HW6 SOLUTION

JI ZENG

Only problems with provided solutions will be graded. Solutions might be concise for some problems, but please be noticed that they don't reflect the wanted level of detailedness of your answer.

Armstrong.6.3
Denote this subset as H and we check H is a subgroup. Clearly, the identity $e \in H$ as $e(i) \in \{2,5,7\}$ for all $i \in \{2,5,7\}$.
Suppose $\phi_1, \phi_2 \in H$, then for any $i \in \{2,5,7\}$, $\phi_2(i) \in \{2,5,7\}$ and hence $\phi_1 \circ \phi_2(i) = \phi_1(\phi_2(2)) \in \{2,5,7\}$. So $\phi_1\phi_2 \in H$.
Take $\phi \in H$, because by cardinality $\{\phi(2), \phi(5), \phi(7)\} = \{2,5,7\}$, we have $\phi^{-1}(i) \in \{2,5,7\}$ for all $i \in \{2,5,7\}$. So $\phi^{-1} \in H$.
So we conclude H is a subgroup. We can count $|H| = 3!6!$.

Armstrong.6.6
Write H^o (resp. H^e) the set of odd (resp. even) permutation in H. It suffices to show that $|H^o| = |H^e|$. By assumption that $H \not\subset A_n$, $H^o \neq \emptyset$, so we can pick $\sigma \in H^o$.
Now consider the map

$$r_\sigma : H \to H, \quad h \mapsto h * \sigma.$$

Because $r_{\sigma^{-1}} \circ r_\sigma = r_\sigma \circ r_{\sigma^{-1}} = \mathrm{id}$, r_σ is bijective. Notice that $r_\sigma(H^e) \subset H^o$, so $|H^e| \leq |H^o|$ because r_σ is injective. Similarly, $r_\sigma(H^o) \subset H^e$ gives $|H^o| \leq |H^e|$.

Problem.A
(a) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 1 & 4 & 2 & 6 & 5 \end{pmatrix}$.
(b) Yes. $\alpha = (17523)$.
(c) $\mathrm{ord}(\alpha) = 5$ and $\mathrm{sign}(\alpha)$ =even. $\alpha \in A_7$.

Problem.C
(a) We check V is a subgroup first. Clearly $e \in V$. And as $\alpha^2 = \beta^2 = \gamma^2 = e$, $\alpha^{-1}, \beta^{-1}, \gamma^{-1} \in V$. And we can check $\alpha\beta = \beta\alpha = \gamma$, $\alpha\gamma = \gamma\alpha = \beta$ and $\beta\gamma = \gamma\beta = \alpha$, so V is closed under multiplication.
The composition table for V is

V	e	α	β	γ
e	e	α	β	γ
α	α	e	γ	β
β	β	γ	e	α
γ	γ	β	α	e

.

We have the composition table for Kelin four group as follows

$\mathbb{Z}_2 \times \mathbb{Z}_2$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Consider the bijective map

$$f : V \to \mathbb{Z}_2 \times \mathbb{Z}_2, \quad e \mapsto (0,0), \alpha \mapsto (1,0), \beta \mapsto (0,1), \gamma \mapsto (1,1).$$

Observe that f is compatible with the composition table, so f is an isomorphism.
(b) Denote $S := \{\sigma \in A_n; \sigma^2 = e\}$. WTS $V = S$. $V \subset S$ is trivial. So we focus on showing $S \subset V$. Pick arbitrary $\sigma \in S$ and consider it's decomposition into disjoint cycles. In general there are five types of the length of the cycles: i) $1-1-1-1$; ii) $2-2$; iii) $2-1-1$; iv) $3-1$ and v) 4. However, σ cannot be in case iii) or v) because it's even. σ cannot be in case iv) because $\sigma^2 = e$.
In case i), $\sigma = e \in V$. In case ii), we can write $\sigma = (ab)(cd)$ for distinct a, b, c, d. WLOG we assume $a = 1$, so if $b = 2$, then $\sigma = \alpha$; if $b = 3$, $\sigma = \beta$; if $b = 4$, $\sigma = \gamma$. Overall, $\sigma \in V$ as wanted.
(c) First we show $\delta V \delta^{-1} \subset V$. By part (b), we wish to show $\delta S \delta^{-1} \subset S$. Pick arbitrary $\sigma \in S$. $\delta\sigma\delta^{-1}$ is even no matter the parity of δ. And $(\delta\sigma\delta^{-1})^2 = \delta\sigma\delta^{-1}\delta\sigma\delta^{-1} = e$. Hence $\delta\sigma\delta^{-1} \in S$ as wanted.
Notice that map $f : V \to \delta V \delta^{-1}, \sigma \to \delta\sigma\delta^{-1}$ is bijective because it has an inverse $g : \delta V \delta^{-1} \to V, \epsilon \mapsto \delta^{-1}\epsilon\delta$. So $|V| = |\delta V \delta^{-1}|$. Therefore $V = \delta V \delta^{-1}$ as wanted.

Problem.D
(a) We check $\alpha(ab)\alpha^{-1}(\alpha(a)) = \alpha(b)$ and $\alpha(ab)\alpha^{-1}(\alpha(b)) = \alpha(a)$. Also for $\alpha(c)$ where $c \neq a, b$, $\alpha(ab)\alpha^{-1}(\alpha(c)) = \alpha(c)$. That means $\alpha(ab)\alpha^{-1}$ interchanges $\alpha(a)$ and $\alpha(b)$ and leave the others fixed. So $\alpha(ab)\alpha^{-1} = (\alpha(a)\alpha(b))$.
(b) For arbitrary $a \in \{1, \ldots, n\}$. Because $n > 2$, take $b \neq c$ distinct from a. By part (a), $\alpha(ab)\alpha^{-1} = (\alpha(a)\alpha(b))$. As α commutes with (ab), we also have $\alpha(ab)\alpha^{-1} = (ab)$. Hence we have

$$(ab) = (\alpha(a)\alpha(b)),$$

hence $\alpha(a) \in \{a, b\}$. Similarly, $\alpha(a) \in \{a, c\}$. So $\alpha(a) \in \{a, b\} \cap \{a, c\} = \{a\}$. Hence $\alpha(a) = a$ for arbitrary a, i.e. $\alpha = e$.
(c) Firstly we prove: $\forall a, b, c \in \{1, \ldots, n\}$ pairwisely distinct, we have

$$\alpha(abc)\alpha^{-1} = (\alpha(a)\alpha(b)\alpha(c)).$$

Indeed, we just check $\alpha(abc)\alpha^{-1}(\alpha(a)) = \alpha(b)$, $\alpha(abc)\alpha^{-1}(\alpha(b)) = \alpha(c)$ and $\alpha(abc)\alpha^{-1}(\alpha(c)) = \alpha(a)$. Also for $\alpha(d)$ with $d \neq a, b, c$ we check $\alpha(abc)\alpha^{-1}(\alpha(d)) = \alpha(d)$, as wanted.
Now for arbitrary $a \in \{1, \ldots, n\}$. Because $n > 3$, take b, c, d pairwisely distinct and distinct from a. Because α commutes with $(abc) \in A_n$, $\alpha(abc)\alpha^{-1} = (abc)$. So by what we have proved, we have

$$(abc) = (\alpha(a)\alpha(b)\alpha(c)),$$

hence $\alpha(a) \in \{a, b, c\}$. Similarly we have $\alpha(a) \in \{a, b, d\}$ and $\alpha(a) \in \{a, c, d\}$. So α sits inside there intersections which is $\{a\}$. So $\alpha(a) = a$ for arbitrary a, as wanted.