A group, $G$, is a set, $A$, endowed with a single binary operation, $\ast$, such that:

1. The operation $\ast$ is associative, meaning that $a \ast (b \ast c) = (a \ast b) \ast c$ for all $a, b, c \in A$.
2. There is an identity element $e \in A$ such that $a \ast e = e \ast a = a$ for all $a \in A$.
3. Every element of $A$ has an inverse, meaning that for each $a \in A$, there exists an element $a^{-1} \in A$ such that $a \ast a^{-1} = a^{-1} \ast a = e$.

If, in addition, the operation $\ast$ is commutative (meaning that $a \ast b = b \ast a$ for all $a$ and $b \in A$), then we say that $G$ is a commutative group or an abelian group. The word “abelian” is in honor of Niels Abel who was one of the founders of abstract algebra (and who lived only to the age of 27).

**Remark 1** A group, $G$, consists of two things: an underlying set of elements $A$ and a binary operation, $\ast$, that is defined on the elements of $A$. Thus $G = \{A, \ast\}$. However, as we did with rings, we will usually abuse notation and not refer to the set $A$. We will just say “the group $G$” and instead of writing “$x \in A$” we will just write “$x \in G$” since no confusion should arise as long as the operation under consideration is understood.

**Example 2** The set of integers, $Z$, with the operation of addition, $+$, is a group. To see this, note that the integers are closed under addition (meaning that the sum of two integers is an integer), that addition of integers is associative, that the number 0 is the additive identity element of the integers,
and that every integer has an additive inverse within the set of integers (for example, the additive inverse of 5 is $-5$). However, $\mathbb{Z}$ is not a group under the operation of multiplication because not every integer has a multiplicative inverse within the set of integers. For example, the multiplicative inverse of 5 (within the set of rational numbers) is $1/5$, but $1/5$ is not an integer. In fact, the only integers that have multiplicative inverses within the set of integers are 1 and $-1$.

**Example 3** The set of rational numbers, $\mathbb{Q}$, is a group under addition but is not a group under multiplication because the rational number 0 does not have a multiplicative inverse. However, if we throw out the number 0, then $\mathbb{Q} - \{0\}$ is a group under multiplication.

**Example 4** If we take any ring $R = \{A, +, *\}$ and ignore the operation of multiplication then $G = \{A, +\}$ is a group (and is in fact an abelian group because addition is commutative in any ring). However, if we take a ring $R = \{A, +, *\}$ and ignore the operation of addition, then $G = \{A, *\}$ is not a group because 0 $\in$ A does not have a multiplicative inverse in A (assuming that $0 \neq 1$).

**Remark 5** If $G$ is a group with operation $*$, then we will usually just write $ab$ instead of $a * b$. 

Figure 1: Niels Abel (1802–1829)
The following proposition states that the identity element, $e$, of a group must be unique and that the inverse, $a^{-1}$, of any element $a \in G$ must also be unique.

**Proposition 6** Let $G$ be a group. Then:

1. If there exists an element $e_1 \in G$ such that $e_1 a = ae_1 = a$ for all $a \in G$, then $e_1 = e$.

2. For any element $a \in G$, if there exists an element $b \in G$ such that $ab = ba = e$, then $b = a^{-1}$.

**Proof.** Suppose that there exists an element $e_1 \in G$ such that $e_1 a = ae_1 = a$ for all $a \in G$. By definition of $e$, we know that also $ea = ae = a$ for all $a \in G$. This means that $e_1 e = ee_1 = e$ and $ee_1 = e_1 e = e_1$ and we conclude that $e_1 = e$.

Now let $a \in G$ and suppose that there exists an element $b \in G$ such that $ab = ba = e$. By definition of $a^{-1}$, we know that also $aa^{-1} = a^{-1}a = e$. This means that $ab = aa^{-1}$ and hence that $a^{-1}(ab) = a^{-1}(aa^{-1})$. By the associative property, we obtain $(aa^{-1})b = (a^{-1}a)a^{-1}$ which then gives $eb = ea^{-1}$ and hence $b = a^{-1}$. $lacksquare$

### 1 Some Basic Examples of Groups

We have already observed that $Z$ and $Q$ are groups under addition and that $Q - \{0\}$ is a group under multiplication. It is also true that the set of real numbers, $R$, and the set of complex numbers, $C$, are groups under addition and that $R - \{0\}$ and $C - \{0\}$ are groups under multiplication. We now provide a few more examples of groups.

