Chapter 5

Orbits and Ornaments

Topics that will be touched upon in this chapter include group actions, orbits, invariants and ornaments.

Transformation groups, by their definition, *act* on certain sets. Thus, the group of movements of the plane acts on (the set of all points of) the plane. The permutation group S_3 acts on the set $\{1, 2, 3\}$. The ability to transform the sets is so inherent in the notion of a group that it is also preserved for arbitrary abstract groups. To give the exact definition of the group action, we shall need the notion of a homomorphism.

5.1 Homomorphism

The notion of a homomorphism generalizes that of an isomorphism. A homomorphism is defined by the same operation-preserving property. only without the requirement that it must be a one-to-one correspondence.

Definition 16 *A homomorphism from the group G into the group H is a mapping $\varphi : G \to H$ such that*

$$\varphi(ab) = \varphi(a)\varphi(b) \tag{5.1}$$

for all $a, b \in G$ (the group operation is here denoted as multiplication, but of course, it may have arbitrary nature).

An isomorphism is thus a one-to-one homomorphism. Some properties of isomorphisms generalize to arbitrary homomorphisms. Thus, the image of the unit $e \in G$ under a homomorphism is always the unit $e' \in H$. Also, for any element $g \in G$ we always have

$$\varphi(g^{-1}) = \varphi(g)^{-1}. \tag{5.2}$$

Both of these equalities easily follow from equation 5.1.

Note that for any two groups G and H the mapping that takes all the elements of G into the unit of H is a homomorphism, called the *trivial homomorphism*.

If $\varphi : G \to G'$ is an isomorphism and G' is a subgroup of a bigger group H, then we can view φ as a mapping from G into H which is, of course, a homomorphism. Such homomorphisms are referred to as *injective*, or *monomorphic homomorphisms*. They are characterized by the property that no two different elements of G go into the same element of H under φ.

The image of G by the trivial homomorphism is the trivial subgroup (consisting of only one element). Note that the image of G by any homomorphism $\varphi : G \to H$ is a subgroup of H. The most interesting class of homomorphisms, in a certain sense dual to the class of monomorphisms, consists of *epimorphic*, or *surjective homomorphisms.* A homomorphism $\varphi : G \to H$ is *surjective*, if its image coincides with the whole of H, or, which is the same, if every element of H is the image of some element of G.

We will consider several examples of surjective homomorphisms.

Problem 37 *Construct a surjective homomorphism of the group of integers $\mathbb{Z}$ with the operation of addition onto the group of residue classes $\mathbb{Z}_m$.*

Solution. The solution is very simple: the mapping p that takes every number a into $\overline{a}$, the class of a modulo m, is the required epimorphism. It preserves the addition, because by definition of the group $\mathbb{Z}_m$ (see p. 93) we have

$$p(a+b) = \overline{a+b} = \overline{a} + \overline{b} = p(a) + p(b).$$

Also, the mapping p is obviously surjective.

Note in passing that p also preserves the product: $p(ab) = p(a)p(b)$, so it is a homomorphism with respect to multiplication, — and you have probably used both of these properties while solving Exercise 95.

Exercise 97. For what values of m and n there exists a homomorphism of $\mathbb{Z}_m$ onto $\mathbb{Z}_n$?

Problem 38 *Find a homomorphism of S_4 onto S_3.*

Solution. Recall (4.1) that S_n denotes the permutation group of n elements. Thus, S_4 consists of 24 permutations of the set of cardinality 4, while S_3 is made up of 6 permutations of the set of cardinality 3. We have seen earlier (exercise 74) that S_3 is isomorphic to the group of functions Φ generated by $1/x$ and $1-x$. Therefore, it is enough to construct a homomorphism of S_4 onto Φ. This can be done as follows.

Consider the expression in four variables

$$x = \frac{a-c}{b-c} : \frac{a-d}{b-d},$$

which is called the *double ratio* of a, b, c and d. If the four letters a, b, c, d in this expression are permuted, the value of the double ration is changed. It is remarkable that the new value can always be expressed through x alone. For example, after the permutation $\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$ (i.e. when $a \mapsto b$, $b \mapsto c$, $c \mapsto d$, $d \mapsto a$) we obtain:

$$\frac{b-d}{c-d} : \frac{b-a}{c-a} = \frac{x}{x-1}.$$

Exercise 98. For each of the 24 permutations of the letters a, b, c, d find the expression of the double ratio after the permutation through its initial value x.

