Chapter 5

Symmetry

L'algèbre n'est qu'une géométrie écrite;
la géométrie n'est qu'une algèbre figurée.

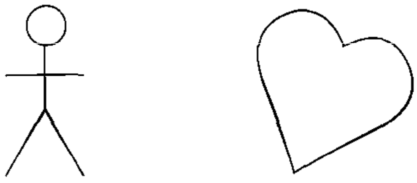
Sophie Germain

The study of symmetry provides one of the most appealing applications of group theory. Groups were first invented to analyze symmetries of certain algebraic structures called field extensions, and because symmetry is a common phenomenon in all sciences, it is still one of the two main ways in which group theory is applied. The other way is through group representations, which will be discussed in Chapter 9. In the first four sections of this chapter, we will study the symmetry of plane figures in terms of groups of rigid motions of the plane. Plane figures provide a rich source of examples and a background for the general concept of group operation, which is introduced in Section 5.

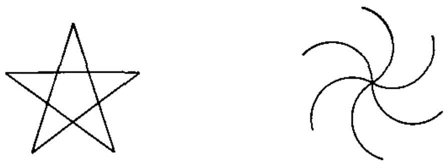
When studying symmetry, we will allow ourselves to use geometric reasoning without bothering to carry the arguments back to the axioms of geometry. That can be left for another occasion.

1. SYMMETRY OF PLANE FIGURES

The possible symmetry of plane figures is usually classified into the main types shown in Figures (1.1–1.3).



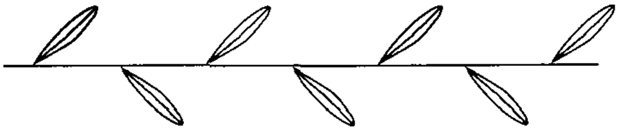
(1.1) **Figure.** Bilateral symmetry.



(1.2) **Figure.** Rotational symmetry.

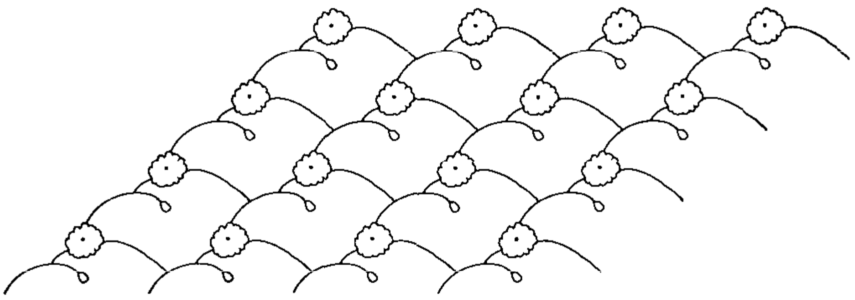
(1.3) **Figure.** Translational symmetry.

A fourth type of symmetry also exists, though it may be slightly less familiar:



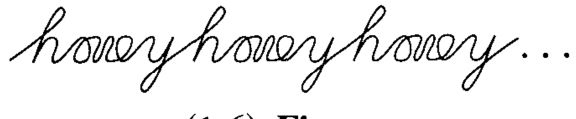
(1.4) **Figure.** Glide symmetry.

Figures such as wallpaper patterns may have two independent translational symmetries, as shown in Figure (1.5):



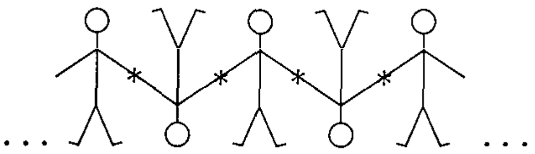
(1.5) **Figure.**

Other combinations of symmetries may also occur. For instance, the star has bilateral as well as rotational symmetry. Figure (1.6) is an example in which translational and rotational symmetry are combined:



(1.6) **Figure.**

Another example is shown in Figure (1.7).



(1.7) **Figure.**

As in Section 5 of Chapter 4, we call a map $m\colon P \longrightarrow P$ from the plane P to itself a *rigid motion,* or an *isometry,* if it is distance-preserving, that is, if for any two points $p, q \in P$ the distance from p to q is equal to the distance from $m(p)$ to $m(q)$. We will show in the next section that the rigid motions are translations, rotations, reflections, and glide reflections. They form a group M whose law of composition is composition of functions.

If a rigid motion m carries a subset F of the plane to itself, we call it a *symmetry* of F. The set of all symmetries of F always forms a subgroup G of M, called the *group of symmetries* of the figure. The fact that G is a subgroup is clear: If m and m' carry F to F, then so does the composed map mm', and so on.

The group of symmetries of the bilaterally symmetric Figure (1.1) consists of two elements: the identity transformation 1 and the reflection r about a line called the axis of symmetry. We have the relation $rr = 1$, which shows that G is a cyclic group of order 2, as it must be, because there is no other group of order 2.

The group of symmetries of Figure (1.3) is an infinite cyclic group generated by the motion which carries it one unit to the left. We call such a motion a *translation* t:

$$G = \{\ldots, t^{-2}, t^{-1}, 1, t, t^2, \ldots\}.$$

The symmetry groups of Figures (1.4, 1.6, 1.7) contain elements besides translations and are therefore larger. Do the exercise of describing their elements.

2. THE GROUP OF MOTIONS OF THE PLANE

This section describes the group M of all rigid motions of the plane. The coarsest classification of motions is into the *orientation-preserving* motions, those which do not flip the plane over, and the *orientation-reversing* motions which do flip it over (see Chapter 4, Section 5). We can use this partition of M to define a map

$$M \longrightarrow \{\pm 1\},$$

by sending the orientation-preserving motions to 1 and the orientation-reversing motions to -1. You will convince yourself without difficulty that this map is a homomorphism: The product of two orientation-reversing motions is orientation-preserving, and so on.

A finer classification of the motions is as follows:

(2.1)

(a) *The orientation-preserving motions:*

(i) *Translation:* parallel motion of the plane by a vector a: $p \rightsquigarrow p+a$.

(ii) *Rotation:* rotates the plane by an angle $\theta \neq 0$ about some point.

(b) *The orientation-reversing motions:*

(i) *Reflection* about a line ℓ.

(ii) *Glide reflection:* obtained by reflecting about a line ℓ, and then translating by a nonzero vector a parallel to ℓ.

(2.2) **Theorem.** The above list is complete. Every rigid motion is a translation, a rotation, a reflection, a glide reflection, or the identity.

This theorem is remarkable. One consequence is that the composition of rotations about two different points is a rotation about a third point, unless it is a translation. This fact follows from the theorem, because the composition preserves orientation, but it is not obvious.

Some of the other compositions are easier to visualize. The composition of rotations through angles θ and η about the same point is again a rotation, through the angle $\theta + \eta$, about that point. The composition of translations by the vectors a and b is the translation by their sum $a + b$.

Note that a translation does not leave any point fixed (unless the vector a is zero, in which case it is the identity map). Glides do not have fixed points either. On the other hand, a rotation fixes exactly one point, the center of rotation, and a reflection fixes the points on the line of reflection. Hence the composition of reflections about two nonparallel lines ℓ_1, ℓ_2 is a rotation about the intersection point $p = \ell_1 \cap \ell_2$. This follows from the theorem, because the composition does fix p, and it is orientation-preserving. The composition of two reflections about parallel lines is a translation by a vector orthogonal to the lines.

In order to prove Theorem (2.2), and also to be able to compute conveniently in the group M, we are going to choose some special motions as generators for the group. We will obtain defining relations similar to the relations (1.18) in Chapter 2 which define the symmetric group S_3, but since M is infinite, there will be more of them.

Let us identify the plane with the space $\mathbb{R}^2$ of column vectors, by choosing a coordinate system. Having done this, we choose as generators the translations, the rotations about the origin, and the reflection about the x_1-axis:

(2.3)

(a) *Translation* t_a by a vector a: $t_a(x) = x + a = \begin{bmatrix} x_1 + a_1 \\ x_2 + a_2 \end{bmatrix}$.

(b) *Rotation* ρ_θ by an angle θ about the origin:

$$\rho_\theta(x) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

(c) *Reflection* r about the x_1-axis: $r(x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_2 \end{bmatrix}$.

Since they fix the origin, the rotations ρ_θ and the reflection r are orthogonal operators on $\mathbb{R}^2$. A translation is not a linear operator—it does not send zero to itself, except of course for translation by the zero vector.

The motions (2.3) are not all of the elements of M. For example, rotation about a point other than the origin is not listed, nor are reflections about other lines.

However, they do generate the group: Every element of M is a product of such elements. It is easily seen that any rigid motion m can be obtained by composing them. Either

$$(2.4) \qquad m = t_a\rho_\theta \quad \text{or else} \quad m = t_a\rho_\theta r,$$

for some vector a and angle θ, possibly zero. To see this, we recall that every rigid motion is the composition of an orthogonal operator followed by a translation [Chapter 4 (5.20)]. So we can write m in the form $m = t_a m'$, where m' is an orthogonal operator. Next, if $\det m' = 1$, then it is one of the rotations ρ_θ. This follows from Theorem (5.5) of Chapter 4. So in this case, $m = t_a\rho_\theta$. Finally, if $\det m' = -1$, then $\det m'r = 1$, so $m'r$ is a rotation ρ_θ. Since $r^2 = 1$, $m' = \rho_\theta r$ in this case, and $m = t_a\rho_\theta r$.

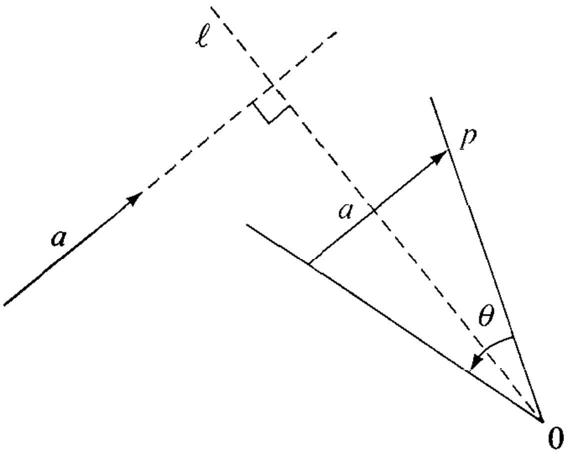
The expression of a motion m as a product (2.4) is unique. For suppose that m is expressed in two ways: $m = t_a\rho_\theta r^i = t_b\rho_\eta r^j$, where i, j are 0 or 1. Since m is orientation-preserving if $i = 0$ and orientation-reversing if $i = 1$, we must have $i = j$, and so we can cancel r from both sides if necessary, to obtain the equality $t_a\rho_\theta = t_b\rho_\eta$. Multiplying both sides on the left by t_{-b} and on the right by $\rho_{-\theta}$, we find $t_{a-b} = \rho_{\eta-\theta}$. But a translation is not a rotation unless both are the trivial operations. So $a = b$ and $\theta = \eta$. □

Computation in M can be done with the symbols t_a, ρ_θ, r using rules for composing them which can be calculated from the formulas (2.3). The necessary rules are as follows:

$$(2.5) \qquad \begin{aligned} t_a t_b &= t_{a+b}, \quad \rho_\theta\rho_\eta = \rho_{\theta+\eta}, \qquad rr = 1, \\ \rho_\theta t_a &= t_{a'}\rho_\theta, \quad \text{where } a' = \rho_\theta(a), \\ r t_a &= t_{a'} r, \quad \text{where } a' = r(a), \\ r\rho_\theta &= \rho_{-\theta} r. \end{aligned}$$

Using these rules, we can reduce any product of our generators to one of the two forms (2.4). The form we get is uniquely determined, because there is only one expression of the form (2.4) for a given motion.

Proof of Theorem (2.2). Let m be a rigid motion which preserves orientation but is not a translation. We want to prove that m is a rotation about some point. It is clear that an orientation-preserving motion which fixes a point p in the plane must be a rotation about p. So we must show that every orientation-preserving motion m which is not a translation fixes some point. We write $m = t_a\rho_\theta$ as in (2.4). By assumption, $\theta \neq 0$. One can use the geometric picture in Figure (2.6) to find the fixed point. In it, ℓ is the line through the origin and perpendicular to a, and the sector with angle θ is situated so as to be bisected by ℓ. The point p is determined by inserting the vector a into the sector, as shown. To check that m fixes p, remember that the operation ρ_θ is the one which is made first, and is followed by t_a.



(2.6) **Figure.** The fixed point of an orientation-preserving motion.

Another way to find the fixed point is by solving the equation $x = t_a\rho_\theta(x)$ algebraically for x. By definition of a translation, $t_a(\rho_\theta(x)) = \rho_\theta(x) + a$. So the equation we need to solve is

$$x - \rho_\theta(x) = a \quad \text{or}$$

(2.7)
$$\begin{bmatrix} 1-\cos\theta & \sin\theta \\ -\sin\theta & 1-\cos\theta \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}.$$

Note that $\det(1 - \rho_\theta) = 2 - 2\cos\theta$. The determinant is not zero if $\theta \neq 0$, so there is a unique solution for x.

