and we notice that the symmetric functions x_1+x_2 and $x_1^2-2x_1x_2+x_2^2$ yield the two asymmetric functions x_1, x_2 when the two-valued radical $\sqrt{\ }$ is introduced. In general, introduction of radicals $\sqrt[p]{\ }$ multiplies the number of values of the function by p and divides symmetry by p, in the sense that the group of permutations leaving the function unaltered is reduced to $1/p$ of its previous size.

Vandermonde and Lagrange found that they could explain the previous solutions of cubic and quartic equations in terms of such symmetry reduction in the corresponding permutation groups, S_3 and S_4. They also found some properties of subgroups. For example, Lagrange essentially found the result now known as "Lagrange's theorem": the order of a subgroup divides the order of the group. However, they were unable to obtain sufficient understanding of the relation between radicals and subgroups of S_n to settle the equations of degree ≥ 5. Ruffini (1799) and Abel (1826) made enough progress with S_5 to be able to prove the unsolvability of the quintic, but none of these authors had a firm enough grip on the relation between radicals and permutations to handle arbitrary equations. They were not, in fact, conscious of the group concept, and it is only with hindsight that we can interpret their results in group-theoretic terms.

The concept, and indeed the word "group," first occurs in Galois (1831b). Along with it is the concept of *normal subgroup*, which finally unlocks the secret of solvability by radicals. A subgroup $H=\{h_1,h_2,\ldots,h_k\}$ of a group G is called normal if

$$\{gh_1,gh_2,\ldots,gh_k\}=\{h_1g,h_2g,\ldots,h_kg\}$$

for each $g\in G$. Galois showed that each equation E has a group G_E consisting of the permutations of the roots which leave rational functions of the roots unaltered, and that the reduction of symmetry accompanied by introduction of a radical corresponds to formation of a normal subgroup. Then solution of E by radicals is possible only if G_E can be reduced to the identity permutation by a chain of normal subgroups (nested in a certain way). If E is the general equation of degree n, then $G_E=S_n$ and the theorem of Ruffini and Abel is recovered by showing that S_n has no such chain of normal subgroups [see, for example, Dickson (1903)].

This brief sketch of Galois' ideas covers only a part of his theory. Another part is his theory of *fields*, which is needed to clarify the notion of rational function. The group theory and the field theory make up what is currently known as "Galois theory" [see, for example, Edwards (1984)].

What one might consider to be the summit of Galois' theory, rising above the confines of algebra, is currently neglected. This is the solution of equations by elliptic and related functions, for which one must consult earlier books such as Jordan (1870) and Klein (1884). The greatest triumph of this theory was the solution of the general quintic equation by elliptic modular functions in Hermite (1858), following a hint in Galois (1831a) (see also Section 6.5).

EXERCISES

The simplest type of permutation is a *transposition*, which swaps two things and leaves the others fixed.

19.2.1 Show that any permutation is a product of transpositions, that is, any arrangement of n things may be achieved by repeated swaps.

The group S_n of all permutations of n things has an important subgroup A_n, consisting of the permutations that are *even* in the following sense.

An *even permutation* f of $\{1,2,\dots,n\}$ is one with an even number of *inversions*, that is, pairs (i,j) for which $i<j$ and $f(i)>f(j)$ [Cramer (1750), p. 658]. This can be visualized by placing the numbers $1,2,\dots,n$ in two rows, one above the other, and drawing a line from k in the top row to $f(k)$ in the bottom row. Figure 19.1 illustrates the permutation $f(1)=2$, $f(2)=3$, $f(3)=1$ in this way.

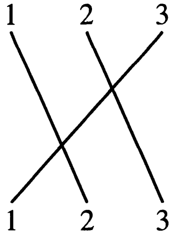

Figure 19.1: A permutation diagram

19.2.2 Explain why a permutation is even if and only if its diagram has an even number of crossings.

19.2.3 Show that the product of even permutations is even, and hence that the even permutations of $\{1,2,\dots,n\}$ form a group A_n.

19.2.4 Show that evenness does not depend on how the numbers $1,2,\dots,n$ are assigned to the n things. (Hint: if the numbers are permuted by g, show that the permutation f is replaced by the permutation $g^{-1}fg$.)