A diligent reader who has solved this exercise will recall that the set of 6 functions obtained is exactly the group of functions that we know as Φ. Denote the rational function that corresponds to the permutation σ, by $f_\sigma(x)$. To show that the mapping $f : \sigma \mapsto f_\sigma(x)$ is a homomorphism, we have to check that $f_{\tau\sigma} = f_\tau \circ f_\sigma$. Indeed, if

$$f_\sigma(x) = \frac{\sigma(a) - \sigma(c)}{\sigma(b) - \sigma(c)} : \frac{\sigma(a) - \sigma(d)}{\sigma(b) - \sigma(d)} = y,$$

then evidently

$$f_{\tau\sigma}(x) = \frac{\tau\sigma(a) - \tau\sigma(c)}{\tau\sigma(b) - \tau\sigma(c)} : \frac{\tau\sigma(a) - \tau\sigma(d)}{\tau\sigma(b) - \tau\sigma(d)} = f_\tau(y)$$

and thus $f_{\tau\sigma}(x) = f_\tau(f_\sigma(x))$.

Now we would like to draw your attention to the following interesting observation. The fact that f is a homomorphism, i.e. satisfies the relation $f_{\tau\sigma} = f\tau \circ f\sigma$, simplifies a great deal the solution of Problem 38. In fact, to prove that the image of f coincides with the set Φ, we do not have to check all the 24 permutations of the four letters as suggested in the Exercise above. It is sufficient to check 3 transpositions, $a \leftrightarrow b$, $b \leftrightarrow c$ and $c \leftrightarrow d$, which generate the group S_4. These transpositions correspond to the functions $1/x$, $1 - x$ and $1/x$, respectively, and we know that the two functions $1/x$ and $1 - x$ generate the group Φ.

Exercise 99. Assign $+1$ to every movement that preserves the orientation and -1 to every movement that changes orientation. Check that this assignment is a homomorphism of the group of all plane movements onto the group of 2 elements $\{+1, -1\}$ with the operation of multiplication.

Problem 39 *Construct a homomorphism of the group G of all proper plane movements onto the group T of complex numbers whose modulus is 1.*

Solution. Recall (2.3) that any proper plane movement can be written analytically as a complex function $f(z) = pz + a$, where $|p| = 1$. We define the mapping $\varphi : G \to T$ by $\varphi(f) = p$. Let us check that this mapping is a group homomorphism. Indeed, the composition of two movements, f and g defined by $g(z) = qz + b$, is

$$g(f(z)) = q(pz + a) + b = qpz + (aq + b),$$

where the coefficient of z is qp. Therefore, $\varphi(gf) = \varphi(g)\varphi(f)$.

Geometrically, the assertion just proved implies that when two rotations, even with different centres, are multiplied, the angles of rotation are added together. In particular, the movement $R_A^\varphi \circ R_B^{-\varphi}$ is always a parallel translation.

To solve the next exercise, you will find the following fact useful: *the angle between the lines l and m is equal to the angle between $R_A^\varphi(l)$ and $R_B^\varphi(m)$.* Indeed, rotations preserve the angles, hence the angle between l and m equals the angle between $R_A^\varphi(l)$ and $R_A^\varphi(m)$ — and the two lines $R_A^\varphi(m)$ and $R_B^\varphi(m)$ are parallel.

Exercise 100. Let BE and CF be the altitudes of the triangle ABC and O the centre of the circumscribed circle. Prove that $AO \perp EF$.

Exercise 101. The *determinant* of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is the number $ad - bc$. The *product* of two matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\begin{pmatrix} m & n \\ p & q \end{pmatrix}$ is the matrix $\begin{pmatrix} am+bp & an+bq \\ cm+dp & cn+dq \end{pmatrix}$. Prove that the set of all matrices with non-zero determinant forms a group, and the determinant is a homomorphism of this group onto the group of non-zero numbers with multiplication.

5.2 Quotient group

Let us look the group of residue classes $\mathbb{Z}_m$ and the homomorphism $\mathbb{Z} \to \mathbb{Z}_m$ from a more general viewpoint. The group $\mathbb{Z}_m$ consists of the cosets of the group $\mathbb{Z}$ modulo the subgroup $m\mathbb{Z}$. This fact can also be stated in the form *$\mathbb{Z}_m$ is the quotient group of $\mathbb{Z}$ modulo $m\mathbb{Z}$*, which is written as $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.

