LISTA DE TAREFAS PENDENTES

ÁLGEBRA

José Antônio O. Freitas

Curso de Verão
DMA - UFV 2015

Notas de Aula[1]

SUMÁRIO

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 $\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$. 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*

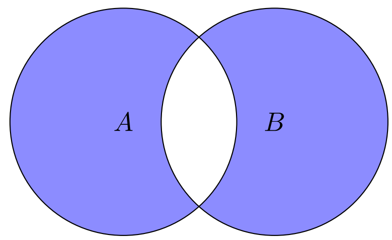
$$A + B = (A - B) \cup (B - A).$$

Assim $\mathcal{B}(X)$ é um grupo comutativo, o elemento neutro e $\emptyset$ 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

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

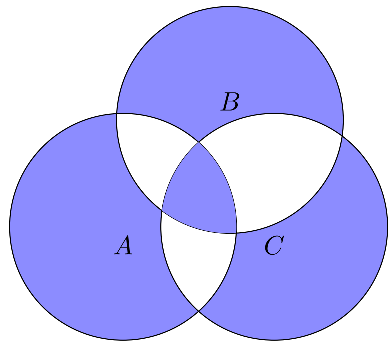
Lema 1.1.2. *Se G é um grupo e $a, b \in G$, então $(ab)^{-1} = b^{-1}a^{-1}$.*

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

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

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

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

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

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

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 $1, \alpha, \alpha^2, \ldots, \alpha^{k-1}$ são todos as potências distintas de α, enquanto que em $1, \alpha, \alpha^2, \ldots, \alpha^{k-1}, \alpha^k$ 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 $H = \{1, \alpha, \alpha^2, \ldots, \alpha^{k-1}\}$. 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. $\diamond$

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 $\{a_1H, a_2H, \dots, a_tH\}$ 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 $i = 1, \dots, t$, 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 $c = a_1b_1$. 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.

$\diamond$

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. $\diamond$

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 $\dfrac{G}{H}$ 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 $\operatorname{Im} \phi = \{y \in H \mid y = \phi(x) \text{ para algum } x \in G\}$ *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*

$$\phi(id) = 1$$
$$\phi(\alpha) = a$$
$$\phi(\beta) = b$$
$$\phi(\alpha\beta) = ab$$
$$\phi(\alpha\beta^2) = ab^2$$

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

$$\overline{\phi} : \frac{G}{\ker\phi} \to \phi(G)$$
$$a\ker\phi \mapsto \phi(a)$$

é um isomorfismo.

(ii) As seguintes funções

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

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*

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

é um isomorfismo.

Prova: Considere o hommorfismo ϕ restrito a K;

$$\psi := \phi|_K : K \to H$$
$$h \mapsto \phi(h).$$

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

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

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

Seja $N = \ker\psi$. Então $N \trianglelefteq G$ e $N \subseteq H$. Agora, seja $L \trianglelefteq G$ tal que $L \subseteq H$. Então $x^{-1}Lx = L \subseteq x^{-1}Hx$ para todo $x \in G$. Assim, $L \subseteq N = \cap_{x\in G}(x^{-1}Hx)$. 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. $\diamond$

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**.*

Exemplos 1.6.1. *(1) Os grupos D_8, $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ e $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ são 2-grupos de ordem 2^3.*

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

(3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ *é um 2-grupo infinito.*

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 $|Z(G)| = p^m > 1$. $\diamond$

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. $\diamond$

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.

$\diamond$

Proposição 1.7.2. *Seja $G = \langle a \rangle = \{\dots, a^{-1}, 1, a, a^2, \dots\}$ 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 $r = 1$.

$\diamond$ $\diamond$

Proposição 1.7.3. *Seja $G = \langle a \rangle = \{1, a, \dots, a^{n-1}\}$ 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. *$G = \langle a \rangle = \{1, a, \dots, a^{n-1}\}$ 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.

◊

1.8 Grupos de Permutações

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

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 $j + k \equiv l$ (mod 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 $\tau_1, \tau_2, \ldots, \tau_l$ 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. *(i) Todo elemento de S_n pode ser escrito como um produto de transposições, isto é, $S_n = \langle transposições\rangle$.*

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

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

Prova:

(i) 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 $(a_1a_2\cdots a_r)$ é um r-ciclo de α, então podemos escrever

$$(a_1a_2\cdots a_r) = (a_1a_r)(a_1a_{r-1})\cdots(a_1a_3)(a_1a_2).$$

Donde obtemos o resultado desejado.

(ii) 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.

(iii) 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.

$\diamond$

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_ib_i) para $i = 2, \dots, k$ 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_ib_i) em (1.5), sem mudar sua quantidade, e supor que $a_2 = a_1$. Se $b_1 = b_2$, então $(a_1b_1)(a_2b_2) = (1)$ 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 $(a_1b_1)(a_1b_2) = (a_1b_2)(b_1b_2)$ e daí podemos reescrever (1.5) como

$$(1) = (a_kb_k)\cdots(a_3b_3)(a_1b_1)(b_1b_2) \tag{1.6}$$

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 $i = 1, \dots, r$. Então o número $(-1)^r$ é chamado de **sinal** de α e denotamos*

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

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

Exemplos 1.8.3. *(1) Seja $\alpha, \beta \in S_n$ onde $\alpha = (123)$ e $\beta = (24)$. Então*

$$\operatorname{sgn}(\alpha) = 1$$
$$\operatorname{sgn}(\beta) = -1.$$

(2) Qualquer transposição em S_n tem sinal -1.

(3) $\text{sgn}(1) = 1$

(4) Se α é um r-ciclo, então $\text{sgn}(\alpha) = (-1)^{r-1}$. *(Exercício!)*

Proposição 1.8.3. *Para $\alpha, \beta \in S_n$ temos*

$$\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta).$$

Prova: Se α é um produto de k transposições e β é um produto de l transposições, então $\alpha\beta$ pode ser escrita como um produto de $k + l$ transposições. Logo

$$\text{sgn}(\alpha\beta) = (-1)^{r+l} = (-1)^r(-1)^l = \text{sgn}(\alpha)\text{sgn}(\beta),$$

como queríamos. ◊

Corolário 1.8.1. *Inversão e conjugação de uma permutação não altera seu sinal.*

Prova: Seja $\alpha \in S_n$. Assim $\alpha\alpha^{-1} = (1)$ e daí $\text{sgn}(\alpha\alpha^{-1}) = \text{sgn}(1) = 1$. Por outro lado, $\text{sgn}(\alpha\alpha^{-1}) = \text{sgn}(\alpha)\text{sgn}(\alpha^{-1})$. Portanto $\text{sgn}(\alpha) = \text{sgn}(\alpha^{-1})$, como queríamos.

Agora, se $\beta = \pi^{-1}\alpha\pi$ para algum $\pi \in S_n$, então

$$\text{sgn}(\beta) = \text{sgn}(\pi^{-1}\alpha\pi) = \text{sgn}(\pi^{-1})\text{sgn}(\alpha)\text{sgn}(\pi) = \text{sgn}(\alpha).$$

◊

Corolário 1.8.2. *O conjunto*

$$A_n = \{\alpha \in S_n \mid \text{sgn}(\alpha) = 1\}$$

*é um subgrupo de S_n chamado de **grupo alternado**.*

Prova: Como $\text{sgn}(1) = 1$, então $(1) \in A_n$. Agora, dados $\alpha, \beta \in A_n$, então $\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta) = 1$. Logo $\alpha, \beta \in A_n$. Como $\text{sgn}(\alpha) = \text{sgn}(\alpha^{-1})$, então $\alpha^{-1} \in A_n$ para todo $\alpha \in A_n$. Portanto A_n é um subgrupo de S_n. ◊

Exemplos 1.8.4. *(1) Em S_2 temos $A_2 = \{(1)\}$.*

(2) Em $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ temos $A_3 = \{(1), (123), (132)\}$.

(3) Em S_n temos $A_4 = \{(1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$.

(4) Para $n \geq 4$ $(123), (124) \in A_n$. Assim A_n não é abeliano.