(2.8) **Corollary.** The motion $m = t_a\rho_\theta$ is the rotation through the angle θ about its fixed point.

Proof. As we just saw, the fixed point of m is the one which satisfies the relation $p = \rho_\theta(p) + a$. Then for any x,

$$m(p + x) = t_a\rho_\theta(p + x) = \rho_\theta(p + x) + a = \rho_\theta(p) + \rho_\theta(x) + a = p + \rho_\theta(x).$$

Thus m sends $p + x$ to $p + \rho_\theta(x)$. So it is the rotation about p through the angle θ, as required. □

Next, we will show that any orientation-reversing motion $m = t_a\rho_\theta r$ is a glide reflection or a reflection (which we may consider to be a glide reflection having glide vector zero). We do this by finding a line ℓ which is sent to itself by m, and so that the motion of m on ℓ is a translation. It is clear geometrically that an orientation-reversing motion which acts in this way on a line is a glide reflection.

The geometry is more complicated here, so we will reduce the problem in two steps. First, the motion $\rho_\theta r = r'$ is a reflection about a line. The line is the one which intersects the x_1-axis at an angle of $\frac{1}{2}\theta$ at the origin. This is not hard to see, geometrically or algebraically. So our motion m is the product of the translation t_a and the reflection r'. We may as well rotate coordinates so that the x_1-axis becomes the line of reflection of r'. Then r' becomes our standard reflection r, and the translation t_a remains a translation, though the coordinates of the vector a will have changed. In this new coordinate system, the motion is written as $m = t_a r$, and it acts as

$$m\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 + a_1 \\ -x_2 + a_2 \end{bmatrix}.$$

This motion sends the line $x_2 = \frac{1}{2}a_2$ to itself, by the translation $(x_1, \frac{1}{2}a_2)^t \rightsquigarrow (x_1 + a_1, \frac{1}{2}a_2)^t$, and so m is a glide along this line. □

There are two important subgroups of M for which we must introduce notation:

(2.9)

T, the group of translations.

$\mathbf{O}$, the group of orthogonal operators.

The group $\mathbf{O}$ consists of the motions leaving the origin fixed. It contains the rotations about the origin and reflections about lines through the origin.

Notice that with our choice of coordinates we get a bijective correspondence

$$\begin{aligned} \mathbb{R}^2 &\longrightarrow T \\ a &\rightsquigarrow t_a. \end{aligned} \tag{2.10}$$

This is an isomorphism of the additive group $(\mathbb{R}^2)^+$ with the subgroup T, because $t_a t_b = t_{a+b}$.

The elements of $\mathbf{O}$ are linear operators. Again making use of our choice of coordinates, we can associate an element $m \in \mathbf{O}$ to its matrix. Doing so, we obtain an isomorphism

$$O_2 \xrightarrow{\sim} \mathbf{O}$$

from the group O_2 of orthogonal 2×2 matrices to $\mathbf{O}$ [see Chapter 4 (5.16)].

We can also consider the subgroup of M of motions fixing a point of the plane other than the origin. This subgroup is related to $\mathbf{O}$ as follows:

(2.11) **Proposition.**

(a) Let p be a point of the plane. Let ρ_θ' denote rotation through the angle θ about p, and let r' denote reflection about the line through p and parallel to the x-axis. Then $\rho_\theta' = t_p \rho_\theta t_p^{-1}$ and $r' = t_p r t_p^{-1}$.

(b) The subgroup of M of motions fixing p is the conjugate subgroup

$$\mathbf{O}' = t_p \mathbf{O} t_p^{-1}.$$

Proof. We can obtain the rotation ρ_θ' in this way: First translate p to the origin, next rotate the plane about the origin through the angle θ, and finally translate the origin back to p:

$$\rho_\theta' = t_p\rho_\theta t_{-p} = t_p\rho_\theta t_p^{-1}.$$

The reflection r' can be obtained in the same way from r:

$$r' = t_p r t_{-p} = t_p r t_p^{-1}.$$

This proves (a). Since every motion fixing p has the form ρ_θ' or $\rho_\theta' r'$ [see the proof of (2.4)], (b) follows from (a). □

There is an important homomorphism φ from M to $\mathbf{O}$ whose kernel is T, which is obtained by dropping the translation from the products (2.4):

(2.12)
$$\begin{gathered} M \xrightarrow{\varphi} \mathbf{O} \\ t_a\rho_\theta \rightsquigarrow \rho_\theta \\ t_a\rho_\theta r \rightsquigarrow \rho_\theta r. \end{gathered}$$

This may look too naive to be a good definition, but formulas (2.5) show that φ is a homomorphism: $(t_a\rho_\theta)(t_b\rho_\eta) = t_a t_{b'}\rho_\theta\rho_\eta = t_{a+b'}\rho_{\theta+\eta}$, hence $\varphi(t_a\rho_\theta t_b\rho_\eta) = \rho_{\theta+\eta}$, and so on. Since T is the kernel of a homomorphism, it is a normal subgroup of M.

Note that we can not define a homomorphism from M to T in this way.

(2.13) **Proposition.** Let p be any point of the plane, and let ρ_θ' denote rotation through the angle θ about p. Then $\varphi(\rho_\theta') = \rho_\theta$. Similarly, if r' is reflection about the line through p and parallel to the x-axis, then $\varphi(r') = r$.

This follows from (2.11a), because t_p is in the kernel of φ. The proposition can also be expressed as follows:

(2.14) *The homomorphism φ does not depend on the choice of origin.* □

3. FINITE GROUPS OF MOTIONS

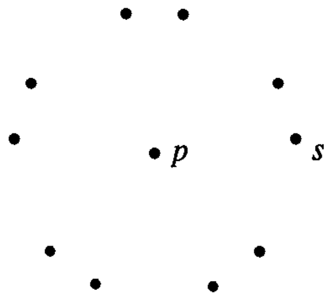
In this section we investigate the possible finite groups of symmetry of figures such as (1.1) and (1.2). So we are led to the study of finite subgroups G of the group M of rigid motions of the plane.

The key observation which allows us to describe all finite subgroups is the following theorem.

(3.1) **Theorem.** *Fixed Point Theorem:* Let G be a finite subgroup of the group of motions M. There is a point p in the plane which is left fixed by every element of G, that is, there is a point p such that $g(p) = p$ for all $g \in G$.

It follows, for example, that any subgroup of M which contains rotations about two different points is infinite.

Here is a beautiful geometric proof of the theorem. Let s be any point in the plane, and let S be the set of points which are the images of s under the various motions in G. So each element $s' \in S$ has the form $s' = g(s)$ for some $g \in G$. This set is called the *orbit* of s under the action of G. The element s is in the orbit because the identity element 1 is in G, and $s = 1(s)$. A typical orbit is depicted below, for the case that G is the group of symmetries of a regular pentagon.



Any element of the group G will permute the orbit S. In other words, if $s' \in S$ and $x \in G$, then $x(s') \in S$. For, say that $s' = g(s)$, with $g \in G$. Since G is a group, $xg \in G$. Therefore, by definition, $xg(s) \in S$. Since $xg(s) = x(s')$, this shows that $x(s') \in S$.

We list the elements of S arbitrarily, writing $S = \{s_1, \ldots, s_n\}$. The fixed point we are looking for is the *center of gravity* of the orbit, defined as

$$p = \tfrac{1}{n}(s_1 + \cdots + s_n), \tag{3.2}$$

where the right side is computed by vector addition, using an arbitrary coordinate system in the plane. The center of gravity should be considered an *average* of the points $s_1, \ldots, s_n$.

(3.3) **Lemma.** Let $S = \{s_1, \ldots, s_n\}$ be a finite set of points of the plane, and let p be its center of gravity, defined by (3.2). Let m be a rigid motion, and let $m(s_i) = s_i'$ and $m(p) = p'$. Then $p' = \frac{1}{n}(s_1' + \cdots + s_n')$. In other words, rigid motions carry centers of gravity to centers of gravity.

Proof. This is clear by physical reasoning. It can also be shown by calculation. To do so, it suffices to treat separately the cases $m = t_a$, $m = \rho_\theta$, and $m = r$, since any motion is obtained from these by composition.

Case 1: $m = t_a$. Then $p' = p + a$ and $s_i' = s_i + a$. It is true that

$$p + a = \tfrac{1}{n}((s_1 + a) + \cdots + (s_n + a)).$$

Case 2: $m = \rho_\theta$ or r. Then m is a linear operator. Therefore

$$p' = m(\tfrac{1}{n}(s_1 + \cdots + s_n)) = \tfrac{1}{n}(m(s_1) + \cdots + m(s_n)) = \tfrac{1}{n}(s_1' + \cdots + s_n'). \qquad \square$$

The center of gravity of our set S is a fixed point for the action of G. For, any element g_i of G permutes the orbit $\{s_1,\ldots,s_n\}$, so Lemma (3.3) shows that it sends the center of gravity to itself. This completes the proof of the theorem. □

Now let G be a finite subgroup of M. Theorem (3.1) tells us that there is a point fixed by every element of G, and we may adjust coordinates so that this point is the origin. Then G will be a subgroup of $\mathbf{O}$. So to describe the finite subgroups G of M, we need only describe the finite subgroups of $\mathbf{O}$ (or, since $\mathbf{O}$ is isomorphic to the group of orthogonal 2×2 matrices, the finite subgroups of the orthogonal group O_2). These subgroups are described in the following theorem.

(3.4) **Theorem.** Let G be a finite subgroup of the group $\mathbf{O}$ of rigid motions which fix the origin. Then G is one of the following groups:

(a) $G = C_n$: the *cyclic group* of order n, generated by the rotation ρ_θ, where $\theta = 2\pi/n$.

(b) $G = D_n$: the *dihedral group* of order $2n$, generated by two elements—the rotation ρ_θ, where $\theta = 2\pi/n$, and a reflection r' about a line through the origin.

The proof of this theorem is at the end of the section.

The group D_n depends on the line of reflection, but of course we may choose coordinates so that it becomes the x-axis, and then r' becomes our standard reflection r. If G were given as a finite subgroup of M, we would also need to shift the origin to the fixed point in order to apply Theorem (3.4). So our end result about finite groups of motions is the following corollary:

(3.5) **Corollary.** Let G be a finite subgroup of the group of motions M. If coordinates are introduced suitably, then G becomes one of the groups C_n or D_n, where C_n is generated by ρ_θ, $\theta = 2\pi/n$, and D_n is generated by ρ_θ and r. □

When $n \geq 3$, the dihedral group D_n is the group of symmetries of a regular n-sided polygon. This is easy to see, and in fact it follows from the theorem. For a regular n-gon has a group of symmetries which contains the rotation by $2\pi/n$ about its center. It also contains some reflections. Theorem (3.4) tells us that it is D_n.

The dihedral groups D_1, D_2 are too small to be symmetry groups of an n-gon in the usual sense. D_1 is the group $\{1, r\}$ of two elements. So it is a cyclic group, as is C_2. But the nontrivial element of D_1 is a reflection, while in C_2 it is rotation through the angle π. The group D_2 contains the four elements $\{1, \rho, r, \rho r\}$, where $\rho = \rho_\pi$. It is isomorphic to the Klein four group. If we like, we can think of D_1 and D_2 as groups of symmetry of the 1-gon and 2-gon:

1-gon. 2-gon.

The dihedral groups are important examples, and it will be useful to have a complete set of defining relations for them. They can be read off from the list of defining relations for M (2.5). Let us denote the rotation ρ_θ ($\theta = 2\pi/n$) by x, and the reflection r by y.

(3.6) **Proposition.** The dihedral group D_n is generated by two elements x, y which satisfy the relations

$$x^n = 1\ ,\quad y^2 = 1\ ,\quad yx = x^{-1}y.$$

The elements of D_n are

$$\{1, x, x^2, \ldots, x^{n-1}\ ; y, xy, x^2y, \ldots, x^{n-1}y\} = \{x^iy^j \mid 0 \le i < n,\quad 0 \le j < 2\}\ .$$

Proof. The elements $x = \rho_\theta$ and $y = r$ generate D_n by definition of the group. The relations $y^2 = 1$ and $yx = x^{-1}y$ are included in the list of relations (2.5) for M: They are $rr = 1$ and $r\rho_\theta = \rho_{-\theta}r$. The relation $x^n = 1$ follows from the fact that $\theta = 2\pi/n$, which also shows that the elements $1, x, \ldots, x^{n-1}$ are distinct. It follows that the elements $y, xy, x^2y, \ldots, x^{n-1}y$ are also distinct and, since they are reflections while the powers of x are rotations, that there is no repetition in the list of elements. Finally, the relations can be used to reduce any product of x, y, x^{-1}, y^{-1} to the form x^iy^j , with $0 \le i < n$, $0 \le j < 2$. Therefore the list contains all elements of the group generated by x,y , and since these elements generate D_n the list is complete. □

Using the first two relations (3.6), the third relation can be written in various ways. It is equivalent to

(3.7) $$yx = x^{n-1}y \text{ and also to } xyxy = 1.$$

Note that when $n = 3$, the relations are the same as for the symmetric group S_3 [Chapter 2(1.18)].