19.2.5 If g is an odd permutation, that is, $g\in S_n-A_n$, show that the set $gA_n=\{gf : f\in A_n\}$ is all the odd permutations in S_n, hence A_n contains exactly half the members of S_n.

19.3 Permutation Groups

Galois understood "group" to mean a group of permutations of a finite set, so his definition stated only that the product of two permutations in the group must again be a member of the group. Associativity, identity, and inverses were consequences of his assumptions, and indeed too obvious to be considered important from his point of view. Galois' work was published only in 1846, and by that time the theory of finite permutation groups had been taken up and systematized by Cauchy (1844). Cauchy likewise required only closure under product in his definition of group, but he recognized the importance of identity and inverses by introducing the notation of 1 for the identity and f^{-1} for the inverse of f.

Cayley (1854) was the first to consider the possibility of more abstract group elements, and with it the need to postulate associativity. (Incidentally, one of the few groups for which associativity is not obvious is that defined by the chord construction on a cubic curve: see Sections 11.6 and 16.5.) He took group elements to be simply "symbols," with a symbolic product of A and B written $A \cdot B$ and subject to the law $A \cdot (B \cdot C) = (A \cdot B) \cdot C$, and a unique element 1 subject to the laws $A \cdot 1 = 1 \cdot A = A$. He still assumed that each group was finite, however; this meant that the existence of inverses did not have to be postulated, only the validity of cancellation.

The existence of inverses in a finite group G, as defined by Cayley, follows from an argument used by Cauchy (1815) and developed more fully in Cauchy (1844). If $A \in G$, then the powers $A^2, A^3, \ldots$ all belong to G and hence they eventually include a recurrence of the same element:

$$A^m = A^n \quad \text{where } m < n.$$

Then, assuming it is valid to cancel A^m from both sides, A^{n-m} is the identity element 1 and A^{n-m-1} is the inverse of A.

The need to postulate inverses first arises with infinite groups, where this argument no longer holds. Geometry was historically the most important source of infinite groups, as we shall see in Section 19.5. It was in extending Cayley's abstract group theory to cover the symmetry groups of infinite tessellations that Dyck (1883) made first mention of inverses in the definition of group. We shall return to Dyck's concept of group in Section 19.6.

A theorem of Cayley (1878) shows that abstraction of the group concept is, in a sense, empty, because every group is essentially the same as a group of permutations. Cayley proved the theorem for finite groups only, where it is more valuable, but the proof easily extends to arbitrary groups (see exercises).

EXERCISES

The proof of Cayley's theorem goes as follows. Given any group G, associate any g in G with the function $\times g$ that sends each $h \in G$ to hg.

19.3.1 Show that function $\times g$ is a permutation of G, by showing that its effect can be undone by the function $\times g^{-1}$.

19.3.2 Show that different group elements g_1, g_2 give different functions $\times g_1$, $\times g_2$, and hence that there is a one-to-one correspondence between the elements g *in* G and the permutations $\times g$ *of* G.

19.3.3 Show that the permutation of G obtained by applying $\times g_1$, then $\times g_2$ is the permutation obtained by applying $\times g_1 g_2$.

Thus the group of permutations $\times g$ is *isomorphic* to the group G, in the sense that there is a one-to-one correspondence between their elements that preserves products. This is the precise way of saying that G is "essentially the same" as a group of permutations.

19.4 Polyhedral Groups

A beautiful illustration of Cayley's theorem that every group is a permutation group is provided by the regular polyhedra, whose symmetry groups turn out to be important subgroups of S_4 and S_5. The regular polyhedra also show us the more literal, geometric, meaning of "symmetry." If we imagine a polyhedron P occupying a region R in space, the symmetries of P can be viewed as the different ways of fitting P into R. Each symmetry is obtained by a rotation from the initial position, and the product of symmetries is the product of rotations.

We begin with the symmetries of the tetrahedron T: T has four vertices, V_1, V_2, V_3, V_4, so each symmetry of T is determined by a permutation of the four things V_1, V_2, V_3, V_4. There are $4 \times 3 = 12$ symmetries, because V_1 can be put at any of the four vertices of R, after which three choices remain for the remaining triangle of vertices V_2, V_3, V_4. One can check, using the fact that a permutation that leaves one element fixed and rotates the other three is even, that all the symmetries of T are even permutations of V_1, V_2, V_3, V_4. But the subgroup A_4 of *all* even permutations in S_4 has $\frac{1}{2} \times 4! = 12$ elements by the exercises in Section 19.2, so the symmetry group of T is precisely A_4.

