Recall: Chapter 7, Problem 6

If n be a positive integer, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$. There are exactly n left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$:

$$\begin{aligned}
0 + H &= n + H = 2n + H = 3n + H = \ldots \\
1 + H &= (n+1) + H = (2n+1) + H = (3n+1) + H = \ldots \\
2 + H &= (n+2) + H = (2n+2) + H = (3n+2) + H = \ldots \\
&\vdots \\
(n-1) + H &= (2n-1) + H = (3n-1) + H = (4n-1) + H = \ldots
\end{aligned}$$

- 2 cosets $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$ are equal $\Leftrightarrow b - a \in n\mathbb{Z}$.
- **Recall:** Just because $aH = bH$ does not mean $ah = bh$ for all (or even any) $h \in H$. In our above example, which demonstrates the additive case, $1 + H = (n+1) + H$, but of course there is *no* $h \in H$ for which $1 + h = n + 1 + h$.

Example, continued

Thus the set of all left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ is

$$S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

Does this remind you of anything?

Example, continued

Thus the set of all left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ is

$$S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

Does this remind you of anything?

What if we write it as

$$S = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}?$$

Example, continued

Thus the set of all left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ is

$$S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

Does this remind you of anything?

What if we write it as

$$S = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}?$$

It looks a lot like $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Can we define an operation so that S is a group?

Example (continued):

Let

$$\begin{aligned} S &= \text{the set of all left cosets of } n\mathbb{Z} \text{ in } \mathbb{Z} \\ &= \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} \end{aligned}$$

What operation could we define that would make S a group?

Example (continued):

Let

$$\begin{aligned} S &= \text{the set of all left cosets of } n\mathbb{Z} \text{ in } \mathbb{Z} \\ &= \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} \end{aligned}$$

What operation could we define that would make S a group?

Define $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}$.

Example (continued):

Let

$$\begin{aligned} S &= \text{the set of all left cosets of } n\mathbb{Z} \text{ in } \mathbb{Z} \\ &= \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} \end{aligned}$$

What operation could we define that would make S a group?

Define $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}$.

Need to check that G is closed under this operation, the operation is

associative, there is an identity element in G, and G is closed under inverses.

Example (continued):

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

- Is S closed under this operation?

Example (continued):

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

- Since $a + b \in \mathbb{Z}$, $a + b + n\mathbb{Z}$ is indeed one of the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$. Thus S is closed under the operation.
- Is the operation associative?

Example (continued):

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

- Since $a + b \in \mathbb{Z}$, $a + b + n\mathbb{Z}$ is indeed one of the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$. Thus S is closed under the operation.
- We can see below that the operation is associative:

$$\begin{aligned} &[(a + n\mathbb{Z}) + (b + n\mathbb{Z})] + (c + n\mathbb{Z}) \\ &\quad = (a + b + n\mathbb{Z}) + (c + n\mathbb{Z}) \\ &\quad = [(a + b) + c] + n\mathbb{Z} \\ &\quad = [a + (b + c)] + n\mathbb{Z} \\ &\quad = (a + n\mathbb{Z}) + (b + c + n\mathbb{Z}) \\ &\quad = (a + n\mathbb{Z}) + [(b + n\mathbb{Z}) + (c + n\mathbb{Z})] \end{aligned}$$

Thus the operation on S is associative.

Example (continued):

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

- Since $a + b \in \mathbb{Z}$, $a + b + n\mathbb{Z}$ is indeed one of the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$. Thus S is closed under the operation.
- Since $[(a + n\mathbb{Z}) + (b + n\mathbb{Z})] + (c + n\mathbb{Z}) = (a + n\mathbb{Z}) + [(b + n\mathbb{Z}) + (c + n\mathbb{Z})]$, the operation is associative.
- Does S contain an identity element?

