1 Homework #2

1. [Bachwich, A.] In $D_4$, find all elements $x$ such that

   (a) $x^3 = F$
   Solution: $S_1 = \{F\}$

   (b) $x^3 = R_{90}$
   Solution: $S_2 = \{R_{270}\}$

   (c) $x^3 = R_0$
   Solution: $S_3 = \{R_0\}$

   (d) $x^2 = R_0$
   Solution: $S_4 = \{R_0, R_{180}, F, F_-, F_\}$

   (e) $x^2 = F_-$
   Solution: $S_5 = \emptyset$

2. [Leonard, R.] Prove that every Cayley table for a group is a Latin square. A Latin square of order $n$ is an $n \times n$ array on $n$ symbols such that each symbol appears exactly once in each row and column. Hint: use Theorem 2.2.

   Let $G$ be a group. By contradiction, assume that an element $q$ appears twice in one column of the Cayley table of $G$. This implies $\exists a, b, c \in G$ such that $b \circ a = q$ and $c \circ a = q$. We know from Theorem 2.2 (Cancellation) that $b \circ a = c \circ a$ implies $b = c$. Therefore, by contradiction, $q$ cannot appear more than once in each column. Similarly $q$ cannot appear more than once in each row.

   We must also prove an element $q$ will appear at least once in each row. Each row has $n$ elements, where $n$ equals the order of the group. Because the operation is closed, there are $n$ possible outcomes between any two elements in $G$. Thus there are $n$ entries in each row of the Cayley table and $n$ possible elements to fill it with. We know from the previous argument that no element can appear more than once in each row, and we know that each entry in the Cayley table must be filled because every operation $a \circ b \in G$ has a solution. By this, we conclude that each element appears at least once in each row because it takes $n$ elements to fill a row of size $n$ without duplicating an element. Similarly, each element has to appear once in each column.

   Therefore, for every row and column, each element will appear exactly once. This makes the Cayley table for $G$ a Latin square.
3. [Berger, E.] Suppose the table below is a Cayley table for an unknown group. Fill in the blank entries. Do not assume e is the identity. Also, Problem 2 will be helpful.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>−</td>
<td>−</td>
<td>−</td>
<td>−</td>
</tr>
<tr>
<td>a</td>
<td>−</td>
<td>b</td>
<td>−</td>
<td>−</td>
<td>e</td>
</tr>
<tr>
<td>b</td>
<td>−</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>−</td>
</tr>
<tr>
<td>c</td>
<td>−</td>
<td>d</td>
<td>−</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>−</td>
<td>−</td>
<td>−</td>
<td>−</td>
<td>−</td>
</tr>
</tbody>
</table>

In the previous problem, we proved that any Cayley table is a Latin square. Thus, we can use the rules of Latin squares to begin filling out the table. By these rules, we know \( d \circ a = e, e \circ a = a, b \circ e = b, b \circ d = a, c \circ b = e, \) and \( c \circ e = c. \)

By the definition of a group, we know there exists an identity element \( e \in G \) such that \( a \circ e = a = e \circ a \) for all \( a \in G. \) Coincidently, since \( e \circ e = e, e \circ a = a, b \circ e = b, \) and \( c \circ e = c \) and we know the identity is unique, we know that \( e \) is our identity element. As such, \( a \circ e = a, d \circ e = d, e \circ b = b, e \circ c = c, \) and \( e \circ d = d. \)

We can solve the remaining entries, \( d \circ d = c, a \circ c = d, d \circ c = b, d \circ b = a \) and \( a \circ b = c, \) using the properties of Latin squares.

<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>d</td>
<td>d</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
</tbody>
</table>

4. [Li, Y.] Suppose that in the definition of a group \( G, \) the condition that there exists an element \( e \) with the property \( a \circ e = e \circ a = a \) for all \( a \in G \) is replaced by \( a \circ e = a \) for all \( a \in G. \) Show that \( e \circ a = a \) for all \( a \in G. \)

Assume that \( e \circ a = x. \) If we operate by the same element, \( a, \) on both sides of the equation,

\[
 a \circ e \circ a = a \circ x.
\]

According to the definition of group, the operation is associative. Therefore

\[
(a \circ e) \circ a = a \circ x.
\]

Since \( a \circ e = a, \) we substitute \( a \circ e \) with \( a. \) We then get \( a \circ a = a \circ x. \) By cancellation, \( x = a. \) Therefore, \( e \circ a = a. \)
5. [Dyke, M.] Suppose that in the definition of a group $G$, the condition that for each element $a \in G$ there exists an element $b \in G$ with the property $a \circ b = b \circ a = e$ is replaced by $a \circ b = e$. Show that $b \circ a = e$. (Note that under this assumption inverses only work on the right hand side.)

Consider the identity element property of groups:

$$e \circ a = a \circ e.$$ 

Use the given right inverse property to replace the $e$ on the left side of the equation

$$(a \circ b) \circ a = a \circ e.$$ 

Using the associativity property of groups, the equation can be rearranged as

$$a \circ (b \circ a) = a \circ e.$$ 

Recall Theorem 2.2, which states that $a \circ b = a \circ c$ implies $b = c$. Applying Theorem 2.2 to $a \circ (b \circ a) = a \circ e$ allows the cancellation of $a$ on the left side of both halves of the equation

$$a \circ (b \circ a) = a \circ e,$$

which yields

$$b \circ a = e,$$

thus proving the desired property $b \circ a = e$. 

3
2 Homework #3

1. [Hoffman, L.] Invent your own Color-five group. Provide a Cayley table and clearly state the identity and each element’s inverse.

\[ \begin{array}{cccccc}
C & O & X & R & B \\
C & C & O & X & R & B \\
O & O & X & R & B & C \\
X & X & R & B & C & O \\
R & R & B & C & O & X \\
B & B & C & O & X & R \\
\end{array} \]

R = Red, \( R^{-1} = \) Oxblood

B = Blue, \( B^{-1} = \) Orange

C = Clear, \( C^{-1} = \) Clear

O = Orange, \( O^{-1} = \) Blue

X = Oxblood, \( X^{-1} = \) Red

The identity is Clear.
2. [Spurlock, J.] Determine the following quantities:

(a) $51 \pmod{13}$

\[ 51 \equiv 12 \pmod{13} \]

(b) $342 \pmod{85}$

\[ 342 \equiv 2 \pmod{85} \]

(c) $82 \cdot 73 \pmod{7}$

\[ 82 \cdot 73 \equiv 5 \cdot 3 = 15 \equiv 1 \pmod{7} \]

(d) $51 + 68 \pmod{7}$

\[ 51 + 68 \equiv 2 + 5 = 7 \equiv 0 \pmod{7} \]

(e) $35 \cdot 24 \pmod{11}$

\[ 35 \cdot 24 \equiv 2 \cdot 2 = 4 \pmod{11} \]

(f) $47 + 68 \pmod{11}$

\[ 47 + 68 \equiv 3 + 2 = 5 \pmod{11} \]

3. [Brubaker, N.] For $n = 5, 8, \text{ and } 12$, find all positive integers less than $n$ that are relatively prime to $n$.