(3.8) **Corollary.** The dihedral group D_3 and the symmetric group S_3 are isomorphic. □

For $n > 3$, the dihedral and symmetric groups are certainly not isomorphic, because D_n has order $2n$, while S_n has order $n!$.

Proof of Theorem (3.4). Let G be a finite subgroup of $\mathbf{O}$. We need to remember that the elements of $\mathbf{O}$ are the rotations ρ_θ and the reflections $\rho_\theta r$.

Case 1: All elements of G are rotations. We must prove that G is cyclic in this case. The proof is similar to the determination of the subgroups of the additive group $\mathbb{Z}^+$ of integers [Chapter 2 (2.3)]. If $G = \{1\}$, then $G = C_1$. Otherwise G contains a nontrivial rotation ρ_θ. Let θ be the smallest positive angle of rotation among the elements of G. Then G is generated by ρ_θ. For let ρ_α be any element of G, where the angle of rotation α is represented as usual by a real number. Let $n\theta$ be the greatest integer multiple of θ which is less than α, so that $\alpha = n\theta + \beta$, with $0 \le \beta < \theta$. Since G is a group and since ρ_α and ρ_θ are in G, the product $\rho_\beta = \rho_\alpha\rho_{-n\theta}$ is also in

G. But by assumption θ is the smallest positive angle of rotation in G. Therefore $\beta = 0$ and $\alpha = n\theta$. This shows that G is cyclic. Let $n\theta$ be the smallest multiple of θ which is $\geq 2\pi$, so that $2\pi \leq n\theta < 2\pi + \theta$. Since θ is the smallest positive angle of rotation in G, $n\theta = 2\pi$. Thus $\theta = 2\pi/n$ for some integer n.

Case 2: G contains a reflection. Adjusting coordinates as necessary, we may assume that our standard reflection r is in G. Let H denote the subgroup of rotations in G. We can apply what has been proved in Case 1 to the group H, to conclude that it is a cyclic group: $H = C_n$. Then the $2n$ products $\rho_\theta{}^i$, $\rho_\theta{}^i r$, $0 \leq i \leq n - 1$, are in G, and so G contains the dihedral group D_n. We must show that $G = D_n$. Now if an element g of G is a rotation, then $g \in H$ by definition of H; hence g is one of the elements of D_n. If g is a reflection, we can write it in the form $\rho_\alpha r$ for some rotation ρ_α (2.8). Since r is in G, so is the product $\rho_\alpha r r = \rho_\alpha$. Therefore ρ_α is a power of ρ_θ, and g is in D_n too. So $G = D_n$. This completes the proof of the theorem. □

4. DISCRETE GROUPS OF MOTIONS

In this section we will discuss the symmetry groups of unbounded figures such as wallpaper patterns. Our first task is to describe a substitute for the condition that the group is finite—one which includes the groups of symmetry of interesting unbounded figures. Now one property which the patterns illustrated in the text have is that they do not admit arbitrarily small translations or rotations. Very special figures such as a line have arbitrarily small translational symmetries, and a circle, for example, has arbitrarily small rotational symmetries. It turns out that if such figures are ruled out, then the groups of symmetry can be classified.

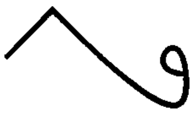
(4.1) **Definition.** A subgroup G of the group of motions M is called *discrete* if it does not contain arbitrarily small translations or rotations. More precisely, G is discrete if there is some real number $\epsilon > 0$ so that

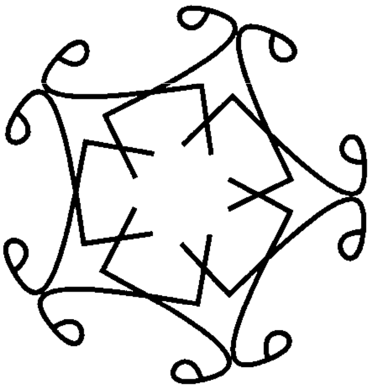
(i) if t_a is a translation in G by a nonzero vector a, then the length of a is at least ϵ: $|a| \geq \epsilon$;

(ii) if ρ is a rotation in G about some point through a nonzero angle θ, then the angle θ is at least ϵ: $|\theta| \geq \epsilon$.

Since the translations and rotations are all the orientation-preserving motions (2.1), this condition applies to all orientation-preserving elements of G. We do not impose a condition on the reflections and glides. The one we might ask for follows automatically from the condition imposed on orientation-preserving motions.

The kaleidoscope principle can be used to show that every discrete group of motions is the group of symmetries of a plane figure. We are not going to give precise reasoning to show this, but the method can be made into a proof. Start with a sufficiently random figure R in the plane. We require in particular that R shall not have any symmetries except for the identity. So every element g of our group will move R to a different position, call it gR. The required figure F is the union of all the figures gR. An element x of G sends gR to xgR, which is also a part of F, and hence it sends F to itself. If R is sufficiently random, G will be its group of symmetries. As we know from the kaleidoscope, the figure F is often very attractive. Here is the result of applying this procedure in the case that G is the dihedral group of symmetries of a regular pentagon:





Of course many figures have the same group or have similar groups of symmetry. But nevertheless it is interesting and instructive to classify figures according to their groups of symmetry. We are going to discuss a rough classification of the groups, which will be refined in the exercises.

The two main tools for studying a discrete group G are its translation group and its point group. The *translation group* of G is the set of vectors a such that $t_a \in G$. Since $t_a t_b = t_{a+b}$ and $t_{-a} = t_a{}^{-1}$, this is a subgroup of the additive group of vectors, which we will denote by L_G. Using our choice of coordinates, we identify the space of vectors with $\mathbb{R}^2$. Then

$$(4.2) \qquad L_G = \{a \in \mathbb{R}^2 \mid t_a \in G\}.$$

This group is isomorphic to the subgroup $T \cap G$ of translations in G, by the isomorphism (2.10): $a \rightsquigarrow t_a$. Since it is a subgroup of G, $T \cap G$ is discrete: A subgroup of a discrete group is discrete. If we translate this condition over to L_G, we find

(4.3) *L_G contains no vector of length $< \epsilon$, except for the zero vector.*

A subgroup L of $\mathbb{R}^{n+}$ which satisfies condition (4.3) for some $\epsilon > 0$ is called a *discrete* subgroup of $\mathbb{R}^n$. Here the adjective *discrete* means that the elements of L are separated by a fixed distance:

(4.4) *The distance between any two vectors $a, b \in L$ is at least ϵ, if $a \neq b$.*

For the distance is the length of $b - a$, and $b - a \in L$ because L is a subgroup.

(4.5) **Proposition.** Every discrete subgroup L of $\mathbb{R}^2$ has one of these forms:

(a) $L = \{0\}$.

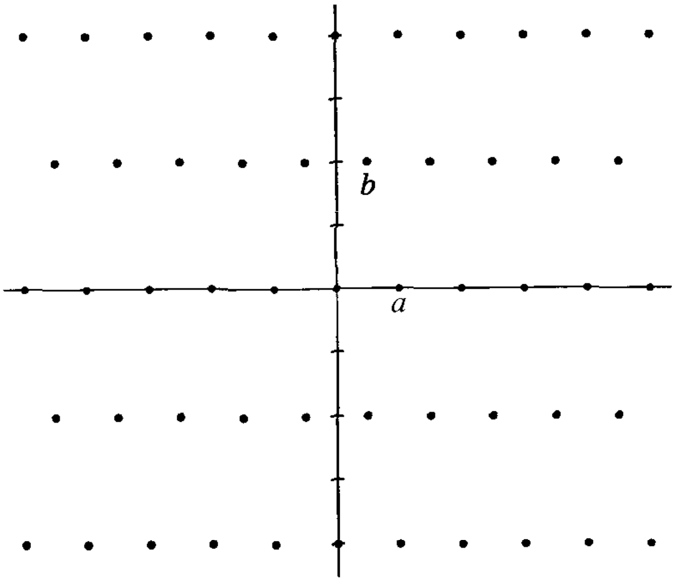
(b) L is generated as an additive group by one nonzero vector a:

$$L = \{ma \mid m \in \mathbb{Z}\}.$$

(c) L is generated by two linearly independent vectors a, b:

$$L = \{ma + nb \mid m,n \in \mathbb{Z}\}.$$

Groups of the third type are called *plane lattices,* and the generating set (a, b) is called a *lattice basis.*



(4.6) **Figure.** A lattice in $\mathbb{R}^2$.

We defer the proof of Proposition (4.5) and turn to the second tool for studying a discrete group of motions—its point group. Recall that there is a homomorphism (2.13) φ: $M \longrightarrow \text{O}$, whose kernel is T. If we restrict this homomorphism to G, we obtain a homomorphism

$$\varphi|_G\colon G \longrightarrow \text{O}. \tag{4.7}$$

Its kernel is $T \cap G$ (which is a subgroup isomorphic to the translation group L_G). The *point group* $\overline{G}$ is the image of G in O. Thus $\overline{G}$ is a subgroup of O.

By definition, a rotation ρ_θ is in $\overline{G}$ if G contains some element of the form $t_a\rho_\theta$. And we have seen (2.8) that $t_a\rho_\theta$ is a rotation through the angle θ about some point in the plane. So the inverse image of an element $\rho_\theta \in \overline{G}$ consists of all of the elements of G which are rotations through the angle θ about some point.

Similarly, let ℓ denote the line of reflection of $\rho_\theta r$. As we have noted before, its angle with the x-axis is $\frac{1}{2}\theta$. The point group $\overline{G}$ contains $\rho_\theta r$ if there is some element $t_a\rho_\theta r$ in G, and $t_a\rho_\theta r$ is a reflection or a glide reflection along a line parallel to ℓ. So the inverse image of $\rho_\theta r$ consists of all elements of G which are reflections and glides along lines parallel to ℓ.

Since G contains no small rotations, the same is true of its point group $\overline{G}$. So $\overline{G}$ is discrete too—it is a discrete subgroup of O.

(4.8) **Proposition.** A discrete subgroup of $\mathbf{O}$ is a finite group.

We leave the proof of this proposition as an exercise. □

Combining Proposition (4.8) with Theorem (3.4), we find the following:

(4.9) **Corollary.** The point group $\overline{G}$ of a discrete group G is cyclic or dihedral. □

Here is the key observation which relates the point group to the translation group:

(4.10) **Proposition.** Let G be a discrete subgroup of M, with translation group $L = L_G$ and point group $\overline{G}$. The elements of $\overline{G}$ carry the group L to itself. In other words, if $\overline{g} \in \overline{G}$ and $a \in L$, then $\overline{g}(a) \in L$.

We may restate this proposition by saying that $\overline{G}$ is contained in the group of symmetries of L, when L is regarded as a set of points in the plane $\mathbb{R}^2$. However, it is important to note that the original group G need not operate on L.

Proof. To say that $a \in L$ means that $t_a \in G$. So we have to show that if $t_a \in G$ and $\overline{g} \in \overline{G}$, then $t_{\overline{g}(a)} \in G$. Now by definition of the point group, $\overline{g}$ is the image of some element g of the group G: $\varphi(g) = \overline{g}$. We will prove the proposition by showing that $t_{\overline{g}(a)}$ is the conjugate of t_a by g. We write $g = t_b\rho$ or $t_b\rho r$, where $\rho = \rho_\theta$. Then $\overline{g} = \rho$ or ρr, according to the case. In the first case,

$$gt_ag^{-1} = t_b\rho t_a\rho^{-1}t_{-b} = t_bt_{\rho(a)}\rho\rho^{-1}t_{-b} = t_{\rho(a)},$$

as required. The computation is similar in the other case. □

The following proposition describes the point groups which can arise when the translation group L_G is a lattice.

(4.11) **Proposition.** Let $H \subset \mathbf{O}$ be a finite subgroup of the group of symmetries of a lattice L. Then

(a) Every rotation in H has order 1, 2, 3, 4, or 6.

(b) H is one of the groups C_n, D_n where $n = 1, 2, 3, 4,$ or 6.

This proposition is often referred to as the *Crystallographic Restriction*. Notice that a rotation of order 5 is ruled out by (4.11). There is no wallpaper pattern with fivefold rotational symmetry. (However, there do exist "quasi-periodic" patterns with fivefold symmetry.)

To prove Propositions (4.5) and (4.11), we begin by noting the following simple lemma:

(4.12) **Lemma.** Let L be a discrete subgroup of $\mathbb{R}^2$.

(a) A bounded subset S of $\mathbb{R}^2$ contains only finitely many elements of L.

(b) If $L \neq \{0\}$, then L contains a nonzero vector of minimal length.

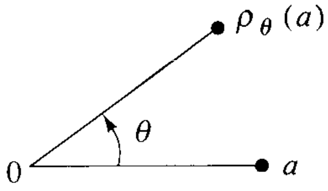
Proof.

