MA446 Grupos e Representações - Exercícios P2

Adair Neto

22 de maio de 2023

Lista 2

Lema 1

Questão: $\text{Inn}(G) \cong G/Z(G)$.

Resolução:

- Considere a aplicação

$$\begin{aligned} \theta : G &\longrightarrow \text{Inn}(G) \\ g &\longmapsto \varphi_g \end{aligned}$$

- em que φ_g é a conjugação com g à esquerda:

$$\begin{aligned} \varphi_g : G &\longrightarrow G \\ h &\longmapsto ghg^{-1} \end{aligned}$$

- θ é claramente sobrejetivo.
- θ é homomorfismo pois

$$\theta(g_1g_2) = \varphi_{g_1g_2} = \varphi_{g_1}\varphi_{g_2} = \theta(g_1)\theta(g_2)$$

- Temos que o núcleo é dado por

$$\ker(\theta) = \{g \in G \mid \theta(g) = 1_{\text{Inn}(G)}\} = \{g \in G \mid ghg^{-1} = h,\ \forall\ h \in G\} = Z(G)$$

- Assim, pelo teorema de isomorfismos,

$$\frac{G}{\ker(\theta)} = \frac{G}{Z(G)} \cong \text{im}(\theta) = \text{Inn}(G)$$

Lema 2 (Questão 2a P2 2020)

Questão: Se $G/Z(G)$ é cíclico, então G é abeliano.

Resolução:

- Como $G/Z(G)$ é cíclico, existe $t \in G/Z(G)$ tal que $G/Z(G) = \langle tZ(G) \rangle$.
- Sejam $g, h \in G$. Podemos escrever

$$gZ(G) = t^nZ(G), \quad hZ(G) = t^mZ(G)$$

- em que $n, m \in \mathbb{Z}$.
- Por outro lado, existem $t_1, t_2 \in Z(G)$ tais que

$$g = t^nt_1, \quad h = t^mt_2$$

- Portanto,

$$gh = t^nt_1t^mt_2 = t^nt^mt_1t_2 = t^mt^nt_2t_1 = t^mt_2t^nt_1 = hg$$

- Logo, G é abeliano.

Lema 3

Questão: Se $H \blacktriangleleft N \blacktriangleleft G$, então $H \blacktriangleleft G$, em que $A \blacktriangleleft B$ significa "A é característico em B".

Resolução:

- Seja $\varphi \in \mathrm{Aut}(G)$.
- Como $N \blacktriangleleft G$, então $\varphi(N) = N$.
- Assim, $\varphi|_N \in \mathrm{Aut}(N)$.
- Portanto, como $H \blacktriangleleft N$,
$$\varphi(H) = \varphi|_N(H) = H$$
- Logo, $H \blacktriangleleft G$.

Lema 4 (Relações de Steinberg)

Questão: Mostre que

$$\begin{aligned} e_{ij}(\lambda)e_{ij}(\mu) &= e_{ij}(\lambda+\mu) \\ [e_{ij}(\lambda), e_{jr}(\mu)] &= e_{ir}(\lambda\mu), && \text{se } i \neq r \\ [e_{ij}(\lambda), e_{rs}(\mu)] &= I_n, && \text{se } i \neq s \text{ e } j \neq r \end{aligned}$$

Observe que, da primeira relação, temos que $e_{ij}(\lambda)^{-1} = e_{ij}(-\lambda)$.

Resolução:

0. Seja e_r um elemento da base de K^n.
1. $e_{ij}(\lambda)e_{ij}(\mu) = e_{ij}(\lambda+\mu)$.
$$\left(e_{ij}(\lambda)e_{ij}(\mu)\right)(e_r) = \left(e_{ij}(\lambda)\right)(e_j + \mu e_i) = (e_j + (\lambda+\mu)e_i) = e_{ij}(\lambda+\mu)(e_r)$$
2. $[e_{ij}(\lambda), e_{jr}(\mu)] = e_{ir}(\lambda\mu)$, se $i \neq r$.
$$\begin{aligned} \left(e_{ij}(\lambda)^{-1}e_{jr}(\mu)^{-1}e_{ij}(\lambda)e_{jr}(\mu)\right)(e_r) &= \left(e_{ij}(-\lambda)e_{jr}(-\mu)e_{ij}(\lambda)e_{jr}(\mu)\right)(e_r) \\ &= \left(e_{ij}(-\lambda)e_{jr}(-\mu)e_{ij}(\lambda)\right)(e_r + \mu e_j) \\ &= \left(e_{ij}(-\lambda)e_{jr}(-\mu)\right)(e_r + \mu e_j + \mu\lambda e_i) \\ &= \left(e_{ij}(-\lambda)\right)(e_r + \mu\lambda e_i) \\ &= e_r + \mu\lambda e_i = e_{ir}(\lambda\mu)(e_r) \end{aligned}$$
3. $[e_{ij}(\lambda), e_{rs}(\mu)] = I_n$, se $i \neq s$ e $j \neq r$
$$\begin{aligned} \left(e_{ij}(\lambda)^{-1}e_{rs}(\mu)^{-1}e_{ij}(\lambda)e_{rs}(\mu)\right)(e_r) &= \left(e_{ij}(-\lambda)e_{rs}(-\mu)e_{ij}(\lambda)e_{rs}(\mu)\right)(e_r) \\ &= \left(e_{ij}(-\lambda)e_{rs}(-\mu)e_{ij}(\lambda)\right)(e_r) \\ &= \left(e_{ij}(-\lambda)e_{rs}(-\mu)\right)(e_r) \\ &= \left(e_{ij}(-\lambda)\right)(e_r) \\ &= e_r \end{aligned}$$

Exercício 1

Questão: Classifique todos os grupos abelianos de ordem $2^3 3^2 5^2$.

Resolução:

- Sabemos que G é isomorfo ao produto direto de $G(p)$ sobre todos os primos p tais que existe $g \in G \setminus \{1_G\}$ com $|g|$ potência de p, i.e.,
$$G = \bigoplus G(p)$$
- Além disso, cada $G(p)$ tem tipo único $(p^{r_1}, p^{r_2}, \ldots, p^{r_k})$ para $r_1 \geq r_2 \geq \ldots \geq r_k > 0$. Assim,
$$G(p) \cong \frac{\mathbb{Z}}{p^{r_1}\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{p^{r_k}\mathbb{Z}}$$

- Portanto, se G é grupo abeliano de ordem $2^3 3^2 5^2$, então

$$G = G(2) \oplus G(3) \oplus G(5)$$

- Possibilidades para G(2):
  - Temos que $|G(2)| = 2^3 = 2^{r_1+\cdots+r_k}$.
  - Se $2^{r_1} = 8$, temos $k = 1$ e $G(2) = \frac{\mathbb{Z}}{8\mathbb{Z}}$.
  - Se $2^{r_1} = 4$, temos $2^{r_2} = 2$, $k = 2$ e $G(2) = \frac{\mathbb{Z}}{4\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$.
  - Se $2^{r_1} = 2$, temos $r_1 = r_2 = r_3$, $k = 3$ e $G(2) = \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$.
- Possibilidades para G(3):
  - Temos que $|G(3)| = 3^2 = 3^{r_1+\cdots+r_k}$.
  - Se $3^{r_1} = 9$, temos $k = 1$ e $G(3) = \frac{\mathbb{Z}}{9\mathbb{Z}}$.
  - Se $3^{r_1} = 3$, temos $r_2 = r_1$, $k = 2$ e $G(3) = \frac{\mathbb{Z}}{3\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$.
- Possibilidades para G(5):
  - Temos que $|G(5)| = 5^2 = 5^{r_1+\cdots+r_k}$.
  - Se $5^{r_1} = 25$, temos $k = 1$ e $G(5) = \frac{\mathbb{Z}}{25\mathbb{Z}}$.
  - Se $5^{r_1} = 5$, temos $r_2 = r_1$, $k = 2$ e $G(5) = \frac{\mathbb{Z}}{5\mathbb{Z}} \oplus \frac{\mathbb{Z}}{5\mathbb{Z}}$.
- Totalizando, temos $3 \cdot 2 \cdot 2 = 12$ possibilidades.

Exercício 2

Questão: Determine todas as permutações em S_8 que comutam com $\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}$. Prove que essas permutações formam um subgrupo de S_8 e calcule a ordem desse subgrupo.

