**Lista facultativa - Exercícios difíceis**

(1) **Seja $p$ um primo e seja $q$ um primo que divide $p-1$. Mostre que o grupo simétrico $S_p$ contem um subgrupo de ordem $pq$.** [Dica: seja $P$ um $p$-Sylow de $S_p$, mostre que $|N_{S_p}(P)| = p(p-1)$.]

O número de $p$-cíclos em $S_p$ é $(p-1)!$ e cada um contem $p-1$ $p$-cíclos, segue que $n_p(S_p) = (p-1)!/(p-1) = (p-2)!$ logo se $P$ é um qualquer $p$-Sylow de $S_p$ temos $|N_{S_p}(P)| = p!/(p-2)! = p(p-1)$. Seja $x$ um elemento de $N_{S_p}(P)$ de ordem $q$, então $P\langle x\rangle \leq N_{S_p}(P) \leq S_p$ tem ordem $pq$.

(2) **Seja $n$ um inteiro positivo. Suponha que todo grupo de ordem $n$ é cíclico. Mostre que $n$ e $\varphi(n)$ são coprimos** (a volta também vale mas é mais difícil). [Dica: lembre-se que se $n = \prod_i p_i^{a_i}$ então

$$\varphi(n) = \prod_i p_i^{a_i-1}(p_i - 1).$$

Se $n$ e $\varphi(n)$ não são coprimos tem dois casos: $n$ é divisível por $p^2$ para algum primo $p$ (neste caso considere $C_p \times C_p$) ou existem dois divisores primos $p$ e $q$ de $n$ tais que $q$ divide $p-1$, aplique o exercício acima.]

Se $n$ é divisível por $p^2$ para algum primo $p$ então o grupo $C_p \times C_p \times C_{n/p^2}$ é não cíclico de ordem $n$ (por exemplo porque contem mais de um subgrupo de ordem $p$). Se $n$ é divisível por dois primos $p$ e $q$ com $q$ que divide $p-1$ então pelo exercício acima existe um grupo $H$ de ordem $pq$ contido em $S_p$. Observe que $H$ não é cíclico porque se fosse cíclico conteria um elemento de ordem $pq$, por outro lado $S_p$ não contem elementos de ordem $pq$ porque um tal elemento deveria conter na sua estrutura cíclica um $p$-cíclo e um $q$-cíclo, e não tem suficientes elementos para construir uma tal permutação. Segue que o grupo $H \times C_{n/pq}$ é não cíclico de ordem $n$.

(3) **Sejam $p$ um primo, $G$ um $p$-grupo finito e $H$ um subgrupo de $G$. Mostre que se $N_G(H) = H$ então $H = G$.**

Por indução sobre $n$ onde $|G| = p^n$. Se $n = 1$ então $H = \{1\}$ ou $H = G$ e $N_G(\{1\}) = G \neq \{1\}$, logo o resultado segue. Agora suponha $n > 1$. Se $N_G(H) = H$ e $H \neq G$ então seja $g \in Z(G)$ um elemento não trivial do centro de $G$ (existe sendo $G$ um $p$-grupo finito) e $N = \langle g\rangle \trianglelefteq G$. Observe que $HN \leq G$ sendo $N \trianglelefteq G$. Se $N \leq H$ então $N_{G/N}(H/N) = H/N$ (se $gN \in N_{G/N}(H/N)$ então $g \in N_G(H)$ logo $g \in H$), segue que $H/N = G/N$ por hipótese de indução e segue $H = G$. Se $N \not\leq H$ então $H$ está contido propriamente em $HN$ e $HN \leq N_G(H)$ sendo $N \leq Z(G)$, isso contradiz $N_G(H) = H$.

(4) **Sejam $p$ e $q$ dois primos distintos, e seja $G$ um grupo de ordem $p^m q$. Mostre que $G$ é solúvel**. [Dica: basta mostrar que $G$ não é simples (por quê?). Sejam $P_1$ e $P_2$ dois $p$-Sylow com $|P_1 \cap P_2|$ o máximo possível, mostre que $P_1 \cap P_2 = \{1\}$ supondo isso falso por contradição e mostrando que definidos $N_1 = N_{P_1}(P_1 \cap P_2)$ e $N_2 = N_{P_2}(P_1 \cap P_2)$ temos que $J = \langle N_1, N_2 \rangle$ (o subgrupo gerado por $N_1$ e $N_2$) não é um $p$-grupo (use o exercício anterior, que implica que $N_i \neq P_1 \cap P_2$ para $i = 1, 2$).]

