## Section 6.2 Introduction to the Algebraic Group

**Purpose of Section**: To introduce the concept of a mathematical structure called an algebraic group. To illustrate group concepts, we introduce the cyclic and dihedral groups.

### Basics of a Group

The idea of a symmetry is fundamental in science and to study them in depth one needs the mathematical machinery of an algebraic group. Group theory is one of the most useful mathematical tools for mathematicians and scientists alike, including for particle physicists where group theory is the language for understanding the structure of particle physics.

**Historical Note:** The word *group* was first used by the 20-year old French genius Evariste Galois in 1830, who wrote his seminal paper on the un-solvability of the $5^{th}$ order polynomial equation on the night before he was killed in a duel. Although many of the greatest mathematicians at the time did not appreciate Galois's brilliance, a letter Galois wrote eventually ended up in the possession of the French mathematician Joseph Liouville, who published Galois's results in 1846. Over the next 50 years, mathematician gradually came to understand the genius of Galois' ideas and his work gradually developed into the theory of groups.

The most fundamental component of a group is its binary operation.

### Binary Operations and the Group

A **binary operation** on a set $A$ is a rule, which assigns to each pair of elements of $A$ a unique element of $A$. Thus, a binary operation is a function $f : A \times A \to A$. Two common binary operations familiar to the reader are $+, \times$ which assign the sum $a+b \in \mathbb{R}$ and product $a \times b \in \mathbb{R}$ to a pair $(a,b) \in \mathbb{R} \times \mathbb{R}$ of real numbers. We now give a formal definition of a group.

**Definition**: An **algebraic group** $G$ is a set of elements with a **binary operation**, often denoted by "$*$", which satisfies the following properties:

- **Closure:** The operation $*$ is a closed operation. That is, if $a,b \in G$, then $a*b \in G$
- **Associative:** The operation $*$ is **associative**. That is, for all $a,b,c \in G$, we have $(a*b)*c = a*(b*c)$.

● **Identity:** $G$ has a unique **identity**[1] $e$. That is, there exists an $e \in G$ such that $a * e = e * a = a$ for all $a \in G$. .

● **Inverse:** Every element $a \in G$ has a unique **inverse**[2] . That is, for every $a \in G$ there exists $a^{-1} \in G$ that satisfies $a * a^{-1} = a^{-1} * a = e$.

We often denote a group $G$ with operation $*$ by $\{G, *\}$.

Often it happens that $a * b = b * a$ for all $a, b \in G$. When this happens the group is called a **commutative** (or **Abelian**) group. We often denote the group operation $a * b$ simply as $ab$, or maybe by $\oplus$ if the group operation is addition or resembles addition. A group is called **finite** if it contains a finite number of elements and the number of elements in the group is called the **order** of the group. If the order of a group $G$ is $n$, we denote this by writing $|G| = n$ If the group is not of finite order, we say it is of **infinite order**.

**In Plain English**

● **Associative:** The associative property

$$(a * b) * c = a * (b * c)$$

says that when three elements $a, b, c \in G$ (keeping them in the same order) are combined, the result is the same regardless of which two elements are combined first. Although most groups have an associative binary relation, there are important examples in mathematics where binary operations are not associative, including the cross product of vectors in vector analysis, and the difference between two numbers[3].

● **Identity:** The identity element of a group depends on the binary relation $*$ and is the element $e \in G$ that leaves every element $a \in G$ unchanged when combined with $e$. In the group of the integers $\mathbb{Z}$ with the binary operation $+$ (addition), the identity is $0$ since $a + 0 = 0 + a = a$ for every integer $a$.

● **Inverse:** The inverse $a^{-1}$ of an element $a$ depends not only on $a$, but on the identity $e$. For example, the inverse of an integer $a$ with group operation addition + and identity 0, is $-a$ since $a + (-a) = (-a) + a = 0$.