Resolução:

- Tome $g \in S_8$.
- Se g comuta com $\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}$, então

$$g\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix} = \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}g$$

- Mas isso equivale a

$$\begin{aligned}\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix} &= g\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}g^{-1} \\ &= g\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}g^{-1}g\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}g^{-1}\end{aligned}$$

- Como $g\begin{pmatrix}i_1 & i_2 & \dots & i_m\end{pmatrix}g^{-1} = \begin{pmatrix}g(i_1) & g(i_2) & \dots & g(i_m)\end{pmatrix}$, temos que

$$\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix} = \begin{pmatrix}g(1) & g(2) & g(3) & g(4)\end{pmatrix}\begin{pmatrix}g(5) & g(6) & g(7) & g(8)\end{pmatrix}$$

- Como os dois ciclos têm a mesma ordem, temos duas possibilidades:
  1. $\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix} = \begin{pmatrix}g(1) & g(2) & g(3) & g(4)\end{pmatrix}$ e $\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix} = \begin{pmatrix}g(5) & g(6) & g(7) & g(8)\end{pmatrix}$.
  2. $\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix} = \begin{pmatrix}g(5) & g(6) & g(7) & g(8)\end{pmatrix}$ e $\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix} = \begin{pmatrix}g(1) & g(2) & g(3) & g(4)\end{pmatrix}$.
- Note que em cada caso temos quatro possibilidades para o primeiro ciclo e quatro para o segundo. Assim, temos dezesseis possibilidades em cada caso, totalizando trinta e duas possibilidades.
- Por fim, sejam g_1, g_2 permutações em S_8 que comutam com $\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}$.
- Portanto,

$$\begin{aligned}g_1g_2^{-1}\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}(g_1g_2^{-1})^{-1} &= g_1(g_2^{-1}\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}g_2)g_1^{-1} \\ &= g_1\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}g_1^{-1} \\ &= \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}\end{aligned}$$

- Logo, $g_1g_2^{-1}$ comuta com $\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix}$ e, assim, temos que essas permutações formam um subgrupo que, conforme vimos, tem ordem trinta e dois.

Exercício 3

Questão: Sejam G um grupo e H um subgrupo característico de G. Prove que se H é cíclico, então todo subgrupo de H é característico e, portanto, normal em G.

Resolução:

- Como H é cíclico, existe $h \in H$ tal que $H = \langle h \rangle$.
- Seja N um subgrupo de H e $\varphi \in \mathrm{Aut}(G)$.
- Como $N \leq H$, temos que N é gerado por h^r para algum $r \in \mathbb{Z}$.
- Assim, cada elemento $a \in N$ pode ser escrito como $a = h^{nr}$, com $n \in \mathbb{Z}$.
- E como H é um subgrupo característico de G, $\varphi(h) = h^s$, para algum $s \in \mathbb{Z}$.
- Dessa forma,
$$\varphi(h^{nr}) = (h^{nr})^s = h^{(ns)r} \in N$$
- Logo, N é subgrupo característico de G e, portanto, normal em G.

Exercício 4

Questão: Sejam G um grupo e H um subgrupo de G tal que $[G : H]$ é finito. Prove que existe um subgrupo N de G tal que $N \lhd G$, $N \subseteq H$ e $[G : N]$ é também finito.

Resolução:

0. Ideia: vamos definir N como o núcleo da ação por produto de G nas classes laterais de H em G.
1. Definir a ação:
   - Seja $X = \{tH\}_{t \in G}$ o conjunto das classes laterais de H em G.
   - Temos que G age sobre X à esquerda via produto, i.e., existe homomorfismo
$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Perm}(X) \\ g &\longmapsto \varphi(g) \end{aligned}$$
   - em que
$$\begin{aligned} \varphi(g) : X &\longrightarrow X \\ tH &\longmapsto g * tH \end{aligned}$$
2. Mostrar que φ é homomorfismo.
   - Dados $g_1, g_2 \in G$,
$$\varphi(g_1 g_2)(tH) = (g_1 g_2) * tH$$
   - Por outro lado,
$$\varphi(g_1)\varphi(g_2)(tH) = \varphi(g_1)(g_2 * tH) = g_1 * (g_2 * tH) = (g_1 g_2) * tH$$
   - Portanto, φ é homomorfismo.
3. Mostrar que cada $\varphi(g)$ é bijetora (i.e. uma permutação de X).
   - Aqui basta notar que $\varphi^{-1}(g)$ dada por $\varphi^{-1}(g)(g * tH) = tH$ é inversa de $\varphi(g)$.
   - De fato,
$$(\varphi^{-1}(g) \circ \varphi(g))(tH) = \varphi^{-1}(g)(g * tH) = tH$$
   - e
$$(\varphi(g) \circ \varphi^{-1}(g))(g * tH) = \varphi(g)(tH) = g * tH$$
4. Calcular o núcleo de φ.
$$\begin{aligned} \ker(\varphi) &= \{g \in G \mid \varphi(g) = 1_{S_X}\} \\ &= \{g \in G \mid g * tH = tH,\ \forall t \in G\} \\ &= \{g \in G \mid t^{-1}gt \in H,\ \forall t \in G\} \\ &= \{g \in G \mid g \in tHt^1,\ \forall t \in G\} \\ &= \bigcap_{t \in G} tHt^{-1} \end{aligned}$$
5. Aplicar teorema de isomorfismos para mostrar que $G/\ker(\varphi)$ é finito.
   - Assim, temos que
$$G/\ker(\varphi) \cong \mathrm{im}(\varphi)$$
   - Como $\mathrm{im}(\varphi)$ é um subgrupo de $\mathrm{Perm}(X)$, que é finito (pois X é finito), temos que $\mathrm{im}(\varphi)$ é finito.
   - Portanto, $G/\ker(\varphi)$ é finito.

- Denotando $N = \ker(\varphi)$, como o núcleo é normal, temos que $N \triangleleft G$ e

$$[G : N] = \left|\frac{G}{N}\right| = \frac{|G|}{|N|} < \infty$$

6. Mostrar que $N \subseteq H$.
    - Como $N = \bigcap_{t \in G} tHt^{-1} \subseteq tHt^{-1}$, tomando $t = 1$ temos que $N \subseteq H$.

Exercício 5

Questão: Classifique todos os grupos de ordem 22.

Resolução:

1. Analisar $\mathrm{Syl}_{11}(G)$.
    - Como $22 = 2 \cdot 11$, pelo Teorema de Sylow, temos que

$$n_{11} \equiv 1 \mod 11, \quad n_{11} \mid |G| = 2 \cdot 11 \implies n_{11} \mid 2 \implies n_{11} \in \{1, 2\}$$

    - Mas $2 \not\equiv 1 \mod 11$ nos dá que $n_{11} = 1$.
    - Assim, $N \in \mathrm{Syl}_{11}(G)$ é o único 11-Sylow subgrupo de G e $|N| = 11$.
    - Note que, se $g \in G$, então como $gNg^{-1} = N$, $gNg^{-1} \in \mathrm{Syl}_{11}(G)$ e N é único, temos que $N \triangleleft G$.
2. Analisar $\mathrm{Syl}_2(G)$.
    - Considere agora $P \in \mathrm{Syl}_2(G)$.
    - Como $|P| = 2$ e $N \triangleleft G$, temos $NP \leq G$.
    - Mostremos que a interseção $N \cap P$ é trivial.

$$g \in N \cap P \implies |g| \mid |N| = 11 \quad \text{e} \quad |g| \mid |P| = 2 \implies |g| = 1 \implies g = 1_G$$

    - Assim, NP é produto semidireto de N por P, i.e. $N \rtimes P$.
3. Avaliar o produto semidireto.
    - Note que $N \cong \mathbb{Z}_{11}$ e $P \cong \mathbb{Z}_2$.
    - Queremos encontrar todos os possíveis homomorfismos de grupos

$$\begin{aligned} \theta : \mathbb{Z}_2 &\longrightarrow \mathrm{Aut}(\mathbb{Z}_{11}) \\ x &\longmapsto \theta(x) \end{aligned}$$

    - Em que

$$\begin{aligned} \rho := \theta(x) : \mathbb{Z}_{11} &\longrightarrow \mathbb{Z}_{11} \\ y &\longmapsto \rho(y) = y^m, \quad 1 \leq m \leq 10 \end{aligned}$$