**Example 7** Let $R$ be the set of real numbers. Then $M_{2,2}(R)$ (which is the set of all $2 \times 2$ matrices with real entries) is an abelian group under addition. However $M_{2,2}(R)$ is not a group under multiplication because some $2 \times 2$ matrices do not have multiplicative inverses. However, any $2 \times 2$ matrix,

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

for which

$$\det(A) = ad - bc \neq 0$$
does have a multiplicative inverse (a unique matrix $A^{-1}$ such that $A^{-1}A = AA^{-1} = I$ where $I$ is the $2 \times 2$ identity matrix). If we restrict our attention only to these invertible $2 \times 2$ matrices, then we do in fact have a group under multiplication. This group is called the **general linear group of degree 2** and is denoted by $GL(R, 2)$. Note that $GL(R, 2)$ is not, however, an abelian group because matrix multiplication is not commutative. For example, the matrix

$$A = \begin{bmatrix} -4 & 4 \\ 4 & 1 \end{bmatrix}$$

is invertible with

$$A^{-1} = \begin{bmatrix} -\frac{1}{20} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{5} \end{bmatrix}$$

so $A \in GL(R, 2)$, and the matrix

$$B = \begin{bmatrix} 0 & 3 \\ -2 & 2 \end{bmatrix}$$

is invertible with

$$B^{-1} = \begin{bmatrix} \frac{1}{3} & -\frac{1}{2} \\ \frac{1}{3} & 0 \end{bmatrix}$$

so $B \in GL(R, 2)$. However

$$AB = \begin{bmatrix} -4 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 0 & 3 \\ -2 & 2 \end{bmatrix} = \begin{bmatrix} -8 & -4 \\ -2 & 14 \end{bmatrix}$$

and

$$BA = \begin{bmatrix} 0 & 3 \\ -2 & 2 \end{bmatrix} \begin{bmatrix} -4 & 4 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 12 & 3 \\ 16 & -6 \end{bmatrix}.$$
Definition 9 The order of a group, \( G \), is the number of elements in \( G \). The order of \( G \) is denoted by \( |G| \). If \( G \) has infinitely many elements, then we say that \( G \) has infinite order and we write \( |G| = \infty \).

Example 10 Referring to the examples that we have already given: If \( Z \) is the group of integers under addition, then \( |Z| = \infty \). Also, \( |GL(R, 2)| = \infty \). If \( Z_6 \) is the group \( \{0, 1, 2, 3, 4, 5\} \) under addition, then \( |Z_6| = 6 \); whereas for \( U_6 = \{1, 5\} \) under multiplication we have \( |U_6| = 2 \).

Definition 11 The Cayley table of a group, \( G \), is the complete table of calculations (using the binary operation) for \( G \).

Example 12 The Cayley table for \( Z_6 \) under addition is

\[
\begin{array}{cccccc}
+ & 0 & 1 & 2 & 3 & 4 & 5 \\
0 & 0 & 1 & 2 & 3 & 4 & 5 \\
1 & 1 & 2 & 3 & 4 & 5 & 0 \\
2 & 2 & 3 & 4 & 5 & 0 & 1 \\
3 & 3 & 4 & 5 & 0 & 1 & 2 \\
4 & 4 & 5 & 0 & 1 & 2 & 3 \\
5 & 5 & 0 & 1 & 2 & 3 & 4 \\
\end{array}
\]

and the Cayley table for \( U_6 \) under multiplication is

\[
\begin{array}{c}
* & 1 & 5 \\
1 & 1 & 5 \\
5 & 5 & 1 \\
\end{array}
\]

Definition 13 Let \( a_1, a_2, \ldots, a_n \) be \( n \) distinct symbols. A Latin Square of size \( n \) is a square array in which each of the symbols \( a_1, a_2, \ldots, a_n \) appears exactly once in each row and column.

It may have been noticed that each of the Cayley tables that we have constructed above is a Latin Square. The following Theorem states that this will always be true for any group of finite order.

