CHAPTER ONE: SYMMETRIES AND GROUPS

1. Definitions

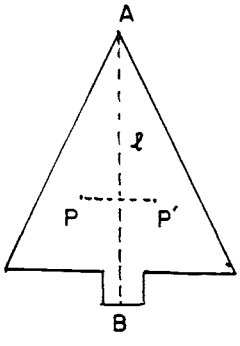
A plane figure is any subset F of the Euclidean plane E.

A symmetry (isometry, rigid motion) of a figure F is a bijective (one-to-one) map α from F onto F that preserves distance: the distance d(P,Q) between points P and Q of F is the same as the distance $d(P\alpha,Q\alpha)$ between their images $P\alpha$ and $Q\alpha$.

We write Sym F for the set of all symmetries of F.

2. Examples

I. A tree. Let F be a conventionalized picture of a tree, as shown. Then F has 'lateral symmetry' in the vertical line ℓ passing through the topmost point A. Explicitly F has a symmetry ρ that maps every point P of F that lies on ℓ to itself, and maps every other point P of F to a point $P\rho$ on the same horizontal as P, and at the same distance from ℓ, but on the other side of ℓ. The map ρ is a reflection with axis ℓ.



Every figure F has a trivial symmetry ε, mapping each point to itself. It is easy to see that ε and ρ are the only symmetries of F,

whence Sym F = {ε,ρ}. One could prove this, for example, by arguing that F contains no other point like A, where the boundary of F makes the same angle as at A, and that F contains no other point like B. From this it follows that, if α is any symmetry of F, then Aα = A and Bα = B. Now α must fix every point of F on the line ℓ, and, for each P not on ℓ, either Pα = P or Pα = Pρ, with the same choice for all P. Thus either α = ε or α = ρ.

If α and β are any two symmetries of a figure F, it is clear from the definition that α followed by β is also a symmetry of F. We write αβ for this product of α followed by β; explicitly, for all points P of F, P(αβ) = (Pα)β. Thus a multiplication (composition) is defined on the set Sym F, and the set Sym F equipped with this multiplication becomes a group, the symmetry group Sym F of F. The multiplication table for the symmetry group Sym F of the tree is shown.

	ε	ρ
ε	ε	ρ
ρ	ρ	ε

It is clear that if ε is the trivial symmetry of a figure F and α is any other symmetry of F, then εα = αε = α. The trivial symmetry ε acts under multiplication exactly as the number 1, and, for this reason, we shall henceforth write 1 rather than ε for the trivial symmetry of any figure.

II. Letters of the alphabet. We write the letters of the alphabet in a highly symmetric form.

The letters A, M, T, U, V, W, and Y evidently admit exactly the same symmetries as the tree: the trivial (or identity) symmetry and reflection in a vertical axis.

The letters B, C, D, E, and K admit a single nontrivial symmetry π, reflection in a horizontal axis. The multiplication table, as shown, is the same as that of the tree, except that ρ has been replaced by π. The two groups are isomorphic: there is a bijective map Ω from one to the other that preserves multiplication: for any two symmetries α and β of the first, the product of their images is the image of their product. $(\alpha\Omega)(\beta\Omega) = (\alpha\beta)\Omega$.

	1	π
1	1	π
π	π	1

The letters F, G, J, L, P, Q, R have only the trivial symmetry. Their symmetry group is the trivial group, Sym F = $\{1\}$, or, in customary notation, Sym F = 1. The multiplication table is as shown.

	1
1	1

The letters N, S, and Z admit only one nontrivial symmetry σ, a half turn, or rotation through π, about the center of the figure. The symmetry group is again isomorphic to that of the tree. We emphasize that although these groups are isomorphic as 'abstract' groups, they are in an obvious sense geometrically different.

The remaining letters H, I, O, X, as drawn, admit all the symmetries 1, ρ, π, σ considered so far, and, in fact, admit no others. Thus, for these figures F, Sym F = $\{1, \rho, \pi, \sigma\}$, with multiplication table as shown. To show, for example, that these are all symmetries of the letter H, it suffices to examine what each symmetry α

	1	ρ	π	σ
1	1	ρ	π	σ
ρ	ρ	1	σ	π
π	π	σ	1	ρ
σ	σ	π	ρ	1

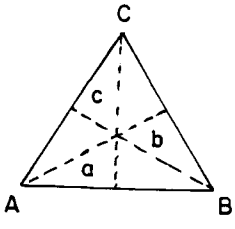
does to the four ends of the vertical lines in the letter H.