Now let G be an arbitrary group and H a subgroup of G. Consider the set of cosets in G modulo H and try to make it into a group, using the construction of $\mathbb{Z}_m$ as an example. The first question that arises is: what cosets should we use, left cosets eH, g_1H, g_2H, ... or right cosets He, Hg_1, Hg_2, ...? This question does not exist for the group $\mathbb{Z}$, since it is commutative.

Recall that the left coset gH is made up of all products gh where $g \in G$ is fixed and h ranges over H, whereas the right coset Hg consists of all products hg. If the group is not commutative, then in general $gH \neq Hg$. For example, take the group of plane movements D_3 as the whole group G and the subset $H = \{\mathrm{id}, S_a\}$ as the subgroup. Then, using the multiplication table (p. 70), we find that

$$\begin{aligned} RH &= \{R \circ \mathrm{id}, R \circ S_a\} = \{R, S_b\}, \\ HR &= \{\mathrm{id} \circ R, S_a \circ R\} = \{R, S_c\}. \end{aligned}$$

However, for the subgroup $C_3 = \{\mathrm{id}, R, R^2\}$ both the left and the right coset decompositions consist of the same two classes: the subgroup C_3 itself and its complement $D_3 \setminus C_3$.

Definition 17 *A subgroup H of a group G is called normal, if for any element $g \in G$ the two cosets gH and Hg coincide.*

If $H \subset G$ is normal, then the following train of equalities is true:

$$(g_1H)(g_2H) = g_1(Hg_2)H = g_1(g_2H)H = g_1g_2H,$$

meaning that if you choose any element of the coset g_1H and any element of the coset g_2H, then their product will belong to one and the same coset $(g_1g_2)H$. Therefore, in the set of cosets over a normal subgroup there is a well defined multiplication: $\bar{g}_1\bar{g}_2 = \overline{g_1g_2}$, where the bar over a letter denotes the coset of an element over the given normal subgroup: $\bar{g} = gH = Hg$. It is evident that this operation is associative; the role of unit element is played by the coset $H = eH$, and the element inverse to gH is $g^{-1}H$. The set of cosets H, g_1H, g_2H, ... thus acquires the structure of a group.

Definition 18 *Let G be a group and H its normal subgroup. The quotient group of G over H, denoted by G/H, is the set of all cosets over H with the product of two cosets given by the rule $\bar{g}_1\bar{g}_2 = \overline{g_1 g_2}$.*

The structure of the quotient group G/H can be read off the multiplication table of G, if the elements in the first row and and the first column of the table are arranged by cosets. Look, for example, at the multiplication table of the group D_3 (p. 70). You can clearly see that the table is split into 4 blocks of the size 3×3 each. Denoting the block that corresponds to rotations by R and the block that corresponds to reflections, by S, we can represent the block structure of the whole table as

	R	S
R	R	R
S	S	R

This table defines a cyclic group of order 2 isomorphic to $\mathbb{Z}_2$. Thus, we can write $D_3/C_3 \cong \mathbb{Z}_2$, where the sign $\cong$ stands for isomorphism.

Problem 40 *Let G be the group of proper movements of the plane, consisting of all rotations and all translations. Denote by N the subgroup of rotations around a fixed point A and by K the subgroup of all translations. Determine whether these subgroups are normal and, if appropriate, find the structure of the quotient groups.*

Solution. The condition of normality $gH = Hg$ can be rewritten as $gHg^{-1} = H$ which means that a subgroup H is normal if and only if, together with every its element, it contains all the conjugate elements. Since conjugation is looking at things from a different viewpoint (see p. 63), a subgroup is normal whenever it looks the same from any standpoint. It is clear that, for a person living in the plane, the set of all translations looks the same, whatever his position be. However, the set of rotations with a fixed centre A looks different for a person placed at A and for a person placed at a different point. Therefore, the subgroup K is normal, whereas the subgroup K is not.

A more rigorous proof of this fact can be obtained, using the result of Exercise 58 (p. 177). The movement conjugate to a translation is always a translation, therefore K is normal. The movement conjugate to a rotation around A by a movement f is a rotation around $f(A)$, therefore N is not normal.

