LISTA DE TAREFAS PENDENTES

Motivação sobre grupos. 5
Teorema de Sylow 36
Grupos livres 36
Grupos Solúveis 36
Grupos Nilpotentes 36

ÁLGEBRA

José Antônio O. Freitas

Curso de Verão
DMA - UFV 2015

Notas de Aula[1]

SUMÁRIO

1 Grupos **5**

1.1 Definição e Propriedades 5

1.2 Subgrupos 9

1.3 Teorema de Lagrange 12

1.4 Subgrupos Normais e Grupos Quocientes 16

1.5 Homomorfismo de Grupos 19

1.6 Classes de Conjugação 26

1.7 Grupos Cíclicos 29

1.8 Grupos de Permutações 31

Bibliografia **37**

Índice Remissivo **39**

CAPÍTULO 1

GRUPOS

Texto introdutório

Motivação sobre grupos.

1.1 Definição e Propriedades

Definição 1.1. *Um **grupo** G é um conjunto não vazio munido com uma operação binária $*$ tal que*

(i) Para todo $x, y, z \in G$: $(x * y) * z = x * (y * z)$, isto é, a operação $*$ é associativa.

*(ii) Existe $e \in G$ tal que $x * e = e * x = x$ para todo $x \in G$. Tal elemento E é chamado de **elemento neutro** ou **unidade**.*

*(iii) Para cada $x \in G$, existe $y \in G$ tal que $x * y = y * x = e$. O elemento y é chamado de **inverso** de x e é denotado por $y = x^{-1}$.*

Denotamos um grupo G, cuja operação binária é $*$, por $(G, *)$. Quando $*$ é a soma, dizemos que $(G, *)$ é um grupo aditivo. Se $*$ é a multiplicação, dizemos que $(G, *)$ é um grupo multiplicativo. Caso não haja possibilidade de confusão em relação à operação do grupo, diremos simplesmente que G é um grupo.

Observação 1.1.1. *Para simplificar a notação vamos escrever $x * y = xy$ para x e y elementos de um grupo $(G, *)$.*

Definição 1.2. *Um grupo $(G, *)$ é chamado de **grupo comutativo** ou **abeliano** quando a operação $*$ é comutativa, ou seja, $x * y = y * x$ para todo $x, y \in G$.*

Exemplos 1.1.1. *(1) Grupos aditivos: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.*

(2) $(M_n(K), +)$ é um grupo abeliano;

(3) $(GL_n(K), \cdot)$, onde K é um corpo e $GL_n(K)$ denota as matrizes invertíveis com entradas em K. $GL_n(K)$ não é um grupo abeliano.

(4) Seja X um conjunto não vazio. Denote por $S_X = \{\sigma : X \to X \mid \sigma \text{ é uma bijeção}\}$. O conjunto S_X com a composição de funções é um grupo. No caso em que $X = \{1, 2, \ldots, n\}$, obtemos $S_n = \{(1), (12), (13), (23), (123), \ldots, (123\cdots n)\}$ o grupo das permutações em n elementos. Em geral, S_X não é abeliano.

(5) Para qualquer inteiro n seja

$$\mu_n = \{\zeta^k : 0 \leq k \leq n\}$$

onde $\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i\text{sen}\,(2\pi/n)$. Então μ_n é um grupo abeliano multiplicativo.

(6) Seja X um conjunto. Se U e V são subconjuntos de X defina

$$U - V = \{x \in U \mid x \notin V\}.$$

*O **grupo Boleano** $\mathcal{B}(X)$ é a família de todos os subconjuntos de X munido da **adição simétrica** $A + B$ onde*

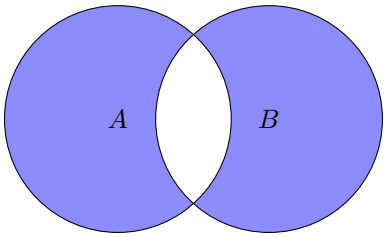
$$A + B = (A - B) \cup (B - A).$$

Assim $\mathcal{B}(X)$ é um grupo comutativo, o elemento neutro é $\emptyset$ e $A^{-1} = A$ pois $A + A = \emptyset$.

Lema 1.1.1. *Seja $(G, *)$ um grupo.*

(i) Vale a lei do cancelamento: se $x * a = x * b$ ou $a * x = b * x$, então $a = b$.

Figura 1.1: A soma $A + B$ é representada pela área em azul:



(ii) O elemento neutro é único.

(iii) Existe um único inverso para cada $x \in G$.

(iv) Para todos $x, y \in G$ temos $(x * y)^{-1} = y^{-1} * x^{-1}$. Por indução, $x_1, x_2, \ldots x_{n-1}, x_n \in G$

$$(x_1 * x_2 * \ldots * x_{n-1} * x_n)^{-1} = x_n^{-1} * x_{n-1}^{-1} * \ldots * x_2^{-1} * x_1^{-1}.$$

(v) Para todo $x \in G, (x^{-1})^{-1} = x$.

Definição 1.3. *Se G é um grupo e se $a \in G$, defina as **potências** a^n, para $n \geq 1$, como sendo*

$$a^1 = a \quad e \quad a^{n+1} = a^n a.$$

Definimos $a^0 = 1$ e se n é um inteiro positivo, definimos

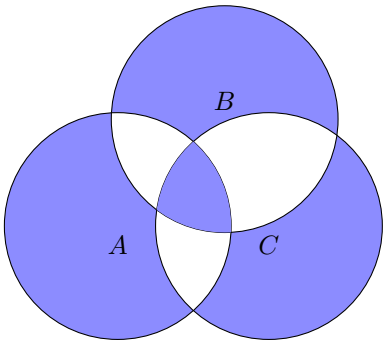
$$a^{-n} = (a^{-1})^n.$$

Lema 1.1.2. *Se G é um grupo e $a, b \in G$, então $(ab)^{-1} = b^{-1}a^{-1}$.*

Lema 1.1.3. *Sejam G um grupo, $a, b \in G$ e $m, n \geq 1$. Então*

$$a^{m+n} = a^m a^n$$
$$(a^m)^n = a^{mn}.$$

Figura 1.2: A associatividade é representada pela área em azul:



Proposição 1.1.1. *Sejam G um grupo, $a, b \in G$ e $m, n \in \mathbb{Z}$.*

(i) *Se a e b comutam, então $(ab)^n = a^n b^n$.*

(ii) $(a^m)^n = a^{mn}$

(iii) $a^m a^n = a^{m+n}$

Definição 1.4. *Seja G um grupo e $a \in G$. Se $a^k = 1$ para algum $k \geq 1$, então o menor expoente $k \geq 1$ é chamado de **ordem** de a. Se não existe tal potência, dizemos que a tem **ordem infinita**.*

Teorema 1.1. *Se $a \in G$ é um elemento de ordem n, então $a^m = 1$ se, e somente se, $n|m$.*

Prova: Suponha que $a^m = 1$. Assim pelo Algorítmo da Divisão de Euclides, existem inteiros q e r tais que

$$a^m = a^{nq+r}$$

onde $0 \leq r \leq n$. Assim

$$a^r = a^m a^{-nq} = 1.$$

Se $r > 0$, obtemos uma contradição com a ordem de a. Logo $r = 0$ e portanto $n|m$. Agora, se $n|m$, então

$$a^m = a^{nq} = 1$$

como queríamos. ♢

Proposição 1.1.2. *Se G é um grupo finito, então todo $x \in G$ tem ordem finita.*

Prova: Seja $x \in G$. Considere o conjunto $\{1, x, x^2, \ldots, x^n, \ldots\}$. Como G é finito, existem inteiros $m > n$ tais que $x^m = x^n$, isto é, $x^{m-n} = 1$. Portanto x tem ordem finita. ◊

1.2 Subgrupos

Definição 1.5. *Seja $(G, \cdot)$. Um conjunto não vazio H de G é um **subgrupo**, que denotaremos por $H \leq G$, quando com a operação de G, o conjunto H é um grupo, isto é, quando as condições seguintes são satisfeitas:*

(i) $h_1 h_2 \in H$ *para todos* $h_1, h_2 \in H$;

(ii) $1 \in H$;

(iii) Se $x \in H$, *então* $x^{-1} \in H$.

Proposição 1.2.1. *Um subconjunto H de um grupo G é um subgrupo se, e somente se, H é não vazio e para quaisquer $x, y \in H$ temos $xy^{-1} \in H$.*

Prova: A ida é imediata. Agora, suponha que H não é vazio e que $xy^{-1} \in H$ para todos $x, y \in H$. Assim tomando $x \in H$ temos $1 = xx^{-1} \in H$. Se $y \in H$, então $y^{-1} = 1y^{-1} \in H$ e finalmente se x e $y \in H$, então $xy = x(y^{-1})^{-1} \in H$. Portanto H é um subgrupo de G. ◊

Exemplos 1.2.1. *(1) Se G é um grupo, então $\{1\}$ e G são subgrupos de G chamados de **trivias**.*

(2) $(2\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$. De maneira geral, se n é um inteiro qualquer, então $(n\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$.

(3) O conjunto $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ é um subgrupo de S_4.