Suponha de saber que um grupo $G$ de ordem $p^m q$ não pode ser simples. Mostraremos que um tal grupo é solúvel por indução sobre $m$. Seja $N$ um subgrupo normal de $G$ com $N \neq \{1\}$ e $N \neq G$. Então $|N|$ e $|G/N|$ têm a forma $p^k$ ou $p^k q$ para algum $k \leq m$. Sabemos que todo grupo de ordem $p^k$ é solúvel (para qualquer $k$), e todo grupo de ordem $p^k q$ com $k < m$ é solúvel por hipótese de indução. Sendo $|N| < |G|$ e $|G/N| < |G|$ segue que $N$ e $G/N$ são solúveis, logo $G$ é solúvel também.

Mostraremos agora que um grupo $G$ de ordem $p^m q$ não é simples. Suponha por contradição $G$ simples, daí existem pelo menos dois $p$-Sylow distintos de $G$. Sejam $P_1, P_2$ dois $p$-Sylow distintos de $G$ com $|P_1 \cap P_2|$ o máximo possível. Mostraremos que $P_1 \cap P_2 = \{1\}$. Sejam $N_i = N_{P_i}(P_1 \cap P_2)$ para $i = 1, 2$, e seja $J := \langle N_1, N_2 \rangle$ o subgrupo de $G$ gerado por $N_1$ e $N_2$. Mostraremos que $J$ não é um $p$-grupo. Suponha que $J$ seja um $p$-grupo por contradição, e seja $P$ um $p$-Sylow de $G$ contendo $J$. Observe que $P \cap P_1$ contem $N_1$, e $N_1 \neq P_1 \cap P_2$ pelo exercício anterior. Mas como $N_1$ contem $P_1 \cap P_2$ deduzimos que $|P \cap P_1| > |P_1 \cap P_2|$, e isso contradiz a maximalidade de $|P_1 \cap P_2|$. Segue que $J$ não é um $p$-grupo, logo contem um $q$-Sylow $Q$. A ação de $G$ no conjunto dos conjugados de $P_1$ é transitiva, e $G = QP_1$, logo a ação de $Q$ também é transitiva (se $P$ é um conjugado de $P_1$ em $G$ então $P = gP_1g^{-1}$ e escrevendo $g = xy$ com $x \in Q$ e $y \in P_1$ obtemos $gP_1g^{-1} = xP_1x^{-1}$). Como $Q \leq J$, $Q$ normaliza $P_1 \cap P_2$, logo

$$P_1 \cap P_2 = \bigcap_{x \in Q} x(P_1 \cap P_2)x^{-1} \leq \bigcap_{x \in Q} xP_1x^{-1} = \bigcap_{g \in G} gP_1g^{-1} = (P_1)_G.$$

Mas $(P_1)_G = \{1\}$ sendo $G$ simples, logo $P_1 \cap P_2 = \{1\}$. Isso mostra que a interseção de dois $p$-Sylow quaisquer é trivial, logo $G$ contem $q(p^m - 1) = |G| - q$ elementos de ordem uma potência de $p$ maior que 1. Segue que tem espaço para um único $q$-Sylow que então é normal em $G$, contradição.

(5) **Sejam $p < q < r$ três primos e seja $G$ um grupo de ordem $pqr$. Mostre que $n_r(G) = 1$.** [Dica: suponha $n_r \neq 1$ por contradição, mostre que $n_r = pq$, mostre que $n_q = 1$ (mostre que se $n_q \neq 1$ então $n_q \geq r$, e conte os elementos), dado um $q$-Sylow $Q$ e um $r$-Sylow $R$ mostre que $RQ/Q \trianglelefteq G/Q$, deduza que $RQ$ contem todos os $r$-Sylow de $G$.]

