1 Homework #8

1. [Berry, K.] Find all isomorphic finite groups in our Group Atlas. Justify your work.

There are 18 groups within the group atlas. We can eliminate isomorphisms between groups that do not have the same order. By grouping these groups based on their order we can see,

Groups of order 3: \( A_3 \)

Groups of order 4: \((\mathbb{Z}_4, +), U(10), \text{Color-4}, \text{Rigid-body-motion-of-a-rectangle}, \text{and Klein-four}\)

Groups of order 5: \( (\mathbb{Z}_5, +), \text{Color-5} \)

Groups of order 6: \( D_3, (\mathbb{Z}_6, +), GL(2, \mathbb{Z}_2), S_3, \text{Color-6}, \text{and Hexaflexagon} \)

Groups of order 8: \( D_4, \text{Quaternions} \)

Groups of order 10: \( D_5 \)

Groups of order 12: \( A_4 \)

The groups in red and underlined are abelian. By properties of isomorphisms, we know that groups of the same order that are abelian can be isomorphisms. By definition we know that to be isomorphic the elements within the groups must also be of the same order. Using the group atlas we can see that,

\((\mathbb{Z}_4, +) \simeq U(10) \simeq \text{Color-4}\)

<table>
<thead>
<tr>
<th>( (\mathbb{Z}_4, +) )</th>
<th>( (\mathbb{Z}_4, +) )</th>
<th>Color – 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>Blue</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>Green</td>
</tr>
<tr>
<td>2</td>
<td>9</td>
<td>Yellow</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>Red</td>
</tr>
</tbody>
</table>

| 0, 1, Blue             | 1, 7, Green             | 2, 9, Yellow | 3, 3, Red |
| 1, 7, Green            | 1, 7, Green             | 2, 9, Yellow | 3, 3, Red |
| 2, 9, Yellow           | 2, 9, Yellow            | 3, 3, Red   | 0, 1, Blue |
| 3, 3, Red              | 3, 3, Red               | 0, 1, Blue  | 1, 7, Green |
| 0, 1, Blue             | 1, 7, Green             | 2, 9, Yellow | 3, 3, Red |
| 1, 7, Green            | 1, 7, Green             | 2, 9, Yellow | 3, 3, Red |
| 2, 9, Yellow           | 2, 9, Yellow            | 3, 3, Red   | 0, 1, Blue |
| 3, 3, Red              | 3, 3, Red               | 0, 1, Blue  | 1, 7, Green |
| 0, 1, Blue             | 1, 7, Green             | 2, 9, Yellow | 3, 3, Red |
The mapping of Rigid-body motions of a rectangle $\simeq$ Klein-four is as follows,

$$
\begin{array}{c|cccc}
\text{Rectangle} & \text{Klein - 4} \\
\hline
R_0 & a \\
R_{180} & b \\
F_1 & c \\
F_- & d \\
\end{array}
$$

$$
\begin{array}{c|cccc}
R_0, a & R_{180}, b & F_1, c & F_-, d \\
\hline
R_0, a & R_{180}, b & F_1, c & F_-, d \\
R_{180}, b & R_0, a & F_-, d & F_1, c \\
F_1, c & F_-, d & R_0, a & R_{180} \\
F_-, c & F_1, c & R_{180} & R_0, a \\
\end{array}
$$

The mapping of $(\mathbb{Z}_5, +) \simeq \text{Color-5}$ is as follows,

$$
\begin{array}{c|c|c|c|c|c}
(\mathbb{Z}_5, +) & \text{Color - 5} \\
\hline
0 & \text{Clear} \\
1 & \text{Orange} \\
2 & \text{Oxblood} \\
3 & \text{Red} \\
4 & \text{Blue} \\
\end{array}
$$

$$
\begin{array}{c|c|c|c|c|c|c}
0, \text{Clear} & 1, \text{Orange} & 2, \text{Oxblood} & 3, \text{Red} & 4, \text{Blue} \\
\hline
0, \text{Clear} & 0, \text{Clear} & 1, \text{Orange} & 2, \text{Oxblood} & 3, \text{Red} & 4, \text{Blue} \\
1, \text{Orange} & 1, \text{Orange} & 2, \text{Oxblood} & 3, \text{Red} & 4, \text{Blue} & 0, \text{Clear} \\
2, \text{Oxblood} & 2, \text{Oxblood} & 3, \text{Red} & 4, \text{Blue} & 0, \text{Clear} & 1, \text{Orange} \\
3, \text{Red} & 3, \text{Red} & 4, \text{Blue} & 0, \text{Clear} & 1, \text{Orange} & 2, \text{Oxblood} \\
4, \text{Blue} & 4, \text{Blue} & 0, \text{Clear} & 1, \text{Orange} & 2, \text{Oxblood} & 3, \text{Red} \\
\end{array}
$$

The mapping of $(\mathbb{Z}_6, +) \simeq \text{Color-6}$ is as follows,

$$
\begin{array}{c|c|c|c|c|c|c}
(\mathbb{Z}_6, +) & \text{Color - 6} \\
\hline
0 & \text{Yellow} \\
1 & \text{Pumpkin} \\
2 & \text{Lavender} \\
3 & \text{Red} \\
4 & \text{Blue} \\
5 & \text{Green} \\
\end{array}
$$

$$
\begin{array}{c|c|c|c|c|c|c}
0, \text{Yellow} & 1, \text{Pumpkin} & 2, \text{Lavender} & 3, \text{Red} & 4, \text{Blue} & 5, \text{Green} \\
\hline
0, \text{Yellow} & 0, \text{Yellow} & \text{Pumpkin} & 2, \text{Lavender} & 3, \text{Red} & 4, \text{Blue} & 5, \text{Green} \\
1, \text{Pumpkin} & 1, \text{Pumpkin} & 2, \text{Lavender} & 3, \text{Red} & 4, \text{Blue} & 5, \text{Green} & 0, \text{Yellow} \\
2, \text{Lavender} & 2, \text{Lavender} & 3, \text{Red} & 4, \text{Blue} & 5, \text{Green} & 0, \text{Yellow} & 1, \text{Pumpkin} \\
3, \text{Red} & 3, \text{Red} & 4, \text{Blue} & 5, \text{Green} & 0, \text{Yellow} & 1, \text{Pumpkin} & 2, \text{Lavender} \\
4, \text{Blue} & 4, \text{Blue} & 5, \text{Green} & 0, \text{Yellow} & 1, \text{Pumpkin} & 2, \text{Lavender} & 3, \text{Red} \\
5, \text{Green} & 5, \text{Green} & 0, \text{Yellow} & 1, \text{Pumpkin} & 2, \text{Lavender} & 3, \text{Red} & 4, \text{Blue} \\
\end{array}
$$
Exploring the remaining groups we find that, $D_3 \simeq S_3 \simeq \text{Hexaflexagon} \simeq GL(2,\mathbb{Z}_2)$ . The mapping follows,

<table>
<thead>
<tr>
<th>$D_3$</th>
<th>$S_3$</th>
<th>Hexaflexagon</th>
<th>$GL(2,\mathbb{Z}_2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_0$</td>
<td>$\varepsilon$</td>
<td>$n$</td>
<td>$I$</td>
</tr>
<tr>
<td>$R_{120}$ (123)</td>
<td>$\uparrow$</td>
<td>$A$</td>
<td></td>
</tr>
<tr>
<td>$R_{240}$ (321)</td>
<td>$\downarrow$</td>
<td>$B$</td>
<td></td>
</tr>
<tr>
<td>$F_1$ (23)</td>
<td>$f$</td>
<td>$C$</td>
<td></td>
</tr>
<tr>
<td>$F_2$ (13)</td>
<td>$\uparrow_f$</td>
<td>$D$</td>
<td></td>
</tr>
<tr>
<td>$F_3$ (12)</td>
<td>$\downarrow_f$</td>
<td>$E$</td>
<td></td>
</tr>
</tbody>
</table>

2. [Brubaker, N.] Find a subgroup of $S_4$ isomorphic to $D_4$. Justify your work.

Let $\phi$ be a bijective function that maps elements from $D_4$ to a subgroup of $S_4$, and call this subgroup $P(D_4)$.

$$\phi : D_4 \rightarrow P(D_4) = \left[ \begin{array}{cccccccc} R_0 & R_{90} & R_{180} & R_{270} & F_{14} & F_{12} & F_{13} & F_{24} \\ \varepsilon & (1234) & (13)(24) & (1432) & (14)(23) & (12)(34) & (13)(24) & (1)(3)(24) \end{array} \right]$$

To show that $\phi$ is an isomorphism we need to show that it is bijective, and that it preserves the operation from $D_4$. By definition, $\phi$ is bijective. To show that $\phi$ preserves the operation in $D_4$, we need the Cayley tables to be identical in structure, which can be seen below.

