3. Integer Equivalence Classes and Symmetries

Let us now investigate some mathematical structures that can be viewed as sets with single operations.

The Integers modulo n

The integers mod n have become indispensable in the theory and applications of algebra. In mathematics they are used in cryptography, coding theory, and the detection of errors in identification codes.

We have already seen that two integers a and b are equivalent *mod n* if n divides a-b. The integers *mod n* also partition Z into n different equivalence classes; we will denote the set of these equivalence classes by Z_n. Consider the integers modulo 12 and the corresponding partition of the integers:

$$[0] = \{. . ., -12, 0, 12, 24, . . . \},$$

$$[1] = \{. . ., -11, 1, 13, 25, . . .\},$$

$$\ldots$$

$$[11] = \{. . ., -1, 11, 23, 35, . . . \}.$$

When no confusion can arise, we will use 0, 1, . . ., 11 to indicate the equivalence classes [0], [1], . . ., [11] respectively. We can do arithmetic on Z_n. For two integers a and b, define *addition modulo n* to be *(a+b) (mod n)*, that is, the remainder when a + b is divided by n. Similarly, *multiplication modulo n* is defined as *(ab) (mod n)*, the remainder when ab is divided by n.

Table 3.1. Multiplication table for Z_6

.	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	0
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Example 3.1. The following examples illustrate integer arithmetic modulo n:

$7 + 4 \equiv 1 \pmod{5}$ $3 + 5 \equiv 0 \pmod{8}$ $3 + 4 \equiv 7 \pmod{12}$

$7 \,.\, 3 \equiv 1 \pmod{5}$ $3 \,.\, 5 \equiv 7 \pmod{8}$ $3 \,.\, 4 \equiv 0 \pmod{12}$.

In particular, notice that it is possible that the product of two nonzero numbers modulo n can be equivalent to 0 modulo n.

Proposition 3.1. Let Z_n be the set of equivalence classes of the *integers mod n* and a, b, c ϵ Z_n. Then,

1. Addition and multiplication are commutative:

$$a + b \equiv b + a \pmod{n}$$

$$ab \equiv ba \pmod{n}$$

2. Addition and multiplication are associative:

$$(a + b) + c \equiv a + (b + c) \pmod{n}$$

$$(ab)c \equiv a(bc) \pmod{n}$$

3. There are both an additive and a multiplicative identity:

$$a + 0 \equiv a \pmod{n}$$

$$a.\ 1 \equiv a \pmod{n}$$

4. Multiplication distributes over addition: $a(b + c) \equiv ab + ac \pmod{n}$

5. For every integer a there is an additive inverse -a: $a + (-a) \equiv 0 \pmod{n}$

6. Let a be a nonzero integer. Then gcd(a; n) = 1 if and only if there exists a multiplicative inverse b for a (mod n); that is, a nonzero integer b such that $ab \equiv 1 \pmod{n}$.

Proof. We will prove (1) and (6) and leave the remaining properties to be left as exercise.

