

Grupos

1) Seja G um grupo. Mostre que se $(ab)^2 = a^2b^2$, para quaisquer $a, b \in G$, então G é abeliano.

$$(ab)^2 = a^2b^2 \Rightarrow abab = a^2b^2$$

$$\Rightarrow a'abab b^{-1} = a'a^2b^2b^{-1} \Rightarrow ba = ab.$$

∴ G é abeliano

2) a) Seja G um grupo no qual $(ab)^i = a^i b^i$, para três inteiros consecutivos i e para quaisquer $a, b \in G$. Mostre que G é abeliano

b) Vale o mesmo $\xrightarrow{\text{resultado}}$ $(ab)^i = a^i b^i$, para apenas dois inteiros consecutivos i ?

a) Suponha que vale para $m-1, n$ e $n+1$.

$$\begin{aligned} (ab)^m &= a^m b^m = a(a^{n-1}b^{n-1})b = a(ab)^{n-1}b \\ &\qquad\qquad\qquad \left. \begin{array}{l} \text{vai de } m-1 \\ \text{vai de } n-1 \end{array} \right\} \Rightarrow (ab)^{n-1} = (ba)^{n-1} \quad (*) \\ a(ba)^{n-1}b & \end{aligned}$$

Usando $(ab)^{n+1} = a^{n+1}b^{n+1}$, obtemos, de modo análogo,

$$(ab)^n = (ba)^n$$

$$\text{Portanto } ab(ab)^{n-1} = ba(ba)^{n-1} \stackrel{(*)}{\Rightarrow} ab = ba$$

b) Nas vale.

Seja G grupo, $|G| = n$.

$$\text{Então } a^n b^n = e = (ab)^n$$

$$a^{n+1}b^{n+1} = ab = (ab)^{n+1}$$

mas nem todo grupo finito é abeliano

(por exemplo, S_3)

3) Seja G um conjunto não vazio com uma operação binária associativa.

Mostre que as seguintes condições são equivalentes:

a) G é um grupo;

b) para todos $a, b \in G$, as equações $bx = a$ e $yb = a$ têm pelo menos uma solução em G ;

c) existe $e \in G$ tq $ae = a$, para todo $a \in G$ e, para todo $a \in G$, existe $b \in G$ tal que $ab = e$ (i.e., tem "unidade à direita" e inverso à direita)

(a) \Rightarrow (b) ok

(b) \Rightarrow (c)

Seja $a \in G$. Entas $\exists e \in G$ tq $ae = a$. Vamos mostrar que $be = b$, $\forall b \in G$.

Para $b \in G$, existe $c \in G$ tq $ca = b$. Entas

$$be = cae = ca = b$$

A outra é imediata

(c) \Rightarrow (a)

Resta mostrar que $ea = a$ e $ba = e$.

Seja $c \in G$ tq $bc = e$. Entas $ba = ba e = \underline{ba}bc = \underline{be}c = bc = e$ (*)

Além disso, $ea = \underline{ab}a = ae = a$.

4) a) Seja G um grupo tal que $a^2 = e$, $\forall a \in G$. Mostre que G é abeliano.

b) O mesmo resultado é válido se G é um grupo tal que $a^3 = e$, para todo $a \in G$?

a) $(ab)^2 = e \Rightarrow abab = e \Rightarrow a(abab)b = ab$
 $"a^2bab^2 = ba"$

b) Não. Considere

$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in GL_3(\mathbb{Z}/3\mathbb{Z}) \right\} \quad (\text{é subgrupo de } GL_3(\mathbb{Z}/3\mathbb{Z}))$$

$M^3 = I$, $\forall M \in G$, mas G não é abeliano

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad) \neq_s$$

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

(Bhattacharya, pág 68 - ex 1.4b)

- 5) Seja G um grupo tal que $(ab)^2 = (ba)^2$, para todos $a, b \in G$ e suponha que $x = e$ é o único elemento de G tal que $x^2 = e$. Mostre que G é abeliano.
- i) O quadrado de cada elemento está no centro de G :

Temos $(ab^{-1}b)^2 = (bab^{-1})^2 = ba^2b^{-1}$ } $\Rightarrow a^2b = ba^2, \forall a, b \in G$.

ii) G é comutativo

Seja $c = ab\bar{a}'\bar{b}'$. Vamos mostrar que $c = e$, mostrando que $c^2 = e$.

Temos

$$\begin{aligned} c^2 &= ab(\bar{a}'\bar{b}'a)(\bar{b}\bar{a}'\bar{b}') = ab(a\bar{a}^2\bar{b}'a)(\bar{b}\bar{a}'\bar{b}') = ab(ab'\bar{a}^2a)(\bar{b}\bar{a}'\bar{b}') \\ &= ab(ab'\bar{a}')(b\bar{a}'\bar{b}') = ab(ab\bar{b}^2\bar{a}')(b\bar{a}'\bar{b}') = ab(ab\bar{a}'\bar{b}^2)(b\bar{a}'\bar{b}') \\ &= ab(ab\bar{a}')(b'\bar{a}'\bar{b}') = (ab)^2 (\bar{a}'\bar{b}')^2 = (ba)^2 (\bar{a}'\bar{b}')^2 = e. \end{aligned}$$

- 6) Sejam m, n inteiros positivos tais que $\text{mdc}(m, n) = 1$. Seja G um grupo em que todas as potências m -ésimas comutem entre si e todas as potências n -ésimas comutam entre si. Mostre que G é abeliano.

i) Vamos mostrar que potências m -ésimas comutam com potências n -ésimas:

Como $\text{mdc}(m, n) = 1$, $\exists r, s \in \mathbb{Z}$ tq $rm + sn = 1$.

$$\begin{aligned} a^m b^n &= (a^m b^n)^{rm+sn} = a^m (b^n a^m)^{rm+sn-1} b^n \\ &= \underbrace{a^m}_{= (b^n a^m)^r} (b^n a^m)^{rm} (b^n a^m)^{-1} \underbrace{(b^n a^m)^{sn}}_{= (b^n a^m)^s} b^n \\ &= (b^n a^m)^{rm} a^m \bar{a}^m b^{-n} b^n (b^n a^m)^{sn} = (b^n a^m)^{rm+sn} = b^n a^m \end{aligned}$$

ii) G é comutativo:

$$ab = a^{rm+sn} b^{rm+sn} = (\bar{a})^m (\bar{a}^s)^n (\bar{b}^r)^m (\bar{b}^s)^n = ba$$

Subgrupos

1) Seja G um grupo e seja S um subconjunto de G . Mostre que S é um subgrupo de G se e somente se $S \neq \emptyset$ e, para todos $a, b \in S$, se $a, b \in S$ entao $ab^{-1} \in S$.

$$\Leftrightarrow S \leq G$$

$$S \neq \emptyset \text{ pois } e \in S.$$

$$a, b \in S \Rightarrow b^{-1} \in S \Rightarrow ab^{-1} \in S$$

\Leftarrow $S \neq \emptyset$. Seja $a \in S$. Entao:

$$\text{i)} e = aa^{-1} \in S$$

$$\text{ii)} \text{ Se } a \in S \text{ entao } a^{-1} = ea^{-1} \in S$$

$$\text{iii)} \text{ Se } a, b \in S \text{ entao } ab = a(b^{-1})^{-1} \in S \quad \therefore S \leq G$$

2) Seja G um grupo e seja $\{H_i : i \in I\}$ uma familia de subgrupos de G .

Mostre que $\bigcap_{i \in I} H_i$ é um subgrupo de G .

$$\text{i)} e \in H_i, \forall i, \text{ pois } H_i \leq G. \text{ logo, } e \in \bigcap_{i \in I} H_i$$

$$\text{ii)} \text{ Sejam } a, b \in \bigcap_{i \in I} H_i, \text{ isto e, } a, b \in H_i, \forall i.$$

$$\text{Como } H_i \leq G, \text{ temos } ab^{-1} \in H_i, \forall i. \text{ logo, } ab^{-1} \in \bigcap_{i \in I} H_i$$

Pelo exercicio anterior, $\bigcap_{i \in I} H_i \leq G$

3) Seja G um grupo, sejam H e K subgrupos de G . Mostre que $H \cup K$ é um subgrupo de G se e somente se $H \subseteq K$ ou $K \subseteq H$.

\Leftarrow Se $H \subseteq K$ entao $H \cup K = K$ é subgrupo
idem se $K \subseteq H$

\Rightarrow Suponha que $H \not\subseteq K$ num $K \not\subseteq H$

Então existem $h \in H \setminus K$ e $k \in K \setminus H$.

Temos $hk, k \in H \cup K$ mas $hk \notin H \cup K$.

(Se $hk \in H$, por exemplo, tiramos)

$$hk = h' \Rightarrow k = h'^{-1}h \in H, \text{ contradição.}$$

4) Seja G um grupo e seja H um subconjunto ^{nao vazio} finito de G tal que $HH = H$.
 Prove que H é um subgrupo de G . E se H não for finito?

Syá $a \in H$. Temos $aH \subseteq H$, por hipótese.

A aplicação $\varphi: H \rightarrow aH \subseteq H$ é injetora
 $h \mapsto ah$

Como H é finito, $\varphi: H \rightarrow H$ é sobjetora
 $h \mapsto ah$.

Em particular, existe $h \in H$ tq $ah = a$, isto é, $e \in H$.

Portanto, existe $h_1 \in H$ tq $ah_1 = e$, isto é, $\bar{a} \in H$

Assim, H é subgrupo de G .

Se H é infinito, o resultado pode nas valer.

Por exemplo, $G = (\mathbb{Z}, +)$ e $H = \mathbb{Z}_+ = \{n \in \mathbb{Z}: n \geq 0\}$

Temos $HH = H$ (aqui, $HH = \mathbb{Z}_+ + \mathbb{Z}_+$) mas H não é subgrupo de G .

5) Syá G um grupo. Dados H um subgrupo de G e $a \in G$, mostre que $aHa^{-1} = \{ah\bar{a}: h \in H\}$ é um subgrupo de G .

Se H é finito, qual a ordem de aHa^{-1} ?

$$e = ae\bar{a} \in aHa^{-1}$$

Se $x, y \in aHa^{-1}$ entao $x = ah_1\bar{a}$, $y = ah_2\bar{a}$

$$xy^{-1} = ah_1\bar{a}(ah_2\bar{a})^{-1} = ah_1\bar{a}a\bar{h}_2\bar{\bar{a}} = \underbrace{ah_1h_2^{-1}\bar{a}}_{\in H} \in aHa^{-1}$$

$\therefore aHa^{-1}$ é subgrupo de G .

Tomemos $\varphi: H \rightarrow aHa^{-1}$ é bijetora
 $h \mapsto ah\bar{a}$

\therefore se H é finito, $|H| = |aHa^{-1}|$

5) a) Seja a um elemento de um grupo G . O normalizador de a em G é

$$N(a) = \{x \in G : xa = ax\}$$

Prove que $N(a)$ é um subgrupo de G .

b) determine o normalizador de S_3 = $\{e, \tau, \tau^2, \tau, \tau\tau, \tau^2\tau\}$

c) determine o normalizador de Q_8 = $\{1, -1, i, -i, j, -j, k, -k\}$.

a) i) $e \in N(a)$ pois $ea = a = ae$

ii) se $x, y \in N(a)$ entao $xya = xay = axy \Rightarrow xy \in N(a)$

iii) $x \in N(a) \Rightarrow xa = ax \Rightarrow x^{-1}(xa)x^{-1} = x^{-1}(ax)x^{-1} \Rightarrow ax^{-1} = x^{-1}a \Rightarrow x^{-1} \in N(a)$

$$\therefore N(a) \leq G$$

b) $N(\tau) = \{e, \tau, \tau^2\}$

c) $N(j) = \{1, -1, j, -j\}$.

7) Seja G um grupo e seja H um subgrupo de G . Considere

$$C_G(H) = \{x \in G : xh = hx, \forall h \in H\}.$$

Mostre que $C_G(H)$ é subgrupo de G

($C_G(H)$ é chamado de centralizador de H em G).

$$C_G(H) \bigcap_{h \in H} N(h)$$

Interseção de subgrupos é subgrupo

$$\therefore C_G(H) \leq G.$$

8) a) O centro de um grupo G é definido como sendo o conjunto

$$Z(G) = \{z \in G : zx = xz, \forall x \in G\}.$$

Prove que $Z(G)$ é subgrupo de G .

b) encontre $Z(S_3)$ e $Z(Q_8)$

a) $Z(G) = \bigcap_{g \in G} N(g) \therefore$ é subgrupo de G .

b) Como $N(\tau) = \{e, \tau, \tau^2\} \neq N(\tau) = \{e, \tau\}$, temos que $ze = N(\tau) \cap N(\tau) \supseteq Z(S_3)$
 $\therefore Z(S_3) = \{e\}$

$$N(j) = \{1, -1, j, -j\}, N(i) = \{1, -1, i, -i\} \Rightarrow \{1, -1\} \supseteq Z(Q_8)$$

é válido. $\therefore Z(Q_8) = \{1, -1\}$.

