Resolução da Prova 1

1. Considere o grupo $\mathrm{GL}_2(\mathbb{Z}_2)$, formado por todas as matrizes 2×2 inversíveis com entradas no corpo $\mathbb{Z}_2$.

   (a) Mostre que $|\mathrm{GL}_2(\mathbb{Z}_2)| = 6$.

   (b) Liste todos os elementos de $\mathrm{GL}_2(\mathbb{Z}_2)$ e encontre suas ordens.

   (c) Mostre que $\mathrm{GL}_2(\mathbb{Z}_2)$ não é abeliano.

   (d) Exiba um conjunto gerador de $\mathrm{GL}_2(\mathbb{Z}_2)$ contendo 2 elementos.

   (e) Este grupo lembra algum grupo que você conhece? Qual? Por quê?

Solução. (a) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_2) \iff ad - bc \neq 0 \iff ad + bc = 1$

$$\iff \begin{cases} ad = 1 \text{ e } bc = 0 \\ ad = 0 \text{ e } bc = 1 \end{cases} \iff \begin{cases} a = d = 1 \text{ e } \begin{cases} b = c = 0 \\ b = 1 \text{ e } c = 0 \\ b = 0 \text{ e } c = 1 \end{cases} \\ b = c = 1 \text{ e } \begin{cases} a = d = 0 \\ a = 1 \text{ e } d = 0 \\ a = 0 \text{ e } d = 1 \end{cases} \end{cases}$$

. Logo, $|\mathrm{GL}_2(\mathbb{Z}_2)| = 6$.

(b) Os elementos de $\mathrm{GL}_2(\mathbb{Z}_2)$ são, portanto,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, E = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Temos $A^2 = B^2 = C^2 = I, D^2 = E, E^2 = D$. Assim, $D^3 = ED = I$ e $E^3 = DE = I$. Logo, I tem ordem 1; A, B, C têm ordem 2; D, E têm ordem 3. (c) Como, por exemplo, $AD = C$ e $DA = B$, segue que $\mathrm{GL}_2(\mathbb{Z}_2)$ não é abeliano. (d) $\mathrm{GL}_2(\mathbb{Z}_2) = \langle A, D \rangle$, por exemplo, pois $I = A^2, B = DA, C = AD$ e $E = D^2$. (Há outras escolhas de geradores.) (e) $\mathrm{GL}_2(\mathbb{Z}_2)$ lembra D_3, pois

$$\mathrm{GL}_2(\mathbb{Z}_2) = \langle D, A \rangle, \text{ com } D^3 = A^2 = I, AD = D^2A, \text{ e}$$
$$D_3 = \langle \sigma, \tau \rangle, \text{ com } \sigma^3 = \tau^2 = \mathrm{id}, \tau\sigma = \sigma^2\tau$$

(Outra possibilidade de justificativa poderia ser dizer que ambos têm ordem 6, não são abelianos e são gerados por 2 elementos, por exemplo.)

2. Seja G um grupo abeliano finito de ordem m, e seja k um inteiro positivo.

   (a) Mostre que se $\mathrm{mdc}(k, m) = 1$, então a função $f\colon G \to G$, definida por $f(a) = a^k$, para todo $a \in G$, é sobrejetora.

   (b) Exiba um exemplo para mostrar que se $\mathrm{mdc}(k, m) \neq 1$, a função f do item anterior pode não ser sobrejetora.

Solução. (a) Como G é finito, para mostrar que f é sobrejetora, basta mostrar que é injetora. Sejam, assim, $a, b \in G$ tais que $f(a) = f(b)$. Então, $a^k = b^k$. Logo, $e_G = a^k(b^k)^{-1} = a^k(b^{-1})^k = (ab^{-1})^k$. Essa última igualdade segue do fato de G ser abeliano. Assim $o(ab^{-1}) \mid k$. Mas também sabemos que $o(ab^{-1}) \mid |G| = m$. Assim, $o(ab^{-1}) \mid \text{mdc}(k, m) = 1$. Segue que $o(ab^{-1}) = 1$, o que é equivalente a $ab^{-1} = e_G$. Portanto $a = b$. Isso prova que f é injetora e, portanto, sobrejetora. (b) Se $V = \{e, a, b, c\}$ denota o grupo de Klein (em que e denota o elemento identidade e $a^2 = b^2 = c^2 = e$), então V é abeliano e tem ordem $m = 4$. Se tomarmos $k = 2$, teremos $\text{mdc}(k, m) = 2 \neq 1$ e a imagem da função $f\colon V \to V$, dada por $f(x) = x^2$, para todo $x \in V$, tem imagem $\{e\}$. Logo, f não é sobrejetora.

