Chapter Four

Elementary Properties of Groups

Is it possible for a group to have two different identity elements? Well, suppose \( e_1 \) and \( e_2 \) are identity elements of some group \( G \). Then

\[
e_1 \ast e_2 = e_2 \quad \text{because } e_1 \text{ is an identity element, and}
\]

\[
e_1 \ast e_2 = e_1 \quad \text{because } e_2 \text{ is an identity element}
\]

Therefore

\[
e_1 = e_2
\]

This shows that in every group there is exactly one identity element.

Can an element \( a \) in a group have two different inverses? Well, if \( a_1 \) and \( a_2 \) are both inverses of \( a \), then

\[
a_1 \ast (a \ast a_2) = a_1 \ast e = a_1
\]

and

\[
(a_1 \ast a) \ast a_2 = e \ast a_2 = a_2
\]

By the associative law, \( a_1 \ast (a \ast a_2) = (a_1 \ast a) \ast a_2 \); hence \( a_1 = a_2 \). This shows that in every group, each element has exactly one inverse.

Up to now we have used the symbol \( \ast \) to designate the group operation. Other, more commonly used symbols are \( + \) and \( \cdot \) ("plus" and "multiply"). When \( + \) is used to denote the group operation, we say we are using additive notation, and we refer to \( a + b \) as the sum of \( a \) and \( b \). (Remember that \( a \) and \( b \) do not have to be numbers and therefore "sum" does not, in general, refer to adding numbers.) When \( \cdot \) is used to denote the group operation, we say we are using multiplicative notation; we usually write \( ab \) instead of \( a \cdot b \), and call \( ab \) the product of \( a \) and \( b \). (Once again, remember that "product" does not, in general, refer to multiplying numbers.) Multiplicative notation is the most popular because it is simple and saves space. In the remainder of this book multiplicative notation will be used except where otherwise indicated. In particular, when we represent a group by a letter such as \( G \) or \( H \), it will be understood that the group's operation is written as multiplication.

There is common agreement that in additive notation the identity element is denoted by 0, and the inverse of \( a \) is written as \( -a \). (It is called the negative of \( a \).) In multiplicative notation the identity element is \( e \) and the inverse of \( a \) is written as \( a^{-1} \) ("\( a \) inverse"). It is also a tradition that + is to be used only for commutative operations.

The most basic rule of calculation in groups is the cancellation law, which allows us to cancel the factor \( a \) in the equations \( ab = ac \) and \( ab = ca \). This will be our first theorem about groups.

**Theorem 1** If \( G \) is a group and \( a, b, c \) are elements of \( G \), then

(i) \( ab = ac \) implies \( b = c \), and

(ii) \( ba = ca \) implies \( b = c \)

It is easy to see why this is true: if we multiply (on the left) both sides of the equation \( ab = ac \) by \( a^{-1} \), we get \( b = c \). In the case of \( ba = ca \), we multiply on the right by \( a^{-1} \). This is the idea of the proof; now here is the proof:

Suppose \( ab = ac \)

Then \( a^{-1}(ab) = a^{-1}(ac) \)

By the associative law, \( (a^{-1}a)b = (a^{-1}a)c \)

that is, \( eb = ec \)

Thus, finally, \( b = c \).

Part (ii) is proved analogously.

In general, we cannot cancel \( a \) in the equation \( ab = ca \). (Why not?)

**Theorem 2** If \( G \) is a group and \( a, b \) are elements of \( G \), then

\( ab = e \) implies \( a = b^{-1} \) and \( b = a^{-1} \)

The proof is very simple: if \( ab = e \), then \( ab = aa^{-1} \), so by the cancellation law, \( b = a^{-1} \). Analogously, \( a = b^{-1} \).

This theorem tells us that if the product of two elements is equal to \( e \), these elements are inverses of each other. In particular, if \( a \) is the inverse of \( b \), then \( b \) is the inverse of \( a \).

