Next, the group $A = \mathrm{Aut}(\mathbb{F}_p{}^+)$ of automorphisms is a subgroup of $\mathrm{Perm}(\mathbb{F}_p{}^+)$. The distributive law shows that multiplication by an element $a \in \mathbb{F}_p{}^\times$ is an automorphism of $\mathbb{F}_p{}^+$. It is bijective, and $a(x + y) = ax + ay$. Therefore the image of $\varphi: G \longrightarrow \mathrm{Perm}(\mathbb{F}_p{}^+)$ is contained in the subgroup A. Finally, an automorphism of $\mathbb{F}_p{}^+$ is determined by where it sends the generator 1, and the image of 1 can not be zero. Using the operations of G, we can send 1 to any nonzero element. Therefore φ is a surjection from G onto A. Being both injective and surjective, φ is an isomorphism. □

9. FINITE SUBGROUPS OF THE ROTATION GROUP

In this section, we will apply the Counting Formula to classify finite subgroups of the rotation group SO_3, which was defined in Chapter 4 (5.4). As happens with finite groups of motions of the plane, there are rather few finite subgroups of SO_3, and all of them are symmetry groups of familiar figures.

(9.1) **Theorem.** Every finite subgroup G of SO_3 is one of the following:

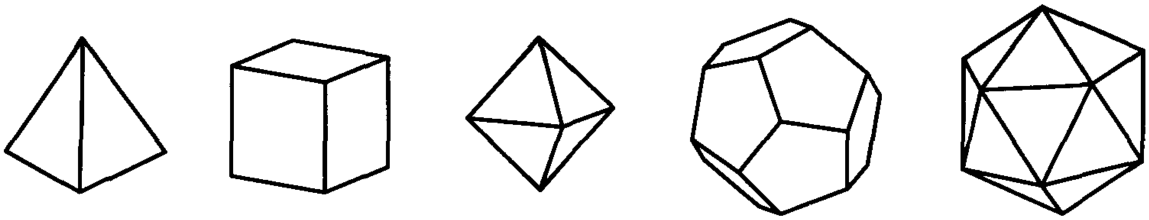
C_k: the *cyclic group* of rotations by multiples of $2\pi/k$ about a line;

D_k: the *dihedral group* (3.4) of symmetries of a regular k–gon;

T: the *tetrahedral group* of twelve rotations carrying a regular tetrahedron to itself;

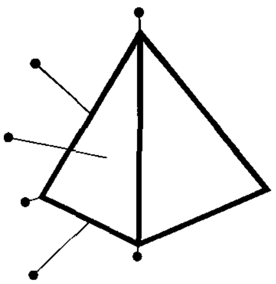
O: the *octahedral group* of order 24 of rotations of a cube, or of a regular octahedron;

I: the *icosahedral group* of 60 rotations of a regular dodecahedron or a regular icosahedron:



We will not attempt to classify the infinite subgroups.

Proof. Let G be a finite subgroup of SO_3, and denote its order by N. Every element g of G except the identity is a rotation about a line ℓ, and this line is obviously unique. So g fixes exactly two points of the unit sphere S in $\mathbb{R}^3$, namely the two points of intersection $\ell \cap S$. We call these points the *poles* of g. Thus a pole is a point p on the unit sphere such that $gp = p$ for some element $g \neq 1$ of G. For example, if G is the group of rotational symmetries of a tetrahedron Δ, then the poles will be the points of S lying over the vertices, the centers of faces, and the centers of edges of Δ.



Let P denote the set of all poles.

(9.2) **Lemma** The set P is carried to itself by the action of G on the sphere. So G operates on P.

Proof. Let p be a pole, say the pole of $g \in G$. Let x be an arbitrary element of G. We have to show that xp is a pole, meaning that xp is left fixed by some element g' of G other than the identity. The required element is xgx^{-1}: $xgx^{-1}(xp) = xgp = xp$, and $xgx^{-1} \neq 1$ because $g \neq 1$. □

We are now going to get information about the group by counting the poles. Since every element of G except 1 has two poles, our first guess might be that there are $2N - 2$ poles altogether. This isn't quite correct, because the same point p may be a pole for more than one group element.

The stabilizer of a pole p is the group of all of the rotations about the line $\ell = (0, p)$ which are in G. This group is cyclic and is generated by the rotation of smallest angle θ in G. [See the proof of Theorem (3.4a).] If the order of the stabilizer is r_p, then $\theta = 2\pi/r_p$.