(4) Seja G um grupo qualquer. COnsidere o subconjunto

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

*Mostre que $Z(G) \leq G$. Este subgrupo $Z(G)$ é chamado de **centro** de G. O grupo G é abeliano se, e só se, $Z(G) = G$.*

Proposição 1.2.2. *Um conjunto não vazio de um grupo finito G é um subgrupo de G se, e somente se, H é fechado, isto é, se dados a e $b \in H$, então $ab \in H$. Em particular, um subconjunto não vazio de S_n é um subgrupo se, e somente se, é fechado.*

Prova: A ida é imediata. Para a volta, como G é finito todos os seus elementos têm ordem finita. Dado $x \in H$, então existe um inteiro n tal que $x^n = 1$. Assim $1 \in H$, pois H é fechado. Além disso, $x^{-1} = x^{n-1} \in H$. Finalmente, se x e $y \in H$, então $xy^{-1} = xy^{m-1} \in H$, onde m é um inteiro tal que $y^m = 1$. Portanto H é um subgrupo de G. ◊

Observações 1.2.1. *(1) A Proposição 1.2.2 pode falhar se G for um grupo infinito. Por exemplo, seja $G = \mathbb{Z}$ o grupo aditivo dos inteiros. O conjunto $H = \mathbb{N}$ é fechado, mas não é um subgrupo de $\mathbb{Z}$.*

(2) Para Galois, 1830, um grupo era simplesmente um conjunto fechado H de S_n. Foi A. Cayley, em 1854 o primeiro a definir um grupo abstrato mencionando explicitamente a associatividade, o inverso e elemento neutro.

Vamos fixar algumas notações: se H e K são subconjuntos de um grupo G (em particular, se H e K são subgrupos de G) definimos

$$HK = \{hk \mid h \in H\, k \in K\}$$
$$H^{-1} = \{h^{-1} \mid h \in H\}.$$

Em geral HK não é um subgrupo de G, mesmo quando H e K o são. (Apresente alguns exemplos!)

Dado um subconjunto não vazio S de G, denotamos

$$\langle S \rangle = \{a_1 \dots a_n \mid n \in \mathbb{N}, a_i \in S \text{ ou } a_i \in S^{-1}\}.$$

Quando o conjunto S for finito, digamos $S = \{a_1, \dots, a_n\}$ escreveremos

$$\langle \{a_1, \dots, a_n\} \rangle = \langle a_1, \dots, a_n \rangle.$$

Quando $g \in G$ escrevemos

$$\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\} = \{g^t \mid t \in \mathbb{Z}\}.$$

Proposição 1.2.3. *Sejam G um grupo e S um subconjunto não vazio de G. Então o conjunto $\langle S\rangle$ é um subgrupo de G.*

Prova: Como $S \neq \emptyset$, então $1 \in \langle S\rangle$. Dados $x, y \in S$ temos

$$x = a_1 a_2 \dots a_m$$
$$y = b_1 b_2 \dots b_n$$

com $a_i, b_j \in S$ ou $a_i, b_j \in S^{-1}$ para todo i e todo j. Logo $y^{-1} = b_n^{-1} \dots b_2^{-1} b_1^{-1}$ para todo j, daí

$$xy^{-1} = a_1 \dots a_m b_n^{-1} \dots b_2^{-1} b_1^{-1} \in \langle S\rangle.$$

Portanto $\langle S\rangle$ é um subgrupo de G. ◊

Definição 1.6. *Sejam G um grupo e S um subconjunto não vazio de G. Então $\langle S\rangle$ é chamado de* ***subgrupo gerado*** *por S.*

Definição 1.7. *Um grupo é* ***cíclico*** *quando ele pode ser gerado por um elemnto, isto é, quando $G = \langle g\rangle$ para algum $g \in G$.*

Definição 1.8. *A* ***ordem*** *de um grupo G é o número de elementos em G.*

Proposição 1.2.4. *Seja G um grupo finito e seja $\alpha \in G$. Então a ordem de α é igual ao número de elementos em $\langle\alpha\rangle$, isto é,*

$$|\alpha| = |\langle\alpha\rangle|.$$

Prova: Como G é finito, existe um menor inteiro $k \geq 1$ tal que $1, \alpha, \alpha^2, \dots, \alpha^{k-1}$ são todos as potências distintas de α, enquanto que em $1, \alpha, \alpha^2, \dots, \alpha^{k-1}, \alpha^k$ temos repetições de potências. Daí $\alpha^k = \alpha^i$ para algum $0 \leq i \leq k-1$. Se $i \geq 1$, então $\alpha^{k-i} = 1$, o que contradiz a escolha de k. Logo $a^k = a^0 = 1$ e assim k é a ordem de α.

Agora seja $H = \{1, \alpha, \alpha^2, \dots, \alpha^{k-1}\}$. Então $|H| = k$. Seja $\alpha^i \in \langle\alpha\rangle$, com $i \in \mathbb{Z}$. Pelo Algorítmo da Divisão de Euclides, existem $q, r \in \mathbb{Z}$ tais que $i = qk + r$, com $0 \leq r < k$. Assim $\alpha^i = \alpha^{qk}\alpha^r = \alpha^r \in H$, isto é, $\langle\alpha\rangle \subseteq H$. Como $H \subseteq \langle\alpha\rangle$ pela definição de H, então $H = \langle\alpha\rangle$. Portanto,

$$|\alpha| = |\langle\alpha\rangle|$$

como queríamos. ◊

Teorema 1.2. *Se $G = \langle a \rangle$ é um grupo cíclico de ordem n, então a^k é um gerador de G se, e somente se, $mdc(k, n) = 1$.*

Prova: Se a^k é um gerador de G, então $a = a^{kt}$ para algum $t \in \mathbb{Z}$. Daí $a^{kt-1} = 1$ e então pelo Teorema 1.1, $n|(kt - 1)$, isto é, $nu = kt - 1$ para algum $u \in \mathbb{Z}$. Logo, $mdc(k, n) = 1$.

Agora, se $mdc(k, n) = 1$, então existem $p, q \in \mathbb{Z}$ tais que $kp + nq = 1$. Daí

$$a = a^{kp+nq} = a^{nq}(a^k)^p = (a^k)^p$$

e então $G = \langle a \rangle$. ◊

Definição 1.9. *O subgrupo $\langle \{xyx^{-1}y^{-1} \mid x, y \in G\} \rangle$ é o **subgrupo dos comutadores** do grupo G. Ele será denotado por G'. Note que G é abeliano se, e somente se, $G' = \{1\}$.*

1.3 Teorema de Lagrange

Sejam G um grupo e H um subgrupo de G. Sobre G defina a relação $\sim_E$ da seguinte maneira

$$y \sim_E x \text{ se, e somente se, exite } h \in H \text{ tal que } y = xh.$$

É imediato verificar que $\sim_E$ é uma relação de equivalência. Dado $x \in G$ a classe de equivalência de x é o conjunto

$$xH = \{y \in G \mid y \sim_E x\} = \{xh \mid h \in H\}$$

que chamaremos de **classe lateral à esquerda** de H em G. Quando não houver chance de confusão, diremos simplesmente classe lateral de x à esquerda. Observe que $y \in xH$ se, e só se, $yH = xH$.

Analogamente, podemos definir a seguinte relação de equivalência:

$$y \sim_D x \text{ se, e somente se, exite } h \in H \text{ tal que } y = hx.$$

Obtemos assim as **classes laterais à direita** de H em G. A classe lateral de x à direita é dada por

$$Hx = \{y \in G \mid y \sim_D x\} = \{hx \mid h \in H\}.$$

Definição 1.10. *Dado um grupo G e H um subgrupo de G, o conjunto das classes laterais à esquerda de H em G é denotado por*

$$\left(\frac{G}{H}\right)_E = \{xH \mid x \in G\}.$$

Analogamente, definimos

$$\left(\frac{G}{H}\right)_D = \{Hy \mid y \in G\}.$$

Definição 1.11. *A cardinalidade do conjunto das classes laterais à esquerda, $(G/H)_E$, é o* ***índice*** *de H em G e será denotado por $[G : H]$.*

Observação 1.3.1. *O índice de H em G também é a cardinalidade do conjunto das classes laterais à direita de H em G. De fato, é imediato verificar que a aplicação*

$$\begin{aligned} \varphi : \left(\frac{G}{H}\right)_E &\to \left(\frac{G}{H}\right)_D \\ xH &\mapsto Hx^{-1} \end{aligned}$$

está bem definida e é uma bijeção.

Proposição 1.3.1. *Todas as classes laterais de H em G têm a mesma cardinalidade, igual à cardinalidade de H.*

Prova: Basta verificar que a aplicação

$$\begin{aligned} \varphi : H &\to \left(\frac{G}{H}\right)_E \\ x &\mapsto xH \end{aligned}$$

é uma bijeção. ◊

Teorema 1.3 (Teorema de Lagrange)**.** *Sejam G um grupo finito e H um subgrupo de G. Então*

$$|G| = |H|[G : H],$$

em particular, a ordem e o índice de H dividem a ordem de G.