Note that if we regarded the letter I as an 'infinitely thin' vertical line segment without horizontal crosspieces, then the maps 1 and ρ would coincide as maps restricted to the points of the figure. Likewise π and σ would coincide, and the symmetry group would reduce to $\{1,\pi\}$. Usually it doesn't matter whether we regard the symmetries of a figure F as maps from F to F, or as maps from the entire plane E to itself which map the subset F to itself. The exceptions arise only in the case that the figure F is contained in some line in E.

Note that if we regarded the letter O as a circle, it would admit as symmetries all rotations, through any angle, about its center, as well as reflections in any diameter. The symmetry group would thus be infinite.

If we regarded the letter X as a cross, made up of two perpendicular line segments bisecting each other, then its symmetry group would contain eight elements.

III. An equilateral triangle. Let F be an equilateral triangle with vertices A, B, C. Let α, β, γ be reflections in the altitudes a, b, c through A, B, C; clearly α, β, γ are symmetries of F. Let σ be rotation through $2\pi/3$ about the center O of F; clearly σ, σ^2, and $\sigma^3 = 1$ are symmetries of F. In fact, these are all symmetries of F.



To prove this, observe that every symmetry of F must permute the set $V = \{A,B,C\}$ of vertices of F, and that, if two symmetries of F permute V in the same way they must be the same. Since there are exactly six permutations of a set V of three elements, Sym F cannot have more than the six elements that we have already found.

We shall not calculate the 6-by-6 multiplication table for Sym F; this is easy enough but rather tedious, and we shall find a simpler way to describe this group abstractly later. However, we illustrate the method by calculating the two products $\alpha\beta$ and $\beta\alpha$. Since α fixes A while interchanging (transposing) B and C, and β fixes B while transposing C and A, and γ fixes C while transposing A and B, we find that $A(\alpha\beta) = (A\alpha)\beta = A\beta = C$, that $B\alpha\beta = C\beta = A$, and that $C\alpha\beta = B\beta = B$. Thus $\alpha\beta$ permutes V in the same way as σ^2, and $\alpha\beta = \sigma^2$. A similar calculation gives $A\beta\alpha = C\alpha = B$, $B\beta\alpha = B\alpha = C$, and $C\beta\alpha = A\alpha = A$, whence $\beta\alpha = \sigma$. We emphasize that $\alpha\beta \neq \beta\alpha$. The group Sym F is noncommutative (nonabelian) and is in fact the smallest nonabelian group.

3. Groups

We now give precise definitions of some of the concepts used above.

Definition. A group is a pair of things, first a nonempty set G of objects called elements, and second an operation of multiplication associating with any two elements x and y of G a third element of G, written as xy and called their product. It is required that this multiplication satisfy three conditions:

(1) For all x, y, z in G, $(xy)z = x(yz)$;

(2) There is an element 1 in G such that, for all x in G,

$1x = x1 = x$;

(3) For all x in G there is an element x^{-1} in G such that

$x^{-1}x = xx^{-1} = 1$.

Remarks. (1) Although we have defined a group to be a set G together with an operation of multiplication defined on G, it is universal practice to speak simply of the group G, leaving the multiplication

to be understood from the context.

(2) If G is a set of mappings and multiplication is defined by applying first one and then the other, then the associative law $(xy)z = x(yz)$ is automatically fulfilled.

(3) If G is a set of mappings and G contains the identity map 1, then the condition $1x = x1 = x$ is automatic.

(4) The existence of an inverse x^{-1} to a map x requires that x be bijective.

(5) It is easy to see that a group cannot contain more than one element e such that $ex = xe = x$ for all x, and that, for given x in a group, there cannot be more than one element y such that $yx = xy = 1$.

(6) Our axioms for a group are deliberately somewhat redundant.