[1] It is not necessary to state that the identity is unique since it can be *proven* that there is only one identity.
[2] Again, it can be proven that the inverse is unique so it is not really necessary to assume uniqueness.
[3] $(a - b) - c \neq a - (b - c)$

Table 1 shows some binary operations of different sets.

| Properties of Binary Operations | | | | |
|---|---|---|---|---|
| **Operation** | **Associative** | **Commutative** | **Identity** | **Inverse** |
| $\cup$ on $P(A)$ | Yes | Yes | Yes | No |
| $\cap$ on $P(A)$ | Yes | Yes | Yes | No |
| gcd on $\mathbb{N}$ | Yes | Yes | No | No |
| $+$ on $\mathbb{R}$ | Yes | Yes | Yes | Yes |
| $-$ on $\mathbb{R}$ | No | No | No | No |
| $\times$ on $\mathbb{Q}$ | Yes | Yes | Yes | Yes |
| min on $\mathbb{R}$ | Yes | Yes | No | No |

Properties of binary operations
Table 1

**Example 1: Group Test** Tell which of the following sets and binary operations define a group.

a) $\{\mathbb{Z},+\}$:
b) $\{\mathbb{Z},(m+n)/2\}$
c) $\{\mathbb{Z},-\}$

**Solution**

a) We leave it to the reader to show $\{\mathbb{Z},+\}$ is a group.

b) Taking the average of two integers does not always result in an integer. Hence the group operation is not closed in $\mathbb{Z}$. No need to check the other properties.

c) The integers $\mathbb{Z}$ with the difference operation is not a group since subtraction is not associative, which can be seen from

$$m-(n-p)\neq(m-n)-p$$

**Abstraction** Abstraction reveals connections between different areas of mathematics since the process of abstraction allows one to see essential ideas, seeing forest if you will and not just the trees. This broad viewpoint can result in making new discoveries in one area of mathematics as a result of knowledge in other areas. A disadvantage might be that highly abstract mathematics is more difficult to master and tends to isolate mathematics from the outside world.

**Cayley Table**

The binary operation of a group can be illustrated by means of a Cayley table as drawn in Figure 1, which shows the products

$$g_i g_j \text{ of elements } g_i \text{ and } g_j \text{ of a group}$$

It is much like the addition or multiplication tables the reader studied as a child, except a Cayley table records any binary operation. A Cayley table is an example of a *Latin square*, meaning that every element of the group occurs once and exactly once in every row and column. We examine the Cayley table to learn about the inner workings of a group.

| $*$ | $g_1 = e$ | $g_2$ | $g_3$ | $\cdots$ | $g_j$ | $\cdots$ |
|---|---|---|---|---|---|---|
| $g_1 = e$ | $e$ | $g_1$ | $g_2$ | $\cdots$ | $g_j$ | $\cdots$ |
| $g_2$ | $g_2$ | $g_2^2$ | $g_2 g_3$ | $\cdots$ | $g_2 g_j$ | $\cdots$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |
| $g_i$ | $g_i g_1$ | $g_i g_2$ | $g_i g_3$ | $\cdots$ | $g_i g_j$ | $\cdots$ |
| $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ | $\cdots$ |

Cayley table for a group
Figure 1

**Example 2: Order Two and Order Three** For the following graphs of order 2 and 3 represented by their Cayley tables, show

a) both groups are commutative
b) find the inverse of each element in each group
c) show both groups are associative.
d) the only groups of order 2, 3 are the ones displayed.
e)

| $*$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

Order 2

| $e$ | $*$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $e$ |
| $b$ | $b$ | $e$ | $a$ |

Order 3

**Solution** We leave this fun for the reader.

**Example 3 Order Four** The set $G=\{a,b,c,d\}$ and binary operation $*$ define the following group of order 4.

| $*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $c$ | $d$ | $a$ |
| $c$ | $c$ | $d$ | $a$ | $b$ |
| $d$ | $d$ | $a$ | $b$ | $c$ |

Order 4 group

a) What is the identity element of the group.
b) Find the inverse of each element.
c) Is the group commutative?
d) Does the associativity property $a*(b*c)=(a*b)*c$ hold?

**Solution**

a) Identity is $a$ since $ab=ba=b, ac=ca=c, ad=da=d$.
b) $a^{-1}=a,\ b^{-1}=d,\ c^{-1}=c,\ d^{-1}=b$
b) Yes, the Cayley table is symmetric around the diagonal.
c) Yes, $a*(b*c)=a*d=d$ and $(a*b)*c=b*c=d$.

