Supplementary Exercises Chs 1–4

4b) $cl(a)$ in the group of quaternions
$cl(a) = \{ xax^{-1} \mid x \in G \} = \{ a, a^3 \}$

c) $cl(b) = \{ xbx^{-1} \mid x \in G \} = \{ b, ba^2 \}$

14. Prove that an Abelian group G of order 6 is cyclic.
N.T.P. G has an element of order 6

Claim 1: G doesn't have an element of order 5
Proof. If $a \in G$ has order 5, then $G = \{e, a, a^2, a^3, a^4, b\}$
Then $ab = a^k$ for some $k = 2,3,4,5 \Rightarrow b = a^{k-1}$ contradiction

Claim 2: G doesn't have an element of order 4
Proof If $a \in G$ has order 4, then $G = \{e, a, a^2, a^3, b, c\}$
Then consider ab, a^2b, a^3b. These should all be distinct and different from a^k or b because otherwise we get a contradiction.
But there aren't enough distinct elements for ab, a^2b, a^3b
so an element of order 4 is not possible

Claim 3 If G has an element of order 3 and an element of order 2, then G has an element of order 6.
Proof. Let $a, b \in G$ s.t. $|a| = 3$, $|b| = 2$.
Consider ab. Because G is Abelian, $(ab)^k = a^k b^k$

$$\left.\begin{aligned}
(ab)^2 &= a^2b^2 = a^2 \neq e \\
(ab)^3 &= a^3b^3 = b^3 = b \neq e \\
(ab)^4 &= a^4b^4 = a \neq e \\
(ab)^5 &= a^5b^5 = a^2 b \neq e \\
(ab)^6 &= a^6b^6 = (a^3)^2 (b^2)^3 = e
\end{aligned}\right\} \Rightarrow |ab| = 6.$$

Claim 4 G cannot have all elements of order 3.
Proof: If a, b, c have orders 3
Then $G = \{e, a, a^2, b, b^2, c, c^2\} \rightarrow 7$ elements, contradiction

Claim 5 G cannot have all elements of order 2
Proof If a, b, c, d, f have orders 2,
then $G = \{e, a, b, c, d, f\}$
$\Rightarrow$ W.O.L.O.G $ab = c \Rightarrow ac = b \Rightarrow bc = a$
$ad = f \Rightarrow af = d \Rightarrow df = a$
$bd = c \Rightarrow bc = d \Rightarrow dc = b$

But then $cf = a$ contradicts with $df = a$, or $cf = b$ with $bc = a$, or $cf = d$ with $df = a$

20. $x, y \in G$. $x \neq e$
$|y| = 2$, and $yxy^{-1} = x^2$.
Find $|x|$.

$yxy^{-1} = x^2 \Rightarrow yxy^{-1}yxy^{-1} = x^4$
$\Rightarrow yx^2y^{-1} = x^4$
$\Rightarrow y(yxy^{-1})y^{-1} = x^4$
$\Rightarrow y^2 x y^{-2} = x^4$
$\Rightarrow e x e = x^4$ b/c $|y| = 2$.
$\Rightarrow x = x^4 \Rightarrow x^3 = e$.
We have $x \neq e$.
Also if $x^2 = e$ then $yxy^{-1} = e$
$\Rightarrow yx = y \Rightarrow x = e$
So $x^2 \neq e$.
Hence $|x| = 3$.

29. $S \neq \emptyset$ with an associative operation. $ax = bx \Rightarrow a = b$ and $xa = xb \Rightarrow a = b$.
Also $\{a^n \mid n = 1, 2, 3, \ldots\}$ is finite $\forall a \in S$
Is S a group?

Assuming S is closed under the operation, we need to show that there is an identity element in S
Since $\{a, a^2, a^3, \ldots\}$ is finite, $a^i = a^j$ for some i, j
W.O.L.O.G assume $i > j \Rightarrow$
$\Rightarrow i - j \in \mathbb{Z}^+$ and $a^{i-j} \in S$
Claim a^{i-j} = identity.
Proof. Let $x \in S$. Then
$a^i x = a^i x \Rightarrow a^j (a^{i-j}x) = a^i x$
$\Rightarrow a^{i-j} x = x$ (b/c $a^i = a^j$ and left cancellation). Similarly show $xa^{i-j} = x$
Also, $a^{-1} = a^{i-j-1}$.

Chapter 5 #6. Show that A_8 contains an element of order 15.

let $\sigma = (123)(45678)$.

$|\sigma| = \text{lcm}(3,5) = 15$.