Examples of groups. The set Sym F of all distance preserving maps from a set F to itself, for F a subset of any geometrical space, is a group. The set of all invertible linear transformations of any vector space is a group. The set of all permutations of any set Ω is a group, Sym Ω, the symmetric group on the set Ω. (No concept of distance enters here, but one can think of an abstract set as a 'space' in which all distances between distinct points are equal.)

Definition. A group H is a subgroup of a group G if H is a subset of G and the multiplication in H is the same as that in G when restricted to elements in H. More simply, a subset H of G is a subgroup if $1 \in H$, if $x \in H$ implies $x^{-1} \in H$, and if $x, y \in H$ implies $xy \in H$.

Definition. An isomorphism ϕ from a group G_1 to a group G_2 is a bijection from G_1 to G_2 that preserves multiplication: $(xy)\phi = (x\phi)(y\phi)$ for all $x, y \in G_1$. Two groups G_1 and G_2 are isomorphic if there exists an isomorphism from G_1 to G_2.

Example. We have seen that if F is an equilateral triangle and V is the set of its vertices, then Sym F and Sym V are isomorphic.

The following rather easy but important theorem clarifies the connection between the class of 'abstract' groups, as given by our definition, and the 'concrete' geometric groups which will interest us in these notes.

CAYLEY'S THEOREM. Every group is isomorphic to a permutation group.

Proof. Let a group G be given. We must choose a set V of objects to be permuted, and we choose this to be G itself, or, more precisely, the set of elements of G. Now the set G = V will play two roles in the discussion, and, for this reason, we retain two names for it, G as the given group and V as the set of objects being permuted.

If g is any element of G and $v \in V$, then (since V = G), $vg \in V$. It is easy to check that the map (right multiplication by g) carrying each v to vg is a permutation of V; we call this permutation $g\phi$. We have thus defined a map ϕ from G to Sym V, carrying each $g \in G$ to $g\phi \in$ Sym V.

If $g\phi = h\phi$, then, for $1 \in V$, $1(g\phi) = 1g = g$ must equal $1(h\phi) = 1h = h$, whence g = h. Thus ϕ is a bijection from G onto a subset $G\phi$ of Sym V. Any two elements of $G\phi$ are of the form $g\phi$ and $h\phi$ for some g, h in G; now, for any v in V, repeated application of the various definitions shows that

$$v\big((g\phi)(h\phi)\big) = \big(v(g\phi)\big)(h\phi) = (vg)(h\phi) = (vg)h = v(gh) = v\big((gh)\phi\big),$$

whence $(g\phi)(h\phi) = (gh)\phi$. We conclude, first, that the product of any two elements of $G\phi$ is again an element of $G\phi$, and deduce easily that $G\phi$ is a subgroup of Sym V, that is, a group of permutations.

We conclude, second, that the map ϕ preserves multiplication; therefore, as a bijection from G to $G\phi$, it is an isomorphism from G to the permutation group $G\phi$. □

Remarks. We have stated Cayley's Theorem in its simplest form. Clearly the proof contains considerable more detailed information.

Cayley's Theorem illustrates one of the central processes in mathematics. One begins with a variety of more or less concrete objects that arise in the daily practice of mathematics, here groups of permutations, or of transformations. Observing certain uniformities, one lists as 'axioms' certain properties that the objects have in common, and passes to the study of all 'abstract' objects satisfying these axioms. With good fortune, and good judgement, one is then able to prove that all objects satisfying these axioms are isomorphic to objects of the class of concrete objects (possibly enlarged by hindsight) in which one was originally interested.

The usefulness of this interplay between the concrete and the abstract is fairly obvious. In studying a variety of concrete objects, here various groups arising in geometry, we are able to unify our discussion within the abstract theory of all groups. In the other direction, it is equally important that, in developing the abstract theory of groups, we frequently can profit from representing an abstract group in concrete form.

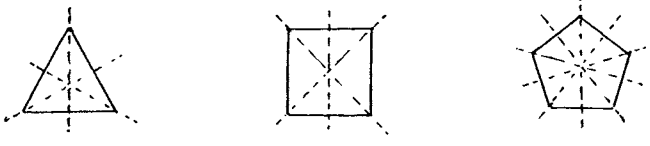
4. Symmetries of regular polygons

A regular polygon is a polygon with $n \geqslant 3$ sides of equal length in which the interior angles, between adjacent sides, are all equal. For $n = 3$, the regular polygon is an equilateral triangle; for $n = 4$ it is a square. We have described already the symmetry group of the equilateral triangle, and the symmetry group Sym F of the regular polygon F of $n > 3$ sides follows the same pattern.