Since $K \subset G$ is normal, the quotient group G/K is defined. To understand its structure, consider the homomorphism $\varphi : G \to T$ studied above in Problem 39. We claim that two elements of G have the same image under φ if and only if they belong to the same coset of G with respect to K. Indeed, let $\varphi(f) = \varphi(g) = p \in T$. If $p = 1$, then both f and g are translations and belong to K. If $p = \cos\alpha + i\sin\alpha \neq 1$, then both f and g are rotations through the angle α, say, $f = R_A^\alpha$ and $g = R_B^\alpha$. In this case $f = R_A^\alpha = R_B^\alpha \circ (R_B^{-\alpha} \circ R_A^\alpha) \in gH$, because $R_B^{-\alpha} \circ R_A^\alpha$ is a translation. Conversely, if f and g belong to one coset over K, then $f = g \circ h$ and $\varphi(f) = \varphi(g)$.

The property that we have just proved implies that φ establishes a one-to-one correspondence between the sets G/K and T which we can denote by $\bar{\varphi}$. The mapping φ obviously agrees with the group operations and thus yields an isomorphism $\varphi : G/K \to T$. The quotient group G/K is thus the same thing as the group of complex numbers with unit modulus or the group of all rotations with a common centre.

Note that the coset decomposition of G over K has a simple geometric meaning: every coset consists of rotations through the same angle around an arbitrary centre. The subgroup K itself (the set of all translations) is the unit coset — it corresponds to the unit of the group T under φ.

Generalizing this argument, we arrive at the following assertion called the *first homomorphism theorem.*

Theorem 10 *If φ is a homomorphism of a group G onto a group H and $K \subset G$ is its kernel, i.e. the set of all elements of G that go into the unit of H under φ, then $G/K \cong H$.*

Note that the kernel K of any homomorphism φ is always a normal subgroup in G, so that the quotient G/K is correctly defined. Indeed, if $k \in K$, then $\varphi(k) = e$, hence $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)e\varphi(g^{-1}) = e$, which means that $gkg^{-1} \in K$.

The first homomorphism theorem implies that the orders of the three groups G, H and K are related by the simple equality $|G| = |H| \cdot |K|$. In particular, we have the following corollary: *if there exists a homomorphism of finite groups $G \to H$, then the order of H is a divisor of the order of G.*

Exercise 102. Is there a homomorphism (a) of D_3 onto $\mathbb{Z}_2$? (b) of D_3 onto $\mathbb{Z}_3$?

Problem 41 *Find the kernel of the homomorphism $\varphi : S_4 \to \Phi$ discussed in Problem 38.*

Solution. Let $K \subset S_4$ be the kernel of φ. Since φ is a surjective homomorphism, i.e. its image coincides with the entire group Φ, the groups S_4/K and Φ are isomorphic and hence $|K| = 24 : 6 = 4$. It is easy to check that the following four permutations:

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}.$$

leave invariant the expression

$$x = \frac{a-c}{b-c} : \frac{a-d}{b-d}.$$

The multiplication table for these four elements coincides, up to the choice of notations, with the multiplication table of the group D_2. Thus, $K \cong D_2$ and the homomorphism theorem in our example can be written as $S_4/D_2 \cong D_3$.

Exercise 103. Find the image and the kernel of the homomorphism of the additive group of functions $f : \mathbb{R} \to \mathbb{R}$ into itself given by the formula $f(x) \mapsto f(x) + f(-x)$.

Exercise 104. Let S be the group of rotations of the plane with a fixed centre and C_n, its cyclic subgroup of order n. Prove that $S/C_n \cong S$.

Exercise 105. Using the first homomorphism theorem, represent the group S of the previous exercise as a quotient group of $(\mathbb{R}, +)$.

5.3 Groups presented by generators and relations

We are now in a position to explain the construction of an abstract group with a given set of generators and defining relations. Before (page 71 in Chapter 3) we have already talked about generators and relations in a given, already defined group. The current problem is inverse: now we want to *define* a group, starting from an arbitrary set of generators and relations between them.

This definition relies on the notion of the quotient group that we have just studied and the notion of a free group that we will now define.

Definition 19 *Let S be an arbitrary set, consisting of letters in a certain alphabet. The free group over S, denoted by $F(S)$, consists of all monomials over S (see page 71), the group operation being given by writing two monomials side by side and using the simplification rules $s^k s^l = s^{k+l}$ and $s^0 = 1$.*

For example, if S consists of one element, then $F(S)$ is the infinite cyclic group.

