18 More Groups, Lagrange’s Theorem and Direct Products

We consider several ways to produce groups.

18.1 The Dihedral Group

The dihedral group $D_n$ is a nonabelian group. This is the set of “symmetries” of a regular $n$-gon: the motions that leave the $n$-gon looking unchanged. One can rotate the polygon $360/n$ degrees, or indeed any multiple thereof. One can also think of reflection around various axes. Specifically, the dihedral group has $2n$ elements. There are $n - 1$ rotations and $n$ flips. For motions $m_1$ and $m_2$, we define $m_1 \ast m_2$ to be the motion obtained by $m_1$ followed by $m_2$.

**Example 18.1.** Consider $D_3$.

This is the symmetry group of an equilateral triangle. Say $r$ is the rotation 120 degrees clockwise, $r'$ the rotation 120 degrees counterclockwise, and $f_i$ the flip around an axis through the center and corner labeled $i$. Then we get the pictures and table.

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$r$</th>
<th>$r'$</th>
<th>$f_1$</th>
<th>$f_2$</th>
<th>$f_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$r$</td>
<td>$r'$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$r$</td>
<td>$r$</td>
<td>$r'$</td>
<td>$e$</td>
<td>$f_2$</td>
<td>$f_3$</td>
<td>$f_1$</td>
</tr>
<tr>
<td>$r'$</td>
<td>$r'$</td>
<td>$e$</td>
<td>$r$</td>
<td>$f_3$</td>
<td>$f_1$</td>
<td>$f_2$</td>
</tr>
<tr>
<td>$f_1$</td>
<td>$f_1$</td>
<td>$f_3$</td>
<td>$f_2$</td>
<td></td>
<td>$e$</td>
<td>$r'$</td>
</tr>
<tr>
<td>$f_2$</td>
<td>$f_2$</td>
<td>$f_1$</td>
<td>$f_3$</td>
<td>$r$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$f_3$</td>
<td>$f_3$</td>
<td>$f_2$</td>
<td>$f_1$</td>
<td>$r'$</td>
<td>$e$</td>
<td></td>
</tr>
</tbody>
</table>

©Wayne Goddard, Clemson University, 2023
In general, in $D_n$ a flip is its own inverse. The inverse of a rotation is another rotation. Other group properties can be checked.

### 18.2 Lagrange’s Theorem

There is a famous result about the relationship between finite groups and subgroups:

**Theorem 18.1 Lagrange’s Theorem.** The order of a subgroup divides the order of the group.

We will attempt a proof of Lagrange’s Theorem in a moment. A special case is that, if the group is finite, then the order of an element divides the order of the group. One consequence of this is **Fermat’s Little Theorem**. This follows from Lagrange’s theorem, because the order of element $a$ is a divisor of the order of $\mathbb{Z}_p^*$, which is $p - 1$.

### 18.3 Coset Groups and a Proof of Lagrange’s Theorem

We show how to partition a group based on a subgroup of a group.

Let $G$ be a group. For a subgroup $H$ and $a \in G$, the **left coset** $aH$ is the set of elements $\{ah : h \in H\}$. That is, take everything in $H$ and multiply on the left by $a$. (Right cosets are defined similarly.)

Note that the elements of $aH$ have to be distinct (by the cancellation law). So, $H$ has the same size as any left coset. Indeed, in particular each coset has the same size. Now, the key observation (which basically says being in the same coset is an equivalence relation):

**Lemma 18.2** If two cosets of $H$ intersect, then they are equal.

**Proof.** Suppose cosets $aH$ and $bH$ intersect. That is, $ah_1 = bh_2$ for some $h_1, h_2 \in H$. Then consider any element of $aH$, say $ah$. Then $ah = bh_2h_1^{-1}h$; since $h_2h_1^{-1}h \in H$, it follows that $ah \in bH$. Similarly, every element of $bH$ is in $aH$. Thus the cosets are identical. ◊

It follows that the left cosets form a partition of $G$, and each coset has the same size. So:

> the order of group $G$ is the order of subgroup $H$ times the number of distinct cosets of $H$.

From this, Lagrange’s theorem follows.
18.4 Direct Sums

Let $G$ and $H$ be groups. The **direct sum** (or direct product) of $G$ and $H$ is a new group written $G \times H$. It is formed by taking all ordered pairs, one element from $G$ and one element of $H$, with vector operation. That is,

$$(a, b) \star (c, d) = (a \star_G c, b \star_H d).$$

It can be checked that the result is a group. The identity is $(e_G, e_H)$. The inverse of $(a, b)$ is $(a^{-1}, b^{-1})$.