Proposição 1.8.4. *Para $n \geq 2$, $|A_n| = \frac{n!}{2}$.*

Prova: A aplicação $\operatorname{sgn} : S_n \to C_2 = \{-1, 1\}$, onde C_2 é um grupo multiplicativo, é um homomorfismo. É fácil ver que $\ker \operatorname{sgn} = A_n$ e daí $|A_n| = \frac{n!}{2}$. ◊

Definição 1.20. *Seja $n \geq 2$. Se $\alpha \in S_n$ e se $\alpha = (a_{11} \dots a_{1r_1}) \cdots (a_{t1} \dots a_{tr_t})$ é a sua decomposição em ciclos disjuntos com $r_1 \leq r_2 \leq \cdots \leq r_t$, dizemos que $r_1, \dots, r_t$ é o **tipo de decomposição** de α.*

Exemplo 1.8.1. *As permutações $\alpha = (45)(67)(123)$ e $\beta = (15)(36)(247)$ têm o mesmo tipo de decomposição, a saber 2, 2, 3.*

Lema 1.8.3. *Seja $n \geq 2$. Dada uma permutação $\rho \in S_n$, seja $\rho = (a_{11} \dots a_{1r_1}) \cdots (a_{t1} \dots a_{tr_t})$ sua decomposição em ciclos disjuntos.*

(i) Se $\sigma \in S_n$, então a permutação $\sigma\rho\sigma^{-1}$ tem a seguinte decomposição em ciclos disjuntos

$$\sigma\rho\sigma^{-1} = (\sigma(a_{11}) \dots \sigma(a_{1r_1})) \cdots (\sigma(a_{t1}) \dots \sigma(a_{tr_t})).$$

Em particular, as permutações ρ e $\sigma\rho\sigma^{-1}$ têm o mesmo tipo de decomposição.

(ii) Reciprocamente, se $\rho, \beta \in S_n$ são permutações com o mesmo tipo de decomposição, então existe $\sigma \in S_n$ tal que $\beta = \sigma\rho\sigma^{-1}$.

(iii) Se as permutações $\rho, \beta \in S_n$ têm o mesmo tipo de decomposição e se a permutação ρ deixa pelo menos duas letras fixas, então existe $\mu \in A_n$ tal que $\beta = \mu\rho\mu^{-1}$.

Prova:

(i) Seja $\tau = (a_1 \dots a_r)$ um r-ciclo qualquer. Queremos mostrar que $\sigma\tau\sigma^{-1} = (\sigma(a_1) \dots \sigma(a_r))$. Para isso, vamos mostrar que

$$\sigma\tau\sigma^{-1}|_{\{\sigma(a_1), \dots, \sigma(a_r)\}} = (\sigma(a_1) \dots \sigma(a_r)).$$

De fato, para $j \in \{1, \dots, r-1\}$ temos

$$\sigma\tau\sigma^{-1}(\sigma(a_j)) = \sigma\tau(\sigma^{-1}(\sigma(a_j))) = \sigma\tau(a_j) = \sigma(a_{j+1})$$

e para $j = r$

$$\sigma\tau\sigma^{-1}(\sigma(a_r)) = \sigma\tau(\sigma^{-1}(\sigma(a_r))) = \sigma\tau(a_r) = \sigma(a_1).$$

Além disso, se $b \notin \{\sigma(a_1), \ldots, \sigma(a_r)\}$, então $\sigma^{-1}(b) \notin \{a_1, \ldots, a_r\}$. Daí $\tau\sigma^{-1}(b) = \sigma^{-1}(b)$ e assim

$$\sigma\tau\sigma^{-1}(b) = \sigma(\tau(\sigma^{-1}(b))) = \sigma\sigma^{-1}(b) = b.$$

Portanto, $\sigma\tau\sigma^{-1} = (\sigma(a_1) \ldots \sigma(a_r))$.

Agora, se $\rho = (a_{11} \ldots a_{1r_1}) \cdots (a_{t1} \ldots a_{tr_t})$, então

$$\begin{aligned}\sigma\rho\sigma^{-1} &= \sigma(a_{11} \ldots a_{1r_1})\sigma^{-1}\sigma(a_{21} \ldots a_{2r_2})\sigma^{-1} \cdots \sigma(a_{t1} \ldots a_{tr_t})\sigma^{-1}\\ &= (\sigma(a_{11}) \ldots \sigma(a_{1r_1}))(\sigma(a_{21}) \ldots \sigma(a_{2r_2})) \cdots (\sigma(a_{t1}) \ldots \sigma(a_{tr_t})).\end{aligned}$$

Mais ainda, para todo $i, j \in \{1, \ldots, t\}$ com $i \neq j$, como $\{a_{i1}, \ldots, a_{ir_i}\} \cap \{a_{j1}, \ldots, a_{jr_j}\} = \emptyset$ então $\{\sigma(a_{i1}), \ldots, \sigma(a_{ir_i})\} \cap \{\sigma(a_{i1}), \ldots, \sigma(a_{jr_j})\} = \emptyset$. Portanto os ciclos obtidos em $\sigma\rho\sigma^{-1}$ são disjuntos.

(ii) Seja $\beta = (b_{11} \ldots b_{1r_1}) \cdots (b_{t1} \ldots b_{tr_t})$ a decomposição em ciclos disjuntos de β. Tome

$$\begin{aligned}\{c_1, \ldots, c_k\} &= \{1, \ldots, n\} \setminus \cup_{i=1}^{t} \{a_{i1}, \ldots, a_{ir_i}\}\\ \{d_1, \ldots, d_k\} &= \{1, \ldots, n\} \setminus \cup_{i=1}^{t} \{b_{i1}, \ldots, b_{ir_i}\}.\end{aligned}$$

Tome $\sigma \in S_n$ dada por

$$\sigma := \begin{pmatrix} a_{11} & \cdots & a_{1r_1} & \cdots & a_{t1} & \cdots & a_{tr_t} & c_1 & \cdots & c_k \\ b_{11} & \cdots & b_{1r_1} & \cdots & b_{t1} & \cdots & b_{tr_t} & d_1 & \cdots & d_k \end{pmatrix}.$$

Aplicando a parte (a), é imediato verificar que $\sigma\rho\sigma^{-1} = \beta$. Observe que para cada ordenação do conjunto $c_1, \ldots, c_k$ obtemos uma permutação diferente que funciona.

(iii) Pela parte (b), existe $\sigma \in S_n$ tal que $\beta = \sigma\rho\sigma^{-1}$. Usando as mesmas notações de (b), como ρ fixa pelo menos duas letras, então $k \geq 2$. Tomando

$$\mu := \begin{cases} \sigma, & \text{se } \sigma \in A_n \\ \sigma(c_1c_2), & \text{se } \sigma \notin A_n \end{cases}.$$

o resultado segue.

$\diamond$

Proposição 1.8.5. *Seja $n \geq 3$. Então $A_n = \langle\{3\text{-ciclos}\}\rangle$.*

Prova: Se (ijk) é um 3-ciclo qualquer, então como $(ijk) = (ik)(ij)$ temos $(ijk) \in A_n$. Logo $\langle\{3\text{-ciclos}\}\rangle \subseteq A_n$. Agora, seja $\tau \in A_n$. Assim $\tau = \sigma_1\sigma_2\cdots\sigma_m$ com σ_i transposição para $i = 1, \ldots, m$ e m par. Logo se mostrarmos que $\sigma_i\sigma_j$ é um 3-ciclo, então τ será um produto de 3-ciclos. Para simplificar a notação, sejam α e β duas transposições. Se α e β são disjuntas, digamos $\alpha = (ij)$ e $\beta = (kl)$, então

$$\alpha\beta = (ij)(kl) = [(ij)(ki)][(ki)(kl)] = (ikj)(ikl)$$

e assim $\alpha\beta$ é um produto de dois 3-ciclos. Se α e β não são disjuntas, digamos $\alpha = (ij)$ e $\beta = (jk)$, então $\alpha\beta = (ij)(jk) = (ijk)$ é um 3-ciclo. Logo $\alpha\beta$ é sempre um produto de 3-ciclos se α e β são transposições. Logo o mesmo ocorre com τ e daí $\tau \in \langle\{3\text{-ciclos}\}\rangle$. Portanto, $A_n = \langle\{3\text{-ciclos}\}\rangle$. $\diamond$

Definição 1.21. *Um grupo G é chamado de **simples** se $\{1\}$ e G são seus únicos subgrupos normais.*

Teorema 1.10. *Seja $n = 3$ ou $n \geq 5$. Então o grupo alternado A_n é um grupo simples.*

Prova: O grupo A_3 tem ordem 3 e portanto é simples.