(a) \[ \{a \in \mathbb{Z} : 0 < a < 5 \ , \ \gcd(a, 5) = 1 \} = \{1, 2, 3, 4\} \]

(b) \[ \{a \in \mathbb{Z} : 0 < a < 8 \ , \ \gcd(a, 8) = 1 \} = \{1, 3, 5, 7\} \]

(c) \[ \{a \in \mathbb{Z} : 0 < a < 12 \ , \ \gcd(a, 12) = 1 \} = \{1, 5, 7, 11\} \]
4. [Carroll, S.] Complete the following Cayley tables.

(a) \((\mathbb{Z}_4, +)\)

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\]

(b) \((\mathbb{Z}_6, +)\)

\[
\begin{array}{c|cccccc}
+ & 0 & 1 & 2 & 3 & 4 & 5 \\
\hline
0 & 0 & 1 & 2 & 3 & 4 & 5 \\
1 & 1 & 2 & 3 & 4 & 5 & 0 \\
2 & 2 & 3 & 4 & 5 & 0 & 1 \\
3 & 3 & 4 & 5 & 0 & 1 & 2 \\
4 & 4 & 5 & 0 & 1 & 2 & 3 \\
5 & 5 & 0 & 1 & 2 & 3 & 4 \\
\end{array}
\]

5. [Kranstz, S.] Prove the following statements concerning inverses in a group \(G\).

(a) For all \(a \in G\), prove \((a^{-1})^{-1} = a\).

Let \(x = (a^{-1})^{-1}\).
Then \(a^{-1} \circ x = e\)
\((a \circ a^{-1}) \circ x = a \circ e\)
\(e \circ x = a\)
\(x = a\).

Therefore \((a^{-1})^{-1}\) does, in fact, equal \(a\).

(b) For all \(a, b \in G\), prove \((a \circ b)^{-1} = b^{-1} \circ a^{-1}\).

We know
\[
(a \circ b) \circ (a \circ b)^{-1} = e
\]
\[a^{-1} \circ (a \circ b) \circ (a \circ b)^{-1} = a^{-1} \circ e\]
\[(a^{-1} \circ a) \circ b \circ (a \circ b)^{-1} = a^{-1}\]
\[e \circ b \circ (a \circ b)^{-1} = a^{-1}\]
\[b \circ (a \circ b)^{-1} = a^{-1}\]
\[(b^{-1} \circ b) \circ (a \circ b)^{-1} = b^{-1} \circ a^{-1}\]
\[e \circ (a \circ b)^{-1} = b^{-1} \circ a^{-1}\]
\[(a \circ b)^{-1} = b^{-1} \circ a^{-1}\].

Therefore \((a \circ b)^{-1} = b^{-1} \circ a^{-1}\).
6. [Rotert, A.] Let $n$ and $a$ be positive integers. Show that the equation $ax \equiv 1 \pmod{n}$ has a solution if and only if $a$ and $n$ are relatively prime.

**Proof (Forward Implication):**

Assume $ax \equiv 1 \pmod{n}$. Then $ax = qn + 1$ is an equivalent statement, where $q \in \mathbb{Z}^+$. We can rewrite $ax = qn + 1$ as $ax - qn = 1$. If we consider the set $S = \{ax + by : (ax + by) > 0 \text{ and } x,y \in \mathbb{Z}\}$, then $ax - qn$ must be in $S$, where $n = b$ and $-q = y$, and using the Division Algorithm as we did in our gcd proof, it can be show that $1 \in S$.

To show that 1 is also the greatest element, consider $d'$ such that $d|a,d|n,d'|a,d'|n$ and $d' > d$. Let $a = d'h$ and $b = d'u \exists h,u \in \mathbb{Z}$. Then $d = as + bt = (d'h)s + (d'u)t = d'(hs + ut)$. This implies that $d'|d$, implying that $d > d'$, a contradiction.

Thus, if $ax \equiv 1 \pmod{n}$, then $\gcd(a,n) = 1$.

**Backward Implication:**

Assume $\gcd(a,n) = 1$. Consider the set $S = \{ax + by : (ax + ny) > 0 \text{ and } x,y \in \mathbb{Z}\}$. This means we have an equation of the form $ax + ny = 1$, because $\gcd(a,n) = 1$. This can be rewritten as $ax = 1 - qn$. If we assume that $q \leq 0$, then this becomes $ax = qn + 1$.

This is equivalent to stating $ax \equiv 1 \pmod{n}$, meaning if $a$ and $n$ are relatively prime, then $ax \equiv 1 \pmod{n}$.

Therefore $ax \equiv 1 \pmod{n}$ if and only if $\gcd(a,n) = 1$.

7. [Wulff, A.] Suppose $a$ and $b$ are integers that divide the integer $c$. If $a$ and $b$ are relatively prime, show that $ab$ divides $c$. Show by example that if $a$ and $b$ are not relatively prime, then $ab$ need not divide $c$. Hint: familiarize yourself with Theorem 0.3.

Presume $a$ and $b$ are relatively prime, and thus share no common factors, aside from 1. This can be taken from the Fundamental Theorem of Arithmetic: for $a,b \in \mathbb{Z}$, they are either prime or a product of primes. Let $a = f_1 \cdot f_2 \cdot f_3 \cdots f_r$ and $b = g_1 \cdot g_2 \cdot g_3 \cdots g_s$, where $r$ and $s$ need not be equal, and no $f_r = g_s$. Let $A$ be the set of factors of $a$, $B$ be the factors of $b$, and $C$ the collection of factors of $c$. If either $a|c$ or $b|c$, then $c$ is a composite of prime factors and $A \subseteq C$ or $B \subseteq C$, respectively. It follows that if $a|c$ and $b|c$, then $A \cup B \subseteq C$, and thus $C$ contains all $f_1, f_2, f_3, \ldots, f_r$ and $g_1, g_2, g_3, \ldots, g_s$. If $A \cup B = C$, then $C = \{f_1, f_2, \ldots, f_r, g_1, g_2, g_3, \ldots, g_s\}$, and $ab = c$. In this case $ab|c$. If $A \cup B \subseteq C$, then there exists other prime numbers $h_1, h_2, \ldots, h_t \in C$, and $c = f_1 \cdots f_r \cdot g_1 \cdots g_s \cdot h_1 \cdots h_t$. Let $u = h_1 \cdots h_t$, and then there exists an integer $u$ such that $c = abu$, and $ab|c$.