In general, there is no quick way to verify the associative property like there is for the commutative property. You have to check *all* possible arrangements to verify the associative property. On the other hand, if one instance where the associative property fails, then the binary operation $*$ is not associative.

**Example 4: Klein 4-Group** Show that the set of four members $G=\{e,a,b,c\}$ described by the following multiplication table in Figure 2 forms a group. This group is called the **Klein[4] 4-group** and is the symmetry group of a rectangle studied in Section 6.1.

| $*$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ |

Multiplication table for the Klein 4-group
Figure 2

[4] Felix Klein (1849-1925) was a German geometer of the 19th century.

**Solution:** We verify the following criterion for a group.

**Closure:** The binary operation is closed since all the members of the multiplication table are members of $G$ .

**Identity:** The element $e$ is the identity since

$$\boxed{\begin{aligned} e*a &= a*e = a \\ e*b &= b*e = b \\ e*c &= c*e = c \end{aligned}}$$

**Inverse:** To find the inverse $r^{-1}$ of an element $r$ follow along the row labeled "$r$" until you get to the group identity $e$, then the inverse $r^{-1}$ is the column label above $e$. In the Klein four-group, each element $e, a, b, c$ is its own inverse

**Associativity:** The hardest requirement to verify for a group is the associative property, which requires we check $(r*s)*t = r*(s*t)$, where $r, s, t$ can be any of the elements $e, a, b, c$. Unfortunately, what this means is we must check $4^3 = 48$ equations. The computations can be simplified by observing the group is commutative. Other shortcuts can be used (as well as computer algebra systems) to shorten the list of elements you must check. For this group, we observe that the group operation $*$ is simply the composition of functions and we can resort to the fact that composition of functions is associative.

**Important Note:** There are only two different groups of order four, the Klein 4-group and what we will see later, the cyclic group $\mathbb{Z}_4$ of clock arithmetic.

**Familiar Groups** You are familiar with more groups that you probably realize. Table 2 shows just a few algebraic groups you might have seen in earlier studies.

| Group | Elements | Operation | Identity | Inverse |
|---|---|---|---|---|
| $\mathbb{Z}$ | $n \in \mathbb{Z}$ | addition | 0 | $-n$ |
| $\mathbb{Q}^+$ | $m/n$<br>$m, n > 0$ | multiplication | 1 | $n/m$ |
| $\mathbb{Z}_n$ | $k \in \{0, 1, 2, ..., n-1\}$ | addition mod $n$ | 0 | $n-k$ |
| $\mathbb{R} - \{0\}$ | $x$ nonzero real number | multiplication | 1 | $1/x$ |
| $\mathbb{R}^2$ | $(a, b) \in \mathbb{R}^2$ | vector addition | $(0,0)$ | $(-a, -b)$ |

Common groups
Table 2

**Cyclic Groups: Modular Arithmetic**

The most common and most simple of all groups are the **cyclic groups**, which are well-known to every child who has learned to keep time.

**Definition:** A **finite cyclic group** $(\mathbb{Z}_n, *)$ of order $n$ is a group that contains an element $g \in Z_n$ called the **generator** of the group, such that

$$\mathbb{Z}_n \left\{ e, g, g^2, g^3, ..., g^{n-1} \right\} .$$

where the "powers" of $g$ are simply repeated multiplications[5] of $g$; that is $g^2 = g * g, g^3 = g^2 * g, ...$ If the group operation is addition, then we would write the generator as

$$\mathbb{Z}_n = \left( e, g, 2g, 3g, ..., (n-1)g \right)$$

An alternate notation for the a finite cyclic group with generator $g$ is $< g >$.

For example, the three rotational symmetries $\{e, R_{120}, R_{240}\}$ of an equilateral triangle form a cyclic group $\mathbb{Z}_3$ with generator $g = R_{120}$ since $R_{120}^2 = R_{240}$, $R_{120}^3 = e$.