<table>
<thead>
<tr>
<th>$D_4$</th>
<th>$R_0$</th>
<th>$R_{90}$</th>
<th>$R_{180}$</th>
<th>$R_{270}$</th>
<th>$F_1$</th>
<th>$F_{-}$</th>
<th>$F_\Box$</th>
<th>$F/$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_0$</td>
<td>$R_0$</td>
<td>$R_{90}$</td>
<td>$R_{180}$</td>
<td>$R_{270}$</td>
<td>$F_1$</td>
<td>$F_{-}$</td>
<td>$F_\Box$</td>
<td>$F/$</td>
</tr>
<tr>
<td>$R_{90}$</td>
<td>$R_{90}$</td>
<td>$R_{180}$</td>
<td>$R_{270}$</td>
<td>$R_0$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
</tr>
<tr>
<td>$R_{180}$</td>
<td>$R_{180}$</td>
<td>$R_{270}$</td>
<td>$R_0$</td>
<td>$R_{90}$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
</tr>
<tr>
<td>$R_{270}$</td>
<td>$R_{270}$</td>
<td>$R_0$</td>
<td>$R_{90}$</td>
<td>$R_{180}$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
</tr>
<tr>
<td>$F_1$</td>
<td>$F_1$</td>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
<td>$F_/ F_\Box$</td>
<td>$R_0$</td>
<td>$R_{180}$</td>
<td>$R_{90}$</td>
<td>$R_{270}$</td>
</tr>
<tr>
<td>$F_{-}$</td>
<td>$F_{-}$</td>
<td>$F_/ F_\Box$</td>
<td>$F_/ F_\Box$</td>
<td>$R_{180}$</td>
<td>$R_0$</td>
<td>$R_{270}$</td>
<td>$R_{90}$</td>
<td></td>
</tr>
<tr>
<td>$F_\Box$</td>
<td>$F_\Box$</td>
<td>$F_/ F_\Box$</td>
<td>$F_/ F_\Box$</td>
<td>$R_{270}$</td>
<td>$R_{90}$</td>
<td>$R_0$</td>
<td>$R_{180}$</td>
<td></td>
</tr>
<tr>
<td>$F/$</td>
<td>$F_/ F_\Box$</td>
<td>$F_/ F_\Box$</td>
<td>$F_/ F_\Box$</td>
<td>$R_{270}$</td>
<td>$R_{90}$</td>
<td>$R_0$</td>
<td>$R_{180}$</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P(D_4)$</th>
<th>$\varepsilon$</th>
<th>(1234)</th>
<th>(13)(24)</th>
<th>(1432)</th>
<th>(12)(34)</th>
<th>(14)(23)</th>
<th>(24)</th>
<th>(13)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\varepsilon$</td>
<td>$\varepsilon$</td>
<td>(1234)</td>
<td>(13)(24)</td>
<td>(1432)</td>
<td>(12)(34)</td>
<td>(14)(23)</td>
<td>(24)</td>
<td>(13)</td>
</tr>
<tr>
<td>(1234)</td>
<td>(1234)</td>
<td>(13)(24)</td>
<td>(1432)</td>
<td>$\varepsilon$</td>
<td>(13)</td>
<td>(24)</td>
<td>(12)(34)</td>
<td>(14)(23)</td>
</tr>
<tr>
<td>(24)</td>
<td>(24)</td>
<td>(14)(23)</td>
<td>(13)</td>
<td>(12)(34)</td>
<td>(1432)</td>
<td>(1234)</td>
<td>$\varepsilon$</td>
<td>(13)(24)</td>
</tr>
<tr>
<td>(13)</td>
<td>(13)</td>
<td>(12)(34)</td>
<td>(24)</td>
<td>(14)(23)</td>
<td>(1234)</td>
<td>(1432)</td>
<td>(13)(24)</td>
<td>$\varepsilon$</td>
</tr>
</tbody>
</table>
3. [Conger, A.]

(a) Show that $U(8)$ is not isomorphic to $U(10)$.

$U(8) = \{1, 3, 5, 7\}$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>7</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

$U(10) = \{1, 3, 7, 9\}$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>3</th>
<th>7</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>1</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

These groups are not isomorphic because in $U(8)$: $|1| = |3| = |5| = |7| = 2$. In $U(10)$: $|1| = |9| = 2$ and $|3| = |7| = 4$. Since $U(8)$ has no elements of order 4, we cannot map $U(8)$ to $U(10)$. Thus they are not isomorphic.

(b) Show that $U(8)$ is isomorphic to $U(12)$.

$U(8) = \{1, 3, 5, 7\}$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>7</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

$U(12) = \{1, 5, 7, 11\}$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>5</th>
<th>7</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>1</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

These groups are isomorphic since they share a Cayley table and are bijective if mapped as

1 → 1
3 → 5
5 → 7
7 → 11

(c) Prove or disprove that $U(20)$ and $U(24)$ are isomorphic.

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$

$U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$

In $U(24)$, the element 1 has order 1 and all other elements have order 2. In $U(20)$, the element 3 has order 4. Since $U(20)$ has an element of order 4 but $U(24)$ does not, the two groups cannot be isomorphic because isomorphic groups preserve order.
4. [Gruenig, S.] Find a homomorphism \( \phi \) from \( U(30) \) to \( U(30) \) with kernel \{1, 11\} and \( \phi(7) = 7 \).

We know that \( \phi(1) = 1 \), \( \phi(11) = 1 \), and \( \phi(7) = 7 \). Working in \( U(30) \) we know that \( 7 \circ 11 = 17 \). Then

\[
\phi(7) \circ \phi(11) = \phi(17) \\
7 \circ 1 = \phi(17) \\
7 = \phi(17).
\]

So \( \phi(17) = 7 \). Similarly, we can find the remaining four elements:

\( \phi(29) \):

\[
\phi(7) \circ \phi(17) = \phi(29) \\
7 \circ 7 = \phi(29) \\
19 = \phi(29).
\]

\( \phi(19) \):

\[
\phi(19) \circ \phi(11) = \phi(29) \\
\phi(19) \circ 1 = 19 \\
\phi(19) = 19.
\]

\( \phi(13) \):

\[
\phi(7) \circ \phi(19) = \phi(23) \\
7 \circ 19 = \phi(13) \\
13 = \phi(13).
\]

\( \phi(23) \):

\[
\phi(13) \circ \phi(11) = \phi(23) \\
13 \circ 1 = \phi(23) \\
13 = \phi(23).
\]

Thus, the homomorphism \( \phi \) is defined as follows:

\[
\begin{align*}
\phi(1) &= 1 \\
\phi(7) &= 7 \\
\phi(13) &= 13 \\
\phi(19) &= 19 \\
\phi(11) &= 1 \\
\phi(17) &= 7 \\
\phi(23) &= 13 \\
\phi(29) &= 19
\end{align*}
\]

\[
\begin{array}{c|cccc}
* & 1 & 7 & 13 & 19 \\
\hline
1 & 1 & 7 & 13 & 19 \\
7 & 7 & 19 & 1 & 13 \\
13 & 13 & 1 & 19 & 7 \\
19 & 19 & 13 & 7 & 1
\end{array}
\]

Note that the above Cayley table is also valid for the factor group \( U(30)/\ker(\phi) \), where the symbols of the Cayley table are representatives of the distinct left (or right) cosets of \( \ker(\phi) \) in \( U(30) \).
5. [Havelka, R.] If $\phi$ is a homomorphism from $G$ to $H$ and $\sigma$ is a homomorphism from $H$ to $K$, show that $\sigma \circ \phi$ is a homomorphism from $G$ to $K$. How are ker($\phi$) and ker($\sigma \circ \phi$) related?

**Proof.** (a) We have $\phi : G \to H$ and $\sigma : H \to K$.

Observe that since $\phi$ is a homomorphism, then $\phi(G)$ is a subset of $H$, likewise $\sigma(H)$ is a subset of $K$.

Now we have $\phi(g) \in H$, then it follows that $\sigma(\phi(g)) \in K$.

We can also see that $\forall a, b \in G$ then $\sigma(\phi(a \circ b)) = \sigma(\phi(a) \circ \phi(b)) = \sigma(\phi(a)) \circ \sigma(\phi(b))$. So $\sigma \circ \phi$ is a homomorphism from $G$ to $K$.

(b) Claim: ker($\phi$) $\leq$ ker($\sigma \circ \phi$).

The definition of the kernel states that ker($\phi$) $\leq$ $G$ and ker($\sigma \circ \phi$) $\leq$ $G$.

Also observe that $\forall p \in$ ker($\phi$), then $\phi(p) = e_2$ and $\sigma(e_2) = e_3$, so $p \in$ ker($\sigma \circ \phi$). Thus ker($\phi$) $\subseteq$ ker($\sigma \circ \phi$). By the two step test, we need to find that ker($\phi$) to be nonempty, has closure, and it has inverses. By the above statement, it can be seen that $e_1 \in$ ker($\phi$), so ker($\phi$) is nonempty.

Consider $a, b \in$ ker($\phi$). Then $\phi(a) = e_2$ and $\phi(b) = e_2$, so $\phi(a \circ b) = \phi(a) \circ \phi(b) = e_2 \circ e_2 = e_2$.

Thus $a \circ b \in$ ker($\phi$).

Now for inverses, since ker($\phi$) is closed, then $\forall a \in$ ker($\phi$), there exists $a^{-1}$ such that

\[
\begin{align*}
a \circ a^{-1} &= e_1 \\
\phi(a \circ a^{-1}) &= \phi(e_1) \\
\phi(a) \circ \phi(a^{-1}) &= e_2 \\
e_2 \circ \phi(a^{-1}) &= e_2 \\
\phi(a^{-1}) &= e_2
\end{align*}
\]

Thus $a^{-1} \in$ ker($\phi$). Therefore ker($\phi$) $\leq$ ker($\sigma \circ \phi$).

6. [Hoffman, L.] If $\phi$ and $\gamma$ are isomorphisms from the cyclic group $\langle a \rangle$ to some group, and $\phi(a) = \gamma(a)$, then prove that $\phi = \gamma$.

**Proof.** We need to show that $\forall b \in \langle a \rangle, \phi(b) = \gamma(b)$. We know the following facts.

(a) For $b \in \langle a \rangle$, $\exists n \in \mathbb{Z}$ such that $b = a^n$.

(b) For $n \in \mathbb{Z}$, $\phi(a^n) = (\phi(a))^n$ and $\gamma(a^n) = (\gamma(a))^n$.

Then, for $b \in \langle a \rangle$,

\[
\phi(b) = \phi(a^n) = (\phi(a))^n = (\gamma(a))^n = \gamma(a^n) = \gamma(b).
\]

Thus $\phi = \gamma$.  □
7. [Leonard, R.] Show that \( \mathbb{Z} \) has infinitely many subgroups isomorphic to \( \mathbb{Z} \).