9) Seja G um grupo. Define-se a ordem de $a \in G$ como sendo o menor inteiro positivo n tal que $a^n = e$, se esse número existir (caso contrário, digamos que a ordem de a é infinita). Mostre que se $a \in G$ tem ordem finita, esse número coincide com a ordem do subgrupo de G gerado por a .

Seja $m = o(a)$. Então

$e, a, a^2, \dots, a^{m-1}$ são todos distintos

(se $0 \leq i < j \leq m-1$ são tq $a^i = a^j$ então $a^{j-i} = e$, contradiz, pois $0 < j-i < m$)

Além disso, para cada $m \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$, com $0 \leq r \leq m-1$ tq

$m = qn+r$. Então

$$a^m = a^{qn+r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r$$

$$\therefore \langle a \rangle = \{e, a, a^2, \dots, a^{m-1}\} \quad \text{e: } |\langle a \rangle| = |\{e, a, \dots, a^{m-1}\}| = m.$$

10) Seja G um grupo de ordem par. Mostre que G contém um elemento de ordem 2.

Se não existe elemento de ordem 2 em G então, $\forall g \in G, g \neq e$, temos $g \neq g^{-1}$. Portanto,

$G = \{e, g_1, g_1^{-1}, g_2, g_2^{-1}, \dots, g_k, g_k^{-1}\}$ terá $2k+1$ elementos.

11) Mostre que se G é um grupo de ordem par então existe um número ímpar de elementos de ordem 2.

Se $g \in G$ é tq $g^2 \neq e$ entas $g \neq g^{-1}$.

Como G tem ordem par, a quantidade de elementos $g \in G$ tq $g^2 \neq e$ é par.

Sobra uma quantidade par de elementos h tq $h^2 = e$.

E é um deles. Sobra uma quantidade ímpar de elementos de ordem 2.

12) Seja a um elemento de um grupo tq $a^n = e$. Mostre que $o(a)|n$.

Escreva $m = q \cdot o(a) + r$, com $0 \leq r < o(a)$.

Temos $e = a^m = a^{q \cdot o(a) + r} = (\underbrace{a^{o(a)}}_e)^q \cdot a^r = a^r \quad \therefore r=0$.

13) Seja G um grupo e sejam $a, b \in G$. Mostre que ab e ba têm a mesma ordem.

Se $\sigma(ab) = n$ então $(ba)^n = \bar{a}^1 a (ba)^{n-1} = \bar{a}^1 (ab)^{n-1} a = e$

$\sigma(ba) \mid n$.

Analogamente $\sigma(ab) \mid \sigma(ba)$.

14) Seja G um grupo e seja $a \in G$ um elemento de ordem n . Se $n = km$, mostre que a^k tem ordem m .

Temos $(a^k)^m = a^{km} = a^n = e$. Logo, $\sigma(a^k) \leq m$.

Se $0 < m' < m$ então $0 < km' < km = n$ e, portanto, $(a^k)^{m'} \neq e$.

Assim, $\sigma(a^k) \geq m$.

$\therefore \sigma(a^k) = m$.

15) Seja G um grupo e seja $a \in G$ um elemento de ordem n . Seja m um inteiro positivo tal que $\text{mdc}(m, n) = 1$. Mostre que $\sigma(a^m) = n$.

Se $k = \sigma(a^m)$, então $a^{mk} = (a^m)^k = e$. Logo, $m \mid mk$.

Como $\text{mdc}(m, n) = 1$, temos $m \mid k$.

Além disso, $(a^m)^n = (a^n)^m = e$. Logo, $k \mid n$. $\therefore k = n$.

16) Mostre que o número de geradores de um grupo cíclico de ordem n é $\varphi(n)$, em que φ é a função de Euler.

$$G = \langle a \rangle, |G| = n \Rightarrow \sigma(a) = n.$$

$$G = \{e, a, a^2, \dots, a^{n-1}\}$$

Se $n=1$ então $G = \{e\} = \langle e \rangle$ e nº de geradores é $1 = \varphi(1)$.

Se $n > 1$ então e não é gerador.

Dado m , $1 \leq m < n$, seja $d = \text{mdc}(m, n)$.

Se $d=1$, então, pelo exercício anterior, $\sigma(a^m) = m$. Logo, a^m é gerador de G .

Se $d > 1$ então $m = m'd$, $n = n'd$, a^d tem ordem n' , pelo exercício anterior ao anterior, portanto

$$(a^m)^{n'} = a^{m d n'} = (a^{dn'})^m = e \rightarrow \sigma(a^m) \leq n' < n \Rightarrow a^m \text{ não gera } G$$

\therefore O número de geradores de G é $\varphi(n)$.

17) Mostre que todo subgrupo de um grupo cíclico é cíclico.

Seja G um grupo cíclico. Então $G = \langle a \rangle$, para algum $a \in G$.

Seja $H \leq G$. Se $H = \{e\}$, H é cíclico. ($H = \langle e \rangle$)

Se $H \neq \{e\}$, considere $m = \min \{ |k| : a^k \in H, k \neq 0 \}$ (existe $k > 0$)
inteiros positivos

Temos $\langle a^m \rangle \subseteq H$.

Para a outra inclusão, seja $h \in H$. Como $H \leq G = \langle a \rangle$, $\exists n \in \mathbb{Z}$ tq $h = a^n$. Escreva $n = mq + r$, com $q, r \in \mathbb{Z}$ e $0 \leq r < m$.

$$H \ni h = a^n = a^{mq+r} = \underbrace{(a^m)^q}_{\in H} \cdot a^r \Rightarrow a^r \in H \Rightarrow r=0 \text{ (pois } m \text{ é minimal)}$$

∴ $h \in \langle a^m \rangle$.

Logo, $H = \langle a^m \rangle$ é cíclico.

18) a) Sejam G um grupo e sejam $a, b \in G$. Mostre que $r(a) = r(b^{-1}ab)$

b) Se G possui apenas um elemento a de ordem n , mostre que $a \in Z(G)$ e que $n=2$ ou $n=1$

a) $a^n = e \Leftrightarrow b^{-1}a^n b = b^{-1}e b = e$. logo, $r(a) = r(b^{-1}ab)$

$$(b^{-1}ab)^n$$

b) Como $r(a) = r(b^{-1}ab)$, $\forall b \in G$, temos

$$a = b^{-1}ab, \forall b \in G, \text{ isto é, } ba = ab, \forall b \in G.$$

Logo, $a \in Z(G)$.

Além disso, $r(a) = r(\tilde{a}')$. Assim, $a = \tilde{a}' \Rightarrow a^2 = e$.

$$\therefore r(a)/2 \Rightarrow r(a) = 1 \text{ ou } r(a) = 2.$$

Se G não é abeliano, $\sigma(a), \sigma(b) < \infty \Rightarrow \sigma(ab) < \infty$

Exemplos:

1) $S_{\mathbb{Z}} = \{f: \mathbb{Z} \rightarrow \mathbb{Z} \text{ bijetivas}\}$.

$$\sigma: x \mapsto -x$$

$$\tau: x \mapsto -x+1$$

$\sigma \circ \tau$ têm ordem 2.

$\tau \circ \sigma: x \mapsto x+1$ têm ordem infinita

2) $A = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad$ têm ordem 2.

$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad AB$ têm ordem infinita

3) Pegue 2 hiperplanos paralelos em \mathbb{R}^n

Reflexões em cada uma delas é uma isometria de ordem 2.

A composição delas é uma translação (tem ordem infinita)

(coloque 2 espelhos, um de frente p/ outro)

Classes laterais, Teorema de Lagrange

1) Seja G um grupo e sejam H e K subgrupos de G cujas ordens sejam relativamente primas. Mostre que $H \cap K = \{e\}$

$H \cap K \leq H$ e $H \cap K \leq K$. logo,

$$|H \cap K| \mid |H| \text{ e } |H \cap K| \mid |K|.$$

Como $\text{mdc}(|H|, |K|) = 1$, temos $|H \cap K| = 1$.

$$\therefore H \cap K = \{e\}.$$

2) Seja G um grupo e sejam $a, b \in G$ tais que $ab = ba$. Se a tem ordem m , b tem ordem n e $\text{mdc}(m, n) = 1$, mostre que a ordem de ab é mn .

$$\text{Seja } k = o(ab). \text{ Temos } (ab)^{mn} = a^{mn}b^{mn} = e \Rightarrow k \mid mn.$$

$$\text{Por outro lado, } e = (ab)^k = a^k b^k \Rightarrow a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle.$$

$$\text{Como } \text{mdc}(m, n) = 1, \text{ temos } \langle a \rangle \cap \langle b \rangle = \{e\}. \text{ logo, } a^k = b^{-k} = e \\ \Rightarrow m \mid k \text{ e } n \mid k \Rightarrow mn \mid k$$

$$\therefore o(ab) = mn.$$

3) Seja G um grupo abeliano que contém um elemento de ordem n e um de ordem m . Mostre que G contém um elemento de ordem $\text{mmc}(m, n)$.

Sejam $a, b \in G$, com $o(a) = n$ e $o(b) = m$.

$$\text{Escriva } n = \underbrace{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}_{m_1} \underbrace{q_1^{\beta_1} \cdots q_t^{\beta_t}}_{m_2}, \quad m = \underbrace{p_1^{\alpha'_1} \cdots p_k^{\alpha'_k}}_{m_1} \underbrace{q_1^{\beta_1} \cdots q_t^{\beta_t}}_{m_2}, \quad p_i, q_j \text{ primos } \neq s \\ \alpha_i \leq \alpha'_i \quad \beta_j \leq \beta'_j$$

$$\text{Então } \text{mmc}(m, n) = m_1 m_2$$

$$\text{Seja } c = a^{n_1} b^{m_2}$$

$$\text{Temos } c^{m_1 n_2} = a^{n_1 m_2} b^{m_2 n_2} = e \quad \therefore o(c) \mid m_1 m_2$$

$$\text{Além disso, se } c^k = e \text{ então } a^{kn_1} = b^{-km_2} \in \langle a^{n_1} \rangle \cap \langle b^{m_2} \rangle$$

$$\text{Como } \text{mdc}(m_2, n_1) = 1, \langle a^{n_1} \rangle \cap \langle b^{m_2} \rangle = \{e\} \quad \begin{matrix} \downarrow \text{tem ordem } n_1 \\ \text{tem ordem } m_2 \end{matrix} \quad \begin{matrix} \downarrow \text{tem ordem } m_1 \\ \text{tem ordem } n_2 \end{matrix}$$

$$\therefore a^{kn_1} = e = b^{-km_2} \Rightarrow n_1 \mid kn_1 \text{ e } m_2 \mid km_2 \Rightarrow n_2 \mid k + m_1 \mid k$$

$$\text{mdc}(m_2, n_1) = 1$$

$$\Downarrow \Rightarrow n_2 m_1 \mid k \Rightarrow n_2 m_1 \mid o(c)$$

$$\therefore o(c) = n_2 m_1 = \text{mmc}(m, n).$$

4) Seja G um grupo e sejam $H \leq G$ e $K \leq G$ dois subgrupos de índice finito em G .

Mostre que $H \cap K$ é um subgrupo de índice finito em G .

Seja $g \in G$. Então

$$g(H \cap K) = \{gh : h \in H\} \cap \{gk : k \in K\},$$

isto é, uma classe lateral de $H \cap K$ em G é a intersecção de uma classe lateral de H em G e uma de K em G .

Logo, existem, no máximo, $[G:H] \cdot [G:K]$ classes laterais de $H \cap K$ em G .

5) Seja G um grupo e sejam $H \leq G$ e $K \leq H$. Mostre que K tem índice finito em G se e somente se H tem índice finito em G e K tem índice finito em H .

Neste caso, mostre que $[G:K] = [G:H][H:K]$.

Basta provar que se $\{a_i H\}_{i \in I}$ são as classes laterais de H em G (distintas) e se $\{b_j K\}_{j \in J}$ são as classes laterais de K em H (distintas). Então:

i) $\{a_i b_j K\}$ são todas as classes laterais de K em G e

ii) $(a_i b_j) \neq (a_k b_e) \Rightarrow a_i b_j K \neq a_k b_e K$.

verificação:

i) Seja $x \in G$. Temos $xH = a_i H$, para algum $i \in I$. Então $a_i^{-1}x \in H$.
Seja $j \in J$ tq $a_i^{-1}xK = b_j K$. Então $xK = a_i b_j K$.