Cyclic groups also describe modular (or clock) arithmetic, which is the type of arithmetic we perform when keeping time on 12-hour clock. This leads us to the cyclic group $Z_{12}$ with elements

$$Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$$

and the group operation on $Z_{12}$ is what you do when you keep time, that is

$$a \oplus b = (a+b) \bmod 12$$

where "mod 12" refers to computing $a \oplus b$ by computing $(a+b)$ then taking its remainder after dividing by 12. When it's 3 P.M., it is 15 hours by military time, but if you're not in the military, you divide 15 by 12 and take the remainder of 3. We also denote the group operation by $\oplus$ to remind us that the operation is addition, only reduced modulo 12. In clock arithmetic, the equation $2 = (9+5) \bmod 12$ says that 5 hours after 9 P.M. it is 2 A.M. The hours of the clock $Z_{12}$ and the binary operation of addition modulo 12 is a binary operation, which is an Abelian group of order 12 called the **cyclic group of order 12** and denoted by $(\mathbb{Z}_{12}, \oplus)$. The Cayley table for this group is shown in Table 3.

[5] We use the word "multiplication" here, but keep in mind the group operation can mean any binary operation, even addition.

| $\oplus$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 8 | 8 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 9 | 9 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 10 | 10 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 11 | 11 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

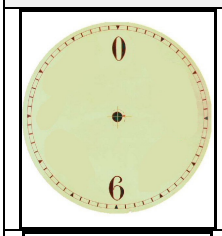
Cayley table for the cyclic group of 12 elements
Table 3

**Notational Note:** Repeated multiplication of an element $g$ of a group by itself results in powers of an element and are denoted by $g^n, n = 1, 2, ...$ The identity is defined as $g^n$ for $n = 0$, i.e. $g^0 = e$.

**Important Note::** The evolution of group theory has resulted in three main areas of application: 1) the theory of algebraic equations, 2) number theory, and 3) geometry. Early researchers in group theory were Joseph-Louis Lagrange (1736-1813), Niels Abel (1802-1829) and Evariste Galois (1811-1832).,

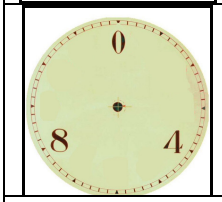
The following Figure 3 shows various clocks that give rise to different cyclic groups.

Cyclic Groups $\mathbb{Z}_n$



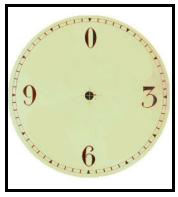

$Z_2$ Cyclic Group Order 2

| $\oplus$ | 0 | 6 |
|---|---|---|
| 0 | 0 | 6 |
| 6 | 6 | 0 |




$Z_3$ Cyclic Group Order 3

| $\oplus$ | 0 | 4 | 8 |
|---|---|---|---|
| 0 | 0 | 4 | 8 |
| 4 | 4 | 8 | 0 |
| 8 | 8 | 0 | 4 |




$Z_4$ Cyclic Group Order 4

| $\oplus$ | 0 | 3 | 6 | 9 |
|---|---|---|---|---|
| 0 | 0 | 3 | 6 | 9 |
| 3 | 3 | 6 | 9 | 0 |
| 6 | 6 | 9 | 0 | 3 |
| 9 | 9 | 0 | 3 | 6 |


$\mathbb{Z}_6$ Cyclic Group Order 6

| $\oplus$ | 0 | 2 | 4 | 6 | 8 | 10 |
|---|---|---|---|---|---|---|
| 0 | 0 | 2 | 4 | 6 | 8 | 10 |
| 2 | 2 | 4 | 6 | 8 | 10 | 0 |
| 4 | 4 | 6 | 8 | 10 | 0 | 2 |
| 6 | 6 | 8 | 10 | 0 | 2 | 4 |
| 8 | 8 | 10 | 0 | 2 | 4 | 6 |
| 10 | 10 | 0 | 2 | 4 | 6 | 8 |

Finite cyclic groups
Figure 3

**Example 5 Relatively Prime Group** Two integers are called **relatively prime** if they have no common factors other than 1, or equivalently, if their greatest common divisor is 1. For example, 4 and 15 are relatively prime but 4 and 14 are not. The positive integers less than 10 that are relatively prime with 10 are 1, 3, 7 and 9. We call this set $U(10) = \{1, 3, 7, 9\}$, and along with the binary operation of multiplication modulo 10, it is a group with the following Cayley table.

| $\otimes$ | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 9 | 1 | 7 |
| 7 | 7 | 1 | 9 | 3 |
| 9 | 9 | 7 | 3 | 1 |

Note that the group is Abelian and that $3^{-1}=7,\ 7^{-1}=3$ since $3\times 7=1$.