We know that $r_p > 1$ because, since p is a pole, the stabilizer G_p contains an element besides 1. By the Counting Formula (7.2),

$$|G_p|\,|O_p| = |G|.$$

We write this equation as

$$r_p n_p = N, \tag{9.3}$$

where n_p is the number of poles in the orbit O_p of p.

The set of elements of G with a given pole p is the stabilizer G_p, minus the identity element. So there are $(r_p - 1)$ group elements with p as pole. On the other hand, every group element g except 1 has two poles. Having to subtract 1 everywhere is a little confusing here, but the correct relation is

$$\sum_{p \in P} (r_p - 1) = 2N - 2. \tag{9.4}$$

Now if p and p' are in the same orbit, then the stabilizers G_p and $G_{p'}$ have the same order. This is because $O_p = O_{p'}$ and $|G| = |G_p|\,|O_p| = |G_{p'}|\,|O_{p'}|$. Therefore we can collect together the terms on the left side of (9.4) which correspond to poles in a given orbit O_p. There are n_p such terms, so the number of poles collected together is $n_p(r_p - 1)$. Let us number the orbits in some way, as $O_1, O_2, \ldots$. Then

$$\sum_i n_i(r_i - 1) = 2N - 2,$$

where $n_i = |O_i|$, and $r_i = |G_p|$ for any $p \in O_i$. Since $N = n_i r_i$, we can divide both sides by N and switch sides, to get the famous formula

$$2 - \frac{2}{N} = \sum_i \left(1 - \frac{1}{r_i}\right). \qquad (9.5)$$

This formula may not look very promising at first glance, but actually it tells us a great deal. The left side is less than 2, while each term on the right is at least $\frac{1}{2}$. It follows that there can be at most three orbits!

The rest of the classification is made by listing the various possibilities:

One orbit: $2 - \frac{2}{N} = 1 - \frac{1}{r}$. This is impossible, because $2 - \frac{2}{N} \geq 1$, while $1 - \frac{1}{r} < 1$.

Two orbits: $2 - \frac{2}{N} = \left(1 - \frac{1}{r_1}\right) + \left(1 - \frac{1}{r_2}\right)$, that is, $\frac{2}{N} = \frac{1}{r_1} + \frac{1}{r_2}$.

We know that $r_i \leq N$, because r_i divides N. This equation can hold only if $r_1 = r_2 = N$. Thus $n_1 = n_2 = 1$. There are two poles p, p', both fixed by every element of the group. Obviously, G is the cyclic group C_N of rotations about the line ℓ through p and p'.

Three orbits: This is the main case: Formula (9.5) reduces to

$$\frac{2}{N} = \frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1.$$

We arrange the r_i in increasing order. Then $r_1 = 2$. For if all r_i were at least 3, then the right side would be ≤ 0, which is impossible.

Case 1: At least two of the orders r_i are 2: $r_1 = r_2 = 2$. The third order $r_3 = r$ can be arbitrary, and $N = 2r$. Then $n_3 = 2$: There is one pair of poles $\{p, p'\}$ making the orbit O_3. Every element g either fixes p and p' or interchanges them. So the elements of G are rotations about $\ell = (p, p')$, or else they are rotations by π about a line ℓ' perpendicular to ℓ. It is easily seen that G is the group of rotations fixing a regular r-gon Δ, the dihedral group D_r. The polygon Δ lies in the plane perpendicular to ℓ, and the vertices and the centers of faces of Δ corresponding to the remaining poles. The bilateral (reflection) symmetries of the polygon in $\mathbb{R}^2$ have become rotations through the angle π when Δ is put into $\mathbb{R}^3$.

Case 2: Only one r_i is 2: The triples $r_1 = 2$, $r_2 \geq 4$, $r_3 \geq 4$ are impossible, because $1/2 + 1/4 + 1/4 - 1 = 0$. Similarly, $r_i = 2$, $r_2 = 3$, $r_3 \geq 6$ can not occur because $1/2 + 1/3 + 1/6 - 1 = 0$. There remain only three possibilities:

(9.6)

(i) $r_i = (2, 3, 3)$, $N = 12$;
(ii) $r_i = (2, 3, 4)$, $N = 24$;
(iii) $r_i = (2, 3, 5)$, $N = 60$.

It remains to analyze these three cases. We will indicate the configurations briefly.