**Proof.** Consider \( \phi : \mathbb{Z} \to n\mathbb{Z} \). We must prove the following:

(a) \( n\mathbb{Z} \subseteq \mathbb{Z} \)
(b) \( \phi \) is a homomorphism
(c) \( \phi \) is bijective

(a) \( n\mathbb{Z} = \{nz : z \in \mathbb{Z} \text{ and } n \in \mathbb{Z}^+\} \), so \( n\mathbb{Z} \) consists of multiples of \( n \). Because there is no common divisor other than 1 for all integers, it must be that \( n\mathbb{Z} \subseteq \mathbb{Z} \). We already know \( n\mathbb{Z} \) is a group, so it must be that \( n\mathbb{Z} \leq \mathbb{Z} \). This is true for all \( n \in \mathbb{Z} \). Since there are an infinite number of possibilities for \( n \), there are an infinite number of subgroups.

(b) We must show the group operation is preserved for \( \phi \)

\[
\phi(a \circ b) = n(a \circ b) = na \circ nb = \phi(a) \circ \phi(b)
\]

So the group operation is preserved, and \( \phi \) is a homomorphism.

(c) It must be shown that \( \phi \) is both injective and surjective. Consider \( \phi(a) = \phi(b) \) If \( \phi(a) = na \) and \( \phi(b) = nb \), it must be that \( a = b \) by cancellation. This indicates that \( \phi \) is injective. Take \( \phi(a) \in n\mathbb{Z} \). The only input that will result in \( na \) is \( a \), so \( \phi \) is surjective.

Thus \( \phi : \mathbb{Z} \to n\mathbb{Z} \) is an isomorphism, and because there are an infinite number of sets \( n\mathbb{Z} \), there are an infinite number of subgroups of \( \mathbb{Z} \) isomorphic to \( \mathbb{Z} \).  

\[\blacksquare\]
2 Homework #9

1. [Stotz, D.] Show that the mapping \( a \rightarrow \log_{10} a \) is an isomorphism from \( \mathbb{R}^+ \) under multiplication to \( \mathbb{R} \) under addition.

Proof. It must be shown that:

(a) \( \phi \) is a homomorphism.
(b) \( \phi \) is injective.
(c) \( \phi \) is surjective.

We now prove the following:

(a) Consider \( a, b \in \mathbb{R}^+ \). By the properties of logarithms,

\[
\phi(ab) = \log_{10}(ab) = \log_{10} a + \log_{10} b = \phi(a) + \phi(b).
\]

Therefore, the group operations are preserved and \( \phi \) is a homomorphism from \( \{\mathbb{R}^+, \ast\} \) to \( \{\mathbb{R}, +\} \).

(b) Consider \( x, y \in \mathbb{R}^+ \) such that \( \phi(x) = \phi(y) \). By our definition of \( \phi \),

\[
\begin{align*}
\phi(x) &= \phi(y) \\
\log_{10}(x) &= \log_{10}(y) \\
10^{\log_{10}(x)} &= 10^{\log_{10}(y)}
\end{align*}
\]

Since \( x = y \), \( \phi \) is injective, as each output has one unique input.

(c) Consider \( a \in \mathbb{R} \). Let \( x = 10^a \), and note that even if \( a < 0 \), \( 10^a \in \mathbb{R}^+ \). By our definition of \( \phi \),

\[
\phi(x) = \log_{10}(x) = \log_{10}(10^a) = a.
\]

Thus \( \phi \) is surjective.

So, \( \phi \) is a bijective homomorphism, and therefore an isomorphism.
2. The following problems deal with finding the left cosets of subgroups.

(a) [Smith, C.] Let \( n \) be a positive integer. Let \( H = \{0, \pm n, \pm 2n, \pm 3n, \ldots \} \). Find all left cosets of \( H \) in \( \mathbb{Z} \). How many are there?

When the operation for a group is addition, cosets are usually designated by \( a + H \) instead of \( aH \).

Possible left cosets are \( 0 + H, 1 + H, 2 + H, 3 + H, \ldots, (n-1) + H, n + H, \ldots \).

Then

\[
0 + H = H, \\
1 + H = \{1, 1 \pm n, 1 \pm 2n, 1 \pm 3n, \ldots\}, \\
2 + H = \{2, 2 \pm n, 2 \pm 2n, 2 \pm 3n, \ldots\}, \\
3 + H = \{3, 3 \pm n, 3 \pm 2n, 3 \pm 3n, \ldots\}, \\
\vdots \\
(n-1) + H = \{(n-1), (n-1) \pm n, (n-1) \pm 2n, (n-1) \pm 3n, \ldots\}, \\
n + H = \{n, n \pm n, n \pm 2n, n \pm 3n, \ldots\} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\} = H.
\]

All the left cosets of \( H \) in \( \mathbb{Z} \) are \( 0 + H, 1 + H, 2 + H, 3 + H, \ldots, (n-1) + H, n + H, \ldots \), since \( n + H \) is really just \( H \). Therefore there are \( n \) cosets of \( H \) in \( \mathbb{Z} \).

(b) [Hjelmfelt, C.] Find all the left cosets of \( \{1, 11\} \) in \( U(30) \).

If \( H = \{1, 11\} \) and \( G = U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\} \), we know by Lagrange’s theorem that the number of distinct cosets is: \(|G|/|H| = 8/2 = 4\).

\[
1 \circ H = \{1, 11\} \\
7 \circ H = \{7, 17\} \\
13 \circ H = \{13, 23\} \\
19 \circ H = \{19, 29\}
\]

The unique left cosets in \( U(30) \) are \( 1H, 7H, 13H, 19H \).

(c) [Keene, L.] Suppose that \( a \) has order 15. Find all the left cosets of \( \langle a^5 \rangle \) in \( \langle a \rangle \).

We know that \( |a| = 15 \), and so

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

Or, \( a^5 \circ a^5 \circ a^5 = e \)

Thus \( |a^5| = 3 \), and \( \langle a^5 \rangle = \{e, a^5, a^{10}\} \leq \langle a \rangle \). Then the cosets are

\[
e \langle a^5 \rangle = \{e, a^5, a^{10}\},
\]

\[
a \langle a^5 \rangle = \{a, a^6, a^{11}\},
\]

\[
a^2 \langle a^5 \rangle = \{a^2, a^7, a^{12}\},
\]

\[
a^3 \langle a^5 \rangle = \{a^3, a^8, a^{13}\},
\]

\[
a^4 \langle a^5 \rangle = \{a^4, a^9, a^{14}\},
\]
\[a^5 \langle a^5 \rangle = \{a^5, a^{10}, a^{15}\} = \{e, a^5, a^{10}\} = e \langle a^5 \rangle.\]

At which point the cycle repeats, giving:

\[e \langle a^5 \rangle = a^5 \langle a^5 \rangle = a^{10} \langle a^5 \rangle,\]

\[a^1 \langle a^5 \rangle = a^6 \langle a^5 \rangle = a^{11} \langle a^5 \rangle,\]

\[a^2 \langle a^5 \rangle = a^7 \langle a^5 \rangle = a^{12} \langle a^5 \rangle,\]

\[a^3 \langle a^5 \rangle = a^8 \langle a^5 \rangle = a^{13} \langle a^5 \rangle,\]

\[a^4 \langle a^5 \rangle = a^9 \langle a^5 \rangle = a^{14} \langle a^5 \rangle.\]

And there are 5 unique left cosets of \( \langle a^5 \rangle \) in \( \langle a \rangle \).

3. [Spurlock, J.] If \( H \) and \( K \) are subgroups of \( G \) and \( g \in G \), show that \( g(H \cap K) = gH \cap gK \).

**Proof.** (\( \subseteq \)) Consider some element \( a \in g(H \cap K) \). This means there is some element \( m \in (H \cap K) \) such that \( a = g \circ m \). Since \( m \in (H \cap K) \), it must be that \( m \in H \) and \( m \in K \).

This means that \( g \circ m \in gH \) and \( g \circ m \in gK \), or \( a \in gH \) and \( a \in gK \), so \( a \in gH \cap gK \). Since \( a \) is arbitrary, \( g(H \cap K) \subseteq gH \cap gK \).

(\( \supseteq \)) Consider some element \( a \in gH \cap gK \). This means there is some element \( h \in H \) such that \( a = g \circ h \), and there is some element \( k \in K \) such that \( a = g \circ k \). Since they are both equal to \( a \), we can say that \( g \circ h = g \circ k \). By cancellation, this means \( h = k \).

Therefore, \( h \in H \) and \( h \in K \), so \( h \in H \cap K \). This means that \( g \circ h = a \in g(H \cap K) \). Since \( a \) is arbitrary, \( g(H \cap K) \supseteq gH \cap gK \).

Having proven containment in both directions, we can say \( g(H \cap K) = gH \cap gK \). \( \blacksquare \)

4. [Taggart, C.] Suppose that \( H \) and \( K \) are subgroups of \( G \) and that there are elements \( a, b \in G \) such that \( aH \subseteq bK \). Prove that \( H \subseteq K \).

**Proof.** (Taggart, C.) Note that \( b \in bK \). Also \( a \in aH \). Since \( a \in aH \) that means \( \exists k \in K \) such that \( a = b \circ k \) so \( a \in bK \). Since \( a \in bK \) that means \( aK = bK \) and \( a^{-1} \circ b \in K \).

Consider \( x \in H \). That means \( \exists c \in K \) such that \( a \circ x = b \circ c \). By performing a left operation with \( a^{-1} \), we get \( x = a^{-1} \circ b \circ c \). We know that \( c \in K \) and that \( a^{-1} \circ b \in K \). This means that their composition is in \( K \), which means \( x \in K \). Therefore \( H \subseteq K \). \( \blacksquare \)

**Proof.** (Conger, A.) Suppose \( aH \subseteq bK \). Since \( H \) and \( K \) are groups, there exist \( e \in H \) and \( f \in K \) such that \( a \circ e = a = b \circ f \) since \( aH \subseteq bK \). Applying \( b^{-1} \) to the left we find \( b^{-1} \circ a = f \). Since \( aH \subseteq bK \),

\[H = a^{-1} (aH) \subseteq a^{-1} (bK) = (a^{-1} \circ b)K = (a^{-1} \circ b)(fK) = ((a^{-1} \circ b) \circ (b^{-1} \circ a))K = K.\]

Thus \( H \subseteq K \). \( \blacksquare \)
We now know that \( a \in K \) and that \( b \in bK \). Since \( aH \subseteq bK \), we know there exists a \( k \in K \) such that \( a \circ b = k \), and therefore \( a \in bK \). Since we know that \( a \in bK \), \( aK = bK \). We also now know that \( a^{-1} \circ b \in K \).