Theorem 14 If \( G \) is a group of finite order, then the Cayley table for \( G \) is a Latin Square.
Proof. Suppose that $G$ is a group that consists of $n$ distinct elements $a_1, a_2, \ldots, a_n$. Then the Cayley table for $G$ appears as follows:

<table>
<thead>
<tr>
<th></th>
<th>$a_1$</th>
<th>$a_2$</th>
<th>\ldots</th>
<th>$a_i$</th>
<th>\ldots</th>
<th>$a_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_1$</td>
<td>$b_{11}$</td>
<td>$b_{12}$</td>
<td>\ldots</td>
<td>$b_{1i}$</td>
<td>\ldots</td>
<td>$b_{1n}$</td>
</tr>
<tr>
<td>$a_2$</td>
<td>$b_{21}$</td>
<td>$b_{22}$</td>
<td>\ldots</td>
<td>$b_{2i}$</td>
<td>\ldots</td>
<td>$b_{2n}$</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>$a_i$</td>
<td>$b_{i1}$</td>
<td>$b_{i2}$</td>
<td>\ldots</td>
<td>$b_{ii}$</td>
<td>\ldots</td>
<td>$b_{in}$</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>$a_n$</td>
<td>$b_{n1}$</td>
<td>$b_{n2}$</td>
<td>\ldots</td>
<td>$b_{ni}$</td>
<td>\ldots</td>
<td>$b_{nn}$</td>
</tr>
</tbody>
</table>

For any given subscript $i$, where $1 \leq i \leq n$, suppose that there exist subscripts $j$ and $k$ with $j \neq k$ such that $b_{ij} = b_{ik}$. (This would mean that the $i$th row of the Cayley table has some entry repeated twice.) Then $a_ia_j = a_ia_k$ and this implies that $a_i^{-1}(a_ia_j) = a_i^{-1}(a_ia_k)$ and hence (by using the associative property) that $a_j = a_k$. However, this is a contradiction because we are assuming that $j \neq k$ and hence that the elements $a_j$ and $a_k$ are distinct. Because of this contradiction, we conclude that $b_{ij} \neq b_{ik}$ for any $j$ and $k$ such that $j \neq k$. Therefore no element of $G$ can appear more than once in any given row of the Cayley table for $G$. In addition, since the Cayley table has $n$ columns, every member of $G$ must appear once in each row. By a similar argument, we can show that every column of the Cayley table contains every member of $G$ appearing exactly once. Thus the Cayley table for $G$ is a Latin Square. 

Remark 15 Although we know that the Cayley table for any finite group must be a Latin Square, the converse of this assertion is not true. In other words, it is not true that every Latin Square corresponds to the Cayley table of a group. For example, suppose we let $G = \{1, 2, 3, 4, 5\}$ with multiplication defined as in the following table:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
This table is a Latin Square. However, $G$ is not a group under this operation because

$$2 \star (3 \star 4) = 2 \star 2 = 1$$

and

$$(2 \star 3) \star 4 = 4 \star 4 = 3$$

which means that the associative property is not satisfied. Another reason that this is not a group is that $3 \star 5 = 1$ but $5 \star 3 \neq 1$.

### 1.1 Groups of Order 1

If we let $e$ be some symbol and let $G = \{e\}$ with binary operation defined by $ee = e$, then $G$ is a group of order 1. Hence there is essentially only one group of order 1. It is called the **trivial group**. The Cayley table of the trivial group is

```
* | e
---+---
e | e
```

### 1.2 Groups of Order 2

If we let $e$ and $a$ be distinct symbols and let $G = \{e, a\}$ with the agreement that $e$ will be the identity element, then the only possible Cayley table for $G$ is

```
* | e | a
---+---+---
e | e | e | a
a | a | e | e
```

There is thus essentially only one group of order 2 (described by the above Cayley table). Note that $Z_2$ under addition has this same Cayley table with $e = 0$ and $a = 1$, and that $U_6$ under multiplication also has this Cayley table with $e = 1$ and $a = 5$. 
1.3 Groups of Order 3

For distinct symbols \( e, a, \) and \( b \) (with the agreement that \( e \) will be the identity element), the only possible Cayley table (that is a Latin Square) is

\[
\begin{array}{c|ccc}
* & e & a & b \\
\hline
e & e & a & b \\
a & a & b & e \\
b & b & e & a \\
\end{array}
\]

Thus there is essentially only one group of order 3. A concrete realization of this group is the group \( \mathbb{Z}_3 \) under addition:

\[
\begin{array}{c|ccc}
+ & 0 & 1 & 2 \\
\hline
0 & 0 & 1 & 2 \\
1 & 1 & 2 & 0 \\
2 & 2 & 0 & 1 \\
\end{array}
\]

1.4 Groups of Order 4

We have seen that there is essentially only one group of order 1, one group of order 2, and one group of order 3. When we use the word “essentially”, that means that the groups in question differ only by the symbols being used. Later we will undertake a more in-depth investigation of the question as to whether two groups of the same order are essentially the same or essentially different. For now, let us show that there exactly two essentially different groups of order 4.