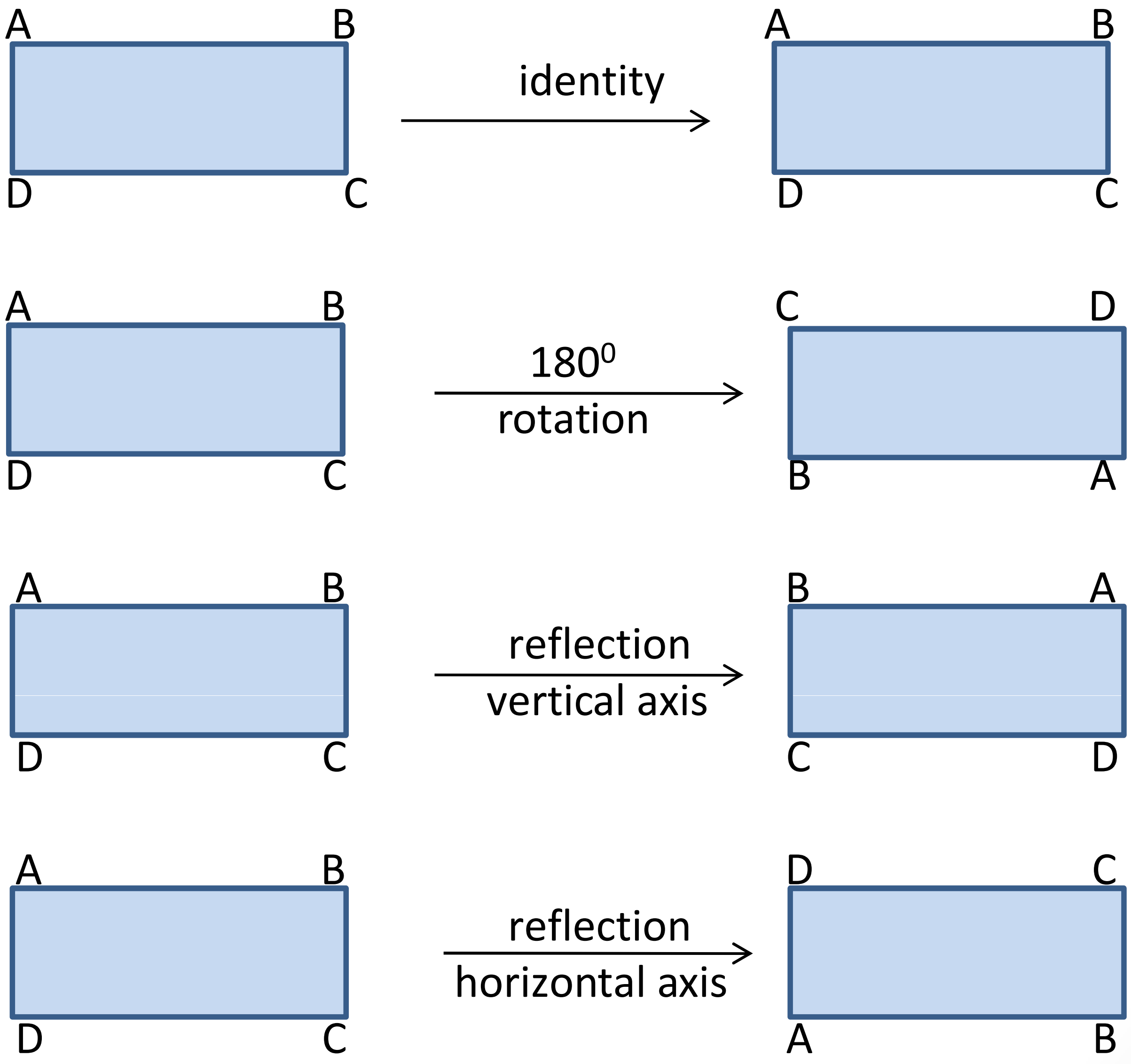
(1) Addition and multiplication are commutative modulo n since the remainder of a+b divided by n is the same as the remainder of b+a divided by n.

(6) Suppose that gcd(a; n) = 1. Then there exist integers r and s such that ar + ns = 1. Since ns = 1-ar, ra ≡ 1 (mod n). Letting b be the equivalence class of r, ab ≡ 1 (mod n).

Conversely, suppose that there exists a b such that ab ≡ 1 (mod n). Then n divides ab-1, so there is an integer k such that ab - nk = 1. Let d = gcd(a; n). Since d divides ab-nk, d must also divide 1; hence, d = 1.