Sejam $n \geq 5$ e $H \neq \{1\}$ um subgrupo normal de A_n. Queremos mostrar que $H = A_n$. Pela Proposição 1.8.5 é suficiente mostrar que H contém todos os 3-ciclos.

Suponha que H contenha um 3-ciclo (abc). Como $n \geq 5$, então $\rho = (abc)$ fixa pelo menos duas letras e daí pelo Lema 1.8.3 para todo 3-ciclo (ijk), existe $\sigma \in A_n$ tal que $(ijk) = \sigma(abc)\sigma^{-1}$. Mas $H \trianglelefteq A_n$, logo $(ijk) \in H$. Portanto $H = A_n$.

Vamos mostrar agora que H sempre contém um 3-ciclo. Como $H \neq \{1\}$, então existe $\sigma \in H$, $\sigma \neq (1)$. Denote $m = |\sigma| > 1$. Seja p um divisor primo de m. Assim $\tau = \sigma^{m/p} \in H$ é tal que $|\tau| = p$. Escreva $\tau = \rho_1\cdots\rho_l$, onde $\rho_i \cap \rho_j = \emptyset$ para todo $i \neq j$. Sabemos que $p = |\sigma| = \text{m.m.c}\{|\rho_1|, \ldots, |\rho_l|\}$. Portanto, ρ_i é um p-ciclo para $i = 1, \ldots, l$.

1^o *Caso:* $p = 2$

Neste caso todos os ρ_i's são transposições e l é um inteiro par pois $\tau \in H \subseteq A_n$. Assim $l \geq 2$ e denotando $\rho_1 = (ab)$, $\rho_2 = (cd)$, temos $\tau = (ab)(cd)\rho_3\cdots\rho_l$. Agora como um 3-ciclo é um produto de duas transposições com um elemento em comum, precisamos encontrar em H um produto da forma $(ik)(ij)$. Para fazer isso, primeiro vamos mostrar que se (ab) e (cd) forem transposições disjuntas, então $(ac)(bd) \in H$. Como (ab) e (cd) são disjuntos, sabemos que para $\sigma = (abc)$ temos $\sigma(ab)(cd)\sigma^{-1} = (\sigma(a)\sigma(b))(\sigma(c)\sigma(d))$. Assim

$$\sigma(ab)(cd)\sigma^{-1} = (bc)(ad).$$

Como $\sigma = (abc)$ e ρ_i, com $i \geq 3$, são disjuntos (pois caso contrário teríamos em τ um r-ciclo com $r \geq 2$), eles comutam. Logo

$$\sigma\tau\sigma^{-1} = (abc)(ab)(cd)\rho_3 \dots \rho_l(abc)^{-1} = (ad)(bc)\rho_l(abc)^{-1} = (ad)(bc)\rho_3 \dots \rho_l \in H$$

pois $\tau \in H \trianglelefteq A_n$ e $(abc) \in A_n$. Mas $\tau^{-1} \in H$, daí

$$\sigma\tau\sigma^{-1}\tau^{-1} = (ad)(bc)\rho_3 \dots \rho_l\rho_l^{-1} \dots \rho_3^{-1}(bc)(ad) = (ad)(bc)(cd)(ab) = (ac)(bd) \in H,$$

como queríamos.

Agora tomando $K \neq a, b, c, d$, o que é possível pois $n \geq 5$, temos

$$(akc)(ac)(bd)(akc)^{-1} = (ak)(bd) \in H,$$

pois $(ac)(bd) \in H \trianglelefteq A_n$ e $(akc) \in A_n$. Portanto $(ac)(bd)(ak)(bd) = (ac)(ak)(bd)(bd) = (akc) \in H$ e com isso $H = A_n$.

2^o *Caso:* $p = 3$

Se $l = 1$, então $\tau = \rho_1$ é um 3-ciclo em H e acabou.

Se $l \geq 1$, denote $\rho_1 = (abc)$ e $\rho_2 = (def)$. Então $\tau = (abc)(def)\rho_3 \dots \rho_l$. Como por hipótese todos os ρ_i's são disjuntos, então a, b, c, d, e e f não aparecem nos outros 3-ciclos $\rho_3, \dots,$ ρ_l. Assim o 3-ciclo (bcd) é disjunto de $\rho_3, \dots, \rho_l$ e com isso comuta com todos eles. Logo

$$(bcd)\tau(bcd)^{-1} = (bcd)(abc)(def)\rho_3 \dots \rho_l(bcd)^{-1} = (acd)(bef)\rho_3 \dots \rho_l \in H$$

e como $\tau^{-1} \in H$ então

$$(bcd)\tau(bcd)^{-1}\tau^{-1} = (bcd)(abc)(def)\rho_3 \dots \rho_l(bcd)^{-1} = (acd)(bef)\rho_3 \dots \rho_l\rho_l^{-1} \dots \rho_3^{-1}(dfe)(acb) = (acd)(bef)(dfe)(a$$

Logo H contém um 5-ciclo e assim em particular um elemento de ordem 5. Daí basta provar o caso $p > 3$.

3^o *Caso:* $p > 3$

Seja $\rho_1 = (a_1a_2a_3a_4\ldots a_p$ e $\tau = (a_1a_2a_3a_4\ldots a_p)\rho_2\cdots\rho_l$. Novamente, por hipótese, todos os ρ_i's são disjuntos e assim $a_1, a_2, a_3, a_4, \ldots, a_p$ não aparecem em $\rho_2, \ldots, \rho_l$. Logo o 3-ciclo $(a_1a_2a_3)$ é disjunto de $\rho_2, \ldots, \rho_l$ e então comuta com eles. Daí

$$(a_1a_2a_3)\tau(a_1a_2a_3)^{-1} = (a_2a_3a_1a_4\ldots a_p)\rho_2\cdots\rho_l \in H$$

e com isso

$$(a_1a_2a_3)\tau(a_1a_2a_3)^{-1}\tau^{-1} = (a_2a_3a_1a_4\ldots a_p)(a_1a_2a_3a_4\ldots a_p)^{-1} \in H.$$

Mas $(a_1a_2a_3a_4\ldots a_p)^{-1} = (a_1a_pa_{p-1}\ldots a_4a_3a_2)$ e com isso

$$(a_2a_3a_1a_4\ldots a_p)(a_1a_pa_{p-1}\ldots a_4a_3a_2) = (a_1a_2a_4) \in H.$$

Logo $H = A_n$, provando assim que A_n é simples se $n = 3$ ou $n \geq 5$. ◊

Teorema 1.11. *Seja* $K = \{(1), (12)(34), (13)(24), (14)(23)\}$. *Então* $K \leq S_n$, *chamado de grupo de Klein pois todos os seus elementos têm ordem 2. Mais ainda,* $\{(1)\}$, K *e* A_4 *são os únicos subgrupos normais de* A_4.

Prova: É imediato verificar que $K \leq S_4$. Provemos então que $K \trianglelefteq S_4$. Como os elementos de S_4 podem ser escritos como produtos de ciclos disjuntos, então $A_4 = \{\text{3-ciclos}\} \cup K$. Daí o único sugrupo de ordem 4 em A_4 é K. Logo $K \trianglelefteq S_4$.

