Chapter 3

Transformation Groups

The notion of a group unifies two different ideas: a geometric one and an algebraic one.

On the geometric side, the notion of a *transformation group* gives a mathematical expression of the general principle of symmetry: the more transformations preserve a given object, the more symmetric it is.

On the algebraic side, the notion of an *abstract group* contains the common features of operations that most often appear in mathematics. Examples of such operations — addition and multiplication of numbers and points, addition of vectors, composition of movements — were considered in the previous chapters.

3.1 A rolling triangle

We begin with an introductory problem where a transformation group comes up in a natural way.

Problem 27 *A regular triangle ABC lies on the plane. One can roll it over the plane by turning it through $180°$ around any of its sides. Suppose that after a certain number of such steps the triangle returns to the initial place, then each of its three vertices will return to its initial position.*

Solution. Let a, b and c be the lines containing the sides of the given triangle in its initial position. After any number of turnovers the sides of the triangle will lie on the lines of the triangular network shown in Fig. 3.1a.

The allowed transformations are compositions of reflections in these lines. Let G be the set of all such transformations. This set contains, for example, rotations through $120°$ around the vertices and glide reflections whose axes coincide with the middle lines of our triangle.

The problem will be solved if we prove that the only plane movement that belongs to G and leaves the triangle in its place, is the identity transformation. Apart from the identity, there are five movements that take the triangle into itself: two nontrivial rotations around its centre and three reflections in its altitudes. We have to show that none of these belongs to the set G.

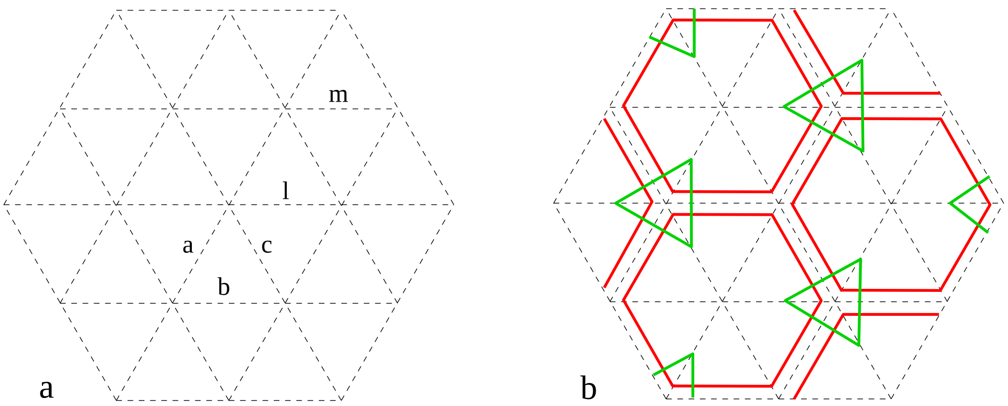


Figure 3.1: Ornament of the rolling triangle

The reader has probably encountered the problems that are solved by constructing an appropriate example (or counterexample). We will use the same trick here — but the example we are going to construct is unusual: it is an *ornament* possessing the following two properties. First, it is symmetric with respect to any of the lines shown in Fig. 3.1a. Second, it is *not* symmetric with respect to the altitudes of the triangle ABC, and its centre is *not* the centre of rotational symmetry for the ornament. The first property implies that the ornament is preserved by any movement that belongs to the set G, while the second means that G contains none of the five nontrivial movements of the triangle. Thus we prove the required result.

It remains to construct an ornament with all the specified properties. An appropriate example is provided by an ancient Chinese ornament (a grating) shown in Fig. 3.1b. Of course, this example is not unique. The general recipe to build such an example can be stated as follows. Choose a completely asymmetric pattern inside the triangle ABC, i.e. a figure which is not preserved by any non-identical movement of the triangle. Then take the union of all figures that are obtained from this pattern by successive reflections in the sides of the triangle. One may imagine that the pattern inside the triangle is dyed with paint leaving a colour trace on the plane when the triangle rolls over.

Exercise 50. Introduce the coordinate system in the plane (see definition 3 on page 18) such that the point A has coordinates $(0, 0)$, point B — coordinates $(6, 0)$, while point C — coordinates $(0, 6)$ (triangle ABC is still supposed to be regular!). Take the pattern consisting of one point $K(3, 1)$. Draw the ornament resulting from this pattern, and describe the coordinates of all its points.

Exercise 51. Will the assertion of Problem 27 still hold, if the regular triangle is replaced by a triangle with angles (a) $45°$, $45°$, $90°$? (b) $30°$, $60°$, $90°$? (c) $30°$, $30°$, $120°$?

3.2 Transformation groups

Definition 10 *A transformation group is a set G of transformations of a certain set which has the following two properties:*

1. *if two transformations f and g belong to G then their composition $f \circ g$ also belongs to G;*

2. *together with every transformation f the set G also contains the inverse transformation f^{-1}.*

These two properties mean that the elements of the set G are interrelated and form a whole which is closed under the composition and taking the inverse. The notion of a set closed with respect to a certain operation has appeared several times in this book, starting from Problem 1.

Example 1. The set of transformations G considered in the discussion of Problem 27 is a transformation group. Property 1 is crucial for the solution of Problem 27. It holds by construction. Property 2 is also valid because the inverse to a series of reflections is the series of the same reflections performed in the inverse order.

Example 2. The set of all transformations of a given set M forms a transformation group denoted by $\mathrm{Tr}(M)$.