Definition 20 *Let R be a set of monomials over S (each monomial r is understood as a relation $r = 1$ between the elements of S). The group with generators and defining relations R is defined as the quotient group $F(S)/H(R)$ where $F(S)$ is the free group over S and $H(R)$ is the minimal normal subgroup of $F(S)$ containing all relations belonging to R (in other words, $H(R)$ is the subgroup of $F(S)$ generated by all elements conjugate to the elements of R).*

An abstract group with generators $s_1, \ldots, s_n$ and relations $r_1, \ldots, r_m$ is denoted by

$$\langle\, r_1, \ldots, r_m \,|\, r_1, \ldots, r_m \,\rangle$$

(Relations on the right are sometimes written simply as monomials over S, each monomial r meaning the equality $r = 1$).

For example, it is easy to understand that

$$\langle\, a \,|\, a^n = 1 \,\rangle$$

is the cyclic group of order n.

Problem 42 *Prove that the group*

$$\langle\, a, b \,|\, ab = 1 \,\rangle$$

is the infinite cyclic group, isomorphic to the additive group of all integers $\mathbb{Z}$.

> **Solution.** The free group $F(a,b)$ consists of all words $a^{k_1}b^{l_1}\dots a^{k_n}b^{l_n}$ of an arbitrary length and with arbitrary integer exponents. To obtain the quotient group, such words should be considered modulo the elements of the subgroup $H(R)$: if $x = yh$ or $x = hy$ where $h \in H(R)$, then x and y belong to one and the same coset. Now, $a = (ab)b^{-1}$, therefore, a is equivalent to b^{-1} and hence every word in a and b is equivalent to some word in b only. We see that every element of the quotient group $F(S)/H(R)$ is a power of $\bar{b}$, so that this group is cyclic.
>
> Note that in every element of the subgroup $H(R)$ the sum of all exponents of a is equal to the sum of all exponents of b, therefore b^n with $n \neq 0$ cannot belong to $H(R)$, which means that all powers of $\bar{b}$ are different. The group $F(S)/H(R)$ is thus infinite.

Remark. In the above argument, the generators a and b play symmetrical roles, because the product ba is conjugate to ab: $ba = a^{-1}(ab)a$ and therefore belongs to the subgroup $H(R)$ — this is one of the reasons why in definition 20 the subgroup $H(R)$ is set to be the *normal* subgroup generated by R.

Exercise 106. What is the group presented by

$$\langle\, a, b \,|\, a^2 = 1,\ b^n = 1,\ aba = b^{-1} \,\rangle\,?$$

Exercise 107. Prove that

$$\langle\, a, b \,|\, aba = bab \,\rangle \cong \langle\, x, y \,|\, x^2 = y^3 \,\rangle\,.$$

5.4 Group actions and orbits

Group actions can be defined in terms of homomorphisms as follows.

Definition 21 *Let G be a group and X be a set. An action of G on X is a homomorphism of the group G into the group of transformations of the set X (see p. 59):*

$$T : G \to \mathrm{Tr}(X).$$

The image of a point $x \in X$ under the action of the transformation T_g is $T_g(x)$, which is often denoted by gx for short.

We should like to stress from the beginning that a given group G can act on a given set X in a variety of different ways, because in general there may exist many different homomorphisms $G \to \mathrm{Tr}(X)$. For example, the symmetry group of a regular triangle D_3

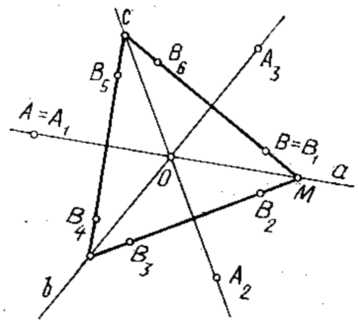


Figure 5.1: Action of the group D_3 on the plane

acts on the plane by definition. However, the action depends on the choice of the regular triangle in question, or more exactly, on the choice of its centre and three symmetry axes.

Figure 5.1 shows a regular triangle with centre O and symmetry axes a, b, c.

Under the action of any element of D_3, the origin (point O) goes into itself. A point lying on one of the lines a, b, c and different from O, gives three different point (including itself). Any other point of the plane gives six different points under the action of the group.