    - Observe que $\mathbb{Z}_2 = \{1, x\}$, $x^2 = 1$ e $\mathbb{Z}_2 = \langle x \rangle$.
    - Com isso, temos que

$$\theta(x)^2 = \theta(x^2) = \theta(1_P) = 1_{\mathrm{Aut}(N)} = \mathrm{id}_N = \rho^2$$

    - Como $\rho(y) = y^m$,

$$\rho^2(y) = \rho(\rho(y)) = \rho(y^m) = (y^m)^m = y^{m^2} = y \implies y^{m^2-1} = 1 \implies 11 = |y| \mid m^2 - 1$$

    - Assim, $11 \mid (m+1)(m-1)$ e, como 11 é primo, temos que $11 \mid m-1$ ou $11 \mid m+1$.
    - Caso $11 \mid m-1$:
        - Então $m = 1$ (porque $1 \leq m \leq 10$) e $\rho = \mathrm{id}_N$.
        - Com isso,

$$\theta(x) = \rho = \mathrm{id}_N \implies xnx^{-1} = n, \quad \forall\ n \in N$$

        - Logo,

$$G = N \rtimes_\theta P = N \times P = \mathbb{Z}_{11} \times \mathbb{Z}_2$$

        - Pelo Teorema Chinês dos Restos, $G \cong \mathbb{Z}_{22}$.
    - Caso $11 \mid m+1$:
        - Então $m = 10 = -1$.
        - Temos que $\rho(y) = y^{-1}$ e $\rho \neq \mathrm{id}_N$.
        - Neste caso, G não é abeliano (é grupo diedral).

Exercício 6a

Questão: Sejam G um p-grupo e $H \lhd G$ um subgrupo normal de ordem p. Prove que $H \subseteq Z(G)$.

Resolução:

1. Construir uma ação de G sobre H.
   - Seja $X = H \setminus \{1_G\}$ e
$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Perm}(X) \\ g &\longmapsto \varphi(g) \end{aligned}$$
   - em que
$$\begin{aligned} \varphi(g) : X &\longrightarrow \mathrm{Perm}(X) \\ x &\longmapsto gxg^{-1} \end{aligned}$$
2. Mostrar que $\varphi(g)$ é trivial.
   - Para concluir que $ghg^{-1} = h$, em que $h \in H$, a ideia é mostrar que $\varphi(g) = 1_{S_X}$ para todo $g \in G$.
   - Como $|\varphi(g)|$ divide $|\mathrm{Perm}(X)|$,
$$|\mathrm{Perm}(X)| = |X|! = (p-1)! \implies |\varphi(g)| \mid (p-1)!$$
   - Por outro lado, $|\varphi(g)|$ divide $|g| = p^m$, para algum $m \in \mathbb{Z}$.
   - Assim, como $\mathrm{mdc}((p-1)!,\ p^m) = 1$, segue que $|\varphi(g)| = 1$ e, portanto, $\varphi(g) = 1_{S_X}$.
   - Logo, $\varphi(g)(x) = gxg^{-1} = x$ e, com isso, $H \subseteq Z(G)$.

Exercício 6b

Questão: Prove que todo p-grupo finito não trivial contém um subgrupo normal de índice p.

Resolução:

1. Veja que é solúvel.
   - Seja G um p-grupo finito não trivial.
   - Sabemos que todo p-grupo finito é solúvel.
   - Isso significa que existe uma cadeia
$$1_G = G^{(n)} \lhd \cdots \lhd G' \lhd G$$
   - em que cada $G'_i \subseteq G'_{i+1}$.
2. Mostre que $G' \neq G$.
   - Caso $G' = G$, temos que $G' = G^{(2)} = \cdots = G^{(n)} = 1_G$, o que contradiz a hipótese de G ser não trivial.
3. Considere o quociente G/G' e use a caracterização de grupos abelianos finitos.
   - Assim, como $G' \neq G$ e $G' \lhd G$, considere o grupo quociente G/G' e a projeção canônica
$$\pi : G \longrightarrow G/G'$$
   - Note que G/G' é p-grupo abeliano finito.
   - Da caracterização de grupos abelianos finitos, temos que
$$G/G' \cong \frac{\mathbb{Z}}{p^{r_1}\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{p^{r_k}\mathbb{Z}}$$
4. Encontre um subgrupo normal de índice p.
   - Note que $H := \left(p\frac{\mathbb{Z}}{p^{r_1}\mathbb{Z}}\right) \oplus \cdots \oplus \frac{\mathbb{Z}}{p^{r_k}\mathbb{Z}}$ é subgrupo de $\frac{\mathbb{Z}}{p^{r_1}\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{p^{r_k}\mathbb{Z}}$ de índice p.
   - Ou seja, H é subgrupo de G/G' de índice p.
   - Logo, $\pi^{-1}(H)$ é subgrupo normal de G de índice p.

Exercício 7

Questão: Seja G um grupo tal que Aut(G) é cíclico. Mostre que G é abeliano.

Resolução:

1. Como Aut(G) é cíclico e todo subgrupo de grupo cíclico é cíclico, temos que Inn(G) é cíclico.
2. Note que $\mathrm{Inn}(G) \cong G/Z(G)$ (Lema 1).
3. Assim, $G/Z(G)$ é cíclico e, portanto, G é abeliano (Lema 2).

Exercício 8

Questão: Achar as ordens dos elementos do grupo $\mathrm{Aut}(S_3)$.

Resolução:

- Lembre que S_3 é gerado por $\begin{pmatrix}1 & 2\end{pmatrix}$ e $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$.
- Assim temos os seguintes elementos em S_3:
  1. 1_{S_3}, de ordem 1.
  2. $\begin{pmatrix}1 & 2\end{pmatrix}$, de ordem 2.
  3. $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$, de ordem 3.
  4. $\begin{pmatrix}1 & 2 & 3\end{pmatrix}^2 = \begin{pmatrix}1 & 3 & 2\end{pmatrix}$, de ordem 3.
  5. $\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\end{pmatrix} = \begin{pmatrix}2 & 3\end{pmatrix}$, de ordem 2.
  6. $\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2\end{pmatrix} = \begin{pmatrix}1 & 3\end{pmatrix}$, de ordem 2.
- Como todo homomorfismo $\varphi : S_3 \longrightarrow S_3$ é completamente determinado por $\varphi(\begin{pmatrix}1 & 2\end{pmatrix})$ e $\varphi(\begin{pmatrix}1 & 2 & 3\end{pmatrix})$.
- E como, se φ é automorfismo, φ preserva a ordem dos elementos.
- Isso nos dá no máximo três opções para $\varphi(\begin{pmatrix}1 & 2\end{pmatrix})$ e no máximo duas para $\varphi(\begin{pmatrix}1 & 2 & 3\end{pmatrix})$. Ou seja, temos no máximo seis possibilidades para φ.
- Como $Z(S_3)$ é trivial e $\mathrm{Inn}(G) \cong G/Z(G)$, temos que $\mathrm{Inn}(S_3) \cong S_3$.
- Por fim,
$$6 = |S_3| = |\mathrm{Inn}(S_3)| \leq |\mathrm{Aut}(S_3)| \leq 6 \implies |\mathrm{Aut}(S_3)| = 6$$
- Logo, $\mathrm{Aut}(S_3)$ tem elementos de ordem um, dois e três.

Exercício 9

Questão: Seja G um p-grupo finito, onde p é primo, e $N \leq G$ tal que $[G : N] = p$. Demonstre que $N \lhd G$.

Resolução:

1. Listar classes laterais.
   - Seja X o conjunto de classes laterais de N em G.
   - Como $[G : N] = p$, temos
   $$X = \{g_1 N, g_2 N, \ldots, g_p N\}$$
2. Agir via produto.
   - Temos que G age sobre X à esquerda via produto:
   $$g(g_i * N) = (gg_i) * N$$
   - Assim, existe
   $$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Perm}(X) \\ g &\longmapsto \varphi(g) \end{aligned}$$
   - em que
   $$\begin{aligned} \varphi(g) : X &\longrightarrow X \\ g_i N &\longmapsto (gg_i) N \end{aligned}$$
3. Mostrar que $\varphi(g)$ é permutação e φ é homomorfismo (ver exercício 4).
4. Aplicar Teorema de Isomorfismos.
   - Pelo Teorema de Isomorfismos,
   $$\frac{G}{\ker(\varphi)} \cong \mathrm{im}(\varphi)$$
   - é um p-grupo.
5. Analisar ordem.
   - Note que
   $$|\mathrm{im}(\varphi)| \mid |\mathrm{Perm}(X)| = p!$$
   - Como $|\mathrm{im}(\varphi)|$ é potência de p, isso implica que $|\mathrm{im}(\varphi)| = p$.
   - Ou seja, $[G : \ker(\varphi)] = p$.
6. Mostrar que $N = \ker(\varphi)$.