∴ Toda classe lateral de K em G é da forma $a_i b_j K$.

ii) Se $a_i b_j K = a_k b_e K$ então $b_j^{-1} a_i^{-1} a_k b_e \in K \subseteq H \stackrel{b_j, b_e \in H}{\Rightarrow} a_i^{-1} a_k \in H$
 $\Rightarrow a_i H = a_k H \Rightarrow a_i = a_k$.

Logo, $b_j K = b_e K$ e, portanto, $b_j = b_e$.

Subgrupos normais e quocientes

2) Neste exercício vamos construir um grupo não abeliano, contendo 8 elementos, cujos subgrupos são todos normais. Considere o seguinte subconjunto de $M_2(\mathbb{C})$

$$Q_8 = \{\text{id}, -\text{id}, I, -I, J, -J, K, -K\}, \text{ em que}$$

$$\text{id} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$

a) verifique as seguintes identidades abaixo:

$$I^2 = J^2 = K^2 = -\text{id}, \quad IJ = K = -JI, \quad IK = -J = KI, \quad JK = I = -KJ.$$

b) mostre que Q_8 com produto usual de matrizes é um grupo não abeliano de ordem 8.

c) encontre I^{-1}, J^{-1}, K^{-1}

d) calcule as ordens de todos os elementos de Q_8

e) liste todos os subgrupos de Q_8 (sao 6)

f) Mostre que todos os subgrupos de Q_8 são normais

g) Determine o centro $Z(Q_8)$ de Q_8 .

a) certas

b) mult. de matrizes é associativa

$$Q_8 Q_8 = Q_8 \quad \text{e } Q_8 \text{ é finito} \Rightarrow Q_8 \text{ é subgrupo}$$

$$IJ = -JI \neq JI \rightarrow \text{mais é abeliano}$$

$$c) I^{-1} = -I, J^{-1} = -J, K^{-1} = -K$$

d) $\pm I, \pm J, \pm K$ têm ordem 4, $-\text{id}$ tem ordem 2, id tem ordem 1

$$e) \langle I \rangle = \{\pm \text{id}, \pm I\}, \quad \langle J \rangle = \{\pm \text{id}, \pm J\}, \quad \langle K \rangle = \{\pm \text{id}, \pm K\}$$

$$\langle \text{id} \rangle = \{\text{id}\}, \quad \langle -\text{id} \rangle = \{\pm \text{id}\}, \quad Q_8$$

f) $\langle I \rangle, \langle J \rangle, \langle K \rangle$ têm índice 2 em Q_8 . logo, são normais em Q_8 .

$\langle \text{id} \rangle, Q_8$ são normais

$\langle -\text{id} \rangle$ é normal pois $\langle -\text{id} \rangle \subseteq Z(Q_8)$

↳ na verdade, é =

$$g) Z(Q_8) = \{\pm \text{id}\}$$

Subgrupos normais e quocientes

- 2) Seja H um subgrupo de índice 2 em um grupo G . Mostre que H é normal em G .
 $[G:H]=2 \Rightarrow$ as classes laterais (à direita ou à esquerda) de H em G são $H \in G \setminus H$.
- Se $x \in H$ então $xH = H = Hx$
Se $x \notin H$ então $xH = G \setminus H = Hx$
 $\therefore xH = Hx, \forall x \in G \quad \therefore H \triangleleft G$.

- 3) Sejam N_1, N_2 subgrupos normais de um grupo G . Mostre que $N_1 \cap N_2$ é um subgrupo normal de G . Mais geralmente, mostre que se $\{N_i : i \in I\}$ é uma família de subgrupos normais de G então $\bigcap_{i \in I} N_i$ é subgrupo normal de G .

Suja $\{N_i : i \in I\}$ uma família de subgrupos normais de G .
ja' vimos que $\bigcap_{i \in I} N_i$ é subgrupo de G .

Além disso, $\forall g \in G$, temos

$$gN_i g^{-1} \subseteq N_i, \text{ pois } N_i \triangleleft G.$$

$$\text{Portanto, } g\left(\bigcap_{i \in I} N_i\right)g^{-1} \subseteq \bigcap_{i \in I} N_i$$

$$\text{Logo, } \bigcap_{i \in I} N_i \triangleleft G.$$

4) Observe

- 5) Seja $GL_n(\mathbb{R})$ o grupo das matrizes de ordem n universíveis sobre \mathbb{R} (com multiplicações). Mostre que $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$ é um subgrupo normal de $GL_n(\mathbb{R})$

$$SL_n(\mathbb{R}) \leq GL_n(\mathbb{R}): \text{Id} \in SL_n(\mathbb{R})$$

$$A, B \in SL_n(\mathbb{R}) \Rightarrow \det(AB) = \det(A)\det(B) = 1 \Rightarrow AB \in SL_n(\mathbb{R})$$

$$A \in SL_n(\mathbb{R}) \Rightarrow \det(A^{-1}) = \det(A)^{-1} = 1 \Rightarrow A^{-1} \in SL_n(\mathbb{R})$$

$$SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R}):$$

se $B \in GL_n(\mathbb{R})$ e $A \in SL_n(\mathbb{R})$ entao

$$\det(BAB^{-1}) = \det(B)\det(A)\det(B)^{-1} = 1 \Rightarrow BAB^{-1} \in SL_n(\mathbb{R}).$$

6) Seja H um subgrupo de um grupo G tal que o produto de duas classes laterais à direita de H em G é sempre uma classe lateral à direita de H em G . Mostre que H é normal em G .

Sijam $x, y \in G$. Pela hipótese, existe $z \in G$ tq

$$HxHy = Hz$$

Como $xy \in HxHy$, temos $Hxy = Hz$, isto é, $HxHy = Hxy$. (*)

Para $x = g$ e $y = g^{-1}$, temos

$$gHg^{-1} = egHg^{-1} \subseteq HgHg^{-1} \stackrel{(*)}{=} Hgg^{-1} = H \quad \therefore H \triangleleft G.$$

7) Seja N um subgrupo normal de um grupo G e seja H um subgrupo de G . Mostre que NH é um subgrupo de G .

Temos que $NH \leq G \Leftrightarrow NH = HN$.

Como $N \triangleleft G$, temos $gN = Ng$, $\forall g \in G$.

Logo, $HN = NH$.

8) Sejam N e M subgrupos normais de um grupo G . Mostre que NM também é normal em G .

Sijam $n \in N$, $m \in M$ e $g \in G$. Então

$$gnm\bar{g}^1 = \underbrace{gn\bar{g}^1}_{\in N} \underbrace{g\bar{m}^1}_{\in M} \in NM \quad \therefore NM \triangleleft G.$$

9) Seja N um subgrupo normal de um grupo G tal que $[G:N] = m$.

Mostre que $a^m \in N$, para todo $a \in G$.

$N \triangleleft G \Rightarrow G/N$ é grupo.

$$|G/N| = [G:N] = m.$$

Logo, $\forall g \in G$, $(gN)^m = N$. Portanto, $g^m \in N$, $\forall g \in G$.

$$\overline{g^m N}$$

10) Seja G um grupo e seja H um subgrupo de G . O normalizador de H em G é definido por

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

Mostre que:

- $N_G(H)$ é um subgrupo de G
- H é um subgrupo normal de $N_G(H)$
- Se H é um subgrupo normal de um subgrupo K de G então $K \subseteq N_G(H)$
- H é normal em G se e somente se $N_G(H) = G$.

a) $eHe^{-1} = H \Rightarrow e \in N_G(H)$

$$x, y \in N_G(H) \Rightarrow xyH(xy)^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1} = H \Rightarrow xy \in N_G(H).$$

$$x \in N_G(H) \Rightarrow x^{-1}H(x^{-1})^{-1} = (xH^{-1}x^{-1})^{-1} = xHx^{-1} = H \Rightarrow x^{-1} \in H.$$

$$\therefore N_G(H) \leq G$$

b) $H \leq N_G(H)$ e se $h \in H$ e $g \in N_G(H)$ então

$$ghg^{-1} \in gHg^{-1} = H$$

$$\therefore H \triangleleft N_G(H)$$

c) Se $H \triangleleft K$ então $kHk^{-1} = H$, $\forall k \in K$

Logo, $k \in N_G(H)$, $\forall k \in K$.

d) Pela definição de $N_G(H)$.

- 11) Seja G um grupo. Para $a, b \in G$, definimos o comutador de a e b por
 $[a, b] = ab\bar{a}^{-1}\bar{b}^{-1}$.
- Denote por G' o subgrupo de G gerado pelo conjunto $\{[a, b] : a, b \in G\}$.
- mostre que G' é normal em G ;
 - mostre que G/G' é abeliano.
 - Syá N um subgrupo normal de G . Mostre que se G/N é abeliano então $G' \subseteq N$.
 - Mostre que se H é um subgrupo de G tq $G' \subseteq H$ então H é normal em G .

(O subgrupo G' de G definido acima chama-se subgrupo comutador (ou derivado) de G .)

a) Observe que inverso de comutador é um comutador:

$$[a, b]^{-1} = (ab\bar{a}^{-1}\bar{b}^{-1})^{-1} = bab^{-1}\bar{a}^{-1} = [b, a]$$

Se $c \in G'$ entao $c = [a_1, b_1][a_2, b_2] \dots [a_n, b_n]$.

$$\begin{aligned} \text{E, para } g \in G, \quad g[a, b]\bar{g}^{-1} &= gaba^{-1}\bar{b}^{-1}\bar{g}^{-1} = (ga\bar{g}^{-1})(gb\bar{g}^{-1})(g\bar{a}^{-1}\bar{g}^{-1})(g\bar{b}^{-1}\bar{g}^{-1}) \\ &= (ga\bar{g}^{-1})(gb\bar{g}^{-1})(ga\bar{g}^{-1})^{-1}(gb\bar{g}^{-1})^{-1} = [gag^{-1}, gbg^{-1}] \end{aligned}$$

$$\therefore g\bar{g}^{-1} = g[a_1, b_1] \dots [a_n, b_n]\bar{g}^{-1} = \underbrace{g[a_1, b_1]\bar{g}^{-1}}_{\in G'} \underbrace{g[a_2, b_2]\bar{g}^{-1}}_{\in G'} \dots \underbrace{g[a_n, b_n]\bar{g}^{-1}}_{\in G'} \in G'$$

$$\therefore G' \triangleleft G$$

$$\text{b) } ab\bar{a}^{-1}\bar{b}^{-1} \in G' \Rightarrow ab(ba)^{-1} \in G' \Rightarrow abG' = baG' \quad \therefore G/G' \text{ é abeliano}$$

$$(aG')(bG') \quad (bG')(aG')$$

$$\text{c) } G/N \text{ abeliano} \Rightarrow (aN)(bN) = (bN)(aN), \forall a, b \in G \Rightarrow ab(ba)^{-1} \in N, \forall a, b \in G$$

$$(ab)\bar{N} \quad (\bar{b}\bar{a})N$$

$$\Rightarrow [a, b] = ab\bar{a}^{-1}\bar{b}^{-1} \in N, \forall a, b \in G \Rightarrow G' \subseteq N$$

d) Sejam $g \in G$ e $h \in H$.

Temos $gh\bar{g}^{-1}\bar{h}^{-1} \in G' \subseteq H$

$$\therefore gh\bar{g}^{-1}\bar{h}^{-1} = h_1, \text{ para algum } h_1 \in H$$

$$\therefore gh\bar{g}^{-1} = h_1h \in H, \forall g \in G, \forall h \in H$$

$$\therefore H \triangleleft G.$$

12) Seja H um subgrupo de um grupo finito G e suponha que H seja o único subgrupo de G de ordem $|H|$. Mostre que H é normal em G .

Por um exercício anterior, vimos que $gH\bar{g}^{-1} \subseteq G$, $\forall g \in G$ e $|gH\bar{g}^{-1}| = |H|$. Como H é único subgrupo de G com ordem $|H|$, temos $gH\bar{g}^{-1} = H$. logo, $H \triangleleft G$.