Example (continued):

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

- Since $a + b \in \mathbb{Z}$, $a + b + n\mathbb{Z}$ is indeed one of the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$. Thus S is closed under the operation.
- Since $[(a + n\mathbb{Z}) + (b + n\mathbb{Z})] + (c + n\mathbb{Z}) = (a + n\mathbb{Z}) + [(b + n\mathbb{Z}) + (c + n\mathbb{Z})]$, the operation is associative.
- $0 + n\mathbb{Z}$ acts as an identity:

$$\begin{aligned}(a + n\mathbb{Z}) + (0 + n\mathbb{Z}) &= (a + 0) + n\mathbb{Z} = a + n\mathbb{Z}\\ (0 + n\mathbb{Z}) + (a + n\mathbb{Z}) &= (0 + a) + n\mathbb{Z} = a + n\mathbb{Z}.\end{aligned}$$

Example (continued):

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

- Since $a + b \in \mathbb{Z}$, $a + b + n\mathbb{Z}$ is indeed one of the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$. Thus S is closed under the operation.
- Since $[(a + n\mathbb{Z}) + (b + n\mathbb{Z})] + (c + n\mathbb{Z}) = (a + n\mathbb{Z}) + [(b + n\mathbb{Z}) + (c + n\mathbb{Z})]$, the operation is associative.
- $0 + n\mathbb{Z}$ acts as an identity:
- Does every element of S have an inverse?

Example (continued):

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

- Since $a + b \in \mathbb{Z}$, $a + b + n\mathbb{Z}$ is indeed one of the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$. Thus S is closed under the operation.
- Since $[(a + n\mathbb{Z}) + (b + n\mathbb{Z})] + (c + n\mathbb{Z}) = (a + n\mathbb{Z}) + [(b + n\mathbb{Z}) + (c + n\mathbb{Z})]$, the operation is associative.
- $0 + n\mathbb{Z}$ acts as an identity:
- For all $a + n\mathbb{Z} \in S$, $-a + n\mathbb{Z}$ is also in S, and of course $-a + n\mathbb{Z}$ is the inverse of $a + n\mathbb{Z}$:

$$(-a + n\mathbb{Z}) + (a + n\mathbb{Z}) = 0 + n\mathbb{Z}.$$

Example (continued):

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

- Since $a + b \in \mathbb{Z}$, $a + b + n\mathbb{Z}$ is indeed one of the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$. Thus S is closed under the operation.
- Since $[(a + n\mathbb{Z}) + (b + n\mathbb{Z})] + (c + n\mathbb{Z}) = (a + n\mathbb{Z}) + [(b + n\mathbb{Z}) + (c + n\mathbb{Z})]$, the operation is associative.
- $0 + n\mathbb{Z}$ acts as an identity:
- For all $a + n\mathbb{Z} \in S$, $-a + n\mathbb{Z}$ is also in S, and of course $-a + n\mathbb{Z}$ is the inverse of $a + n\mathbb{Z}$:

$$(-a + n\mathbb{Z}) + (a + n\mathbb{Z}) = 0 + n\mathbb{Z}.$$

Thus G is a group under the above operation.

Example (continued):

Conclusion:

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

S is a group.

Example (continued):

Conclusion:

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

S is a group.

Important Note: While the inverse of $a + n\mathbb{Z}$ *is* $-a + n\mathbb{Z}$, it might not be written like that.

Example (continued):

Conclusion:

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

S is a group.

Important Note: While the inverse of $a + n\mathbb{Z}$ *is* $-a + n\mathbb{Z}$, it might not be written like that.

Example: The inverse of $1 + n\mathbb{Z}$ *is* $-1 + n\mathbb{Z}$, but that coset doesn't appear in the above list of elements in G.

Example (continued):

Conclusion:

Let $S = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, and define the operation on S to be

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \stackrel{def}{=} (a + b) + n\mathbb{Z}.$$

S is a group.

Important Note: While the inverse of $a + n\mathbb{Z}$ *is* $-a + n\mathbb{Z}$, it might not be written like that.