- Tome $g \in \ker(\varphi)$.
- Então
$$gg_1\mathrm{N} = \varphi(g)(g_1\mathrm{N}) = g_1\mathrm{N}$$
- Note que podemos tomar um dos $g_i\mathrm{N}$ como sendo igual a N.
- Assim, tomamos, s.p.g, $g_1 = 1_\mathrm{G}$.
- Portanto,
$$g\mathrm{N} = \mathrm{N} \implies \ker(\varphi) \subseteq \mathrm{N}$$
- Por outro lado,
$$p = [\mathrm{G} : \ker(\varphi)] = [\mathrm{G} : \mathrm{N}][\mathrm{N} : \ker(\varphi)] = p[\mathrm{N} : \ker(\varphi)]$$
- O que implica que $[\mathrm{N} : \ker(\varphi)] = 1$ e, portanto, $\mathrm{N} = \ker(\varphi)$.
- Como N é núcleo de um homomorfismo, temos que $\mathrm{N} \lhd \mathrm{G}$.

Exercício 10

Questão: Seja G um p-grupo não abeliano de ordem p^3. Demonstre que $\mathrm{Z(G)} = \mathrm{G}'$.

Resolução:

- Como G é não abeliano, temos que $\mathrm{Z(G)} \neq \mathrm{G}$.
- E como G é p-grupo finito, temos que $\mathrm{Z(G)} \neq 1_\mathrm{G}$.
- Esses dois fatos implicam que $|\mathrm{G/Z(G)}| \notin \{1, p^3\}$.
- Mas
$$|\mathrm{G/Z(G)}| \mid |\mathrm{G}| \implies |\mathrm{G/Z(G)}| \in \{p, p^2\}$$
  - Se $|\mathrm{G/Z(G)}| = p$, então $\mathrm{G/Z(G)}$ é cíclico.
  - Assim, G é abeliano, o que contradiz nossa hipótese.
  - Portanto, $|\mathrm{G/Z(G)}| = p^2$.
- Isso implica que $\mathrm{G/Z(G)}$ é abeliano.
- Portanto, $1 \subseteq \mathrm{G}' \subseteq \mathrm{Z(G)}$.
- Note que $\mathrm{G}' = 1$ equivale a G ser abeliano.
- Assim,
$$|\mathrm{Z(G)}| = \frac{|\mathrm{G}|}{\left|\frac{\mathrm{G}}{\mathrm{Z(G)}}\right|} = \frac{p^3}{p^2} = p$$
- E
$$1 \neq |\mathrm{G}'| \mid |\mathrm{Z(G)}| = p \implies |\mathrm{G}'| = |\mathrm{Z(G)}|$$
- Logo, $\mathrm{G}' = \mathrm{Z(G)}$.

Exercício 11

Questão: Mostrar que A_4 é um grupo solúvel.

Resolução:

- Vamos mostrar que
$$1 \lhd \mathrm{V} \lhd \mathrm{A}_4$$
- em que:
  - V é o **grupo de Klein** dado por
$$\mathrm{V} = \{\begin{pmatrix}1\end{pmatrix}, \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\}$$
  - $\mathrm{A}_4/\mathrm{V} \cong \mathbb{Z}_3$.
  - $\mathrm{V} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
- Mostremos que $\mathrm{V} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ e que $\mathrm{V} \lhd \mathrm{S}_4$.
  - Observe que V é formado pelos elementos de S_4 que são produtos de 2-ciclos disjuntos e pela identidade.
  - Assim, $\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}$ e $\begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}$ geram V e como eles possuem ordem dois, segue que $\mathrm{V} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
  - Tomando $\sigma \in \mathrm{S}_4$ e $i, j, k, l \in \{1, 2, 3, 4\}$ temos
$$\sigma\begin{pmatrix}i & j\end{pmatrix}\begin{pmatrix}k & l\end{pmatrix}\sigma^{-1} = \sigma\begin{pmatrix}i & j\end{pmatrix}\sigma^{-1}\sigma\begin{pmatrix}k & l\end{pmatrix}\sigma^{-1} = \begin{pmatrix}\sigma(i) & \sigma(j)\end{pmatrix}\begin{pmatrix}\sigma(k) & \sigma(l)\end{pmatrix} \in \mathrm{V}$$

- Logo, $V \lhd S_4$ e, portanto, $V \lhd A_4$.
- Por fim, mostremos que $A_4/V \cong \mathbb{Z}_3$.
  - Note que
$$\left|\frac{A_4}{V}\right| = \frac{|A_4|}{|V|} = \frac{12}{4} = 3$$
  - Como 3 é primo, temos que A_4/V é cíclico, portanto abeliano, e de ordem 3.
  - Assim, como $V \lhd A_4$, V é solúvel (pois V é abeliano) e A_4/V é solúvel, temos que A_4 é solúvel.

Exercício 12

Questão: Seja G um grupo finito com $H \lhd G$, $|H| = n$, $[G : H] = m$ e $\mathrm{mdc}(n, m) = 1$. Mostre que H é o único subgrupo de G de ordem n e então H é subgrupo característico.

Resolução:

1. Aplicar Teorema de Isomorfismos.
   - Suponha, por contradição, que existe um outro subgrupo K de G tal que $|K| = n$.
   - Como $H \lhd G$, temos que G/H é grupo.
   - Considere a projeção canônica $\pi : G \longrightarrow G/H$.
   - Pelo Teorema de Isomorfismos,
$$\pi(K) = \frac{KH}{H} \cong \frac{K}{H \cap K}$$
2. Analisar a ordem de $\pi(K)$.
   - Note que
$$|\pi(K)| \mid |K| = n \quad \text{e} \quad |\pi(K)| \mid |G/H| = m$$
   - Mas $\mathrm{mdc}(n, m) = 1$ implica que $|\pi(K)| = 1$ e, com isso, $\pi(K) = 1_{G/H}$.
   - Ou seja, $\pi(K) \subseteq \ker(\pi) = H$.
   - Como $|K| = |H|$, segue que $K = H$.
3. Mostrar que H é subgrupo característico.
   - Considere $\varphi \in \mathrm{Aut}(G)$.
   - Aplicando φ a H temos que $|\varphi(H)| = |H|$.
   - Portanto, $\varphi(H) = H$ e H é subgrupo característico.

Exercício 13a

Questão: Seja G um grupo de ordem 30. Mostre que cada Sylow 3-subgrupo e Sylow 5-subgrupo de G é normal.

Resolução:

1. Análise prévia.
   - Pelo Teorema de Sylow,
$$n_3 \equiv 1 \mod 3, \quad n_3 \mid |G| = 30 \implies n_3 \mid 10 \implies n_3 \in \{1, 10\}$$
$$n_5 \equiv 1 \mod 5, \quad n_5 \mid |G| = 30 \implies n_3 \mid 6 \implies n_5 \in \{1, 6\}$$
2. Caso $n_3 = 10$ e $n_5 = 6$.
   - Neste caso,
$$\mathrm{Syl}_3(G) = \{P_1, \ldots, P_{10}\}, \quad \mathrm{Syl}_5(G) = \{Q_1, \ldots, Q_6\}, \quad |P_j| = 3,\ |Q_i| = 5$$
   - Como 3 é primo, $P_i \cap P_j = 1_G$ para $i \neq j$.
   - Analogamente, como 5 é primo, $Q_i \cap Q_j = 1_G$ para $i \neq j$.
   - Contemos os elementos de
$$\left(\dot{\bigcup_{1 \le i \le 10}} (P_i \setminus 1_G)\right) \dot{\bigcup} \left(\dot{\bigcup_{1 \le j \le 6}} (Q_j \setminus 1_G)\right)$$
   - Temos $2 \cdot 10$ elementos de ordem 3 e $6 \cdot 4$ elementos de ordem 5.
   - Mas $20 + 24 > 30 = |G|$, o que é impossível.
3. Caso $n_3 = 1$ e $n_5 = 6$.
   - Como P é o único 3-Sylow subgrupo de G, temos $P \lhd G$.