Exercise 52. Prove that every transformation group contains the identity transformation.

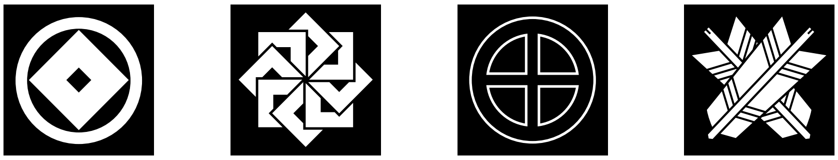
Apart from the group G, in the discussion of Problem 27 we have dealt with two more groups: the group $\mathcal{M}$ of all movements of the plane and the symmetry group of symmetries of a regular triangle D_3.

The groups G and D_3 are contained in $\mathcal{M}$; this fact is usually expressed by saying that they are *subgroups* of $\mathcal{M}$. In general, given an arbitrary plane figure Φ, one can consider the set of all plane movements that take Φ into itself. This set is denoted by $\mathrm{Sym}(\Phi)$ and called the *symmetry group* or *group of movements* of the figure Φ. Every element of this group is referred to as a *symmetry* of the figure Φ Thus, the group D_3 is the symmetry group of a regular triangle: $\mathrm{Sym}(\triangle) = D_3$. Group G used in Problem 27, is also a symmetry group of a certain figure, namely, of the ornament depicted in Fig. 3.1b. To verify this fact, we only have to check that any movement preserving the ornament, is a composition of several reflections in the lines of the triangular grid.

Exercise 53. Make sure this is indeed true.

The notion of a symmetry group is a source of numerous interesting examples of transformation groups. Let us consider some of them.

Problem 28 *Fig. 3.2 shows ancient Japanese family insignias (kamon). Find the symmetry group of each kamon. Which symmetry groups are the same and which are different?*

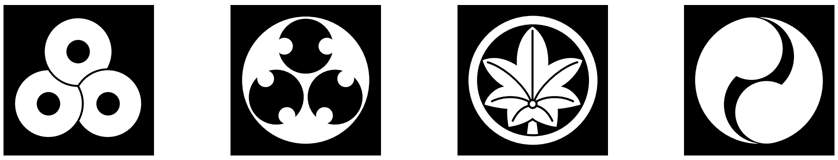


a *b* *c* *d*

Figure 3.2: First set of *kamon*

Solution. Figure Φ_1 is axial symmetric with respect to the four axes at angles of 45° from each other; it also does not change under rotations through 90°, 180° and 270°. The group $\mathrm{Sym}(\Phi_1)$, like any transformation group, also contains the identity transformation, therefore, the total number of its elements is 8. The group $\mathrm{Sym}(\Phi_2)$ also contains eight elements, but it is different from $\mathrm{Sym}(\Phi_1)$, because all its elements are rotations. Figure Φ_3 has the same symmetry as Φ_1: four reflections and four rotations, including the identical one. Finally, figure Φ_4 has no nontrivial transformations, and its symmetry group consists of only one element, the identity transformation.

Exercise 54. Find the symmetry groups of the figures 3.3, a—d. Compare them among themselves and also with the groups of Problem 28.



a *b* *c* *d*

Figure 3.3: Second set of *kamon*

3.3 Classification of finite groups of movements

Symmetry groups of all figures displayed in Fig. 3.2 and Fig. 3.3 consist either of several rotations or of several rotations and an equal number of reflections (including the identity). This observation can be generalized as a theorem. To state it, we need some terminology.

A transformation group is said to be *finite* if it consists of a finite number of elements. The symmetry groups of all figures 3.2 and 3.3 are finite. A group which which consists of an infinite number of elements is referred to as an *infinite group*. The group $\mathcal{M}$ of all plane movements and the group G (Problem 27) are infinite.

The *order* of a group is the number of elements it contains. A finite group is a group of finite order.

The group that consists of rotations around a common centre through multiples of $360°/n$, is called the *cyclic group of order* n and denoted by C_n. The group that contains the same rotations and n reflections in the lines passing through the same centre and such that the angle between any two neighbouring lines is $180°/n$, is called the *dihedral group of order* $2n$ and denoted by D_n.

For example, the symmetry groups of the eight figures that we considered (Fig. 3.2 and 3.3) are D_4, C_8, D_4, C_1, C_3, D_3, D_1, C_2.

Theorem 6 *Any finite group of plane movements is either a* C_n *or a* D_n.

Proof To prove the theorem, we first note that a finite group cannot contain parallel translations, because, if it contains a translation by vector $\mathbf{a}$, it must also contain an infinite number of translations by multiple vectors $n\mathbf{a}$.

If the group contains a glide reflection, it also contains its square, which is a parallel translation, and therefore cannot be finite. We conclude that any finite group of plane movements consists entirely of rotations and reflections.

All rotations belonging to the group must have a common centre, because the following exercise shows that a group containing two rotations with different centres, also contains a parallel translation.

Exercise 55. Prove that if A and B are two different points of the plane and the angles φ and ψ are not multiples of $360°$, then the product $R_B^{-\psi} \circ R_A^{-\varphi} \circ R_B^{\psi} \circ R_A^{\varphi}$ is a nontrivial translation.