Definition 22 *The set of all points obtained from a given point x under the action of a group, is called the orbit of this point:*

$$\mathcal{O}(x) = \{T_g(x) \mid g \in G\}.$$

The cardinality of the set $\mathcal{O}(x)$ is referred to as the length of the orbit.

In the previous example we had orbits of three different kinds: of length 1, 3 and 6.

It is clear that any point always belongs to its own orbit, because it goes into itself under the action of the neutral element of the group. A point whose orbit consists of only one point is called a *fixed point* of the action. In our example the only fixed point was point O.

Look at Fig. 5.1. The orbit of the point $A = A_1$ consists of three points A_1, A_2, A_3. If you take A_2 or A_3 as the initial point, you will get the same orbit. This is a manifestation of the general property: *the orbit of any point belonging to the orbit of a point x coincides with $\mathcal{O}(x)$.* Indeed, if $y \in \mathcal{O}(x)$, then $y = hx$ for a certain group element $h \in G$. Then $\mathcal{O}(y) = \{gy|g \in G\} = \{ghx|g \in G\}$, but the axioms of the group imply that, for any fixed element $h \in G$, the set of all products gh where g ranges through G, coincides with the set G.

This observation implies the following important fact: *any two orbits either coincide or do not have common elements.* In fact, if two orbits $\mathcal{O}(x)$ and $\mathcal{O}(y)$ have a common element z, then $\mathcal{O}(x) = \mathcal{O}(z) = \mathcal{O}(y)$.

The meaning of the word *orbit* and the splitting of the set into orbits can be very clearly seen for the action of the circle S, understood as the multiplicative group of complex numbers with modulus 1, on the complex plane by means of multiplication (Fig. 5.2). This

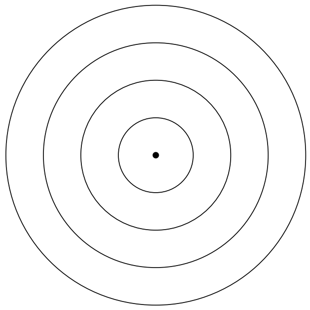


Figure 5.2: Orbits of the group S

action has one fixed point (number 0), while the rest of the plane splits into concentric circles which are the orbits.

Exercise 108. Let D_3 be the symmetry group of a regular triangle in the complex plane, whose centre is at the origin and one of the symmetry axes is axis x. Consider the action of this group on the finite set $\{0, 1, -1, 2, -2, i\sqrt{3}, -i\sqrt{3}, 4, -4, 2+2i\sqrt{3}, 2-2i\sqrt{3}, -2+2i\sqrt{3}, -2-2i\sqrt{3}, \}$. Find the orbits of this action.

Problem 43 *Define a natural action of the group of rational expressions Φ (Exercise 74) on a suitable set.*

Solution. A rational expression in one variable can be considered as a function, i.e. as a mapping of the real line into itself. Unfortunately, these mappings are not defined at all points of the real line $\mathbb{R}$, because the denominators sometimes become zero. There are two natural ways to mend this situation. One is to exclude the two points 0 and 1 from $\mathbb{R}$ (note that these are the only values of x where the denominators may vanish). Another one is to add one extra point ∞ to $\mathbb{R}$ and extend the functions to this point according to the rule:

	F_1	F_2	F_3	F_4	F_5	F_6
0	∞	1	0	1	∞	0
1	1	0	1	∞	0	∞
∞	0	∞	∞	0	1	1

This table defines a genuine action of the group Φ on the set $\mathbb{R} \cup \infty$. It shows, in particular, that the three points 0, 1 and ∞ form one orbit and that the action of Φ on this orbit defines the isomorphism of Φ with the permutation group on three symbols S_3.

Exercise 109. Find one more 3-element orbit of this action and prove that all the remaining orbits consist of 6 elements.

Exercise 110. Functions $F_i \in \Phi$ can also be considered as functions of a *complex* variable. Therefore, the action of the group Φ can be prolonged to the set $\mathbb{C} \cup \infty$. Find a 2-element orbit of this action and prove that all the other orbits, except this one and the two 3-element orbits indicated above consist of 6 elements.

5.5 Enumeration of orbits

Consider one more example of a group action.