(a) Recall that a subset S of $\mathbb{R}^n$ is called bounded if it is contained in some large box, or if the points of S do not have arbitrarily large coordinates. Obviously, if S is bounded, so is $L \cap S$. Now a bounded set which is infinite must contain some elements arbitrarily close to each other—that is, the elements can not be separated by a fixed positive distance ϵ. This is not the case for L, by (4.4). Thus $L \cap S$ is finite.

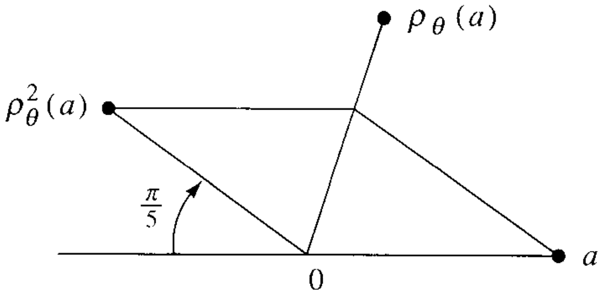
(b) When we say that a nonzero vector a has minimal length, we mean that every nonzero vector $v \in L$ has length at least $|a|$. We don't require the vector a to be uniquely determined. In fact we couldn't require this, because whenever a has minimal length, $-a$ does too.

Assume that $L \neq \{0\}$. To prove that a vector of minimal length exists, we let $b \in L$ be any nonzero vector, and let S be the disc of radius $|b|$ about the origin. This disc is a bounded set, so it contains finitely many elements of L, including b. We search through the nonzero vectors in this finite set to find one having minimal length. It will be the required shortest vector. □

Proof of Proposition (4.11). The second part of the proposition follows from the first, by (3.6). To prove (a), let θ be the smallest nonzero angle of rotation in H, and let a be a nonzero vector in L of minimal length. Then since H operates on L, $\rho_\theta(a)$ is also in L; hence $b = \rho_\theta(a) - a \in L$. Since a has a minimal length, $|b| \geq |a|$. It follows that $\theta \geq 2\pi/6$.



Thus ρ_θ has order ≤ 6. The case that $\theta = 2\pi/5$ is also ruled out, because then the element $b' = \rho_\theta{}^2(a) + a$ is shorter than a:

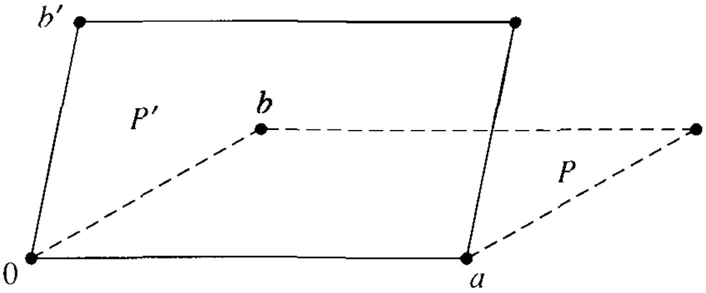


This completes the proof. □

Proof of Proposition (4.5). Let L be a discrete subgroup of $\mathbb{R}^2$. The possibility that $L = \{0\}$ is included in the list. If $L \neq \{0\}$, there is a nonzero vector $a \in L$, and we have two possibilities:

Case 1: All vectors in L lie on one line ℓ through the origin. We repeat an argument used several times before, choosing a nonzero vector $a \in L$ of minimal length. We claim that L is generated by a. Let v be any element of L. Then it is a real multiple $v = ra$ of a, since $L \subset \ell$. Take out the integer part of r, writing $r = n + r_0$, where n is an integer and $0 \leq r_0 < 1$. Then $v - na = r_0 a$ has length less than a, and since L is a group this element is in L. Therefore $r_0 = 0$. This shows that v is an integer multiple of a, and hence that it is in the subgroup generated by a, as required.

Case 2: The elements of L do not lie on a line. Then L contains two linearly independent vectors a', b'. We start with an arbitrary pair of independent vectors, and we try to replace them by vectors which will generate the group L. To begin with, we replace a' by a shortest nonzero vector a on the line ℓ which a' spans. When this is done, the discussion of Case 1 shows that the subgroup $\ell \cap L$ is generated by a. Next, consider the parallelogram P' whose vertices are $0, a, b', a + b'$:



(4.13) **Figure.**

Since P' is a bounded set, it contains only finitely many elements of L (4.12). We may search through this finite set and choose a vector b whose distance to the line ℓ is as small as possible, but positive. We replace b' by this vector. Let P be the parallelogram with $0, a, b, a + b$. We note that P contains no points of L except for its vertices. To see this, notice first that any lattice point c in P which is not a vertex must lie on one of the line segments $[b, a + b]$ or $[0, a]$. Otherwise the two points c and $c - a$ would be closer to ℓ than b, and one of these points would lie in P'. Next, the line segment $[0, a]$ is ruled out by the fact that a is a shortest vector on ℓ. Finally, if there were a point c on $[b, a + b]$, then $c - b$ would be an element of L on the segment $[0, a]$. The proof is completed by the following lemma.

(4.14) **Lemma.** Let a, b be linearly independent vectors which are elements of a subgroup L of $\mathbb{R}^2$. Suppose that the parallelogram P which they span contains no element of L other than the vertices $0, a, b, a + b$. Then L is generated by a and b, that is,

$$L = \{ma + nb \mid m, n \in \mathbb{Z}\}.$$

Proof. Let v be an arbitrary element of L. Then since (a,b) is a basis of $\mathbb{R}^2$, v is a linear combination, say $v = ra + sb$, where r,s are real numbers. We take out the integer parts of r, s, writing $r = m + r_0$, $s = n + s_0$, where m, n are integers and $0 \leq r_0, s_0 < 1$. Let $v_0 = r_0 a + s_0 b = v - ma - nb$. Then v_0 lies in the parallelogram P, and $v_0 \in L$. Hence v_0 is one of the vertices, and since r_0, $s_0 < 1$, it must be the origin. Thus $v = ma + nb$. This completes the proof of the lemma and of Proposition (4.5). □

Let L be a lattice in $\mathbb{R}^2$. An element $v \in L$ is called *primitive* if it is not an integer multiple of another vector in L. The preceding proof actually shows the following:

(4.15) **Corollary.** Let L be a lattice, and let v be a primitive element of L. There is an element $w \in L$ so that the set (v, w) is a lattice basis. □

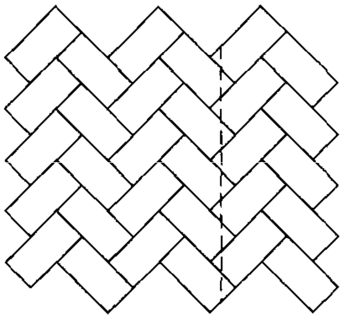
Now let us go back to our discrete group of motions $G \subset M$ and consider the rough classification of G according to the structure of its translation group L_G. If L_G is the trivial group, then the homomorphism from G to its point group is bijective and G is finite. We examined this case in Section 3.

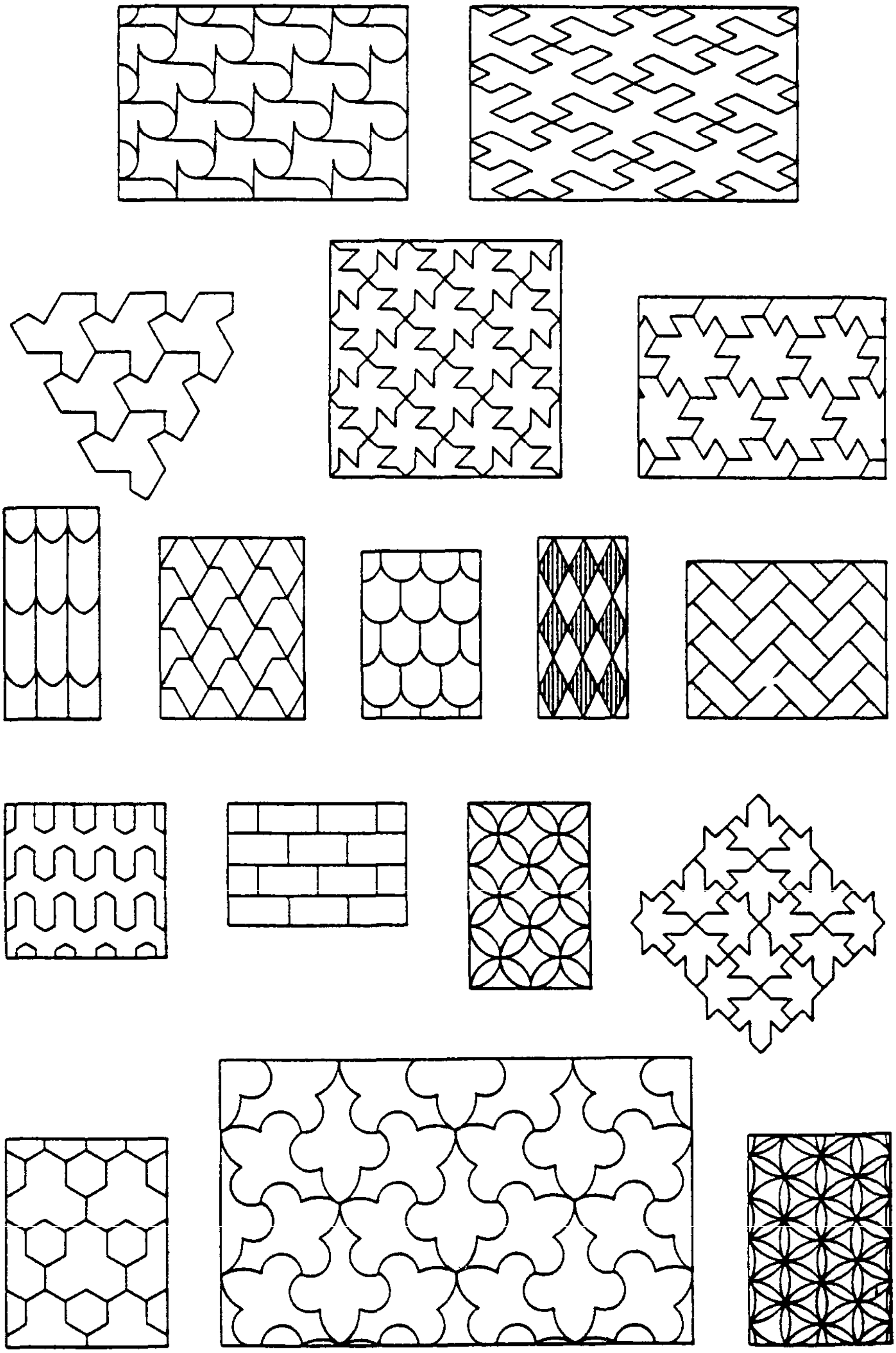
The discrete groups G such that L_G is infinite cyclic are the symmetry groups of frieze patterns such as (1.3). The classification of these groups is left as an exercise.

If L_G is a lattice, then G is called a *two-dimensional crystallographic group*, or a *lattice group*. These groups are the groups of symmetries of wallpaper patterns and of two-dimensional crystals.

The fact that any wallpaper pattern repeats itself in two different directions is reflected in the fact that its group of symmetries will always contain two independent translations, which shows that L_G is a lattice. It may also contain further elements—rotations, reflections, or glides—but the crystallographic restriction limits the possibilities and allows one to classify crystallographic groups into 17 types. The classification takes into account not only the intrinsic structure of the group, but also the type of motion that each group element represents. Representative patterns with the various types of symmetry are illustrated in Figure (4.16).

Proposition (4.11) is useful for determining the point group of a crystallographic group. For example, the brick pattern shown below has a rotational symmetry through the angle π about the centers of the bricks. All of these rotations represent the same element ρ_π of the point group $\overline{G}$. The pattern also has glide symmetry along the dotted line indicated. Therefore the point group $\overline{G}$ contains a reflection. By Proposition (4.11), $\overline{G}$ is a dihedral group. On the other hand, it is easy to see that the only nontrivial rotations in the group G of symmetries are through the angle π. Therefore $\overline{G} = D_2 = \{1, \rho_\pi, r, \rho_\pi r\}$.





(4.16) **Figure.** Sample patterns for the 17 plane crystallographic groups.

The point group $\overline{G}$ and the translation group L_G do not completely characterize the group G. Things are complicated by the fact that a reflection in $\overline{G}$ need not be the image of a reflection in G—it may be represented in G only by glides, as in the brick pattern illustrated above.

As a sample of the methods required to classify the two-dimensional crystallographic groups, we will describe those whose point group contains a rotation ρ through the angle $\pi/2$. According to Proposition (4.11), the point group will be either C_4 or D_4. Since any element of G which represents ρ is also a rotation through $\pi/2$ about some point p, we may choose p to be the origin. Then ρ can be thought of as an element of G too.