If $a$ and $b$ are not relatively prime, then $\exists f_r \in A$, and $\exists g_s \in B$ such that, $f_r = g_s$. For example consider $a = 6 = 2 \cdot 3$, $b = 8 = 2^3$, and $c = 24 = 2^3 \cdot 3$. In this case $A = \{2, 3\}$, and $B = \{2, 2, 2\}$. Note that $A \cap B \neq \emptyset$. So, while $a|c$, and $b|c$, $ab = 48$, which does not divide 24.
3 Homework #4

1. For each group in the following list: (i) find the order of the group and the order of each element in the group. (ii) Find all subgroups of the following groups. State the order of each subgroup.

(a) [Dyke, M.] Klein-four group

Klein-four

| g  | |g| | H     | |H| |
|----|---|----|-------|---|
| a  | 1 | {a} | 1     |   |
| b  | 2 | {a, b} | 2   |   |
| c  | 2 | {a, c} | 2   |   |
| d  | 2 | {a, d} | 2   |   |
|    |   | {a, b, c, d} | 4   |   |

(b) [Feather, R.] U(10)

U(10)

| g  | |g| | H     | |H| |
|----|---|----|-------|---|
| 1  | 1 | {1} | 1     |   |
| 3  | 4 | {1, 9} | 2   |   |
| 7  | 4 | U(10) | 4   |   |
| 9  | 2 |     |   |   |

(c) [Franck, D.] (Z₅, +)

Z₅

| g  | |g| | H     | |H| |
|----|---|----|-------|---|
| 0  | 1 | {0} | 1     |   |
| 1  | 5 | Z₅  | 5     |   |
| 2  | 5 |     |   |   |
| 3  | 5 |     |   |   |
| 4  | 5 |     |   |   |

(d) [Kittler, S.] Hexaflexagon group

Hexaflexagon

| g  | |g| | H     | |H| |
|----|---|----|-------|---|
| n  | 1 | {n} | 1     |   |
| f  | 2 | {n, f} | 2   |   |
| ↑  | 3 | {n, ↑, ↓} | 3   |   |
| ↓  | 3 | {n, ↑f} | 2   |   |
| ↑f | 2 | {n, ↓f} | 2   |   |
| ↓f | 2 | {n, f, ↑, ↓, ↑f, ↓f} | 6   |   |
(e) [Ogden, A.] $D_4$

$$D_4$$

| $g$  | $|g|$ | $H$                  | $|H|$ |
|------|------|----------------------|------|
| $R_0$ | 1    | $\{R_0\}$           | 1    |
| $R_{90}$ | 4    | $\{R_{180}, R_0\}$  | 2    |
| $R_{180}$ | 2    | $\{F_+, R_0\}$     | 2    |
| $R_{270}$ | 4    | $\{F_-, R_0\}$     | 2    |
| $F_+$   | 2    | $\{F_+, R_0\}$     | 2    |
| $F_-$   | 2    | $\{F_-, R_0\}$     | 2    |
| $F_\slash$ | 2    | $\{R_0, R_{180}, F_+, F_\slash\}$ | 4 |
| $F_\backslash$ | 2    | $\{R_0, R_{180}, F_-, F_\backslash\}$ | 4 |
|         |      | $\{R_{90}, R_{180}, R_{270}, R_0\}$ | 4 |

(f) [Smith, C.] Quaternions

Quaternions

| $g$  | $|g|$ | $H$                  | $|H|$ |
|------|------|----------------------|------|
| 1    | 1    | $\{1\}$             | 1    |
| $-1$ | 2    | $\{1, -1\}$         | 2    |
| $i$  | 4    | $\{1, -1, i, -i\}$  | 4    |
| $-i$ | 4    | $\{1, -1, j, -j\}$  | 4    |
| $j$  | 4    | $\{1, -1, k, -k\}$  | 4    |
| $-j$ | 4    | $\{1, -1, i, -i, j, -j, k, -k\}$ | 8 |
| $k$  | 4    |                      |      |
| $-k$ | 4    |                      |      |
4 Homework #5

1. [Berry, K.] List the six elements of $GL(2, \mathbb{Z}_2)$. Show that the group is not abelian.

The group $GL(2, \mathbb{Z}_2)$ is the set of $2 \times 2$ matrices with nonzero determinants with coefficients from the group $\mathbb{Z}_2 = \{0, 1\}$. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. The determinant of $A$ is $\det A = ad - bc$. If $ad - bc \neq 0$, then $A$ is nonsingular.

The six elements are

$$GL(2, \mathbb{Z}_2) = \left\{ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$

The group $GL(2, \mathbb{Z}_2)$ is not abelian, as it is not commutative. Taking two elements from the group and multiplying them together in a different order will not have the same result. For example:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

and

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Thus $GL(2, \mathbb{Z}_2)$ is not abelian.

2. [Cochran-Bjerke, L.] Find a cyclic subgroup of order 4 in $U(40)$.

$U(40)$ is all the numbers that are relatively prime to 40. Let’s start with 3 because 1 is the identity.

$3 \cdot 3 \equiv 9 \pmod{40}$

$3 \cdot 3 \cdot 3 \equiv 27 \pmod{40}$

$3 \cdot 3 \cdot 3 \cdot 3 \equiv 81 \pmod{40} = 1$

Since we get back to the identity 1 we can say:

$$\langle 3 \rangle = \{1, 3, 9, 27\},$$

and 3 creates a cyclic subgroup of order 4 of $U(40)$. 
3. [Deschamp, B.] Consider $G = GL(2, \mathbb{R})$.

(a) Find $C \left( \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right)$.

Note that we need to know when

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$ 

Or

$$\begin{bmatrix} a + b & a \\ c + d & c \end{bmatrix} = \begin{bmatrix} a + c & b + d \\ a & b \end{bmatrix}.$$ 

Equating entries yields

$$a + b = a + c \quad a = b + d \quad c + d = a \quad c = b.$$ 

Combining these results yields $b = a - d$, and so $c = a - d$. This information tells us

$$C \left( \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right) = \left\{ \begin{bmatrix} a & a - d \\ a - d & d \end{bmatrix} : a, d \in \mathbb{R} \text{ and } a, d \neq 0 \right\}.$$ 

(b) Find $C \left( \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right)$.