Agora seja $H \neq \{(1)\}$ um subgrupo normal em A_4. Se H contém um 3-ciclo, digamos (123), então $(132) = (123)^{-1} \in H$. ASSIM $(124) = (324)(132)(324)^{-1} \in H$ pois $H \trianglelefteq A_4$. Mas $A_4 = \langle (123), (124) \rangle$ e com isso $H = A_4$.

Se H não contém nenhum 3-ciclo, então ele deve conter um elemento diferente de (1), digamos $(12)(34)$. Assim $(13)(24) = (234)(12)(34)(234)^{-1} \in H$ e $(14)(23) = (12)(34)(13)(24) \in H$. Portanto $H = K$ e o resultado está provado. ◊

Corolário 1.8.3. *(i) Seja* $n = 3$ *ou* $n \geq 5$. *Então os grupos* $\{(1)\}$, A_n *e* S_n *são os únicos subgrupos normais de* S_n. *Em particular, o grupo alternado* A_n *é o único subgrupo normal de* S_n *de índice 2.*

(ii) *Sejam $n = 4$ e K o grupo de Klein. Então $\{(1)\}$, K, A_4 e S_4 são os únicos subgrupos normais de S_4. Em particular, o grupo alternado A_4 é o único subgrupo de S_4 de índice 2.*

Corolário 1.8.4. *Seja $n \geq 5$. Então*

(i) $(S_n)' = A_n$, $(A_n)' = A_n$;

(ii) $Z(S_n) = \{(1)\}$, $Z(A_n) = \{(1)\}$;

(iii) $\mathcal{I}(S_n) \cong S_n$, $\mathcal{I}(A_n) \cong A_n$.

1.9 Teoremas de Sylow

Definição 1.22. *Sejam G um grupo, C um conjunto e $\mathcal{P}(C)$ o grupo de permutações de C. Uma* ***representação de G no grupo de permutações de C*** *é um homomorfismo $\rho : G \to \mathcal{P}(C)$. Dizemos também que G* ***opera sobre o conjunto*** *C.*

Exemplos 1.9.1. 1. *Sejam G um grupo. Denote por G_0 o conjunto formado pelos elementos de G, sem a operação de grupo. Defina $C = G_0$ e seja*

$$\begin{aligned}\mathcal{I} : G &\to \mathcal{P}(G_0)\\ g &\mapsto \mathcal{I}_g : G_0 \to G_0\\ &\qquad\qquad a \mapsto gag^{-1}.\end{aligned}$$

É imediato verificar que $\mathcal{I}$ é um homomorfismo de grupos, logo uma representação de G no grupo de permutações do conjunto G_0.

2. *Seja G um grupo e seja H um subgrupo normal de G. Considere a aplicação*

$$\begin{aligned}\mathcal{I} : G &\to \mathcal{P}(H_0)\\ g &\mapsto \mathcal{I}_g : H_0 \to H_0\\ &\qquad\qquad a \mapsto gag^{-1}.\end{aligned}$$

é uma representação do grupo G no grupo das permutações do conjunto H_0.

3. *Seja G um grupo e seja $C = \{H \mid H \leq G\}$. A aplicação*

$$\begin{aligned} \mathcal{I} : G &\to \mathcal{P}(C) \\ a &\mapsto \mathcal{I}_a : C \to C \\ &\qquad\qquad a \mapsto aHa^{-1}. \end{aligned}$$

Sejam G um grupo, C um conjunto e $\rho : G \to \mathcal{P}(C)$ uma representação de G. Sobre o conjunto G definimos uma relação de equivalência dada por: para todos $x, y \in C$

$$x \sim y \text{ se, e somente se, existe } g \in G \text{ tal que } \rho(g)(x) = y$$

onde $\rho(g) \in \mathcal{P}(C)$.

Definição 1.23. *Seja $x \in C$. A **órbita** de x é o conjunto*

$$\mathrm{orb}(x) := \{y \in C \mid y \sim x\} = \{\rho(a)(x) \mid a \in G\}.$$

*O **estabilizador** de x é o conjunto de elementos de G que deixam o elemento x fixo, isto é,*

$$E(x) := \{a \in G \mid \rho(a)(x) = x\}.$$

É imediato verificar que o estabilizador $E(x)$ é um subgrupo de G.

Teorema 1.12. *Seja $\rho : G \to \mathcal{P}(C)$ uma representação do grupo G no grupo de permutações do conjunto C. Seja $x \in G$. Então a aplicação ψ dada por*

$$\psi : \mathrm{orb}(x) \to \{\textit{Classes laterais à esquerda de } E(X) \textit{ em } G\} \tag{1.8}$$

$$\rho(a)(x) \mapsto aE(x) \tag{1.9}$$

é uma bijeção. Em particular, no caso de G ser um grupo finito, temos $|\mathrm{orb}(x)| = [G : E(x)]$ e que $|\mathrm{orb}(x)|$ divide $|G|$.

Definição 1.24. *Dado um subgrupo H de um grupo G, o conjunto*

$$N_G(H) = \{a \in G \mid aHa^{-1} = H\}$$

*é chamado de **normalizador de** H **em** G.*

Proposição 1.9.1. *Seja H um subgrupo de um grupo G. Então $N_G(H)$ é um subgrupo de G e $H \trianglelefteq N_G(H)$. Mais ainda, $H \trianglelefteq G$ se, e somente se, $N_G(H) = G$.*

Lema 1.9.1. *No caso da representação*

$$\begin{aligned} \mathcal{I} : G &\to \mathcal{P}(C) \\ a &\mapsto \mathcal{I}_a : C \to C \\ & \qquad\qquad a \mapsto aHa^{-1}. \end{aligned}$$

onde G é um grupo e $C = \{H \mid H \leq G\}$ temos

$$|\{conjugados\ de\ H\ em\ G\}| = [G : N_G(H)].$$

Prova: Basta aplicar o Teorema 1.12. ◇

Teorema 1.13 (1^0 Teorema de Sylow)**.** *Seja G um grupo finito tal que $|G| = p^m b$, onde p é primo e* m.d.c $\{p, b\} = 1$. *Então, para cada i, $0 \leq i \leq m$, existe um subgrupo H de G tal que $|H| = p^i$.*

Prova: A demonstração será por indução sobre a ordem de G.

Se $|G| = 1$, então nada há a fazer. Assim, suponha que $|G| > 1$ e que o teorema seja válido para todo grupo de ordem menor que a ordem de G. Seja p o primo que aparece no enunciado do teorema. Considere o centro, $Z(G)$, de G. Temos duas possibilidades para o primo p.

1^o *Caso:* $p \mid |Z(G)|$

Neste caso, pelo Teorema de Cauchy, existe $g \in Z(G)$, $g \neq 1$ tal que $|g| = p$. Seja $N =< g >$, assim como $N \trianglelefteq Z(G)$ e $Z(G)$ é característico em G, segue que $N \trianglelefteq G$. Logo G/N é um grupo e $|G/N| = p^{m-1}b < |G|$ e daí pela hipótese de indução, para cada t, $0 \leq t \leq m-1$, existe $\overline{S}$ subgrupo de G/N tal que $|\overline{S}| = p^t$. Agora, considere o homomorfismo

$$\begin{aligned} f : G &\to G/N \\ g &\mapsto Ng \end{aligned}$$

Temos que $f^{-1}(\overline{S})$ é um subgrupo de G tal que $\ker(f) \subset f^{-1}(\overline{S})$. Inicialmente temos $\ker(f) = N$ pois como $f(g) = Ng$, se tomarmos $g \in N$ teremos $Ng = N$. Agora dado

$g \in \ker(f)$, $f(g) = Ng = N$ e como $\overline{S}$ é um subgrupo de G/N temos que $N \in \overline{S}$ e assim $f(g) \in \overline{S}$ e consequentemente $g \in f^{-1}(\overline{S})$, ou seja, $\ker(f) \subset f^{-1}(\overline{S})$. Daí

$$|f^{-1}(\overline{S})| = |N||\overline{S}| = p^{t+1},$$

e assim para cada $n,\ 0 \leq n \leq m$, existe H subgrupo de G tal que $|H| = p^n$.