13) Se N e M são subgrupos normais de um grupo G e $N \cap M = \{e\}$, mostre que $nm = mn$, $\forall n \in N$ e $m \in M$.

$$N \triangleleft G \Rightarrow mn\bar{m}^{-1} \in N$$

$$\therefore mn\bar{m}^{-1}\bar{n}^{-1} \in N$$

Como $M \triangleleft G$, também temos $mn\bar{m}^{-1}\bar{n}^{-1} \in M$.

$$\text{logo, } mn\bar{m}^{-1}\bar{n}^{-1} \in N \cap M = \{e\} \Rightarrow mn = nm.$$

14) Seja $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}, ac \neq 0 \right\}$ e seja $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$

Mostre que

a) N é um subgrupo normal de G

b) G/N é abeliano

Basta mostrar que $N = G'$

Temos

$$\left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right)^{-1} = \left(\begin{array}{cc} \bar{a} & -\bar{a}'\bar{b}\bar{c}' \\ 0 & \bar{c}' \end{array} \right) \in \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \left(\begin{array}{cc} a_1 & b_1 \\ 0 & c_1 \end{array} \right) = \left(\begin{array}{cc} aa_1 & ab_1 + bc_1 \\ 0 & cc_1 \end{array} \right)$$

Logo,

$$\left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \left(\begin{array}{cc} a_1 & b_1 \\ 0 & c_1 \end{array} \right) \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right)^{-1} \left(\begin{array}{cc} a_1 & b_1 \\ 0 & c_1 \end{array} \right)^{-1} = \left(\begin{array}{cc} 1 & * \\ 0 & 1 \end{array} \right) \in N$$

Além disso, $\forall b \in \mathbb{R}$,

$$\left(\begin{array}{cc} 1 & b \\ 0 & 1 \end{array} \right) = \left(\begin{array}{cc} 1 & b/2 \\ 0 & 1 \end{array} \right) \left(\begin{array}{cc} -1 & 0 \\ 0 & 1 \end{array} \right) \left(\begin{array}{cc} 1 & b/2 \\ 0 & 1 \end{array} \right)^{-1} \left(\begin{array}{cc} -1 & 0 \\ 0 & 1 \end{array} \right)^{-1} \in G'$$

$$\therefore N = G'$$

15) Seja G um grupo com centro $Z(G)$. Mostre que se $G/Z(G)$ é abeliano então G é abeliano.

Se $G/Z(G) = \langle g^r Z(G) \rangle$ então, para $x, y \in G$, temos:

$$xZ(G) = g^r Z(G)$$

$$yZ(G) = g^s Z(G), \text{ para algum } r, s \in \mathbb{Z}.$$

$$\therefore x \in g^r Z(G) \text{ e } y \in g^s Z(G)$$

Logo, $\exists z_1, z_2 \in Z(G)$ tq $x = g^r z_1$, $y = g^s z_2$.

$$xy = \underbrace{g^r z_1}_{\text{todos comutam.}} g^s z_2 = yx$$

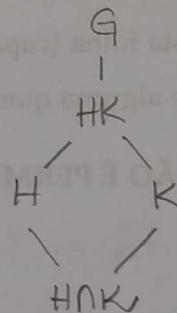
16) Seja G um grupo finito e H um subgrupo normal em G tal que $\text{mdc}(H, [G:H]) = 1$. Prove que H é o único subgrupo de G de ordem igual a $|H|$.

Suponha que $K \leq G$ com $|K| = |H|$

Como $H \trianglelefteq G$, temos que $HK \leq G$

Além disso,

$$[G:H] = [G:HK][HK:H] \quad (*)$$



Temos também,

$$[HK:H] = \frac{|HK|}{|H|} = \frac{|K|}{|H \cap K|} = \frac{|H|}{|H \cap K|}$$

Portanto, $[HK:H] \mid |H| \quad \left. \right\} \Rightarrow [HK:H] \mid \text{mdc}(|H|, [G:H]) = 1$

De (*), temos $[HK:H] \mid [G:H]$

$$\therefore [HK:H] = 1 \Rightarrow HK = H \Rightarrow H = K.$$

17) (*) Seja G um grupo de ordem n^2 com $n+1$ subgrupos de ordem n . Tais que a interseção de quaisquer dois desses subgrupos seja trivial. Mostre que G é abeliano. Isso só faz sentido p/ $n \geq 2$.

i) Se H e K são 2 desses subgrupos então $HK = G$

$$\text{pois } |HK| = \frac{|H||K|}{|H \cap K|}$$

ii) Cada um desses subgrupos é normal em G :

Observe que $\bigcup_{i=1}^{n+1} H_i = G$, em que $H_i \leq G$ e $|H_i| = n$, pois

$$|\bigcup_{i=1}^{n+1} H_i| = (n+1)(n-1) + 1 = n^2$$

\therefore Se $h \in H$, $g \in G$ e $g^{-1}hg \notin H$ então $g^{-1}hg = k \in K$, para algum outro $K \leq G$ com $|K| = n$.

Como $HK = G$, $\exists h_1 \in H$, $k_1 \in K$ tq $h_1k_1 = g$.

$$k_1^{-1}h_1^{-1}h_1k_1 = k \Rightarrow h_1^{-1}hh_1 = k_1k_1^{-1} \in H \cap K = \{e\}$$

$$\therefore h_1^{-1}hh_1 = e \Rightarrow h = e \text{ e } k = e \rightarrow \leftarrow$$

iii) G é abeliano

Se $h \in H$ e $k \in K$ então

$$\begin{aligned} hkh^{-1}k^{-1} &= (hkh^{-1})k^{-1} \in K \\ h(hkh^{-1}) &\in H \end{aligned} \Rightarrow hkh^{-1}k^{-1} \in H \cap K = \{e\} \Rightarrow kh = hk$$

Falta mostrar que cada H é abeliano

Se $h_1, h_2 \in H$, devemos mostrar que $h_1^{-1}h_2h_1 = h_2$

Sabemos que $h_1^{-1}h_2h_1 = h_3$.

Logo, para $k \in K$, $k \neq h$ (\exists pq $n \geq 2$) e $k \neq e$, temos

$$\underbrace{k^{-1}h_1^{-1}h_2h_1k}_{\in H} = k^{-1}h_3k = h_3$$

$$(h_1k)^{-1}h_2(h_1k) = h_2.$$

Exemplos: $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, 3 subgrupos: $\langle (1,0) \rangle, \langle (1,1) \rangle, \langle (0,1) \rangle$

$G = \mathbb{Z}_3 \times \mathbb{Z}_3$: 4 subgrupos: $\langle (1,0) \rangle, \langle (0,1) \rangle, \langle (1,1) \rangle, \langle (1,2) \rangle$.

Homomorfismos

- 10) Seja G um grupo abeliano finito de ordem n , onde n é um inteiro positivo.
Seja r um inteiro positivo tal que $\text{mdc}(n, r) = 1$. Mostre que todo elemento $g \in G$ pode ser escrito na forma $g = x^r$, para algum $x \in G$. (Sugestão: mostre que $g \mapsto g^r$ é um isomorfismo de G em G)

Não precisa do isomorfismo, nem que G seja abeliano.

$$\text{mdc}(n, r) = 1 \Rightarrow \exists s, t \in \mathbb{Z} \text{ tq } ns + rt = 1$$

$$\therefore g = g^{ns+rt} = (g^n)^s (g^t)^r = (g^t)^r$$

11) Seja G um grupo. Por automorfismo de G entende-se um isomorfismo de G em G .

Seja $\text{Aut}(G)$ o conjunto de todos os automorfismos de G .

a) Mostre que $\text{Aut}(G)$ é um grupo com operação binária dada pela composição de funções.

b) Seja $g \in G$ e defina $\varphi_g: G \rightarrow G$ por $\varphi_g(a) = gag^{-1}$, para todo $a \in G$. Mostre que $\varphi_g \in \text{Aut}(G)$, para todo $g \in G$. O automorfismo φ_g chama-se automorfismo interno definido por g .

c) Seja $\text{Inn}(G)$ o subconjunto de $\text{Aut}(G)$ formado por todos os automorfismos internos de G . Mostre que $\text{Inn}(G)$ é um subgrupo normal de $\text{Aut}(G)$.

d) Mostre que $\text{Inn}(G) \cong G/\text{Z}(G)$.

(Sugestão: Considere o homo $\Psi: G \rightarrow \text{Aut}(G)$ dado por $\Psi(g) = \varphi_g$)

e) Determine o grupo de automorfismos de um grupo cíclico de ordem finita.

f) Determine o grupo de automorfismos do grupo cíclico de ordem infinita.

g) Determine o grupo de automorfismos de S_3 .

c) $\Psi \in \text{Aut}(G)$, $\varphi_g \in \text{Inn}(G)$

$$(\Psi \varphi_g \Psi^{-1})(a) = \Psi(g)\Psi^{-1}(a)\bar{g} = \Psi(g)\Psi^{-1}(a)\Psi(g)^{-1} = \varphi_{\Psi(g)}(a) \quad \therefore \Psi \varphi_g \Psi^{-1} = \varphi_{\Psi(g)} \in \text{Inn}(G)$$

d) Seja $\Psi: G \rightarrow \text{Aut}(G)$

$$g \mapsto \Psi(g) = \varphi_g$$

$$\Psi \text{ é homo: } \Psi(g_1 g_2)(x) = g_1 g_2 x g_2^{-1} g_1^{-1} = \varphi_{g_1} \varphi_{g_2}(x) = \varphi(g_1) \varphi(g_2)(x), \forall x \in G.$$

$$\text{Im } \Psi = \text{Inn}(G)$$

$$g \in \text{ker } \Psi \Leftrightarrow \Psi(g)(x) = x, \forall x \in G \Leftrightarrow gx\bar{g} = x, \forall x \in G \Leftrightarrow gx = xg, \forall x \in G \Leftrightarrow g \in \text{Z}(G)$$

Pelo Teo do Homo, $G/\text{Z}(G) \cong \text{Inn}(G)$.

e) G cíclico de ordem n

$$G = \langle a \rangle, |G| = n.$$

$\Psi: G \rightarrow G$ está determinado pela imagem de a .

$$\Psi(a) = a^r, \text{ para algum } r \in \{0, 1, \dots, n-1\}$$

Ψ é isomorfismo $\Leftrightarrow \text{mdc}(r, n) = 1$

$$\text{Aut}(G) \cong \text{U}(\mathbb{Z}_n, +, \cdot) \quad (\Psi_r \Psi_s = \Psi_{rs})$$

f) $G = \langle a \rangle$, a de ordem infinita

$$\Psi(a) = a^r \text{ é automorfismo} \Leftrightarrow r = \pm 1 \quad (\text{c.c. mas é sobre}).$$

$$\therefore \text{Aut}(G) \cong C_2$$

$$g) \text{Z}(S_3) = \{\text{id}\} \Rightarrow S_3 \cong \text{Inn}(S_3) \subseteq \text{Aut}(S_3)$$

Em $\text{Aut} S_3$ existem no máx 6 elementos (pois $\Psi((1\ 2\ 3)) = \Psi((1\ 2))$ definem Ψ e existem 2 elementos de ordem 3 e 3 de ordem 2 em S_3)

$$\therefore 6 = |\text{Inn } S_3| \leq |\text{Aut}(G)| \leq 6 \Rightarrow \text{Aut}(G) = 6 \text{ e } \therefore \text{Aut}(G) = \text{Inn}(G) \cong S_3$$

Grupos de permutações

4) Seja H um subgrupo de S_n . Mostre que $H \subseteq A_n$ ou $[H : H \cap A_n] = 2$.

$\varphi: S_n \rightarrow \{1, -1\}$ é homomorfismo de grupos, com $\text{ker } \varphi = A_n$

$$\sigma \mapsto \text{sgn}(\sigma)$$

$$\varphi(H) \subseteq \{1, -1\}$$

• Se $\varphi(H) = \{1\}$ então $H \subseteq A_n$

• Se $\varphi(H) = \{1, -1\}$ então $\varphi|_H: H \rightarrow \{1, -1\}$ é homo sobrejetor

Pelo T. Homomorfismo,

$$H/\text{ker } \varphi|_H \cong \{1, -1\};$$

Como $\text{ker } \varphi|_H = H \cap A_n$, temos

$$H/H \cap A_n \cong \{1, -1\}. \quad \text{Em particular, } [H : H \cap A_n] = 2.$$

5) a) Qual é a ordem de um n -ciclo?

b) Qual é a ordem de um produto de r ciclos disjuntos de ordens n_1, n_2, \dots, n_r ?

c) Para quais inteiros positivos m um m -ciclo é uma permutação par?

a) Seja $\sigma = (i_1 i_2 \dots i_r)$ um r -ciclo. Então i_1, \dots, i_r são \neq_s ,

$$\sigma(i_j) = i_{j+1} \text{ se } 1 \leq j < r \text{ e } \sigma(i_r) = i_1 \quad \therefore \sigma(i_j) = i_{j+r \pmod r}$$

$$\therefore \forall s > 0, \text{ temos } \sigma^s(i_j) = i_{j+s \pmod r}$$

Se $0 < s < r$, temos $\sigma^s(i_1) = i_{1+s} \neq i_1$, pois $1 < 1+s \leq r$. $\therefore \sigma^s \neq \text{id}$.