Prova: Seja $\{a_1H, a_2H, \ldots, a_tH\}$ a família de todas as classes laterais distintas de H em G. Então

$$G = a_1H \cup a_2H \cup \cdots \cup a_tH$$

e assim

$$|G| = |a_1H| + |a_2H| + \cdots + |a_tH|.$$

Mas, $|H| = |a_iH|$ para todo $i = 1, \ldots, t$, onde $t = [G : H]$. Portanto

$$|G| = |H|[G : H]$$

como queríamos. ◊

Corolário 1.3.1. *Sejam G um grupo finito e $\alpha \in G$. Então a ordem de α divide a ordem de G.*

Prova: Segue da Proposição 1.2.4 pois $|\alpha| = |\langle\alpha\rangle|$. ◊

Corolário 1.3.2. *Seja G um grupo. Se $K \leq H \leq G$ com $K \trianglelefteq G$ e $H \trianglelefteq G$, então*

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

Prova: A prova é deixada para o leitor. ◊

Corolário 1.3.3. *Se G é um grupo finito, então $a^{|G|} = 1$ para todo $a \in G$.*

Prova: Se a possui ordem, então pelo Corolário 1.3.1, devemos ter $|G| = dm$ para algum $m \geq 1$. Logo $a^{|G|} = a^{dm} = 1$. ◊

Corolário 1.3.4. *Se p é um número primo, então todo grupo G de ordem p é cíclico.*

Prova: Se $a \in G$, $a \neq 1$, então a tem ordem $d > 1$, o que é impossível. Logo $G = \langle a\rangle$. ◊

Proposição 1.3.2. *Seja G um grupo abeliano.*

(i) Se $a, b \in G$ são dois elementos de ordem finita tais que $mdc\{|a|, |b|\} = 1$, então $|ab| = |a||b|$.

(ii) Se $r := sup\{|g| : g \in G\}$ é finito, então $|x|$ divide r para cada $x \in G$.

Prova:

(i) Sejam $|a| = m$, $|b| = n$ e $z = |ab|$. Como a e b comutam, temos $(ab)^{mn} = (a^m)^n(b^n)^m = 1$. Logo z é um divisor de mn. Agora, $(ab)^z = 1$, daí $a^z = b^{-z} \in \langle a\rangle \cap \langle b\rangle$. Mas $mdc(m,n) = 1$, logo $\langle a\rangle \cap \langle b\rangle = \{1\}$. Então $a^z = b^z = 1$ e portanto z é um múltiplo de m e de n. Como m e n são relativamente primos, z é um múltiplo de mn. Portanto, $z = mn$ como queríamos.

(ii) Inicialmente vamos provas a seguinte afirmação:

"Se a, $b \in G$ são dois elementos de ordem finita, então existe $c \in G$ tal que $|c| = mmc\{|a|, |b|\}$."

Sejam $m = |a|$ e $n = |b|$. Se $mdc(m,n) = 1$, então pelo item anterior podemos tomar $c = ab$. Se $mdc(m,n) \neq 1$, escreva

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}} \cdots p_t^{\alpha_t}$$
$$m = p_1^{\beta_1} \cdots p_k^{\beta_k} p_{k+1}^{\beta_{k+1}} \cdots p_t^{\beta_t}$$

onde $0 \leq \alpha_i < \beta_i$ para $i = 1, \ldots, k$, $\alpha_j \geq \beta_j \geq 0$ para $j = k+1, \ldots, t$ e os primos p_i são todos distintos.

Considere os elementos

$$a_1 = a^{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}$$
$$b_1 = b^{p_{k+1}^{\beta_{k+1}} \cdots p_t^{\beta_t}}.$$

Assim

$$|a_1| = p_{k+1}^{\alpha_{k+1}} \cdots p_t^{\alpha_t}$$
$$|b_1| = p_1^{\beta_1} \cdots p_k^{\beta_k}.$$

e então $mdc\{|a_1|, |b_1|\} = 1$ e pelo item anterior basta tomar $c = a_1 b_1$. Logo a afirmação está provada.

Para provar o item b), suponha que $r := sup\{|g| \mid g \in G\}$ é finito e tome $y \in G$ tal que $|y| = r$. Suponha que existe $x \in G$ tal que $|x|$ não divide $|y|$. Assim $s = mdc\{|x|, |y|\} > r$ e pela afirmação anterior existe $x \in \langle x, y\rangle \subseteq G$ tal que $|c| = s > r$, o que contradiz a definição de r.

◊

Proposição 1.3.3. *Seja G um grupo e sejam $K < H < G$. Então*

$$[G : K] = [G : H][H : K].$$

1.4 Subgrupos Normais e Grupos Quocientes

Sejam G um grupo e H um subgrupo de G. Considere o conjunto das classes laterais à esquerda de H em G:

$$\left(\frac{G}{H}\right) = \{xh \mid x \in G\}.$$

Queremos definir uma operação em G/H de modo que este conjunto se torne um grupo. O meio natural de fazer isso é definindo

$$(xH) \cdot (yH) = (xy)H \tag{1.1}$$

onde x , $y \in G$. Como uma mesma classe lateral possui vários representantes distintos, precisamos garantir que esta operação está bem definida, isto é, se escolhermos outros representantes das classes xH e yH o resultado não se altera. Para isso sejam x, $y \in G$ e h, $k \in H$. Então x e xh são representantes da mesma classe xH, y e yH são representantes da mesma classe yH. Assim precisamos ter

$$xyH = xhykH,$$

para todos x, $y \in G$ e para todos y, $k \in H$. Isto é, devemos ter

$$\begin{aligned} y^{-1}x^{-1}xyH &= y^{-1}x^{-1}xhykH \\ H &= y^{-1}hyH \end{aligned}$$

para todo $y \in G$ e $h \in H$. Portanto a operação (1.1) está bem definida em G/H se, e somente se,

$$y^{-1}hy \in H$$

para todo $y \in G$ e todo $h \in H$.

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

(i) *a operação (1.1) está bem definida;*

(ii) $g^{-1}Hg \subseteq H$, *para todo* $g \in G$;

(iii) $g^{-1}Hg = H$, *para todo* $g \in G$;

(iv) $gH = Hg$, *para todo* $g \in G$.

Prova: $(i) \Leftrightarrow (ii)$ Já foi feito.

$(iii) \Leftrightarrow (iv)$ Imediato.

$(iii) \Rightarrow (ii)$ Imediato.

$(ii) \Rightarrow (ii)$ Suponha que $gHG^{-1} \subseteq H$ para todo $g \in G$. Sejam $h \in H$ e $g \in G$. Temos

$$h = g^{-1}(ghg^{-1})g \in g^{-1}(gHg^{-1})g \subseteq g^{-1}Hg,$$

como queríamos. ◊

Definição 1.12. *Um subgrupo H é um* ***subgrupo normal*** *de G, e escrevemos $H \trianglelefteq G$, se ele satisfaz as afirmações equivalentes da Proposição 1.4.1. Neste caso, como as classes laterais à esquerda de H são iguais às classes laterais à direita de H, vamos chamá-las simplesmente de* ***classes laterais*** *de H.*

Exemplos 1.4.1. *(1)* $\{1\}$ *e G são subgrupos normais de G.*

(2) $Z(G) \trianglelefteq G$. *Mais geralmente, se* $H \leq Z(G)$, *então* $H \trianglelefteq G$.

(3) $G' = \{xyx^{-1}y^{-1} \mid x, y \in G\}$ *é um subgrupo normal de G.*

(4) Se $[G : H] = 2$, *então* $H \trianglelefteq G$.

(5) Se G é abeliano, então todo subgrupo de G é normal.

Teorema 1.4. *Seja G um grupo e seja H um subgrupo normal de G. Então o conjunto das classes laterais, com o operação induzida de G, é um grupo.*

Definição 1.13. *Sejam G um grupo e H um subgrupo normal de G. O grupo de suas classes laterais, com a operação induzida de G, é chamado de* ***grupo quociente*** *de G por H e será denotado por $\frac{G}{H}$ ou G/H.*

Proposição 1.4.2. *Se G é um grupo finito tal que para todo $g \in G$, $g^2 = 1$, então $|G| = 2^k$ para algum $k \in \mathbb{N}$.*

Prova: Como $g^2 = 1$, para todo $g \in G$, então G é abeliano e assim todos os seus subgrupos são normais.

Se $|G| = 1$, nada há a fazer. Suponha então que o resultado seja válido para todo grupo G de ordem menor que $|G| = n > 1$. Tome $g \in G$, $g \neq 1$. Sabemos que $g^2 = 1$, assim $H = \langle g \rangle = \{1, g\}$ e H é normal em G. Considere o grupo $(G/H, \cdot)$. Um vez que $x^2 = 1$, então $(xH)^2 = x^2H = H$, isto é, para todo $xH \in G/H$, vale que $(xH)^2 = \bar{1}$. Além disso,

$$\left|\frac{G}{H}\right| = [G : H] = \frac{n}{2} < n.$$

Logo pela hipótese de indução, $|G/H| = 2^{k-1} = n/2$. Portanto, $|G| = n = (n/2)2 = 2^k$, como queríamos. ◊

Proposição 1.4.3. *Se G é um grupo com $|G| = 2p$, p primo ímpar, então*

$$G = \{1, a, b, b^2, \ldots, b^{p-1}, ab, ab^2, \ldots, ab^{p-1}\}$$

onde $|a| = 2$, $|b| = p$ e $ab = b^i a$ com $i = 1$ ou $i = p - 1$.