(4.17) **Proposition.** Let G be a lattice group whose point group contains a rotation ρ through the angle $\pi/2$. Choose coordinates so that the origin is a point of rotation by $\pi/2$ in G. Let a be a shortest vector in $L = L_G$, let $b = \rho(a)$, and let $c = \frac{1}{2}(a + b)$. Denote by r the reflection about the line spanned by a. Then G is generated by one of the following sets: $\{t_a, \rho\}$, $\{t_a, \rho, r\}$, $\{t_a, \rho, t_c r\}$. Thus there are three such groups.

Proof. We first note that L is a square lattice, generated by a and b. For, a is in L by hypothesis, and Proposition (4.10) asserts that $b = \rho(a)$ is also in L. These two vectors generate a square sublattice L' of L. If $L \neq L'$, then according to Lemma (4.14) there is an element $w \in L$ in the square whose vertices are $0, a, a + b$ and which is not one of the vertices. But any such vector would be at a distance less than $|a|$ from at least one of the vertices v, and the difference $w - v$ would be in L but shorter than a, contrary to the choice of a. Thus $L = L'$, as claimed.

Now the elements t_a and ρ are in G, and $\rho t_a \rho^{-1} = t_b$ (2.5). So the subgroup H of G generated by the set $\{t_a, \rho\}$ contains t_a and t_b. Hence it contains t_w for every $w \in L$. The elements of this group are the products $t_w \rho^i$:

$$H = \{t_w \rho^i \mid w \in L, 0 \leq i \leq 3\}.$$

This is one of our groups. We now consider the possible additional elements which G may contain.

Case 1: Every element of G preserves orientation. In this case, the point group is C_4. Every element of G has the form $m = t_u \rho_\theta$, and if such an element is in G then ρ_θ is in the point group. So $\rho_\theta = \rho^i$ for some i, and $m\rho^{-i} = t_u \in G$ too. Therefore $u \in L$, and $m \in H$. So $G = H$ in this case.

Case 2: G contains an orientation-reversing motion. In this case the point group is D_4, and it contains the reflection about the line spanned by a. We choose coordinates so that this reflection becomes our standard reflection r. Then r will be represented in G by an element of the form $m = t_u r$.

Case 2a: The element u is in L; that is, $t_u \in G$. Then $r \in G$ too, so G contains its point group $\overline{G} = D_4$. If $m' = t_w \rho_\theta$ or if $t_w \rho_\theta r$ is any element of G, then $\rho_\theta r$ is in G

too; hence $t_w \in G$, and $w \in L$. Therefore G is the group generated by the set $\{t_a, \rho, r\}$.

Case 2b: The element u is not in L. This is the hard case.

(4.18) **Lemma.** Let U be the set of vectors u such that $t_u r \in G$. Then

(a) $L + U = U$.

(b) $\rho U = U$.

(c) $U + rU \subset L$.

Proof. If $v \in L$ and $u \in U$, then t_v and $t_u r$ are in G; hence $t_v t_u r = t_{v+u} r \in G$. This shows that $c + v \in U$ and proves (a). Next, suppose that $u \in U$. Then $\rho t_u r \rho = t_{\rho u} \rho r \rho = t_{\rho u} r \in G$. This shows that $\rho u \in U$ and proves (b). Finally, if $u, v \in U$, then $t_u r t_v r = t_{u+rv} \in G$; hence $u + rv \in L$, which proves (c). □

Part (a) of the lemma allows us to choose an element $u \in U$ lying in the square whose vertices are $0, a, b, a + b$ and which is not on the line segments $[a, a + b]$ and $[b, a + b]$. We write u in terms of the basis (a, b), say $u = xa + yb$, where $0 \leq x, y < 1$. Then $u + ru = 2xa$. Since $u + ru \in L$ by (4.18c), the possible values for x are $0, \frac{1}{2}$. Next, $\rho u + a = (1 - y)a + xb$ lies in the square too, and the same reasoning shows that y is 0 or $\frac{1}{2}$. Thus the three possibilities for u are $\frac{1}{2}a$, $\frac{1}{2}b$, and $\frac{1}{2}(a + b) = c$. But if $u = \frac{1}{2}a$, then $\rho u = \frac{1}{2}b$, and $ru = u = \frac{1}{2}a$. So $c = \frac{1}{2}(a + b) \in L$ (4.18b,c). This is impossible because c is shorter than a. Similarly, the case $u = \frac{1}{2}b$ is impossible. So the only remaining case is $u = c$, which means that the group G is generated by $\{t_a, \rho, t_c r\}$. □

5. *ABSTRACT SYMMETRY: GROUP OPERATIONS*

The concept of symmetry may be applied to things other than geometric figures. For example, complex conjugation $(a + bi) \rightsquigarrow (a - bi)$ may be thought of as a symmetry of the complex numbers. It is compatible with most of the structure of $\mathbb{C}$: If $\overline{\alpha}$ denotes the complex conjugate of α, then $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ and $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$. Being compatible with addition and multiplication, conjugation is called an *automorphism* of the field $\mathbb{C}$. Of course, this symmetry is just the bilateral symmetry of the complex plane about the real axis, but the statement that it is an automorphism refers to its algebraic structure.

Another example of abstract "bilateral" symmetry is given by a cyclic group H of order 3. We saw in Section 3 of Chapter 2 that this group has an automorphism φ, which interchanges the two elements different from the identity.

The set of automorphisms of a group H (or of any other mathematical structure H) forms a group $\operatorname{Aut} H$, the law of composition being composition of maps. Each automorphism should be thought of as a *symmetry* of H, in the sense that it is a permutation of the elements of H which is compatible with the structure of H. But instead of being a geometric figure with a rigid shape, the structure in this case is the group law. The group of automorphisms of the cyclic group of order 3 contains two elements: the identity map and the map φ.

So the words *automorphism* and *symmetry* are more or less synonymous, except that automorphism is used to describe a permutation of a set which preserves some algebraic structure, while symmetry often refers to a permutation which preserves a geometric structure.

These examples are special cases of a more general concept, that of an operation of a group on a set. Suppose we are given a group G and a set S. An *operation* of G on S is a rule for combining elements $g \in G$ and $s \in S$ to get an element gs of S. In other words, it is a law of composition, a map $G \times S \longrightarrow S$, which we generally write as multiplication:

$$g, s \rightsquigarrow gs.$$

This rule is required to satisfy the following axioms:

(5.1)

(a) $1s = s$ for all s (1 is the identity of G).

(b) *Associative law:* $(gg')s = g(g's)$, for all $g, g' \in G$ and $s \in S$.

A set S with an operation of G is often called a *G-set*. This should really be called a *left operation,* because elements of G multiply on the left.

Examples of this concept can be found manywhere. For example, let $G = M$ be the group of all rigid motions of the plane. Then M operates on the set of points of the plane, on the set of lines in the plane, on the set of triangles in the plane, and so on. Or let G be the cyclic group $\{1, r\}$ of order 2, with $r^2 = 1$. Then G operates on the set S of complex numbers, by the rule $r\alpha = \overline{\alpha}$. The fact that the axioms (5.1) hold in a given example is usually clear.

The reason that such a law of composition is called an operation is this: If we fix an element g of G but let $s \in S$ vary, then *left multiplication by g* defines a map from S to itself; let us denote this map by m_g. Thus

$$m_g \colon S \longrightarrow S \tag{5.2}$$

is defined by

$$m_g(s) = gs.$$

This map describes the way the element g operates on S. Note that m_g is a *permutation* of S; that is, it is bijective. For the axioms show that it has the two-sided inverse

$$m_{g^{-1}} = \textit{multiplication by } g^{-1}\text{:}$$

$m_{g^{-1}}(m_g(s)) = g^{-1}(gs) = (g^{-1}g)s = 1s = s$. Interchanging the roles of g and g^{-1} shows that $m_g(m_{g^{-1}}(s)) = s$ too.

The main thing that we can do to study a set S on which a group G operates is to decompose the set into orbits. Let s be an element of S. The *orbit* of s in S is the set

$$O_s = \{s' \in S \mid s' \in gs \text{ for some } g \in G\}. \tag{5.3}$$

It is a subset of S. (The orbit is often written as $Gs = \{gs \mid g \in G\}$, in analogy with the notation for cosets [Chapter 2 (6.1)]. We won't do this because Gs looks too much like the notation for a stabilizer which we are about to introduce.) If we think of elements of G as operating on S by permutations, then O_s is the set of images of s under the various permutations m_g. Thus, if $G = M$ is the group of motions and S is the set of triangles in the plane, the orbit O_Δ of a given triangle Δ is the set of all triangles congruent to Δ. Another example of orbit was introduced when we proved the existence of a fixed point for the operation of a finite group on the plane (3.1).

The orbits for a group action are equivalence classes for the relation

$$s \sim s' \text{ if } s' = gs \text{ for some } g \in G. \tag{5.4}$$

The proof that this is an equivalence relation is easy, so we omit it; we made a similar verification when we introduced cosets in Section 6 of Chapter 2. Being equivalence classes, the orbits partition the set S:

(5.5) *S is a union of disjoint orbits.*

The group G operates on S by operating independently on each orbit. In other words, an element $g \in G$ permutes the elements of each orbit and does not carry elements of one orbit to another orbit. For example, the set of triangles of the plane can be partitioned into congruence classes, the orbits for the action of M. A motion m permutes each congruence class separately. Note that the orbits of an element s and of gs are equal.

If S consists of just one orbit, we say that G operates *transitively* on S. This means that every element of S is carried to every other one by some element of the group. Thus the group of symmetries of Figure (1.7) operates transitively on the set of its legs. The group M of rigid motions of the plane operates transitively on the set of points of the plane, and it operates transitively on the set of lines in the plane. It does not operate transitively on the set of triangles in the plane.

The *stabilizer* of an element $s \in S$ is the subgroup G_s of G of elements leaving s fixed:

$$G_s = \{g \in G \mid gs = s\}. \tag{5.6}$$

It is clear that this is a subgroup. Just as the kernel of a group homomorphism $\varphi\colon G \longrightarrow G'$ tells us when two elements $x, y \in G$ have the same image, namely, if $x^{-1}y \in \ker \varphi$ [Chapter 2 (5.13)], we can describe when two elements $x, y \in G$ act in the same way on an element $s \in S$ in terms of the stabilizer G_s:

(5.7) $$xs = ys \textit{ if and only if } x^{-1}y \in G_s.$$

For $xs = ys$ implies $s = x^{-1}ys$, and conversely.

As an example of a nontrivial stabilizer, consider the action of the group M of rigid motions on the set of points of the plane. The stabilizer of the origin is the subgroup O of orthogonal operators.

Or, if S is the set of triangles in the plane and Δ is a particular triangle which happens to be equilateral, then the stabilizer of Δ is its group of symmetries, a subgroup of M isomorphic to D_3 (see (3.4)). Note that when we say that a motion m stabilizes a triangle Δ, we don't mean that m fixes the points of Δ. The only motion which fixes every point of a triangle is the identity. We mean that in permuting the set of triangles, the motion carries Δ to itself. It is important to be clear about this distinction.

6. THE OPERATION ON COSETS

Let H be a subgroup of a group G. We saw in Section 6 of Chapter 2 that the left cosets $aH = \{ah \mid h \in H\}$ form a partition of the group [Chapter 2 (6.3)]. We will call the set of left cosets the *coset space* and will often denote it by G/H, copying this notation from that used for quotient groups when the subgroup is normal.

The fundamental observation to be made is this: Though G/H is not a group unless the subgroup H is normal, nevertheless *G operates on the coset space G/H* in a natural way. The operation is quite obvious: Let g be an element of the group, and let C be a coset. Then gC is defined to be the coset

(6.1) $$gC = \{gc \mid c \in C\}.$$

Thus if $C = aH$, then gC is the coset gaH. It is clear that the axioms (5.1) for an operation are satisfied.

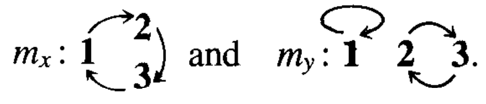
Note that the group G operates transitively on G/H, because G/H is the orbit of the coset $1H = H$. The stabilizer of the coset $1H$ is the subgroup $H \subset G$. Again, note the distinction: Multiplication by an element $h \in H$ does not act trivially on the elements of the coset $1H$, but it sends that coset to itself.

To understand the operation on cosets, you should work carefully through the following example. Let G be the group D_3 of symmetries of an equilateral triangle. As in (3.6), it may be described by generators x,y satisfying the relations $x^3 = 1$, $y^2 = 1$, $yx = x^2y$. Let $H = \{1, y\}$. This is a subgroup of order 2. Its cosets are

(6.2) $$C_1 = H = \{1, y\},\ C_2 = \{x, xy\},\ C_3 = \{x^2, x^2y\},$$

and G operates on $G/H = \{C_1, C_2, C_3\}$. So, as in (5.2), every element g of G determines a permutation m_g of $\{C_1, C_2, C_3\}$. The elements x, y operate as

(6.3)



In fact, the six elements of G yield all six permutations of three elements, and so the map

$$\begin{aligned} G &\longrightarrow S_3 \approx \operatorname{Perm}(G/H) \\ g &\rightsquigarrow m_g \end{aligned}$$

is an isomorphism. Thus the dihedral group $G = D_3$ is isomorphic to the symmetric group S_3. We already knew this.