Além disso, $\sigma^r(i_j) = i_{j+r \pmod r} = i_j, \forall j \in \{1, \dots, r\}$ } $\Rightarrow \sigma^r = \text{id}$.

$$\sigma^r(j) = j \text{ se } j \in \{1, 2, \dots, n\} \setminus \{i_1, \dots, i_r\}$$

$$\therefore \text{ord}(\sigma) = r$$

b) A ordem é $\text{mmc}(n_1, n_2, \dots, n_r)$ pois:

$\forall a, b \in G$, $ab = ba$ e $\langle a \rangle \cap \langle b \rangle = \{e\}$ então $\text{ord}(ab) = \text{mmc}(\text{ord}(a), \text{ord}(b))$

(observe que se $\sigma, \tau \in S_n$ são permutações disjuntas então $\langle \sigma \rangle \cap \langle \tau \rangle = \{e\}$).

c) m -ciclo é par $\Leftrightarrow m$ é ímpar.

6) Seja p um número primo. Mostre que todo elemento de ordem p em S_p é um p -ciclo. Mostre que S_p não possui elementos de ordem k_p , para $k \geq 2$.

Seja $\sigma \in S_p$ um elemento de ordem p .

Temos $\sigma \neq \text{id}$.

Escriva $\sigma = \alpha_1 \dots \alpha_t$ produto de ciclos disjuntos de compr. ≥ 2 .

Se α_i é r_i -ciclo então $r_1 + \dots + r_t \leq p$ e $r_i > 0, \forall i$.

• Se $t > 1$ então $r_i < p$, $\forall i = 1, \dots, t$ e $\sigma(\sigma) = \text{mmc}(r_1, \dots, r_t)$ não é múltiplo de p (pois $p \nmid r_i, \forall i = 1, \dots, t$).

∴ se $\sigma(\sigma) = p$ então σ é um ciclo. E deve ser um p -ciclo (pois a ordem de um r -ciclo é r)

7) Se $\sigma \in S_p$ tem ordem k_p então $p \mid \sigma(\sigma)$. Já vimos que, para isso, σ deve ser um p -ciclo. logo, $\sigma(\sigma) = p$. ∴ $k_p = 1$.

8) Sejam t, n inteiros positivos e p um primo. Mostre que o grupo S_n possui elementos de ordem p^t se, e somente se, $n \geq p^t$.

$$(\Leftarrow) n \geq p^t$$

$\sigma = (1 \ 2 \ \dots \ p^t)$ é um p^t -ciclo. ∴ $\sigma(\sigma) = p^t$.

$$(\Rightarrow) \sigma(\sigma) = p^t \quad (\because \sigma \neq \text{id})$$

Se $\sigma = \alpha_1 \dots \alpha_s$, α_i produto de ciclos disjuntos, deve existir i tq α_i é p^t -ciclo (c.c. $p^t + \text{mmc}(r_1, \dots, r_s)$, em que r_i é ordem de α_i).

$$\therefore n \geq p^t \quad (\text{pois } r_1 + \dots + r_s \leq n)$$

algum delas é p^t

9) Mostre que as possíveis ordens dos elementos do grupo S_7 são 1, 2, 3, 4, 5, 6, 7, 10 e 12.

A decompr. de $\sigma \in S_7$ em produto de ciclos disjuntos tem as possíveis compr. de ciclos:

$$7, 6+1, 5+2, 5+1+1, 4+3, 4+2+1, 4+1+1+1, 3+3+1, 3+2+1+1, \\ 3+1+1+1+1, 2+2+2+1, 2+2+1+1+1, 2+1+1+1+1+1$$

Logo, as possíveis ordens para $\sigma \in S_7$ são:

$$7, 6, 10, 5, 12, 4, 3, 6, 2, 1$$

D) a) Mostre que S_n é gerado por $(1\ 2), (1\ 3), \dots, (1\ n-1), (1\ n)$

b) Mostre que S_n é gerado por $(1\ 2)$ e $(1\ 2\dots n)$

c) Mostre que A_n é gerado pelos 3-ciclos de S_n , se $n \geq 3$.

a) $(i\ j) = (1\ j)(1\ i)(1\ j)$

Como S_n é gerado por transposições, segue o resultado

b) Seja $\alpha = (1\ 2\dots n)$

$$\alpha(1\ 2)\alpha^{-1} = (2\ 3)$$

$$\alpha(2\ 3)\alpha^{-1} = (3\ 4)$$

:

Basta mostrar que $(j\ j+1)$, $j=1, \dots, n-1$, geram $(1\ i)$, $i=2, \dots, n$.

$$(1\ i) = (i-1\ i)(i-2\ i-1)\dots(2\ 3)(1\ 2)(2\ 3)\dots(i-1\ i)$$

c) (Feito em aula)

Todos 3-ciclos são pares. Logo, os 3-ciclos estão em A_n .

Seja $\sigma \in A_n$. Então $\sigma = \tau_1 \tau_2 \dots \tau_{2k-1} \tau_{2k}$, em que τ_i são transposições.

Basta mostrar que produto de 2 transposições é produto de 3-ciclos.

• $\tau_1 = (a\ b)$, $\tau_2 = (c\ d)$, a, b, c, d distintos

$$\tau_1 \tau_2 = (a\ b)(c\ d) = (a\ b\ c)(b\ c\ d)$$

• $\tau_1 = (a\ b)$, $\tau_2 = (b, c)$, a, c distintos

$$\tau_1 \tau_2 = (a\ b)(b\ c) = (a\ b\ c)$$

• $\tau_1 = \tau_2$ OK

- 10) a) Seja $\sigma \in S_n$ o r-ciclo $(i_1 i_2 \dots i_r)$ e seja $\alpha \in S_n$. Mostre que
 $\alpha \sigma \alpha^{-1} = (\alpha(i_1) \alpha(i_2) \dots \alpha(i_r))$.
- b) Se τ, τ são dois r-ciclos, mostre que existe $\alpha \in S_n$ tq $\alpha \sigma \alpha^{-1} = \tau$.
- c) Prove que duas permutações são conjugadas se e somente se elas têm a mesma estrutura cíclica.

a) Vamos mostrar que

$$\underbrace{\alpha \sigma}_{\beta} = \underbrace{(\alpha(i_1) \alpha(i_2) \dots \alpha(i_r)) \alpha}_{\tau}$$

Para $i_j \in \{i_1, \dots, i_r\}$, temos

$$\beta(i_j) = \alpha \sigma(i_j) = \alpha(i_{j+1 \text{ mod } r})$$

$$\tau(i_j) = (\alpha(i_1) \alpha(i_2) \dots \alpha(i_r))(\alpha(i_j)) = \alpha(i_{j+1 \text{ mod } r})$$

Se $k \notin \{i_1, \dots, i_r\}$ entao

$$\beta(k) = \alpha \sigma(k) = \alpha(k) \quad k \neq i_j$$

$$\tau(k) = (\alpha(i_1) \dots \alpha(i_r)) \alpha(k) = \alpha(k)$$

$$\therefore \beta = \tau, \text{ ie}, \alpha \sigma \alpha^{-1} = (\alpha(i_1) \dots \alpha(i_r))$$

b) $\sigma = (i_1, \dots, i_r)$, $\tau = (k_1, \dots, k_r)$ dois r-ciclos em S_n

Então i_1, \dots, i_r são todos distintos, assim como k_1, \dots, k_r
 $\in \{1, \dots, n\}$

Logo, $\exists \alpha \in S_n$ tq $\alpha(i_j) = k_j$.

Pela parte a) $\alpha \sigma \alpha^{-1} = \tau$.

c) $\Leftrightarrow \sigma, \tau \in S_n$ permutações conjugadas : $\exists \alpha \in S_n$ tq $\tau = \alpha \sigma \alpha^{-1}$

$\sigma = \sigma_1 \dots \sigma_t$ produto de ciclos disjuntos, σ_i um r_i -ciclo.

$\tau = \alpha \sigma \alpha^{-1} = \underbrace{\alpha \sigma_1 \alpha^{-1}}_{\text{e } r_1\text{-ciclo}} \underbrace{\alpha \sigma_2 \alpha^{-1}}_{\text{e } r_2\text{-ciclo}} \dots \underbrace{\alpha \sigma_t \alpha^{-1}}_{\text{e } r_t\text{-ciclo}}$ são disjuntos, pois α é biêto

$\therefore \tau$ e σ têm a mesma decomposição cíclica.

\Leftarrow $\sigma, \tau \in S_n$, $\sigma = \underline{\sigma_1 \dots \sigma_t}$, $\tau = \underline{\tau_1 \dots \tau_t}$, σ_i, τ_i r_i -ciclos.
 disjuntos disjuntos

Como $\sigma_1, \dots, \sigma_t$ são disjuntos e τ_1, \dots, τ_t também, escrevendo

$$\sigma_i = (j_1^i, \dots, j_{r_i}^i), \quad \tau_i = (k_1^i, \dots, k_{r_i}^i), \quad \exists \alpha \in S_n \text{ tq } \alpha(j_s^i) = k_s^i$$

Dai $\alpha \sigma \alpha^{-1} = \tau$.

1) Mostre que A_4 não contém subgrupos de ordem 6 (e, portanto, não vale a reciprocidade do Teorema de Lagrange). (fiz na aula).

OBS: Se G é um grupo e $H \leq G$ é um subgrupo de índice 2 então $x^2 \in H, \forall x \in H$.

(pois $H \triangleleft G$ e G/H é um grupo de ordem 2. logo, $\forall x \in G, (xH)^2 = H$, i.e., $x^2 \in H$).

Se $\exists H \leq A_4$ com $|H| = 6$ então $[A_4 : H] = 2$.

Então $x^2 \in H, \forall x \in A_4$.

Observe que $\{x^2 : x \in A_4\} = \{id, \text{ todos os } 3\text{-ciclos}\}$ tem 9 elementos
∴ não existe subgrupo de ordem 6 em A_4 .

Mais dem desse fato:

M. Brennan, D. Mactale:

Variations on a theme: A_4 definitely has no subgroups of order six!

Math. Magazine 73(1), 2000, 34-40.

- 2) Uma matriz de permutação é uma matriz obtida a partir da matriz identidade $n \times n$ permutando-se suas colunas. Denote por P_n o conjunto de todas as matrizes de permutação $n \times n$.
- Mostre que P_n forma um grupo com a multiplicação usual de matrizes
 - Mostre que a função $\Theta: S_n \rightarrow P_n$, em que $\Theta(\sigma)$ denota a matriz cuja i -ésima coluna coincide com a $\sigma(i)$ -ésima coluna da matriz identidade, é um isomorfismo
 - Prove que $\text{sgn}(\sigma) = \det(\Theta(\sigma))$.

Seja V um espaço vetorial sobre algum corpo com base fixada $B = \{e_1, \dots, e_n\}$.

$S_n \cong S_B$, já que B tem n elementos

Cada elemento $\sigma \in S_n \cong S_B$ determina um operador linear T_σ de V inversível.
 $T_\sigma(e_i) = e_{\sigma(i)}$, $i=1, \dots, n$.

Observe que $[T_\sigma]_B = \Theta(\sigma)$ definida no item B e, para $\tau, \tau \in S_n$,

$$T_{\sigma\tau} = T_\sigma T_\tau \text{. Logo, } [T_{\sigma\tau}]_B = \Theta(\sigma)\Theta(\tau). \quad (1)$$

$$\text{Além disso, } \{[T_\sigma]_B : \sigma \in S_n\} = P_n. \quad (2)$$

Por (1) e (2), P_n é grupo (subgrupo dos operadores inversíveis de V com composição) e Θ é homomorfismo

- $\sigma = \tau \Rightarrow T_\sigma = T_\tau$, pois todo operador fica definido por seus valores numa base
 $\therefore \Theta$ é injetor
- dada $A \in P_n$, seja σ a permutação das colunas que produz A .
Então $[T_\sigma]_B = A$. $\therefore \Theta$ é sobreyetor.