If we take \( x \in H \), then we know there must exists \( c \in K \) such that \( a \circ x = b \circ c \). If we perform a left operation with \( a^{-1} \), we then have \( a^{-1} \circ a \circ x = a^{-1} \circ b \circ c \), which can be simplified to \( x = a^{-1} \circ b \circ c \).

We now know that \( a^{-1} \circ b \circ c \in K \), since \( K \) has closure. Thus \( x = a^{-1} \circ b \circ c \in K \). Therefore \( H \subseteq K \).

Proof. (Cosand, K.) Note that because \( H \) is a subgroup of \( G \), \( a \in aH \) by Coset Lemma #1. Then \( a \in bK \), which means \( \exists k \in K \) such that \( a = b \circ k \) and \( a^{-1} = (b \circ k)^{-1} = k^{-1} \circ b^{-1} \).

Now let \( x \in H \), which means that \( a \circ x \in bK \) and \( \exists y \in K \) such that \( a \circ x = b \circ y \). Then

\[
\begin{align*}
  a^{-1} \circ a \circ x &= a^{-1} \circ b \circ y \\
  x &= a^{-1} \circ b \circ y \\
  x &= (k^{-1} \circ b^{-1}) \circ b \circ y \\
  x &= k^{-1} \circ (b^{-1} \circ b) \circ y \\
  x &= k^{-1} \circ y
\end{align*}
\]

Because \( K \) is a subgroup of \( G \), \( k^{-1} \in K \). Since \( k^{-1}, y \in K \), and \( K \) is closed, \( k^{-1} \circ y \in K \). Therefore, \( x \in K \), and \( H \subseteq K \).

Proof. (Dyke, M.) Since we know that \( H \) is a subgroup of \( G \), the identity must be in \( H \) (\( e \in H \)). Therefore, \( a = a \circ e \in aH \subseteq bK \). Then \( \exists c \in K \) such that \( a = b \circ c \).

Note that \( a^{-1} = (b \circ c)^{-1} = c^{-1} \circ b^{-1} \), so \( c^{-1} \in K \). If we take \( x \in H \), we need to show \( x \in K \) to support the fact that \( H \subseteq K \). Using our knowledge of groups, we know \( a \circ x \in a \circ H \). Therefore, \( a \circ x \in bK \), which suggests that there exists \( y \in K \) with the property that \( a \circ x = b \circ y \). Let’s lay this out:

\[
x = (a^{-1} \circ a) \circ x = a^{-1} \circ (a \circ x) = a^{-1} \circ (b \circ y) = (c^{-1} \circ b^{-1}) \circ b \circ y = c^{-1} \circ y.
\]

As \( c, y \in K \), and \( K \) is a subgroup, then \( c^{-1} \circ y \in K \). Thus, \( x \in K \), and \( H \subseteq K \).

Proof. (Franck, D.) Since we know that \( H \) is a subgroup of \( G \), the identity must be in \( H \) (\( e \in H \)). Therefore, \( a = a \circ e \in aH \subseteq bK \). Then \( \exists c \in K \) such that \( a = b \circ c \).

Note that \( a^{-1} = (b \circ c)^{-1} = c^{-1} \circ b^{-1} \), so \( c^{-1} \in K \). If we take \( x \in H \), we need to show \( x \in K \) to support the fact that \( H \subseteq K \). Using our knowledge of groups, we know \( a \circ x \in a \circ H \). Therefore, \( a \circ x \in bK \), which suggests that there exists \( y \in K \) with the property that \( a \circ x = b \circ y \). Let’s lay this out:

\[
x = (a^{-1} \circ a) \circ x = a^{-1} \circ (a \circ x) = a^{-1} \circ (b \circ y) = (c^{-1} \circ b^{-1}) \circ b \circ y = c^{-1} \circ y.
\]

As \( c, y \in K \), and \( K \) is a subgroup, then \( c^{-1} \circ y \in K \). Thus, \( x \in K \), and \( H \subseteq K \).

Proof. (Gruenig, S.) By (1) of our coset lemma, we know that \( a \in aH \). Since \( aH \subseteq bK \), \( a \) is also an element of \( bK \). Then by (4) of our coset lemma, since \( a \in bK \), we know that \( bK = aK \), so replacing \( bK \) with \( aK \) in our relationship gives \( aH \subseteq aK \). By definition, this means that for all \( h \in H \) there exists some \( k \in K \) such that \( ah = ak \), and by cancellation, \( h = k \). Since this is true \( \forall h \in H \), \( H \subseteq K \).
Proof. (Havelka, R.) Observe that the definitions of \( aH \) and \( bK \) are \( aH = \{ a \circ h : h \in H \} \) and \( bK = \{ b \circ k : k \in K \} \). Since \( H \subseteq G \) and \( K \subseteq G \), then \( h, k \in G \).

We have \( aH \subseteq bK \), so for all \( a, h \in aH \), there exists a \( b \circ k \in bK \) where \( a \circ h = b \circ k \). Note, it can be seen that \( h = (a^{-1} \circ b) \circ k \) and \( (b^{-1} \circ a) \circ h = k \). So \( h \in (a^{-1} \circ b)K \) and \( k \in (b^{-1} \circ a)H \). Now \( H \) is a group, so \( e \in H \). This means that \( (b^{-1} \circ a) \circ e = (b^{-1} \circ a) = k \), thus \( b^{-1} \circ a \in K \). Since \( K \) is a group, then the inverse of \( b^{-1} \circ a \) is also in \( K \). So \( (b^{-1} \circ a)^{-1} = a^{-1} \circ b \in K \).

Let \( a^{-1} \circ b = k_2 \), and observe that \( k_2 \in K \). Now \( h = (a^{-1} \circ b) \circ k \) becomes \( h = k_2 \circ k \), and it can be seen that since \( k_2, k \in K \) and \( k_2 \circ k \in K \). Thus, from the fact that \( h = k_2 \circ k \), then \( h \in K \).

Thus all elements \( h \in H \) are also elements in \( K \), therefore \( H \subseteq K \).

Proof. (Leonard, R.) We know \( aH \subseteq bK \), so there exists a \( (b \circ k) \in bK \) such that \( b \circ k = a \circ h \) for every \( (a \circ h) \in aH \). Therefore

\[
h = a^{-1} \circ b \circ k.
\]

We can see from the above that

\[
a^{-1} \circ b \circ k \in H.
\]

We want to show \( a^{-1} \circ b \in K \). If this is in \( K \), then we know \( h \in K \), because \( K \) is closed and \( a^{-1} \circ b \circ k = h \). We know by the coset lemma that \( a \in aH \) and \( b \in bK \), and so there exists \( k \in K \) such that \( a = b \circ k \) and \( a \in bK \). By the lemma, we then see that \( aK = bK \), and we can write

\[
a \circ k_1 = b \circ k_2,
\]

or

\[
k_1 = a^{-1} \circ b \circ k_2.
\]

Therefore \( a^{-1} \circ b \in K \), because \( k_1 \in K \). Therefore \( h \in K \). Since \( h \in K \), we see that \( H \subseteq K \).

Proof. (Norstedt, Z.) Let \( c \in aH \). We know that \( \exists h \in H \) such that \( c = a \circ h \). We also know that \( c \in bK \), so \( c = b \circ k \), for some \( k \in K \).

Then \( c = a \circ h = b \circ k \), and \( a = b \circ k \circ h^{-1} \). Note that \( a \in aH \), so \( a = b \circ (k \circ h^{-1}) \in bK \), and thereby \( k \circ h^{-1} \in K \). Because \( k \) was taken out of \( K \), \( k^{-1} \in K \), since \( K \) is a subgroup. Thus,

\[
k^{-1} \circ (k \circ h^{-1}) = (k^{-1} \circ k) \circ h^{-1} = h^{-1} \in K,
\]

by closure. Therefore, \( (h^{-1})^{-1} = h \in K \), and \( H \subseteq K \).

Moreover, as \( H \) and \( K \) are both groups, \( H \leq K \).
Proof. (Smith, C.) We know $H$ is subgroup of $G$, and by the coset Lemma (1) $a \in aH$. Also $aH \subseteq bK$, and since $aH$ is a subset of $bK$, we know $a \in bK$. Because $bK$ is a coset and $K$ is a subgroup of $G$, $a = b \circ k$ for some $k \in K$.

Consider $h \in H$. We know $a \circ h \in aH$ and using substitution

$$a \circ h = (b \circ k_1) \circ h = b \circ (k_1 \circ h) \in aH.$$  

Because $aH \subseteq bK$ and $b \circ (k_1 \circ h) \in bK$, we now know $b \circ k_1 \circ h = b \circ k_2$, for some $k_1, k_2 \in K$. Using cancellation we get

$$
\begin{align*}
  k_1 \circ h &= k_2 \\
  k_1^{-1} \circ k_1 \circ h &= k_1^{-1} \circ k_2 \\
  e \circ h &= k_1^{-1} \circ k_2 \\
  h &= k_1^{-1} \circ k_2.
\end{align*}
$$

Because $k_1^{-1}$ and $k_2$ are both in $K$ and $h = k_1^{-1} \circ k_2$, then $h \in K$, and $h \in H$. Therefore $H \subseteq K$. □

Proof. (Spurlock, J.) Since $H$ is a subgroup of $G$, we know that $a \in aH$ by part 1 of the coset lemma. Since $aH \subseteq bK$, this means there exists some $k \in K$ such that $a = b \circ k$. Applying $b^{-1}$, we find that $k = b^{-1} \circ a$. By part 6 of the coset lemma, this means $bK = aK$, and therefore $aH \subseteq aK$.