Denote all rotations that belong to a given finite group, by R_A^0, R_A^{φ}, $\ldots$, R_A^{ω}, where the angles φ, $\ldots$, ω are chosen to be positive and not exceeding $360°$. Suppose that ψ is the smallest of these angles. Then all the remaining angles must be multiples of ψ. Indeed, suppose that φ is not divisible by ψ. Then it can be written as $\varphi = k\psi + \xi$ where k is an integer and $0 < \xi < \psi$. The rotation through ξ must also belong to the group under study, and we arrive at a contradiction.

Note that ψ must be equal to $360°/n$ for some integer n — otherwise a certain power of the rotation R_A^{ψ} would represent a rotation by an angle smaller than ψ. We have thus proved that all the rotations present in any finite group of plane movements, are $R_A^{k\psi}$, where $k = 0, 1, \ldots, n-1$ and $\psi = 360°/n$. If the group contains no reflections, then it is the group C_n.

Now suppose that the group contains n rotations and at least one reflection. We are going to prove that the number of reflections in the group is exactly n.

Indeed, if R_1, R_2, $\ldots$, R_n are n different rotations and S a reflection, then the n compositions $S \circ R_1$, $S \circ R_2$, $\ldots$, $S \circ R_n$ represent n different reflections that belong to the group. Thus, the number of reflections is no smaller than n. Similarly, the number of rotations in the group is no smaller than the number of reflections, because, if S_1, S_2, $\ldots$, S_m are m different reflections, then $S_1 \circ S_1$, $S_1 \circ S_2$, $\ldots$, $S_1 \circ S_m$ are m different rotations (including the identity).

We have thus proved that any finite group of plane movements is either a C_n or it consists of n rotations with a common centre and equal number of reflections. If $n = 1$, what we get is the group D_1 of order 2 that contains one reflection and the identity transformation. If $n \geq 2$, we have to show that the axes of all reflections pass through the centre of rotations. First remark that a finite group may not contain two reflections whose axes are parallel, because their product would produce a translation by a non-zero vector. Thus any two axes must have a common point. The product of the two reflections whose axes intersect at a point P making the angle φ belongs to the group and is a rotation around P through the angle 2φ. Hence the point P coincides with the common centre A of all rotations, while the angle φ is a multiple of $180°/n$. The group under study is thus D_n. This completes the proof.

Exercise 56. Can a plane figure have

1. exactly two symmetry axes?

2. exactly two centres of symmetry?

Exercise 57. Name the most symmetrical, i.e. having the biggest symmetry group, bounded plane figure.

3.4 Conjugate transformations

In the discussion of Problem 28 above we said that the symmetry groups of figures Φ_1 and Φ_3 are the same: $\mathrm{Sym}(\Phi_1) = \mathrm{Sym}(\Phi_3)$. What is the precise meaning of this equality? In a more general setting: what is the precise meaning of the classification theorem we have proved in the previous section? Let us think a little about these questions.

The equality of the two symmetry groups like $\mathrm{Sym}(\Phi_1)$ and $\mathrm{Sym}(\Phi_3)$ has the verbal meaning, i.e. the two sets of plane movements coincide only if the two figure are placed in the plane in such a way that their centres and symmetry axes coincide. Otherwise the sets $G = \mathrm{Sym}(\Phi_1)$ and $H = \mathrm{Sym}(\Phi_3)$ would be different, although closely related to each other. We will now elucidate this relation.

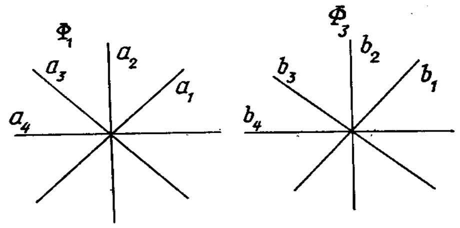


Figure 3.4: Conjugate symmetry groups

Denote the centre of rotations and the symmetry axes for the group G by A and a_1, …, a_4. Denote the same objects for the group H by B and b_1, …, b_4, respectively (see Figure 3.4). Let f be a plane movement that carries B into A and each b_i into a_i. The transformations of the group G can be obtained from the transformations that belong to the group H in the following way. Consider, for example, the reflection in the line b_3. First move the figure Φ_1 with the help of the movement f^{-1}, then apply reflection in b_3 to it, then move it back with the help of f. It is easy to see that after all these actions the figure has undergone a reflection in the line a_3.

In general, for any element h of the group H the composition $f \circ h \circ f^{-1}$ is an element of G. More precisely, if h is a reflection in b_i, then $f \circ h \circ f^{-1}$ is a reflection in a_i; if h is a rotation around B, then $f \circ h \circ f^{-1}$ is a rotation around A through the same angle.

Definition 11 *Two transformations $h \in H$ and $g = f \circ h \circ f^{-1} \in G$ are said to be conjugate. The transition from h to g is called conjugation by f.*

We have encountered conjugate transformations before, when we derived the complex number formula for the rotation with an arbitrary centre and in Exercise 37 (Chapter 2).

Two groups of movements are said to be *conjugate*, if the list of elements of one group becomes the list of elements of the second group upon conjugation by a certain (one and the same) movement. The symmetry groups of two copies of one and the same figure placed arbitrarily in the plane, are always conjugate. The conjugation is effectuated by a movement that carries one of the copies into another.

In general, conjugation should be understood as looking at an object from a different viewpoint. The conjugating movement is the one which relates the two viewpoints (or systems of reference, in physical terminology).

