1. Find orders of all elements of $\mathbb{Z}_4$.
   \[|0| = 1, \ |1| = 4, \ |2| = 2, \ |3| = 2, \ |1| = 4 \equiv_4 0, \ |2| = 2, \ |3| = 2 \equiv_4 0, \ |1| = 4 \equiv_4 0, \ |2| = 2, \ |3| = 2 \equiv_4 0.\]

2. Find orders of all elements of $U(14)$.
   \[U(14) = \{1, 3, 5, 9, 11, 13\}, \ |1| = 1 \text{ (since } 1.1 \equiv_{12} 1), \ |5| = 6, \ |3| = 5 \equiv_{14} 11 \neq 1, \ |3| = 3 \equiv_{14} 13 \neq 1, \ |5| = 14 \equiv_{14} 5 \neq 1 \text{ and } \ |5| = 14 \equiv_{14} 1\text{. Similarly, } |3| = 6, |9| = 3, |9| = 9 \equiv_{14} 11, |9| = 9 \equiv_{14} 99 \equiv_{14} 1.\]

3. Find orders of all elements of $\mathbb{Z}$.
   \[|0| = 1 \text{ (0 is the identity of the additive group } \mathbb{Z}).\]

   Let $a \neq 0 \in \mathbb{Z}$. Then $na \neq 0 \forall n \in \mathbb{Z}^+$. \[\implies |a| = \infty \text{ So all nonzero elements of } \mathbb{Z} \text{ have infinite order.}\]

4. Find orders of all elements in $\mathbb{R}^+$, the group of nonzero real numbers under multiplication.
   \[|1| = 1 \text{ (1 is the identity of the multiplicative group } \mathbb{R}^+ \text{ ) and } |1| = 2.\]

   Let $a \in \mathbb{R}^+$ such that $a \in \{-1, 1\}$. Then $a^n \neq 1 \forall n \in \mathbb{Z}^+$. \[\implies |a| = \infty \text{ So all elements of } \mathbb{R}^+, \text{ other than } -1 \text{ and } 1, \text{ have infinite order.}\]

5. Prove that in any group, an element and its inverse have the same order.
   \[\text{Case 1. } |a| \neq \infty \implies \exists m \in \mathbb{Z}^+ \text{ such that } a^m = e \iff \exists m \in \mathbb{Z}^+ \text{ such that } (a^{-1})^m = e \iff |a^{-1}| \neq \infty (\text{since } a^m = e \iff (a^{-1})^m = e) \iff e = (a^{-1})^{-1} \iff (a^{-1})^m = e.\]

   \[\text{Case 2. Assume } |a| = m_1 \text{ and } |a^{-1}| = m_2. \text{ Prove } m_1 = m_2. \text{ If } a^m = e \text{ (since } |a| = m_1) \iff (a^{-1})^m = e \iff (a^{-1})^{-1} m_1 = e \iff (a^{-1})^{-1} m_2 = e. \text{ Now } (a^{-1}) m_1 = e \text{ and } |a^{-1}| = m_2. \text{ Then } m_2 \leq m_1. \text{ If } (a^{-1})^{m_2} = e \text{ (since } |a^{-1}| = m_2) \iff (a^{-1})^{m_2} = e \iff |a| = m_1 \iff m_1 \leq m_2 \text{ (def. of order). Also, } (a^{-1})^{m_1} = (a^{-1})^{-1}(e) \iff e \iff |a^{-1}| = m_2 \iff m_2 \leq m_1.\]

6. Prove that an abelian group with two elements of order 2 must have a subgroup of order 4.
   Let $G$ be an abelian group and $a, b \in G$ such that $|a| = 2$ and $|b| = 2$. Then $H = \{e, a, b, ab\}$ is closed and therefore, by finite subgroup test, a subgroup of $G$.