One group of order 4 is the additive group \( \mathbb{Z}_4 \) which has the following Cayley table:

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\]

If we introduce abstract symbols \( e, a, b, \) and \( c \), then the table for \( \mathbb{Z}_4 \) has the
Another group of order 4 is the **Klein 4-group** which is the set \( K = \{(0,0), (0,1), (1,0), (1,1)\} \) with an addition operation, \( \oplus \), defined by adding the component of the elements of \( K \) modulo 2. The Cayley table of the Klein 4-group is as follows:

\[
\begin{array}{cccc}
  \oplus & (0,0) & (0,1) & (1,0) & (1,1) \\
(0,0) & (0,0) & (0,1) & (1,0) & (1,1) \\
(0,1) & (0,1) & (0,0) & (1,1) & (1,0) \\
(1,0) & (1,0) & (1,1) & (0,0) & (0,1) \\
(1,1) & (1,1) & (1,0) & (0,1) & (0,0) \\
\end{array}
\]

With abstract symbols being used, the table of the Klein 4-group has the form

\[
\begin{array}{cccc}
  \ast & e & a & b & c \\
  e & e & a & b & c \\
  a & a & e & c & b \\
  b & b & c & e & a \\
  c & c & b & a & e \\
\end{array}
\]

By looking at the abstract versions of the tables of \( Z_4 \) and the Klein 4-group, it can be see that these are essentially different groups. In particular, \( Z_4 \) has only one non-identity element whose square is the identity element \( b^2 = e \) but \( a^2 \neq e \) and \( c^2 \neq e \). However the square of every element in the Klein 4-group is the identity element. Thus the elements of these two groups “behave differently” in an algebraic sense and there is no way to make them “behave” the same by just changing the symbols that are being used to denote members of the groups.

We conclude by showing that \( Z_4 \) and the Klein 4-group are essentially the *only* two groups of order 4. To see this, suppose that if \( G = \{e, a, b, c\} \) is a group of order 4 (with identity element \( e \)). We will consider three possible cases:
Case 1: Suppose that the square of every element of \( G \) is \( e \). Thus \( a^2 = e \), \( b^2 = e \), and \( c^2 = e \). This means that the Cayley table of \( G \) must have the form

\[
\begin{array}{cccc}
* & e & a & b & c \\
e & e & a & b & c \\
a & a & e & ? & ? \\
b & b & ? & e & ? \\
c & c & ? & ? & e \\
\end{array}
\]

However, there is only one way to complete this table in order to make it be a Latin Square and that is

\[
\begin{array}{cccc}
* & e & a & b & c \\
e & e & a & b & c \\
a & a & e & c & b \\
b & b & c & e & a \\
c & c & b & a & e \\
\end{array}
\]

which means that this group is essentially the same as the Klein 4–group.

Case 2: Suppose that the squares of exactly two of the non–identity elements of \( G \) are the identity element. (Without loss of generality, we may assume that these elements are \( a \) and \( b \).) Thus we are assuming that \( a^2 = e \), \( b^2 = e \), but \( c^2 \neq e \). This assumption gives a Cayley table of the form

\[
\begin{array}{cccc}
* & e & a & b & c \\
e & e & a & b & c \\
a & a & e & ? & ? \\
b & b & ? & e & ? \\
c & c & ? & ? & ? \\
\end{array}
\]

However, if this Cayley table is to be a Latin Square, then the question mark in the lower right hand corner must also me \( e \) meaning that we must have \( c^2 = e \). Therefore this case cannot occur in a group of order 4.

Case 3: Suppose that the square of exactly one of the non–identity elements of \( G \) is equal to \( e \). Without loss of generality, suppose that we name this element \( b \). Thus we are assuming that \( a^2 \neq e \), \( b^2 = e \), and \( c^2 \neq e \).
This gives a Cayley table of the form

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

Since we are not allowing that $a^2 = e$ or that $c^2 = e$, then the question marks in the boxes must be either $b$ or $c$. However, the question mark in the box in the lower right corner cannot be $c$ because then we would not have a Latin Square. Thus this question mark must be $b$ and this gives us

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

If we replace the remaining question mark in the box with $b$ also, then we obtain

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

which is the Cayley table for $Z_4$. If, instead, we replace the question mark with $c$, then we obtain

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

and there is no way to continue in order to arrive at a Latin Square.

We thus see that $Z_4$ and the Klein 4–group are essentially the only two groups of order 4.