3. Seja G um grupo, e sejam K e H subgrupos de G.

   (a) Mostre que $b^{-1}Kb$ é um subgrupo de G, qualquer que seja $b \in G$.

   (b) Mostre que se $a, b \in G$, então ou $aH \cap Kb = \emptyset$ ou $aH \cap Kb$ é uma classe lateral à esquerda de $H \cap b^{-1}Kb$ em G.

Solução. (a) Dado $b \in G$, $b^{-1}Kb$ é um subgrupo de G, pois

- $e_G = b^{-1}e_Gb \in b^{-1}Kb$, uma vez que $e_G \in K$;
- se $x, y \in b^{-1}Kb$, então existem $k, k' \in K$ tais que $x = b^{-1}kb$ e $y = b^{-1}k'b$. Assim $xy = (b^{-1}kb)(b^{-1}k'b) = b^{-1}(kk')b \in b^{-1}Kb$, uma vez que $kk' \in K$;
- se $x \in b^{-1}Kb$, então existe $k \in K$ tal que $x = b^{-1}kb$. Assim, $x^{-1} = (b^{-1}kb)^{-1} = b^{-1}k^{-1}b \in b^{-1}Kb$, uma vez que $k^{-1} \in K$.

(b) É claro que se $aH \cap Kb$ é uma classe lateral, então $aH \cap Kb \neq \emptyset$. Resta, postanto, mostrar que se $aH \cap Kb \neq \emptyset$, então $aH \cap Kb$ é uma classe lateral à esquerda de $H \cap b^{-1}Kb$ em G. Suponha, então, que $x \in aH \cap Kb$. Mostremos que $aH \cap Kb = x(H \cap b^{-1}Kb)$. Como $x \in aH \cap Kb$, existem $h \in H$ e $k \in K$ tais que $x = ah = kb$. ($\subseteq$) Dado $z \in aH \cap Kb$, existem $h' \in H$ e $k' \in K$ tais que $z = ah' = kb'$. Assim, $z = a(hh^{-1})h' = x(h^{-1}h')$ e $h^{-1}h' \in H$. Mas também temos $h^{-1}h' = (a^{-1}kb)^{-1}(a^{-1}k'b) = b^{-1}k^{-1}aa^{-1}k'b = b^{-1}(k^{-1}k')b \in b^{-1}Kb$. Vimos assim, que $z = x(h^{-1}h')$ e que $h^{-1}h' \in H \cap b^{-1}Kb$. Logo, $z \in x(H \cap b^{-1}Kb)$. ($\supseteq$) Se $w \in x(H \cap b^{-1}Kb)$, então, existe $\tilde{h} \in H \cap b^{-1}Kb$, tal que $w = x\tilde{h}$. Logo, $w = x\tilde{h} = a(h\tilde{h}) \in aH$, pois $\tilde{h} \in H$. Ainda, como $\tilde{h} \in b^{-1}Kb$, existe $\tilde{k} \in K$ tal que $\tilde{h} = b^{-1}\tilde{k}b$. Logo, $w = x\tilde{h} = kb(b^{-1}\tilde{k}b) = (k\tilde{k})b \in Kb$. Portanto, temos $w \in aH \cap Kb$.

4. Seja G um grupo, e seja H um subgrupo de G.

   (a) Dê a definição de índice de H em G.

   (b) Mostre que se H tem índice finito em G, então, para todo $a \in G$, existe um inteiro positivo r tal que $r \leq [G : H]$ e $a^r \in H$.

Solução. (a) Se existir apenas uma quantidade finita de classes laterais à esquerda de H em G distintas, o índice de H em G, denotado por $[G : H]$, é definido como sendo o número de classes laterais à esquerda de H em G distintas. (Neste caso, a quantidade de classes laterais à direita de H em G distintas também é finita e elas são em número de $[G : H]$.) Se existirem

infinitas classes laterais à esquerda de H em G distintas, dizemos que H tem índice infinito em G. (E, neste caso, a quantidade de classes laterais à direita de H em G distintas também é infinita.) (b) Denote $m = [G : H]$, e considere as seguintes classes laterais à esqueda de H em G:

$$aH,\ a^2H,\ \ldots,\ a^{m+1}H.$$

Como existem apenas m classes laterais à esquerda de H em G distintas, na listagem acima deve haver, pelo menos, uma repetição, ou seja, existem inteiros i, j tais que $1 \leq i < j \leq m+1$ e $a^iH = a^jH$. Assim, $(a^i)^{-1}a^j \in H$. Fazendo $r = j - i$, temos, então, $1 \leq r \leq m$ e $a^r = a^{j-i} \in H$.