7. Find the order of each element of the group $\mathbb{Z}_{15}$, the group of integers under addition modulo 10.
   \[|1| = 3, |2| = 4, |5| = 6, |8| = 5, |5| = 2, |0| = 1.\]

8. \(a\) Find the order of each element of the group $U(30)$, the group of positive integers less than 30 and relatively prime to 30 under multiplication modulo 30.
   
   \[U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}: \ |1| = 1, |7| = 4, |11| = 2, |13| = 4, |17| = 4, |19| = 2, |23| = 4, \text{ and } |29| = 2.\]

\(b\) Give a multiplication table for $U(30)$.
   
   \[U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}: \ |1| = 1, |7| = 4, |11| = 2, |13| = 4, |17| = 4, |19| = 2, \]

\[\text{Handout#3} \quad \text{Fall, 2010}\]
10. If $H$ and $K$ are subgroups of $G$, show that $H \cap K$ is a subgroup of $G$.

Apply the 1-step subgroup test: (1): $e \in H$ and $e \in K$ (since $H$ and $K$ are subgroups of $G$). Thus $e \in H \cap K$.

(2) Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. So $a, b^{-1} \in H$ and $a, b^{-1} \in K$ (since $H$ and $K$ are subgroups of $G$). So $ab^{-1} \in H$ and $ab^{-1} \in K$ (since $H$ and $K$ are subgroups of $G$). Hence $ab^{-1} \in H \cap K$.

11. Let $G$ be a finite abelian group and let $a, b \in G$. Prove that the set $< a, b > = \{a^ib^j | i, j \in \mathbb{Z} \}$ is a subgroup of $G$. Apply the One-Step subgroup Test to $H = < a, b > = \{a^ib^j | i, j \in \mathbb{Z} \}$.

First, show that $H \neq \emptyset$. The identity $e = a^0b^0$ of $G$ is in $H$. Next, let $a^ib^j, a^kb^l \in H$. Prove
13. Let $G$ be a group that contains elements $a$ and $b$ such that $(a^ib)(a^kb)^{-1} \in H$.

19. (a) Let $G$ be an abelian group. What is $Z(G)$?

20. (5 points) Consider the group $\mathbb{Z}_8$ of integers modulo 8, under addition modulo 8. Find $(a^ib)(a^kb)^{-1} = (a^ib)(b^{k-1}a^{-k})^{-1}$ (since $(ab)^{-1} = b^{-1}a^{-1} \forall a, b \in G = (a^ib)^{-1}b^{-1}a^{-k}$ (notation) = $a^i(b^{k-1})a^{-k}$ (associative law in the group $G$) = $a^ia^{-k}(b^{k-1})$ (since $G$ is abelian and $b^{k-1}, a^{-k} \in G$, $(b^{k-1})a^{-k} = a^{-k}(b^{k-1}) = a^{-k}b^{k-1}$ (laws of exponent). So $(a^ib)^{-1} = a^{-k}b^{k-1} \in H$ (since $i - k, j - l \in \mathbb{Z}$).

12. (a) Construct a multiplication table for $U(10)$.

\[
\begin{array}{cccc}
1 & 3 & 7 & 9 \\
3 & 1 & 7 & 9 \\
7 & 1 & 3 & 9 \\
9 & 7 & 3 & 1 \\
\end{array}
\]

(b) Find the order of each element of $U(10)$.

| $|1| = 1$ | $|3| = 4$ | $|7| = 4$ | $|9| = 2$. |

13. List all elements of the cyclic subgroup $< 7 >$ of the group $U(18) = \{1, 5, 7, 11, 13, 17\}$. Since $7^0 = 1, 7^1 = 7, 7^2 = 49 \equiv_{18} 13, 7^3 \equiv_{18} 91 \equiv_{18} 1, |7| = 3$ and $< 7 >= \{1, 7, 13\}$.

15. Let $G$ be a group and $a, b \in G$ such that $(ab)^4 = a^2b^2(ab)^2$.

(a) Which element of $G$ is the product $(a^2b)(a^2)$?