This means that, for any $h \in H$, there exists a $k \in K$ such that $a \circ h = a \circ k$. By cancellation, this means $h = k$, and thus $H \subseteq K$. □
3 Homework #10


Proof. Note that $H \subseteq K$, and since $H$ is a subgroup of $G$, then by the Finite Subgroup Test $H$ is a subgroup of $K$. Since $H \leq K$, $K \leq G$, and $H \leq G$, then using Lagrange’s Theorem we have


Consider

$$|G : K| \cdot |K : H| = \frac{|G|}{|K|} \cdot \frac{|K|}{|H|} = \frac{|G|}{|H|} = |G : H|.$$ 

Thus


2. [Havelka, R.] Let $|G| = 15$. If $G$ has only one subgroup of order 3 and only one of order 5, prove that $G$ is cyclic. Generalize to $|G| = pq$, where $p$ and $q$ are prime.

Proof. By Lagrange’s Theorem, for any $g \in G$ then the divisors of $|G|$ can be the order of $g$, or $|g| = 1, p, q, pq$. Let $H, K \leq G$ such that $|H| = p$ and $|K| = q$. Then the following conditions are possible for $g \in G$.

(a) If $|g| = 1$, then $g = e$, and $g$ is in all the subgroups of $G$.
(b) If $|g| = p$, then $g \in H$, and $H = \langle g \rangle$.
(c) If $|g| = q$, then $g \in K$ and $K = \langle g \rangle$.
(d) If $|g| = pq$, then $g \in G$ and no proper subgroups of $G$.

Then consider $g \in G$ such that $|g| = pq$. It is necessary to verify that such an element exists in $G$. Since $|H| = p$, $|K| = q$, and $H \cap K = \{e\}$, then the number of elements that are not exclusively in only $G$ is $p + q - 1$. Observe that $pq > p + q - 1$, for all primes $p$ and $q$, or in other words, $|G| > p + q - 1$. Thus $\exists g_1 \in G$, neither in $H$ nor $K$, such that $|g_1| = pq$.

Claim: $\langle g_1 \rangle = G$, for this $g_1 \in G$.

(\(\subseteq\)) It follows by definition that $\langle g \rangle \subseteq G$.

(\(\supseteq\)) Since $|g_1| = |\langle g_1 \rangle| = pq$, then $G \subseteq \langle g_1 \rangle$, since every element of $G$ must be created by $\langle g_1 \rangle$.

Therefore $\langle g_1 \rangle = G$, and $G$ is cyclic. \(\blacksquare\)
3. [Franck, D.] Let $G$ be a group of order 25. Prove that $G$ is cyclic or $g^p = e$ for all $g \in G$. Generalize to any group of order $p^2$, where $p$ is prime. Does your proof work for this generalization?

Proof. If we let $g \in G$ and $p$ be prime, then we know that $|G| = p^2$, so the order of $g$ divides the order of $p^2$. Then $|g|$ could be 1, $p$, or $p^2$.

If we assume $|g| = 1$, this means that $g = e$, so $g^p = e$.

If we have $|g| = p$, then $g^p = e$.

Lastly, if we assume $|g| = p^2$, then by definition, we know that $|\langle g \rangle| = p^2$. Clearly, $\langle g \rangle \subseteq G$. Also, since $|\langle g \rangle| = p^2$ and $|G| = p^2$, then $G \subseteq \langle g \rangle$. Thus $G = \langle g \rangle$, and $G$ is cyclic.

Thus, $G$ is either cyclic or $g^p = e$, $\forall g \in G$. ■

4. [Kittler, S.] Prove that if $G$ is a finite group, the index of $Z(G)$ cannot be prime.

Proof. (Kittler, S.) By contradiction, assume $|G : Z(G)| = p$, where $p$ is prime, and $|Z(G)| = k$, for some positive integer $k$. Thus $|G| = pk$. Take $g \in G \setminus Z(G)$. Consider $C(g)$, where $|G : C(g)| = x$, $|C(g) : Z(G)| = y$, and $xy = p$. The only way for this to be true is if either (1) $x = 1$ and $y = p$, or (2) $x = p$ and $y = 1$.

For case 1: $|G : C(g)| = 1$ and $|C(g) : Z(G)| = p$. Thus $G = C(g)$, which means $g \circ x = x \circ g$, $\forall x \in G$, which is the definition of the center and $g \in Z(G)$, and this is a contradiction.

For case 2: $|G : C(g)| = p$ and $|C(g) : Z(G)| = 1$. Thus $C(g) = Z(G)$, and $g \in C(g) = Z(G)$. Thus $g \in Z(G)$, and this is a contradiction.

Thus $|G : Z(G)|$ cannot be prime. ■

Proof. (Dyke, M.) There are two cases to consider.

Case 1:

Assume $G$ is an abelian group. Then $Z(G) = G$. The index of $Z(G)$ is $\frac{|G|}{|Z(G)|}$, which equals 1 in this case. Therefore, the index of $Z(G)$ is not prime, because 1 is not a prime number.

Case 2:

Assume $G$ is non-abelian. By the contrapositive of Theorem 9.3, $G/Z(G)$ is not cyclic. Then by the contrapositive of our second corollary of Lagrange’s Theorm, $G/Z(G)$ cannot have prime order. Because $G/Z(G)$ is the collection of left cosets of $Z(G)$ in $G$, in this case there is a non-prime number of left cosets of $Z(G)$ in $G$. Therefore, by definition of the index, the index of $Z(G)$ is not prime.

Since the index of $Z(G)$ is not prime in both cases, it can never be prime. ■
Proof. (Taggart, C.) Assume to the contrary that $|G : Z(G)| = p$, where $p$ is prime. Since $Z(G) \triangleleft G$, there is a factor group $G/Z(G)$, which has $p$ elements. Since $|G/Z(G)|$ is prime, it is cyclic, and thus $\exists a \in G$ such that $G/Z(G) = \{ Z(G), aZ(G), a^2Z(G), ..., a^{p-1}Z(G) \}$. Since this group contains all the left cosets of $Z(G)$, all the elements of $G$ are contained within one of these cosets.

Consider $b \in G$ such that $b = a^k \circ z_1$, $\exists k \in \mathbb{Z}$ and $\exists z_1 \in Z(G)$. Also consider $c \in G$ such that $c = a^j \circ z_2$, $\exists j \in \mathbb{Z}$ and $\exists z_2 \in Z(G)$. Then

$$b \circ c = a^k \circ z_1 \circ a^j \circ z_2 = a^k \circ a^j \circ z_1 \circ z_2 = a^{k+j} \circ z_2 \circ z_1 = a^j \circ a^k \circ z_2 \circ z_1 = a^j \circ z_2 \circ a^k \circ z_1 = c \circ b.$$ 

Since $b, c$ are arbitrary elements in $G$, then $b \circ c = c \circ b$, $\forall b, c \in G$. So $|Z(G)| = |G|$, and $|G : Z(G)| = 1$. This is a contradiction. Thus $|G : Z(G)|$ cannot be prime. $\blacksquare$
4 An Application of Cosets to Permutation Groups

Lagrange’s Theorem and its corollaries dramatically demonstrate the fruitfulness of the coset concept. We next consider an application of cosets to permutation groups.

Definition 1 (Stabilizer of a Point). Let $G$ be a group of permutations of a set $S$. For each $i$ in $S$, let $\text{stab}_G(i) = \{ \phi \in G : \phi(i) = i \}$. We call $\text{stab}_G(i)$ the stabilizer of $i$ in $G$.

Proposition 1. For all $i \in S$, the stabilizer, $\text{stab}_G(i)$, is a subgroup of $G$.

Proof. Using the two-step subgroup test, we must show:

1. $\text{stab}_G(a)$ is non-empty.
2. $\alpha\beta \in \text{stab}_G(a)$.
3. $\alpha^{-1} \in \text{stab}_G(a)$.

Then

1. Let $a \in S$. Note that because $\varepsilon(a) = a$, we know $\varepsilon \in \text{stab}_G(a)$. Therefore, $\text{stab}_G(a)$ is non-empty.
2. Let $\alpha, \beta \in \text{stab}_G(a)$. Since we know $\beta \in \text{stab}_G(a)$, then $\beta(a) = a$. Note $(\alpha\beta)(a) = \alpha(\beta(a)) = \alpha(a) = a$, so $\alpha\beta \in \text{stab}_G(a)$.
3. Consider $\alpha(a) = a$. By performing a left hand operation using $\alpha^{-1}$, we can show $\alpha^{-1} \in \text{stab}_G(a)$. Note that

\[
\begin{align*}
\alpha(a) &= a \\
\alpha^{-1}(\alpha(a)) &= \alpha^{-1}(a) \\
(\alpha^{-1}\alpha)(a) &= \alpha^{-1}(a) \\
\varepsilon(a) &= \alpha^{-1}(a) \\
a &= \alpha^{-1}(a).
\end{align*}
\]

Since $\alpha \in \text{stab}_G(a)$, we can also conclude that $\alpha^{-1} \in \text{stab}_G(a)$. Thus, $\text{stab}_G(a) \leq G$, by the two-step subgroup test.

Definition 2 (Orbit of a Point). Let $G$ be a group of permutations of a set $S$. For each $s$ in $S$, let $\text{orb}_G(s) = \{ \phi(s) : \phi \in G \}$. The set $\text{orb}_G(s)$ is a subset of $S$ called the orbit of $s$ under $G$. We use $|\text{orb}_G(s)|$ to denote the number of elements in $\text{orb}_G(s)$.
Example 1. Let $G = \{(1)(2)(3)(4), (12)(3)(4), (1)(2)(34), (12)(34)\}$, which is a group. Then
\[
\text{orb}_{G}(1) = \{1, 2\}, \quad \text{stab}_{G}(1) = \{(1)(2)(3)(4), (1)(2)(34)\},
\]
\[
\text{orb}_{G}(2) = \{2, 1\}, \quad \text{stab}_{G}(2) = \{(1)(2)(3)(4), (1)(2)(34)\},
\]
\[
\text{orb}_{G}(3) = \{3, 4\}, \quad \text{stab}_{G}(3) = \{(1)(2)(3)(4), (12)(3)(4)\},
\]
\[
\text{orb}_{G}(4) = \{4, 3\}, \quad \text{stab}_{G}(4) = \{(1)(2)(3)(4), (12)(3)(4)\}.
\]

Example 2. Let $G = \{(1)(2)(3), (1)(23), (2)(13), (3)(12), (123), (132)\}$, which is a group. Then
\[
\text{orb}_{G}(1) = \{1, 3, 2\}, \quad \text{stab}_{G}(1) = \{(1), (1)(23)\},
\]
\[
\text{orb}_{G}(2) = \{2, 3, 1\}, \quad \text{stab}_{G}(2) = \{(2), (2)(13)\},
\]
\[
\text{orb}_{G}(3) = \{3, 2, 1\}, \quad \text{stab}_{G}(3) = \{(3), (3)(12)\}.
\]

Theorem 1 (Orbit-Stabilizer Theorem). Let $G$ be a finite group of permutations of a set $S$. Then, for any $i$ from $S$, $|G| = |\text{orb}_{G}(i)||\text{stab}_{G}(i)|$.