The most important property of conjugate subgroups is that they have the same internal structure. Let us explain the exact mathematical meaning of this phrase. Let G and H be two groups of plane movements that are conjugated by movement f. If $g = f \circ h \circ f^{-1}$, then we will say that g and h *correspond* to each other and write $g \leftrightarrow h$. This correspondence is one-to-one, because h can be uniquely expressed in terms of g as $f^{-1} \circ g \circ f$.

Then the following two facts hold:

1. If $g_1 \leftrightarrow h_1$ and $g_2 \leftrightarrow h_2$, then $g_1 \circ g_2 \leftrightarrow h_1 \circ h_2$.
2. If $g \leftrightarrow h$, then $g^{-1} \leftrightarrow h^{-1}$.

Both facts are verified in a straightforward way:

1. $g_1 \circ g_2 = (f \circ h_1 \circ f^{-1}) \circ (f \circ h_2 \circ f^{-1}) = f \circ (h_1 \circ h_2) \circ f^{-1}$.
2. $(f \circ h \circ f^{-1})^{-1} = f \circ h^{-1} \circ f^{-1}$.

Thus, both group operations (composition and taking the inverse) in one group correspond to their respective counterparts in another group under the correspondence under study. This phenomenon is called *isomorphism*, and we will study it in detail later in this chapter.

Now we will derive formulas for conjugation in the group of plane movements.

Problem 29 *Find the movement which is conjugate to the rotation R_A^α by means of the reflection S_l.*

Solution. By virtue of the general remark that we made above, to get the conjugate movement one has to look at the given rotation 'from under the plane', displacing one's viewpoint by means of the reflection S_l. It is fairly evident that the result is the rotation through $-\alpha$ around the point A' which is symmetric to A with respect to l. We will perform a rigorous check of this result, i.e. prove that $S_l \circ R_A^\alpha \circ S_l^{-1} = R_{A'}^{-\alpha}$.

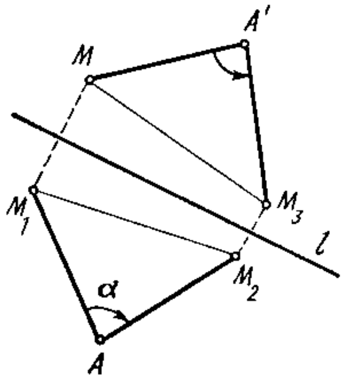


Figure 3.5: Conjugation of a rotation by a reflection

Indeed, let M be an arbitrary point in the plane (see Fig. 3.5). Let M_1 be its image under the movement S_l^{-1} (which, in fact, is the same thing as S_l). Suppose that M_1 goes into M_2 under R_A^α and M_2 goes into M_3 under S_l. Then $\triangle MA'M_3 = \triangle M_1AM_2$, whence $M_3 = R_{A'}^{-\alpha}(M)$.

Exercise 58. Compile a complete table of all conjugations in the group of plane movements, i.e. find $f \circ g \circ f^{-1}$ for every $g = T_{\mathbf{a}}, R_A^\alpha, S_l, U_l^{\mathbf{a}}$ and every $f = T_{\mathbf{b}}, R_B^\beta, S_m, U_m^{\mathbf{b}}$.

To acquire the freedom in the manipulations with plane movements, we suggest that the reader make and practice a simple tool that we call 'dihedral instrument'. It consists of a regular polygon cut from cardboard and of the same polygon drawn on a piece of paper. The vertices of either polygon should be consecutively numbered by 1, 2, ...

With the help of this instrument, one can study the dihedral group D_n. To find the product of two elements of D_n, one must first place the cardboard thing on paper in its initial position, so that the vertices with the same numbers coincide, then perform the given movements one after another and, comparing the numbers of vertices, try to figure out what is the composed movement. In the same way one can also compute the table of conjugations.

Exercise 59. Using appropriate dihedral instruments, fill in the multiplication and conjugation tables for the groups D_3 and D_4.

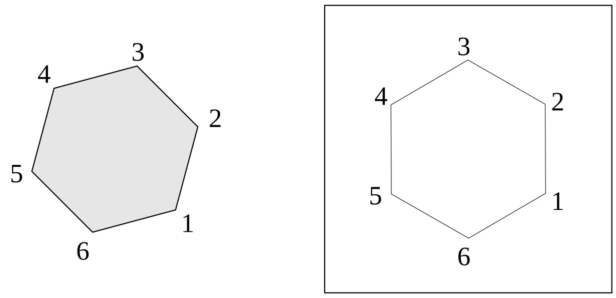


Figure 3.6: Instrument for studying the dihedral group

Looking at the table of conjugate movements (the answer to Exercise 58), one can notice that a translation $T_{\mathbf{a}}$ does not change when conjugated by another translation $T_{\mathbf{b}}$:

$$T_{\mathbf{b}} \circ T_{\mathbf{a}} \circ T_{\mathbf{b}}^{-1} = T_{\mathbf{a}}.$$

This equation is equivalent to $T_{\mathbf{b}} \circ T_{\mathbf{a}} = T_{\mathbf{a}} \circ T_{\mathbf{b}}$ which means that any two translations *commute*, in other words, they are interchangeable with respect to composition. (We remind that we have already mentioned commutativity in the discussion of Problem 24.)

A transformation group where any two elements commute is called *commutative*.