Symmetries

Figure 3.1. Rigid motions of a rectangle



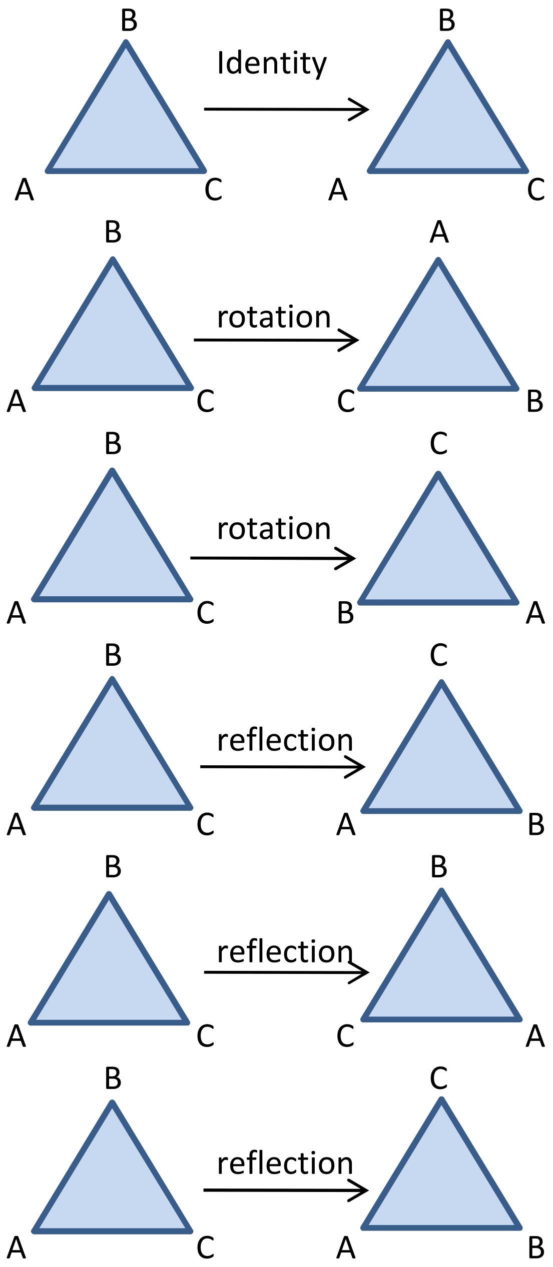
A **symmetry** of a geometric figure is a rearrangement of the figure preserving the arrangement of its sides and vertices as well as its distances and angles. A map from the plane to itself preserving the symmetry of an object is called a **rigid motion**. For example, if we look at the rectangle in Figure 3.1, it is easy to see that a rotation of 180^0 or 360^0 returns a rectangle in the plane with the same orientation as the original rectangle and the same relationship among the vertices. A reflection of the rectangle across either the vertical axis or the horizontal axis can also be seen to be a symmetry. However, a 90^0 rotation in either direction cannot be a symmetry unless the rectangle is a square.

Example 3.3. Suppose that S = {1, 2, 3}. Define a map π : S → S by π(1) = 2, π(2) = 1, π(3) = 3. This is a bijective map. An alternative way to write π is

$$\begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

For any finite set S, a one-to-one and onto mapping π: S → S is called a **permutation** of S.

Example 3.4.



$$i = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

$$\mu_3 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

4. Group

Definition 4.1. A nonempty set G is said to be a *group* if in G there is defined a **binary operation** * such that:

- (G1) Given a, b, c ∈G, then a* (b * c)= *(a * b) * c.*

(This is described by saying that the ***associative law*** holds in *G.)*

- (G2) There exists a special element e ∈ G such that

$$a * e = e * a = a, \text{ for all } a \in G$$

(e is called the ***identity* or *unit element*** of *G).*

- (G3) For every *a* ∈ G there exists an element *b* ∈ *G* such that

$$a * b = b * a = e$$

(We write this element *b* as a^{-1} and call it the ***inverse*** of *a* in *G.)*

The binary operation * in G is usually called the *product,* but keep in mind that this has nothing to do with product as we know it for the integers, rationals, reals, or complexes. In fact, as we shall see below, in many familiar examples of groups that come from numbers, what we call the product in these groups is actually the addition of numbers. *However, a general group need to have no relation whatsoever to a set of numbers.* We reiterate: A group is no more, no less, than a nonempty set with a binary operation * satisfying the three group axioms.

Before starting to look into the nature of groups, we look at some examples.

Example 4.1. Let Z be the set of all integers and let * be the ordinary addition, +, in Z. That Z is closed and associative under * are basic properties of the integers. What serves as the unit element, e, of Z under *? Clearly, since $a = a * e = a + e$, we have e =0, and 0 is the required identity element under addition. What about a^{-1}? Here too, since $e = 0 = a * a^{-1} = a + a^{-1}$, the a^{-1} in this instance is $-a$, and clearly $a *(-a) = a + (-a) = 0$.

Example 4.2. Let Q be the set of all rational numbers and let the operation * on Q be the ordinary addition of rational numbers. As above, 0 is easily shown to be a group under *. Note that Z∈Q and both *Z* and Q are groups under the same operation *.

Example 4.3. Let Q' be the set of all *nonzero* rational numbers and let the operation * on Q' be the ordinary multiplication of rational numbers. By the familiar properties of the rational numbers we see that Q' forms a group relative to *.