The following proposition relates an arbitrary group operation to the operation on cosets:

(6.4) **Proposition.** Let S be a G-set, and let s be an element of S. Let H be the stabilizer of s, and let O_s be the orbit of s. There is a natural bijective map

$$G/H \xrightarrow{\varphi} O_s$$

defined by

$$aH \rightsquigarrow as.$$

This map is compatible with the operations of G in the sense that $\varphi(gC) = g\varphi(C)$· for every coset C and every element $g \in G$.

The proposition tells us that every group operation can be described in terms of the operations on cosets. For example, let $S = \{v_1, v_2, v_3\}$ be the set of vertices of an equilateral triangle, and let G be the group of its symmetries, presented as above. The element y is a reflection which stabilizes one of the vertices of the triangle, say v_1. The stabilizer of this vertex is $H = \{1, y\}$, and its orbit is S. With suitable indexing, the set (6.2) of cosets maps to S by the map $C_i \rightsquigarrow v_i$.

Proof of Proposition (6.4). It is clear the map φ, if it exists, will be compatible with the operation of the group. What is not so clear is that the rule $gH \rightsquigarrow gs$ defines a map at all. Since many symbols gH represent the same coset, we must show that if a and b are group elements and if $aH = bH$, then $as = bs$ too. This is true, because we know that $aH = bH$ if and only if $b = ah$ for some h in H [Chapter 2 (6.5)]. And when $b = ah$, then $bs = ahs = as$, because h fixes s. Next, the orbit of s consists of the elements gs, and φ carries gH to gs. Thus φ maps G/H onto O_s, and φ is surjective. Finally, we show that φ is injective. Suppose aH and bH have the same image: $as = bs$. Then $s = a^{-1}bs$. Since H was defined to be the stabilizer of s, this implies that $a^{-1}b = h \in H$. Thus $b = ah \in aH$, and so $aH = bH$. This completes the proof. □

(6.5) **Proposition.** Let S be a G-set, and let $s \in S$. Let s' be an element in the orbit of s, say $s' = as$. Then

(a) The set of elements g of G such that $gs = s'$ is the left coset

$$aG_s = \{g \in G \mid g = ah \text{ for some } h \in G_s\}.$$

(b) The stabilizer of s' is a *conjugate subgroup* of the stabilizer of s:

$$G_{s'} = aG_sa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in G_s\}.$$

We omit the proof. □

As an example, let us recompute the stabilizer of a point p in the plane, for the operation of the group of motions. We have made this computation before, in (2.11b). We have $p = t_p(0)$, and the stabilizer of the origin is the orthogonal group $\mathbf{O}$. Thus by (6.5b),

$$G_p = t_p\mathbf{O}t_p^{-1} = t_p\mathbf{O}t_{-p} = \{m \in M \mid m = t_p\rho_\theta t_{-p} \text{ or } m = t_p\rho_\theta r t_{-p}\}.$$

We know on the other hand that G_p consists of rotations and reflections about the point p. Those are the motions fixing p. So $t_p\mathbf{O}t_p^{-1}$ consists of these elements. This agrees with (2.11).

7. THE COUNTING FORMULA

Let H be a subgroup of G. As we know from Chapter 2 (6.9), all the cosets of H in G have the same number of elements: $|H| = |aH|$. Since G is a union of nonoverlapping cosets and the number of cosets is the index, which we write as $[G:H]$ or $|G/H|$, we have the fundamental formula for the order $|G|$ of the group G (see [Chapter 2 (6.10)]):

(7.1) $$|G| = |H||G/H|.$$

Now let S be a G-set. Then we can combine Proposition (6.4) with (7.1) to get the following:

(7.2) **Proposition.** *Counting Formula*: Let $s \in S$. Then

$$(\text{order of } G) = (\text{order of stabilizer})(\text{order of orbit})$$

$$|G| = |G_s||O_s|.$$

Equivalently, the order of the orbit is equal to the index of the stabilizer:

$$|O_s| = [G : G_s].$$

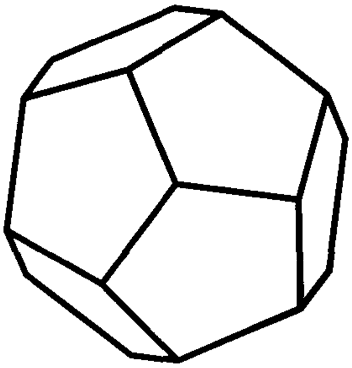
There is one such equation for every $s \in S$. As a consequence, the order of an orbit divides the order of the group.

A more elementary formula uses the partition of S into orbits to count its elements. We label the different orbits which make up S in some way, say as $O_1, \ldots, O_k$. Then

(7.3) $$|S| = |O_1| + |O_2| + \cdots + |O_k|.$$

These simple formulas have a great number of applications.

(7.4) **Example.** Consider the group G of orientation-preserving symmetries of a regular dodecahedron D. It follows from the discussion of Section 8 of Chapter 4 that these symmetries are all rotations. It is tricky to count them without error. Consider the action of G on the set S of the faces of D. The stabilizer of a face s is the group of rotations by multiples of $2\pi/5$ about a perpendicular through the center of s. So the order of G_s is 5. There are 12 faces, and G acts transitively on them. Thus $|G| = 5 \cdot 12 = 60$. Or, G operates transitively on the vertices v of D. There are three rotations, including 1, which fix a vertex, so $|G_v| = 3$. There are 20 vertices; hence $|G| = 3 \cdot 20 = 60$, which checks. There is a similar computation for edges. If e is an edge, then $|G_e| = 2$, so since $60 = 2 \cdot 30$, the dodecahedron has 30 edges.



Following our general principle, we should study restriction of an operation of a group G to a subgroup. Suppose that G operates on a set S, and let H be a subgroup of G. We may restrict the operation, to get an operation of H on S. Doing so leads to more numerical relations.

Clearly, the H-orbit of an element s will be contained in its G-orbit. So we may take a single G-orbit and decompose it into H-orbits. We count the orders of these H-orbits, obtaining another formula. For example, let S be the set of 12 faces of the dodecahedron, and let H be the stabilizer of a particular face s. Then H also fixes the face opposite to s, and so there are two H-orbits of order 1. The remaining faces make up two orbits of order 5. In this case, (7.3) reads as follows.

$$12 = 1 + 1 + 5 + 5.$$

Or let S be the set of faces, and let K be the stabilizer of a vertex. Then K does not fix any face, so every K-orbit has order 3:

$$12 = 3 + 3 + 3 + 3.$$

These relations give us a way of relating several subgroups of a group.

We close the section with a simple application of this procedure to the case that the G-set is the coset space of a subgroup:

(7.5) **Proposition.** Let H and K be subgroups of a group G. Then the index of $H \cap K$ in H is at most equal to the index of K in G:

$$[H : H \cap K] \leq [G : K].$$

Proof. To minimize confusion, let us denote the coset space G/K by S, and the coset $1K$ by s. Thus $|S| = [G : K]$. As we have already remarked, the stabilizer of s is the subgroup K. We now restrict the action of G to the subgroup H and decompose S into H-orbits. The stabilizer of s for this restricted operation is obviously $H \cap K$. We don't know much about the H-orbit O of s except that it is a subset of S. We now apply Proposition (7.2), which tells us that $|O| = [H : H \cap K]$. Therefore $[H : H \cap K] = |O| \leq |S| = [G : K]$, as required. □

8. PERMUTATION REPRESENTATIONS

By its definition, the symmetric group S_n operates on the set $S = \{\mathbf{1},\ldots,\mathbf{n}\}$. A *permutation representation* of a group G is a homomorphism

$$\varphi: G \longrightarrow S_n. \tag{8.1}$$

Given any such representation, we obtain an operation of G on $S = \{\mathbf{1},\ldots,\mathbf{n}\}$ by letting m_g (5.2) be the permutation $\varphi(g)$. In fact, operations of a group G on $\{\mathbf{1},\ldots,\mathbf{n}\}$ correspond in a bijective way to permutation representations.

More generally, let S be any set, and denote by Perm(S) the group of its permutations. Let G be a group.

(8.2) **Proposition.** There is a bijective correspondence

$$\begin{bmatrix}\text{operations}\\ \text{of } G \text{ on } S\end{bmatrix} \longleftrightarrow \begin{bmatrix}\text{homomorphisms}\\ G \longrightarrow \text{Perm}(S)\end{bmatrix}$$

defined in this way: Given an operation, we define $\varphi: G \longrightarrow \text{Perm}(S)$ by the rule $\varphi(g) = m_g$, where m_g is multiplication by g (5.2).

Let us show that φ is a homomorphism, leaving the rest of the proof of (8.2) as an exercise. We've already noted in Section 5 that m_g is a permutation. So as defined above, $\varphi(g) \in \text{Perm}(S)$. The axiom for a homomorphism is $\varphi(xy) = \varphi(x)\varphi(y)$, or $m_{xy} = m_x m_y$, where multiplication is composition of permutations. So we have to show that $m_{xy}(s) = m_x(m_y(s))$ for every $s \in S$. By Definition (5.2), $m_{xy}(s) = (xy)s$ and $m_x(m_y(s)) = x(ys)$. The associative law (5.1b) for group operations shows that $(xy)s = x(ys)$, as required. □

The isomorphism $D_3 \longrightarrow S_3$ obtained in Section 6 by the action of D_3 on the cosets of H (6.2) is a particular example of a permutation representation. But a homomorphism need not be injective or surjective. If $\varphi: G \longrightarrow \text{Perm}(S)$ happens to be injective, we say that the corresponding operation is *faithful*. So to be faithful, the operation must have the property that $m_g \neq$ identity, unless $g = 1$, or

$$\textit{if } gs = s \textit{ for every } s \in S, \textit{ then } g = 1.$$

The operation of the group of motions M on the set S of equilateral triangles in the plane is faithful, because the identity is the only motion which fixes *all* triangles.

The rest of this section contains a few applications of permutation representations.

(8.3) **Proposition.** The group $GL_2(\mathbb{F}_2)$ of invertible matrices with mod 2 coefficients is isomorphic to the symmetric group S_3.

Proof. Let us denote the field $\mathbb{F}_2$ by F, and the group $GL_2(\mathbb{F}_2)$ by G. We have listed the six elements of G before [Chapter 3 (2.10)]. Let $V = F^2$ be the space of column vectors. This space consists of the following four vectors: $V = \{0, e_1, e_2, e_1 + e_2\}$. The group G operates on V and fixes 0, so it operates on the set of three nonzero vectors, which form one orbit. This gives us a permutation representation $\varphi \colon G \longrightarrow S_3$. Now the image of e_1 under multiplication by a matrix $P \in G$ is the first column of P, and similarly the image of e_2 is the second column of P. Therefore P can not operate trivially on these two elements unless it is the identity. This shows that the operation of G is faithful, and hence that the map φ is injective. Since both groups have order 6, φ is an isomorphism. □

(8.4) **Proposition.** Let c_g denote conjugation by g, the map $c_g(x) = gxg^{-1}$. The map $f \colon S_3 \longrightarrow \text{Aut}(S_3)$ from the symmetric group to its group of automorphisms which is defined by the rule $g \rightsquigarrow c_g$ is bijective.

Proof. Let A denote the group of automorphisms of S_3. We know from Chapter 2 (3.4) that c_g is an automorphism. Also, $c_{gh} = c_g c_h$ because $c_{gh}(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = c_g(c_h(x))$ for all x. This shows that f is a homomorphism. Now conjugation by g is the identity if and only if g is in the center of the group. The center of S_3 is trivial, so f is injective.

It is to prove surjectivity of f that we look at a permutation representation of A. The group A operates on the set S_3 in the obvious way; namely, if α is an automorphism and $s \in S_3$, then $\alpha s = \alpha(s)$. Elements of S_3 of different orders will be in distinct orbits for this operation. So A operates on the subset of S_3 of elements of order 2. This set contains the three elements $\{y, xy, x^2y\}$. If an automorphism α fixes both xy and y, then it also fixes their product $xyy = x$. Since x and y generate S_3, the only such automorphism is the identity. This shows that the operation of A on $\{y, xy, x^2y\}$ is faithful and that the associated permutation representation $A \longrightarrow \text{Perm}\{y, xy, x^2y\}$ is injective. So the order of A is at most 6. Since f is injective and the order of S_3 is 6, it follows that f is bijective. □

(8.5) **Proposition.** The group of automorphisms of the cyclic group of order p is isomorphic to the multiplicative group $\mathbb{F}_p^{\times}$ of nonzero elements of $\mathbb{F}_p$.

