plication is well defined. Then $(\mathbf{Z}/(n),\cdot)$ is a semigroup with identity, and the set $(\mathbf{Z}/(n))^*$ consisting of the invertible elements in $\mathbf{Z}/(n)$ forms a multiplicative group of order $\phi(n)$, where ϕ is the Euler function.

(c) Permutations under usual composition

Let X be a nonempty set, and let G be the set of bijective mappings on X to X (i.e., permutations of X). Then G is a group under the usual composition of mappings. The unit element of G is the identity map of X, and the other group postulates are easily verified by direct applications of results on mappings (see Chapter 1).

This group is called the *group of permutations* of X (or the *symmetric group* on X) and is denoted as S_X. If $|X| = n, S_X$ is a group of order $n!$.

(d) Symmetries of a geometric figure

Consider permutations of the set X of all points of some geometric figures. Call a permutation $\sigma: X \to X$ a "symmetry" of S when it preserves distances, that is, when $d(a,b) = d(\sigma(a),\sigma(b))$, where $d(a,b)$ denotes the distance between the points $a,b \in X$. If σ,τ are two symmetries, then

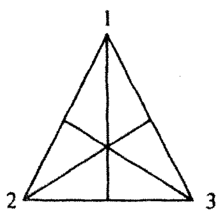
$$d((\sigma\tau)(a),(\sigma\tau)(b)) = d(\sigma(\tau(a)),\sigma(\tau(b))) = d(\tau(a),\tau(b)) = d(a,b).$$

Thus, $\sigma\tau$ is also a symmetry. Further, if σ is a symmetry then

$$d(\sigma^{-1}(a),\sigma^{-1}(b)) = d(\sigma(\sigma^{-1}(a)),\sigma(\sigma^{-1}(b))) = d(a,b).$$

So σ^{-1} is also a symmetry. Clearly, the identity permutation is a symmetry. Hence, the set of symmetries of S forms a group under composition of mappings.

Let us consider a special case when X is the set of points on the perimeter of an equilateral triangle:



The counterclockwise rotations through 0, $2\pi/3$, and $4\pi/3$ are three of the symmetries that move the vertices in the following manner:

$$\begin{matrix}1\to 1\\ 2\to 2,\\ 3\to 3\end{matrix}\qquad \begin{matrix}1\to 2\\ 2\to 3,\\ 3\to 1\end{matrix}\qquad \text{and}\qquad \begin{matrix}1\to 3\\ 2\to 1,\\ 3\to 2\end{matrix}$$

respectively. These are commonly written as

$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\qquad a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\qquad a^2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

(*Note.* Performing a rotation through $4\pi/3$ is equivalent to, or is a resultant of, performing a rotation through $2\pi/3$ and then again through $2\pi/3$. This explains our symbol a^2 for the rotation through $4\pi/3$.)

Three other symmetries are the reflections in the altitudes through the three vertices, namely,

$$\begin{matrix}1\to 1\\ 2\to 3,\\ 3\to 2\end{matrix}\qquad \begin{matrix}2\to 2\\ 3\to 1,\\ 1\to 3\end{matrix}\qquad \text{and}\qquad \begin{matrix}3\to 3\\ 1\to 2.\\ 2\to 1\end{matrix}$$

These may be rewritten as

$$b=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad a^2b=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \text{and}\quad ab=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

respectively, where the "product" is composition of mappings.

Since any symmetry of the equilateral triangle is determined by its effect on three vertices, the set of six symmetries is a complete list of symmetries of an equilateral triangle. We denote this group by D_3, called the dihedral group of degree 3. Since D_3 is a subset of S_3 and each has six elements, $D_3 = S_3$.

Similar considerations apply to any regular polygon of n sides. This is discussed later in Section 5.

(e) Linear groups

Let $\mathrm{GL}(n,F)$ be the set of $n \times n$ invertible matrices over a field F. Then $\mathrm{GL}(n,F)$ is a group under multiplication, called the general linear group (in dimension n). Consider the subset $\mathrm{SL}(n,F)$ of $\mathrm{GL}(n,F)$ consisting of matrices of determinant 1. Let $A,B \in \mathrm{SL}(n,F)$. Then $\det(AB) = (\det A)(\det B) = 1$, so $AB \in \mathrm{SL}(n,F)$. Clearly, $I_n \in \mathrm{SL}(n,F)$. Also, $\det(A^{-1})(\det A) = \det(I_n) = 1$ implies $\det(A^{-1}) = 1$, so $A^{-1} \in \mathrm{SL}(n,F)$. Therefore, $\mathrm{SL}(n,F)$ is also a group under multiplication.