$\Theta''(\sigma)$

Para mostrar c) vamos usar o fato de que S_n é gerado pelas

transposições $(i \ i+1)$ (Além do fato que Θ é homo e $\det(AB) = \det A \det B$)

Basta mostrar, então, que se $\sigma = (i \ i+1)$ então $\det(\Theta(\sigma)) = -1$.

$$\Theta(\sigma) = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \downarrow & \\ i & & & & 1 \\ & \nearrow & & & \\ & & 0 & 1 & \\ & & & 1 & 0 \\ & & & & \ddots \\ & & & & 1 \end{bmatrix}$$

Desenvolvendo pela i -ésima coluna,

$$\det \Theta(\sigma) = (-1)^{i+i+1} \text{Id}_{(n-1) \times (n-1)} = (-1)^{2i+1} = -1$$

13) Mostre que D_n é isomórfico ao subgrupo de S_n gerado pelas permutações

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix} \in \begin{pmatrix} 1 & 2 & 3 & & n-1 & n \\ 1 & n & n-1 & & 3 & 2 \end{pmatrix}$$

Síam $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix} \in \tau = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}$

$$\sigma = (1 \ 2 \ \dots \ n) \quad n\text{-áclo}$$

$$\tau = (2 \ n)(3 \ n-1) \dots \quad (\text{produto de transpoções})$$

$$\therefore \sigma^n = \text{id}, \quad \tau^2 = \text{id}.$$

Além disso, $\tau \sigma \tau^{-1} = \tau \sigma \tau = (\tau(1) \ \tau(2) \ \dots \ \tau(n)) = (1 \ n \ n-1 \ \dots \ 3 \ 2)$
 $= (n \ n-1 \ \dots \ 3 \ 2 \ 1) = \sigma^{-1}$
ex 2b)

$$\therefore \langle \sigma, \tau \rangle \cong D_n.$$

15) Encontre um grupo G que contenha subgrupos H e K tq K seja normal em H , H seja normal em G mas K não seja normal em G .

$$G = A_4$$

$$H = \{\text{id}, (1 \ 2)(3 \ 4), (1 \ 4)(3 \ 2), (1 \ 3)(2 \ 4)\}$$

$$K = \{\text{id}, (1 \ 2)(3 \ 4)\}$$

Também temos $G = D_4 = \{\text{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$,

$$\sigma^4 = \text{id}, \quad \tau\sigma = \sigma^3\tau$$

$$H = \{\text{id}, \sigma^2, \tau, \sigma^2\tau\}$$

$$K = \{\text{id}, \tau\}$$

14) Determine todos os subgrupos normais de S_4 .

(yves, pag 210)

• Os únicos subgrupos normais de A_4 são

{id}, $V = \{id, (12)(34), (13)(24), (14)(23)\} \subseteq A_4$

Os três subgrupos acima são normais em A_4 (e são em S_4 também).

Seja $H \trianglelefteq A_4$, $H \neq \{id\}$.

$$A_4 = \{id, (12)(34), (13)(24), (14)(23), (123), (134), (124), (234), (132), (143), (142), (243)\}$$

• Se H contém um 3-ciclo, contém todas:

$$(123) \in H \Rightarrow (132) = (123)^{-1} \in H$$

$$(134)(123)(134)^{-1} = (234) \Rightarrow (234), (243) \in H$$

$$(234)(123)(234)^{-1} = (134) \Rightarrow (134), (143) \in H$$

$$(324)(132)(324)^{-1} = (124) \Rightarrow (124), (142) \in H.$$

$$\therefore A_4 \subseteq H \Rightarrow H = A_4.$$

• Se H não contém 3-ciclos, contém um produto de 2 2-ciclos. Daí $H = V$:

$$(12)(34) \in H \Rightarrow (234)(12)(34)(234)^{-1} = (13)(42) \in H$$

$$(14)(23) = (13)(24)(12)(34) \in H$$

$$\therefore H = V.$$

Seja agora $H \trianglelefteq S_4$.

Se $H \subseteq A_4$ entao $H \trianglelefteq A_4$. Portanto, $H = \{id\}$, V ou A_4 .

Se $H \not\subseteq A_4$ entao H contém uma permutação ímpar.

Permutações ímpares de S_4 : transposições (6)
4-ciclos (6)

Se H contém uma transposição, contém todas. $\therefore H = S_4$.

Se H contém um 4-ciclo, contém todos os 4-ciclos.

\therefore contém os quadrados dos 4-ciclos (elementos de V).

$\therefore H$ tem pelo menos 10 elementos

Temos ainda que $[H : H \cap A_4] = 2$ (exercício 4)

$$\therefore |H \cap A_4| \geq 5. \Rightarrow H \cap A_4 = A_4.$$

$\hookrightarrow A_4$ não possui subgr de ordem 6

$$\therefore |H| > 12 \Rightarrow H = S_4$$

16) Seja $n=3$ ou $n \geq 5$. Mostre que $\{e\}$, A_n e S_n são os únicos subgrupos normais de S_n . (Em particular, A_n é o único subgrupo de S_n de índice 2). (Yves, pág 210).

$\{e\}$, A_n e S_n são normais em S_n .

$n=3$: ok.

$\forall n \geq 5$: Sabemos que A_n é simples.

\therefore Se $H \triangleleft G$ e $H \subseteq A_n$ entao $H = \{e\}$ ou $H = A_n$.

Sugonha que $H \not\subseteq A_n$. Vamos mostrar que $H = S_n$.

Sabemos que $[H : H \cap A_n] = 2$.

Além disso $H \cap A_n \triangleleft A_n \therefore H \cap A_n = A_n$ (neste caso, $H = S_n$)

ou $H \cap A_n = \{e\}$. Daí H tem 2 elementos.

$H = \{e, \tau\}$, em que τ é produto de uma quantidade ímpar³ de transposições disjuntas.

(Se τ é uma única transposição então todas as transposições estão em H)

Seja $\tau = (i \ j)(k \ l) \dots$

Se $\tau = (i \ k)$ entao

$H \ni \tau \tau^{-1} = (k \ j)(i \ l) \dots \neq \tau$, contradicção

$\therefore A_n \cap H = \{e\}$ não ocorre.

Os únicos subgrupos normais de S_n são $\{e\}$, A_n , S_n , se $n \geq 5$.

A_n é o único subgrupo de índice 2 em S_n .

I) (math.stackexchange.com)

Se $[S_n : H] = 2$ então $H \triangleleft S_n$ e $S_n/H \cong C_2 = \{1, -1\}$

Então existe $f: S_n \rightarrow \{1, -1\}$ homomorfismo sobjetor com ker $f = H$.

Todas as transposições em S_n são conjugadas. Portanto $f(\tau) \in C_2$ é o mesmo elemento, para qualquer transposição $\tau \in S_n$ (visto que C_2 é comutativo $f(\sigma\tau\sigma^{-1}) = f(\sigma)f(\tau)f(\sigma)^{-1} = f(\tau)$)

S_n é gerado por transposições. logo, C_2 é gerado por $f(\tau)$, para $\tau \in S_n$ transp.

$$\therefore f(\tau) = -1 \quad \therefore \text{ker } f \cong A_n.$$

II) com sugestão do Livro de Hungerford.

i) Se $r, s \in \{1, 2, \dots, n\}$ são distintos então $A_n (n \geq 3)$ é gerado pelos 3-ciclos $\{(r s k) : 1 \leq k \leq n, k \neq r, s\}$.

ii) Se $[G : H] = 2$ então H contém os quadrados de todos os elementos de G

iii) Se $[G : H] = 2$ então H contém todos os elementos de ordem ímpar de G .

ii) Seja $g \in G$. Por Lagrange, $(gh)^2 = h$. logo, $g^2 \in H$.

iii) Se $\text{ord}(g) = 2k+1$, para $k \in \mathbb{N}$, então

$$H = g^{2k+1}H = gH \underbrace{(g^2)^k H}_{\text{"H por (ii)"}} = gh \quad \therefore g \in H.$$

III) (Alfa Ex 6.20)

i) Se $[G : H] = 2$ e $x, y \notin H$ então $xy \in H$
pois $x, y \notin H \Rightarrow xH = y^{-1}H$, já que existem apenas 2 classes
 $\therefore xy \in H$.

ii) $[G : H] = 2 \Rightarrow H \triangleleft G$. Se H contém uma transposição, contém todas. Daí $H = S_n$
 $\therefore H$ não contém transposições. \therefore por i) $\forall \tau, \sigma \in S_n$ transposições, $\sigma\tau \in H$
 $\therefore A_n \subseteq H$. Daí $A_n = H$

↳ A_n é o conjunto formado por elementos que se decomponem como produtos de no par de transposições.

J.B. Nganou: How rare are subgroups of index 2?, Math Magazine, 85(3), 2012, 215-220

Machala, D.: Minimum Counterexamples in Group Theory, Math. Magazine, 54(1), 1981, 23-28

Produto direto

18) Sejam G_1, \dots, G_n grupos e seja $a = (a_1, \dots, a_n)$ um elemento do produto direto $G = G_1 \times \dots \times G_n$. Suponha que, para cada $i=1, \dots, n$, o elemento a_i tenha ordem finita r_i no grupo G_i . Mostre que a ordem de a em G é igual a $\text{mmc}(r_1, \dots, r_n)$.

Sep $r = \text{mmc}(r_1, \dots, r_n)$. Então

$$a^r = (a_1^r, \dots, a_n^r) = (e_{G_1}, \dots, e_{G_n}) = e_G, \text{ pois } r_i | r, \forall i=1, \dots, n$$

Por outro lado, se $k \geq 1$ é tq $a^k = e_G$, então

$$(e_{G_1}, \dots, e_{G_n}) = e_G = a^k = (a_1^k, \dots, a_n^k) \Rightarrow r_i | k, \forall i=1, \dots, n$$

$$\Rightarrow \underbrace{\text{mmc}(r_1, \dots, r_n)}_r | k \quad \therefore \sigma(a) = r = \text{mmc}(r_1, \dots, r_n).$$

19) a) Seja G um grupo e sejam H e K subgrupos normais de G tq $HK = G$ e $H \cap K = \{e_G\}$. Mostre que $G \cong HK$.

b) Sejam G_1, G_2 dois grupos e seja $G = G_1 \times G_2$ o produto direto deles. Considere os seguintes subconjuntos de G :

$$H = \{(a_1, e_2) : a_1 \in G_1\}, K = \{(e_1, a_2) : a_2 \in G_2\},$$

onde e_i denota o elemento identidade de G_i . Mostre que H e K são subgrupos normais de G tq $HK = G$ e $H \cap K = \{e_G\}$.

a) $\varphi: H \times K \rightarrow G$ é isomorfismo (vamos que se $H, K \trianglelefteq G$ e $H \cap K = \{e_G\}$ entao $hk = kh, \forall h \in H, \forall k \in K$)

$$\varphi((h_1, k_1)(h_2, k_2)) = \varphi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2 = h_1 k_1 h_2 k_2 = \varphi(h_1, k_1) \varphi(h_2, k_2)$$

$$(h, k) \in \ker \varphi \Rightarrow hk = e \Rightarrow h = k^{-1} \in H \cap K = \{e_G\} \Rightarrow (h, k) = (e_1, e_2) \therefore \varphi \text{ é injetiva}$$

$$\text{Im } \varphi = HK = G \quad \therefore \text{ é sobre.}$$

b) Seja $\pi_1: G \rightarrow G_1$

$$(a_1, a_2) \mapsto a_1$$

π_1 é homo sobrejetor e $\ker \pi_1 = H$ $\therefore H \trianglelefteq G$.

Analogamente, $K \trianglelefteq G$.

$$H \cap K = \{(e_1, e_2)\} = \{e_G\}$$

$$(a_1, a_2) = (a_1, e_2) (e_1, a_2) \in HK \quad \therefore G = HK$$

11

9

20) Sejam G_1, G_2 grupos, seja N_1 um subgrupo normal de G_1 e seja N_2 um subgrupo normal de G_2 . Mostre que $N_1 \times N_2$ é um subgrupo normal de $G_1 \times G_2$ e que $\frac{G_1 \times G_2}{N_1 \times N_2} \cong \frac{G_1}{N_1} \times \frac{G_2}{N_2}$

Seja $\varphi: G_1 \times G_2 \longrightarrow \frac{G_1}{N_1} \times \frac{G_2}{N_2}$
 $(g_1, g_2) \mapsto (g_1 N_1, g_2 N_2)$

φ é homomorfismo sobjetivo

$$\ker \varphi = \{(g_1, g_2) \in G_1 \times G_2 : g_1 N_1 = N_1 \wedge g_2 N_2 = N_2\} = N_1 \times N_2$$

Pelo Teo do Homo, $\frac{G_1 \times G_2}{N_1 \times N_2} \cong \frac{G_1}{N_1} \times \frac{G_2}{N_2}$

21) Seja G um grupo e sejam H_1, \dots, H_n subgrupos normais de G tais que $G = H_1 \dots H_n$ e $H_i \cap H_1 \dots H_{i-1} = \{e\}$, para todo $i = 2, \dots, n$. Mostre que G é isomórfico ao produto direto de H_1, \dots, H_n . Dizemos, neste caso, que G é produto direto interno de H_1, \dots, H_n .

