# QUIZ 2 VERSION B SOLUTIONS
# MATH 103A, SUMMER 2021

(1) (a) False. The set $\mathbf{Z}^{\geq 0}$ is not a group under addition as the additive inverse of any positive integer is negative. For example, suppose $1 \in \mathbf{Z}^{\geq 0}$ has an additive inverse $k \in \mathbf{Z}^{\geq 0}$ and $1+k=0$. We arrive at a contradiction by noting that $1 > 0$ implies $0 = 1 + k > 0$.

(b) False. The set $\mathbf{R} \setminus \{0\}$ does not contain 0, the neutral element for addition.

(c) False. Since 21 does not divide 3, $[3]_{21} \neq [0]_{21}$. However $\gcd(3, 21) = 3 \neq 1$ so the element $[3]_{21}$ does not have a multiplicative inverse in the set $\mathbf{Z}_{21} \setminus \{[0]_{21}\}$.

(d) True. A short computation shows

$$f([5]_{13}) = [5]_{13}^4 = [25]_{13}^2 = [-1]_{13}^2 = [1]_{13}.$$

Since $[1]_{13}$ is the neutral element in $\mathbf{Z}_{13}^{+}$ and $f([5]_{13}) = [1]_{13}$, we obtain that $[5]_{13} \in \ker(f)$.

(e) True. If $|Z(S_n)| > 1$ for some $n \geq 3$, then we may pick $\sigma \in Z(S_n)$ such that $\sigma$ is not the trivial element. Since $\sigma$ non-trivial, there is some $1 \leq i \leq n$ such that $\sigma(i) = j \neq i$. Since $n \geq 3$, pick $1 \leq k \leq n$ such that $j \neq k$ and $k \neq i$. Let $\tau \in S_n$ be the transposition that swaps $j, k$ and keeps everything else fixed. Then

$$\sigma(\tau(i)) = \sigma(i) = j, \quad \tau(\sigma(i)) = \tau(j) = k \neq j.$$

Hence $\sigma\tau \neq \tau\sigma$ so $\sigma \notin Z(S_n)$.

(2) The multiplicative group $\mathbf{Z}_{19}^{\times}$ contains all equivalence classes $[k]_{19}$ such that $\gcd(k, 19) = 1$. Since $\gcd(8, 19) = 1$, $[8]_{19} \in \mathbf{Z}_{19}^{\times}$. To find $x$ such that $[8]_{19}^{-1} = [x]_{19}$, it suffices to solve

$$8x \equiv 1 \mod 19.$$

Using the division algorithm,

$$\begin{aligned} 19 &= 2 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

As a product of $2 \times 2$ matrices, we may write this as

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 19 \\ 8 \end{pmatrix}.$$

Multiplying the matrices,

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 & -7 \\ * & * \end{pmatrix} \begin{pmatrix} 19 \\ 8 \end{pmatrix}.$$

Hence $3 \cdot 19 - 7 \cdot 8 = 1$ and we conclude

$$[x]_{19} = [8]_{19}^{-1} = [-7]_{19} = [12]_{19}.$$

(3) Let $x, y \in G$ be two arbitrary elements. As $G$ is a group both $x$ and $y$ have inverses $x^{-1}$ and $y^{-1}$. Moreover we recall that for any $a, b \in G$ $(ab)^{-1} = b^{-1}a^{-1}$. Using this fact with $a = y^{-1}, b = x^{-1}$ and the definition of $f$, we get

$$xy = (x^{-1})^{-1}(y^{-1})^{-1} = (y^{-1}x^{-1})^{-1} = f(y^{-1}x^{-1}).$$

Since $f$ is a homomorphism,

$$xy = f(y^{-1}x^{-1}) = f(y^{-1})f(x^{-1}) = yx.$$

We conclude that $G$ is abelian.

(4) (a) Using the given relations, we get $\tau\sigma = \sigma^{-1}\tau$, $\sigma^{-1} = \sigma^6$ and $\tau = \tau^{-1}$. So

$$\tau\sigma^2\tau\sigma = \tau\sigma^2(\tau\sigma) = \tau\sigma^2(\sigma^{-1}\tau) = (\tau\sigma)\tau = \sigma^{-1}\tau^2 = \sigma^{-1} = \sigma^6.$$

(b) Let $\gamma = \sigma^4$. Then

$$\tau\sigma\gamma = \tau\sigma\sigma^4 = \tau\sigma^5$$
$$\gamma\tau\sigma = \sigma^4\tau\sigma = \sigma^{-3}\tau\sigma = \tau\sigma^3\sigma = \tau\sigma^4.$$

If $\tau\sigma^5 = \tau\sigma^4$ then $\sigma = \text{id}$. This is impossible as $\sigma$ has order 7 in $D_{14}$. Hence $\gamma(\tau\sigma) \neq (\tau\sigma)\gamma$ and $\gamma \notin C_{D_{14}}(\tau\sigma)$.

(c) We first note that

$$\sigma^{-6} \circ \gamma([0]_{14}) = \sigma^{-6}([6]_{14}) = [0]_{14}.$$

Moreover

$$\sigma^{-6} \circ \gamma([1]_{14}) = \sigma^{-6}([5]_{14}) = [-1]_{14} = \tau([1]_{14}).$$

Therefore $\sigma^{-6} \circ \gamma = \tau$ or $\gamma = \sigma^6 \circ \tau$. Using the relations, we can now simplify this to

$$\gamma = \sigma^6\tau = \sigma^{-1}\tau = \tau\sigma.$$