The full permutation group S_4 can be realized by the symmetries of the cube. The four elements of the cube that are permuted are the long diagonals AA', BB', CC', DD' (Figure 19.2). One has to check, first, that each permutation of the diagonals is actually realizable. While doing this, it will become apparent that the position of the diagonals (bearing in mind that end points could be swapped) really determines the position of the cube (Exercise 19.5.1). S_4 is also the symmetry group of the octahedron, because of the dual relationship between cube and octahedron seen in Figure 19.3. Each symmetry of the cube is clearly a symmetry of its dual octahedron, and conversely.

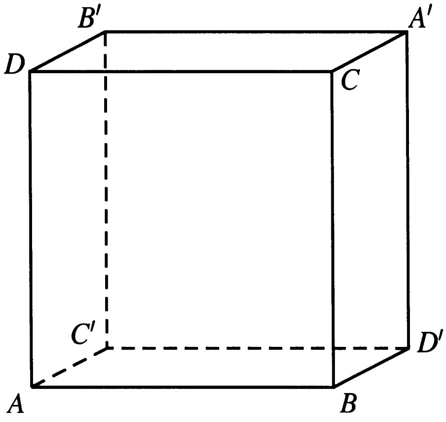

Figure 19.2: The cube and its diagonals

Likewise, the dual relationship between dodecahedron and icosahedron (Figure 19.3) shows that they have the same symmetry group. This group turns out to be A_5, the subgroup of even permutations in S_5. The five elements of the dodecahedron whose even permutations determine these symmetries are tetrahedra formed from sets of four diagonals [see Figure 19.4, which is from Coxeter and Moser (1980), p. 35].

For more information on the polyhedral groups, see Klein (1884). This book relates the theory of equations to the symmetries of the regular polyhedra and functions of a complex variable. The complex variable makes its appearance when the regular polyhedra are replaced by regular tessellations of the sphere $\mathbb{C} \cup \{\infty\}$, and their symmetries by linear fractional

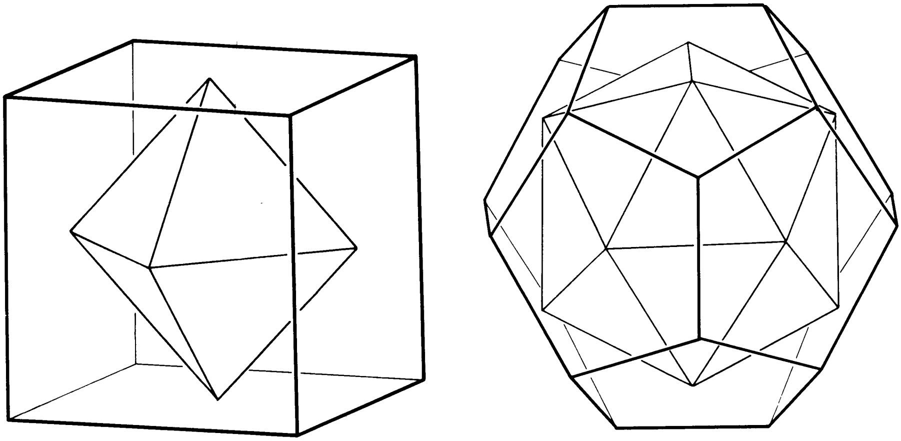

Figure 19.3: Dual polyhedra

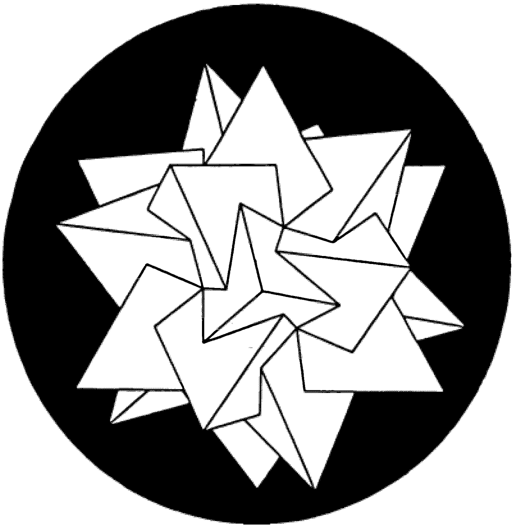

Figure 19.4: The tetrahedra in a dodecahedron

transformations, as in Section 18.6. Klein (1876) showed that, with trivial exceptions, *all* finite groups of linear fractional transformations come from the symmetries of the regular polyhedra in this way.