**Proof.** By Lagrange’s Theorem, $|G|/|\text{stab}_{G}(i)|$ is the number of distinct left cosets of $\text{stab}_{G}(i)$ in $G$. To prove this, we must show

1. The relation between the left cosets of $\text{stab}_{G}(i)$ and the elements in the orbit of $i$ is well-defined.
2. There is an injective(one-to-one) relation between the left cosets of $\text{stab}_{G}(i)$ and the elements in the orbit of $i$.
3. There is a surjective(onto) relation between the left cosets of $\text{stab}_{G}(i)$ and the elements in the orbit of $i$.

Then

1. To show that $T$ is a well-defined function, we must show that $\alpha \text{stab}_{G}(i) = \beta \text{stab}_{G}(i)$ implies $\alpha(i) = \beta(i)$. But $\alpha \text{stab}_{G}(i) = \beta \text{stab}_{G}(i)$ implies $\alpha^{-1} \beta \in \text{stab}_{G}(i)$, so that $(\alpha^{-1} \beta)(i) = i$, and therefore, $\beta(i) = \alpha(i)$.
2. To show the mapping is injective, we define a correspondence $T$ by mapping the coset $\alpha \text{stab}_{G}(i)$ to $\alpha(i)$ under $T$. Assume that $\beta(i) = \alpha(i)$. Then $(\alpha^{-1} \beta)(i) = i$. But this implies that there is a $\alpha^{-1} \beta \in \text{stab}_{G}(i)$. Therefore, $\alpha \text{stab}_{G}(i) = \beta \text{stab}_{G}(i)$, which shows it is injective.
3. To show $T$ is onto $\text{orb}_{G}(i)$, let $j \in \text{orb}_{G}(i)$. Then $\alpha(i) = j$ for some $\alpha \in G$. Clearly $T(\alpha \text{stab}_{G}(i)) = \alpha(i) = j$, therefore $T$ is onto.

\[\blacksquare\]

**Definition 3** (Partition). A partition of a set $S$ is a collection of non-empty disjoint subsets of $S$ whose union is $S$.

**Example 3** (Quaternions). Since a partition is made of non-empty disjoint subsets, we can take elements from an existing group to create disjoint subsets. Using the Quaternions, a partition would consist of
\[
\{1, j, -1\}, \{-1\}, \{k, -k\}, \{-j, i\}.
\]
Note that every set is disjoint and the collection of the elements makes up the Quaternion group.
Proposition 2. The orbits of the members of $S$ constitute a partition of $S$.

Proof. We need to show

1. Each orbit is non-empty and every element is contained in an orbit.
2. The cycles are either equal, $\text{orb}_G(i) = \text{orb}_G(j)$, or disjoint, $\text{orb}_G(i) \cap \text{orb}_G(j) = \emptyset$.

Then

1. We know that $\forall a \in S$ will have an $\text{orb}_G(a)$ such that $a \in \text{orb}_G(a)$.
2. If the cycles are disjoint, we are done. If the intersection of the orbits is equal to the empty set, we need to show the orbits are equal to zero. Assume $\text{orb}_G(i) \cap \text{orb}_G(j) \neq \emptyset$, where $i \neq j$. Let $k \in \text{orb}_G(i) \cap \text{orb}_G(j)$. So, for some $\alpha, \beta \in G$, $\alpha(i) = k = \beta(j)$. Then we can show

   \[
   \begin{align*}
   \beta^{-1}(k) &= (\beta^{-1}\beta)(j) \\
   \beta^{-1}(\alpha(i)) &= \varepsilon(j) \\
   (\beta^{-1}\alpha)(i) &= j.
   \end{align*}
   \]

   Similarly, we can use the same process to show that $i = (\alpha^{-1}\beta)(j)$. Also, since $\beta^{-1}\alpha \in G$ and $\alpha^{-1}\beta \in G$, then $j = (\beta^{-1}\alpha)(i) \in \text{orb}_G(i)$, and $i \in \text{orb}_G(j)$.

   Take $x \in \text{orb}_G(i)$. We need to show $x \in \text{orb}_G(j)$, by finding $\gamma \in G$, such that $\gamma(j) = x$. There exists a $\mu \in G$, such that $\mu(i) = x$. Then

   \[
   \begin{align*}
   \mu(\alpha^{-1}(\beta(j))) &= \mu(i) = x \\
   (\mu\alpha^{-1}\beta)(j) &= x.
   \end{align*}
   \]

   Let $\gamma = \mu\alpha^{-1}\beta \in G$. Then $\gamma(j) = x$, and $x \in \text{orb}_G(j)$.

   Thus $\text{orb}_G(i) \subseteq \text{orb}_G(j)$. Similarly, $\text{orb}_G(j) \subseteq \text{orb}_G(i)$. Hence $\text{orb}_G(i) = \text{orb}_G(j)$.

   Therefore, the orbits of the members of $S$ constitute a partition of $S$. \qed
5 Homework #11

1. [Berger, E.] Let \( \phi \) be a homomorphism from \( G_1 \) to \( G_2 \). Prove that \( \ker(\phi) \) is a normal subgroup of \( G_1 \).

   **Proof.** Recall the Normal Subgroup Test: A subgroup \( H \) of \( G \) is normal in \( G \) if and only if \( xHx^{-1} \subseteq H \), for all \( x \) in \( G \). Assume \( k \in \ker(\phi) \) and \( g \in G_1 \). We are trying to prove that \( gkg^{-1} \in \ker(\phi) \).

   So 
   \[
   \phi(g \circ k \circ g^{-1}) = \phi(g) \circ \phi(k) \circ \phi(g^{-1}) = \phi(g) \circ e_2 \circ (\phi(g))^{-1} = \phi(g) \circ (\phi(g))^{-1} = e_2.
   \]

   As such, \( gkg^{-1} \in \ker(\phi) \), so \( \ker(\phi) \) is a normal subgroup of \( G_1 \).

2. [Kranstz, S.] In \( D_4 \), let \( K = \{R_0, F_\wedge\} \), and let \( L = \{R_0, F_\wedge, F_\vee, R_{180}\} \). Show that \( K \triangleleft L \triangleleft D_4 \) but that \( K \) is not normal in \( D_4 \). (Normality is not transitive.) Hint: a problem in the extra exercises will help you avoid the endless calculations needed to show normality.

   **Proof.** In order to show \( K \triangleleft L \triangleleft D_4 \) more easily, use Problem 7 from below.

   Note that 
   \[
   |D_4 : L| = \frac{|D_4|}{|L|} = \frac{8}{4} = 2.
   \]

   Therefore \( L \triangleleft D_4 \). Also 
   \[
   |L : K| = \frac{|L|}{|K|} = \frac{4}{2} = 2.
   \]

   Thus \( K \triangleleft L \).

   However, \( K \) is not normal in \( D_4 \). A counterexample will be provided in order to prove that \( \exists \, x \in D_4 \) such that \( xK \neq Kx \). Let \( x = F_- \). So 
   \[
   xK = \{F_-, R_{270}\},
   \]

   and 
   \[
   Kx = \{F_-, R_{90}\}.
   \]

   Since \( xK \) does not equal \( Kx \), then \( K \) is not normal in \( D_4 \).}

3. [Henson, T.] Consider the following factor groups using subgroups of \( \mathbb{Z} \). (I used Excel to help organize and compute the cosets.)

   (a) Viewing \(<3>\) and \(<12>\) as subgroups of \( \mathbb{Z} \), prove that \( <3>/<12> \) is isomorphic to \( \mathbb{Z}_4 \).

   Note that for this group \( <a> = \{an : n \in \mathbb{Z}\} \). Thus 
   \[
   <3> = \{\ldots, -3, 0, 3, 6, 9, 12, \ldots\},
   \]

   and 
   \[
   <12> = \{\ldots, -12, 0, 12, 24, 36, 48, \ldots\},
   \]

   \[
   <3>/<12> = \{<12>, a + <12>, b + <12>, \ldots\},
   \]

   \( \forall a, b \in <3> \).
The resulting cosets are

\[ 0 + \langle 12 \rangle = \{ \ldots, 0, 12, 24, 36, 48, 60, \ldots \}, \]
\[ 3 + \langle 12 \rangle = \{ \ldots, 3, 15, 27, 39, 51, 63, \ldots \}, \]
\[ 6 + \langle 12 \rangle = \{ \ldots, 6, 18, 30, 42, 54, 66, \ldots \}, \]

and

\[ 9 + \langle 12 \rangle = \{ \ldots, 9, 21, 33, 45, 57, 69, \ldots \}. \]

We know that these are the only cosets as any other multiple of 3 will just be a shifted version of one of these four cosets. Now, let's put these cosets into a Cayley table to compare them to \((\mathbb{Z}_4, +)\).