$\sigma \in A_8$ b/c $\sigma = \underbrace{(13)(12)(48)(47)(46)(45)}_{6 \text{ transpositions}}$

#7. Possible orders of elements:

For a permutation σ, $|\sigma| = \text{lcm}$(lengths of disjoint cycles that make it up)

In S_6, ① $\sigma = (a_1a_2a_3a_4a_5) \Rightarrow |\sigma| = 5$

or ② $\sigma = (a_1a_2a_3a_4) \Rightarrow |\sigma| = 4$

or ③ $\sigma = (a_1a_2a_3)(a_4a_5) \Rightarrow |\sigma| = 6$

or ④ $\sigma = (a_1a_2a_3) \Rightarrow |\sigma| = 3$

or ⑤ $\sigma = (a_1a_2)(a_3a_4) \Rightarrow |\sigma| = 2$

or ⑥ $\sigma = (a_1a_2) \Rightarrow |\sigma| = 2$

or ⑦ $\sigma = (a_1) \Rightarrow |\sigma| = 1$ $\Rightarrow$ $\boxed{\text{possible orders in } S_6 \; \{1,2,3,4,5,6\}}$

Among the cases above in ①, ④, ⑤ ⑦ σ would be in A_6 so possible orders in A_6 are $\{1,2,3,5\}$

In S_7, $\sigma = (a_1a_2a_3a_4a_5a_6a_7) \Rightarrow |\sigma| = 7$ $(\in A_7)$

$\sigma = (a_1a_2a_3a_4a_5a_6) \Rightarrow |\sigma| = 6$

$\sigma = (a_1a_2a_3a_4a_5)(a_6a_7) \Rightarrow |\sigma| = 10$

$\sigma = (a_1a_2a_3a_4a_5) \Rightarrow |\sigma| = 5$ $(\in A_7)$

$\sigma = (a_1a_2a_3a_4)(a_5a_6a_7) \Rightarrow |\sigma| = 12$

$\sigma = (a_1a_2a_3a_4)(a_5a_6) \Rightarrow |\sigma| = 4$ $(\in A_7)$

$\sigma = (a_1a_2a_3a_4) \Rightarrow |\sigma| = 4$

$\sigma = (a_1a_2a_3)(a_4a_5a_6) \Rightarrow |\sigma| = 3$ $(\in A_7)$

$\sigma = (a_1a_2a_3)(a_4a_5)(a_6a_7) \Rightarrow |\sigma| = 6$ $(\in A_7)$

$\sigma = (a_1a_2a_3)(a_4a_5) \Rightarrow |\sigma| = 6$

$\sigma = (a_1a_2a_3) \Rightarrow |\sigma| = 3$ $(\in A_7)$

$\sigma = (a_1a_2)(a_3a_4)(a_5a_6) \Rightarrow |\sigma| = 2$

$\sigma = (a_1a_2)(a_3a_4) \Rightarrow |\sigma| = 2$ $(\in A_7)$

$\sigma = (a_1a_2) \Rightarrow |\sigma| = 2$

$\sigma = (a_1) \Rightarrow |\sigma| = 1$ $(\in A_7)$

possible orders in $S_7 = \{1,2,3,4,5,6,7,10,12\}$

in $A_7 = \{1,2,3,4,5,6,7\}$

#19. $H \leq S_n \Rightarrow$ either all $\sigma \in H$ is even or exactly half of the permutations in H is even.

Proof: Suppose $\exists$ odd $\sigma \in H$. Then $\sigma\sigma \in H$

So, there is at least one even permutation p in H.

For each α odd in H, αp is even

So, # odds in $H \leq$ # evens in H.

Similarly for each α even in H, $\alpha\sigma$ is odd

So, # evens in $H \leq$ # odd in H

$\Rightarrow$ # evens = # odds in H

$\Rightarrow$ Half of the permutations in H are odd.

#36. In S_4, find a cyclic & a noncyclic subgroups of order 4

let $H = \langle(1,2,3,4)\rangle$ (cyclic)

The $|H| = |(1234)| = 4$

let $K = \{(1),(12),(34),(12)(34)\}$

K is not cyclic because none of the elements generate K.

K is closed under composition and under taking inverses (verify!)

So, K is a subgroup of order 4 and it is not cyclic.

#48 Use Verhoeff check digit scheme to append a check digit to 45723.

According to Verhoeff scheme, if the check digit is a, we have $\sigma(4) * \sigma^2(5) * \sigma^3(7) * \sigma^4(2) * \sigma^5(3) * \sigma^6(a) = 0$.

From table 5.3, we get

$2 * 9 * 5 * 5 * 6 * \sigma^6(a) = 0$

$\Rightarrow \sigma^6(a) = 0$.

Again from the table, $a = 5$.