- E temos $\mathrm{Syl}_5(G) = \{Q_1, \ldots, Q_6\}$, com $|Q_i| = 5$.
- Assim, $PQ \lhd G$ e o produto é semi-direto.
- Como $\mathrm{mdc}(|P|, |Q|) = 1$, temos $P \cap Q = 1_G$ e, assim, $|PQ| = |P||Q|$.
- Definamos $T = PQ$. Assim, $|T| = 15$ e temos que $[G : T] = 2$ e, portanto, $T \lhd G$.
- Note que $Q \leq T \lhd G$ e $gQg^{-1} \subseteq T$ para todo $g \in G$.
- Mas $Q \in \mathrm{Syl}_5(G) = \{gQg^{-1} \mid g \in G\}$.
- Portanto,
$$Q_i \subseteq T \implies \mathrm{Syl}_5(G) = \mathrm{Syl}_5(T)$$
- Como
$$m_5 = |\mathrm{Syl}_5(T)|, \quad m_5 \mid |T|, \quad m_5 \equiv 1 \mod 5$$
- Temos que
$$6 = n_5 = m_5 \mid |T| = 15 \implies 6 \mid 15$$
- o que é uma contradição.

4. Caso $n_3 = 10$ e $n_5 = 1$.
   - Pela mesma conta do caso anterior, temos que este caso é impossível.
5. Logo, $n_3 = 1$ e $n_5 = 1$ e cada Sylow 3-subgrupo e Sylow 5-subgrupo de G é normal.

Exercício 13b

Questão: Seja G um grupo de ordem 30. Mostre que existe um subgrupo $N \lhd G$ tal que $[G : N] = 2$.

Resolução:

- Pela parte anterior, temos que $P \in \mathrm{Syl}_3(G)$ e $Q \in \mathrm{Syl}_5(G)$ são únicos.
- Como $P \lhd G$ e $Q \lhd G$, tomamos $N = PQ$.
- Usando que P e Q são cíclicos, $P \cong \mathbb{Z}_3$ e $Q \cong \mathbb{Z}_5$.
- E dado que $\mathrm{mdc}(|P|, |Q|) = 1$, temos $P \cap Q = 1$.
- Assim, pelo Teorema Chinês dos Restos, $N = P \times Q = \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$.
- Como $|N| = 15$, temos que $[G : N] = 2$ pelo Teorema de Lagrange.

Exercício 13c

Questão: Seja G um grupo de ordem 30. Classifique os grupos de ordem 30.

Resolução:

1. Escrever G como produto semi-direto.
   - Escrevemos $G = NS$ em que $S \in \mathrm{Syl}_2(G)$ e $S = \langle x \rangle$. Como $|S| = 2$, temos que $|x| = 2$.
   - Como $\mathrm{mdc}(|N|, |S|) = \mathrm{mdc}(15, 2) = 1$ (dos itens anteriores), temos que $N \cap S = 1_G$. E como $N \lhd G$, segue que $G = N \rtimes S$.
2. Caracterizar o produto semi-direto.
   - Consideremos o homomorfismo
$$\begin{aligned} \varphi : S &\longrightarrow \mathrm{Aut}(N) \\ x &\longmapsto \varphi(x) \end{aligned}$$
   - Em que
$$\begin{aligned} \varphi(x) : N &\longrightarrow N \\ g &\longmapsto xgx^{-1} \end{aligned}$$
   - Note que $x^2 = 1$ implica que $\varphi(x)^2 = \varphi(x^2) = \varphi(1_G) = \mathrm{id}_N$.
   - Queremos encontrar os elementos de $\mathrm{Aut}(\mathbb{Z}_{15})$ de ordem dois.
   - Se $|\varphi(x)| = 1$, então $\varphi(x) = \mathrm{id}_N$. Assim, $G = N \rtimes S = N \times S \cong \mathbb{Z}_{15} \times \mathbb{Z}_2 = \mathbb{Z}_{30}$.
   - Denotemos $\theta = \varphi(x)$. Se $|\theta| = 2$, então
$$\mathrm{Syl}_3(\mathbb{Z}_{15}) = \{\mathbb{Z}_3\}, \quad \mathrm{Syl}_5(\mathbb{Z}_{15}) = \{\mathbb{Z}_5\}$$
   - Assim, $\mathbb{Z}_{15} = \mathbb{Z}_3 \times \mathbb{Z}_5$ e $\theta(\mathbb{Z}_3) \in \mathrm{Syl}_3(\mathbb{Z}_{15})$. Isso implica que $\theta(\mathbb{Z}_3) = \mathbb{Z}_3$. Analogamente, temos que $\theta(\mathbb{Z}_5) = \mathbb{Z}_5$.
   - Consideremos as restrições $\theta_1 = \theta|_{\mathbb{Z}_3}$ e $\theta_2 = \theta|_{\mathbb{Z}_5}$. Assim, $\theta_1 \in \mathrm{Aut}(\mathbb{Z}_3)$ e $\theta_2 \in \mathrm{Aut}(\mathbb{Z}_5)$.

- Como $\mathbb{Z}_3$ é cíclico, $\mathbb{Z}_3 = \langle y \rangle = \{1, y, y^2\}$. Portanto, $\theta_1 = \mathrm{id}_{\mathbb{Z}_3}$ ou $\theta_1(y) = y^2$, em que $\theta_1 = \mathrm{id}_{\mathbb{Z}_3}$.
- E como $\mathbb{Z}_5$ é cíclico, $\mathbb{Z}_5 = \langle b \rangle = \{1, b, b^2, b^3, b^4\}$. Assim, $\theta_2 = \mathrm{id}_{\mathbb{Z}_5}$ ou $\theta_2(b) = b^i$, em que $\theta_2^2(b) = b^{i^2}$ e $1 \leq i \leq 4$.
- Dessa forma, temos que $|\theta_i| \in \{1, 2\}$, o que equivale a $|\theta| \in \{1, 2\}$.
- Como $b = \theta_2^2(b)$, $b^{i^2} = b \iff i^2 \equiv 1 \mod 5$. Portanto, $i \equiv \pm 1 \mod 5$. Assim, $i \equiv -1 \mod 5$.
- E temos que $\theta_1 = \mathrm{id}_{\mathbb{Z}_3}$ ou $\theta_1(y) = y^{-1}$ e $\theta_2 = \mathrm{id}_{\mathbb{Z}_5}$ ou $\theta_2(b) = b^{-1}$.

3. Listar possibilidades.
   - Com isso, temos as seguintes possibilidades:
     1. Se $\theta_1 = \mathrm{id}_{\mathbb{Z}_3}$ e $\theta_2 = \mathrm{id}_{\mathbb{Z}_5}$, então $\theta = \mathrm{id}$ e $\mathrm{G} = \mathbb{Z}_{30}$ é grupo abeliano.
     2. Se $\theta_1 = \mathrm{id}_{\mathbb{Z}_3}$ e $\theta_2 \neq \mathrm{id}_{\mathbb{Z}_5}$, então $\mathrm{Z(G)} = \mathbb{Z}_3$.
     3. Se $\theta_1 \neq \mathrm{id}_{\mathbb{Z}_3}$ e $\theta_2 = \mathrm{id}_{\mathbb{Z}_5}$, então $\mathrm{Z(G)} = \mathbb{Z}_5$.
     4. Se $\theta_1 \neq \mathrm{id}_{\mathbb{Z}_3}$ e $\theta_2 \neq \mathrm{id}_{\mathbb{Z}_5}$, então $\mathrm{Z(G)} \cap \mathbb{Z}_{15} = 1_{\mathrm{G}}$.
   - Note que nenhum dos quatro casos acima são isomorfos.

Exercício 14

Questão: Seja G um grupo de ordem 175 e P um Sylow 7-subgrupo de G. Mostre que $\mathrm{P} \subseteq \mathrm{Z(G)}$.