$\forall i \geq 2, H_1 \dots H_{i-1} \triangleleft G$, pois $H_1, \dots, H_{i-1} \triangleleft G$.

$$H_i \cap H_1 \dots H_{i-1} = \{e\} \Rightarrow h_k k = k h_i, \forall h \in H_1 \dots H_{i-1}, \forall i \geq 2. \text{ Em particular } h_i h_j = h_j h_i, \forall h_i \in H_i, h_j \in H_j, i \neq j.$$

Seja $\varphi: H_1 \times \dots \times H_n \longrightarrow G$

$$(h_1, \dots, h_n) \mapsto h_1 \dots h_n$$

φ é homo: $h = (h_1, \dots, h_n), k = (k_1, \dots, k_n) \in H_1 \times \dots \times H_n$

$$\begin{aligned} \varphi(hk) &= \varphi(h_1 k_1, \dots, h_n k_n) = h_1 k_1 h_2 k_2 \dots h_{n-1} k_{n-1} h_n k_n \\ &= h_1 k_1 \dots h_{n-1} h_n k_{n-1} k_n = \dots = h_1 \dots h_n k_1 \dots k_n = \varphi(h) \varphi(k) \end{aligned}$$

$\hookrightarrow k_i$ comuta com $h_j, \forall j > i$.

$$(h_1, \dots, h_n) \in \ker \varphi \Rightarrow h_1 h_2 \dots h_n = e \Rightarrow h_n = (h_1 h_2 \dots h_{n-1})^{-1} \in H_n \cap H_1 \dots H_{n-1} = \{e\}$$

$$\Rightarrow h_n = e \wedge h_1 \dots h_{n-1} = e \Rightarrow h_{n-1} = (h_1 \dots h_{n-2})^{-1} \in H_{n-1} \cap H_1 \dots H_{n-2} = \{e\}$$

$$\Rightarrow \dots \Rightarrow h_1 = \dots = h_n = e \therefore \varphi \text{ é injetor}$$

$$\text{Im } \varphi = H_1 \dots H_n = G.$$

$\therefore \varphi$ é isomorfismo.

22) Seja G um grupo e sejam H_1, \dots, H_n subgrupos de G . Mostre que G é o produto direto interno de H_1, \dots, H_n se e somente se

a) $h_i h_j = h_j h_i$, $\forall h_i \in H_i$ e $h_j \in H_j$, com $i \neq j$

b) Todo elemento de $g \in G$ se escreve de maneira única na forma

$$g = h_1 \dots h_n, \text{ com } h_i \in H_i, i=1, \dots, n.$$

(\Rightarrow) H_1, \dots, H_n são tais que $H_1 \dots H_n = G$, $H_i \triangleleft G \forall i$, e $H_i \cap H_1 \dots H_{i-1} = \{e\}$,

a) $H_i \cap H_1 \dots H_{i-1} = \{e\}, \forall i \geq 2 \Rightarrow H_i \cap H_j = \{e\}, \forall i \neq j$. $\forall i \geq 2$.

Como $H_i, H_j \triangleleft G$, temos $h_i h_j = h_j h_i, \forall h_i \in H_i, \forall h_j \in H_j$.

b) Se $g = h_1 \dots h_n = k_1 \dots k_n$, com $h_i, k_i \in H_i$ entao

$$h_n k_n^{-1} = (h_1 \dots h_{n-1})^{-1} (k_1 \dots k_{n-1}) \in H_n \cap H_1 \dots H_{n-1} = \{e\}$$

$$\Rightarrow h_n k_n^{-1} = e \quad \text{e} \quad h_1 \dots h_{n-1} = k_1 \dots k_{n-1}$$

$$\begin{matrix} \downarrow \\ h_n = k_n \end{matrix} \quad \begin{matrix} \downarrow \\ h_{n-1} k_{n-1}^{-1} = (h_1 \dots h_{n-2})^{-1} (k_1 \dots k_{n-2}) \in H_{n-1} \cap \\ H_1 \dots H_{n-2} \end{matrix}$$

$$\therefore h_{n-1} = k_{n-1} \text{ e } h_1 \dots h_{n-2} = k_1 \dots k_{n-2} \text{ etc... } \therefore h_1 = k_1 = \{e\}$$

(\Leftarrow) $H_i \triangleleft G$ pois, dados $x \in H_i$ e $g \in G$. ($g = h_1 \dots h_n$, com $h_i \in H_i$)

$$gxg^{-1} = h_1 \dots h_n x h_n^{-1} \dots h_1^{-1} = h_1 \dots h_n h_m^{-1} \dots h_{i+1}^{-1} x h_i \dots h_1^{-1}$$

os elementos de H_i comutam com os de H_j se $i \neq j$

$$= h_1 \dots h_i x h_i^{-1} \dots h_1^{-1} = h_i x h_i^{-1} h_1 \dots h_{i-1} h_{i-1}^{-1} \dots h_1^{-1} = h_i x h_i^{-1} \in H_i$$

$$H_1 \dots H_n = G \quad \text{OK}$$

se $x \in H_i \cap H_1 \dots H_{i-1}$ entao

$$H_i \ni x = h_1 \dots h_{i-1}, \text{ com } h_j \in H_j, j=1, \dots, i-1$$

$$e = h_1 \dots h_{i-1} x e \dots e \Rightarrow h_1 = e \dots = h_{i-1} = x$$

única

$$\therefore H_i \cap H_1 \dots H_{i-1} = \{e\}$$

24) Digamos que um grupo G é o produto semidireto (interno) de N por H se G contém subgrupos N e H tais que

$$\text{i)} N \triangleleft G \quad \text{ii)} NH = G \quad \text{iii)} N \cap H = \{e\}.$$

Resolva cada um dos itens abaixo

a) Mostre que se G é o produto semidireto interno de N por H entao os elementos de G podem ser expressos de maneira única na forma nh , com $n \in N$, $h \in H$.

Se $n_1 h_1 = n_2 h_2$ entao $n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H = \{e\} \Rightarrow n_1 = n_2$ e $h_1 = h_2$.

b) Seja G um produto semidireto de N por H . Mostre que

$$\theta: H \rightarrow \text{Aut}(N)$$

$$h \mapsto \theta_h, \text{ em que } \theta_h(n) = hn h^{-1}, \forall n \in N$$

θ é um homomorfismo.

θ_h é a restrição a N do automorfismo interno $\varphi_h: G \rightarrow G$

$$g \mapsto hg h^{-1}$$

$\therefore \theta_h$ é homo injeto

$$\text{Im } \theta_h = \{hn h^{-1} : n \in N\} = N, \text{ pois } N \triangleleft G.$$

$\therefore \theta_h$ é sobre N .

$$\therefore \theta_h \in \text{Aut}(N)$$

Vemos que $G \rightarrow \text{Aut}(G)$ é homo de grupos. Logo, $h \mapsto \theta_h = \varphi_h|_N$ também é.

$$g \mapsto \varphi_g$$

c) Sejam N e H dois grupos e seja $\theta: H \rightarrow \text{Aut}(N)$ um homomorfismo. Defina a seguinte operação binária no conjunto $N \times H = \{(n, h) : n \in N, h \in H\}$:

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \theta(h_1)(n_2), h_1 h_2).$$

Mostre que $N \times H$ com essa operação binária forma um grupo, chamado produto semidireto (externo) de N por H e denotado $N \rtimes_{\theta} H$.

• operação é associativa:

$$(n_1, h_1) \cdot ((n_2, h_2) \cdot (n_3, h_3)) = (n_1, h_1) \cdot (n_2 \theta(h_2)(n_3), h_2 h_3)$$

$$= (n_1 \theta(h_1)(n_2 \theta(h_2)(n_3)), h_1 h_2 h_3) = (n_1 \theta(h_1)(n_2) \theta(h_1) \theta(h_2)(n_3), h_1 h_2 h_3)$$

$$\downarrow \theta \text{ é homo} \\ = (n_1 \theta(h_1)(n_2) \theta(h_1 h_2)(n_3), h_1 h_2 h_3)$$

$$= (n_1 \theta(h_1)(n_2), h_1 h_2) \cdot (n_3, h_3) = ((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3)$$

• unidade: (e_N, e_H) , pois $\downarrow \text{id}_N \text{ pois } \theta \text{ é homo}$

$$(e_N, e_H) \cdot (n, h) = (e_N \theta(e_H)(n), h) = (e_N n, h) = (n, h)$$

$$(n, h) \cdot (e_N, e_H) = (n \theta(e_H)(e_N), h) = (n e_N, h) = (n, h)$$

$$\forall (n, h) \in N \times H$$

• inverso de (n, h) . Seja $n_1 \in N$ tq $\theta(h)(n_1) = \bar{n}'$ (\exists pois $\theta(h)$ é bijetor)

$$(n, h) \cdot (n_1, h^{-1}) = (n \theta(h)(n_1), h h^{-1}) = (e_N, e_H)$$

$$(n, h) \cdot (n_1, h^{-1}) = (n_1 \theta(h)^{-1}(n), h^{-1} h) = (e_N, e_H) \quad (\theta(h)(n_1) = \bar{n}' \Rightarrow \theta(h)(n_1^{-1}) = n)$$

$$\therefore \theta(h)^{-1}(n) = n_1^{-1}$$

d) Mostre que $N^* = \{(n, e) \in N \times_{\theta} H : n \in N\}$ é um subgrupo normal de $N \times_{\theta} H$ e que $N \times_{\theta} H$ é o produto semidireto de N^* por $H^* = \{(e, h) \in N \times_{\theta} H : h \in H\}$.

N^* e H^* são subgrupos de $N \times_{\theta} H$

$$\begin{cases} (n_1, e)(n_2, e) = (n_1 \theta(e)(n_2), e) = (n_1 n_2, e) \in N^* \\ (e, e) \in N^* \\ (n, e)^{-1} = (n^{-1}, e) \in N^* \end{cases}$$

$$\begin{cases} (e, h_1)(e, h_2) = (e \theta(h_1)(e), h_1 h_2) = (e, h_1 h_2) \in H^* \\ (e, e) \in H^* \\ (e, h)^{-1} = (e, h^{-1}) \in H^* \end{cases}$$

N^* é normal em $N \times_{\theta} H$:

$$(n, h)(n_1, e)(n_1, h)^{-1} = (n, h)(n_1, e)(n_1, h^{-1}) = (n, h \cdot h^{-1}) = (n, e) \in N^*$$

$$N^* \cap H^* = \{(e, e)\}$$

$$e \neq (n, h) \in N \times_{\theta} H, (n, h) = (n, e)(e, h) \in N^* H^*$$

e) Mostre que se G é o produto semidireto interno de N por H então $G \cong N \times_{\theta} H$, onde θ é o homomorfismo do item b)

$$\text{Sua } \varphi: N \times_{\theta} H \longrightarrow G \\ (n, h) \mapsto nh.$$

$$\begin{aligned} \text{É homo: } \varphi((n_1, h_1)(n_2, h_2)) &= \varphi(n_1 \theta_{h_1}(n_2), h_1 h_2) = \varphi(n_1 h_1 n_2 h_1^{-1}, h_1 h_2) = \\ &= n_1 h_1 n_2 h_1^{-1} h_1 h_2 = n_1 h_1 n_2 h_2 = \varphi(n_1, h_1) \varphi(n_2, h_2) \end{aligned}$$

$$\text{É injetor: } (n, h) \in \ker \varphi \Rightarrow nh = e = ee \Rightarrow n = e \cdot h = e, \text{ por (a)}$$

$$\text{É sobre, pois } \text{Im } \varphi = NH = G.$$

f) Mostre que o grupo diédral D_n é um produto semidireto de um grupo cíclico de ordem n por um grupo cíclico de ordem 2.

$$\text{Sejam } C_n = \langle b \rangle, C_2 = \langle a \rangle$$

$$\begin{aligned} \theta: C_2 &\longrightarrow \text{Aut}(C_n) \\ a &\mapsto \theta(a)(b) = b^{-1} \end{aligned} \quad \theta(a) \in \text{Aut}(C_n), \text{ pois } C_n \text{ é abeliano.}$$

$$C_n \times_{\theta} C_2 = \langle \sigma = (b, e), \tau = (e, a) \rangle \quad (\text{pois } b \text{ gera } C_n \text{ e } a \text{ gera } C_2)$$

$$\sigma^n = (b, e)^n = (b^n, e) = (e, e) \quad \tau^2 = (e, a)^2 = (e, a^2) = (e, e)$$

$$\tau \sigma \tau = (e, a)(b, e)(e, a) = (b^{-1}, a)(e, a) = (b^{-1}, e) = \sigma^{-1}$$