Chapter 5 #50. $S = \{A, 2, 3, 4, \dots, J, Q, K\}$

If $\sigma^2 = \begin{pmatrix} A & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & J & Q & K \\ 10 & 9 & Q & 8 & K & 3 & 4 & A & 5 & J & 6 & 2 & 7 \end{pmatrix}$

find σ.

Note that $\sigma^2 = (A\ 10\ J\ 6\ 3\ Q\ 2\ 9\ 5\ K\ 7\ 4\ 8)$

Let $\sigma = (a_1 a_2 a_3 a_4 a_5 \dots a_{13})$.

Then $\sigma^2 = (a_1 a_3 a_5 a_7 a_9 a_{11} a_{13} a_2 a_4 a_6 a_8 a_{10} a_{12})$

$\Rightarrow a_1 = A,\ a_3 = 10,\ a_5 = J, \dots$

$\Rightarrow \sigma = (A\ 9\ 10\ 5\ J\ K\ 6\ 7\ 3\ 4\ Q\ 8\ 2)$

Chapter 6 #4. Show that $U_8 \not\cong U_{10}$.

$U_{10} = \{1, 3, 7, 9\}$ and $U_{10} = \langle 3 \rangle$ cyclic.

However $U_8 = \{1, 3, 5, 7\}$ and $|a| = 2\ \forall a \in U_8$ so U_8 is not cyclic.

A cyclic group & a non-cyclic group can not be isomorphic!

#5. Show that $U_8 \cong U_{12}$.

$U_8 = \{1, 3, 5, 7\}$ with $|3| = |5| = |7| = 2$

$U_{12} = \{1, 5, 7, 11\}$ with $|5| = |7| = |11| = 2$

let $\phi: U_8 \to U_{12}$

$1 \mapsto 1$
$3 \mapsto 5$
$5 \mapsto 7$
$7 \mapsto 11$

show that ϕ is an isomorphism!

#6. Show that the notion of group isomorphism is transitive.

let G, H, K be groups with $G \cong H$ and $H \cong K$.

Suppose $\alpha: G \to H$ and $\beta: H \to K$ are isomorphisms

Claim: $\beta \circ \alpha: G \to K$ is an isomorphism (hence $G \cong K$)

① $\beta \circ \alpha$ is 1-1 and onto b/c β and α are 1-1 and onto

② $(\beta \circ \alpha)(g_1 \cdot g_2) = \beta(\alpha(g_1 \cdot g_2)) = \beta(\alpha(g_1) \cdot \alpha(g_2))$

b/c α is an isomorphism & $g_1, g_2 \in G$

$= \beta(\alpha(g_1)) \cdot \beta(\alpha(g_2)) = (\beta \circ \alpha)(g_1) \cdot (\beta \circ \alpha)(g_2) \Rightarrow \beta \circ \alpha$ preserves the operation

b/c β is an isomorphism and $\alpha(g_1), \alpha(g_2) \in H$

Hence $\beta \circ \alpha$ is an isomorphism.

#18. $\phi: \mathbb{Z}_{50} \to \mathbb{Z}_{50}$ isomorphism, $\phi(7) = 13$. Find $\phi(x)$

$\mathbb{Z}_{50} = \langle 1 \rangle$ & ϕ is an isomorphism

So, $\phi(x) = \phi(\underbrace{1 + 1 + 1 + \dots + 1}_{x\text{ times}}) = \underbrace{\phi(1) + \phi(1) + \dots + \phi(1)}_{x\text{ times}} = x \cdot \phi(1)$

So all we need to determine is $\phi(1)$.

Now, $\phi(7) = 7 \cdot \phi(1) = 13 \Rightarrow 7 \cdot \phi(1) = 63 \pmod{50} \Rightarrow \phi(1) = 9$

$\Rightarrow \phi(x) = 9x$

#22. Prove or disprove that $U_{20} \cong U_{24}$.

This is not true b/c in U_{24} all elements have order 2 (check!)

However in U_{20}, 3 has order 4.

Because isomorphisms preserve orders, we can't have $U_{20} \cong U_{24}$.

#25. Prove that $\mathbb{Z}$ under + is not isomorphic to $\mathbb{Q}$ under +

Suppose $\phi: \mathbb{Q} \to \mathbb{Z}$ is an isomorphism. Because ϕ is onto, $1 \in \mathbb{Z} \Rightarrow \exists x \in \mathbb{Q}$ s.t. $\phi(x) = 1$

Since $x = \frac{x}{2} + \frac{x}{2}$

we have $\phi(x) = \phi(\frac{x}{2}) + \phi(\frac{x}{2})$

$1 = 2 \cdot \phi(\frac{x}{2})$

$\mathbb{Z} \not\ni \frac{1}{2} = \phi(\frac{x}{2})$

contradiction!