Let F be a regular polygon with $n \geqslant 3$ sides, and let G = Sym F. It is clear that G contains a rotation σ about the center of F through an angle of $2\pi/n$; moreover, $\sigma^1 = \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are all distinct, while $\sigma^n = \sigma^0 = 1$. Thus G contains n rotational symmetries $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$.

By looking at what happens to the n vertices of F, it is clear that these are all the symmetries of F that preserve orientation, that is, preserve the cyclic order of vertices around the polygon, or do not 'turn the polygon over'.

It turns out that all other symmetries of F are reflections. At each vertex P there is an 'altitude' or 'diameter' p of F, passing through the center O of F; if n is odd, p bisects a side of F opposite P, while if n is even p ends at a vertex Q opposite P. If n is even, there is also a line through O bisecting two opposite sides. Whether n is odd or even, there are in all exactly n such 'diameters', which are clearly axes for reflectional symmetries of F.



We prove that G consists of exactly these 2n elements. First, if α is an orientation preserving symmetry of F, then $\alpha = \sigma^k$ for some integer k. Let ρ be any one of the n reflectional symmetries described above. If α reverses orientation, then, since ρ also reverses orientation, $\rho\alpha$ preserves orientation. It follows that $\rho\alpha = \sigma^k$ for some k, and that $\alpha = \rho^{-1}\sigma^k$ or, since $\rho^2 = 1$, that $\alpha = \rho\sigma^k$. We have proved the following:

(1) G consists of exactly 2n elements: n rotations $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ and n reflections $\rho, \rho\sigma, \rho\sigma^2, \ldots, \rho\sigma^{n-1}$.

(2) G is generated by σ and ρ: every element of G can be written as a product of powers of σ and powers of ρ.

Next, rather than describing a multiplication table for G, we describe rules for multiplying elements of G. First, from the equations $\sigma^n = 1$ and $\rho^2 = 1$, we are clearly permitted to reduce the exponent k on an element σ^k modulo n, and the exponent h on an element ρ^h modulo 2. In addition to the two relations $\sigma^n = 1$ and $\rho^2 = 1$, each involving only one of the generators σ and ρ, we verify a further relation $\rho\sigma\rho = \sigma^{-1}$ involving both of them, by direct calculation, by intuition, or from experience, say driving a screw into the underside of a table. From this relation it follows that $\sigma\rho = \rho\sigma^{-1}$ and, generally, $\sigma^k\rho = \rho\sigma^{-k}$.

We now show that the three relations above form a set of defining relations in the sense that if w_1 and w_2 are any two words in the generators σ and ρ, that is, products of powers of σ and ρ, and if w_1 and w_2 represent the same element of the group G, then the equation $w_1 = w_2$ follows from the three relations. More explicitly, we show that w_1 and w_2 can be reduced to the same form by repeated application of the rules of reducing k in σ^k modulo n, of reducing h in ρ^h modulo 2, and of replacing any part $\sigma^k\rho$ by $\rho\sigma^{-k}$. This is fairly obvious, but, to be precise, we reason by induction, at each stage diminishing the number of parts of the form $\sigma^k\rho^h$. If no such part occurs, w_1 (or w_2) is in one of the 2n canonical forms σ^k of $\rho\sigma^k$ for k = 0,1,...,n-1. If such a part does occur, we may suppose first of all that all parts ρ^h are of the form ρ. Now we must have either $w_i = \sigma^k\rho$ or w_i contains $\rho\sigma^k\rho$; applying the rule $\sigma^k\rho = \rho\sigma^{-k}$ either gives $w_i = \rho\sigma^{-k}$ or replaces the part $\rho\sigma^k\rho$ by $\rho^2\sigma^{-k} = \sigma^{-k}$. This completes the induction, and shows that both w_1 and w_2 are reducible to canonical form. Now, if w_1 and w_2 represent the same element of G, these two canonical forms must be the same, and we have established the equation $w_1 = w_2$.