Prova: Como $|G| = 2p$, que é par, existe $a \in G$, $a \neq 1$ tal que $a^2 = 1$, isto é, $a = a^{-1}$. Agora, pela Proposição 1.4.2, existe $c \in G$ tal que $|c| = p$ ou $|c| = 2p$. Se $|c| = 2p$, então $|c^2| = p$. Logo existe $b \in G$ tal que $|b| = p$. Seja $H = \langle b \rangle$. Como $[G : H] = 2$, então $H \trianglelefteq G$. Assim para $a \in G$ e $b \in H$ temos $aba^{-1} \in H$. Consequentemente, existe $1 \leq i \leq p - 1$ tal que $aba^{-1} = b^i$. É fácil verificar que $(aba^{-1})^n = b^{ni}$ para todo n. Então como $|a| = 2$

$$b^{i^2} = (aba^{-1})^i = ab^i a^{-1} = b,$$

ou seja, $b^{i^2} - 1 = 1$. Mas $|b| = p$, daí $p|(i^2 - 1)$. Logo $p|(i - 1)$ ou $p|(i + 1)$. Como $1 \leq i \leq p - 1$, então $i = 1$ ou $i = p - 1$.

Agora, $[G : H] = 2$, então $G = H \cup aH$ pois $|a| = 2$, $|b| = p$ e p é um primo ímpar. Portanto,

$$G = \{1, a, b, b^2, \ldots, b^{p-1}, ab, ab^2, \ldots, ab^{p-1}\}$$

onde $ab = b^i a$ com $i = 1$ ou $i = p - 1$. ◊

Observação 1.4.1. *No caso em que $i = 1$, obtemos um grupo abeliano cíclico de ordem $2p$. E no caso em que $i = p - 1$, temos um grupo não abeliano chamado **grupo dihedral** de ordem $2p$.*

Notação 1.13.1. *No caso geral, o grupo G da Proposição 1.4.3 será denotado por*

$$D_{2n} = \langle a, b \mid a^2 = b^n = 1, ab = b^{n-1}a \rangle = \{1, a, b, \ldots, b^{n-1}, ab, \ldots, ab^{n-1}\}. \tag{1.2}$$

*E é chamado de **grupo dihedral** de ordem $2n$. Em alguns casos, utiliza-se também a notação D_n para o grupo (1.2)*

Proposição 1.4.4. *Sejam G um grupo e G' seu subgrupo dos comutadores. Então,*

(i) G/G' é abeliano.

(ii) G' é o menor subgrupo normal de G com esta propriedade, isto é, se $H \trianglelefteq G$ é tal que G/H é abeliano, então $G' \subseteq H$.

Proposição 1.4.5. *Sejam G um grupo e $Z(G)$ seu centro. Se o quociente $G/Z(G)$ é cíclico, então $G = Z(G)$. Em particular, o índice de $Z(G)$ em G nunca é igual a um número primo.*

Prova: Seja $\overline{z}$ um gerador de $G/Z(G)$. Dado $g \in G$, existe $i \in \mathbb{Z}$ tal que $\overline{g} = \overline{z}^i$. Logo $g = z^i h$ para algum $h \in Z(G)$. Sejam $g_1, g_2 \in G$, com $g_1 = z^i h_1$ e $g_2 = z^j h_2$, para alguns $i, j \in \mathbb{Z}$ e $h_1, h_2 \in H$. Assim

$$g_1 g_2 = z^i h_1 z^j h_2 = z^{i+j} h_1 h_2 = z^j h_2 z^i h_1 = g_2 g_1.$$

Portanto G é abeliano, isto é, $G = Z(G)$ ◊

1.5 Homomorfismo de Grupos

Definição 1.14. *Se $(G, \cdot)$ e $(H, *)$ são grupos, então a aplicação $\phi : G \to H$ é um **homomorfismo de grupos** se*

$$\phi(x \cdot y) = \phi(x) * \phi(y) \tag{1.3}$$

para todos $x, y \in G$. Se ϕ também é uma bijeção, então ϕ é chamada de um ***isomorfismo****. Os grupos G e H são chamados de* ***isomorfos*** *e escrevemos $G \cong H$, se existe um isomorfismo $\phi : G \to H$.*

Exemplos 1.5.1. *(1) $Id : G \to G$ tal que $Id(g) = g$ é o homomorfismo* ***identidade****.*

(2) $e : G \to H$ tal que $e(g) = 1_H$ é o homomorfismo ***trivial****.*

(3) Seja $n \in \mathbb{Z}$ fixo. Então $\phi_n : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ tal que $\phi_n(z) = nz$ é um homomorfismo. De modo geral, se G é um grupo abeliano, então $\phi_n : (G, \cdot) \to (G, \cdot)$ tal que $\phi_n(g) = g^n$ é um homomorfismo.

(4) Seja $H \trianglelefteq G$, então $\pi : G \to G/H$ tal que $\pi(g) = gH$ é um homomorfismo chamado de ***projeção canônica****.*

(5) Seja $g \in G$ fixo. Então $\phi_g : G \to G$ tal que $\phi_g(x) = gxg^{-1}$ é um isomorfismo.

Lema 1.5.1. *Seja $\phi : G \to H$ um homomorfismo de grupos.*

(i) $\phi(1_G) = 1_H$

(ii) $\phi(g^{-1}) = (\phi(g))^{-1}$

(iii) $\phi(g^n) = (\phi(g))^n$ *para todo* $n \in \mathbb{Z}$.

Prova: Exercício. ◊

Lema 1.5.2. *Sejam G e H grupos e $\phi : G \to H$ um homomorfismo. Então:*

(i) O conjunto $\ker \phi = \{x \in G \mid \phi(x) = 1_H\}$ *é um subgrupo normal de G chamado de* ***núcleo*** *ou* ***kernel*** *de ϕ.*

(ii) O conjunto $\operatorname{Im} \phi = \{y \in H \mid y = \phi(x)$ *para algum* $x \in G\}$ *é um subgrupo de H chamado de* ***imagem*** *de ϕ.*

(iii) Sejam $\phi : (G, \cdot) \to (H, *)$ e $\psi : (H, *) \to (\mathcal{G}, \times)$ dois homomorfismos de grupos. Então a composição $\psi \circ \phi : (G, \cdot) \to (\mathcal{G}, \times)$ é um homomorfismo.

Prova: Exercício. ◊

Lema 1.5.3. *Seja $\phi : G \to H$ um homomorfismo de grupos.*

(i) Se $P \leq G$, então $\phi(P) \leq H$ e $\phi^{-1}(\phi(P)) = P \ker\phi$.

(ii) Se $R \leq H$, então $\phi^{-1}(R)$ é um subgrupo de G contendo $\ker\phi$ e $\phi(\phi^{-1}(R)) = R \cap \operatorname{Im}\phi$.

Prova:

(i) A prova de que $\phi(P)$ é um subgrupo de H é deixada para o leitor. Provemos que $\phi^{-1}(\phi(P)) = P\ker\phi$. Seja $xk \in P$. Temos

$$\phi(xk) = \phi(x)\phi(k) = \phi(x) \in \phi(P)$$

daí $P\ker\phi \subseteq \phi^{-1}(\phi(P))$. Agora, seja $y \in \phi^{-1}(\phi(P))$. Por definição, $\phi(y) \in \phi(P)$ e assim existe $x \in P$ tal que $\phi(x) = \phi(y)$. Isto é, $\phi(x^{-1}y) = 1_H$, donde $x^{-1}y \in \ker\phi$. Logo $y = x(x^{-1}y) \in P\ker\phi$. Portanto, $\phi^{-1}\phi(P) = P\ker\phi$.

(ii) Como $R \leq H$, então $1_H \in R$ e como $\phi(x) = 1_H$ para todo $x \in \ker\phi$, então $\ker\phi \subseteq \phi^{-1}(R)$. Fica a cargo do leitor provar que $\phi^{-1}(R)$ é um subgrupo de G. Provemos que $\phi(\phi^{-1}(R)) = R \cap \operatorname{Im}\phi$.

A inclusão $\phi(\phi^{-1}(R)) \subseteq R \cap \operatorname{Im}\phi$ é imediata. Agora, seja $y \in R \cap \operatorname{Im}\phi$. Assim existe $x \in G$ tal que $\phi(x) = y$. Mas $y \in R$, daí $x \in \phi^{-1}(R)$ e então $y = \phi(x) \in \phi(\phi^{-1}(R))$. Portanto, $\phi(\phi^{-1}(R)) = R \cap \operatorname{Im}\phi$.

◊

Exemplos 1.5.2. *(1) O grupo dihedral D_6 é dado por*

$$D_6 = \langle a, b \mid a^2 = b^3 = 1,\ ab = b^2a\rangle.$$

Agora, $S_3 = \{id, \alpha, \beta, \beta^2, \alpha\beta, \alpha\beta^2\}$ onde

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

A aplicação $\phi : S_3 \to D_6$ tal que

$$\begin{aligned}\phi(id) &= 1\\ \phi(\alpha) &= a\\ \phi(\beta) &= b\\ \phi(\alpha\beta) &= ab\\ \phi(\alpha\beta^2) &= ab^2\end{aligned}$$

é um homomorfismo bijetor. Portanto $S_3 \cong D_6$.

(2) *Seja $G = \langle a\rangle = \{\ldots, a^{-1}, 1, a, a^2, \ldots\}$ um grupo cíclico infinito. É fácil verificar que $\phi : (\mathbb{Z}, +) \to (G, \cdot)$ dada por $\phi(t) = a^t$ é um isomorfismo. Portanto $\mathbb{Z} \cong G$.*

Teorema 1.5 (Teorema do Isomorfismo)**.** *Seja $\phi : (G, \cdot) \to (H, *)$ um homomorfismo de grupos.*

(i) A função

$$\begin{aligned}\overline{\phi} : \frac{G}{\ker\phi} &\to \phi(G)\\ a\ker\phi &\mapsto \phi(a)\end{aligned}$$

é um isomorfismo.