Note that we need to know when

$$\begin{bmatrix} e & f \\ g & h \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix}.$$ 

Or

$$\begin{bmatrix} g & h \\ e & f \end{bmatrix} = \begin{bmatrix} g & h \\ e & f \end{bmatrix}.$$ 

Equating entries yields

$$f = g \quad e = h \quad h = e \quad g = f.$$ 

Combining these results yields $f = g$ and $e = h$. This information tells us

$$C \left( \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right) = \left\{ \begin{bmatrix} e & f \\ f & e \end{bmatrix} : e, f \in \mathbb{R} \text{ and } e^2 - f^2 \neq 0 \right\}.$$ 

(c) Find $Z(G)$. Hint: Use (a) and (b) to limit your search by using Problem 6.

We know the center is equal to the intersection of the centralizers, and so any matrix in the center must also match the forms of the matrices found in (a) and (b). From (b) we learn that $a = d$ in (a). Also, it must be that $a - d = f$, but since $a$ is used elsewhere in (a), the only option is if $f = 0$. Then it must be that the only matrix that satisfies (a) and (b) has the form

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = aI.$$
5. [Cosand, K.] Prove that for each $H, K \subseteq G$, where $G$ is a group. Prove that

$$H \cap K = \{g \in G : g \in H \text{ and } g \in K\}$$

is a subgroup of $G$.

By the two-step subgroup test, we must show that

(a) $H \cap K$ is non-empty

(b) $\forall a, b \in H, K$, $a \circ b \in H \cap K$

(c) $\forall a \in H, K$, $a^{-1} \in H \cap K$

(a) By the definition of $H \cap K$, any element is in $H \cap K$ if and only if that element is in both $H$ and $K$. Because $H$ and $K$ are groups, they must, by definition, contain the identity: $e \in H, K$. Therefore $e \in H \cap K$ and $H \cap K$ is nonempty.

(b) Because $H$ and $K$ are groups, they are both closed: $a \circ b \in H$ and $a \circ b \in K$. It follows that $a \circ b \in H \cap K$.

(c) Because $H$ and $K$ are groups, they must, by definition, contain the inverse of all their elements: $\forall a \in H, K$, $a^{-1} \in H, K$ and $a^{-1} \in H \cap K$.

Because all parts have been proven, $H \cap K$ satisfies the two-step subgroup test, and $H \cap K$ is a group. Because $H$ and $K$ can only consist of elements of $G$, $H \cap K$ can only consist of elements of $G$, so $H \cap K \leq G : H \leq G$ and $K \leq G$.

4. [Gates, S.] Assume that $H, K \leq G$, where $G$ is a group. Prove that

$$H \cap K = \{g \in G : g \in H \text{ and } g \in K\}$$

is a subgroup of $G$.

By the two-step subgroup test, we must show that

(a) $H \cap K$ is non-empty

(b) $\forall a, b \in H, K$, $a \circ b \in H \cap K$

(c) $\forall a \in H, K$, $a^{-1} \in H \cap K$

(a) By the definition of $H \cap K$, any element is in $H \cap K$ if and only if that element is in both $H$ and $K$. Because $H$ and $K$ are groups, they must, by definition, contain the identity: $e \in H, K$. Therefore $e \in H \cap K$ and $H \cap K$ is nonempty.

(b) Because $H$ and $K$ are groups, they are both closed: $a \circ b \in H$ and $a \circ b \in K$. It follows that $a \circ b \in H \cap K$.

(c) Because $H$ and $K$ are groups, they must, by definition, contain the inverse of all their elements: $\forall a \in H, K$, $a^{-1} \in H, K$ and $a^{-1} \in H \cap K$.

Because all parts have been proven, $H \cap K$ satisfies the two-step subgroup test, and $H \cap K$ is a group. Because $H$ and $K$ can only consist of elements of $G$, $H \cap K$ can only consist of elements of $G$, so $H \cap K \leq G : H \leq G$ and $K \leq G$.

5. [Cosand, K.] Prove that for each $a$ in a group $G$ the centralizer of $a$, $C(a)$, is a subgroup of $G$.

Proof: Use the Two-step method. By the definition of a centralizer we know $C(a)$ is a subset of $G$, $a \circ C(a) \subseteq G$. We know the centralizer is nonempty because it contains the identity, $e \in C(a)$. We need to show: for every $b, c \in C(a)$ that (a) $b \circ c \in C(a)$ and (b) $b^{-1} \in C(a)$.

(a) Assume $b, c \in C(a)$. We know $b \circ a = a \circ b$ and $c \circ a = a \circ c$. We can now write $(b \circ c) \circ a = b \circ (c \circ a)$, by associativity. Then, $b \circ (c \circ a) = b \circ (a \circ c)$, since $c \in C(a)$. Next, $b \circ (a \circ c) = (b \circ a) \circ c$, by associativity. Finally, $(b \circ a) \circ c = (a \circ b) \circ c$, since $b \in C(a)$. We can now conclude that $a \circ (b \circ c) = (b \circ c) \circ a$, which means $b \circ c \in C(a)$.

(b) Take $b \in C(a)$. We know $b \circ a = a \circ b$. If we perform a left operation with $b^{-1}$, then $b^{-1} \circ b \circ a = b^{-1} \circ a \circ b$. This can be first simplified to $e \circ a = b^{-1} \circ a \circ b$, and then $a = b^{-1} \circ a \circ b$. Next, if we perform a right operation with $b^{-1}$, then $a \circ b^{-1} = b^{-1} \circ a \circ b \circ b^{-1}$. This can first be simplified to $a \circ b^{-1} = b^{-1} \circ a \circ c$, and then $a \circ b^{-1} = b^{-1} \circ a$. Therefore, we can conclude that $b^{-1} \in C(a)$. Thus, since $b \circ c \in C(a)$ and $b^{-1} \in C(a)$, by the Two-step test, $C(a) \leq G$. 

12
6. [Gruenig, S.] Let $G$ be a group. Show that

$$Z(G) = \bigcap_{a \in G} C(a).$$

In order for $Z(G) = \bigcap_{a \in G} C(a)$, we must show that (1) $Z(G)$ is a subset of $\bigcap_{a \in G} C(a)$, and (2) $\bigcap_{a \in G} C(a)$ is a subset of $Z(G)$.