The regular polyhedra were also the source of another approach to groups: *presentation by generators and relations*. Hamilton (1856) showed that the icosahedral group can be generated by three elements ι, χ, λ subject to the relations

$$\iota^2 = \chi^3 = \lambda^5 = 1, \quad \lambda = \iota\chi. \tag{1}$$

This means that any element of the icosahedral group is a product (possibly with repetitions) of ι, χ, λ and that any relation between ι, χ, λ follows from the relations (1). Dyck (1882) gave similar presentations of the cube and tetrahedron groups, and for the groups of certain finite tessellations, as part of the first general discussion of generators and relations. We return to this in Section 19.6.

EXERCISES

19.4.1 Show that each permutation of the diagonals of a cube is realizable, for example, by showing that each transposition is realizable.

19.4.2 Show that a permutation of the diagonals uniquely determines the position of the cube.

19.5 Groups and Geometries

As the regular polyhedra show, geometric symmetry is fundamentally a group-theoretic notion. More generally, many notions of "equivalence" in geometry can be explained as properties that are preserved by certain groups of transformations. However, some revision of classical notions was necessary before geometry could benefit from group-theoretic ideas.

The oldest notion of geometric equivalence is that of *congruence*. The Greeks understood figures F_1 and F_2 to be congruent if there was a rigid motion of F_1 that carried it into F_2. The disadvantage of this idea was that motion had meaning only for the individual figure. The "product" of motions of different figures was meaningless, and hence one did not have a groups of motions.

The step that paved the way for the introduction of group theory into geometry was the extension of the idea of motion to the whole plane by Möbius (1827), which gave a meaning to the product of motions. In fact, Möbius considered all continuous transformations of the plane that preserve straightness of lines and gave separate attention to several subclasses of these transformations: those that preserve length (congruences), shape (similarities), and parallelism (affinities). He showed that the most general continuous transformations preserving straightness were just the projective transformations. Thus in one stroke Möbius defined the notions of congruence, similarity, affinity, and projective equivalence as properties that were invariant under certain classes of transformations of the plane. That the classes in question were groups was obvious as soon as one recognized the concept of group. It is an indication of the slowness with which the group concept was recognized that the restatement of Möbius' ideas in terms of groups occurred only with Klein (1872).

Klein's formulation became known as the *Erlanger Programm* because he announced it at the University of Erlangen. His idea is to associate each geometry with a group of transformations that preserve its characteristic properties. For example, plane Euclidean geometry is associated with the group of transformations of the plane that preserve the Euclidean distance $\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}$ between points (x_1,y_1) and (x_2,y_2). Plane projective geometry is associated with the group of projective transformations. Plane hyperbolic geometry, in view of the projective model, can be associated with the group of projective transformations that map the unit circle onto itself. An important influence on the Erlanger Programm was indeed Cayley (1859), where this group was first shown to determine a geometry, and the subsequent realization of Klein (1871) that the elements of this group are the rigid motions of hyperbolic geometry.

When geometry is reformulated in this way, certain geometric questions become questions about groups. A regular tessellation, for example, corresponds to a subgroup of the full group of motions, consisting of those motions that map the tessellation onto itself. In the case of hyperbolic geometry, where the problem of classifying tessellations is formidable, the interplay between geometric and group-theoretic ideas proved to be very fruitful. In the work of Poincaré (1882,1883) and Klein (1882b), group theory is the catalyst for a new synthesis of geometric, topological, and combinatorial ideas, which are described in Sections 19.6 and 22.7.

Exercises

If we view geometric objects (points, lines, curves, and so on) as subsets X of a space S, then relations such as congruence arise from groups of transformations of S in the following way. There is a group G of maps $g: S \rightarrow S$, and each geometric object X has a *G-orbit* $\{g(X): g \in G\}$, consisting of the objects onto which X is mapped by elements of G.