2^o *Caso:* $p \nmid |Z(G)|$

Neste caso, sejam $G^* = G - Z(G)$ e S_{G^*} o conjunto de todas as bijeções de G^* em G^* (S_{G^*} é um grupo com a operação de composição de funções). Considere a aplicação

$$\begin{aligned} \phi : G &\to S_{G^*} \\ g &\mapsto \phi_g : G^* \to G^* \\ &\qquad x \mapsto x^g = gxg^{-1} \end{aligned}$$

Inicialmente temos que ϕ está bem definida. De fato, seja $y \notin Z(G)$, então $y^x \notin Z(G)$, pois caso contrário teríamos $y^x \in Z(G)$ e com isso $(y^x)^{x^{-1}} \in Z(G)$. Finalmente, $(y^x)^{x^{-1}} = x^{-1}(xyx^{-1})x = y \notin Z(G)$. Mais ainda, ϕ é um homomorfismo de grupos, pois se $g, h \in G$, então

$$\begin{aligned} \phi_{gh}(x) = x^{gh} &= (gh)x(gh)^{-1} = (gh)x(h^{-1}g^{-1}) = g(hxh^{-1})g^{-1} \\ &= g(\phi_h(x))g^{-1} = \phi_g(\phi_h(x)) = (\phi_g\phi_h)(x). \end{aligned}$$

Logo $\phi_{gh} = \phi_g\phi_h$ e assim ϕ é uma representação de G em S_{G^*}.

Agora, observando que $\phi_g(x) = gxg^{-1} = y \in G^*$, denote por $\mathrm{orb}_\phi(x)$ a classe de equivalência de x em G^*. Temos

$$\mathrm{orb}_\phi(x) = \{y \in G^* : y \sim x\} = \{y \in G^* : \phi_g(x) = y,\ \text{para algum}\ \ g \in G\}$$

e assim

$$G^* = \bigcup \mathrm{orb}_\phi(x)$$

e segue também que $|G^*| = \sum |\mathrm{orb}_\phi(x)|$.

Pela Proposição 1.6.3, temos

$$|\mathrm{orb}_\phi(x)| = |G : C_x|,$$

onde

$$\begin{aligned} C_x &= \{g \in G : \phi_g(x) = x\} = \{g \in G : gxg^{-1} = x\} \\ &= \{g \in G : gx = xg\} = C_G(x) \end{aligned}$$

e daí $|\text{orb}_\phi(x)| = |G : C_G(x)|$.

Como $G^* = G - Z(G)$ temos que $|G^*| = |G| - |Z(G)|$ e como $p \mid |G|$ e $p \nmid |Z(G)|$, então $p \nmid |G^*|$. Por outro lado, $|G^*| = \sum |G : C_G(x)|$ e assim existe $x \in G^*$ tal que $p \nmid |G : C_G(x)|$. Como $x \in G^*$, então $x \notin Z(G)$ e assim $C_G(x)$ é um subgrupo próprio de G, ou seja, $|C_G(x)| < |G|$ e daí pela hipótese de indução $C_G(x)$ possui um subgrupo de ordem p^n para cada $p^n \mid |C_G(x)|$ e consequentemente o mesmo ocorre em G. $\diamond$

Corolário 1.9.1. *Seja G um grupo finito e seja p um número primo. Seja p^m a maior potência de p que divide $|G|$. Então existe um subgrupo de G de ordem p^m.*

Definição 1.25. *Sejam G um grupo finito tal que $|G| = p^m b$, onde p é primo e* m.d.c $\{p, b\} = 1p$. *Os subgrupos de G que têm ordem p^m são chamados de **p-subgrupos de Sylow** de G.*

Lema 1.9.2. *Sejam G um grupo finito e p um número primo. Sejam H um p-subgrupo de Sylow de G e K um p-subgrupo qualquer de G. Então $K \cap N_G(H) = K \cap H$.*

Prova: Suponhamos que $K \cap H \subsetneq K \cap N_G(H)$ e seja $x \in K \cap N_G(H) \backslash H$. O elemento x tem ordem igual a uma potência de p pois $x \in K$ e por hipótese K é um p-grupo de G. Como $x \in N_G(H)$, então $\langle x \rangle$ é um subgrupo de $N_G(H)$. Mas $H \trianglelefteq N_G(H)$ e daí $\langle x \rangle H$ é um subgrupo de $N_G(H)$ e portanto um subgrupo de G. Além disso, sabemos que

$$|\langle x \rangle H| = \frac{|\langle x \rangle||H|}{|\langle x \rangle \cap H|},$$

onde $|\langle x \rangle|$ e $|H|$ são potências de p e $|\langle x \rangle \cap H| < |\langle x \rangle|$ pois $x \notin H$. Logo, $\langle x \rangle H$ é um p-subgrupo de G de ordem maior que $|H|$, o que é um absurdo pois H é um p-subgrupo de Sylow de G. $\diamond$

Teorema 1.14 (2^o Teorema de Sylow)**.** *Seja G um grupo finito, p um número primo e seja n_p o número de p-subgrupos de Sylow de G. Então:*

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

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

(iii) Se S é um p-subgrupo de Sylow de G, então $n_p = [G : N_G(S)]$.

Prova:

Seja S um p-subgrupo de Sylow qualquer de G. Considere o conjunto $C = \{aSa^{-1} \mid a \in G\}$. Por definição o conjunto C é a órbita de S na representação por conjugação $\mathcal{I} : G \to \mathcal{P}(D)$ onde $D = \{H \leq G\}$. Portanto pelo Teorema 1.12

$$|C| = [G : N_G(S)].$$

Para os itens *(i)* e *(ii)* basta mostrar que se H é um p-subgrupo qualquer de G, então H está contido num conjugado de S em G.

Assim, considere a seguinte representação de P:

$$\begin{aligned} \mathcal{I} : P &\to \mathcal{P}(C) \\ g &\mapsto \mathcal{I}_g : C \to C \\ &\qquad gSg^{-1} \mapsto agSg^{-1}a^{-1}. \end{aligned}$$

Sejam $\mathcal{O}_1, \ldots, \mathcal{O}_k$ as órbitas distintas desta representação e para cada $\mathcal{O}_i$ escolha um representante $S_i = g_iSg_i^{-1}$ dentro de $\mathcal{O}_i$. Temos

$$|C| = \sum_{i=1}^{k} |\mathcal{O}_i| \tag{1.10}$$

e além disso, pelo Teorema 1.12 temos $|\mathcal{O}_i| = [P : E(S_i)] = [P : P \cap N_G(S_i)]$ e pelo Lema 1.9.2 temos $[P : P \cap N_G(S_i)] = [P : P \cap S_i]$. Portanto obtemos

$$|C| = \sum_{i=1}^{k} [P : P \cap S_i]. \tag{1.11}$$

Assim de (1.10) e (1.11) encontramos

$$[G : N_G(S)] = \sum_{i=1}^{k} [P : P \cap S_i]. \tag{1.12}$$

Cada parcela $[P : P \cap S_i]$ é igual a 1 ou a um múltiplo de p, pois P é um p-grupo. Por outro lado, o primo p não divide $[G : S]$ pois S é um p-subgrupo de Sylow e daí não divide $[G : N_G(S)]$. Consequentemete existe um j tal que p não divide $[P : P \cap S_j]$, ou seja, tal que $[P : P \cap S_j] = 1$ e portanto tal que $P \subseteq S_j$.

Agora, pelo item (i) temos $\{p\text{-subgrupos de Sylow}\} = \{\text{conjugados de } S\}$. Logo $n_p = [G : N_G(S)]$. Assim provamos o item *(iii)*. $\diamond$

Teorema 1.15 (3º Teorema de Sylow)**.** *Sejam p um número primo e G um grupo finito de ordem $|G| = p^m b$, com* m.d.c $\{p, b\} = 1$*. Seja n_p o número de p-subgrupos de Sylow de G. Então*

$$\begin{cases} n_p \mid b \\ n_p \equiv 1 \pmod p \end{cases}.$$

Prova: Seja S um p-subgrupo de Sylow de G. É imediato que $[G : N_G(S)]$ divide $[G : S] = b$.