Example 4.4. Let R^+ be the set of all *positive real* numbers and let the operation * on R^+ be the ordinary product of real numbers. Again it is easy to check that R^+ is a group under *.

Example 4.5. The integers mod n form a group under addition modulo n. Consider Z_5, consisting of the equivalence classes of the integers 0, 1, 2, 3, and 4. We define the group operation on Z_5 by modular addition. We write the binary operation on the group additively; that is, we write m + n. The element 0 is the identity of the group and each element in Z5 has an inverse. For instance, 2+3 = 3+2 = 0. Table 4.1 is a Cayley table for Z_5. By proposition 3.1., $Z_n = \{0, 1, . . . , n − 1\}$ is a group under the binary operation of *addition mod n* (Verify!).

Table 4.1. Multiplication table for Z_5

.	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	0	2
3	0	3	0	3	0
4	0	4	2	0	4

Example 4.6. Not every set with a binary operation is a group. For example, if we let modular multiplication be the binary operation on Z_n, then Z_n fails to be a group. The element 1 acts as a group identity since 1·k=k·1=k for any k ∈ Z_n; however, a multiplicative inverse for 0 does not exist since 0·k = k·0 = 0 for every k in Z_n. Even if we consider the set $Z_n\setminus\{0\}$, we still may not have a group. For instance, let 2∈Z_6. Then 2 has no multiplicative inverse since 0·2=0 ; 1·2=2; 2·2=4; 3·2=0; 4·2=2; 5·2=4

By proposition 3.1., every nonzero k does have an inverse in Z_n if k is relatively prime to n. Denote the set of all such nonzero elements in Z_n by U(n). Then U(n) is a group called the group of units of Z_n. Table 4.2. is a Cayley table for the group U(8).

Table 4.2. Multiplication table for U(8)

.	**1**	**3**	**5**	**7**
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Definition 4.2. A group G is said to be a ***finite group*** if it has a finite number of elements. The number of elements in G is called the ***order* of G** and is denoted by IGI.

Definition 4.3. A group G is said to be ***abelian*** if *a* *b = *b* *a for all *a, b* ∈ *G.*

Example 4.7. The symmetries of an equilateral triangle described in Example 3.4. form a nonabelian group. As we observed, it is not necessarily true that αβ = βα for two symmetries α and β. Using Table 4.3., which is a Cayley table for this group, we can easily check that the symmetries of an equilateral triangle are indeed a group. We will denote this group by either S_3 or D_3, for reasons that will be explained later.

Table 4.3. Symmetries of an equilateral triangle

o	**i**	$\boldsymbol{\rho_1}$	$\boldsymbol{\rho_2}$	$\boldsymbol{\mu_1}$	$\boldsymbol{\mu_2}$	$\boldsymbol{\mu_3}$
i	i	ρ_1	ρ_2	μ_1	μ_2	μ_3
$\boldsymbol{\rho_1}$	ρ_1	ρ_2	i	μ_3	μ_1	μ_2
$\boldsymbol{\rho_2}$	ρ_2	i	ρ_1	μ_2	μ_3	μ_1
$\boldsymbol{\mu_1}$	μ_1	μ_2	μ_3	i	ρ_1	ρ_2
$\boldsymbol{\mu_2}$	μ_2	μ_3	μ_1	ρ_2	i	ρ_1
$\boldsymbol{\mu_3}$	μ_3	μ_1	μ_2	ρ_1	ρ_2	i

Example 4.8. We use $M_2(R)$ to denote the set of all 2 × 2 matrices. Let $GL_2(R)$ be the subset of $M_2(R)$ consisting of invertible matrices; that is, a matrix

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

is in $GL_2(R)$ if there exists a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$, where I is the 2×2 identity matrix. For A to have an inverse is equivalent to requiring that the determinant of A be nonzero; that is, $\det A = ad - bc \neq 0$. The set of invertible matrices forms a group called the ***general linear group***. The identity of the group is the identity matrix. The identity of the group is the identity matrix. The inverse can be calculated easily.

The product of two invertible matrices is again invertible. Matrix multiplication is associative, satisfying the other group axiom. For matrices it is not true in general that AB = BA; hence, $GL_2(R)$ is another example of a non-abelian group.