Suponha $n_r > 1$ por contradição. Como os divisores de $pq$ são 1, $p$, $q$ e $pq$, e $p, q < r$, pelo teorema de Sylow $n_r(G) = pq$. Mostraremos que $n_q(G) = 1$. Se $n_q(G) > 1$ então como os divisores de $pr$ são 1, $p$, $r$, $pr$ e $p < q$ obtemos $n_q(G) \in \{r, pr\}$ logo em todo caso $n_q(G) \geq r$. Segue que $G$ contem $(r-1)pq$ elementos de ordem $r$ e pelo menos $(q-1)r$ elementos de ordem $q$, dando pelo menos $(r-1)pq+(q-1)r = |G|-pq+qr-r > |G|$ elementos, uma contradição. Segue que $n_q(G) = 1$. Seja $Q$ o único $q$-Sylow de $G$ e seja $R$ um $r$-Sylow de $G$. Como $Q \trianglelefteq G$ podemos considerar o quociente $G/Q$. Observe que $|G/Q| = pqr/q = pr$ e $|RQ/Q| = |R/R \cap Q| = |R| = r$ logo $RQ/Q$ é um $r$-Sylow de $G/Q$. Mas $G/Q$ tem ordem $pr$, logo $n_r(G/Q) = 1$ pelo teorema de Sylow (sendo $p < r$), segue que $RQ/Q \trianglelefteq G/Q$ logo $RQ \trianglelefteq G$. Segue que $RQ$ é um subgrupo normal de $G$ contendo um $r$-Sylow, logo pelo teorema de Sylow $RQ$ contem todos os $r$-Sylow de $G$. Segue que $n_r(G) = n_r(RQ) \in \{1, q\}$ pelo teorema de Sylow, e isso contradiz $n_r(G) = pq$.

(6) **Mostre que $S_5$ contem exatamente 5 subgrupos de indice 5.**

Seja $H$ um subgrupo de $S_5$ de indice 5, assim $|H| = 24$. Observe que o 4-cíclo $\sigma = (1234)$ está contido em um 2-Sylow $P$ de $S_5$ (pelo teorema de Sylow) e como os 2-Sylow de $H$ são 2-Sylow de $S_5$ (porque 8 divide $|H|$) existe $g \in S_5$ com $gPg^{-1} \leq H$ (pelo teorema de Sylow). Segue que $g\sigma g^{-1}$ é um 4-cíclo contido em $H$, logo $H$ admite uma órbita $O$ em $X = \{1, 2, 3, 4, 5\}$ de tamanho maior ou igual a 4. Por outro lado $H$ não é transitivo sobre $X$ porque a sua ordem não é divisível por 5, logo $H$ está contido no estabilizador do único elemento de $X$ fora de $O$. Por outro lado tal estabilizador tem ordem 24 logo é igual a $H$. Isso mostra que $H$ é exatamente igual a um dos cinco estabilizadores.

(7) **Encontre todos os grupos com exatamente 3 classes de conjugação**.

Sejam $x_1$, $x_2$, $x_3$ representantes das classes de conjugação de $G$ e sejam $c_i = |C_G(x_i)|$ e suponha $c_1 \leq c_2 \leq c_3 = n = |G|$. A equação das classes pode ser escrita

$$1 = 1/c_1 + 1/c_2 + 1/n.$$

Obtemos $1 \leq 3/c_1$ logo $c_1 \leq 3$. Não pode ser $c_1 = 1$, e se $c_3 = 3$ então $(c_1, c_2, c_3) = (3, 3, 3)$. Agora suponha $c_1 = 2$. Temos $1 = 1/2+1/c_2+1/n$ logo $1/2 = 1/c_2 + 1/n \leq 2/c_2$ então $3 \leq c_2 \leq 4$. Segue que $(c_1, c_2, c_3) = (2, 3, 6), (2, 4, 4)$. Mas $(2, 4, 4)$ pode ser excluido porque todo grupo de ordem 4 é abeliano. Segue que um grupo $G$ com exatamente três classes de conjugação tem ordem 3, no qual caso $G \cong C_3$, ou tem ordem 6, no qual caso $G \cong S_3$ (lembrando que os grupos de ordem 6 são $C_6$ e $S_3$).