Example: The inverse of $1 + n\mathbb{Z}$ *is* $-1 + n\mathbb{Z}$, but that coset doesn't appear in the above list of elements in G.
Remember, $-1 + n\mathbb{Z} = (n-1) + n\mathbb{Z}$.

Question:

Is this always true? If we're given any group G, and any subgroup H, will the set of left cosets $\{aH | a \in G\}$ always be a group?

Consider

$$S_3 = \left\{\epsilon, \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\end{pmatrix}\right\}.$$

Consider

$$S_3 = \left\{\epsilon, \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\end{pmatrix}\right\}.$$

Let $\alpha = \begin{pmatrix}1 & 2\end{pmatrix}$, $\beta = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$.
Then $\beta^2 = \begin{pmatrix}1 & 3 & 2\end{pmatrix}$, $\alpha\beta = \begin{pmatrix}2 & 3\end{pmatrix}$, and $\alpha\beta^2 = \begin{pmatrix}1 & 3\end{pmatrix}$.

Next consider the subgroup $H = \left\{\epsilon, \begin{pmatrix}1 & 2\end{pmatrix}\right\} = \{1, \alpha\}$.

By using a Cayley table, we can quickly find the set of all cosets of H in S_3:

	ϵ	α	β	β^2	$\alpha\beta$	$\alpha\beta^2$
ϵ	ϵ	α	β	β^2	$\alpha\beta$	$\alpha\beta^2$
α	α	ϵ	$\alpha\beta$	$\alpha\beta^2$	β	β^2
β	β	$\alpha\beta^2$	β^2	ϵ	α	$\alpha\beta$
β^2	β^2	$\alpha\beta$	ϵ	β	$\alpha\beta^2$	α
$\alpha\beta$	$\alpha\beta$	β^2	$\alpha\beta^2$	α	ϵ	β
$\alpha\beta^2$	$\alpha\beta^2$	β	α	$\alpha\beta$	β^2	ϵ

We can thus see that the $\dfrac{6}{2} = 3$ left cosets of H in S_3 are:

$$\epsilon H = \{\epsilon, \alpha\} \qquad \beta H = \{\beta, \alpha\beta^2\} \qquad \alpha\beta H = \{\alpha\beta, \beta^2\}$$

The $\frac{6}{2} = 3$ left cosets of H in S_3 are:

$$\epsilon H = \{\epsilon, \alpha\} \qquad \beta H = \{\beta, \alpha\beta^2\} \qquad \alpha\beta H = \{\alpha\beta, \beta^2\}$$

Try to define an operation on the set of cosets analogously to the way we did in our first example,

$$xH \circ yH = (x \circ y)H.$$

The $\frac{6}{2} = 3$ left cosets of H in S_3 are:

$$\epsilon H = \{\epsilon, \alpha\} \qquad \beta H = \{\beta, \alpha\beta^2\} \qquad \alpha\beta H = \{\alpha\beta, \beta^2\}$$

Try to define an operation on the set of cosets analogously to the way we did in our first example,

$$xH \circ yH = (x \circ y)H.$$

$$\begin{aligned} \beta H \circ \alpha\beta H &= (\beta \circ \alpha\beta)H = \alpha H = \epsilon H \\ \alpha\beta^2 H \circ \alpha\beta H &= (\alpha\beta^2 \circ \alpha\beta)H = \beta^2 H = \alpha\beta H \end{aligned}$$

The $\frac{6}{2} = 3$ left cosets of H in S_3 are:

$$\epsilon H = \{\epsilon, \alpha\} \qquad \beta H = \{\beta, \alpha\beta^2\} \qquad \alpha\beta H = \{\alpha\beta, \beta^2\}$$

Try to define an operation on the set of cosets analogously to the way we did in our first example,

$$xH \circ yH = (x \circ y)H.$$

$$\begin{aligned} \beta H \circ \alpha\beta H &= (\beta \circ \alpha\beta)H = \alpha H = \epsilon H \\ \alpha\beta^2 H \circ \alpha\beta H &= (\alpha\beta^2 \circ \alpha\beta)H = \beta^2 H = \alpha\beta H \end{aligned}$$

Thus $\beta H = \alpha\beta^2 H$, but $\beta H \circ \alpha\beta H \neq (\alpha\beta^2 \circ \alpha\beta)H$!
The operation isn't even well-defined!