Proof. The method here is to use the additive group $\mathbb{F}_p^{+}$ as the model for a cyclic group of order p. It is generated by the element 1. Let us denote the multiplicative group $\mathbb{F}_p^{\times}$ by G. Then G operates on $\mathbb{F}_p^{+}$ by left multiplication, and this operation defines an injective homomorphism $\varphi \colon G \longrightarrow \text{Perm}(\mathbb{F}_p)$ to the group of permutations of the set $\mathbb{F}_p$ of p elements.

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 $\varphi\colon G \longrightarrow \mathrm{Perm}(\mathbb{F}_p{}^+)$ 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:

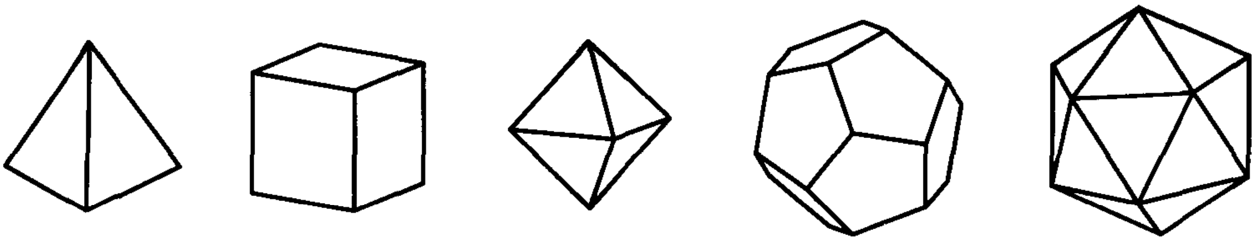
C_k: the *cyclic group* of rotations by multiples of $2\pi/k$ about a line;

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;

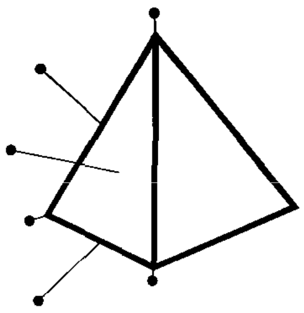
O: the *octahedral group* of order 24 of rotations of a cube, or of a regular octahedron;

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

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

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 $\mathbf{O}$ 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.

11. (a) Compute the eigenvalues and eigenvectors of the linear operator $m = \rho_\theta r$.

(b) Prove algebraically that m is a reflection about a line through the origin, which subtends an angle of $\frac{1}{2}\theta$ with the x-axis.

(c) Do the same thing as in (b) geometrically.

12. Compute the glide vector of the glide $t_a \rho_\theta r$ in terms of a and θ.

13. (a) Let m be a glide reflection along a line ℓ. Prove geometrically that a point x lies on ℓ if and only if x, $m(x)$, $m^2(x)$ are colinear.

(b) Conversely, prove that if m is an orientation-reversing motion and x is a point such that x, $m(x)$, $m^2(x)$ are distinct points on a line ℓ, then m is a glide reflection along ℓ.

14. Find an isomorphism from the group SM to the subgroup of $GL_2(\mathbb{C})$ of matrices of the form $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$, with $|a| = 1$.

15. (a) Write the formulas for the motions (2.3) in terms of the complex variable $z = x + iy$.

(b) Show that every motion has the form $m(z) = \alpha z + \beta$ or $m(z) = \alpha \bar{z} + \beta$, where $|\alpha| = 1$ and β is an arbitrary complex number.

3. Finite Groups of Motions

1. Let D_n denote the dihedral group (3.6). Express the product $x^2yx^{-1}y^{-1}x^3y^3$ in the form x^iy^j in D_n.

2. List all subgroups of the group D_4, and determine which are normal.

3. Find all proper normal subgroups and identify the quotient groups of the groups D_{13} and D_{15}.

4. (a) Compute the cosets of the subgroup $H = \{1, x^5\}$ in the dihedral group D_{10} explicitly.

(b) Prove that D_{10}/H is isomorphic to D_5.

(c) Is D_{10} isomorphic to $D_5 \times H$?

5. List the subgroups of $G = D_6$ which do not contain $N = \{1, x^3\}$.

6. Prove that every finite subgroup of M is a conjugate subgroup of one of the standard subgroups listed in Corollary (3.5).

4. Discrete Groups of Motions

1. Prove that a discrete group G consisting of rotations about the origin is cyclic and is generated by ρ_θ where θ is the smallest angle of rotation in G.

2. Let G be a subgroup of M which contains rotations about two different points. Prove algebraically that G contains a translation.

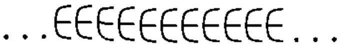
3. Let (a, b) be a lattice basis of a lattice L in $\mathbb{R}^2$. Prove that every other lattice basis has the form $(a', b') = (a, b)P$, where P is a 2×2 integer matrix whose determinant is ± 1.

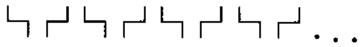
4. Determine the point group for each of the patterns depicted in Figure (4.16).

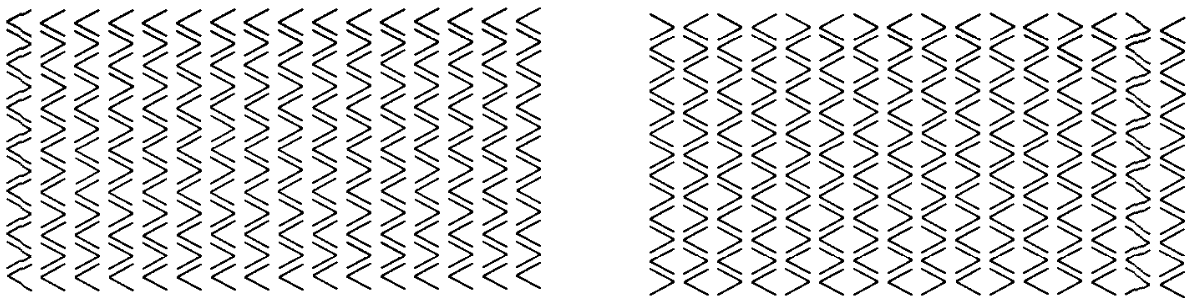
5. (a) Let B be a square of side length a, and let $\epsilon > 0$. Let S be a subset of B such that the distance between any two points of S is $\geq \epsilon$. Find an explicit upper bound for the number of elements in S.

(b) Do the same thing for a box B in $\mathbb{R}^n$.

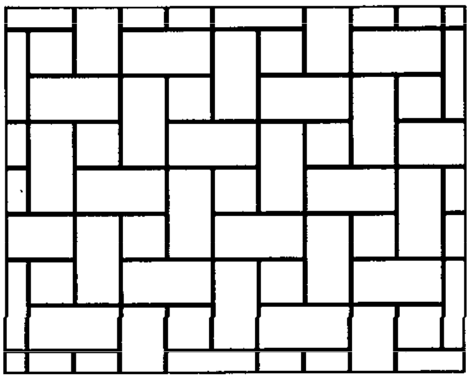
6. Prove that the subgroup of $\mathbb{R}^+$ generated by 1 and $\sqrt{2}$ is dense in $\mathbb{R}^+$.
7. Prove that every discrete subgroup of $\mathbf{O}$ is finite.
8. Let G be a discrete subgroup of M. Prove that there is a point p_0 in the plane which is not fixed by any point of G except the identity.
9. Prove that the group of symmetries of the frieze pattern

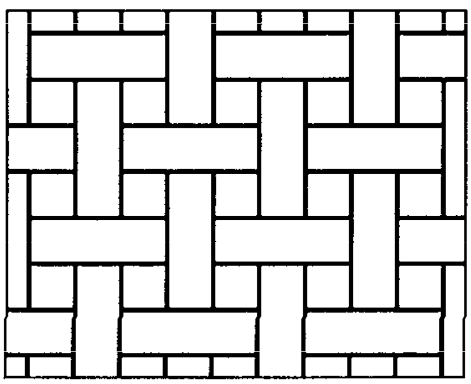


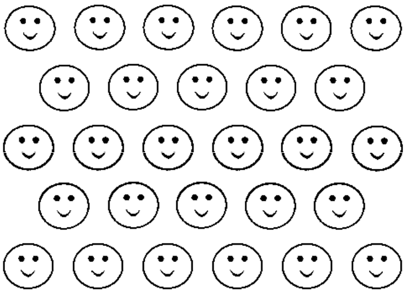
is isomorphic to the direct product $C_2 \times C_\infty$ of a cyclic group of order 2 and an infinite cyclic group.
10. Let G be the group of symmetries of the frieze pattern 
   (a) Determine the point group $\overline{G}$ of G.
   (b) For each element $\overline{g} \in \overline{G}$, and each element $g \in G$ which represents $\overline{g}$, describe the action of g geometrically.
   (c) Let H be the subgroup of translations in G. Determine $[G:H]$.
11. Let G be the group of symmetries of the pattern

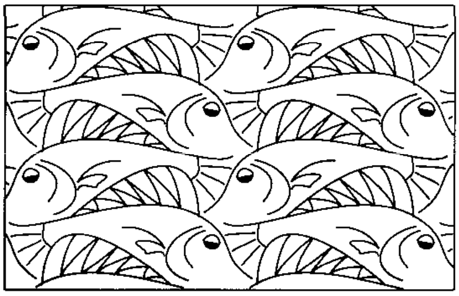


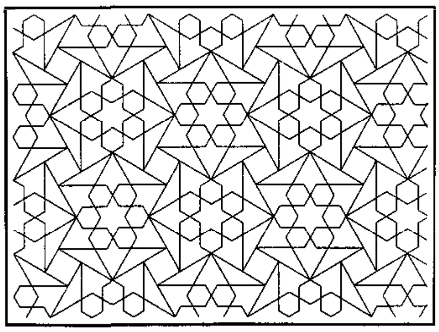
Determine the point group of G.
12. Let G be the group of symmetries of an equilateral triangular lattice L. Find the index in G of the subgroup $T \cap G$.
13. Let G be a discrete group in which every element is orientation-preserving. Prove that the point group $\overline{G}$ is a cyclic group of rotations and that there is a point p in the plane such that the set of group elements which fix p is isomorphic to $\overline{G}$.
14. With each of the patterns shown, find a pattern with the same type of symmetry in (4.16).

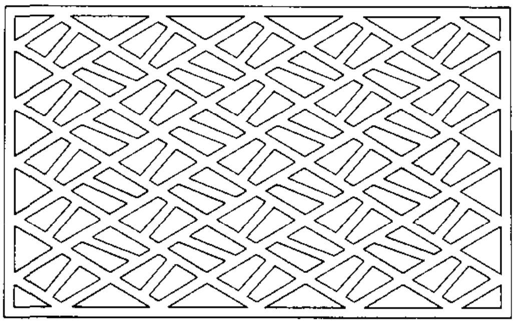












15. Let N denote the group of rigid motions of the line $\ell = \mathbb{R}^1$. Some elements of N are

$$t_a\colon \longrightarrow x + a, \quad a \in \mathbb{R}, \quad s\colon x \longrightarrow -x.$$

(a) Show that $\{t_a, t_a s\}$ are all of the elements of N, and describe their actions on ℓ geometrically.

(b) Compute the products $t_a t_b, s t_a, ss$.

(c) Find all discrete subgroups of N which contain a translation. It will be convenient to choose your origin and unit length with reference to the particular subgroup. Prove that your list is complete.

***16.** Let N' be the group of motions of an infinite ribbon

$$R = \{(x,y) \mid -1 \leq y \leq 1\}.$$

It can be viewed as a subgroup of the group M. The following elements are in N':

$$\begin{aligned} t_a\colon (x,y) &\longrightarrow (x + a, y) \\ s\colon (x,y) &\longrightarrow (-x, y) \\ r\colon (x,y) &\longrightarrow (x, -y) \\ \rho\colon (x,y) &\longrightarrow (-x, -y). \end{aligned}$$

(a) Show that these elements generate N', and describe the elements of N' as products.

(b) State and prove analogues of (2.5) for these motions.

(c) A frieze pattern is any pattern on the ribbon which is periodic and not degenerate, in the sense that its group of symmetries is discrete. Since it is periodic, its group of symmetries will contain a translation. Some sample patterns are depicted in the text (1.3, 1.4, 1.6, 1.7). Classify the symmetry groups which arise, identifying those which differ only in the choice of origin and unit length on the ribbon. I suggest that you begin by trying to make patterns with different kinds of symmetry. Please make a careful case analysis when proving your results. A suitable format would be as follows: Let G be a discrete subgroup containing a translation.

Case 1: Every element of G is a translation. Then ...,

Case 2: G contains the rotation ρ but no orientation-reversing symmetry. Then ..., and so on.

***17.** Let L be a lattice of $\mathbb{R}^2$, and let a, b be linearly independent vectors lying in L. Show that the subgroup $L' = \{ma + nb \mid m, n \in \mathbb{Z}\}$ of L generated by a, b has finite index, and that the index is the number of lattice points in the parallelogram whose vertices are $0, a, b, a + b$ and which are not on the "far edges" $[a, a + b]$ and $[b, a + b]$. (So, 0 is included, and so are points which lie on the edges $[0, a]$, $[0, b]$, except for the points a, b themselves.)