The next theorem gives us important information about computing inverses.
Theorem 3 If \( G \) is a group and \( a, b \) are elements of \( G \), then

(i) \((ab)^{-1} = b^{-1}a^{-1}\) and

(ii) \((a^{-1})^{-1} = a\)

The first formula tells us that the inverse of a product is the product of the inverses in reverse order. The next formula tells us that \( a \) is the inverse of the inverse of \( a \). The proof of (i) is as follows:

\[
(ab)(b^{-1}a^{-1}) = a[(bb^{-1})a^{-1}] \quad \text{by the associative law}
\]

\[
= a[e^{-1}] \quad \text{because } bb^{-1} = e
\]

\[
= aa^{-1}
\]

\[
= e
\]

Since the product of \( ab \) and \( b^{-1}a^{-1} \) is equal to \( e \), it follows by Theorem 2 that they are each other’s inverses. Thus, \((ab)^{-1} = b^{-1}a^{-1}\). The proof of (ii) is analogous, but simpler: \( a^{-1}a^{-1} = e \), so by Theorem 2 \( a \) is the inverse of \( a^{-1} \), that is, \( a = (a^{-1})^{-1} \).

The associative law states that the two products \( ab(c) \) and \( (ab)c \) are equal; for this reason, no confusion can result if we denote either of these products by writing \( abc \) (without any parentheses), and call \( abc \) the product of these three elements in this order.

We may next define the product of any four elements \( a, b, c, \) and \( d \) in \( G \) by

\[
abcd = a(bcd)
\]

By successive uses of the associative law we find that

\[
a(b)c = ab(cd) = (ab)(cd) = (ab)cd
\]

Hence the product \( abcd \) (without parentheses, but without changing the order of its factors) is defined without ambiguity.

In general, any two products, each involving the same factors in the same order, are equal. The net effect of the associative law is that parentheses are redundant.

Having made this observation, we may feel free to use products of several factors, such as \( a_1a_2 \cdots a_n \), without parentheses, whenever it is convenient. Incidentally, by using the identity \((ab)^{-1} = b^{-1}a^{-1}\) repeatedly, we find that

\[
(a_1a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1}a_1^{-1}
\]

If \( G \) is a finite group, the number of elements in \( G \) is called the order of \( G \). It is customary to denote the order of \( G \) by the symbol \(|G|\).

**EXERCISES**

**Remark on notation** In the exercises below, the exponential notation \( a^n \) is used in the following sense: if \( a \) is any element of a group \( G \), then \( a^n \) means \( a \cdot a \cdots a \) (where \( n \) factors of \( a \), for any positive integer \( n \).

**A. Solving Equations in Groups**

Let \( a, b, \) and \( c \) be elements of a group \( G \). In each of the following, solve for \( x \) in terms of \( a, b, \) and \( c \).

**Example** Solve simultaneously:

\[x^2 = b \quad \text{and} \quad x^5 = e\]

From the first equation, \( b = x^2\).

Squaring, \( b^2 = x^4\).

Multiplying on the left by \( x \), \( xb^2 = xx^4 = x^5 = e \). (Note: \( x^5 = e \) was given.)

Multiplying by \((b^2)^{-1}\), \( xb^2(b^2)^{-1} = e(b^2)^{-1}\). Therefore, \( x = (b^2)^{-1}\).

Solve:

1. \( axb = c\)
2. \( x^2b = xa^{-1}c\)

Solve simultaneously:

1. \( x^2a = bxc^{-1}\) and \( axc = xac\)
2. \( ax^2 = b\) and \( x^5 = c\)
3. \( x^3 = a^2\) and \( x^5 = e\)
4. \( (xax)^3 = bx\) and \( x^2a = (xa)^{-1}\)

**B. Rules of Algebra in Groups**

For each of the following rules, either prove that it is true in every group \( G \), or give a counterexample to show that it is false in some groups. (All the counterexamples you need may be found in the group of matrices \( \{I, A, B, C, D, K\} \) described on page 28.)