(8) **Encontre todos os grupos com exatamente** $4$ **classes de conjugação**.

Sejam $x_1$, $x_2$, $x_3$, $x_4$ representantes das classes de conjugação de $G$ e sejam $c_i = |C_G(x_i)|$ e suponha $c_1 \leq c_2 \leq c_3 \leq c_4 = n = |G|$. A equação das classes pode ser escrita

$$1 = 1/c_1 + 1/c_2 + 1/c_3 + 1/n.$$

Obtemos $1 \leq 4/c_1$ logo $c_1 \leq 4$. Não pode ser $c_1 = 1$ (a única classe com um elemento corresponde à parcela $1/n$), logo $c_1 \in \{2, 3, 4\}$.

- Suponha $c_1 = 2$. Temos
  $$1/2 = 1/c_2 + 1/c_3 + 1/n \leq 3/c_2$$
  logo $3 \leq c_2 \leq 6$ (não podendo ser $c_2 = 2$).
  - Se $c_2 = 3$ então $1/6 = 1/c_3 + 1/n \leq 2/c_3$ logo $7 \leq c_3 \leq 12$, logo $(c_3, n) = (7, 42), (8, 24), (9, 18), (10, 15), (12, 12)$. como $c_3$ divide $n$ o caso $(10, 15)$ não acontece.
  - Se $c_2 = 4$ então $1/4 = 1/c_3 + 1/n \leq 2/c_3$ logo $5 \leq c_3 \leq 8$, logo $(c_3, n) = (5, 20), (6, 12), (8, 8)$.
  - Se $c_2 = 5$ então $3/10 = 1/c_3 + 1/n \leq 2/c_3$ logo $5 = c_2 \leq c_3 \leq 6$, logo $(c_3, n) = (5, 10)$.
  - Se $c_2 = 6$ então $1/3 = 1/c_3 + 1/n \leq 2/c_3$ logo $c_3 = 6$ (sendo $c_3 \geq c_2$) e $(c_3, n) = (6, 6)$.
- Suponha $c_1 = 3$. Temos
  $$2/3 = 1/c_2 + 1/c_3 + 1/n \leq 3/c_2$$
  logo $3 = c_1 \leq c_2 \leq 4$ ou seja $c_2 \in \{3, 4\}$.
  - Se $c_2 = 3$ então $1/3 = 1/c_3 + 1/n \leq 2/c_3$ logo $4 \leq c_3 \leq 6$, logo $(c_3, n) = (4, 12), (6, 6)$.
  - Se $c_2 = 4$ então $5/12 = 1/c_3 + 1/n \leq 2/c_3$ logo $c_3 = 4$ e $(c_3, n) = (4, 6)$ que não é possível porque $4$ não divide $6$.
- Suponha $c_1 = 4$. Sendo $c_1 \leq c_2 \leq c_3 \leq n$ obtemos $(c_1, c_2, c_3, n) = (4, 4, 4, 4)$.

Segue que as únicas possibilidades para $(c_1, c_2, c_3, n)$ são $(2, 3, 7, 42)$, $(2, 3, 8, 24)$, $(2, 3, 9, 18)$, $(2, 3, 12, 12)$, $(2, 4, 5, 20)$, $(2, 4, 6, 12)$, $(2, 4, 8, 8)$, $(2, 5, 5, 10)$, $(2, 6, 6, 6)$, $(3, 3, 4, 12)$, $(3, 3, 6, 6)$, $(4, 4, 4, 4)$.

Se $n = 6$ já sabemos que $G$ tem $3$ ou $6$ classes de conjugação, isso elimina $(2, 6, 6, 6)$ e $(3, 3, 6, 6)$.