Agora, considere a expressão (1.12) obtida na demonstração do Teorema 1.14. Tomando $P = S$ temos

$$[G : N_G(S)] = \sum_{i=1}^{k} [S : S \cap S_i]$$

onde $S_1, \ldots, S_k$ são representantes das distintas órbitas $\mathcal{O}_1, \ldots, \mathcal{O}_k$ da seguinte representação

$$\mathcal{I} : S \to \mathcal{P}(C)$$

onde C é o conjunto dos p-subgrupos de Sylow de G. Fazendo $S_1 = S$ obtemos

$$[G : N_G(S)] = [S : S \cap S] + \sum_{i=2}^{k} [S : S \cap S_i] \equiv 1 \pmod p.$$

Assim o resultado segue. $\diamond$

Proposição 1.9.2. *Sejam H um p-subgrupo de Sylow de um grupo finito G e $K \leq G$. Se $H \subseteq K$, então $K = N_G(K)$.*

Prova: Seja $x \in N_G(K)$. Como $H \subseteq K \trianglelefteq N_G(K)$, segue que $xHx^{-1} \subseteq K$. Mas H e xHx^{-1} são p-subgrupos de Sylow de K, daí existe $y \in H$ tal que $xHx^{-1} = yHy^{-1}$. Assim $y^{-1}x \in N_G(H) \subseteq K$. Ou seja, $x \in K$ e portanto $N_G(H) = H$. $\diamond$

Corolário 1.9.2. *Seja H um p-subgrupo de Sylow de um grupo finito G. Então $N_G(N_G(H)) = N_G(H)$.*

Prova: Basta tomar $K = N_G(H)$ na proposição anterior. $\diamond$

Exemplos 1.9.2. 1. *Se $|G| = 6$, então $n_2 = 1$ ou $n_2 = 3$. Sem outras informações sobre G não é possível determinar o valor de n_2.*

2. *Seja G um grupo de ordem 380. Então $|G| = 2^2 \cdot 5 \cdot 19$. Assim em G, existem subgrupos de ordem 2, 4, 5, e 19. Para o caso do subgrupo de ordem 5 pelo Terceiro Teorema de Sylow, Teorema 1.15, temos $n_5 \equiv 1 \pmod 5$ e $n_5 \mid 2^2 \cdot 19$. Logo $n_5 = 1$ ou $n_5 = 76$. De modo análogo, obtemos $n_{19} = 1$ ou $n_{19} = 20$. Sejam $H, K \leq G$ tais que $|H| = 5$ e $|K| = 19$.*

   Se $n_5 = 76$, então G possui $76 \times 4 = 304$ elementos de ordem 5, pois a interseção de dois subgrupos distintos de G com ordem 5 é trivial. E se $n_{19} = 20$, então existem $20 \times 18 = 360$ elementos de ordem 19, o que é impossível pois $|G| = 380$. Portanto, $n_5 = 1$ ou $n_{19} = 1$ e daí H ou K é normal em G. Considere então o subgrupo HK de G de ordem $5 \cdot 19$, pois $H \cap K = \{1\}$. Aplicando o Terceiro Teorema de Sylow ao grupo HK, existem um único subgrupo de ordem 5, que é obrigatoriamente H e somente um subgrupo de ordem 19, que é K. Assim $H \trianglelefteq HK$ e $K \trianglelefteq HK$. Daí $HK \subseteq N_G(H)$ e com isso $n_5 = [G : N_G(H)] \leq [G : HK] = 2^2$. Mas $n_5 = 1$ ou $n_5 = 76$. Logo $n_5 = 1$. Analogamente, $HK \subseteq N_G(K)$ e dái $n_{19} = 1$ pois $n_{19} = [G : N_G(K)] \leq [G : HK] = 2^2$.

   Portanto G não é simples.

3. *Todo grupo de ordem 159 é cíclico.*

   De fato, seja G um grupo de ordem 159. Assim como $|G| = 3 \cdot 53$, então existem subgrupos $H, K \leq G$ tais que $|H| = 3$ e $|K| = 53$. Além disso, sejam n_3 e n_{53} o número de 5-subgrupos de Sylow e de 53-subgrupos de Sylow de G. Então

$$n_3 \mid 53, \; n_3 \equiv 1 \pmod 3$$
$$n_{59} \mid 3, \; n_{53} \equiv 1 \pmod{53}.$$

   Logo $n_3 = 1$ e $n_{53} = 1$. Daí $H \trianglelefteq G$ e $K \trianglelefteq G$. Com isso HK é um subgrupo de G de ordem $3 \cdot 53$ pois $H \cap K = \{1\}$. Então $G = HK$. Finalmente, tomando x gerador de H e y gerador de K é fácil mostrar que $G = \langle xy \rangle$, como queríamos.

4. *Seja G um grupo de ordem $56 = 2^3 \cdot 7$. Então G possui um subgrupo normal de ordem 7 ou um subgrupo normal de ordem 8.*

   De fato, seja n_7 o número de 7-subgrupos de Sylow de G. Então

$$n_7 \mid 8$$
$$n_7 \equiv 1 \pmod 7.$$

   Daí $n_7 = 1$ ou $n_7 = 8$. Se $n_7 = 1$, então este 7-subgrupo de Sylow é normal em G.

   Se $n_7 = 8$, então se K_1 e K_2 são dois 7-subgrupos de Sylow de G e distintos, então $K_1 \cap K_2 = \{1\}$. Logo existem $8 \times 6 = 48$ elementos distintos de ordem 7. Como $|G| = 56$ e G possui um subgrupo H tal que $|H| = 8$, então estes 8 elementos restantes devem pertencer a H pois nenhum elemento de ordem 7 pode pertencer a H. Portanto H é único, ou seja, $H \trianglelefteq G$. Ou seja, G possui um subgrupo normal de ordem 8.

5. *Seja G um grupo tal que $|G| = p(p+2)$, onde p e $p+2$ são primos, chamados de primos gêmeos. Então G é cíclico.*

   De fato, seja $q = p + 2$. Assim $n_q \mid p$ e $n_q \equiv 1 \pmod q$. Logo $n_q = 1$. Portanto seja $H \leq G$ tal que $|H| = q$. Então $H \trianglelefteq G$.

   Agora $n_p \mid q$ e $n_p \equiv 1 \pmod q$. Daí $n_p = 1$ e $K \trianglelefteq G$, onde $|K| = p$. Além disso, $H \cap K = \{1\}$ e HK é um subgrupo de G de ordem $p(p+2)$. Portanto $G \cong H \times K$. Mas $H \cong \mathbb{Z}_{p+2}$ e $K \cong \mathbb{Z}_p$. Portanto $G \cong \mathbb{Z}_p \times \mathbb{Z}_{p+2} \cong \mathbb{Z}_{p(p+2)}$ é um grupo cíclico.

Grupos livres

1.10 Grupos Solúvies

O conceito de grupos solúveis foi introduzido por E. Galois quando estudava o problema de resolver equações algébricas por meio de radicais.

Definição 1.26. *Um grupo G é chamado de **solúvel** se contém uma cadeia de subgrupos*

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G \tag{1.13}$$

*tal que cada G_{i-1} é normal em G_i e o grupo quociente G_i/G_{i-1}, $1 \leq i \leq n$, é abeliano. Uma cadeia de G com esta propriedade chama-se uma **série subnormal abeliana** de G e os quocientes respectivos, chamam-se os **fatores** da série.*

Exemplos 1.10.1. 1. *Todo grupo abeliano é solúvel.*

2. *O grupo S_3 é solúvel. De fato, em S_3 tomando $\sigma = (123)$ e $H = \langle\sigma\rangle$, então $|G/H| = 2$. Logo $H \trianglelefteq S_3$ e G/H é abeliano. Como H é cíclico, então H é abeliano e com isso a cadeia $\{1\} \subseteq H \subseteq S_3$ é uma série subnormal abeliana para S_3.*

3. *O grupo S_4 é solúvel. De fato, uma série subnormal abeliana para S_4 é dada por $\{1\} \subseteq K \subseteq A_4 \subseteq S_4$, onde K é o grupo de Klein.*

4. *Para $n \geq 5$, S_n e A_n não são solúveis.*

5. *O grupo dihedral D_{2n} é solúvel. Basta tomar a série $\{1\} \subseteq H \subseteq D_{2n}$, onde H é o subgrupo gerado por b, tal que $|b| = n$.*

Proposição 1.10.1. *Todo p-grupo finito é solúvel.*

Prova: Suponha que G é um grupo com $|G| = p^n$, com $n \geq 1$. Queremos encontrar série subnormal

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_t = G$$

tal que $G_{i-1} \trianglelefteq G_i$ e G_i/G_{i-1} é abeliano para $1 \leq i \leq n$.