1. If \( x^2 = e \), then \( x = e \).
2. If \( x^2 = a^2 \), then \( x = a \).
3. \((ab)^2 = a^2b^2\)
4. If \( x^2 = x \), then \( x = e \).
5. For every \( x \in G \), there is some \( y \in G \) such that \( x = y^2 \). (This is the same as saying that every element of \( G \) has a “square root.”)
6. For any two elements \( x \) and \( y \) in \( G \), there is an element \( z \) in \( G \) such that \( y = xz \).
C. Elements That Commute

If \( a \) and \( b \) are in \( G \) and \( ab = ba \), we say that \( a \) and \( b \) commute. Assuming that \( a \) and \( b \) commute, prove the following:

1. \( a^{-1} \) and \( b^{-1} \) commute.
2. \( a \) and \( b^{-1} \) commute. (Hint: First show that \( a = b^{-1}ab \).)
3. \( a \) commutes with \( ab \).
4. \( a^2 \) commutes with \( b^2 \).
5. \( ax^{-1} \) commutes with \( xb^{-1} \), for any \( x \in G \).
6. \( ab = ba \) if \( aba^{-1} = b \).

(The abbreviation iff stands for "if and only if." Thus, first prove that if \( ab = ba \), then \( aba^{-1} = b \). Next, prove that if \( aba^{-1} = b \), then \( ab = ba \). Proceed roughly as in Exercise A. Thus, assuming \( ab = ba \), solve for \( b \). Next, assuming \( aba^{-1} = b \), solve for \( ab \).)
7. \( ab = ba \) iff \( aba^{-1}b^{-1} = e \).

D. Group Elements and Their Inverses

Let \( G \) be a group. Let \( a, b, c \) denote elements of \( G \), and let \( e \) be the neutral element of \( G \).

1. Prove that if \( ab = e \), then \( ba = c \). (Hint: See Theorem 2.)

2. Prove that if \( abc = e \), then \( cab = e \) and \( bca = e \).

3. State a generalization of parts 1 and 2

Prove the following:
4. If \( ax = a^{-1} \), then \( yax = a^{-1} \).
5. Let \( a, b, \) and \( c \) each be equal to its own inverse. If \( ab = e \), then \( bc = a \) and \( ca = b \).
6. If \( abc \) is its own inverse, then \( bca \) is its own inverse, and \( cab \) is its own inverse.
7. Let \( a \) and \( b \) each be equal to its own inverse. Then \( ba \) is the inverse of \( ab \).
8. \( a = a^{-1} \) iff \( aa = e \). (That is, \( a \) is its own inverse iff \( a^2 = e \).)
9. Let \( c = e^{-1} \). Then \( ab = e \) iff \( abc = e \).

E. Counting Elements and Their Inverses

Let \( G \) be a finite group, and let \( S \) be the set of all the elements of \( G \) which are not equal to their own inverse. That is, \( S = \{ x \in G : x \neq x^{-1} \} \). The set \( S \) can be divided up into pairs so that each element is paired off with its own inverse. (See diagram on the next page.) Prove the following:

† When the exercises in a set are related, with some exercises building on preceding ones so that they must be done in sequence, this is indicated with a symbol † in the margin to the left of the heading.

† In any finite group \( G \), the number of elements not equal to their own inverse is an even number.

† The number of elements of \( G \) equal to their own inverse is odd or even, depending on whether the number of elements in \( G \) is odd or even.

† If the order of \( G \) is even, there is at least one element \( x \) in \( G \) such that \( x \neq e \) and \( x = x^{-1} \).

† In parts 4 to 6, let \( G \) be a finite abelian group, say, \( G = \{ e, a_1, a_2, \ldots, a_n \} \).