(ii) As seguintes funções

$$\begin{aligned}\{\textit{subgrupos de } G \textit{ que contêm } \ker\phi\} &\longleftrightarrow \{\textit{subgrupos de } \phi(G)\}\\ P &\xmapsto{\ \psi\ } \phi(P)\\ \phi^{-1}(R) &\xmapsto{\ \sigma\ } R\end{aligned}$$

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

(a) Se $P \trianglelefteq G$, então $\phi(P) \trianglelefteq \phi(G)$.

(b) Se $R \trianglelefteq \phi(G)$, então $\phi^{-1}(R) \trianglelefteq G$.

Prova:

(i) Inicialmente precisamos verificar que $\overline{\phi}$ está bem definida. Para isso sejam $a_1 \ker\phi = a_2 \ker\phi$. Assim $a_1 = a_2 k$, onde $k \in \ker\phi$. Então

$$\phi(a_1) = \phi(a_2 k) = \phi(a_2),$$

logo $\overline{\phi}(a_1 \ker\phi) = \overline{\phi}(a_2 \ker\phi)$ e então $\overline{\phi}$ está bem definida. Além disso, da definição de $\overline{\phi}$ vemos que esta aplicação é sobrejetora.

Agora, sejam $a_1 \ker\phi$, $a_2 \ker\phi \in \ker\phi$. Então

$$\overline{\phi}((a_1 \ker\phi)(a_2 \ker\phi)) = \overline{\phi}((a_1 a_2)\ker\phi) = \phi(a_1 a_2) = \phi(a_1)\phi(a_2) = \overline{\phi}(a_1 \ker\phi)\overline{\phi}(a_2 \ker\phi)$$

e daí $\overline{\phi}$ é um homomorfismo. Finalmente, se $a \ker\phi \in \ker\overline{\phi}$ então

$$\overline{\phi}(a \ker\phi) = \overline{\phi}(1_G \ker\phi)$$

daí $\phi(g) = \phi(1_G) = 1_H$, ou seja, $g \in \ker\phi$. Portanto $\ker\overline{\phi} = \{\ker\phi\}$ e então $\overline{\phi}$ é injetora. Portanto $\overline{\phi}$ é um isomorfismo de grupos. Logo

$$\frac{G}{\ker\phi} \cong \phi(G).$$

(ii) Pelo Lema 1.5.3 sabemos que $\phi^{-1}(\phi(P)) = P\ker\phi$ para todo $P \leq G$ e que $\phi(\phi^{-1}(R)) = R \cap \phi(G)$ para todo $R \leq H$. Assim se $\ker\phi \subseteq P$, então $\phi^{-1}(\phi(P)) = P$ e se $R \leq \phi(G)$, então $\phi(\phi^{-1}(R)) = R$. Logo as funções ψ e σ são inversas uma da outra, isto é, são bijeções.

Agora falta provar os demais itens:

(a) Sejam $a \in \phi(P)$ e $b \in \phi(G)$. Então existem $x \in P$ e $y \in G$ tais que $\phi(x) = a$ e $\phi(y) = b$. Queremos mostrar que $b^{-1}ab \in \phi(P)$. De fato,

$$b^{-1}ab = \phi(y^{-1})\phi(x)\phi(y) = \phi(y^{-1}xy) \in \phi(P)$$

pois $P \trianglelefteq G$. Portanto, $\phi(P) \trianglelefteq \phi(G)$.

(b) Dados $a \in G$ e $x \in \phi^{-1}(R)$, queremos mostrar que $a^{-1}xa \in \phi^{-1}(R)$. Temos

$$\phi(a^{-1}xa) = \phi(a)^{-1}\phi(x)\phi(a) \in R$$

pois $R \trianglelefteq \phi(G)$. Logo $a^{-1}xa \in \phi^{-1}(R)$, isto é, $\phi^{-1}(R) \trianglelefteq G$, como queríamos.

◊

Corolário 1.5.1. *Seja $\phi : G \to H$ um homomorfismo de grupos e seja $K \leq G$. Então a função*

$$\begin{aligned} \psi : \frac{K}{K \cap \ker \phi} &\to \phi(K) \\ a(K \cap \ker \phi) &\mapsto \phi(a) \end{aligned}$$

é um isomorfismo.

Prova: Considere o hommorfismo ϕ restrito a K;

$$\begin{aligned} \psi := \phi|_K : K &\to H \\ h &\mapsto \phi(h). \end{aligned}$$

É imediato verificar que $\psi(K) = \phi(K)$ e que $\ker \psi = \ker \phi$. Logo pelo Teorema do Isomorfismo, Teorema 1.5, temos $K/\ker \psi \cong \psi(K)$, isto é,

$$\frac{K}{K \cap \ker \phi} \cong \phi(K).$$

◊

Corolário 1.5.2. *Seja H um subgrupo normal de G. Então a função*

$$\{\textit{subgrupos (normais) de } G \textit{ que contêm } H\} \longleftrightarrow \{\textit{subgrupos (normais) de } G/H\}.$$

é uma bijeção.

Prova: É fácil verificar que $\phi : G \to G/H$ dada por $\phi(a) = aH$ é um homomorfismo sobrejetivo. Aplicando a segunda parte do Teorema do Isomorfismo, Teorema 1.5, obtemos o resultado. ◊

Teorema 1.6 (Teorema da Representação)**.** *Seja G um grupo e H um subgrupo de G tal que $[G : H] = n$. Então existe $N \subseteq H$, com $N \trianglelefteq G$ tal que G/N é um grupo isomorfo a um subgrupo de S_n. Mais ainda, N é o "maior" subgrupo normal de G que está contido em H.*

Prova: Seja $S = G/H = \{Hx_1, \ldots, Hx_n\}$ e $\mathcal{P}(S)$ o grupo das permutações do conjunto S. É claro que $\mathcal{P}(S) \cong S_n$.

Considere a seguinte aplicação

$$\psi : G \to \mathcal{P}(S)$$
$$a \mapsto \psi_a$$

onde $\psi_a : S \to S$ é tal que $\psi_a(Hx_i) = Hx_i a^{-1}$.

Inicialmente para $a \in G$ temos $\psi_a(Hx_i) = \psi_a(Hx_j)$ se, e só se, $Hx_i a^{-1} = Hx_j a^{-1}$. Isto é, $Hx_i = Hx_j$, logo ψ_a é injetora. Como $|S| = n$, então ψ_a é sobrejetiva e daí $\psi_a \in \mathcal{P}(S)$. Logo $\psi_a \in \mathcal{P}(S)$ para todo $a \in G$.

Verifiquemos agora que ψ é um homomorfismo de grupos. Dados $a, b \in G$ queremos mostrar que $\psi(ab) = \psi(a)\psi(b)$. Mas $\psi(ab) = \psi_{ab}$. Seja $Hx_i \in S$. Temos

$$\psi_{ab}(Hx_i) = Hx_i(ab)^{-1} = (Hx_i b^{-1})a^{-1} = \psi_a(\psi_b(Hx_i)) = (\psi_a \circ \psi_b)(Hx_i).$$

Portanto ψ é um homomorfismo de grupos.

Agora,

$$\ker \psi = \{a \in G \mid \psi(a) = Id_S\} = \{a \in G \mid Hx_i a^{-1} = Hx_i, i = 1, \ldots, n\}.$$

Daí $a \in \ker \psi$ se, e só se, $Hx_i a^{-1} = Hx_i$ para todo $i = 1, \ldots, n$. Mas isso ocorre se, e só se, $Hx_i = Hx_i a$ para todo $i = 1, \ldots, n$. Logo $a \in \ker \psi$ se, e só se, $H = Hx_i a x_i^{-1}$ para todo $i = 1, \ldots, n$. Daí $a \in \ker \psi$ se, e só se, $x_i a x_i^{-1} \in H$ para todo $i = 1, \ldots, n$ e então $a \in \ker \psi$ se, e só se, $a \in x_i^{-1} H x_i$ para todo $i = 1, \ldots, n$. Mas $G = Hx_1 \cup \cdots \cup Hx_n$, uma união disjunta e como $(hx_i)^{-1} H (hx_i) = x_i^{-1} H x_i$ para todo $h \in H$, então $a \in \ker \psi$ se, e só se, $a \in x^{-1} H x$ para todo $x \in G$. Ou seja, $a \in \ker \psi$ se, e somente se, $a \in \cap_{x \in G}(x^{-1} H x)$. Portanto $\ker \psi = \cap_{x \in G}(x^{-1} H x)$.

Seja $N = \ker \psi$. Então $N \trianglelefteq G$ e $N \subseteq H$. Agora, seja $L \trianglelefteq G$ tal que $L \subseteq H$. Então $x^{-1} L x = L \subseteq x^{-1} H x$ para todo $x \in G$. Assim, $L \subseteq N = \cap_{x \in G}(x^{-1} H x)$. Portanto N é o "maior" subgrupo normal de G contido em H.