Resolução:

1. Aplicar Teorema de Sylow.
   - Note que $|\mathrm{G}| = 175 = 5^2 7$.
   - Pelo Teorema de Sylow, n_7, o número de Sylow 7-subgrupo de G é tal que

$$n_7 \equiv 1 \mod 7 \quad \text{e} \quad n_7 \mid 5^2 7$$

   - Assim, $n_7 \mid 5^2$ e $n_7 \in \{1, 5, 5^2\}$.
   - Temos que $n_7 = 1$ (pois $n_7 \equiv 1 \mod 7$).
   - Ou seja, existe um único $\mathrm{P} \in \mathrm{Syl}_7(\mathrm{G})$ e, portanto $\mathrm{P} \lhd \mathrm{G}$.
2. Mostrar que $\mathrm{P} \subseteq \mathrm{Z(G)}$.
   - Consideremos o homomorfismo

$$\begin{aligned} \varphi : \mathrm{G/P} &\longrightarrow \mathrm{Aut(P)} \\ g\mathrm{P} &\longmapsto \varphi(g\mathrm{P}) \end{aligned}$$

   - em que $\varphi(g\mathrm{P})$ é a conjugação com g à esquerda:

$$\begin{aligned} \varphi(g\mathrm{P}) : \mathrm{P} &\longrightarrow \mathrm{P} \\ h &\longmapsto ghg^{-1} \end{aligned}$$

   - Mostrar que φ é um homomorfismo bem-definido (ver exercício 4).
   - Como $|\mathrm{P}| = 7$ é cíclico, temos que existe $x \in \mathrm{P}$ tal que $\mathrm{P} = \langle x \rangle$.
   - Assim, todo automorfismo θ de P pode ser escrito como $\theta(x) = x^i$, com $i \in \{1, 2, 3, 4, 5, 6\}$.
   - Ou seja, $|\mathrm{Aut(P)}| = 6$.
   - Como $\mathrm{mdc}(|\mathrm{G/P}|, |\mathrm{Aut(P)}|) = \mathrm{mdc}(25, 6) = 1$, temos que $\varphi(g\mathrm{P}) = \mathrm{id}_{\mathrm{Aut(P)}}$.
   - Isto é, $ghg^{-1} = h$ para todo $h \in \mathrm{P}$ e $g \in \mathrm{G}$.
   - Logo, $\mathrm{P} \subseteq \mathrm{Z(G)}$.

Exercício 15a

Questão: Sejam p e q primos, $p < q$, e G um grupo de ordem pq. Mostre que se $(q-1)/p \notin \mathbb{Z}$, então G é cíclico.

Resolução:

1. Aplicar Teorema de Sylow para q.
   - Sabemos que

$$n_q \mid |\mathrm{G}| = pq \quad \text{e} \quad n_q \equiv 1 \mod q$$

   - Assim, $n_q \in \{1, p\}$ e q divide $n_q - 1$. Portanto, $n_q \neq p$.
   - Como $n_q = 1$, temos um único q-subgrupo de Sylow Q de G.
   - Portanto, $\mathrm{Q} \lhd \mathrm{G}$.

- Como $|Q| = q$ é primo, temos que $Q \cong \mathbb{Z}_q$.

2. Aplicar Teorema de Sylow para p.
   - Seja $P \in \mathrm{Syl}_p(G)$.
   - Como $|P| = p$, temos $P \cong \mathbb{Z}_p$.
3. Mostrar que o produto é semi-direto.
   - Note que $|P \cap Q|$ divide $|P|$ e Q. Portanto, $|P \cap Q| = 1$.
   - Como $Q \triangleleft G$ e $|QP| = pq = |G|$, temos $G = Q \rtimes P$.
4. Analisar produto semi-direto.
   - Observe que P age sobre Q permutando os elementos de $Q \setminus \{1_G\}$.
   - Como P e Q são cíclicos, escreva $P = \langle y \rangle$ e $Q = \langle x \rangle$.
   - Assim, $yxy^{-1} = x^i$ para algum $i \in \{1, 2, \dots, q-1\}$.
   - Como $y^p = 1_G$, temos que $x = y^p x y^{-p} = x^{i^p}$. Portanto, q divide $i^p - 1$.
   - Considere o grupo $\mathbb{Z}_q^*$, que sabemos ter ordem $q - 1$.
   - Como $q \mid i^p - 1$, temos que $i^p = 1$ em $\mathbb{Z}_q^*$.
   - Portanto, $|i| \mid p$. Mas p é primo e, assim, $|i| \in \{1, p\}$.
   - Caso $|i| = 1$, então $i = 1$ e G é abeliano. Neste caso, pelo Teorema Chinês dos Restos, $G \cong P \times Q$ é cíclico.
   - Caso $|i| = p$, então i gera um subgrupo de $\mathbb{Z}_q^*$ de ordem p. Portanto, $p \mid |\mathbb{Z}_q^*| = q - 1$, o que contradiz nosso enunciado.

Exercício 15b

Questão: Sejam p e q primos, $p < q$, e G um grupo de ordem pq. Mostre que se $(q-1)/p \in \mathbb{Z}$, então a menos de isomorfismo existe único G não abeliano.

Resolução:

1. Notar que existe subgrupo H de ordem p.
   - Se $(q-1)/p \in \mathbb{Z}$, então como $\mathbb{Z}_q^*$ é um grupo cíclico, existe um único $H \leq \mathbb{Z}_q^*$ de ordem p, que também é cíclico.
   - Suponha que $i_1, i_2 \in H$ com $|i_1| = p = |i_2|$. Então i_1 e i_2 são geradores de H.
2. Mostrar que $G_1 = Q \rtimes P$, com ação de P sobre Q dada por $yxy^{-1} = x^{i_1}$, e $G_2 = Q \rtimes P$, com ação dada por $yxy^{-1} = x^{i_2}$, são isomorfos.
   - Usando i_2 como gerador de H, temos que $i_1 = i_2^a$ para algum $a \in \{1, 2, \dots, p-1\}$, o que equivale a $i_1 \equiv (i_2)^a \mod q$.
   - Defina $\varphi : G_1 \longrightarrow G_2$ tal que $\varphi|_Q = \mathrm{id}_Q$ e $\varphi(y^j) = y^{ja}$.
   - Com isso,
   $$\varphi(x^i y^j) = x^i y^{aj}$$
   - Mostre que φ é homomorfismo de grupos.
     - Tomemos $0 \leq a_1, a_2 \leq q-1$ e $0 \leq b_1, b_2 \leq p-1$.
     - Temos o seguinte produto em G_1:
     $$\begin{aligned}(x^{a_1} y^{b_1})(x^{a_2} y^{b_2}) &= x^{a_1} y^{b_1} x^{a_2} y^{-b_1} y^{b_1+b_2} = x^{a_1} (y^{b_1} x y^{-b_1})^{a_2} y^{b_1+b_2} \\ &= x^{a_1} (x^{i_1^{b_1}})^{a_2} y^{b_1+b_2} = x^{a_1 + a_2 i_1^{b_1}} y^{b_1+b_2}\end{aligned}$$
     - Analogamente, em G_2:
     $$(x^{a_1} y^{b_1})(x^{a_2} y^{b_2}) = x^{a_1 + a_2 i_2^{b_1}} y^{b_1+b_2}$$
     - Assim, em G_1,
     $$\varphi((x^{a_1} y^{b_1})(x^{a_2} y^{a_2})) = \varphi(x^{a_1 + a_2 i_1^{b_1}} y^{b_1+b_2}) = x^{a_1 + a_2 i_1^{b_1}} y^{(b_1+b_2)a}$$
     - E em G_2,
     $$\begin{aligned}\varphi((x^{a_1} y^{b_1}))\varphi((x^{a_2} y^{b_2})) &= (x^{a_1} y^{ab_1})(x^{a_2} y^{ab_2}) = x^{a_1 + a_2 i_2^{ab_1}} y^{ab_1 + ab_2} \\ &= \varphi((x^{a_1} y^{b_1})(x^{a_2} y^{a_2}))\end{aligned}$$
     - pois $i_1 \equiv (i_2)^a \mod q$ implica que $x^{a_1 + a_2 i_2^{ab_1}} = x^{a_1 + a_2 i_1^{ab_1}}$ em Q.
   - Claramente, φ é bijetivo. Assim, φ é isomorfismo de grupos.

Exercício 16

Questão: Exiba os Sylow 7-subgrupos de S_{14}, justificando a sua resposta.