† Prove the following:

† 4 \( (a_1a_2 \cdots a_n)^2 = e \)

† 5 If there is no element \( x \neq e \) in \( G \) such that \( x = x^{-1} \), then \( a_1a_2 \cdots a_n = e \).

† 6 If there is exactly one \( x \neq e \) in \( G \) such that \( x = x^{-1} \), then \( a_1a_2 \cdots a_n = e \).

† F. Constructing Small Groups

In each of the following, let \( G \) be any group. Let \( e \) denote the neutral element of \( G \).

1. If \( a, b \) are any elements of \( G \), prove each of the following:
   (a) \( a^2 = e \), then \( a = e \).
   (b) If \( ab = a \), then \( b = e \).
   (c) If \( ab = b \), then \( a = e \).

2. Explain why every row of a group table must contain each element of the group exactly once. (Hint: Suppose \( x \) appears twice in the row of \( a \):

   \[
   \begin{array}{ccc}
   \vdots & y_1 & \cdots \\
   : & : & : \\
   \vdots & x & \cdots \\
   \vdots & \vdots & \vdots \\
   e & \vdots & x \\
   \end{array}
   \]

   Now use the cancellation law for groups.)

3. There is exactly one group on any set of three distinct elements, say the set \( \{ e, a, b \} \). Indeed, keeping in mind parts 1 and 2 above, there is only one way of completing the following table. Do so! You need not prove associativity.
4 There is exactly one group $G$ of four elements, say $G = \{e, a, b, c\}$, satisfying
the additional property that $xx = e$ for every $x \in G$. Using only part 1 above,
complete the following group table of $G$:

<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>e</td>
<td>e</td>
<td>e</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
<td>c</td>
</tr>
</tbody>
</table>

5 There is exactly one group $G$ of four elements, say $G = \{e, a, b, c\}$, such that
$xx = e$ for some $x \neq e$ in $G$, and $yy = e$ for some $y \in G$ (say, $aa = e$ and $bb = e$).
Complete the group table of $G$, as in the preceding exercise.

6 Use Exercise E3 to explain why the groups in parts 4 and 5 are the only
possible groups of four elements (except for renaming the elements with different
symbols).

**G. Direct Products of Groups**

If $G$ and $H$ are any two groups, their direct product is a new group, denoted by
$G \times H$, and defined as follows: $G \times H$ consists of all the ordered pairs $(x, y)$
where $x$ is in $G$ and $y$ is in $H$. That is,

$$G \times H = \{(x, y) : x \in G \text{ and } y \in H\}$$

The operation of $G \times H$ consists of multiplying corresponding components:

$$(x, y) \cdot (x', y') = (xx', yy')$$

If $G$ and $H$ are denoted additively, it is customary to denote $G \times H$ additively:

$$(x, y) + (x', y') = (x + x', y + y')$$

1 Prove that $G \times H$ is a group by checking the three group axioms, (G1) to (G3):

(G1) $(x, y_1)(x_1, y_2) = (x + x_1, y + y_2)$

(G2) $(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_1 + y_2)$

(G3) $e = (e, e)$, the identity element of $G \times H$.

1. Prove that $G \times H$ is a group by checking the three group axioms, (G1) to (G3):

   (G1) $(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_1 + y_2)$

   (G2) $(e, e)(x, y) = (x, y)$, the identity element of $G \times H$.

2. For each $(a, b) \in G \times H$, the inverse of $(a, b)$ is $(a^{-1}, b^{-1})$. Check.

3. If $x^2 = e$, then $x$ has a square root.

4. If $a^2 = e$, then $a$ has a cube root.

5. If $x^2 = e$, then $x$ has a cube root.

6. If $a^2 = e$, then $a$ has a square root.

7. If $x^2 = e$, then $a$ has a cube root. (HINT: Show that $xax$ is a cube root of $a^{-1}$.)

8. If $xax = e$, then $ab$ has a square root.