Resolução da Prova Substitutiva

1. Seja G um grupo, sejam $a, b \in G$, e seja k um inteiro não nulo. Demonstre as implicações a seguir.

   (a) Se a tem ordem finita igual a r, então a^k tem ordem igual a $\dfrac{r}{\text{mdc}(k,r)}$.

   (b) Se a tem ordem infinita, então a^k tem ordem infinita.

   (c) Se a tem ordem finita igual a r, b tem ordem finita igual a s, $\text{mdc}(r,s) = 1$ e $ab = ba$, então ab tem ordem rs.

Solução. (a) Seja $d = \text{mdc}(k,r)$. Então $d > 0$ e existem $k', r' \in \mathbb{Z}$ tais que $k = dk', r = dr'$ e $\text{mdc}(k', r') = 1$. Como $r > 0$ e $d > 0$, segue $r' > 0$. Mostremos que a^k tem ordem r'. Como $(a^k)^{r'} = a^{dk'r'} = (a^r)^{k'} = (e_G)^{k'} = e_G$, segue que a^k tem ordem finita e $t := \text{o}(a^k) \leq r'$. Por outro lado, $e_G = (a^k)^t = a^{kt}$ e, portanto, $a^{|k|t} = e_G$. Assim, $dr' = r = \text{o}(a)$ divide $|k|t = d|k'|t$. Isso implica que r' divide $|k'|t$. Mas $\text{mdc}(|k'|, r') = \text{mdc}(k', r') = 1$ e, portanto, r' tem que dividir t. Logo $r' \leq t$. Conclui-se que $t = r'$. (b) Se a^k tivesse ordem finita, digamos, igual a t, teríamos $a^{kt} = (a^k)^t = e_G$. Assim, $a^{|k|t} = e_G$, e a teria ordem finita. (c) Por um lado, $(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = (e_G)^s(e_G)^r = e_G$ (a primeira igualdade segue de $ab = ba$). Logo, $t := \text{o}(ab) \leq rs$. Por outro lado, como $ab = ba$, temos $a^t b^t = (ab)^t = e_G$. Isso implica $a^t = b^{-t} \in H := \langle a \rangle \cap \langle b \rangle$. Como H é um subgrupo de $\langle a \rangle$, que, por sua vez, é um grupo finito com $|\langle a \rangle| = \text{o}(a) = r$, segue, do Teorema de Lagrange que $|H|$ divide r. Por um argumento análogo, $|H|$ também divide s, e, portanto, $|H|$ divide $\text{mdc}(r,s) = 1$. Logo, $H = \{e_G\}$. Assim, $a^t = e_G$ e $b^t = (b^{-t})^{-1} = (e_G)^{-1} = e_G$. Ou seja, temos $r = \text{o}(a)$ e $s = \text{o}(b)$, ambos, dividindo t. Como $\text{mdc}(r,s) = 1$, segue que rs divide t e, assim, $rs \leq t$. Logo $t = rs$.

2. Seja n um inteiro maior do que um. Considere o grupo simétrico S_n. Para cada $i = 1, \ldots, n$, defina o seguinte subconjunto de S_n:

$$X_i = \{\sigma \in S_n : \sigma(i) = i\}.$$

   (a) Mostre que, para cada $i = 1, \ldots, n$, X_i é um subgrupo de S_n.

   (b) Mostre que, para cada $i = 1, \ldots, n$, tem-se $[S_n : X_i] = n$.

Solução. Fixe $i \in \{1, \ldots, n\}$. (a) $e_{S_n} = \text{id} \in X_i$, pois $\text{id}(i) = i$; se $\sigma, \tau \in X_i$, então $(\sigma\tau)(i) = \sigma(\tau(i)) = \sigma(i) = i$, logo, $\sigma\tau \in X_i$; se $\sigma \in X_i$, então $\sigma(i) = i$ e, portanto, $\sigma^{-1}(i) = \sigma^{-1}(\sigma(i)) = \text{id}(i) = i$, logo $\sigma^{-1} \in X_i$. Segue que X_i é, de fato, um subgrupo de S_n. (b) Seja $\mathcal{C}$ o conjunto das classes laterais à esquerda de X_i em S_n. Então, a função

$$\begin{array}{rcl} f : \mathcal{C} & \longrightarrow & \{1, \ldots, n\} \\ \sigma X_i & \longmapsto & \sigma(i) \end{array}$$

está bem definida e é injetora, pois, para todos $\sigma, \tau \in S_n$, temos $\sigma X_i = \tau X_i \Leftrightarrow \tau^{-1}\sigma \in X_i \Leftrightarrow (\tau^{-1}\sigma)(i) = i \Leftrightarrow \sigma(i) = \tau(i)$. Além disso, f é também sobrejetora, pois, dado $j \in \{1, \ldots, n\}$, a permutação

$$\sigma = \begin{cases} \mathrm{id} & \text{se } i = j \\ (i\ j) & \text{se } i \neq j \end{cases}$$

satisfaz $f(\sigma X_i) = \sigma(i) = j$. Logo, $[S_n : X_i] = |\mathcal{C}| = |\{1, \ldots, n\}| = n$.