Finalmente pelo Teorema do Isomorfismo, Teorema 1.5, temos

$$\frac{G}{\ker \psi} = \frac{G}{N} \cong \psi(G) \leq \mathcal{P}(S) \cong S_n,$$

como queríamos. ◊

Corolário 1.5.3 (Teorema de Cayley)**.** *Se G é um grupo de ordem n, então G é isomorfo a um subgrupo de S_n.*

Prova: Basta tomar $H = \{1\}$ no Teorema da Representação, Teorema 1.6. ◊

1.6 Classes de Conjugação

Seja G um grupo. Dados $x, y \in G$ defina

$$x \sim_G y \text{ se, e somente se, existe } a \in G \text{ tal que } y = a^{-1}xa.$$

Proposição 1.6.1. *Seja G um grupo. A relação $\sim_G$ define uma relação de equivalência em G.*

Prova: A prova é deixada para o leitor. ◊

Definição 1.15. *Se $x \sim_G y$, dizemos que x e y são elementos **conjugados** em G.*

Denote $a^{-1}xa = x^a$, onde x e $a \in G$. As seguintes propriedades são válidas:

(1) $x^{1_G} = x$ para todo $x \in G$.

(2) Se $y = x^a$, então $x = y^{a^{-1}}$ para todos x, y e $a \in G$.

(3) $(x^a)^b = x^{ab}$ para todos x, a e $b \in G$.

A classe de equivalência de x é dada por

$$C_x = \{y \in G \mid x \sim_G y\} = \{x^a \mid a \in G\}$$

e é chamada de **classe de conjugação** de x em G.

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

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

uma união disjunta. Assim

$$|G| = |C_{x_1}| + |C_{x_2}| + \cdots + |C_{x_n}|.$$

Observe que $C_x = \{x\}$ se, e somente se, $x \in Z(G)$ e daí a equação anterior pode ser escrita como

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |C_x|. \tag{1.4}$$

A equação (1.4) é chamada de **equação de classes**.

Proposição 1.6.2. *Seja G um grupo e $x \in G$. Então o conjunto $C_G(x) = \{a \in G \mid ax = xa\}$ é um subgrupo de G.*

Prova: A cargo do leitor. ◊

Proposição 1.6.3. *Seja G um grupo finito e $x \in G$. Então*

$$[G : C_G(x)] = |C_x|.$$

Em particular, $|C_x|$ é um divisor de $|G|$ para todo $x \in G$.

Prova: Sejam $H = C_G(x)$ e $G/H = \{Ha \mid a \in G\}$ o conjunto de todas as classes laterais à direita de H em G. Pelo Teorema de Lagrange, Teorema 1.3, $|G| = [G : H]|H|$. Agora, considere a aplicação

$$\begin{aligned} \phi : \frac{G}{H} &\to C_x \\ Ha &\mapsto x^a. \end{aligned}$$

Claramente ϕ é sobrejetora. Sejam $Ha, Hb \in G/H$ tais que $\phi(Ha) = \phi(Hb)$. Daí $x^a = x^b$ e então $x^{ab^{-1}} = 1$, isto é, $ab^{-1} \in C_G(x) = H$ e portanto $Ha = Hb$. Logo ϕ é injetiva. Assim

$$|C_x| = [G : C_G(x)]$$

como queríamos. ◊

Definição 1.16. *Seja p um número primo e G um grupo. Se $|G| = p^n$, $n \in \mathbb{N}$, dizemos que G é um p-**grupo**.*

Observação 1.6.1. *Pelo Teorema de Lagrange, Teorema 1.3, todo subgrupo de um p-grupo também é um p-grupo.*

Teorema 1.7. *Se G é um p-grupo e $|G| = p^n > 1$, então $|Z(G)| = p^m > 1$.*

Prova: Pela Equação de classes, (1.4), obtemos

$$|Z(G)| = |G| - \sum_{x \notin Z(G)} |C_x|.$$

Mas para todo $x \notin Z(G)$, temos $|C_x| > 1$ e como $|C_x|$ divide $|G|$, então $|C_x| = p^{\alpha_x}$ para todo $x \notin Z(G)$. Como $|G| = p^n > 1$, então devemos ter $|Z(G)| = p^m > 1$. ◊

Corolário 1.6.1. *Se p é um número primo e $|G| = p^2$, então G é um grupo abeliano.*

Teorema 1.8 (Teorema de Cauchy)**.** *Seja p um divisor primo da ordem de um grupo finito G. Então existe $a \in G$ tal que $|a| = p$.*

Prova: Vamos usar indução sobre a ordem de G. Se $|G| = 1$, nada há a fazer. Vamos supor que o teorema é válido para todo grupo H tal que $1 \leq |H| < |G|$. Temos três casos para analizar.

Caso 1: G é cíclico.

Seja $G = \langle x \rangle$ e seja p um divisor primo de $|G|$. Neste caso $|x| = p^{\alpha k}$, onde $\alpha \geq 1$. Tome $a = x^{p^{\alpha-1}k}$. Então $a^p = 1$ e nenhum outra potência r de a menor que p é tal que $a^r = 1$. Portanto $|a| = p$ como queríamos.

Caso 2: G é abeliano e não cíclico.

Seja p um divisor primo de $|G|$ e seja $x \in G$, $x \neq 1$. Se p divide $|x|$ então pelo *Caso 1*, existe $a \in \langle x \rangle$ tal que $|a| = p$ e assim o teorema está provado.

Suponha então que p não divide $|x|$. Seja $N = \langle x \rangle$. Como G é abeliano, então $L = G/N$ é um grupo tal que p divide $|L| = [G : N]$. Mas $1 \leq |L| < |G|$, assim pela hipótese de indução existe $\overline{b} \in L$ tal que $\overline{b} \neq \overline{1}$ e $|\overline{b}| = p$. Assim $b \notin N$ e $b^p \in N$. Seja $|N| = r$, então $(b^p)^r = 1$ e portanto p divide $|b|$. Logo pelo *Caso 1*, existe $a \in \langle b \rangle$ tal que $|a| = p$ e então o teorema está provado.

Caso 3: G não abeliano

Neste caso $Z(G) \neq G$. Se p divide $|Z(G)|$, então basta usar o *Caso 2*. Assim suponha que p não divide $|Z(G)|$. Temos

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} [G : C_G(x)].$$

Como p divide $|G|$ então existe $x \notin Z(G)$ tal que p não divide $[G : C_G(x)]$. Portanto p divide $|H|$ onde $H = C_G(x) \neq G$. Como $1 \leq |H| < |G|$, então pela hipótese de indução, existe $a \in H$ tal que $|a| = p$.

Portanto o teorema está provado. ◊

1.7 Grupos Cíclicos

Proposição 1.7.1. *(i) Se $H \subseteq \mathbb{Z}$, então H é um subgrupo de $(\mathbb{Z}, +)$ se, e somente se, $H = n\mathbb{Z}$ para algum $n \in \mathbb{N}$.*

(ii) $n\mathbb{Z} \subseteq m\mathbb{Z}$ se, e somente se, $m|n$. Neste caso temos $[m\mathbb{Z} : n\mathbb{Z}] = \frac{n}{m}$.

Prova:

(i) Se $H = n\mathbb{Z}$, com $n \in \mathbb{N}$, então é fácil verificar que $H \leq \mathbb{Z}$.

Agora seja $H \leq \mathbb{Z}, H \neq \{0\}$. Tome $n = \min\{x \in H \mid x > 0\}$. Como $n \in H$ e como $H \leq \mathbb{Z}$, então $n\mathbb{Z} \subseteq H$. Dado $a \in H$, existem q e $r \in \mathbb{Z}$ tais que $a = qn + r$ com $0 \leq r < n$. Mas $a, n \in H$ daí $r \in H$ e então pela minimalidade de n devemos ter $r = 0$. Logo $a \in n\mathbb{Z}$ e portanto $H = n\mathbb{Z}$.

(ii) É imediato verificar que $n\mathbb{Z} \subseteq m\mathbb{Z}$ se, e somente se, $m|n$. Suponha que $n\mathbb{Z} \leq m\mathbb{Z} \leq \mathbb{Z}$. Assim pelo Corolário 1.3.2 temos

$$\frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}},$$

daí

$$\left|\frac{\mathbb{Z}/n\mathbb{Z}}{m\mathbb{Z}/n\mathbb{Z}}\right| = \left|\frac{\mathbb{Z}}{m\mathbb{Z}}\right|.$$

Então

$$\frac{n}{[m\mathbb{Z} : n\mathbb{Z}]} = m$$

e portanto $[m\mathbb{Z} : n\mathbb{Z}] = \dfrac{n}{m}$, como queríamos.

◊

Proposição 1.7.2. *Seja $G = \langle a \rangle = \{\ldots, a^{-1}, 1, a, a^2, \ldots\}$ um grupo cíclico de ordem infinita. Então:*

(i) A função $\phi : (\mathbb{Z}, +) \to (G, \cdot)$ dada por $\phi(t) = a^t$ é um isomorfismo.

(ii) O elemento a^r gera G se, e somente se, $r = -1$ ou $r = 1$.

Prova: Prova:

(i) É fácil verificar que ϕ definida desse jeito é um isomorfismo.

(ii) Como ϕ é um isomorfismo, então a^r gera G se, e somente se, r gera $\mathbb{Z}$. Mas os únicos geradores de $\mathbb{Z}$ são $r = -1$ ou $r = 1$.