**Isomorphic Groups: Groups that are the Same**

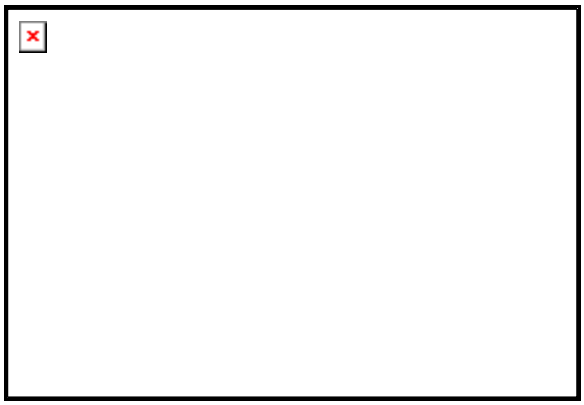
Sometimes groups appear different when looking at their Cayley tables, but after relabeling their elements, one discovers they are the same group. For example, consider two groups illustrated in Table 4.

| $\oplus$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

| $\times$ | 1 | $i$ | -1 | $-i$ |
|---|---|---|---|---|
| 1 | 1 | $i$ | -1 | $-i$ |
| $i$ | $i$ | -1 | $-i$ | 1 |
| -1 | -1 | $-i$ | 1 | $i$ |
| $-i$ | $-i$ | 1 | $i$ | -1 |

Isomorphic groups
Table 4

The group at the left is the cyclic group $\mathbb{Z}_4=\{0,1,2,3\}$ and the group at the right consists of the four numbers $G=\{0,\ i,\ -1,\ i\}$ which lie on the unit circle in the complex plane, where the group operation is multiplication. See Figure 4.



Isomorphism between an additive and multiplicative group
Figure 4

If you look carefully at the two Cayley tables, you will see that the the numbers 0,1,2,3 in the table for $\mathbb{Z}_4$ are arranged in the same order as the numbers $1,\ i,-1,-i$ in the table for $G$. If we make the correspondences

$$0\leftrightarrow 1,\ 1\leftrightarrow i,\ 2\leftrightarrow -1,\ 3\leftrightarrow -i,\ \oplus\leftrightarrow\times$$

we see that the the groups $\mathbb{Z}_4$ and $G$ are really the same, they simply use different symbols. When two groups are the same but only uses different symbols in their description, the groups are called **isomorphic**. In this example, the one-to-one correspondence given above is called an **isomorphism** between the groups. This motivates the following formal definition of an isomorphism.

**Definition:** Let $\{G_1, *\}$ and $\{G_2, \oplus\}$ be groups with respective group operations $*$ and $\oplus$. An **isomorphism** $T: G_1 \to G_2$ from $G_1$ to $G_2$ is a one-to-one and onto mapping from $G_1$ onto $G_2$ that preserves group operations. That is

$$T(a*b) = T(a) \oplus T(b)$$

for all $a, b \in G_1$. When there exists an isomorphism from one group to the other, the groups are called **isomorphic** (i.e. the same from an abstract point of view).

Roughly speaking, this says that the two operations, mapping and group operations can be carried out in either order; i.e. you can operate then map $T(a*b)$, or you can map and then operate, $T(a) \oplus T(b)$, the results are the same.