3. Seja G um grupo e sejam H, K subgrupos normais de G. Considere a função

$$\varphi \colon G \longrightarrow \frac{G}{H} \times \frac{G}{K}$$

definida por $\varphi(a) = (aH, aK)$, para todo $a \in G$.

   (a) Mostre que φ é um homomorfismo.

   (b) Descreva o núcleo de φ em termos dos subgrupos H e K.

   (c) Suponha que H e K tenham, ambos, índice finito em G. Mostre que se $\mathrm{mdc}([G : H], [G : K]) = 1$, então φ é sobrejetora e $[G : H \cap K] = [G : H][G : K]$.

Solução. (a) φ é um homomorfismo, pois, para todos $a, b \in G$, temos $\varphi(ab) = (abH, abK) = \big((aH)(bH), (aK)(bK)\big) = (aH, aK)(bH, bK) = \varphi(a)\varphi(b)$. (b) Dado $a \in G$, temos $a \in \ker\varphi \Leftrightarrow (aH, aK) = \varphi(a) = e_{G/H \times G/K} = (e_{G/H}, e_{G/K}) = (H, K) \Leftrightarrow aH = H$ e $aK = K \Leftrightarrow a \in H \cap K$. Logo, $\ker\varphi = H \cap K$. (c) Sejam $r = [G : H]$ e $s = [G : K]$. Como $\mathrm{mdc}(r, s) = 1$, existem $m, n \in \mathbb{Z}$ tais que $rm + sn = 1$. Assim, dado $a \in G$, $aH = (aH)^{rm+sn} = \big((aH)^r\big)^m (a^{sn}H) \overset{*}{=} (H)^m(a^{sn}H) = (e_{G/H})^m a^{sn}H = a^{sn}H$ (a igualdade $*$ segue do fato de $aH \in G/H$, que é um grupo de ordem $[G : H] = r$). Assim $\varphi(a^{sn}) = (a^{sn}H, a^{sn}K) = \big(aH, ((aK)^s)^n\big) = (aH, K)$, uma vez que $aK \in G/K$, que é um grupo de ordem $[G : K] = s$. De modo análgo, dado $b \in G$, mostra-se que $bK = b^{rm}K$ e, portanto, $\varphi(b^{rm}) = (H, bK)$. Logo, dados $a, b \in G$, temos $\varphi(a^{sn}b^{rm}) = \varphi(a^{sn})\varphi(b^{rm}) = (aH, K)(H, bK) = (aH, bK)$. Logo, φ é sobrejetora e, pelo primeiro teorema do isomorfismo,

$$\frac{G}{H \cap K} = \frac{G}{\ker\varphi} \cong \mathrm{Im}\,\varphi = \frac{G}{H} \times \frac{G}{K}.$$

Portanto, $[G : H \cap K] = \left|\dfrac{G}{H \cap K}\right| = \left|\dfrac{G}{H} \times \dfrac{G}{K}\right| = \left|\dfrac{G}{H}\right| \left|\dfrac{G}{K}\right| = [G : H][G : K]$.

4. Seja G um grupo finito e seja H um subgrupo de G tal que $[G : H] = p$, em que p é o menor primo que divide a ordem de G. Mostre que H é um subgrupo normal de G.

   (*Sugestão:* Mostre que H coincide com o núcleo de um homomorfismo de domínio G, definido por uma ação adequada de G em um conjunto.)

Solução. Seja $X = \{aH : a \in G\}$. Então, G age em X por translação:

$$\begin{array}{rcl} \varphi \colon G & \longrightarrow & S(X) \\ g & \longmapsto & \varphi_g \colon X \to X \\ & & \quad aH \mapsto gaH \end{array}$$

O homomorfismo φ satisfaz $\ker\varphi \subseteq H$, uma vez que se $g \in \ker\varphi$, então $gaH = \varphi_g(aH) = \varphi(g)(aH) = \mathrm{id}(aH) = aH$, para todo $a \in G$; em particular, tomando $a = e_G$, segue $gH = H$. Mostremos que $H = \ker\varphi$. Pelo primeiro teorema do isomorfismo, temos $\dfrac{G}{\ker\varphi} \cong \mathrm{Im}\,\varphi \leq S(X) \cong S_p$, uma vez que $|X| = [G : H] = p$. Portanto, $r := [G : \ker\varphi] = \left|\dfrac{G}{\ker\varphi}\right|$ divide $|S_p| = p!$, digamos, $p! = rn$. Por outro lado, $r = [G : \ker\varphi] = [G : H][H : \ker\varphi] = pt$, onde $t := [H : \ker\varphi]$. Nosso objetivo é mostrar que $t = 1$. Temos: $p! = rn = ptn$ e, portanto, $tn = (p-1)!$. Se $t \neq 1$, existiria um primo q tal que $q \mid t$. Como t divide $|H|$ (pois $t = [H : \ker\varphi]$), e $|H|$ divide $|G|$, teríamos $q \mid |G|$. Mas $t \mid (p-1)!$, o que implicaria $q \mid (p-1)!$, e, portanto, $q < p$, uma contradição com a escolha de p. Logo $[H : \ker\varphi] = 1$, e, portanto, $H = \ker\varphi$, que é normal em G.