Problem 30 *Find all finite commutative groups of plane movements.*

Solution. We know the list of all finite groups of plane movements: it is made up of C_n and D_n for all $n = 1, 2, 3, \ldots$

Every cyclic group C_n is commutative. This follows from the fact that the group of all rotations with the common centre is commutative, because the product of rotations through angles α and β is a rotation through $\alpha + \beta$, irrelevant of the order in which the composition is taken.

The group D_1 is commutative, because it consists of only two elements, one of which is the identity. It is easy to see that the group D_2 is commutative, too. In fact, it consists of two reflections S_1 and S_2 whose axes are mutually perpendicular, a half-turn rotation R and an identity transformation. According to the rules we have derived earlier the composition $S_1 \circ S_2$ is a rotation through 180° in one direction, while $S_2 \circ S_1$ is a rotation through 180° in the opposite direction. Hence, $S_1 \circ S_2 = S_2 \circ S_1$. Therefore, $S_1 \circ R = S_1 \circ S_2 \circ S_1 = R \circ S_1$. Similarly, $S_2 \circ R = R \circ S_2$.

Now consider the group D_n for $n \geq 3$. Choose two reflections that belong to this group and whose axes are adjacent, i.e. make an angle of $180°/n$. Their products are rotations through the angle $360°/n$, in the positive or negative direction, depending on the order the product is taken. Since $n \geq 3$, these two products are different. Therefore, the group D_n is non-commutative.

The complete list of finite commutative groups of plane movements thus includes D_1, D_2 and all groups C_n.

The property of commutativity of can be easily read off its multiplication table: a group is commutative if and only if its multiplication table is symmetric with respect to the main diagonal. The readers who did exercise 59 have a visual evidence of the fact that the groups D_3 and D_4 are not commutative. However, even if the table is not symmetric as a whole, it always contains pairs of equal elements that occupy symmetric positions. Such pairs correspond to the pairs of commuting elements of the group.

Exercise 60. Indicate all pairs of commuting elements in the groups D_3 and D_4.

3.5 Cyclic groups

There is another way to explain why the cyclic group C_n is commutative. Let R denote the rotation through $360°/n$. Then all the elements of the group can be represented as powers of R, i.e. $R^2 = R \circ R$, $R^3 = R \circ R \circ R$, $\ldots$, $R^n = \mathrm{id}$, and it is clear that we always have $R^k \circ R^l = R^{k+l} = R^l \circ R^k$.

A transformation f such that its powers exhaust the set of all elements of the group is referred to as the *generator*, or the *generating element* of the group. To better understand the meaning of this notion, let us imagine that we have no group, but only one transformation f of a certain set M. The question is whether there exists a transformation group that contains this transformation f. The answer to this question is always positive. The smallest group containing a given transformation f can be constructed in the following way.

If a group contains an element f, then, according to the first defining property of a group, it must contain all its powers f^2, f^3, etc. By the second property, it also must contain the inverse transformation f^{-1} and therefore all its powers $(f^{-1})^2$, $(f^{-1})^3$, etc.

Exercise 61. Prove that $(f^{-1})^k = (f^k)^{-1}$.

The transformation $(f^{-1})^k$, where k is a natural number, is called a negative power of f and is also denoted by f^{-k}. The zeroth power of any transformation is by definition the identity transformation. Now observe that the set of all integer powers of a given transformation $\ldots, f^{-2}, f^{-1}, f^0, f^1, f^2, \ldots,$ *always* forms a group, because of the identities $f^k \circ f^l = f^{k+l}$, $(f^k)^{-1} = f^{-k}$ which hold not only for natural, but also for all integer values of k and l. This set of all powers of f is called *the group generated by f*.

Two possibilities may arise.

1. All the powers f^k are different. In this case the group generated by f is infinite and is referred to as an *infinite cyclic group.*

2. Among the powers of f there are some that coincide. Then there is a positive power of f which is equal to the identity transformation. Indeed, if f^k and f^l is any pair of coinciding powers, $k > l$, then $f^{k-l} = \mathrm{id}$. Denote by n the smallest positive exponent satisfying $f^n = \mathrm{id}$. The number n is called the *order* of the transformation f. In this case the group generated by f consists of exactly n different transformations $f, f^2, \ldots, f^n$. (All of these are different indeed, because if we had $f^k = f^l$ with $0 < l < k \leq n$, then we would get $f^{k-l} = \mathrm{id}$ contrary to the choice of n.)

In this case the group generated by f is a *finite cyclic group of order* n. In particular, this notion includes the cyclic groups of rotations C_n considered above.

When the transformation f generates an infinite group, we can also say that f has *infinite order*. The order of the identical transformation is 1 by definition, and the group it generates consists of only one element and is referred to as the *trivial group*. An involutive transformation generates a group of order 2, consisting of itself and the identity.