(1) Consider $b \in Z(G)$. Since $b$ is an element of $Z(G)$, we know $g \circ b = b \circ g$ for all $g \in G$. Looking at the definition of the centralizer, $C(a) = \{ g \in G : g \circ a = a \circ g \}$, we can see that since $b$ is commutative with all $g \in G$ it belongs to the centralizer of every element in $G$. In other words, if $b$ is an element of $Z(G)$, it must also be an element of $\bigcap_{a \in G} C(a)$. Therefore, $Z(G) \subseteq \bigcap_{a \in G} C(a)$.

(2) Now consider $c \in \bigcap_{a \in G} C(a)$. Since $c \in C(a)$, we know that $c \circ a = a \circ c$. Furthermore, since $c$ is in $\bigcap_{a \in G} C(a)$, we know $c \circ a = a \circ c$ is true for all $a \in G$. And since $Z(G) = \{ g \in G : g \circ a = a \circ g, \forall a \in G \}$, $c$ must also be an element of $Z(G)$, and $\bigcap_{a \in G} C(a) \subseteq Z(G)$.

We’ve now shown that (1) $Z(G) \subseteq \bigcap_{a \in G} C(a)$ and that (2) $\bigcap_{a \in G} C(a) \subseteq Z(G)$. The only way this is possible is if the two sets are equal. Therefore $Z(G) = \bigcap_{a \in G} C(a)$.

7. [Norstedt, Z.] Prove that if an abelian group has more than three elements of order 2, then it has at least seven elements of order 2. Find an example that shows this is not true for non-abelian groups.

Let $G$ be an abelian group and $a, b, c, d \in G$ such that $|a|, |b|, |c|, |d| = 2$ and $a \neq b \neq c \neq d$.

Consider $a \circ b = f$, $a \circ c = g$, and $a \circ d = h$. Because $b \neq c \neq d$, then $f \neq g \neq h$. (Note that if $f = g$, then $a \circ b = a \circ c$, and then $a = c$, which cannot happen.) Next consider $f^2 = (a \circ b) \circ (a \circ b)$. Since $G$ is abelian, $f^2 = (a \circ a) \circ (b \circ b) = a^2 \circ b^2$. This is equivalent to $e \circ e = e$, due to the fact that $|a| = |b| = 2$. Thus, $f^2 = e$, and $|f| = 2$. This can be similarly shown for $g^2$ and $h^2$; only the symbols change.

Therefore, if an abelian group has more than three elements with order 2, it has at least seven elements with order 2.

For a non-abelian counter-example, consider $D_4$.

There are exactly five elements in $D_4$, $\{ R_{180}, F_x, F_y, F_x, F_y \}$, that have order 2. This is more than three and less than seven.
5 Homework #6

1. [Henson, T.] Let

\[ \alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix} \quad \text{and} \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}. \]

(a) Write \( \alpha \) and \( \beta \) as the product of disjoint cycles.

\( \alpha = (12345)(678), \beta = (1)(23847)(56) \)

(b) Compute \( \alpha \circ \beta \).

\[ \alpha \circ \beta = (12345)(678)(1)(23847)(56) = (12485736) \]

or \( \alpha \circ \beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 & 7 & 1 & 3 & 5 \end{bmatrix} \)

(c) Compute \( \beta \circ \alpha \).

\[ \beta \circ \alpha = (1)(23847)(56)(12345)(678) = (13746285) \]

or \( \beta \circ \alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 7 & 6 & 1 & 2 & 4 & 5 \end{bmatrix} \)

2. [Hjelmfelt, C.] Write the Cayley table for \( S_3 \).

<table>
<thead>
<tr>
<th></th>
<th>( \varepsilon )</th>
<th>(1)(23)</th>
<th>(2)(13)</th>
<th>(3)(12)</th>
<th>(123)</th>
<th>(132)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \varepsilon )</td>
<td>( \varepsilon )</td>
<td>(1)(23)</td>
<td>(2)(13)</td>
<td>(3)(12)</td>
<td>(123)</td>
<td>(132)</td>
</tr>
<tr>
<td>(1)(23)</td>
<td>(1)(23)</td>
<td>( \varepsilon )</td>
<td>(123)</td>
<td>(132)</td>
<td>(2)(13)</td>
<td>(3)(12)</td>
</tr>
<tr>
<td>(2)(13)</td>
<td>(2)(13)</td>
<td>(132)</td>
<td>( \varepsilon )</td>
<td>(123)</td>
<td>(3)(12)</td>
<td>(1)(23)</td>
</tr>
<tr>
<td>(3)(12)</td>
<td>(3)(12)</td>
<td>(123)</td>
<td>(132)</td>
<td>( \varepsilon )</td>
<td>(1)(23)</td>
<td>(2)(13)</td>
</tr>
<tr>
<td>(123)</td>
<td>(123)</td>
<td>(3)(12)</td>
<td>(1)(23)</td>
<td>(2)(13)</td>
<td>(132)</td>
<td>( \varepsilon )</td>
</tr>
<tr>
<td>(132)</td>
<td>(132)</td>
<td>(2)(13)</td>
<td>(3)(12)</td>
<td>(1)(23)</td>
<td>( \varepsilon )</td>
<td>(123)</td>
</tr>
</tbody>
</table>
3. [Quasney, R.] Suppose that a group is generated by two elements $a$ and $b$ (meaning if $S = \{a, b\}$, then $G = \langle S \rangle$). Given that $a^3 = b^2 = e$ and $b \circ a^2 = a \circ b$, construct the Cayley table for the group. You will need to show your work for these computations. Associativity will play a prominent role in these computations, and your work should reflect its use.