◊ ◊

Proposição 1.7.3. *Seja $G = \langle a \rangle = \{1, a, \ldots, a^{n-1}\}$ um grupo cíclico de ordem finita igual a n. Então:*

(i) A função $\overline{\phi} : (\mathbb{Z}/n\mathbb{Z}, +) \to (G, \cdot)$ dada por $\phi(\bar{t}) = a^t$ é um isomorfismo.

(ii) O elemento a^r gera G se, e somente se, $mdc(m, n) = 1$.

Prova:

(i) Da Proposição 1.7.3 obtemos que ϕ de $\mathbb{Z}$ em G dada por $\phi(r) = a^r$ é sobrejetora. Além disso, $\ker \phi = n\mathbb{Z}$. Logo

$$\frac{\mathbb{Z}}{\ker \phi} = \frac{\mathbb{Z}}{n\mathbb{Z}} \cong G.$$

(ii) Como $\overline{\phi}$ é um isomorfismo, então a^m gera G se, e somente se, m gera $\mathbb{Z}/n\mathbb{Z}$. O que ocorre se, e somente se, $mdc(m, n) = 1$.

◊

Proposição 1.7.4. *$G = \langle a \rangle = \{1, a, \ldots, a^{n-1}\}$ um grupo cíclico de ordem finita igual a n. Então:*

(i) Se $H \leq G$, então H é cíclico. Mais ainda, $H = \langle a^m \rangle$ onde m é o menor inteiro positivo tal que $a^m \in H$. O subgrupo H tem ordem igual a $\frac{n}{m}$.

(ii) Se d é um divisor de n, então existe um único subgrupo H de G com ordem igual a a. Mais ainda, $H = \langle a^{\frac{n}{d}} \rangle$.

Prova:

(i) Seja m o menor inteiro positivo $a^m \in H$. Daí $\langle a^m \rangle \subseteq H$. Agora, seja $a^\alpha \in H$. Então existem $q, r \in \mathbb{Z}$ tais que $\alpha = mq + r$ com $0 \leq r < m$. Daí $a^\alpha = a^{mq}a^r$. Como $a^\alpha, a^m \in H$ e $H \leq G$, então $a^r \in H$. Logo $r = 0$, devido à minimalidade de m. Portanto $H = \langle a^m \rangle$.

Agora, $(a^m)^{n/m} = 1$. Seja $k < n/m$ tal que $(a^m)^k = 1$. Logo $n|mk$, mas $mk < n$, logo $k = 0$. Portanto $|a^m| = \dfrac{n}{m}$.

(ii) Seja d um divisor de n. Pelo item anterior, o grupo $H = \langle a^{n/d} \rangle$ tem ordem d. Vamos provar que H é único. Seja K um subgrupo de G de ordem d. Novamente pelo item anterior, $K = \langle a^m \rangle$ tal que $|K| = \frac{n}{m} = d$. Assim $m = \dfrac{n}{d}$ e daí $K = \langle a^{n/d} \rangle = H$, como queríamos.

$\diamond$

1.8 Grupos de Permutações

Definição 1.17. *Um permutação* $\alpha \in S_n$ *é denominada um* r-***ciclo*** *se existem elementos distintos* $a_1, \ldots, a_r \in \{1, \ldots, n\}$ *tais que*

$$\begin{aligned} \alpha(a_1) &= a_2 \\ \alpha(a_2) &= a_3 \\ &\vdots \\ \alpha(a_{r-1}) &= a_r \\ \alpha(a_r) &= a_1 \end{aligned}$$

e tais que $\alpha(j) = j$ *para todo* $j \in \{1, \ldots, n\} \backslash \{a_1, \ldots, a_r\}$. *Tal r-ciclo será denotado por* $(a_1 a_2 \cdots a_r)$. *O número r é chamado o* ***comprimento*** *do ciclo. Se* $r = 2$, *então chamamos os* 2*-ciclos de* ***transposições****. O único* 1*-ciclo é a identidade, que denotaremos por* (1).

Exemplos 1.8.1. *Em S_5:*

- *A permutação* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ *é um 5-ciclo denotado por* $\alpha = (12345)$. *Também podemos escrever* $\alpha = (23451)$ *ou* $\alpha = (34512)$ *ou* $\alpha = (45123)$.
- *A permutação* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$ *é um 3-ciclo denotado por* $\alpha = (143)$. *Também podemos escrever* $\alpha = (431)$ *ou* $\alpha = (314)$.
- *A permutação* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$ *é um 2-ciclo denotado por* $\alpha = (24)$ *ou* $\alpha = (42)$.
- *A permutação* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ *não é um r-ciclo qualquer que seja r. Mas podemos escrever* $\alpha = (135)(24)$ *ou* $\alpha = (24)(135)$.

Definição 1.18. *Seja $\alpha \in S_n$ um r-ciclo e seja $\beta \in S_n$ um s-ciclo. As permutações α e β são* ***disjuntas*** *se nenhum elemento de $\{1, \ldots, n\}$ é movido por ambas, isto é, para todo $a \in \{1, \ldots, n\}$ temos $\alpha(a) = a$ ou $\beta(a) = a$.*

Exemplos 1.8.2. *Em S_5 os ciclos* (134) *e* (25) *são disjuntos, enquanto que* (135) *e* (25) *não são disjuntas.*

Lema 1.8.1. *Sejam $\alpha, \beta \in S_n$. Se α e β são permutações disjuntas então $\alpha\beta = \beta\alpha$.*

Prova: É suficiente mostrar que $(\alpha\beta)(i) = (\beta\alpha)(i)$ para todo $i = 1, \ldots, n$. Se β move i, digamos $\beta(i) = j \neq i$, então β também move j. Caso contrário teríamos $\beta(i) = j = \beta(j)$, o que contradiz o fato de que β é injetora. Como α e β são disjuntas, então $\alpha(i) = i$ e $\alpha(j) = j$. Daí $(\alpha\beta)(i) = \alpha(j) = j = \beta(i) = (\beta\alpha)(i)$. De modo análogo, mostra-se que se α move i, então $(\alpha\beta)(i) = (\beta\alpha)(i)$. Se α e β fixam i, então $(\alpha\beta)(i) = \alpha(i) = i = \beta(i) = (\beta\alpha)(i)$. Portanto $\alpha\beta = \beta\alpha$. ◇

Lema 1.8.2. *Se $\alpha \in S_n$ é um r-ciclo, então $|\alpha| = r$.*

Prova: Seja $\alpha = (a_1 a_2 \ldots a_r)$. Mostra-se, por indução em k, que $\alpha^k(a_j) = a_{j+k}$, onde $j + k \equiv l \pmod{r}$ se $j + k > r$. Assim

$$\alpha^r(a_k) = a_{k+r} = a_k$$

para todo $k = 1, \ldots, r$. Portanto $|\alpha|$ divide r. Agora, se $|\alpha| = l < r$, então $\alpha^l = (1)$ e daí $\alpha^l(i_k) = i_k$ para todo $k = 1, \ldots, r$. Mas,

$$\alpha^l(a_1) = a_{l+1} \neq a_1$$

pois α é um r-ciclo. Portanto $|\alpha| = r$. ◊

Proposição 1.8.1. *Seja $\alpha \in S_n$, $\alpha \neq (1)$. Então a permutação α é igual a um produto de ciclos disjuntos de comprimento ≥ 2. Mais ainda, tal decomposição é única a menos da ordem dos fatores.*

Prova: Como $\alpha \neq (1)$, então existe $i_1 \in \{1, \ldots, n\}$ tal que $\alpha(i_1) \neq i_1$. Considere a sequência i_1, $\alpha(i_1)$, $\alpha^2(i_1)$, ... Então existe um menor inteiro positivo r_1, $2 \leq r_1 \leq n$ tal que i_1, $\alpha(i_1)$, $\ldots$, $\alpha^{r_1-1}(i_1)$ são elementos distintos e $\alpha^{r_1}(i_1) \in \{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)\}$. Se $\alpha^{r_1}(i_1) = \alpha^j(i_1)$, com $j \neq 0$ então $\alpha^{r_1-j}(i_1) = i_1$, o que contradiz a escolha de r_1. Daí $\alpha^{r_1}(i_1) = i_1$. Assim a restrição de α ao conjunto $\{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)\}$ é tal que

$$\alpha|_{\{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)\}} = (i_1 \alpha(i_1) \ldots \alpha^{r_1-1}(i_1)).$$

Denote este r_1-ciclo por $\sigma_1 = (i_1 \alpha(i_1) \ldots \alpha^{r_1-1}(i_1))$.

Se a restrição de α ao complementar de $\{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)\}$ é a identidade, então $\alpha = \sigma_1$. Caso contrário, tome $i_2 \in \{1, 2, \ldots, n\} \backslash \{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1)\}$ tal que $\alpha(i_2) \neq i_2$. De modo análogo ao caso anterior, existe $r_2 \geq 2$ tal que

$$\alpha|_{\{i_2, \alpha(i_2), \ldots, \alpha^{r_2-1}(i_2)\}} = (i_2 \alpha(i_2) \ldots \alpha^{r_2-1}(i_2)).$$

Denote este r_2-ciclo por $\sigma_2 = (i_2 \alpha(i_2) \ldots \alpha^{r_2-1}(i_2))$. Note que σ_1 e σ_2 são disjuntas.