Grupos abelianos finitos

25) Descreva todos os grupos abelianos de ordem $2^3 \cdot 3^4 \cdot 5$

$$P(3) = |\{3, 2+1, 1+1+1\}| = 3$$

$$P(4) = |\{4, 3+1, 2+2, 2+1+1, 1+1+1+1\}| = 5$$

$$P(1) = 1$$

São 15 grupos:

$$C_2^3 \times C_3^4 \times C_5 \cong C_{2^3 3^4 5}$$

$$C_2^2 \times C_2 \times C_3^4 \times C_5 \cong C_{2^2 3^4 5} \times C_2$$

$$C_2 \times C_2 \times C_2 \times C_3^4 \times C_5 \cong C_{2,3^4,5} \times C_2 \times C_2$$

$$C_2^3 \times C_3^3 \times C_3 \times C_5 \cong C_{2^3 3^3 5} \times C_3$$

$$C_2 \times C_2 \times C_3^3 \times C_3 \times C_5 \cong C_{2,3^3,5} \times C_{2,3}$$

$$C_2 \times C_2 \times C_2 \times C_3^3 \times C_3 \times C_5 \cong C_{2,3^2,5} \times C_{2,3} \times C_2$$

$$C_2^3 \times C_3^2 \times C_3^2 \times C_5 \cong C_{2^3,3^2,5} \times C_3^2$$

$$C_2^2 \times C_2 \times C_3^2 \times C_2 \times C_5 \cong C_{2^2,3^2,5} \times C_{2,3^2}$$

$$C_2 \times C_2 \times C_2 \times C_3^2 \times C_3^2 \times C_5 \cong C_{2,3^2,5} \times C_{2,3^2} \times C_2$$

$$C_2^3 \times C_3^2 \times C_3 \times C_3 \times C_5 \cong C_{2^3,3^2,5} \times C_3 \times C_3$$

$$C_2^2 \times C_2 \times C_3^2 \times C_3 \times C_3 \times C_5 \cong C_{2^2,3^2,5} \times C_{2,3} \times C_3$$

$$C_2 \times C_2 \times C_2 \times C_3^2 \times C_3 \times C_3 \times C_5 \cong C_{2,3^2,5} \times C_{2,3} \times C_{2,3}$$

$$C_2^3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_5 \cong C_{2^3,3,5} \times C_3 \times C_3 \times C_3$$

$$C_2^2 \times C_2 \times C_3 \times C_3 \times C_3 \times C_3 \times C_5 \cong C_{2^2,3,5} \times C_{2,3} \times C_3 \times C_3$$

$$C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_3 \times C_3 \times C_5 \cong C_{2,3,5} \times C_{2,3} \times C_{2,3} \times C_3.$$

26) Mostre que um grupo abeliano finito não é cíclico se e somente se ele contiver um subgrupo isomórfico a $\mathbb{Z}_p \times \mathbb{Z}_p$, para algum primo p positivo.

(\Rightarrow) Se G é abeliano e não é cíclico, a decomposição

$G \cong C_{m_1} \times \dots \times C_{m_s}$ com $m_i | m_{i-1}$, $i \geq 2$, e $m_i > 1$, $\forall i = 1, \dots, s$, tem pelo menos 2 fatores.

Seja $C_{m_1} = \langle a \rangle$, $C_{m_2} = \langle b \rangle$ e seja p primo tq $p | m_2$.

Então $p | m_1$ (pois $m_2 | m_1$).

Escreva $m_1 = rp$ e $m_2 = sp$. Daí $\sigma(a^r) = p = \sigma(b^s)$

Então $\langle a^r \rangle \times \langle b^s \rangle \times \langle e \rangle \times \dots \times \langle e \rangle$ é subgrupo de G isomórfico a $\mathbb{Z}_p \times \mathbb{Z}_p$.

(\Leftarrow) Observe que $\mathbb{Z}_p \times \mathbb{Z}_p$ não é um grupo cíclico (não possui elementos de ordem p^2).

Se G possui um subgrupo isomórfico a $\mathbb{Z}_p \times \mathbb{Z}_p$, G não pode ser cíclico, já que todo subgrupo de um grupo cíclico é cíclico.

27) Mostre que um grupo abeliano finito não é divisível por um quadrado então o grupo é cíclico.

$|G| = p_1 \dots p_r$, p_i primos distintos

$G \cong H_1 \times \dots \times H_r$ com $|H_i| = p_i$

∴ Cada H_i é isomórfico a \mathbb{Z}_{p_i} .

∴ $G \cong \mathbb{Z}_{p_1} \times \dots \times \mathbb{Z}_{p_r} \cong \mathbb{Z}_{p_1 \dots p_r}$ é cíclico
 $\downarrow p_i \neq s$

28) Sejam G_1, G_2, G_3 grupos abelianos finitos. Mostre que se $G_1 \times G_2 \cong G_1 \times G_3$ entao $G_2 \cong G_3$.

Sejam $G_1 \cong C_{p_1^{\alpha_1}} \times \dots \times C_{p_k^{\alpha_k}}$ p_i 's primos mas necessaria e $\alpha_i \geq 1$

$G_2 \cong C_{q_1^{\beta_1}} \times \dots \times C_{q_s^{\beta_s}}$ q_j 's

$G_3 \cong C_{t_1^{\gamma_1}} \times \dots \times C_{t_r^{\gamma_r}}$ t_i 's

as decomposições de G_1, G_2 e G_3 como produtos de p -grupos cíclicos.

Como $G_1 \times G_2 \cong G_1 \times G_3$, temos, pela uniridade dos fatores, que $\{p_1^{\alpha_1}, \dots, p_k^{\alpha_k}, q_1^{\beta_1}, \dots, q_s^{\beta_s}\} = \{p_1^{\alpha_1}, \dots, p_k^{\alpha_k}, t_1^{\gamma_1}, \dots, t_r^{\gamma_r}\}$

$$\therefore \{q_1^{\beta_1}, \dots, q_s^{\beta_s}\} = \{t_1^{\gamma_1}, \dots, t_r^{\gamma_r}\}$$

Assim, $G_2 \cong C_{q_1^{\beta_1}} \times \dots \times C_{q_s^{\beta_s}} = C_{t_1^{\gamma_1}} \times \dots \times C_{t_r^{\gamma_r}} \cong G_3$.

29) Seja G um grupo e seja $Z(G)$ o centro de G .

a) Mostre que se $G/Z(G)$ for cíclico entao G será abeliano

b) Mostre que se G tem ordem p^2 , onde p é um número primo, entao G é abeliano

c) Suponha que G não seja abeliano e que $|G| = p^3$, onde p é um número primo. Mostre que $Z(G) = G'$ e que $G/Z(G) \cong G_p \times C_p$, onde G_p denota o grupo cíclico de ordem p .

a) Seja $G/Z(G) = \langle gZ(G) \rangle$.

Para $x, y \in G$, $xZ(G) = g^r Z(G)$, $yZ(G) = g^s Z(G)$, para alguns $r, s \in \mathbb{Z}$.

$\therefore x = g^r z_1, y = g^s z_2$, com $z_1, z_2 \in Z(G)$

$$\Rightarrow xy = g^r z_1 g^s z_2 \xrightarrow{z_i \in Z(G)} g^{r+s} z_1 z_2 = g^s z_2 g^r z_1 = yx.$$

$\therefore G$ é abeliano

b) Sabemos que $|Z(G)| > 1$ se G é um p -grupo.

Assim, $Z(G) = G$ (se $Z(G) \neq G$, $|G/Z(G)| = p \Rightarrow G/Z(G)$

é cíclico $\Rightarrow G$ abeliano $\Rightarrow Z(G) = G$).

c) Novamente, $|Z(G)| > 1$

• $|Z(G)| = p^3 \Rightarrow Z(G) = G \Rightarrow G$ abeliano

• $|Z(G)| = p^2$ mas ocorre, pn a) (novamente, $|G/Z(G)| = p$). então

$\therefore Z(G) = p$.

$|G/Z(G)| = p^2$. Por b), $G/Z(G)$ é abeliano

• Além disso, $G/Z(G)$ não pode ser cíclico.

$\therefore G/Z(G) \cong G_p \times G_p$.

Para concluir sobre o comutador G' , observe que $G/Z(G)$ é abeliano. logo, $G' \subseteq Z(G)$.

Por outro lado, $G' \neq \{e\}$, pois G não é abeliano

Portanto, $G' = Z(G)$ (já que $|Z(G)| = p$)

Acções

3) Seja G um grupo de ordem p^k , em que p é um número primo e $k > 0$.
 Mostre que se H é um subgrupo de ordem p^{k-1} então H é normal em G .
 Se $|H| = p^{k-1}$ então $[G:H] = p$.

Seja $\varphi: G \rightarrow S_{G/H}$ (classes laterais à esquerda)
 $g \mapsto \varphi_g: G/H \rightarrow G/H$
 $xH \mapsto \varphi_g(xH) = gxH$.

ja'sabemos que φ é uma ação de G em G/H e

$$\ker \varphi = \bigcap_{x \in G} xHx^{-1} \subseteq H \quad (\text{pois } H = eHe^{-1} \supseteq \bigcap_{x \in G} xHx^{-1}).$$

$$\hookrightarrow (ge \in \ker \varphi \Leftrightarrow gxH = xH, \forall x \in G \Leftrightarrow x^{-1}gx \in H, \forall g \in G \Leftrightarrow g \in xHx^{-1}, \forall x \in G)$$

$$|\ker \varphi| = p^t, \text{ para algum } t \leq k-1$$

$$\text{Logo, } |G/\ker \varphi| = p^{k-t}$$

$$\text{Temos } G/\ker \varphi \cong \text{Im } \varphi \leq S_{G/H}$$

$$\text{Portanto, } |\text{Im } \varphi| \mid p! \Rightarrow |G/\ker \varphi| \mid p! \Rightarrow p^{k-t} \mid p!$$

$$\text{Logo, } k-t \leq 1 \Rightarrow t \geq k-1$$

$$\therefore t = k-1 \therefore \ker \varphi = H \quad \therefore H \triangleleft G$$

3) Seja G um p -grupo finito, onde p é um primo positivo. Seja H um subgrupo normal de G tal que $H \neq \{e\}$. Mostre que $H \cap Z(G) \neq \{e\}$.

$$|H| = p^k, \text{ com } k \geq 1 \quad (\text{pois } H \neq \{e\} \text{ e } G \text{ é } p\text{-grupo})$$

G age em G por conjugações

$$\begin{aligned} \varphi: G &\rightarrow S_G \\ g &\mapsto \varphi_g: G \rightarrow G \\ &x \mapsto gxg^{-1} \end{aligned}$$

$$\left(\begin{array}{l} \text{ou faz logo} \\ \varphi: G \rightarrow S_H \\ g \mapsto \varphi_g: H \rightarrow H \\ h \mapsto ghg^{-1} \end{array} \right)$$

$$\forall h \in H, \{ghg^{-1}: g \in G\} \subseteq H, \text{ pois } H \triangleleft G.$$

$$\text{Logo, } |H| = \sum_{h \in H} |\{ghg^{-1}: g \in G\}| = |Z(G) \cap H| + \sum_{\substack{h \in H, \\ h \notin Z(G)}} |\{ghg^{-1}: g \in G\}|$$

(tomando 1 representante de cada classe)

$$\text{Como } p \mid |\{ghg^{-1}: g \in G\}|, \forall h \in H, h \notin Z(G) \text{ temos que } p \mid |Z(G) \cap H|$$

$$\therefore Z(G) \cap H \neq \{e\}$$

33) Seja G um grupo que age em um conjunto S . Para cada $g \in G$, considere o seguinte subconjunto de S

$$S^g = \{x \in S : g \cdot x = x\}$$

Mostre que o número de órbitas distintas da ação de G em S é dado por

$$\frac{1}{|G|} \sum_{g \in G} |S^g|$$

Vamos contar quantos pares $(g, x) \in G \times S$ satisfazem $g \cdot x = x$, de 2 maneiras:

Fixando cada $g \in G$, esse número é $\sum_{x \in S} |S^g|$ (1)

Fixando agora $x \in S$, esse número é $\sum_{g \in G} |\text{stab}(x)|$ (2) ($\text{stab}(x) = \{g \in G : g \cdot x = x\}$)

São O_{x_1}, \dots, O_{x_r} as órbitas distintas da ação de G em S . Então

$$(2) = \sum_{i=1}^r \sum_{x \in O_{x_i}} |\text{stab}(x)|$$

Temos ainda que $|O_x| = [G : \text{stab}(x)]$

$$\therefore \forall y \in O_x, [G : \text{stab}(y)] = |O_y| = |O_x| = [G : \text{stab}(x)].$$

Logo, $\sum_{x \in O_{x_i}} |\text{stab}(x_i)| = |O_{x_i}| |\text{stab}(x_i)| = |G|$

$$\downarrow |O_{x_i}| = \frac{|G|}{|\text{stab}(x_i)|}$$

Como (1) = (2), segue que $\sum_{g \in G} |S^g| = r |G|$

$$\therefore r = \frac{1}{|G|} \sum_{g \in G} |S^g|$$