Question:

For what groups G, and for what subgroups H, does the set of all left (right) cosets of H in G form a group under the operation $aH * bH \stackrel{def}{=} (a * b)H$?

Properties of cosets:

Let H be a subgroup of a group G, and let a and b belong to G. Then,

1. $a \in aH$
2. $aH = H \iff a \in H$
3. $aH = bH \iff a \in bH$
4. $aH = bH$ or $aH \bigcap bH = \emptyset$
5. $aH = bH \iff a^{-1}b \in H$
6. $|aH| = |bH| = |H|$
7. $\boxed{aH = Ha \iff H = aHa^{-1}}$
8. $aH \leq G \iff a \in H$

Analogous results hold for right cosets!

Cayley table for S_3

Let

$$\alpha = \begin{pmatrix} 1 & 2 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \qquad \beta^2 = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$$

$$\alpha\beta = \begin{pmatrix} 2 & 3 \end{pmatrix} \qquad \alpha\beta^2 = \begin{pmatrix} 1 & 3 \end{pmatrix}$$

	ϵ	α	β	β^2	$\alpha\beta$	$\alpha\beta^2$
ϵ	ϵ	α	β	β^2	$\alpha\beta$	$\alpha\beta^2$
α	α	ϵ	$\alpha\beta$	$\alpha\beta^2$	β	β^2
β	β	$\alpha\beta^2$	β^2	ϵ	α	$\alpha\beta$
β^2	β^2	$\alpha\beta$	ϵ	β	$\alpha\beta^2$	α
$\alpha\beta$	$\alpha\beta$	β^2	$\alpha\beta^2$	α	ϵ	β
$\alpha\beta^2$	$\alpha\beta^2$	β	α	$\alpha\beta$	β^2	ϵ

In Class Work

Show that $< R_{90} > \triangleleft D_4$.

To make your life easier, here is the Cayley table for D_4:

$\circ$	R_0	R_{90}	R_{180}	R_{270}	H	N	V	P
R_0	R_0	R_{90}	R_{180}	R_{270}	H	N	V	P
R_{90}	R_{90}	R_{180}	R_{270}	R_0	P	H	N	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	P	H	N
R_{270}	R_{270}	R_0	R_{90}	R_{180}	N	V	P	H
H	H	N	V	P	R_0	R_{90}	R_{180}	R_{270}
N	N	V	P	H	R_{270}	R_0	R_{90}	R_{180}
V	V	P	H	N	R_{180}	R_{270}	R_0	R_{90}
P	P	H	N	V	R_{90}	R_{180}	R_{270}	R_0

Solutions:

Method 1: Using the definition of normal

Show that $< R_{90} > \triangleleft D_4$.

1. If $a \in < R_{90} >$, then of course $a < R_{90} > = < R_{90} > = < R_{90} > a$, by Property 1 of the lemma in Chapter 7.
   Note: $a < R_{90} >$ consists of all the rotations in D_4.
2. If $a \notin < R_{90} >$, then a is a reflection.
   In that case (see the Cayley table), $a < R_{90} >$ consists of all the reflections in D_4. Similarly, $< R_{90} > a$ also consists of all the reflections in D_4. Thus $a < R_{90} > = < R_{90} > a$.

Conclusion: Thus no matter what a is, $a < R_{90} > = < R_{90} > a$, and so $< R_{90} >$ is normal.

Solutions:

Method 2: Using one of our Results

Show that $< R_{90} > \triangleleft D_4$.

Since $|D_4| = 8$ and $| < R_{90} > | = 4$,

$$[D_4 :< R_{90} >] = 2,$$

and so by the example we just did, $< R_{90} >$ must be normal.