $p(3) \times p(2) = 3 \times 2 = 6$ grupos abelianos não-isomorfos com 200 elementos.

A menos de isomorfismo, os grupos abelianos com 200 elementos são:

Apenas um desses grupos é cíclico. Qual é o grupo cíclico com 200 elementos?

$\mathbb{Z}_8 \times \mathbb{Z}_{25}$, $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$,
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$ e $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$.

Exercícios

1. Sejam $(G, \cdot)$ e $(G', \star)$ grupos, com elementos neutros, respectivamente, e e e'. Seja $G \times G' = \{(a, a') \; a \in G \text{ e } ; \; a' \in G'\}$.

   (a) Mostre que $G \times G'$ é um grupo com a operação

   $$(a, a') \cdot (b, b') = (a \cdot b, a' \star b').$$

   (b) Sejam H e H' subgrupos de G e G', respectivamente.

      i. Mostre que $H \times H'$ é um subgrupo de $G \times G'$.

      ii. Mostre que $H \times H'$ é um subgrupo normal de $G \times G'$ se, e somente se, H e H' são subgrupos normais de G e G', respectivamente.

iii. Sejam H e H' subgrupos normais de G e G', respectivamente. Seja $\pi : G \times G' \longrightarrow G/H \times G'/H'$ definida por $\pi(a, a') = (Ha, H'a')$. Mostre que π é um homomorfismo sobrejetor de grupos com Núcleo$(\pi) = H \times H'$. Conclua que $G \times G'/H \times H'$ é um grupo isomorfo a $G/H \times G'/H'$.

(c) Mostre que $e \times G'$ e $G \times e'$ são subgrupos normais de $G \times G'$.

(d) Seja $\varphi : G \times G' \longrightarrow G$ definida por $\varphi(a, a') = a$. Mostre que φ é um homomorfismo sobrejetor de grupos com Núcleo$(\varphi) = e \times G'$.

(e) Conclua que $G \times G'/e \times G'$ é um grupo isomorfo a G.

2. Classifique os grupos abelianos de ordens 18, 27 e 108.

3. Classifique os grupos de ordem 455.

4. Classifique os grupos de ordem $7^2 \times 11^2$.

5. Classifique os grupos abelianos G com $|\, G \,| \in \{8, 12, 36\}$.

6. Seja $(G, \cdot)$ um grupo abeliano finito. Seja m um inteiro que divide $|\, G \,|$. Mostre que existe um subgrupo K de G tal que $|\, K \,| = m$.

Nos grupos abelianos finitos vale a recíproca do Teorema de Lagrange.

7. Seja $(G, \cdot)$ um grupo isomorfo a $\mathbb{Z}_n \times \mathbb{Z}_m$, onde mdc$(m, n) = 1$. Mostre que G é cíclico.