Prove that $ab = ba$.
\[(ab)^4 = (a^{2}b^{2})(ab)^2 \implies (ab)^2(abb)^2 = (a^{2}b^{2})(ab)^2 \implies (ab)^2 = a^{2}b^{2} \text{(since $(ab)^2 \in G$ (right cancellation)).} \text{ Now $(ab)^2 = a^{2}b^{2} \iff abab = aabb$ (notation and associative law) \iff ba = ab (left cancellation of $a$)} \iff ba = ab \text{(right cancellation of $b$).}

16. Let $G$ be an abelian group with identity $e$ and let $H$ be the set of all elements of $G$ that satisfy $x^3 = 1$; that is $H = \{x \in G| x^3 = e\}$. Prove that $H$ is a subgroup of $G$.

Apply the 2-step subgroup subgroup test: (1) Since $e^3 = e, e \in H$. (2) Let $x, y \in H$. Then $(xy)^3 = x^3y^3$ (G is abelian) = $xy$ (since $x, y \in H$) = $e$. Thus $xy \in H$. (3) Let $x \in H$. Then $(x^{-1})^3 = (x^{-1})(x^{-1})(x^{-1})$ (notation) = $(e)^{-1}$ (since $x \in H$) = $e$. Hence $x^{-1} \in H$.

17. List all elements of the cyclic subgroup $< 3 >$ of the group $U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$. Since $3^0 = 1, 3^1 = 3, 3^2 = 9, 3^3 = 27 \equiv_{10} 7, 3^4 = 81 \equiv_{10} 1, |3| = 4$ and $< 3 >= \{1, 3, 9, 7\}$.

18. Let $G$ be a group and $x \in G$. If $|x| = 10$, then compute $|x^8|$ and $|x^3|$.

| $|x| = \frac{10}{\gcd(8, 10)} = \frac{10}{2} = 5$ and $|x^3| = \frac{10}{\gcd(3, 10)} = \frac{10}{1} = 10$. |

19. (a) Let $G$ be an abelian group. What is $Z(G)$?

(b) Let $G$ be a group and $a, b, c \in G$. What is the inverse of the element $abc$?

\[c^{-1}b^{-1}a^{-1} \cdot \]

(c) Let $G$ be a group. What is the centraliser, $C(e)$, of the identity $e$ of $G$?

G.

20. (5 points) Consider the group $\mathbb{Z}_8$ of integers modulo 8, under addition modulo 8. Find

(a) $|G|=3$ is even, since $8.3=24 \equiv 0 \mod 8$, and $k.3 \neq 8$, for $1 \leq k < 8$.

(b) $|G|=6$, since $4.6=24 \equiv 0 \mod 8$, and $k.3 \neq 8$, for $1 \leq k < 4$.

22. Suppose $G$ is a group and $a, b, c \in G$.

(a) Show that $(b^{-1}a)^3 = b^{-1}a^3b$.

$(b^{-1}a)^3 = (b^{-1}a)(b^{-1}ab)(b^{-1}ab) = b^{-1}a(bb^{-1})a(bb^{-1})ab = b^{-1}a(e)a(e)ab = b^{-1}aaba = b^{-1}a^3b$.

(b) What is the inverse of the element $abc$?

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

23. Find a multiplication table for the group that contains elements $a$ and $b$ such that $G$ is defined by the following Cayley table:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

(a) Find the center, $Z(G)$, of $G$.

(b) Find the centralizer of each member of $G$.

24. If $H$ is a subgroup of $G$, then by the centraliser of $H$, we mean the set $C(H) = \{ x \in G | xh = hx \text{ for all } h \in H \}$. Prove that $C(H)$ is a subgroup of $G$.

Apply the 2-step subgroup test to $C(H)$: (1) Since $eh = he \in H$, $e \in C(H)$. (2) Let $a, b \in C(H)$.

Show $(ab)h = h(ab) \in H$. Let $h \in H$. Then $(ab)h = a(hb) = (ah)b = (ha)b = h(ab)$.

So $ab \in C(H)$.

(3) Let $a \in C(H)$. Show $a^{-1}h = ha^{-1} \in H$. Let $h \in H$. Then $ah = ha$ (since $a \in C(H)$).

$\Rightarrow a^{-1}aha^{-1} = a^{-1}ha^{-1}$ (since $a^{-1} \in G$) $\Rightarrow ha^{-1} = a^{-1}h$. So $a^{-1} \in C(H)$.