(9.7)

(i) $n_i = (6, 4, 4)$. The poles in the orbit O_2 are the vertices of a regular tetrahedron Δ, and G is the group of rotations fixing it: $G = T$. Here n_1 is the number of edges of Δ, and n_2, n_3 are the numbers of vertices and faces of Δ.

(ii) $n_i = (12, 8, 6)$. The poles in O_2 are the vertices of a cube, and the poles in O_3 are the vertices of a regular octahedron. $G = O$ is the group of their rotations. The integers n_i are the numbers of edges, vertices, and faces of a cube.

(iii) $n_i = (30, 20, 12)$. The poles of O_2 are the vertices of a regular dodecahedron, and those in O_3 are the vertices of a regular icosahedron: $G = I$.

There is still some work to be done to prove the assertions of (9.7). Intuitively, the poles in an orbit should be the vertices of a regular polyhedron because they form a single orbit and are therefore evenly spaced on the sphere. However this is not quite accurate, because the centers of the edges of a cube, for example, form a single orbit but do not span a regular polyhedron. (The figure they span is called a *truncated* polyhedron.)

As an example, consider (9.7iii). Let p be one of the 12 poles in O_3, and let q be one of the poles of O_2 nearest to p. Since the stabilizer of p is of order 5 and operates on O_2 (because G does), the images of q provide a set of five nearest neighbors to p, the poles obtained from q by the five rotations about p in G. Therefore the number of poles of O_2 nearest to p is a multiple of 5, and it is easily seen that 5 is the only possibility. So these five poles are the vertices of a regular pentagon. The 12 pentagons so defined form a regular dodecahedron. □

We close this chapter by remarking that our discussion of the motions of the plane has analogues for the group M_3 of rigid motions of 3-space. In particular, one can define the notion of *crystallographic group*, which is a discrete subgroup whose translation group is a three-dimensional lattice L. To say that L is a lattice means that there are three linearly independent vectors a, b, c in $\mathbb{R}^3$ such that $t_a, t_b, t_c, \in G$. The crystallographic groups are analogous to lattice groups in $M = M_2$, and crystals form examples of three-dimensional configurations having such groups as symmetry. We imagine the crystal to be infinitely large. Then the fact that the molecules are arranged regularly implies that they form an array having three independent translational symmetries. It has been shown that there are 230 types of crystallographic groups, analogous to the 17 lattice groups (4.15). This is too long a list to be very useful, and so crystals have been classified more crudely into seven *crystal systems*. For more about this, and for a discussion of the 32 crystallographic point groups, look in a book on crystallography.

> *Un bon héritage vaut mieux que le plus joli problème de géométrie,*
> *parce qu'il tient lieu de méthode générale,*
> *et sert à resoudre bien des problèmes.*
>
> Gottfried Wilhelm Leibnitz

EXERCISES

1. Symmetry of Plane Figures

1. Prove that the set of symmetries of a figure F in the plane forms a group.
2. List all symmetries of **(a)** a square and **(b)** a regular pentagon.
3. List all symmetries of the following figures.
   (a) (1.4) **(b)** (1.5) **(c)** (1.6) **(d)** (1.7)
4. Let G be a finite group of rotations of the plane about the origin. Prove that G is cyclic.

2. The Group of Motions of the Plane

1. Compute the fixed point of $t_a\rho_\theta$ algebraically.
2. Verify the rules (2.5) by explicit calculation, using the definitions (2.3).
3. Prove that O is not a normal subgroup of M.
4. Let m be an orientation-reversing motion. Prove that m^2 is a translation.
5. Let SM denote the subset of orientation-preserving motions of the plane. Prove that SM is a normal subgroup of M, and determine its index in M.
6. Prove that a linear operator on $\mathbb{R}^2$ is a reflection if and only if its eigenvalues are 1 and -1, and its eigenvectors are orthogonal.
7. Prove that a conjugate of a reflection or a glide reflection is a motion of the same type, and that if m is a glide reflection then the glide vectors of m and of its conjugates have the same length.
8. Complete the proof that (2.13) is a homomorphism.
9. Prove that the map $M \longrightarrow \{1, r\}$ defined by $t_a\rho_\theta \rightsquigarrow 1$, $t_a\rho_\theta r \rightsquigarrow r$ is a homomorphism.
10. Compute the effect of rotation of the axes through an angle η on the expressions $t_a\rho_\theta$ and $t_a\rho_\theta r$ for a motion.