**Example 6: Relatively Prime Group** The group $U(10)$ in Example 5 of positive integers less than 10 relatively prime to 10, described by the Cayley table:

| $\otimes$ | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 9 | 1 | 7 |
| 7 | 7 | 1 | 9 | 3 |
| 9 | 9 | 7 | 3 | 1 |

Group of relative prime numbers with 10
$U(10)$

is isomorphic to the cyclic group $\mathbb{Z}_4 = \{0,1,2,3\}$. If we make the correspondence

$$1 \leftrightarrow 0,\ 3 \leftrightarrow 1,\ 9 \leftrightarrow 2,\ 7 \leftrightarrow 3$$

we get the familiar Cayley table for $\mathbb{Z}_4$.

| $\otimes$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Cyclic group
$\mathbb{Z}_4$

**Example 7: An Isomorphism You Know** Let $G_1 = (0, \infty)$ be the positive real numbers with group operation of multiplication, and $G_2 = \mathbb{R}$ the real numbers with group operation of addition. The bijection $T : (0, \infty) \to \mathbb{R}$ defined by

$$T(x) = \log x$$

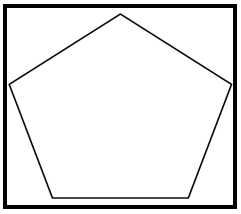
is an isomorphism since it satisfies

$$T(xy) = \log(xy) = \log x + \log y = T(x) + T(y) \ .$$

**Dihedral Groups: Symmetries of Regular Polygons**

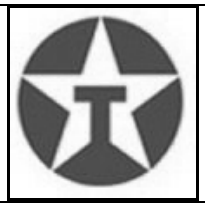
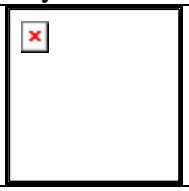
In Section 6.1, we saw how the symmetries of a figure form an arithmetic system where one can "multiply" symmetries much like we multiply ordinary numbers. The set of symmetries of an object along with the arithmetic operation of composition of symmetries forms a group of symmetries for the figure. Every figure, no matter how "non symmetric," has at least *one* symmetric group. The more symmetric a figure, the more elements in its symmetry group. A rectangle has four symmetries, whereas the more "symmetrical" square has eight symmetries. Can you find them?

A polygon is called **regular** if all its sides have the same length and all its interior angles are the same. An equilateral triangle is a regular 3-gon, a square is a regular 4-gon, a pentagon is a regular 5-gon and so on. The symmetry group of a regular $n$-gon has $n$ rotational symmetries and $n$ flip symmetries for a total of $2n$ symmetries. This group is called the **dihedral group** of the $n$-gon and denoted by $D_n$ Can you find the 10 symmetries of the dihedral group $D_5$ of the pentagon drawn in Figure 5?



Find the symmetric group $D_5$
Figure 5

Figure 6 shows commercial figures whose symmetry groups are dihedral groups..

| | |
|---|---|
|  2 symmetries | $D_1$ one rotation (0 degrees), one vertical flip |
|  4 symmetries | $D_2$ two rotations, two flips |
|  6 symmetries | $D_3$ three rotations, three flips |
|  8 symmetries | $D_4$ four rotations, four flips |
|  10 symmetries | $D_5$ five rotations, five flips |

Dihedral symmetry groups
Figure 6

**Important Note:** A cyclic group of order $n$ defines $n$ symmetry rotations of an object about a point. A dihedral group of order $2n$ defines $n$ symmetry rotations of an object about a point, plus $n$ symmetry reflections of the object through a line.

**Historical Note:** At the International Congress of Mathematicians in 1900, the German mathematician David Hilbert posed 23 problems for mathematicians to solve in the next century. Hilbert's 18th problem asked whether crystallographic groups in $n$ dimensions were always finite. The problem was solved in 1910 by German mathematician L. Bieberbach, who proved they are finite in every dimension. Finding the *number* of these groups is another matter. In $\mathbb{R}^3$ there are 230 symmetry groups; in $\mathbb{R}^4$ there are 4783.