18. (a) Find a subset F of the plane which is not fixed by any motion $m \in M$.
(b) Let G be a discrete group of motions. Prove that the union S of all images of F by elements of G is a subset whose group of symmetries G' contains G.
(c) Show by an example that G' may be larger than G.
*(d) Prove that there exists a subset F such that $G' = G$.

***19.** Let G be a lattice group such that no element $g \neq 1$ fixes any point of the plane. Prove that G is generated by two translations, or else by one translation and one glide.

***20.** Let G be a lattice group whose point group is $D_1 = \{1, r\}$.
(a) Show that the glide lines and the lines of reflection of G are all parallel.
(b) Let $L = L_G$. Show that L contains nonzero vectors $a = (a_1, 0)^t$, $b = (0, b_2)^t$.
(c) Let a and b denote the smallest vectors of the type indicated in (b). Then either (a, b) or (a, c) is a lattice basis for L, where $c = \frac{1}{2}(a + b)$.
(d) Show that if coordinates in the plane are chosen so that the x–axis is a glide line, then G contains one of the elements $g = r$ or $g = t_{\frac{1}{2}a}r$. In either case, show that $G = L \cup Lg$.
(e) There are four possibilities described by the dichotomies (c) and (d). Show that there are only three different kinds of group.

21. Prove that if the point group of a lattice group G is C_6, then $L = L_G$ is an equilateral triangular lattice, and G is the group of all rotational symmetries of L about the origin.

22. Prove that if the point group of a lattice group G is D_6, then $L = L_G$ is an equilateral triangular lattice, and G is the group of all symmetries of L.

***23.** Prove that symmetry groups of the figures in Figure (4.16) exhaust the possibilities.

5. Abstract Symmetry: Group Operations

1. Determine the group of automorphisms of the following groups.
(a) C_4 (b) C_6 (c) $C_2 \times C_2$

2. Prove that (5.4) is an equivalence relation.

3. Let S be a set on which G operates. Prove that the relation $s \sim s'$ if $s' = gs$ for some $g \in G$ is an equivalence relation.

4. Let φ: $G \longrightarrow G'$ be a homomorphism, and let S be a set on which G' operates. Show how to define an operation of G on S, using the homomorphism φ.

5. Let $G = D_4$ be the dihedral group of symmetries of the square.
   (a) What is the stabilizer of a vertex? an edge?
   (b) G acts on the set of two elements consisting of the diagonal lines. What is the stabilizer of a diagonal?
6. In each of the figures in exercise 14 of Section 4, find the points which have nontrivial stabilizers, and identify the stabilizers.
*7. Let G be a discrete subgroup of M.
   (a) Prove that the stabilizer G_p of a point p is finite.
   (b) Prove that the orbit O_p of a point p is a discrete set, that is, that there is a number $\epsilon > 0$ so that the distance between two distinct points of the orbit is at least ϵ.
   (c) Let B, B' be two bounded regions in the plane. Prove that there are only finitely many elements $g \in G$ so that $gB \cap B'$ is nonempty.
8. Let $G = GL_n(\mathbb{R})$ operate on the set $S = \mathbb{R}^n$ by left multiplication.
   (a) Describe the decomposition of S into orbits for this operation.
   (b) What is the stabilizer of e_1?
9. Decompose the set $\mathbb{C}^{2\times 2}$ of 2×2 complex matrices for the following operations of $GL_2(\mathbb{C})$:
   (a) Left multiplication
   *(b) Conjugation
10. (a) Let $S = \mathbb{R}^{m\times n}$ be the set of real $m \times n$ matrices, and let $G = GL_m(\mathbb{R}) \times GL_n(\mathbb{R})$. Prove that the rule $(P, Q), A \rightsquigarrow PAQ^{-1}$ defines an operation of G on S.
   (b) Describe the decomposition of S into G-orbits.
   (c) Assume that $m \leq n$. What is the stabilizer of the matrix $[I \,|\, 0]$?
11. (a) Describe the orbit and the stabilizer of the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ under conjugation in $GL_n(\mathbb{R})$.
   (b) Interpreting the matrix in $GL_2(\mathbb{F}_3)$, find the order (the number of elements) of the orbit.
12. (a) Define automorphism of a field.
   (b) Prove that the field $\mathbb{Q}$ of rational numbers has no automorphism except the identity.
   (c) Determine Aut F, when $F = \mathbb{Q}[\sqrt{2}]$.

6. The Operation on Cosets

1. What is the stabilizer of the coset aH for the operation of G on G/H?
2. Let G be a group, and let H be the cyclic subgroup generated by an element x of G. Show that if left multiplication by x fixes every coset of H in G, then H is a normal subgroup.
3. (a) Exhibit the bijective map (6.4) explicitly, when G is the dihedral group D_4 and S is the set of vertices of a square.
   (b) Do the same for D_n and the vertices of a regular n-gon.
4. (a) Describe the stabilizer H of the index **1** for the action of the symmetric group $G = S_n$ on $\{\mathbf{1}, \ldots, \mathbf{n}\}$ explicitly.
   (b) Describe the cosets of H in G explicitly for this action.
   (c) Describe the map (6.4) explicitly.

5. Describe all ways in which S_3 can operate on a set of four elements.
6. Prove Proposition (6.5).
7. A map $S \longrightarrow S'$ of G-sets is called a *homomorphism* of G-sets if $\varphi(gs) = g\varphi(s)$ for all $s \in S$ and $g \in G$. Let φ be such a homomorphism. Prove the following:
   (a) The stabilizer $G_{\varphi(s)}$ contains the stabilizer G_s.
   (b) The orbit of an element $s \in S$ maps onto the orbit of $\varphi(s)$.

7. The Counting Formula

1. Use the counting formula to determine the orders of the group of rotational symmetries of a cube and of the group of rotational symmetries of a tetrahedron.
2. Let G be the group of rotational symmetries of a cube C. Two regular tetrahedra Δ, Δ' can be inscribed in C, each using half of the vertices. What is the order of the stabilizer of Δ?
3. Compute the order of the group of symmetries of a dodecahedron, when orientation-reversing symmetries such as reflections in planes, as well as rotations, are allowed. Do the same for the symmetries of a cube and of a tetrahedron.
4. Let G be the group of rotational symmetries of a cube, let S_e, S_v, S_f be the sets of vertices, edges, and faces of the cube, and let H_v, H_e, H_f be the stabilizers of a vertex, an edge, and a face. Determine the formulas which represent the decomposition of each of the three sets into orbits for each of the subgroups.
5. Let $G \supset H \supset K$ be groups. Prove the formula $[G : K] = [G : H][H : K]$ without the assumption that G is finite.
6. (a) Prove that if H and K are subgroups of finite index of a group G, then the intersection $H \cap K$ is also of finite index.
   (b) Show by example that the index $[H : H \cap K]$ need not divide $[G : K]$.

8. Permutation Representations

1. Determine all ways in which the tetrahedral group T (see (9.1)) can operate on a set of two elements.
2. Let S be a set on which a group G operates, and let $H = \{g \in G \mid gs = s \text{ for all } s \in S\}$. Prove that H is a normal subgroup of G.
3. Let G be the dihedral group of symmetries of a square. Is the action of G on the vertices a faithful action? on the diagonals?
4. Suppose that there are two orbits for the operation of a group G on a set S, and that they have orders m, n respectively. Use the operation to define a homomorphism from G to the product $S_m \times S_n$ of symmetric groups.
5. A group G operates faithfully on a set S of five elements, and there are two orbits, one of order 3 and one of order 2. What are the possibilities for G?
6. Complete the proof of Proposition (8.2).
7. Let $F = \mathbb{F}_3$. There are four one-dimensional subspaces of the space of column vectors F^2. Describe them. Left multiplication by an invertible matrix permutes these subspaces. Prove that this operation defines a homomorphism φ: $GL_2(F) \longrightarrow S_4$. Determine the kernel and image of this homomorphism.

*8. For each of the following groups, find the smallest integer n such that the group has a faithful operation on a set with n elements.
(a) the quaternion group H (b) D_4 (c) D_6

9. Finite Subgroups of the Rotation Group

1. Describe the orbits of poles for the group of rotations of an octahedron and of an icosahedron.
2. Identify the group of symmetries of a baseball, taking the stitching into account and allowing orientation-reversing symmetries.
3. Let O be the group of rotations of a cube. Determine the stabilizer of a diagonal line connecting opposite vertices.
4. Let $G = O$ be the group of rotations of a cube, and let H be the subgroup carrying one of the two inscribed tetrahedra to itself (see exercise 2, Section 7). Prove that $H = T$.
5. Prove that the icosahedral group has a subgroup of order 10.
6. Determine all subgroups of the following groups:
(a) T (b) I
7. Explain why the groups of symmetries of the cube and octahedron, and of the dodecahedron and icosahedron, are equal.

*8. (a) The 12 points $(\pm 1, \pm\alpha, 0), (0, \pm 1, \pm\alpha)(\pm\alpha, 0, \pm 1)$ form the vertices of a regular icosahedron if α is suitably chosen. Verify this, and determine α.
(b) Determine the matrix of the rotation through the angle $2\pi/5$ about the origin in $\mathbb{R}^2$.
(c) Determine the matrix of the rotation of $\mathbb{R}^3$ through the angle $2\pi/5$ about the axis containing the point $(1, \alpha, 0)$.

*9. Prove the crystallographic restriction for three-dimensional crystallographic groups: A rotational symmetry of a crystal has order 2, 3, 4, or 6.

Miscellaneous Problems

1. Describe completely the following groups:
(a) Aut D_4 (b) Aut H, where H is the quaternion group
2. (a) Prove that the set Aut G of automorphisms of a group G forms a group.
(b) Prove that the map φ: $G \longrightarrow$ Aut G defined by $g \rightsquigarrow$ (conjugation by g) is a homomorphism, and determine its kernel.
(c) The automorphisms which are conjugation by a group element are called *inner automorphisms*. Prove that the set of inner automorphisms, the image of φ, is a normal subgroup of Aut G.
3. Determine the quotient group Aut H/Int H for the quaternion group H.

*4. Let G be a lattice group. A *fundamental domain* D for G is a bounded region in the plane, bounded by piecewise smooth curves, such that the sets gD, $g \in G$ cover the plane without overlapping except along the edges. We assume that D has finitely many connected components.
(a) Find fundamental domains for the symmetry groups of the patterns illustrated in exercise 14 of Section 4.
(b) Show that any two fundamental domains D, D' for G can be cut into finitely many congruent pieces of the form $gD \cap D'$ or $D \cap gD'$ (see exercise 7, Section 5).

(c) Conclude that D and D' have the same area. (It may happen that the boundary curves intersect infinitely often, and this raises some questions about the definition of area. Disregard such points in your answer.)

***5.** Let G be a lattice group, and let p_0 be a point in the plane which is not fixed by any element of G. Let $S = \{gp_0 \mid g \in G\}$ be the orbit of p_0. The plane can be divided into polygons, each one containing a single point of S, as follows: The polygon Δ_p containing p is the set of points q whose distance from p is the smallest distance to any point of S:

$$\Delta_p = \{q \in \mathbb{R}^2 \mid \operatorname{dist}(q, p) \le \operatorname{dist}(q, p') \text{ for all } p' \in S\}.$$

(a) Prove that Δ_p is a polygon.

(b) Prove that Δ_p is a fundamental domain for G.

(c) Show that this method works for all discrete subgroups of M, except that the domain Δ_p which is constructed need not be a bounded set.

(d) Prove that Δ_p is bounded if and only if the group is a lattice group.

***6.** (a) Let $G' \subset G$ be two lattice groups. Let D be a fundamental domain for G. Show that a fundamental domain D' for G' can be constructed out of finitely many translates gD of D.

(b) Show that $[G : G'] < \infty$ and that $[G : G'] = \operatorname{area}(D')/\operatorname{area}(D)$.

(c) Compute the index $[G : L_G]$ for each of the patterns (4.16).

***7.** Let G be a finite group operating on a finite set S. For each element $g \in G$, let S^g denote the subset of elements of S fixed by g: $S^g = \{s \in S \mid gs = s\}$.

(a) We may imagine a true–false table for the assertion that $gs = s$, say with rows indexed by elements of G and columns indexed by elements. Construct such a table for the action of the dihedral group D_3 on the vertices of a triangle.

(b) Prove the formula $\sum_{s \in S} |G_s| = \sum_{g \in G} |S^g|$.

(c) Prove *Burnside's Formula*:

$$|G| \cdot (\textit{number of orbits}) = \sum_{g \in G} |S^g|.$$

8. There are $70 = \binom{8}{4}$ ways to color the edges of an octagon, making four black and four white. The group D_8 operates on this set of 70, and the orbits represent equivalent colorings. Use Burnside's Formula to count the number of equivalence classes.

9. Let G be a group of order n which operates nontrivially on a set of order r. Prove that if $n > r!$, then G has a proper normal subgroup.