Observe que em geral se $X$ é um grupo finito cuja ordem é divisível por $p^2$ onde $p$ é um primo então $|C_X(x)| \neq p$ para todo $x \in X$. De fato se $|C_X(x)| = p$ então sendo $x \in C_X(x)$ temos $C_X(x) = \langle x \rangle$ e $x$ tem ordem $p$, seja $P$ um $p$-Sylow de $G$ contendo $x$. Seja $z$ um elemento não trivial do centro $Z(P)$ de $P$. Como $z \in C_X(x)$ e $|C_X(x)| = p$ segue que $x \in C_X(x) = \langle z \rangle \leq Z(P)$, daí $P \leq C_X(x)$ e isso contradiz o fato que $p^2$ divide $|P|$.

Isso elimina os casos $(2,3,8,24)$, $(2,3,9,18)$, $(2,3,12,12)$, $(2,4,5,20)$, $(2,4,6,12)$, $(2,4,8,8)$.

O caso $(2,3,7,42)$: Como $|G| = 2 \cdot 21$, sabemos que existe $N \trianglelefteq G$ de índice 2, ou seja ordem 21. Seja $x \in G$ de ordem 2. Como $|C_G(x)| = 2$, o elemento $x$ tem $|G : C_G(x)| = 21$ conjugados em $G$, em particular $G$ contem pelo menos 21 elementos de ordem 2. Por outro lado nenhum elemento de $N$ tem ordem 2, e $|N| = 21 = |G - N|$, isso implica que os elementos de ordem 2 são os elementos de $G - N = \{xn \ : \ n \in N\}$. Segue que $xn$ tem ordem 2 para todo $n \in N$, ou seja $xnxn = 1$, ou seja $xnx^{-1} = n^{-1}$ (sendo $x^{-1} = x$). Mas então se $n, m \in N$ temos por um lado $xnmx^{-1} = (nm)^{-1} = m^{-1}n^{-1}$ e por outro lado $xnmx^{-1} = xnx^{-1} \cdot xmx^{-1} = n^{-1}m^{-1}$. Segue que $m^{-1}n^{-1} = n^{-1}m^{-1}$, que pode ser escrito $nm = mn$. Isso mostra que $N$ é abeliano, logo está contido no centralizador dos seus elementos, e contradiz o fato que existem centralizadores de ordem 3 e 7 (lembrando que $N$ contem todos os elementos de ordem 3 e 7).

Segue que as únicas possibilidades são

$$(2,5,5,10), \ (3,3,4,12), \ (4,4,4,4).$$

- No caso $(2,5,5,10)$ seja $P$ um 2-Sylow, então $|G : P| = 5$ e $G$ não é abeliano, segue que a representação permutacional $G \to S_5$ é injetiva sendo $P_G = \{1\}$ (se fosse $P_G = P$ sendo $|P| = 2$ o gerador de $P$ pertenceria ao centro de $G$ logo teria centralizador de ordem 10). Além disso $G$ contem um 5-Sylow normal logo $G$ está contido no normalizador de um 5-Sylow de $S_5$, que podemos escolher como sendo o normalizador de $Q = \langle (12345) \rangle$. Observe que $S_5$ contem 4! 5-cíclos logo $n_5(S_5) = 4!/4 = 6$ logo $|N_{S_5}(Q)| = 5!/6 = 20$. $N_{S_5}(Q)$ contem um único subgrupo de ordem 10, que é a sua interseção com $A_5$. Trata-se do grupo diedral $D_{10}$, segue que $G \cong D_{10}$.
- No caso $(3,3,4,12)$ seja $P$ um 3-Sylow de $G$, temos $|G : P| = 4$, considere a representação permutacional associada $G \to S_4$ com núcleo $P_G$. Observe que $P$ não é normal em $G$ porque $G$ tem duas classes de elementos de ordem 3, cada uma com quatro elementos, logo $G$ contem $4+4 = 8$ elementos de ordem 3. Segue que $P_G = \{1\}$ logo $G \to S_4$ é injetiva e $G$ é isomorfo a um subgrupo de $S_4$ de ordem 12, logo $G \cong A_4$.
- O caso $(4,4,4,4)$ corresponde aos grupos abelianos $C_4$ e $C_2 \times C_2$.

Segue que os únicos grupos finitos com exatamente 4 classes de conjugação são $C_4$, $C_2 \times C_2$, $A_4$ e $D_{10}$.