16 Introduction to Groups

16.1 Definition

The structure $\mathbb{Z}_n$ we saw earlier is an example of a more general situation. A group is a set of elements $G$ together with a single binary operation, call it $\star$, such that it obeys the following rules:

1. $G$ is closed under the operation $\star$: that is, for all $a, b \in G$ it holds that $a \star b \in G$;
2. Associative law: $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c$;
3. There is an identity $e$ such that for all $a \in G$ we have $a \star e = e \star a = a$; and
4. Inverses exist: for all $a \in G$, there is an $a^{-1}$ such that $a \star a^{-1} = a^{-1} \star a = e$.

Note that commutativity is not assumed. Indeed, a group is called abelian if it satisfies:

5. Commutative law: $a \star b = b \star a$ for all $a, b$

In many of our examples, the group operation is addition or multiplication. For example:

- The positive real numbers form an abelian group under multiplication. Here 1 is the identity, and the inverse of $r$ is $1/r$. Note that all the real numbers does not work, since 0 has no inverse.
- The integers form an abelian group under addition. Here 0 is the identity, and the inverse of $r$ is $-r$.
- The set of all $2 \times 2$ nonsingular matrices forms a nonabelian group under matrix multiplication. The identity matrix $I$ is the identity, and the inverse of matrix $A$ is $A^{-1}$.

Notation for the operation: We use the standard symbol if it is a common specific operation, like addition or multiplication. Otherwise, we often use “implicit multiplication” notation: with elements simply written next to each other. The associative law means we can omit brackets completely.
16.2 Basic Facts

Some fundamental properties are the following:

Lemma 16.1
(a) The identity element is unique.
(b) The inverse of an element is unique.
(c) \((a^{-1})^{-1} = a\).
(d) \((ab)^{-1} = b^{-1}a^{-1}\).

Proof. We show (d). The rest are left as an exercise. To show that something is the inverse, one needs to show that multiplying by it produces the identity. So,

\[
(ab) \ast (b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = e.
\]

Similarly, \((b^{-1}a^{-1})(ab) = e\). ♦

Note that because we do not assume commutativity, we have to be explicit about whether we are doing the operation on the left or on the right. Nevertheless, \(a \ast b = a \ast c\) implies, multiplying on the left by \(a^{-1}\), that \(b = c\). This is often referred to:

Cancellation Law: if \(a \ast b = a \ast c\) then \(b = c\); if \(b \ast a = c \ast a\) then \(b = c\).

One can produce a table, where the \((i, j)\) entry gives the result of the operation applied to the \(i\)th entry and the \(j\)th entry. Note that each row contains every element exactly once. Why? Every element must be there, since, for any given \(a\) and \(b\), the equation \(a \ast x = b\) has a solution, namely \(x = a^{-1} \ast b\). By the cancellation law, this solution is unique.

For example, here is the table for a group with four elements \(\{e, a, b, c\}\).

\[
\begin{array}{cccc}
<table>
<thead>
<tr>
<th></th>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>e</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>e</td>
</tr>
</tbody>
</table>
\end{array}
\]
16.3 Modular Groups

Modular arithmetic is where we find two famous abelian groups.

- \( \mathbb{Z}_n \). This is the set of integers \( \{0, 1, \ldots, n - 1\} \) with the operation addition modulo \( n \). The element 0 is the identity, and, apart from 0, \( n - a \) is the inverse of \( a \).

- \( \mathbb{Z}_n^* \). This is the set of integers in the range 1 up to \( n - 1 \) that are relatively prime to \( n \), together with multiplication modulo \( n \).

---

Example 16.1. Here is the table for \( \mathbb{Z}_{12}^* \)

<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>

It takes some checking to see that \( \mathbb{Z}_n^* \) is indeed always a group. First, if we multiply two numbers that are relatively prime to \( n \), then the result is still relatively prime to \( n \). So even when we do the mod \( n \) part, the result is in \( \mathbb{Z}_n^* \). Thus we have closure. The value 1 is, of course, the identity. Recall that the existence of inverses comes from Extended Euclid’s algorithm: if gcd\((a, n) = 1\), then there are \( s \) and \( t \) such that \( as + nt = 1 \). Now, if \( s \) and \( n \) have a common factor, then that is a common factor of \( as + nt \), a contradiction. So the inverse \( s \) is relatively prime to \( a \), and hence in the set.

16.4 Subgroups

An important concept is a \textbf{subgroup}. This is a subset of the elements that contains the identity, and is closed under multiplication and inverses. For example, for the group \( \mathbb{Z} \) with addition, the even integers form a subgroup. In general there are always at least two subgroups: the group itself and \( \{e\} \). These are called the \textbf{trivial} subgroups.

---

Example 16.2. The subgroups of \( \mathbb{Z}_n \)

The subset of \( \mathbb{Z}_n \) consisting of all multiples of \( a \) is a subgroup for any \( a \).
The set of $2 \times 2$ matrices with determinant 1 form a subgroup of the set of all nonsingular $2 \times 2$ matrices.

A group/subgroup is generated by a set $X$ if it consists of all arbitrary products of elements in $X$ and their inverses. A group that is generated by a single element is called a cyclic group.

We use the notation $a^n$ as the notation for $n$ $a$’s multiplied together. Consider the sequence $e, a, a^2, a^3, a^4, \ldots$. If the group is finite, there must come a point in the sequence that we have a repeat. Suppose that first repeat is $a^n$, and that $a^n$ equals $a^m$ for $m < n$. Then by cancellation $a^{n-m} = e$. So, actually there is no repeat until we reach $e$. The first positive power of $a$ that equals the identity is called the order of $a$. We also use the term order of a group to be the number of elements in the overall group. Thus, the order of an element $a$ is the order of the subgroup generated by $a$.

**Exercises**

16.1. (a) Show that the identity element is unique.
   (b) Show that the inverse of an element is unique.

16.2. Explain why the following is not a group:

$$
\begin{array}{cccc}
  e & a & b & c \\
  e & e & a & b \\
  a & a & a & e \\
  b & b & e & b \\
  c & c & e & c \\
\end{array}
$$

16.3. Consider the multiplicative group $\mathbb{Z}_{15}^*$
   (a) List the elements of the group.
   (b) Give the identity element.
   (c) Give the inverse of 7.
   (d) Give an element other than the identity that is self-inverse.

16.4. Let $q = 2^{100}$. Determine how many elements of $\mathbb{Z}_q$ have order $q$.

16.5. Show that a nonempty subset $S$ is a subgroup if and only if $a \ast b^{-1} \in S$ for all $a$ and $b$ in $S$. 
16.6. (a) Show that the intersection of two subgroups is again a subgroup.
   (b) What about union?

16.7. Show that every subgroup of \( \mathbb{Z}_n \) is given by the set of multiples of some integer \( a \).

16.8. Show that any subgroup of a cyclic group is itself cyclic.

16.9. (a) Show that if \( F \) and \( H \) are subgroups of an abelian group, then the set of products \( \{ fh : f \in F, h \in H \} \) is also a subgroup.
   (b) Explain where in your proof you used the fact that the group is abelian.

16.10. Consider the set \( \mathbb{Z}[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in \mathbb{Z} \} \). Show that \( \mathbb{Z}[\sqrt{2}] \) is a group under addition.

16.11. Fix some set \( X \). Let \( G \) be the set of all subsets of \( X \). For \( A, B \in G \), define \( A \triangle B \) to be the set of all elements that are in exactly one of \( A \) or \( B \); that is, \( A \triangle B = (A - B) \cup (B - A) \). Show that \( G \) is an abelian group under \( \triangle \).