<table>
<thead>
<tr>
<th>+</th>
<th>0 + \langle 12 \rangle</th>
<th>3 + \langle 12 \rangle</th>
<th>6 + \langle 12 \rangle</th>
<th>9 + \langle 12 \rangle</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 + \langle 12 \rangle</td>
<td>0 + \langle 12 \rangle</td>
<td>3 + \langle 12 \rangle</td>
<td>6 + \langle 12 \rangle</td>
<td>9 + \langle 12 \rangle</td>
</tr>
<tr>
<td>3 + \langle 12 \rangle</td>
<td>3 + \langle 12 \rangle</td>
<td>6 + \langle 12 \rangle</td>
<td>9 + \langle 12 \rangle</td>
<td>0 + \langle 12 \rangle</td>
</tr>
<tr>
<td>6 + \langle 12 \rangle</td>
<td>6 + \langle 12 \rangle</td>
<td>9 + \langle 12 \rangle</td>
<td>0 + \langle 12 \rangle</td>
<td>3 + \langle 12 \rangle</td>
</tr>
<tr>
<td>9 + \langle 12 \rangle</td>
<td>9 + \langle 12 \rangle</td>
<td>0 + \langle 12 \rangle</td>
<td>3 + \langle 12 \rangle</td>
<td>6 + \langle 12 \rangle</td>
</tr>
</tbody>
</table>

Compare this with the Cayley Table for \((\mathbb{Z}_4, +)\).

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Clearly the Cayley tables match and the elements map as follows:

\[ 0 + \langle 12 \rangle \rightarrow 0, \]
\[ 3 + \langle 12 \rangle \rightarrow 1, \]
\[ 6 + \langle 12 \rangle \rightarrow 2, \]
\[ 9 + \langle 12 \rangle \rightarrow 3. \]

As a result, \(\langle 3 \rangle / \langle 12 \rangle\) is isomorphic to \(\mathbb{Z}_4\).

(b) Similarly, prove \(\langle 8 \rangle / \langle 48 \rangle\) is isomorphic to \(\mathbb{Z}_6\).

Here

\[ \langle 8 \rangle = \{ \ldots, -8, 0, 8, 16, 24, 32, \ldots \}, \]
\[ \langle 48 \rangle = \{ \ldots, -48, 0, 48, 96, 144, 192, \ldots \}, \]

and

\[ \langle 8 \rangle / \langle 48 \rangle = \{ \langle 48 \rangle, a + \langle 48 \rangle, b + \langle 48 \rangle, \ldots \}, \]

\(\forall a, b \in \langle 8 \rangle\).

The resulting cosets are

\[ 0 + \langle 48 \rangle = \{ \ldots, 0, 48, 96, 144, 192, 240, \ldots \}, \]
$8 + \langle 48 \rangle = \{ \ldots, 8, 56, 104, 152, 200, 248, \ldots \}$,
$16 + \langle 48 \rangle = \{ \ldots, 16, 64, 112, 160, 208, 256, \ldots \}$,
$24 + \langle 48 \rangle = \{ \ldots, 24, 72, 120, 168, 216, 264, \ldots \}$,
$32 + \langle 48 \rangle = \{ \ldots, 32, 80, 128, 176, 224, 272, \ldots \}$,
$40 + \langle 48 \rangle = \{ \ldots, 40, 88, 136, 184, 232, 280, \ldots \}$.

We know that these are the only cosets as any other multiple of 8 will simply be a shifted version on these six cosets. Now we make a Cayley table of the cosets and compare them to $(\mathbb{Z}_6, +)$.

<table>
<thead>
<tr>
<th>+</th>
<th>$0 + \langle 48 \rangle$</th>
<th>$8 + \langle 48 \rangle$</th>
<th>$16 + \langle 48 \rangle$</th>
<th>$24 + \langle 48 \rangle$</th>
<th>$32 + \langle 48 \rangle$</th>
<th>$40 + \langle 48 \rangle$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0 + \langle 48 \rangle$</td>
<td>$0 + \langle 48 \rangle$</td>
<td>$8 + \langle 48 \rangle$</td>
<td>$16 + \langle 48 \rangle$</td>
<td>$24 + \langle 48 \rangle$</td>
<td>$32 + \langle 48 \rangle$</td>
<td>$40 + \langle 48 \rangle$</td>
</tr>
<tr>
<td>$8 + \langle 48 \rangle$</td>
<td>$8 + \langle 48 \rangle$</td>
<td>$16 + \langle 48 \rangle$</td>
<td>$24 + \langle 48 \rangle$</td>
<td>$32 + \langle 48 \rangle$</td>
<td>$40 + \langle 48 \rangle$</td>
<td>$0 + \langle 48 \rangle$</td>
</tr>
<tr>
<td>$16 + \langle 48 \rangle$</td>
<td>$16 + \langle 48 \rangle$</td>
<td>$24 + \langle 48 \rangle$</td>
<td>$32 + \langle 48 \rangle$</td>
<td>$40 + \langle 48 \rangle$</td>
<td>$0 + \langle 48 \rangle$</td>
<td>$8 + \langle 48 \rangle$</td>
</tr>
<tr>
<td>$24 + \langle 48 \rangle$</td>
<td>$24 + \langle 48 \rangle$</td>
<td>$32 + \langle 48 \rangle$</td>
<td>$40 + \langle 48 \rangle$</td>
<td>$0 + \langle 48 \rangle$</td>
<td>$8 + \langle 48 \rangle$</td>
<td>$16 + \langle 48 \rangle$</td>
</tr>
<tr>
<td>$32 + \langle 48 \rangle$</td>
<td>$32 + \langle 48 \rangle$</td>
<td>$40 + \langle 48 \rangle$</td>
<td>$0 + \langle 48 \rangle$</td>
<td>$8 + \langle 48 \rangle$</td>
<td>$16 + \langle 48 \rangle$</td>
<td>$24 + \langle 48 \rangle$</td>
</tr>
<tr>
<td>$40 + \langle 48 \rangle$</td>
<td>$40 + \langle 48 \rangle$</td>
<td>$0 + \langle 48 \rangle$</td>
<td>$8 + \langle 48 \rangle$</td>
<td>$16 + \langle 48 \rangle$</td>
<td>$24 + \langle 48 \rangle$</td>
<td>$32 + \langle 48 \rangle$</td>
</tr>
</tbody>
</table>

Compare this with the Cayley table for $(\mathbb{Z}_6, +)$.

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Clearly, the Cayley tables match and the elements map as follows:

$0 + \langle 48 \rangle \rightarrow 0$,
$8 + \langle 48 \rangle \rightarrow 1$,
$16 + \langle 48 \rangle \rightarrow 2$,
$24 + \langle 48 \rangle \rightarrow 3$,
$32 + \langle 48 \rangle \rightarrow 4$,
$40 + \langle 48 \rangle \rightarrow 5$.

As a result, $\langle 8 \rangle / \langle 48 \rangle$ is isomorphic to $\mathbb{Z}_6$.

(c) Generalize to arbitrary integers $k$ and $n$. You don’t need to provide a proof, just a conjecture.

Let $k, n \in \mathbb{Z}$. If $k|n$, then $\langle k \rangle / \langle n \rangle$ is isomorphic to $\mathbb{Z}_{n/k}$.
4. [Norstedt, Z.] If \( H \) is a normal subgroup of a group \( G \), prove that

\[
C(H) = \{ g \in G : g \circ h = h \circ g, \forall h \in H \},
\]

the centralizer of \( H \) in \( G \), is a normal subgroup of \( G \).

**Proof.** Begin by the Normal Subgroup Test. First, this test requires that \( C(H) \) be a subgroup of \( G \). Then, if \( gC(H)g^{-1} \subseteq C(H) \), \( \forall g \in G \), we can conclude that \( C(H) \) is a normal subgroup of \( G \).

As the identity commutes with all elements of \( H \), \( e \in C(H) \), and \( C(H) \) is non-empty. Continue by the One-Step Subgroup Test.

Let \( a, b \in C(H) \) and consider \( h_1 \circ (a \circ b^{-1}) \), where \( h_1 \in H \). Because anything in \( C(H) \) commutes with everything in \( H \), \( h_1 \circ (a \circ b^{-1}) = a \circ h_1 \circ b^{-1} \). We know that \( b \) commutes with \( h_1 \), so \( b \circ h_1 = h_1 \circ b \). Applying \( b^{-1} \) on both the left and the right results in

\[
b^{-1} \circ h_1 \circ b \circ b^{-1} = b^{-1} \circ b \circ h_1 \circ b^{-1}
\]

\[
b^{-1} \circ h_1 \circ e = e \circ h_1 \circ b^{-1}
\]

\[
b^{-1} \circ h_1 = h_1 \circ b^{-1},
\]

and \( b^{-1} \) also commutes with \( h_1 \). Hence, \( a \circ (h_1 \circ b^{-1}) = a \circ b^{-1} \circ h_1 \), and \( h_1 \circ (a \circ b^{-1}) = (a \circ b^{-1}) \circ h_1, \forall h_1 \in H \). Thus, \( a \circ b^{-1} \in C(H) \), and \( C(H) \leq G \) by the One-Step Subgroup Test.

Next, consider \( h_1 \circ g \). Because \( H \) is a normal subgroup of \( G \), we know that \( h_1 \circ g = g \circ h_2 \) for some \( h_2 \in H \). Applying \( g^{-1} \) on both the left and right yields

\[
g^{-1} \circ h_1 \circ g \circ g^{-1} = g^{-1} \circ g \circ h_2 \circ g^{-1},
\]

\[
g^{-1} \circ h_1 \circ e = e \circ h_2 \circ g^{-1},
\]

\[
g^{-1} \circ h_1 = h_2 \circ g^{-1}.
\]

Thus, if \( h_1 \circ g = g \circ h_2 \), then \( g^{-1} \circ h_1 = h_2 \circ g^{-1} \).