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
<th>$a^2$</th>
<th>$a \circ b$</th>
<th>$b \circ a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
<td>$a^2$</td>
<td>$a \circ b$</td>
<td>$b \circ a$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$a^2$</td>
<td>$a \circ b$</td>
<td>$e$</td>
<td>$b \circ a$</td>
<td>$b$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$b \circ a$</td>
<td>$e$</td>
<td>$a \circ b$</td>
<td>$a^2$</td>
<td>$a$</td>
</tr>
<tr>
<td>$a^2$</td>
<td>$a^2$</td>
<td>$e$</td>
<td>$b \circ a$</td>
<td>$a$</td>
<td>$b$</td>
<td>$a \circ b$</td>
</tr>
<tr>
<td>$a \circ b$</td>
<td>$a \circ b$</td>
<td>$b$</td>
<td>$a \circ a$</td>
<td>$e$</td>
<td>$a^2$</td>
<td></td>
</tr>
<tr>
<td>$b \circ a$</td>
<td>$b \circ a$</td>
<td>$a \circ b$</td>
<td>$a^2$</td>
<td>$b$</td>
<td>$a$</td>
<td>$e$</td>
</tr>
</tbody>
</table>

First, we determine out elements can be $e, a, b, a^2, a \circ b, b \circ a, b \circ a^2, a^2 \circ b$. We can remove $b \circ a^2$ since we know it equals $a \circ b$. Also, we can remove $a^2 \circ b$ because:

\[
a \circ b = b \circ a^2
\]
\[
(a^2 \circ a) \circ b = a^2 \circ (b \circ a^2)
\]
\[
a^3 \circ b = a^2 \circ b \circ a^2
\]
\[
e \circ b = a^2 \circ b \circ a^2
\]
\[
b = a^2 \circ b \circ a^2
\]
\[
b \circ a = a^2 \circ b \circ (a^2 \circ a)
\]
\[
b \circ a = a^2 \circ b \circ a^3
\]
\[
b \circ a = a^2 \circ b \circ e
\]
\[
b \circ a = a^2 \circ b
\]

Non-obvious calculations:

(a)

\[
a \circ (a \circ b) = (a \circ a) \circ b
\]
\[
= a^2 \circ b
\]
\[
= b \circ a
\]

(b)

\[
a \circ (b \circ a) = a \circ (a^2 \circ b)
\]
\[
= (a \circ a^2) \circ b
\]
\[
= a^3 \circ b
\]
\[
= e \circ b
\]
\[
= b
\]

15
(c) \[ b \circ (a \circ b) = b \circ (b \circ a^2) \]
\[ = (b \circ b) \circ a^2 \]
\[ = b^2 \circ a^2 \]
\[ = e \circ a^2 \]
\[ = a^2 \]

(d) \[ b \circ (b \circ a) = (b \circ b) \circ a \]
\[ = b^2 \circ a \]
\[ = e \circ a \]
\[ = a \]

(e) \[ a^2 \circ a^2 = a \circ a \circ a \circ a \]
\[ = (a \circ a \circ a) \circ a \]
\[ = a^3 \circ a \]
\[ = e \circ a \]
\[ = a \]

(f) \[ a^2 \circ (a \circ b) = (a^2 \circ a) \circ b \]
\[ = a^3 \circ b \]
\[ = e \circ b \]
\[ = b \]

(g) \[ a^2 \circ (b \circ a) = (a^2 \circ b) \circ a \]
\[ = (b \circ a) \circ a \]
\[ = b \circ (a \circ a) \]
\[ = b \circ a^2 \]
\[ = a \circ b \]

(h) \[ (a \circ b) \circ a = (b \circ a^2) \circ a \]
\[ = b \circ (a^2 \circ a) \]
\[ = b \circ a^3 \]
\[ = b \circ e \]
\[ = b \]

(i) \[ (a \circ b) \circ b = a \circ (b \circ b) \]
\[ = a \circ b^2 \]
\[ = a \circ e \]
\[ = a \]
(j) \[ (a \circ b) \circ (a \circ b) = (a \circ b) \circ (b \circ a^2) \]
\[ = a \circ (b \circ b) \circ a^2 \]
\[ = a \circ b^2 \circ a^2 \]
\[ = a \circ e \circ a^2 \]
\[ = a \circ a^2 \]
\[ = a^3 \]
\[ = e \]

(k) \[ (a \circ b) \circ (b \circ a) = a \circ (b \circ b) \circ a \]
\[ = a \circ b^2 \circ a \]
\[ = a \circ e \circ a \]
\[ = a \circ a \]
\[ = a^2 \]

(l) \[ (b \circ a) \circ a = b \circ (a \circ a) \]
\[ = b \circ a^2 \]
\[ = a \circ b \]

(m) \[ (b \circ a) \circ b = (a^2 \circ b) \circ b \]
\[ = a^2(b \circ b) \]
\[ = a^2 \circ b^2 \]
\[ = a^2 \circ e \]
\[ = a^2 \]

(n) \[ (b \circ a) \circ a^2 = b \circ (a \circ a^2) \]
\[ = b \circ a^3 \]
\[ = b \circ e \]
\[ = b \]

(o) \[ (b \circ a) \circ (a \circ b) = b \circ (a \circ a) \circ b \]
\[ = (b \circ a^2) \circ b \]
\[ = (a \circ b) \circ b \]
\[ = a \circ (b \circ b) \]
\[ = a \circ b^2 \]
\[ = a \circ e \]
\[ = a \]
(p)
\[(b \circ a) \circ (b \circ a) = (a^2 \circ b) \circ (b \circ a)\]
\[= a^2 \circ (b \circ b) \circ a\]
\[= a^2 \circ b^2 \circ a\]
\[= a^2 \circ e \circ a\]
\[= a^2 \circ a\]
\[= a^3\]
\[= e\]

4. [Cosand, K.] Find the order of the following permutations.

(a) \((14)\)
\[(14) \circ (14) = (1)(4)\]
\[|(14)| = 2\]

(b) \((147)\)
\[(147) \circ (147) = (174)\]
\[(147) \circ (147) \circ (147) = (1)(4)(7)\]
\[|(147)| = 3\]

(c) \((14762)\)
\[(14762) \circ (14762) = (17246)\]
\[(14762) \circ (14762) \circ (14762) = (16427)\]
\[(14762) \circ (14762) \circ (14762) \circ (14762) = (1)(4)(7)(6)(2)\]
\[|(14762)| = 5\]

(d) Use (a), (b), and (c) to develop and prove a lemma concerning the order of \(\alpha = (a_1a_2\cdots a_k)\).

Hint: Use the fact that \(\alpha(a_i) = a_{i+1}\), for \(1 \leq i < k\), and \(\alpha(a_k) = a_1\).

Lemma: The order of a cycle \(\alpha = (a_1a_2\cdots a_k)\) is \(k\), or the length of the cycle.