Problem 31 *Which elements of the group C_{12} are generators of this group? What are the subgroups generated by other elements?*

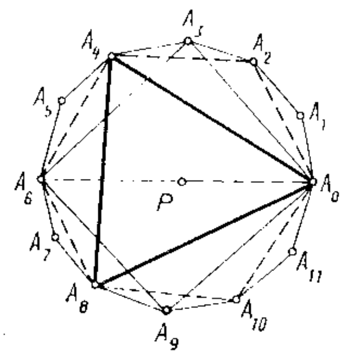


Figure 3.7: Cyclic group C_{12} and its subgroup

Solution. The group C_{12} consists of 12 rotations through angles which are multiples of 30°. All these rotations are powers the rotation through 30° which is, by this reason, a generator of the group. The inverse rotation (by 330°) is obviously a generator, too. To facilitate the study of the other elements, we use Figure 3.7 where every element of the group is represented by a vertex of the regular 12-gon: A_0 corresponds to the identity, A_1 is the rotation through 30°, etc. Consider the elements of the group one by one and, for every element, mark all the vertices of the polygon that correspond to the powers of this element. We will see that:

- There are two more rotations — through 150 and 210 degrees — that generate the whole group.
- Rotations through 60 and 300 degrees have order 6 and generate the group C_6 visualized as a hexagon $A_0A_2A_4A_6A_8A_{10}$ in Figure 3.7.
- Rotations through 90 and 270 degrees generate the group of order 4 (the square $A_0A_3A_6A_9$).
- Rotations through 120 and 240 degrees generate the group of order 3 (the triangle $A_0A_4A_8$).
- The rotation through 180° which is an involution, generates the group C_2 depicted as the line segment A_0A_6.

This result can be summarized in a table where the upper line is for the values of k, while the lower line shows the order of the rotation R^k (R being the rotation through 30°):

0	1	2	3	4	5	6	7	8	9	10	11
1	12	6	4	3	12	2	12	3	4	6	12

Exercise 62. Using the notion of the greatest common divisor (GCD) of two numbers, find a general formula for the order of the element f^k in a cyclic group of order n generated by f.

A transformation belonging to a finite group is a generator of this group if and only if its order is equal to the order of the group. The number of generating elements in the cyclic group C_n is denoted by $\varphi(n)$ and the function φ is called the *Euler function.* For example, the table above shows that $\varphi(12) = 4$.

Exercise 63. (a) Compile the table of values of the function $\varphi(n)$ for $n = 2, 3, \ldots, 15$. (b) Find a general formula for $\varphi(n)$ in terms of the prime decomposition of the number n.

Now let us see what are the orders of different plane movements according to their type. It is clear that non-identical translations and glide reflections have an infinite order, because under the repeated action of such a transformation any point occupies infinitely many new positions (Fig. 3.8, a and b).

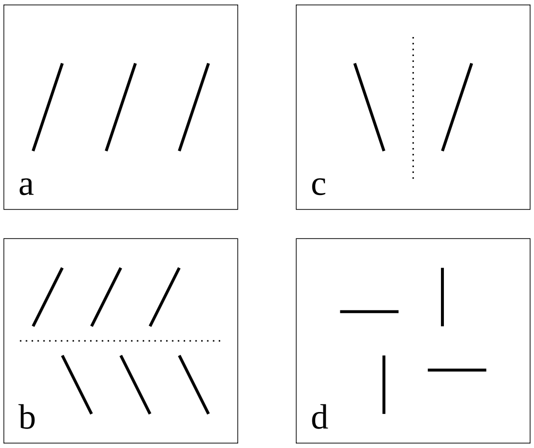


Figure 3.8: Order of translation, reflection and glide reflection

Exercise 64. Is it possible that a plane figure remain unmoved under a non-trivial translation or a glide symmetry?

Any reflection has order 2 (Fig. 3.8c).

Rotations may have different orders. If the angle of rotation is measured by a rational number of degrees $360° \cdot m/n$ where m/n is an irreducible fraction, then the rotation has a finite order n (Fig. 3.8d). For an irrational number of degrees the order is infinite.

Exercise 65. Verify the previous assertion for the rotations of Problem 31. Prove the general fact.

3.6 Generators and relations

Cyclic groups, i.e. groups generated by one element, constitute the simplest class of groups. Now we will consider the groups that cannot be generated by one element.

To begin with, let us prove that the group D_n, where $n \geq 2$, is not cyclic. In fact, we have already seen that, if $n > 2$ then D_n is not commutative and hence is not cyclic. In the case $n = 2$ note that every non-identical element of the group D_2 is of order 2 and thus the group does not contain any element of order 4.

A natural question arises: what is the smallest set of elements of the group D_n which generates the whole group, i.e. allows to express any element of the group using multiplications and taking the inverse? It turns out that two elements are enough and $\{R, S\}$, where R is the rotation through $360°/n$ and S an arbitrary reflection, is an example of such a set. In fact, every rotation belonging to D_n can be represented as R^k, while every reflection as $R^k \circ S$.

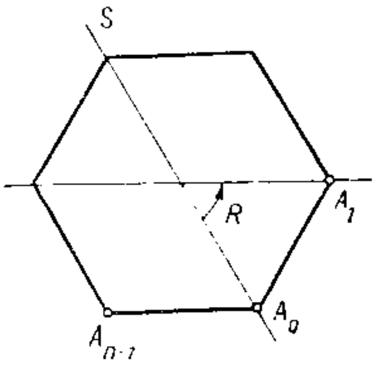


Figure 3.9: Group D_n

The first of these two assertions is evident. To prove the other, note that all the movements $R^k \circ S$ for $k = 0, 1, \ldots, n-1$ are different. Indeed, an equality $R^k \circ S = R^l \circ S$, when multiplied by S on the right, would imply $R^k = R^l$ which is a contradiction. Now observe that all these movements are improper, i.e. reflections, not rotations. Since the total number of reflections in the group D_n is n, we deduce that each of them must appear in the list S, $R \circ S$, $\ldots$, $R^{n-1} \circ S$.