Na verdade, vamos mostar que é possível encontrar uma cadeia de subgrupos normais de G tais que

$$\{1\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_t = G$$

tal que cada quociente H_{i+1}/H_i é de ordem p e está contido no centro de G/H_i, $1 \leq i \leq t-1$. Vamos mostrar tal fato por indução em n. Se $n = 1$, nada há a fazer. Suponha então que a afirmação é válida para todo grupo de ordem p^{n-1} e seja G um grupo de ordem p^n. Comom $|G| = p^n > 1$, então $Z(G) \neq \{1\}$. Seja $x \in Z(G)$, $x \neq 1$ tal que $|x| = p$. Denote por $K = \langle x\rangle$. Considere $\pi : G \to G/K$ a projeção canônica. Denote por $\overline{G} = G/K$. Assim $|\overline{G}| = p^{n-1}$ e aplicando a hipótese de indução, existe uma cadeia de subgrupos normais de $\overline{G}$

$$\{\overline{1}\} = \overline{K_1} \subseteq \overline{K_2} \subseteq \cdots \subseteq \overline{K_t} = \overline{G}$$

tal que $\overline{K_{i+1}}/\overline{K_i}$ tem ordem p e está contido no centro de $\overline{G}/\overline{K_i}$, $1 \leq i \leq t-1$. Agora do Teorema dos Isomorfismos, todo subgrupo normal de $\overline{G}$ é da forma $\overline{K_i} = K_i/K$, onde K_i é um subgrupo normal de G que contém K. Também do Teorema dos Isomorfismos temos

$$\frac{\overline{K_{i+1}}}{\overline{K_i}} = \frac{\frac{K_{i+1}}{K}}{\frac{K_i}{K}} \cong \frac{K_{i+1}}{K_i}.$$

Logo K_{i+1}/K_i tem ordem p e está contido no centro de G/K_i, $1 \leq i \leq t-1$. Logo

$$\{1\} = K_0 \subseteq K_1 = \langle x \rangle \subseteq K_2 \subseteq \cdots \subseteq K_t = G$$

é uma cadeia normal de G cujos quocientes têm ordem p como queríamos. Portanto G é solúvel. $\diamond$

Definição 1.27. *1. Dados um grupo G e dois elementos $x, y \in G$ o **comutador** de x e y é o elemento*

$$[x, y] = x^{-1}y^{-1}xy \in G.$$

*Mais geralmente, um **comutador de comprimento** $n \geq 2$ é definido indutivamente por*

$$[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n],$$

onde $x_i \in G$ para $i = 1, \ldots, n$.

2. *Dados dois subconjuntos H e K de um grupo G, denotamos por $[H, K]$ o subgrupo de G gerado por*

$$[H, K] = \langle \{[x, y] = x^{-1}y^{-1}xy \mid x \in H, y \in K\} \rangle.$$

*Em particular o grupo $G' = [G, G]$ é chamado de **subgrupo comutador** ou **subgrupo derivado de** G. Indutivamente podemos definir uma sequeência de subgrupos de G da forma:*

$$\begin{aligned} &G^{(0)} = G \\ &G^{(1)} = [G^{(0)}, G^{(0)}] = [G, G] = G' \\ &\vdots \\ &G^{(n)} = [G^{(n-1)}, G^{(n-1)}]. \end{aligned}$$

3. *O subgrupo $G^{(n)}$ definido anteriormente é chamado de **n-ésimo grupo derivado** de G e a sequência*

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(n)} \supseteq \cdots$$

*chama-se **sequência derivada** de G.*

Lema 1.10.1. *Sejam G e H grupos e $\phi : G \to H$ um homomorfismo de grupos. Dados $x, y \in G$ temos $\phi([x, y]) = [\phi(x), \phi(y)]$.*

Prova: De fato

$$\phi([x, y]) = \phi(x^{-1}y^{-1}xy) = \phi(x^{-1})\phi(y^{-1})\phi(x)\phi(y) = [\phi(x), \phi(y)].$$

$\diamondsuit$

Definição 1.28. *Um subgrupo H de um grupo G é chamado de **subgrupo característico** se $\phi(H) = H$ para todo automorfismo $\phi : G \to G$. Denotamos tal fato por H car G.*

Observação 1.10.1. *Como $\phi_a : G \to G$ dada por $\phi_a(x) = a^{-1}xa$ é um automorfismo de G, então todo subgrupo característico de G é em particular normal em G.*

Proposição 1.10.2. *Seja H um subgrupo de um grupo G. Se H é característico em G, então H' também é característico em G. Em particular, $G^{(i)}$ é característico em G para todo $i \in \mathbb{N}$.*

Prova: Como $H' = \langle\{x^{-1}y^{-1}xy \mid x, y \in H\}\rangle$, basta mostrar que $\phi([x, y]) \in H'$ para todo $\phi : G \to G$ automorfismo.

Inicialmente temos $\phi([x, y]) = [\phi(x), \phi(y)]$ e como H *car* G $\phi(x), \phi(y) \in H$. Daí $\phi([x, y]) \in H'$. Portanto $\phi(H') = H'$, ou seja, H' é característico em G.

Agora como $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$, logo $\phi(G^{(n)}) = [\phi(G^{(n-1)}), \phi(G^{(n-1)})]$. Assim por indução segue que $G^{(i)}$ é característico em G para todo $i \geq 1$. $\diamondsuit$

Teorema 1.16. *Um grupo G é solúvel se, e somente se, sua série derivada termina, isto é, se existe um inteiro positivo n tal que $G^{(n)} = \{1\}$.*

Prova: Se existe n tal que $G^{(n)} = \{1\}$, então temos a série

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(n)} = \{1\}. \tag{1.14}$$

Inicialmente cada $G^{(i)}$ é normal em G pois é característico em G. Logo $G^{(i)}$ é normal em $G^{(i-1)}$ para $1 \leq i \leq n$. Agora, $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] = (G^{(i-1)})'$ e assim $G^{(i-1)}/G^{(i)}$ é abeliano para $1 \leq i \leq n$. Portanto a série (1.14) é uma série subnormal abeliana para G, ou seja, G é solúvel.