**Multiplying Groups**

There are only two (non-isomorphic) groups of order 6, the dihedral group $D_3$ and the cyclic group $\mathbb{Z}_6$. Sometimes groups can be factored into smaller groups somewhat like the number 6 can be factored as $6 = 3 \times 2$. The cyclic group $\mathbb{Z}_6$ can be factored as the Cartesian product

$$\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2 = \{(m,n) : m \in \mathbb{Z}_3, n \in \mathbb{Z}_2\}$$

of the two smaller cyclic groups $\mathbb{Z}_3$ and $\mathbb{Z}_2$. If we define the group operation on the Cartesian product as

$$(m_1, n_1) \oplus (m_2, n_2) = ((m_1 + m_2) \bmod 3, (n_1 + n_2) \bmod 2)$$

we arrive at the Cayley table in Figure 7.

| $\oplus$ | $(0,0)$ | $(1,1)$ | $(2,0)$ | $(0,1)$ | $(1,0)$ | $(2,1)$ |
|---|---|---|---|---|---|---|
| $(0,0)$ | $(0,0)$ | $(1,1)$ | $(2,0)$ | $(0,1)$ | $(1,0)$ | $(2,1)$ |
| $(1,1)$ | $(1,1)$ | $(2,0)$ | $(0,1)$ | $(1,0)$ | $(2,1)$ | $(0,0)$ |
| $(2,0)$ | $(2,0)$ | $(0,1)$ | $(1,0)$ | $(2,1)$ | $(0,0)$ | $(1,1)$ |
| $(0,1)$ | $(0,1)$ | $(1,0)$ | $(2,1)$ | $(0,0)$ | $(1,1)$ | $(2,0)$ |
| $(1,0)$ | $(1,0)$ | $(2,1)$ | $(0,0)$ | $(1,1)$ | $(2,0)$ | $(0,1)$ |
| $(2,1)$ | $(2,1)$ | $(0,0)$ | $(1,1)$ | $(2,0)$ | $(0,1)$ | $(0,0)$ |

Multiplication table for $\mathbb{Z}_3 \times \mathbb{Z}_2$

Figure 7

which if we make the following identification

$$0 \leftrightarrow (0,0), 1 \leftrightarrow (1,1), 2 \leftrightarrow (2,0), 3 \leftrightarrow (0,1), 4 \leftrightarrow (1,0), 5 \leftrightarrow (2,1)$$

the multiplication table in Figure 7 is the same as the multiplication table for the cyclic group $\mathbb{Z}_6$ shown in Figure 8

| $\oplus$ | 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 |

Multiplication table for $\mathbb{Z}_6$

Figure 8

## Problems

1. **Groups?** Do the following sets with given binary operations form a group? If they do, find the identity element and the inverse of each element. If it does not form a group, explain why not.

a) even integers, addition
b) $\{-1,1\}$, multiplication
c) nonzero complex numbers, multiplication
d) nonzero rational numbers, multiplication
e) positive rational numbers, multiplication
f) complex numbers $1,-1,i,-i$, multiplication
g) positive irrational numbers together with 1, multiplication
h) integers, subtraction.

2. **Odd Integers Under Addition** Give reasons why the odd integers under addition do not form a group?

3. **Finish the Group** Complete the following Cayley table for a group of order three.

| $*$ | $e$ | $a$ | $b$ |
|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ |
| $a$ | $a$ | | |
| $b$ | $b$ | | |

4. **Finish the Group** Complete the following Cayley table for a group of order four without looking at the Cayley tables of the Klein 4- group or the cyclic group of order 4 in the text.

| $*$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | | | |
| $b$ | $b$ | | | |
| $c$ | $c$ | | | |

5. **Verification of a Group** Do the nonzero integers with the operation of multiplication form a group?

6. **Group You are Familiar With** Show $\{\mathbb{Z},+\}$ is a group.

7. **Property of a Group** Verify that for all elements $a,b$ in a group, the following identity holds.

$$(ab)^{-1} = b^{-1}a^{-1} .$$

Hint: Show $(ab)\left(b^{-1}a^{-1}\right) = e$.

**General Properties of Groups**

8. **Unique Identity** Show that a group has exactly one identity.

9. **Unique Inverse** Show that every element in a group has no more than one inverse.

10. **Heisenberg Group** A group that plays an important role in quantum mechanics is the Heisenberg group which consists of all matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

where $x, y, z$ are real numbers and the group operation is matrix multiplication. Show this is a group.