Se a restrição de α ao complementar de $\{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1), i_2, \alpha(i_2), \ldots, \alpha^{r_2-1}(i_2)\}$ é a identidade, então $\alpha = \sigma_1\sigma_2$. Caso contrário, tome $i_3 \in \{1, 2, \ldots, n\} \backslash \{i_1, \alpha(i_1), \ldots, \alpha^{r_1-1}(i_1), i_2, \alpha(i_2), \ldots, \alpha^{r_2-1}(i_2)\}$ tal que $\alpha(i_3) \neq i_3$ e repita o processo anterior. Claramente depois de um número finito de etapas este processo irá terminar e obteremos que $\alpha = \sigma_1\sigma_2 \cdots \sigma_t$, onde $\sigma_1, \ldots, \sigma_t$ são ciclos disjuntos de comprimento ≥ 2.

Suponha agora que também temos $\alpha = \tau_1\tau_2 \cdots \tau_l$ com τ_1, τ_2, ..., τ_l ciclos disjuntos de comprimento ≥ 2. Temos $\tau_1 \cdots \tau_l(i_1) = \alpha(i_1) \neq i_1$ e como os τ_i's são disjuntos, então existe um único τ_j tal que $\tau_j(i_1) = \alpha(i_1)$. Mas os ciclos τ_i's comutam, assim podemos

supor que $j = 1$ e então $\tau_1(i_1) = \alpha(i_1)$. Mostremos que $\tau_1 = \sigma_1$. O ciclo τ_1 não pode fixar $\alpha(i_1)$, isto é, $\tau_1(\alpha(i_1)) \neq \alpha(i_1)$ pois $\tau_1(i_1) = \alpha(i_1) \neq i_1$. Como os τ_j's são ciclos disjuntos, então $\tau_j(\alpha(i_1)) = \alpha(i_1)$ para $j \geq 2$. Assim $\tau_1(\alpha(i_1)) = \alpha^2(i_1)$ e daí $\tau_1(\alpha^k(i_1)) = \alpha^{k+1}(i_1)$ para todo $k \geq 0$. Logo $\tau_1 = \sigma_1$. Aplicando o mesmo raciocínio com i_2 obtemos que $\tau_2 = \sigma_2$. Continuando com o procedimento obtemos que $t = l$ e que a menos da ordem $\sigma_j = \tau_j$ para cada $j = 1, \ldots, t$. ◇

Proposição 1.8.2. *1. Todo elemento de S_n pode ser escrito como um produto de transposições, isto é, $S_n = \langle$transposições$\rangle$.*

2. $S_n = \langle(12), (13), \ldots, (1n)\rangle$.

3. $S_n = \langle(12), (23), \ldots, (n-1n)\rangle$.

Prova:

1. Inicialmente temos $(1) = (12)(12) \in \langle$transposições$\rangle$. Agora, pela Proposição 1.8.1, dada uma permutação $\alpha \in S_n$, é suficiente mostrar que cada r-ciclo de α pode ser escrito como um produto de transposições. Assim se $(a_1 a_2 \cdots a_r)$ é um r-ciclo de α, então podemos escrever

$$(a_1 a_2 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_3)(a_1 a_2).$$

   Donde obtemos o resultado desejado.

2. Pela parte (a), basta mostrar que toda transposição (ij) pertence a $\langle(12), (13), \ldots, (1n)\rangle$. De fato

$$(ij) = (1i)(1j)(1i)$$

   para $i \neq j$, como queríamos.

3. Para todo inteiro $r \geq 2$, temos

$$(1i+1) = (1i)(ii+1)(1i),$$

   assim o subgrupo $\langle(12), (23), \ldots, (n-1n)\rangle$ contém $(1i)$, para cada $i = 2, \ldots, n$. Logo pelo item (b), $S_n = \langle(12), (23), \ldots, (n-1n)\rangle$, como queríamos.

◇

Observações 1.8.1. *1. Um elemento $\alpha \in S_n$ pode ser escrito como um produto de transposições disjuntas se, e somente se, sua ordem for igual a 2.*

2. A decomposição de $\alpha \in S_n$ em um produto de transposições não é única. Por exemplo:

(a) para $\alpha = (123) \in S_4$ temos: $\alpha = (13)(12) = (23)(13) = (13)(42)(12)(14)$,

(b) para $\alpha = (24) \in S_4$ temos: $\alpha = (24) = (13)(12)(13)(34)(23)$.

Apesar da decomposição não ser única, existe um invariante nessa decomposição que é a paridade do número de transposições que aparecem em α.

Teorema 1.9. *Seja $\alpha \in S_n$. Se $\alpha = \sigma_1 \cdots \sigma_r = \tau_1 \cdots \tau_l$, onde σ_i e τ_i são transposições para todo $i = 1, \ldots, r$ e $j = 1, \ldots, l$ então $r \equiv l \pmod 2$.*

Prova: Inicialmente note que toda transposição tem ordem 2, daí podemos escrever

$$(1) = \alpha\alpha^{-1} = \sigma_1 \cdots \sigma_r \tau_l \cdots \tau_1.$$

Assim é suficiente mostrar que a identidade só pode ser escrita como um número par de transposições. Assim $r + l$ é par e então teremos $r \equiv l \pmod 2$.

Suponha então que

$$(1) = (a_k b_k) \cdots (a_2 b_2)(a_1 b_1) \tag{1.5}$$

onde $k \geq 1$ e suponha que $a_i \neq b_i$ para todo i. Provemos que k é par. Como $a_i \neq b_i$, então $k > 1$. Assim $k \geq 2$ e faremos a prova por indução em k. Suponha então que em qualquer produto de transposições que seja a identidade e que contenha menos do que k transposições, ocorra uma quantidade par de transposições.

Considere um produto da forma (1.5). Alguma transposição $(a_i b_i)$ para $i = 2, \ldots, k$ deve mover a_1, caso contrário não obteríamos a identidade. Assim podemos supor que $a_1 = a_j$ para algum $j > 1$. Agora,

$$(ab)(cd) = (cd)(ab)$$
$$(ac)(bc) = (bc)(ab).$$

Assim podemos mudar a ordem das transposições $(a_i b_i)$ em (1.5), sem mudar sua quantidade, e supor que $a_2 = a_1$. Se $b_1 = b_2$, então $(a_1 b_1)(a_2 b_2) = (1)$ em (1.5) e obtemos um produto de $k-2$ transposições dando a identidade. Daí pela hipótese de indução $k-2$ é par e logo k é par.

Se $b_1 \neq b_2$, então $(a_1 b_1)(a_1 b_2) = (a_1 b_2)(b_1 b_2)$ e daí podemos reescrever (1.5) como

$$(1) = (a_k b_k) \cdots (a_3 b_3)(a_1 b_1)(b_1 b_2) \tag{1.6}$$

onde somente os dois primeiros fatores de (1.5) foram alterados. Note que o número de transposições que podem mover a_1 foi reduzida em 1. Repita o argumento com (1.6). Assim existe a_j, com $j \geq 3$, tal que $a_j = a_1$. Com isso ou reduzimos o número de transposições em (1.6) e aí usamos a hipótese de indução ou então reescrevemos (1.6) sem mudar o número total de transposições, mas reduzindo em 1 o número de transposições que movem a_1. Continuando com este processo, chegaremos na situação em que as duas primeiras transposições se cancelam, caso contrário somente a primeira transposição de (1.5) moveria a_1 e portanto não seria a identidade. Chegando nesse instante a hipótese de indução garante que k é par. ♢

Definição 1.19. *Seja $\alpha \in S_n$. Escreva $\alpha = \tau_1 \cdots \tau_r$ onde τ_i é uma transposição para cada $i = 1, \ldots, r$. Então o número $(-1)^r$ é chamado de **sinal** de α e denotamos*

$$(\alpha) = (-1)^\alpha = (-1)^r. \tag{1.7}$$

*Permutações com sinal 1 são chamadas de **pares** e aquelas com sinal -1 são chamada de **ímpares**.*

Teorema de Sylow

Grupos livres

Grupos Solúveis

Grupos Nilpotentes

BIBLIOGRAFIA

[1] Garcia, A.; Lequain, Y., *Elementos de Álgebra*, Impa, 2010.

[2] Gonçalves, A, *Introdução à Álgebra*, Projeto Euclides, Impa, 2006.

[3] Lang, S., *Algebra*, Boston: Addison-Wesley, 1984.

[4] Newman, M., *Integral Matrices*, Monographs and Textbooks in Pure and Applied Mathematics, Vol. 45, Academic Press; 1st edition 1972.

ÍNDICE REMISSIVO

Classe de Conjugação, 26

Elementos
- Conjugados, 26

Equação de Classes, 27

Grupos, 5
- *p*-grupos, 27
- índice, 13
- Abelianos, 6
- Associatividade, 5
- Centro, 9
- classe lateral à direita, 12
- classe lateral à esquerda, 12
- Cíclicos, 11
- Dihedral, 19
- Elemento neutro, 5
- Inverso, 5
- Ordem, 11
- Potências de um elemento, 7
- Quociente, 18
- Triviais, 9

Homomorfismo, 19
- Imagem, 20
- Isomorfismo, 20
- Projeção Canônica, 20

Homorfismo
- Kernel, 20

Ordem
- de elemento, 8

Permutações
- *r*-ciclo, 31
- Ímpares, 36
- disjuntas, 32
- Pares, 36
- Sinal, 36
- transposições, 31

Subgrupos, 9
- dos comutadores, 12
- gerados por um conjunto, 11