Group theory - Midterm exam 2023: Solutions

(1) By the extended Euclidean algorithm, we have

$$\begin{aligned} 73 - 51 &= 22 & 22 - 3\cdot(51 - 2\cdot 22) &= 1 \\ 51 - 2\cdot 22 &= 7 & 7\cdot 22 - 3\cdot 51 &= 1 \\ 22 - 3\cdot 7 &= 1 & 7\cdot(73-51) - 3\cdot 51 &= 1, \end{aligned}$$

and so $1 = -10\cdot 51 + 7\cdot 73$. So the class is $\overline{3\cdot(-10)\cdot 51 + 2\cdot 7\cdot 73} = \overline{-508} = \overline{3215}$.

(2) (a) The order of a product of pairwise disjoint cycles is the least common multiple of the lengths of those cycles. An element in S_{11} which has order 8 can be written either as an 8−cycle or as a product of an 8-cycle and a 2-cycle(pairwise disjoint). The number of combinations for (8-cycle) is $\binom{11}{8}\frac{8!}{8} = 165\cdot 7!$, and the number of combinations (8-cycle)(2-cycle) is $\binom{11}{8}\frac{8!}{8}\binom{3}{2}\frac{2!}{2} = 3\cdot 165\cdot 7!$, and so in total there are $4\cdot 165\cdot 7! = 660\cdot 7!$ such elements.

(b) $\sigma = (1\,9\,8\,7\,3)(2\,5\,9\,3\,4\,8)(1\,3\,7)(1\,5)(5\,9\,7\,6) = (1\,8\,2\,5)(4\,7\,6)$ and we have $\sigma^{94} = (1\,8\,2\,5)^2(4\,7\,6)^1 = (1\,2)(4\,7\,6)(5\,8)$.

(3) Suppose G is abelian. Let $g, h \in G$. Then, we have $\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} \overset{G\ commutative}{=} g^{-1}h^{-1} = \varphi(g)\varphi(h)$ since G is commutative by assumption. Thus φ is a homomorphism.

Now suppose φ is a homomorphism. For $g, h \in G$, we have $\varphi(gh) = \varphi(g)\varphi(h)$ so $(gh)^{-1} = g^{-1}h^{-1}$. Thus $ghg^{-1}h^{-1} = 1$ and we obtain $gh = hg$. Hence G is abelian.

(4) (a) Let $\alpha = \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}, \beta = \begin{bmatrix} w & 0 \\ 0 & 1 \end{bmatrix} \in H$ and $\tau = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \in G$. Then

$$\alpha\cdot(\beta\cdot\tau) = \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}\left(\begin{bmatrix} w & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x & y \\ 0 & z \end{bmatrix}\right) = \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} wx & wy \\ 0 & z \end{bmatrix} = \begin{bmatrix} twx & twy \\ 0 & z \end{bmatrix}$$

*alternatively one could use associativity of matrix multiplication and

$$(\alpha\beta)\cdot\tau = \left(\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} w & 0 \\ 0 & 1 \end{bmatrix}\right)\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} tw & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} twx & twy \\ 0 & z \end{bmatrix}.$$

and thus, $\alpha\cdot(\beta\cdot\tau) = (\alpha\beta)\cdot\tau$. For $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, we have $1\cdot\tau = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\cdot\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} = \tau$ and hence this is a group action.

-2 points if they swap G and H.

(b) The stabiliser $H_\tau = \left\{\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} \in H : \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}\cdot\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\right\}$. It follows that $\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} t & -t \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ and thus $t = 1$. Thus, $H_\tau = \left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right\}$.

(c) The kernel of the action is given by

Ker $= \left\{\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} \in H : \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}\cdot\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \text{ for all } \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} \in G\right\}$. It follows that $\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} tx & ty \\ 0 & z \end{bmatrix} = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}$ and thus $t = 1$. Thus, Ker $= \left\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right\}$.

*Alternatively, one could deduce the kernel must be trivial since it may be given as the intersection of the stabilisers.

(5) $\underline{s^2 = 1 \Longrightarrow [\varphi(s)]^2 = I_2}$: $[\varphi(s)]^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\underline{r^4 = 1 \Longrightarrow [\varphi(r)]^4 = I_2}$:

$$[\varphi(r)]^4 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^4 = \left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right)^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\underline{sr = r^{-1}s \Longrightarrow \varphi(s)\varphi(r) = \varphi(r)^{-1}\varphi(s)}$: Since $\varphi(s)\varphi(r) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $\varphi(r)^{-1}\varphi(s) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^{-1}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, the equality holds. Hence, φ extends to a group homomorphism.

(6) (a) Note that $H \neq \emptyset$ since the identity element 1 is in H as it is contained in every subgroup H_i. Let $x, y \in H$. Since $H = \cap H_i$, we have $x, y \in H_i$ for all i. Since H_i is a subgroup, it follows that $xy^{-1} \in H_i$ for all i. Thus, $xy^{-1} \in H = \cap H_i$ and $H \leq G$. Alternatively, one could show that H is closed under products and inverses separately.

(b) Suppose H_1 is cyclically generated by x_1, i.e. $H_1 = \langle x_1 \rangle$. Let $x_1^m \in H_1$ be such that m is the smallest positive integer satisfying $x_1^m \in H$. We claim that $H = \langle x_1^m \rangle$. Let $x \in H$. Then $x = x_1^a \in H_1$ for some integer a. By the division algorithm, $a = mq + r$ for some $0 \leq r < m$. Then $x_1^a = x_1^{mq+r} = (x_1^m)^q x_1^r$ implies that $x_1^r = (x_1^a)(x_1^m)^{-q} \in H$ since H is a (sub)group and both x_1^a and $x_1^m \in H$. Since m is the smallest positive integer such that $x_1^m \in H$, we have $r = 0$, thus $x = (x_1^m)^q \in \langle x_1^m \rangle$ and $H = \langle x_1^m \rangle$.