Proof: Consider the element \(a_i\). Then, \(\alpha = (a_1a_2\cdots a_i\cdots a_k)\). To permute from \(a_i\) to \(a_k\) we can write \(\alpha^{k-i}(a_i) = a_k\), and we know we will never cycle back to \(a_i\). To permute from \(a_k\) back to \(a_1\) we know this takes one permutation so \(\alpha^1(a_k) = a_1\), and we do not ever get to \(a_i\). Finally, to permute from \(a_1\) to \(a_i\), we know the number of permutations necessary is \(i - 1\) so \(\alpha^{i-1}(a_1) = a_i\). We can apply all of these ideas to each \(a_i\). Putting all of this together, \(\alpha^k(a_i) = \alpha^{i-1}(\alpha(\alpha^{k-i}(a_1))) = \alpha^{i-1}(\alpha(a_k)) = \alpha^{i-1}(a_1) = a_i\). Therefore, the order of a cycle \(\alpha = (a_1a_2\cdots a_k)\) is \(k\).
5. [Keene, L.] Prove the following statements concerning order in groups.

(a) Prove that in a group an element and its inverse have the same order.

Proof: To prove that in a given group, an element and its inverse have the same order, let $G$ be a group with the element $a \in G$. Let

$$|a| = n$$

and so

$$a^n = e.$$ 

By applying $a^{-1}$ to each side of the equation $n$ times (as follows)

$$\underbrace{a \circ a \circ a \cdots a}_{n \text{ times}} = e$$

$$\underbrace{a \circ a \circ a \cdots a \circ a^{-1}}_{n-1 \text{ times}} = e \circ a^{-1}$$

$$\underbrace{a \circ a \circ a \cdots a \circ e}_{n-1 \text{ times}} = a^{-1}$$

$$\underbrace{a \circ a \circ a \cdots a \circ a^{-1}}_{n-1 \text{ times}} = a^{-1} \circ a^{-1}$$

$$\underbrace{a \circ a \circ a \cdots a \circ e}_{n-2 \text{ times}} = a^{-1} \circ a^{-1}$$

$$\vdots$$

$$\underbrace{a_1 \circ a^{-1}}_{n \text{ times}} = \underbrace{a^{-1} \circ a^{-1} \cdots a^{-1} \cdots a^{-1}}_{n \text{ times}}$$

$$e = \underbrace{a^{-1} \circ a^{-1} \cdots a^{-1} \cdots a^{-1}}_{n \text{ times}}$$

$$e = (a^{-1})^n$$

$$|a^{-1}| = n.$$ 

Note that $n$ is the smallest integer for which this is true. Thus we can determine that

$$|a| = |a^{-1}|.$$ 

By this logic, we have determined that, in a given group, an element and its inverse have the same order.

(b) Prove that in any group $G$, for $a, b \in G$, $|a \circ b| = |b \circ a|$.

Proof: To prove that in any group $G$ for $a, b \in G$, that $|a \circ b| = |b \circ a|$. Let

$$|a \circ b| = n$$

$$\underbrace{(a \circ b) \circ (a \circ b) \cdots (a \circ b) \circ (a \circ b)}_{n \text{ times}} = e$$
By the definition of a group, we know that operations are associative. Because of this fact, we can rearrange the equation to the following.

\[
\underbrace{(a \circ b) \circ (a \circ b) \circ \cdots \circ (a \circ b)}_{n \text{ times}} \circ (a \circ b) = e
\]

\[
\underbrace{a \circ (b \circ a) \circ (b \cdots a) \circ (b \circ a)}_{n-1 \text{ times}} \circ a \circ (b \circ a)^{n-1} \circ b = a^{-1} \circ e
\]

\[
e \circ (b \circ a)^{n-1} \circ b = a^{-1} \circ e
\]

\[
(b \circ a)^{n-1} \circ b \circ a = a^{-1} \circ a
\]

\[
(b \circ a)^{n-1} \circ (b \circ a) = e
\]

Then

\[
(a \circ b)^n = e,
\]

and so

\[
|a \circ b| = n.
\]

By this logic, we have determined that

\[
|a \circ b| = n = |b \circ a|.
\]

We now know that the order of \(a \circ b\) is equal to the order of \(b \circ a\).

(c) If \(a, b,\) and \(c\) are elements of a group, give an example to show that it need not be the case that

\[
|a \circ b \circ c| = |c \circ b \circ a|.
\]

Hint: look in \(D_4\).

In \(D_4\), let \(a, b,\) and \(c\) be assigned as follows:

\[
a = R_{90}, \quad b = F_{\\setminus}, \quad c = F_{\\setminus}.
\]

\[
|a \circ b \circ c| = R_{90} \circ F_{\\setminus} \circ F_{\\setminus} = R_0, \quad \text{and} \quad |R_0| = 1.
\]

\[
|c \circ b \circ a| = F_{\\setminus} \circ F_{\\setminus} \circ R_{90} = R_{180}, \quad \text{and} \quad |R_{180}| = 2.
\]

We have therefore proven that \(|a \circ b \circ c|\) does not necessarily equal \(|c \circ a \circ b|\) in a given group \(G\).
6 Homework #7

1. [Bachwich, A.] Determine whether the following permutations are even or odd. Show your work.

(a) (135)
Solution: (135) = (31)(35). Since (135) can be expressed as the product of two transpositions, it is even.

(b) (1356)
Solution: (1356) = (53)(51)(56). Since (1356) can be expressed as the product of three transpositions, it is odd.

(c) (13567)
Solution: (13567) = (65)(63)(61)(67). Since (1356) can be expressed as the product of four transpositions, it is even.

(d) (12)(134)(152)
Solution: (12)(134)(152) = (234)(51) = (15)(32)(34). Since (12)(134)(152) can be expressed as the product of three transpositions, it is odd.

(e) (1243)(3521)
Solution: (1243)(3521) = (1)(2)(354) = (12)(21)(53)(54). Since (1243)(3521) can be expressed as the product of four transpositions, it is even.
2. [Carroll, S.] In $S_4$, find a cyclic subgroup of order 4 and a noncyclic subgroup of order 4.

Cyclic subgroup: Let $\alpha = (1234)$. Then $\alpha^2 = (13)(24)$, $\alpha^3 = (1432)$ and $\alpha^4 = (1)(2)(3)(4)$, since a single element in this set can generate all the other elements in the set, it is cyclic. To prove it’s a subgroup make a Cayley Table and check for closure.

Cayley Table for Cyclic Set:

<table>
<thead>
<tr>
<th></th>
<th>$(1)(2)(3)(4)$</th>
<th>$(1234)$</th>
<th>$(13)(24)$</th>
<th>$(1432)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1432)$</td>
<td>$(1432)$</td>
<td>$(1)(2)(3)(4)$</td>
<td>$(1234)$</td>
<td>$(13)(24)$</td>
</tr>
</tbody>
</table>

We have closure, so this is a cyclic subgroup of order 4.