11.**Direct Product of Groups** Define a group $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$ consisting of the Cartesian product

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \left\{(a,b) : a,b \in \mathbb{Z}_2\right\}$$

and binary operation

$$(a,b) \oplus (c,d) = \left((a+c) \bmod 2,\ (b+d) \bmod 2\right)$$

Show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a group under this operation. This group plays an important role in coding theory.

12. **Mod 3 Multiplication** Create the multiplication table for the integers 1, 2 where multiplication defined as mod(3) arithmetic.

13. **Mod 4 Multiplication** Create the multiplication table for the integers 1,2,3 for modular arithmetic $\text{mod}(4)$ and show that this does not define a group. In other that the numbers $1, 2, ..., n-1$ forms a group under $\text{mod}(n)$ multiplication, it must be true that $n$ is a prime number.

14**. Mod 5 Multiplication** Create the multiplication table for the integers 1,2,3,4 where multiplication defined as mod(5) arithmetic.

15. **Relative Prime Group *U*(10)** For each positive integer $n$, the set of positive integers 1,2,…, $n$ that are relatively prime[6] with $n$ is denoted by $U(n)$. For example, $U(10) = \{1,3,7,9\}$. The set $U(n)$ is a group under multiplication modulo $n$.

a) Draw the Cayley table for $U(10)$.
b) Is the group Abelian?
c) What is the inverse of each element?

16 **Relative Prime Group *U*(8)** For each positive integer $n$ the set of positive integers 1,2,…, $n$ that are relatively prime with $n$ is denoted by $U(n)$. For example, $U(8) = \{1,3,5,7\}$. The set $U(n)$ is a group under multiplication modulo $n$.

a) Draw the Cayley table for $U(8)$.
b) Is the group Abelian?
c) What is the inverse of each element?

17. **Isomorphic Groups** Show that the following Group C and Group D are isomorphic by interchanging the 3rd and 4th columns of C, and then the 3rd and 4th rows to get the table for D.

| $\oplus$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Group C

[6] Two numbers are relatively prime if and only if the greatest common divisor of both numbers is 1

| $\otimes$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

Group D

18 **Infinite Group** Show that the set of all rational numbers $x$ in the interval $[0,1)$ form an infinite group if the group operation is defined as

$$x+y=\begin{cases} x+y & \text{if } 0\le x+y<1 \\ x+y-1 & \text{if } x+y\ge 1 \end{cases}$$

19. **Groups and Latin Squares** The Cayley table for a group forms what is called a **Latin square.** That is, every element of the group occurs exactly once in every row and exactly once in every column. The converse is not true however, since there are Latin squares that do not form groups. Find a Latin square for the numbers $\{0, 1, 2\}$ that does not form a group.

20. **Modular Fun** Compute the following sums and products in the given cyclic group $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$.

a) $\mathbb{Z}_4$ : $1+7$ and $3\times 7$
b) $\mathbb{Z}_5$ : $9+7$ and $5\times 7$
c) $\mathbb{Z}_6$ : $10+7$ and $2\times 7$
d) $\mathbb{Z}_9$ : $11+20$ and $3\times 7$
e) $\mathbb{Z}_{10}$ : $100+7$ and $30\times 10$
f) $\mathbb{Z}_{11}$ : $11+11$ and $11\times 7$
g) $\mathbb{Z}_{11}$ : $12+7$ and $10\times 10$
h) $\mathbb{Z}_{15}$ : $14+1$ and $3\times 6$

21. **Modular Group** The set of all $2\times 2$ matrices

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

whose entries are integers with the group operation matrix multiplication, is a group called the **modular group**. It is the symmetry group for 2-dimensional **lattices**, which are infinitely large wire meshes which are all vectors have the form $a\hat{u}+b\hat{v}\in\mathbb{R}^2$ where $\hat{u},\hat{v}$ are two fixed basis vectors (each pair of basic vectors determines a mesh) and $a,b$ range over the integers .

a) Draw the mesh for the basis vectors $\hat{u} = (1,0), \hat{v} = (1,1)$ .
b) Show that the member of the modular group

$$\begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix}$$

distorts the plane but is a symmetry for the mesh; i.e. it maps the mesh onto itself.

ΓΣΘΨΞΠΩ