We have thus proved that the pair $\{R, S\}$ is a set of generators of the group

$$D_n = \{\mathrm{id}, R, \ldots, R^{k-1}, S, R \circ S, \ldots, R^{k-1} \circ S\}.$$

Let us describe the multiplication rule of the group D_n in terms of these expressions through R and S.

- The composition of R^k and R^l is R^{k+l}. If $k+l>n$, this can be replaced by R^{k+l-n} to coincide literally with an element of the above list.
- In the same way, $R^k \circ (R^l \circ S) = R^{k+l} \circ S$, or, if $k+l>n$, it is better to write $R^k \circ (R^l \circ S) = R^{k+l-n} \circ S$.
- Let us find the composition $(R^k \circ S) \circ R^l$. Recall (Problem 29) that $S \circ R^k \circ S = R^{-k}$. Multiplying this equality by S on the right, we get: $S \circ R^k = R^{-k} \circ S$. Therefore,

$$(R^k \circ S) \circ R^l = R^k \circ (S \circ R^l) = R^k \circ (R^{-l} \circ S) = R^{k-l} \circ S.$$

- A similar argument shows that $(R^k \circ S) \circ (R^l \circ S) = R^{k-l}$.

In terms of the generators R and S, the multiplication table for the group D_n can be represented as follows:

	R^l	$R^l \circ S$
R^k	R^{k+l}	$R^{k+l} \circ S$
$R^k \circ S$	$R^{k-l} \circ S$	R^{k-l}

where, in case of necessity, the exponent of R can be increased or decreased by n, using the fact that $R^n = \mathrm{id}$.

For specific values of n, this short table can be expanded to its full form. For example, if $n=3$, we get the following full table:

	id	R	R^2	S_a	S_b	S_c
id	id	R	R^2	S_a	S_b	S_c
R	R	R^2	id	S_b	S_c	S_a
R^2	R^2	id	R	S_c	S_a	S_b
S_a	S_a	S_c	S_b	id	R^2	R
S_b	S_b	S_a	S_c	R	id	R^2
S_c	S_c	S_b	S_a	R^2	R	id

An important observation is that the complete multiplication table of the group D_n follows from just three relations between the generating elements R and S:

$$S^2 = \mathrm{id}; \quad (S \circ R)^2 = \mathrm{id}; \quad R^n = \mathrm{id}\,. \tag{3.1}$$

All other relations between R and S can be formally deduced from these three using the definition of a group. As an example, let us check this for the relation $S \circ R^k \circ S = R^{-k}$ that we have used when working on the multiplication table.

The second relation in 3.1 can be expanded as

$$S \circ R \circ S \circ R = \mathrm{id}$$

or, equivalently, as

$$S \circ R \circ S = R^{-1}.$$

Taking into account that $S^2 = \mathrm{id}$, the n-th power of the last equality gives:

$$S \circ R^k \circ S = R^{-k}.$$

It turns out that relations 3.1 constitute a complete set of *defining relations* for the group D_n in the following sense: if a group is generated by two elements S and R which satisfy the relations 3.1 and *no other relation except for those that are formal consequences of these three*, then the order of this group is $2n$ and its structure is the same as the structure of the group D_n.

We will now try to give a general definition of generators and defining relations of a transformation group. Let $S = \{s_1, \dots, s_n\}$ be a finite subset of a group G. By a *monomial over S* we understand a product of the form $M = s_{i_1}^{k_1} s_{i_2}^{k_2} \cdots s_{i_m}^{k_m}$, where i_1, ..., i_m are numbers between 1 and n and the exponents k_1, ..., k_n are arbitrary integers. A *relation* between s_1, ..., s_n is a monomial r over S which is equal to id in the group G. Relations can also be written in the form $r_1 = r_2$, which is equivalent to $r_1 r_2^{-1} = \mathrm{id}$.

Definition 12 *Let G be a transformation group, $S \subset G$ its subset and R a certain set of relations between the elements of S*

We say that the set S is a set of generators and the R a set of defining relations for the group G, if

1. Any element of G can be represented as a monomial over S.

2. Any relation between the elements of S is a formal consequence of the relations belonging to the set R.

By a formal consequence of relations $r_1 = \mathrm{id}$, ..., $r_m = \mathrm{id}$, where every r_i is a monomial over the set S, we mean a new monomial $r = \mathrm{id}$ which can be deduced from the given set using the group operations (multiplication and taking the inverse) and their properties, such as associativity, simplification rules $s^k s^l = s^{k+l}$, $s^0 = \mathrm{id}$ and the fact that equalities $ab = \mathrm{id}$ and $ba = \mathrm{id}$ are equivalent. For example, relations $ab^2 = \mathrm{id}$ and $ba^2 = \mathrm{id}$ imply that $b = a^{-2}$ and hence $a^3 = \mathrm{id}$.

Let us note that in a certain sense, the nature of the elements $s_1, \dots, s_n$ is here irrelevant: later (page 103 in Chapter 5) we will give a definition of an abstract group with a prescribed set of generators and relations.

We pass to some exercises where the notion of defining relations is crucial.

Problem 32 *Suppose that A and B are two transformations that satisfy the relations*

$$A^3 = \mathrm{id}; \quad B^5 = \mathrm{id}; \quad AB = B^4 A \tag{3.2}$$

and do not satisfy any relations that do not follow from these three by group axioms. Prove that the group generated by A and B is a cyclic group of order 3.

Solution. To simplify the formulas, both in the statement and the discussion of Problem 32 we omit the symbol of composition (small circle) and correspondingly use the word 'multiplication' instead of 'composition'.