Note that the direct sum of abelian groups is itself abelian.

---

**Example 18.2.** Consider $\mathbb{Z}_2 \times \mathbb{Z}_2$.

This contains $(0, 0)$, $(0, 1)$, $(1, 0)$ and $(1, 1)$. Its table is:

<table>
<thead>
<tr>
<th></th>
<th>(0, 0)</th>
<th>(0, 1)</th>
<th>(1, 0)</th>
<th>(1, 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0)</td>
<td>(0, 0)</td>
<td>(0, 1)</td>
<td>(1, 0)</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>(0, 1)</td>
<td>(0, 1)</td>
<td>(0, 0)</td>
<td>(1, 1)</td>
<td>(1, 0)</td>
</tr>
<tr>
<td>(1, 0)</td>
<td>(1, 0)</td>
<td>(1, 1)</td>
<td>(0, 0)</td>
<td>(0, 1)</td>
</tr>
<tr>
<td>(1, 1)</td>
<td>(1, 1)</td>
<td>(1, 0)</td>
<td>(0, 1)</td>
<td>(0, 0)</td>
</tr>
</tbody>
</table>

18.5 Group Isomorphism

What makes two groups the same? We say that groups $G$ and $H$ are **isomorphic** if there is a bijective mapping $f: G \rightarrow H$, such that $f(a \star_G b) = f(a) \star_H f(b)$. By bijective, we mean that every element of $G$ is paired with a unique element of $H$ and vice versa. The mapping $f$ is called an **isomorphism**.

**Example 18.3.** $\mathbb{Z}_6^*$ is isomorphic to $\mathbb{Z}_2$.

For, the former has set $\{1, 5\}$ and the latter has set $\{0, 1\}$. If we map $1 \mapsto 0$ and $5 \mapsto 1$, then the mapping is bijective, and the operation is preserved (the table looks the same).

Indeed, it is not hard to show that all groups with 2 elements are isomorphic.

**Example 18.4.** $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$.

The bijection is $(a, b) \rightarrow (3a + 2b) \mod 6$. 

Example 18.5. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$.

(Think how the tables compare.)

Note:

- To show two groups are isomorphic, find a bijection.
- To show two groups are not isomorphic, find a property that one of them has that the other one doesn’t.

There is a general theorem about such products:

**Theorem 18.3** The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to the group $\mathbb{Z}_{mn}$ if and only if $m$ and $n$ are relatively prime.

We leave the proof as an exercise.

**Exercises**

18.1. Determine the group of symmetries of the following shapes:

(a) The letter: $\mathcal{S}$

(b) The plus sign: $\mathbf{+}$

(c) A flower

(d) This shape is infinite: $\cdots \longrightarrow \longrightarrow \longrightarrow \longrightarrow \cdots$

18.2. Prove that two cosets $aH$ and $bH$ are equal if and only if $b^{-1}a \in H$. 
18.3. Consider the group of $2 \times 2$ matrices with nonzero determinant.

(a) Give an element of order 2.
(b) Give a nontrivial/proper subgroup.

18.4. Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_5$.

(a) What is the order of the group?
(b) What is the identity?
(c) List all elements of order 5.

18.5. Consider the complex numbers $\{1, -1, i, -i\}$ with operation multiplication. What group is this isomorphic to?

18.6. Prove that, if $G$ has even order, then it must have an element of order 2.

18.7. Show that if $p$ is a prime, then all groups of order $p$ are cyclic and indeed isomorphic.

18.8. Suppose groups $G$ and $H$ each have order 100 and each contain an element of order 100. Prove that $G$ and $H$ are isomorphic.

18.9. Prove that every group of order 15 is cyclic.

18.10. Consider the following table for a group.

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

(a) What is the identity?
(b) Give an element of order 4.
(c) Is the group abelian? (Justify your answer.)
(d) Explain why we know this is not the dihedral group $D_4$. 
18.11. (a) Determine all the subgroups of the dihedral group $D_4$.  
(b) Determine all the subgroups of the dihedral group $D_5$. 

18.12. Determine all the subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. 

18.13. (a) Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is not isomorphic to $\mathbb{Z}_{mn}$ if $m$ and $n$ are not relatively prime. 
(b) Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_{mn}$ if $m$ and $n$ are relatively prime. 

18.14. Let group $G = \mathbb{Z}_{9409} \times \mathbb{Z}_{97}$. Note that 97 is prime and that $9409 = 97^2$. 
(a) What is the identity element in $G$? 
(b) How many elements of order 97 does $G$ have? Justify your answer. 
(c) How many elements of order 98 does $G$ have? Justify your answer.