Resolução:

- Seja $P \in \mathrm{Syl}_7(S_{14})$.
- Como $|S_{14}| = 14!$, temos $|P| = 7^2 = p^2$, $p = 7$ primo, o que implica que P é abeliano.
- Da classificação de grupos abelianos finitos, temos duas possibilidades: ou $P = \mathbb{Z}_p \times \mathbb{Z}_p$ ou $P = \mathbb{Z}_{p^2}$.
- Escreva
$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} \quad \text{e} \quad b = \begin{pmatrix} 8 & 9 & 10 & 11 & 12 & 13 & 14 \end{pmatrix}$$
- Como $|a| = |b| = p$, temos que $\langle a, b\rangle$ é abeliano e, portanto, isomorfo a $\mathbb{Z}_7 \times \mathbb{Z}_7$.
- Como cada par de p-Sylow subgrupos são conjugados, temos que existe $\sigma \in S_{14}$ tal que
$$P = \langle \sigma a \sigma^{-1}, \sigma b \sigma^{-1}\rangle \in \mathrm{Syl}_7(S_{14}), \quad \langle a, b\rangle = \langle a\rangle \times \langle b\rangle, \quad ab = ba$$

Exercício 17a

Questão: Demonstre que os subgrupos de $Z_i(G)$ são característicos, i.e., invariantes sobre todos os automorfismos de G.

Resolução:

0. Procedemos por indução em i.
1. Para $i = 0$:
   - Temos que $Z_0(G) = 1_G$ e assim $\varphi(1_G) = 1_G \subseteq Z_0(G)$ para todo automorfismo φ de G.
2. Para $i = 1$:
   - Tomemos $\varphi \in \mathrm{Aut}(Z(G))$, $z \in Z(G)$ e $g \in G$.
   - Queremos mostrar que $\varphi(Z(G)) \subseteq Z(G)$, i.e., $\varphi(z)g = g\varphi(z)$
   - Como φ é automorfismo,
$$\varphi(z)g = \varphi(z)\varphi(\varphi^{-1}(g)) = \varphi(z\varphi^{-1}(g)) = \varphi(\varphi^{-1}(g)z) = \varphi(\varphi^{-1}(g))\varphi(z) = g\varphi(z)$$
   - Logo, $\varphi(Z(G)) = Z(G)$.
3. Passo indutivo: suponha que $Z_i(G)$ é característico.
   - Pela hipótese de indução, temos que se $\varphi(G) \in \mathrm{Aut}(G)$, então $\varphi(Z_i(G)) = Z_i(G)$.
   - Definimos $\tilde{\varphi} \in \mathrm{Aut}(G/Z_i(G))$ como $\tilde{\varphi}(gZ_i(G)) = \varphi(g)Z_i(G)$.
   - Mostrar que $\tilde{\varphi}$ é bem definido e é automorfismo.
   - Com isso,
$$\frac{\varphi(Z_{i+1}(G))}{Z_i(G)} = \tilde{\varphi}\left(Z\left(\frac{G}{Z_i(G)}\right)\right) = Z\left(\frac{G}{Z_i(G)}\right) = \frac{Z_{i+1}(G)}{Z_i(G)}$$
   - Logo,
$$\varphi(Z_{i+1}(G)) = Z_{i+1}(G)$$

Exercício 17b

Questão: Demonstre que os subgrupos $G^{(m)}$ são característicos.

Resolução:

0. Procedemos por indução em m.
1. Para $m = 1$:
   - Temos que $G^{(1)} = G'$.
   - Seja $[a, b] \in G'$ arbitrário.
   - Se $\varphi \in \mathrm{Aut}(G)$, então
$$\varphi([a, b]) = [\varphi(a),\ \varphi(b)]$$
   - Logo, pela arbitrariedade de $[a, b]$, temos que $\varphi(G') \subseteq G'$.
2. Passo indutivo: suponha que $G^{(m)}$ é subgrupo característico de G.
   - Note que $G^{(m+1)} = (G^{(m)})'$ é subgrupo característico de $G^{(m)}$, pelo caso $m = 1$.
   - Então, pelo Lema 3, como $G^{(m+1)}$ é subgrupo característico de $G^{(m)}$ e $G^{(m)}$ é subgrupo característico de G, então $G^{(m+1)}$ é subgrupo característico de G.

Exercício 18

Questão: Seja $G = \{A = (a_{ij}) \in M_n(\mathbb{R}) \mid a_{ij} = 0 \text{ se } i > j,\ a_{ij} = 1 \text{ se } i = j\}$. Demonstre que G é nilpotente.

Resolução:

- Ilustrando com $n = 4$:

$$Z_0(G) = 1_G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad Z_1(G) = Z(G) = \begin{pmatrix} 1 & 0 & 0 & * \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$Z_2(G) = \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad Z_3(G) = G = \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

  - Sabemos de Álgebra Linear que, se $A \in G$ então $A - I_n$ é nilpotente (onde $I_n = 1_G$ é a matriz identidade).
- Sabemos que G é nilpotente se, e somente se, existe uma cadeia

$$1_G = K_0 \leq K_1 \leq \cdots \leq K_m = G$$

- tal que $[K_{i+1}, G] \subseteq K_i$ para todo i.
- Defina

$$K_i = \{A \in G \mid (A - I_n)^{i+1} = 0_n\}$$

- Note que $K_0 = I_n$ e $K_{n-1} = G$.
- Mostrar que $K_i \lhd G$ para todo i.
  - Seja $A \in G$ e $B \in K_i$.

$$(ABA^{-1} - I_n)^{i+1} = (A(B - I_n)A^{-1})^{i+1} = A(B - I_n)^{i+1}A^{-1} = 0_n$$

  - Logo, $ABA^{-1} \in K_i$.
- Mostrar que $[K_{r+1}, G] \leq K_r$.
  - Observe que cada K_r é gerado pelas matrizes elementares $e_{ij}(\lambda)$ com $j \geq (n-r) + i$ e $\lambda \in \mathbb{R}$.
  - Assim, basta considerar os geradores $e_{ij}(\lambda)$ de K_{r+1}, em que $j \geq (n - (r+1)) + i$, e os geradores $e_{st}(\mu)$ de $K_{n-1} = G$, em que $j \geq 1 + i$.
  - Das relações de Steinberg (Lema 4), temos:

$$\begin{aligned} [e_{ij}(\lambda), e_{jr}(\mu)] &= e_{ir}(\lambda\mu), && \text{se } i \neq r \\ [e_{ij}(\lambda), e_{rs}(\mu)] &= I_n, && \text{se } i \neq s \text{ e } j \neq r \end{aligned}$$

  - Portanto,

$$[e_{ij}(\lambda), e_{st}(\mu)] = \begin{cases} e_{it}(\lambda\mu), & \text{se } j = s,\ i \neq t \\ I_n, & \text{se } j \neq s,\ i \neq t \end{cases}$$

  - Observe que isso nos dá justamente as matrizes que geram K_r. Logo, $[K_{r+1}, G] \leq K_r$.

Exercício 19

Questão: Seja $G = \{A = (a_{ij}) \in M_n(\mathbb{R}) \mid a_{ij} = 0 \text{ se } i > j\}$. Demonstre que G é solúvel.

Resolução:

- Ilustrando com $n = 4$:

$$G_4 = 1_G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad G_3 = \begin{pmatrix} 1 & 0 & 0 & * \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad G_2 = \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$G_1 = \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad G_0 = G = \begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix}$$

– Note que G/G_4 é isomorfo ao subgrupo das matrizes diagonais:

$$G/G_4 \cong \left\{ \begin{pmatrix} * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \end{pmatrix} \in M_4(\mathbb{R}) \right\} \cong \mathbb{R}^* \times \mathbb{R}^* \times \mathbb{R}^* \times \mathbb{R}^*$$

– Além disso, $G_1 \cong \mathbb{R}$ com a operação adição, $G_2/G_1 \cong \mathbb{R}^2$ também com a operação adição.

- Com isso, temos uma cadeia
$$1_G = G_1 \lhd \cdots \lhd G_1 \lhd G_0 = G$$

Questão 1a (P2 2021)

Questão: Enuncie o Teorema de Sylow.

Resolução:

0. Seja G um grupo finito e p primo tal que $p \mid |G|$.
1. Se $H \leq G$ tal que $|H|$ é potência de p, então existe $P \in \mathrm{Syl}_p(G)$ tal que $H \subseteq P$.
2. Cada par de p-subgrupos de Sylow de G são conjugados.
3. Se n_p é o número de p-subgrupos de Sylow de G, então $n_p \equiv 1 \mod p$ e $n_p \mid |G|$.