Agora suponha que G é solúvel. Assim existe uma série subnormal abeliana

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{1\}$$

onde G_{i+1} é normal em G_i e G_i/G_{i+1} é abeliano, $1 \leq i \leq t$. Vamos mostrar por indução em i que $G^{(i)} \leq G_i$. Como $G^{(0)} = G = G_0$, a base da indução é verdadeira. Suponha então que $G^{(i)} \leq G_i$. Como G_i/G_{i+1} é abeliano e $G_{i+1} \trianglelefteq G_i$, então $(G_i)' \leq G_{i+1}$. Mas pela hipótese de indução, $G^{(i)} \leq G_i$ daí

$$G^{(i+1)} = (G^{(i)})' \leq (G_i)' \leq G_{i+1}$$

como queríamos. Em particular, $G^{(n)} \leq G_n = \{1\}$, isto é, $G^{(n)} = \{1\}$. Portanto a série derivada termina. $\diamond$

Proposição 1.10.3. *Todo quociente de um grupo solúvel é solúvel.*

Prova: Seja

$$\{1\} = G_t \leq G_{t-1} \leq \cdots \leq G_2 \leq G_1 \leq G_0 = G$$

uma série subnormal abeliana para G. Seja $N \trianglelefteq G$. Assim NG_i é um subgrupo de G para $i = 1, \ldots, t$ e com isso obtemos uma série de subgrupos

$$\{1\} \leq N = NG_t \leq \cdots \leq NG_2 \leq NG_1 \leq NG_0 = G. \tag{1.15}$$

Mostremos que tal série é subnormal. Primeiro, como $NG_{i+1} \leq G$, então $(NG_{i+1})(NG_{i+1}) = NG_{i+1}$. Mais ainda, $NG_{i+1}N \leq (NG_{i+1})(NG_{i+1})$, daí

$$(ng_i)^{-1}(NG_{i+1})(ng_i) = g^{-1}(n^{-1}NG_{i+1}n)g_i \leq g_i^{-1}NG_{i+1}Ng_i \leq g_i^{-1}(NG_{i+1})g_i.$$

Agora, $N \trianglelefteq G$, logo $g_i^{-1}N = Ng^{-1}$ e então

$$(ng_i)^{-1}(NG_{i+1})(ng_i) \leq g_i^{-1}NG_{i+1}g_i = Ng_i^{-1}G_{i+1}g_i.$$

Mas $G_{i+1} \trianglelefteq G_i$ e com isso $Ng_i^{-1}G_{i+1}g_i \leq NG_{i+1}$. Portanto $(ng_i)^{-1}(NG_{i+1})(ng_i) \leq NG_{i+1}$, isto é, $NG_{i+1} \trianglelefteq NG_i$ para $0 \leq i \leq t$.

Como consequência do Teorema dos Isomorfismos temos

$$\frac{G_i}{G_i \cap (NG_{i+1})} \cong \frac{(NG_{i+1})G_i}{NG_{i+1}} = \frac{NG_i}{NG_{i+1}}$$

pois $G_{i+1}G_i = G_i$. Como $G_{i+1} \trianglelefteq (G_i \cap NG_i)$, então novamente pelo Teorema dos Isomorfismos a função $G/G_{i+1} \to G_i/(G_i \cap NG_{i+1})$ é sobrejetora. Logo o homomorfismo $G_i/G_{i+1} \to NG_i/NG_{i+1}$ é sobrejetor. Como G_i/G_{i+1} é abeliano, então NG_i/NG_{i+1} é abeliano. Portanto a série

$$\{\overline{1}\} = \frac{NG_t}{N} \leq \frac{NG_{t-1}}{N} \leq \cdots \leq \frac{NG_1}{N} \leq \frac{NG_0}{N} = \frac{G}{N}$$

é uma série subnormal abeliana para G/N, ou seja, G/N é solúvel. ◊

Proposição 1.10.4. *Todo subgrupo H de um grupo solúvel G é solúvel.*

Prova: Como G é solúvel, existe

$$\{1\} = G_t \leq G_{t-1} \leq \cdots \leq G_2 \leq G_1 \leq G_0 = G$$

uma série subnormal abeliana. Seja H um subgrupo de G e considere a série

$$\{1\} = H \cap G_t \leq H \cap G_{t-1} \leq \cdots \leq H \cap G_2 \leq H \cap G_1 \leq H \cap G_0 = H. \tag{1.16}$$

Se $h_{i+1} \in H \cap G_{i+1}$ e $g_i \in H \cap G_i$, então $g_i^{-1}h_{i+1}g_i \in H$ e também $g_i^{-1}h_{i+1}g_i \in G_{i+1}$ pois $G_{i+1} \trianglelefteq G_i$. Daí $g_i^{-1}h_{i+1}g_i \in H \cap G_{i+1}$, isto é, $H \cap G_{i+1} \trianglelefteq H \cap G_i$. Além disso,

$$\frac{H \cap G_i}{H \cap G_{i+1}} = \frac{H \cap G_i}{(H \cap G_i) \cap G_{i+1}} \cong \frac{G_{i+1}(H \cap G_i)}{G_{i+1}} \leq \frac{G_i}{G_{i+1}}$$

e como G_i/G_{i+1} é abeliano, então $(H \cap G_i)/(H \cap G_{i+1})$ é abeliano. Portanto (1.16) é uma série subnormal abeliana para H, ou seja, H é solúvel. ◊

Proposição 1.10.5. *Seja H um subgrupo normal de um grupo G. Se ambos H e G/H são solúveis, então G é solúvel.*

Prova: Como G/H e H são solúveis, existem séries subnormais abelianas

$$\{\overline{1}\} = \overline{K_0} \leq \overline{K_1} \leq \cdots \leq \overline{K_m} = G/H$$
$$\{1\} = P_0 \leq P_1 \leq \cdots \leq P_n = H.$$

Assim existem subgrupos $K_i \leq G$ tais que $\overline{K_i} = K_i/H$, $K_i \supseteq H$ e $K_i \trianglelefteq K_{i+1}$. Mais ainda

$$\frac{\overline{K_{i+1}}}{\overline{K_i}} \cong \frac{K_{i+1}}{K_i}$$

e daí K_{i+1}/K_i é abeliano. Logo

$$\{1\} = P_0 \leq P_1 \leq \cdots \leq P_{n-1} \leq P_n = H = K_0 \leq K_1 \leq \cdots \leq K_m = G$$

é uma série subnormal abeliana para G. Portanto, G é solúvel. ◊

Corolário 1.10.1. *Se H e K são grupos solúveis, então $H \times K$ é solúvel.*

Prova: Como $(H \times K)/H \cong K$, o resultado segue da proposição anterior. ◊

Proposição 1.10.6. *Um grupo solúvel finito G contém uma série subnormal abeliana cujos fatores são todos cíclicos de ordem prima.*

Prova: A demonstração será por indução na ordem de G. Se $|G| = 1$, não há nada a fazer. Suponha então que $|G| = n > 1$ e que o resultado vale para todo grupo solúvel de ordem menor que n. Se $|G| = p$, com p primo então o resultado é verdadeiro. Assim suponha que a ordem de G não é um primo. Como G é solúvel, existe $H \trianglelefteq G$. Como $|H|$ e $|G/H|$ são menores que n, segue pela hipótese de indução que existem séries subnormais abelianas com fatores cíclicos

$$\{1\} = H_0 \leq H_1 \leq \cdots \leq H_m = H$$
$$\{\overline{1}\} = \overline{P_0} \leq \overline{P_1} \leq \cdots \leq \overline{P_n} = G/H.$$

Logo existem $P_i \leq G$, $H \subseteq P_i$, $P_i \trianglelefteq P_{i+1}$, $i = 0, \ldots, n-1$. Como

$$\frac{\overline{P_{i+1}}}{\overline{P_i}} = \frac{\frac{P_{i+1}}{H}}{\frac{P_i}{H}} \cong \frac{P_{i+1}}{P_i}$$

e então

$$\{1\} = H_0 \leq H_1 \leq \cdots \leq H_m = H = P_0 \leq P_1 \leq \cdots \leq P_m = G$$

é uma série subnormal para G onde os quocientes são cíclicos de ordem prima. $\diamond$

No início do secúlo passado W. Burnside provou, usando representações de grupos que:

Teorema 1.17 (Teorema de Burnside)**.** *Todo grupo finito cuja ordem é divisível no máximo por dois primos é solúvel.*

Burnside também conjeturou que: "Todo grupo de ordem ímpar é solúvel". Em um trabalho de mais de 200 páginas, W. Feit e J. Thompson provaram tal conjetura.

Teorema 1.18 (W. Feit & J. Thompson)**.** *Todo grupo de ordem prima é solúvel.*

1.11 Grupos Nilpotentes

Definição 1.29. *Um grupo G é chamado de **nilpotente** se existe uma série de subgrupos*

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_{n-1} \leq G_n = G \tag{1.17}$$

tal que cada subgrupo G_{i-1} é normal em G e cada quociente $G_i/G_{i-1} \subseteq Z(G/G_{i-1})$ para $1 \leq i \leq n$.

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