Finally, let \( k \in C(H) \) and consider \( h_1 \circ (g \circ k \circ g^{-1}) \). Since \( H \triangleleft G \), \( h_1 \circ g = g \circ h_2 \), and

\[
(h_1 \circ g) \circ k \circ g^{-1} = g \circ h_2 \circ k \circ g^{-1}.
\]

By the definition of \( C(H) \), we know that \( k \) commutes with all elements of \( H \), so

\[
g \circ (h_2 \circ k) \circ g^{-1} = g \circ k \circ h_2 \circ g^{-1}.
\]

By what was shown above, \( h_2 \circ g^{-1} = g^{-1} \circ h_1 \), and hence

\[
g \circ k \circ (h_2 \circ g^{-1}) = g \circ k \circ g^{-1} \circ h_1.
\]

Thus, \( h_1 \circ (g \circ k \circ g^{-1}) = (g \circ k \circ g^{-1}) \circ h_1 \), and \( g \circ k \circ g^{-1} \) commutes with all \( h_1 \in H \) for all \( k \in K \). Therefore, by definition \( g \circ k \circ g^{-1} \in C(H), \forall g \in G \), or equivalently \( gC(H)g^{-1} \subseteq C(H) \), and \( C(H) \triangleleft G \) by the Normal Subgroup Test. \( \blacksquare \)
5. [Kizzier, A.] Prove the following properties of rings. Let $a$, $b$, and $c$ be elements of a ring $R$. Then

3. \((-a)(-b) = ab\).

\[
\begin{align*}
0 &= 0(-b) \\
0 &= (-a + a)(-b) \\
0 &= (-a)(-b) + a(-b) \\
0 &= (-a)(-b) - (ab) \\
ab &= (-a)(-b).
\end{align*}
\]

4. \(a(b - c) = ab - ac\) and \((b - c)a = ba - ca\).

\[
\begin{align*}
a(b - c) &= a(b + (-c)) \\
&= ab + a(-c) \\
&= ab + (-ac) \\
&= ab - ac.
\end{align*}
\]

Furthermore, if $R$ has unity 1, then

5. \((-1)a = -a\).

Using rule number 2, \((-1)a = -(1a) = -a\).

6. \((-1)(-1) = 1\).

Using rule number 3, \((-1)(-1) = 1 \cdot 1 = 1\).

7. The unity element is unique.

Let $x, y \in R$ such that for each $r \in R$, we have $rx = xr = r$ and $ry = yr = r$. This means that $x$ and $y$ are both unity elements. If we choose $r = y$ and use our first equation, then $xy = yx = y$. If we choose $r = x$ and use our second equation, then $xy = yx = x$. Then $x = y$, and the unity element is unique.

8. Multiplicative inverses are unique.

Let $r \in R$. Suppose that $x, y \in R$ such that $rx = xr = 1$ and $ry = yr = 1$. This means that $x$ and $y$ are both multiplicative inverses of $r$. Then $xr = yr$. Since $x$ is a multiplicative inverse of $r$, then $xrx = yrx$. So

\[
\begin{align*}
x &= x \cdot 1 \\
&= x(rx) \\
&= y(rx) \\
&= y \cdot 1 \\
&= y.
\end{align*}
\]

Since $x = y$, then multiplicative inverses are unique.
6. [Rotert, A.] Suppose that $R$ is a ring and that $a^2 = a$ for all $a \in R$. Show that $R$ is commutative. (A ring in which $a^2 = a$ for all $a$ is called a **Boolean** ring, in honor of the English mathematician George Boole (1815-1864).) Hint: consider for $a, b \in R$ the quantity $(a + b)^2$.

**Proof.** Consider $a, b \in R$. Then

\[
(a + b)^2 = a^2 + ab + ba + b^2 \\
(a + b) = a + ab + ba + b \\
(a + b) = ab + ba + (a + b) \\
0 = ab + ba \quad \text{(By cancellation)} \\
ab = -ba.
\]

This second step works because $R$ is a ring, and is thus closed, so $(a + b) = c, \exists c R$, and $c^2 = c$. Using this, then, we can say

\[
ab = (ab)^2 \\
\quad = (-ba)^2 \\
\quad = (-ba)(-ba) \\
\quad = (ba)(ba) \\
\quad = (ba)^2 \\
\quad = ba.
\]

Therefore, we can conclude that a Boolean ring is commutative.

7. [Franck, D.] Prove that if $H$ has index 2 in $G$, then $H$ is normal in $G$. Hint: use the definition of a normal subgroup, not the Normal Subgroup Test.

**Proof.** Let $H$ be a subgroup of index 2 in group $G$. Choose $g \in G$. We need to show that $gH = Hg$. By definition, we know that the index suggests that there will be two distinct left cosets of $H$ in $G$. This leaves two cases to consider.

If $g \in H$, then $gH = Hg$, because we know that $gH = H$ and $Hg = H$, by a previous proof. Thus $gH = Hg$ in this case.

Otherwise, if we have $g \in G \setminus H$, we know that $gH \neq H$, since $g \notin H$. This suggests that $gH = G \setminus H$ and $Hg = G \setminus H$. Therefore, $gH = Hg$ in this case, as well.

Thus, by the definition of a normal subgroup, the subgroup $H$ is normal in $G$.  ■
8. [Cosand, K.] Let $G$ be a finite group, and let $H$ be a normal subgroup of $G$. Prove that the order of the element $gH$ in $G/H$ must divide the order of $g$ in $G$.

**Proof. (Cosand, K.)** Let $|g| = n$, then we know $g^n = e$. Let $|gH| = k$. If we consider $(gH)^n$, then we know $(gH)^n = (g^n)H = eH = H$. Note that $H$ is the identity for the factor group $G/H$. By Corollary 2 on Page 79 in the book, we know for a group $G$ and $a \in G$ with $|a| = k$, that if $a^n = e$, then $k$ divides $n$. If we apply this idea to our current problem, we can conclude that $k|n$.

**Proof. (Gates, S.)** Consider the mapping $\psi : G \to G/H$ given by $\psi(g) = gH$. If $\phi$ preserves the group operation, $\psi$ is a homomorphism. By definition of the quotient group, the operation is $aH \circ bH = (a \circ b)H$. Consider, then, for $a,b \in G$:

$$
\psi(a) \circ \psi(b) = aH \circ bH = (a \circ b)H = \psi(a \circ b).
$$

Thus the group operation is preserved, and $\psi$ is a homomorphism.

Also consider $|g| = k$, and recall that $H$ is the identity of $G/H$. Then for $gH \in G/H$

$$
(gH)^k = \psi(g)^k = \psi(g^k) = \psi(e) = H.
$$

Thus $(gH)^k = H$, or the order of $gH$ in $G/H$ divides $k$, the order of $g$ in $G$.

9. [Leonard, R.] Let $\phi$ be an isomorphism from a group $G_1$ onto a group $G_2$. Prove that if $H$ is a normal subgroup of $G_1$, then $\phi(H)$ is a normal subgroup of $G_2$.

**Proof.** The first step of this proof is to prove that $\phi(x)\phi(H) = \phi(xH)$. To do this, we will use a containment argument.

(⊇) Take $a \in \phi(x)\phi(H)$. Then $a = \phi(x)\phi(h), \exists h \in H$. Moreover

$$
a = \phi(x)\phi(h)
= \phi(x \circ h).
$$

Thus $a \in \phi(xH)$.

(⊆) Take $a \in \phi(xH)$. Then $a = \phi(x \circ h), \exists h \in H$. Moreover

$$
a = \phi(x \circ h)
= \phi(x) \circ \phi(h).
$$

Thus $a \in \phi(x)\phi(H)$.

Since $a$ is in both $\phi(x)\phi(H)$ and $\phi(xH)$, it must be that $\phi(xH) = \phi(x)\phi(H)$. Similarly, we can show $\phi(Hx) = \phi(H)\phi(x)$.

Since $H \triangleleft G_1$, we know that $xH = Hx, \forall x \in G_1$, and that $\phi(H) \leq G_2$.

Consider $y \in G_2$. Since $\phi$ is surjective, we know $\exists x \in G_1$ such that $\phi(x) = y$. Thus

$$
y\phi(H) = \phi(x)\phi(H) = \phi(xH) = \phi(Hx) = \phi(H)\phi(x) = \phi(H)y
$$

and we see that $\phi(H) \triangleleft G_2$, because $y\phi(H) = \phi(H)y, \forall y \in G_2$.

26
10. [Franck, D.] Show, by example, that for fixed nonzero elements $a$ and $b$ in a ring, the equation $ax = b$ can have more than one solution. How does this compare with groups?

If we use the ring $\mathbb{Z}_{12}$, and choose $a = 2$ and $b = 6$, then the equation $ax = b$ will have two solutions: $x = 3$ and $x = 9$.

Let's prove these. If $x = 3$, then $2 \cdot 3 \equiv 6 \pmod{12}$. Likewise, if $x = 9$, then $2 \cdot 9 \equiv 18 \equiv 6 \pmod{12}$.

Thus there are two solutions for the equation $ax = b$.

Alternatively, with groups, if $a \circ x = b$, then $x = a^{-1} \circ b$, so there is always one unique solution.

11. [Gruenig, S.] Find an integer $n$ that shows that the rings $\mathbb{Z}_n$ need not have the following properties that the ring of integers has.

(a) $a^2 = a$ implies $a = 0$ or $a = 1$.
(b) $ab = 0$ implies $a = 0$ or $b = 0$.
(c) $ab = ac$ and $a \neq 0$ imply $b = c$.

Consider the ring $\mathbb{Z}_6$.

(a) Let $a = 3$. Then $3^2 = 9 \equiv 3 \pmod{6}$. So $a^2 = a$, and $a^2 = a$ does not imply $a = 0$ or $a = 1$ for $\mathbb{Z}_6$.

(b) Let $a = 2$ and $b = 3$. Then $2 \cdot 3 = 6 \equiv 0 \pmod{6}$. So $ab = 0$ does not imply $a = 0$ or $b = 0$ for $\mathbb{Z}_6$.

(c) Let $a = 3$, $b = 3$, and $c = 1$. Consider $ab$ and $ac$. Then $ab = 3 \cdot 3 = 9 \equiv 3 \pmod{6}$, and $bc = 3 \cdot 1 = 3$. So $ab = ac$, but $b \neq c$. Thus, $ab = ac$ does not imply $b = c$ for $\mathbb{Z}_6$.

Therefore, the integer 6 shows that the rings $\mathbb{Z}_n$ need not have these properties.