If $\alpha = (12)(34)$ then $\alpha^2 = (1)(2)(3)(4)$

If $\beta = (13)(24)$ then $\beta^2 = (1)(2)(3)(4)$.

If $\gamma = (14)(23)$ then $\gamma^2 = (1)(2)(3)(4)$.

Therefore no element can operate on itself to generate the other elements in the set. To prove it’s a subgroup, make a Cayley Table and check for closure.

Cayley Table for Noncyclic Set:

|-------|----------------|-----------|------------|----------|

We have closure, so this is a noncyclic subgroup of order 4. Note that since each element is its own inverse all other elements in the subgroup are required to complete this subgroup of order 4, any one element operating on itself will only yield the identity and itself therefore it is noncyclic.
3. [Cosand, K.] Let \( n \) be a positive integer. If \( n \) is odd, is an \( n \)-cycle an odd or an even permutation? If \( n \) is even, is an \( n \)-cycle an odd or an even permutation? Prove your result.

Proof: Let \( \alpha = (a_1a_2\cdots a_{n-1}a_n) \). We know \( \alpha \) can be written as the product of transpositions, \( \alpha = (a_1a_n)(a_1a_{n-1})\cdots(a_1a_3)(a_1a_2) \). Since we have \( n \) symbols, we know we must have \( n-1 \) transpositions because \( a_1 \) pairs exactly once with each of the other symbols. Therefore, if \( n \) is odd, then \( n-1 \) is even, and we can conclude the \( n \)-cycle is an even permutation. Similarly, if \( n \) is even, then \( n-1 \) is odd, and we can conclude the \( n \)-cycle is an odd permutation.

4. [Cosand, K.] Develop and prove a lemma that computes \((a_1a_2\cdots a_k)^{-1}\).

Lemma: \((a_1a_2\cdots a_k)^{-1} = (a_ka_{k-1}\cdots a_2a_1)\).

Proof: Let \( \alpha_1 = (a_1a_2\cdots a_k) \), and \( \alpha_2 = (a_ka_{k-1}\cdots a_2a_1) \). We need to show \( \alpha_1 \circ \alpha_2 = \varepsilon \).

1. Take \( \alpha_1 \) and \( \alpha_2 \) and decompose them into transpositions.
2. Take \( \alpha_1 \circ \alpha_2 \) and determine if they equal \( \varepsilon \).

Showing 1:

\[
\alpha_1 = (a_1a_2\cdots a_k) = (a_1a_k)(a_1a_{k-1})\cdots(a_1a_3)(a_1a_2)
\]

and

\[
\alpha_2 = (a_ka_{k-1}\cdots a_2a_1) = (a_1a_ka_{k-1}\cdots a_3a_2) = (a_1a_2)(a_1a_3)\cdots(a_1a_{k-1})(a_1a_k).
\]

Now, to show 2:

\[
\alpha_1 \circ \alpha_2 = (a_1a_k)(a_1a_{k-1})\cdots(a_1a_3)(a_1a_2)(a_1a_2)(a_1a_3)\cdots(a_1a_{k-1})(a_1a_k).
\]

We know \((a_ia_j)(a_ia_j) = \varepsilon\). Therefore, in the middle of the composition, we can see the last transposition for \( \alpha_1 \) is \((a_1a_2)\) and the first transposition for \( \alpha_2 \) is \((a_1a_2)\). Thus, we know \((a_1a_2)(a_1a_2) = \varepsilon\). The next two transpositions next to each other would be \((a_1a_3)\) and \((a_1a_3)\), which also reduces to \( \varepsilon \). By continuing this process until we reduce each pair of transpositions to \( \varepsilon \), we eventually see \( \alpha_1 \circ \alpha_2 = \varepsilon \). We know inverses are unique and we found one, so this must be the inverse. Therefore, we can conclude \((a_1a_2\cdots a_k)^{-1} = (a_ka_{k-1}\cdots a_2a_1)\).
5. [Gates, S.] Prove that \( A_n \) is a subgroup of \( S_n \).

By the two-step subgroup test, we must show that

\[
\begin{align*}
A_n & \subseteq S_n & (1) \\
A_n & \text{ is non-empty} & (2) \\
\forall \alpha, \beta \in A_n, \ & \alpha \circ \beta \in A_n & (3) \\
\forall \alpha \in A_n, \ & \alpha^{-1} \in A_n & (4)
\end{align*}
\]

By the definition of \( A_n \), any element is in \( A_n \) if and only if that element is in \( S_n \) and is even, so we know \( A_n \subseteq S_n \), proving \( 1 \).

The identity, \( \varepsilon \), was proven to be even. This means \( \varepsilon \in A_n \) and \( A_n \) is non-empty, so \( 2 \) has been proven.

Consider \( \alpha = (a_1a_2 \cdots a_k) \) and \( \beta = (b_1b_2 \cdots b_j) \). Because \( \alpha, \beta \in A_n \), \( \alpha \) and \( \beta \) are even, meaning they can be decomposed to an even number of transpositions:

\[
\begin{align*}
\alpha &= (a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2), \\
\beta &= (b_1b_j)(b_1b_{j-1}) \cdots (b_1b_2).
\end{align*}
\]

Following this, we have:

\[
\alpha \circ \beta = (a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)(b_1b_j)(b_1b_{j-1}) \cdots (b_1b_2).
\]

The product has the number of transpositions from \( \alpha \) plus the number of transpositions from \( \beta \). Because both of these numbers are even, the sum of these two numbers is even. Therefore \( \alpha \circ \beta \) is even, and \( \alpha \circ \beta \in A_n \), proving \( 3 \).

First, write \( \alpha \) as the product of disjoint cycles

\[
\alpha = \alpha_1 \alpha_2 \cdots \alpha_k,
\]

where each \( \alpha_i \) is a cycle. Second, consider, from homework 7 problem 4, that the inverse of a cycle uses the same number of transpositions as the original cycle. This means \( \alpha^{-1} \) must have the same number of transpositions as \( \alpha \). Thus, if \( \alpha \) had can be written as an even number of transpositions, then \( \alpha^{-1} \) can also be written as an even number of transpositions. Therefore, \( \alpha^{-1} \in A_n \), and \( 4 \) is proven.

Because \( 1, 2, 3, \) and \( 4 \) have been proven, \( A_n \) satisfies the Two-step subgroup test, and \( A_n \leq S_n \).