An arbitrary element of the group G generated by A and B can be written as

$$B^{k_1}A^{l_1}B^{k_2}A^{l_2}\ldots B^{k_m}A^{l_m}$$

where, in virtue of 3.2, we can assume that $0 \le k_i \le 4$ and $0 \le l_i \le 2$. Let us transform this 'word' using the following rule: *each time that an A appears next to a B on the left, replace AB by B^4A.* Applying this rule sufficiently many times, we will sooner or later push all B's to the left and arrive at a word of this type: B^kA^l, where, like before, we are in a position to assume that $0 \le k_i \le 4$ and $0 \le l_i \le 2$.

Since the integer k may take 5 different values and the integer l three different values, we see that the total number of products B^kA^l is no greater than 15. It turns out, however, that not all of these elements are different. Indeed, we can deduce the following chain of equalities from the defining relations 3.2:

$$B = A^3B = A^2B^4A = AB^{16}A^2 = B^{64}A^3 = B^4,$$

where we have used the above described rule together with the observation: *the letter A when going through a B from left to right, multiplies its exponent by 4.* Therefore, $B^3 = \mathrm{id}$ which, together with the known identity $B^5 = \mathrm{id}$, implies that $B = \mathrm{id}$.

The group G is thus in fact generated by only one element A satisfying $A^3 = \mathrm{id}$. It remains to note that this generator A *cannot* be trivial, because the relation $A = \mathrm{id}$ is *not* a consequence of the relations 3.2. Indeed, if we take a 120 degree rotation for A and the identity transformation for B, then all the three relations 3.2 are true, while the relation $A = \mathrm{id}$ is false.

Exercise 66. Let A and B be two nontrivial movements of the plane such that $ABA^2 = \mathrm{id}$ and $B^2A = \mathrm{id}$. What is the order of the group generated by A and B? What kind of movements are A and B?

Similar arguments can be used in the following exercise which, at first glance, looks totally unrelated to the theory of transformation groups.

Exercise 67. The language of the tribe Aiue has only 4 letters: A, I, U and E. The letter E is special. When used by itself, it means a certain word, but when added to any word in the beginning, the middle or the end, it does not change its meaning. Furthermore, each of the letters A, U, I, pronounced seven times in a row, makes a synonym of the word E. The following word fragments are also considered as synonyms: UUUI and IU, AAI and IA, UUUA and AU. The total number of people in the tribe is 400. Is it possible that all of them have different names?

Exercise 68. Find all pairs of generators in the group D_n. For each pair indicate the defining relations.

The notion of defining relations can be used for groups that have any number of generators. For example, the cyclic group of order n is the group with one generator R and one defining relation $R^n = \mathrm{id}$. An infinite cyclic group is the group with one generator T which is not subject to any relations. We should like to emphasize once again the meaning of the last phrase. What we mean here is that there are no *non-trivial* relations for T, i.e. relations that involve T and id and do not follow from the general properties of groups. Here is an example of a trivial relation: $T^{-1}T^4T^{-3} = \mathrm{id}$.

We shall now give an example of the group with three generators. Consider the group of plane movements which was denoted by G in Problem 27 and which we will now denote by $p3m1$, its official crystallographic symbol (see Chapter 4 for a detailed discussion of crystallographic groups). By definition, the group $p3m1$ is generated by an infinite number of reflections, namely, the reflections in all the lines shown in Figure 3.1a.

It turns out, however, that this group is also generated by only three reflections S_a, S_b, S_c where a, b and c are the sides of an equilateral triangle which forms the unit of the lattice shown in Figure 3.1a. To prove this fact, we have to show that the reflection S_x in any line x that belongs to the triangular lattice under study, can be expressed in terms of S_a, S_b, S_c.

Consider, for example, the reflection S_l (notation of Figure 3.1a). Since the line l is symmetric to a with respect to c, we see that the movement S_l can be obtained from S_a using the conjugation by S_c, i.e. $S_l = S_c \circ S_a \circ S_c$. Also, since $S_l(b) = m$, we have $S_m = S_l \circ S_b \circ S_l = S_c \circ S_a \circ S_c \circ S_b \circ S_c \circ S_a \circ S_c$.

A similar argument allows to express any reflection S_x through S_a, S_b, S_c, because any line x belonging to the lattice can be obtained from the lines a, b, c by an appropriate series of reflections S_a, S_b, S_c.

We now observe that the three generators satisfy the following relations:

$$S_a^2 = S_b^2 = S_c^2 = \mathrm{id}, \tag{3.3}$$
$$(S_a \circ S_b)^3 = (S_b \circ S_c)^3 = (S_c \circ S_a)^3 = \mathrm{id}\,. \tag{3.4}$$

Exercise 69. Let F_1, F_2, F_3 be three plane movements that generate an infinite group and satisfy the relations

$$F_1^2 = F_2^2 = F_3^2 = (F_1 \circ F_2)^3 = (F_2 \circ F_3)^3 = (F_3 \circ F_1)^3 = \mathrm{id}\,.$$

Show that F_1, F_2, F_3 are reflections in the sides of a regular triangle.

This exercise shows that relations 3.4 and 3.4, supplied with the additional requirement of infiniteness, determine the group uniquely as the group of plane movements. Actually, it can be proved that these relations are the *defining relations* for the group $p3m1$ in the sense explained above.