Questão 1b1 (P2 2021)

Questão: Seja G um grupo de ordem 68. Mostre que existe um único 17-Sylow subgrupo P de G. Descreva G como produto semidireto $G = PQ$ definindo o grupo Q. A quais grupos Q pode ser isomorfo?

Resolução:

1. Existe um único 17-Sylow subgrupo P de G.
   - Note que $68 = 2^2 \cdot 17$.
   - Pelo Teorema de Sylow,
   $$n_{17} \equiv 1 \mod 17 \quad \text{e} \quad n_{17} \mid 68 \implies n_{17} \mid 2^2$$
   - Assim, $n_{17} \in \{1, 2, 4\}$.
   - Mas $2 \not\equiv 1 \mod 17$ e $4 \not\equiv 1 \mod 17$. Portanto, $n_{17} = 1$.
   - Assim, só existe um 17-Sylow subgrupo de G, que denotaremos por P, e temos que $P \lhd G$.
   - Como P tem ordem prima, temos que P é cíclico e, assim, $P \cong \mathbb{Z}_{17}$.
2. Descreva G como produto semidireto $G = PQ$.
   - Seja $Q \in \mathrm{Syl}_2(G)$.
   - Note que $P \cap Q$ é trivial. De fato,
   $$g \in P \cap Q \implies |g| \mid |P| = 17 \quad \text{e} \quad |g| \mid |Q| = 4 \implies |g| = 1$$
   - Assim, o produto PQ é semidireto.
   - Além disso, $|Q||P| = 2^2 \cdot 17 = |G|$. Ou seja, $G = P \rtimes Q$.
3. A quais grupos Q pode ser isomorfo?
   - Se $n_2 = 1$, então $Q \lhd G$ e o produto $G = P \times Q$ é direto.
   - Nesse caso, ...
   - Se $n_2 = 17$, ...
   - Caso Q cíclico, então $Q \cong \mathbb{Z}_4$ ou $Q \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Questão 1b2 (P2 2021)

Questão: Mostre que G é solúvel.

Resolução: Como $|G| = p^2 q$ com p e q primos distintos, temos que G é solúvel.

Questão 1b3 (P2 2021)

Questão: Descrever todos os elementos de ordem w e os elementos de ordem 4 em $\mathrm{Aut}(\mathbb{Z}_{17})$.

Resolução:

- Queremos encontrar a ação de Q sobre $P \cong \mathbb{Z}_{17}$ por meio de conjugação:

$$\begin{aligned} \theta : Q &\longrightarrow \mathrm{Aut}(\mathbb{Z}_{17}) \\ q &\longmapsto \theta(q) \end{aligned}$$

Questão 1b4 (P2 2021)

Questão: Mostrar que se G não é abeliano, ele não é único a menos de isomorfismo.

Resolução:

Questão 2b (P2 2021)

Questão: Demonstrar que se p é primo, cada grupo G de ordem p^2 é abeliano.

Resolução:

- Pelo Teorema de Lagrange, como $Z(G) \leq G$, temos que $|Z(G)| \mid |G|$.
- Assim, $|Z(G)| \in \{1, p, p^2\}$.
- Como G é um p-grupo finito, temos que $Z(G) \neq 1_G$.
- Se $|Z(G)| = p$, então

$$|G/Z(G)| = [G : Z(G)] = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$$

- Assim, $G/Z(G)$ é cíclico e, portanto, G é abeliano (pelo Lema 2). Mas este caso implica que $Z(G) = G$, o que é uma contradição com as ordens de cada grupo.
- Logo, $|Z(G)| = p^2$, $Z(G) = G$ e G é abeliano.

Questão 3b (P2 2021)

Questão: Quais dos seguintes grupos são solúveis e quais são nilpotentes:

1. $\mathbb{Z}_5 \times \mathbb{Z}$.
2. A_5.
3. $S_3 \times \mathbb{Z}$.

Resolução:

1. Note que $\mathbb{Z}_5 \times \mathbb{Z}$ é abeliano, portanto é nilpotente e solúvel.
2. A_5 não é solúvel, logo não é nilpotente.
3. $S_3 \times \mathbb{Z}$.
   - Lembre que subgrupo de solúvel/nilpotente é solúvel/nilpotente.
   - Como $Z(S_3) = 1$, temos que S_3 não é nilpotente. Assim, $S_3 \times \mathbb{Z}$ não é nilpotente.
   - Porém, S_3 é solúvel com cadeia $1_G \lhd A_3 \lhd S_3$ e $S_3/A_3 \cong \mathbb{Z}_2$ e $A_3 \cong \mathbb{Z}_3$.
   - Assim, como $\mathbb{Z}$ é abeliano e, portanto solúvel, temos que $S_3 \times \mathbb{Z}$ é solúvel.

Questão 4b (P2 2021)

Questão: Sejam p um primo e G um p-grupo finito tal que G/G' é cíclico. Mostre que G é um grupo abeliano.

Resolução:

- Como G é um p-grupo finito, temos que G é nilpotente.
- Portanto, existe uma cadeia

$$1_G = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_n(G) = G$$

- em que $Z_{i+1}(G)/Z_i(G)$ é abeliano.
- Suponha, por contradição, que $n \geq 2$.
  - Temos que $G/Z_{n-1}(G)$ é abeliano.
  - Ou seja, $G' \leq Z_{n-1}(G)$.
  - Mas como G/G' é cíclico e $G/Z_{n-1}(G)$ é um quociente de G/G', temos que $G/Z_{n-1}(G)$ é cíclico.

- Por definição, Z_{n-1}/Z_{n-2} é o centro de G/Z_{n-2}.
- Além disso,

$$\frac{G}{Z_{n-1}} \cong \frac{G/Z_{n-2}}{Z_{n-1}/Z_{n-2}}$$

- Como G/Z_{n-2} quocientado pelo seu centro é cíclico, pelo Lema 2, G/Z_{n-2} é abeliano.
- Ou seja, $Z(G/Z_{n-2}) = G/Z_{n-2}$.
- Isso implica que $Z_{n-1} = G$, o que é absurdo.

- Logo, $n = 1$ e, assim, G é abeliano.

Questão 5a (P2 2021)

Questão: Verdadeiro ou falso: produto direto de grupo solúvel com grupo nilpotente é solúvel.

Resolução:

- Falso.
- Considere o produto direto $S \times P$ de um grupo solúvel, mas não nilpotente S (ex. S_3), com um grupo nilpotente P.
- Como todo subgrupo de nilpotente é nilpotente, temos que S é nilpotente, o que é absurdo.

Questão 5b (P2 2021)

Questão: Verdadeiro ou falso: se N é subgrupo normal em G com ambos G/N e N p-grupos finitos, então G é solúvel.

Resolução:

- Verdadeiro.
- Como G/N e N são p-grupos finitos, ambos são solúveis.
- Assim, $N \lhd G$, N e G/N solúveis implica que G é solúvel.

Questão 1b (P2 2020)

Questão: Escrever a definição de grupos solúveis e a definição de grupos nilpotentes.

Resolução:

1. Grupos solúveis.
   - Um grupo é dito **solúvel** se existe uma cadeia de subgrupos

$$1 = G_n \lhd \cdots \lhd G_{i+1} \lhd G_i \lhd \cdots \lhd G_1 \lhd G_0 = G$$

   - em que $G_{i+1} \lhd G_i$ e G_i/G_{i+1} é grupo abeliano.
   - Equivalentemente, podemos definir a partir de uma cadeia

$$1 = H_n \lhd \cdots H_1 \lhd H_0 = G$$

   - com $H_i = G^{(i)}$, H_i/H_{i+1} abeliano e H_i característico em G.
2. Grupos nilpotentes.
   - Um grupo é dito **nilpotente** se existe uma cadeia de subgrupos

$$1_G = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_i(G) \leq Z_{i+1} \leq \cdots \leq Z_n(G) = G$$

   - em que $Z_i(G) \lhd G$ e

$$Z\left(\frac{G}{Z_i(G)}\right) = \frac{Z_{i+1}(G)}{Z_i(G)}$$

   - Equivalentemente, podemos definir a partir de uma cadeia

$$1_G = K_0 \leq K_1 \leq \cdots \leq K_n = G$$

   - tal que $[K_{i+1}, G] \subseteq K_i$ para todo i.