Problem 44 *Let Q be a cube in space and G the group of all space rotations that take Q into itself (i.e. the proper symmetry group of Q). Make up the list of all elements of G and describe the action of this group on the set of faces of the cube.*

Solution. Apart from the identity, the group G contains:

- 6 rotations through 180° around the lines that go through the midpoints of two parallel edges (like AA' in Fig. 5.3),
- 3 rotations through 180° around the lines connecting the midpoints of two opposite faces (like BB'),
- 6 rotations through 90° around the same lines, and
- 8 rotations through 120° around the lines that contain a pair of opposite vertices of the cube (like CC').

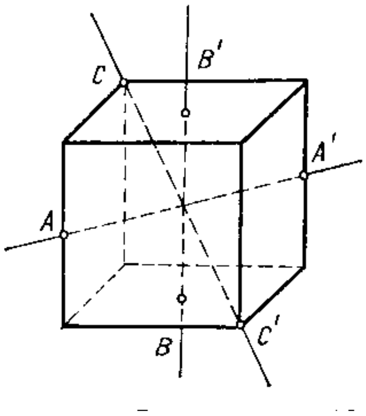


Figure 5.3: Rotations of the cube

The group G thus consists of 24 elements.

The natural action of the group G on the set of faces F of the cube is *transitive*, i.e. any face can be taken into any other by a suitable element of the group. In other words, the set F, which consists of 6 points, makes one orbit of the group action. For any face $f \in F$ there are exactly 4 rotations that preserve it: the identity and the three rotations around the line passing through the midpoint of this face. Note that $6 \cdot 4$ gives 24, the order of the group.

Exercise 111. Describe the action of G on the set of edges E and on the set of vertices V.

So far, we have found transitive actions of the group G on the sets of order 6, 8 and 12. Note that all these numbers are divisors of 24, the order of the group. The number 24 has some more divisors, and it turns out that for every divisor one can construct a set of corresponding cardinality that consists of certain geometric elements of the cube and on which our group acts transitively. Figure 5.4 shows the sets of 4, 3 and 2 elements endowed with a natural transitive action of our group: these are the set D of big diagonals, the set M of middle lines and the set T of regular tetrahedra inscribed in the cube.

Definition 23 *A set with a transitive action of a group is called a homogeneous space of this group.*

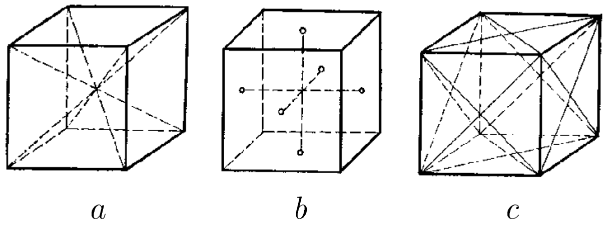


Figure 5.4: Homogeneous spaces of the symmetry group of the cube

In each of these cases we have a homomorphism of the group G into the group of transformations of the corresponding set.

Exercise 112. For which of the sets F, E, V, D, M, T this homomorphism is (a) an epimorphism? (b) an isomorphism?

We can also consider the action of the group G on more complicated objects that consist of several elements of the above sets.

Problem 45 *Describe the orbits of the action of our group G on the set of all pairs (f, e) where $f \in F$ is an arbitrary face, while $e \in E$ is an arbitrary edge of the cube Q.*

Solution. The set in question can be denoted as $F \times E$ (the Cartesian product of the sets F and E). It consists all in all of $6 \cdot 12 = 72$ elements which come in three different categories: the edge e can either belong to the face f (as in Fig. 5.5a), have one common vertex with f (as in Fig. 5.5b) or, finally, have no common points with f (Fig. 5.5c).

It is clear that a pair edge–face belonging to one of these types cannot go into a pair of another type under any movement. Let us prove that any two pairs of the same type can be transformed one into another by a suitable movement. Suppose that we are given two pairs (f_1, e_1), (f_2, e_2) of the first type (edge lies in the face).

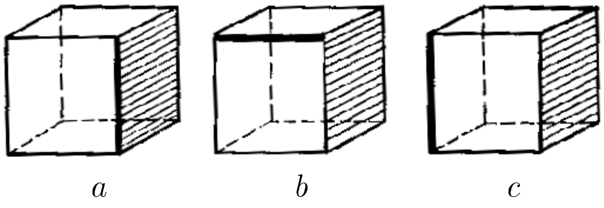


Figure 5.5: Different pairs face–edge

First we find a rotation which takes f_1 into f_2. Then, using the 4 rotations that preserve this face, we can move e_1 to the position of e_2, and that's all. The two other cases are treated similarly.

We have thus proved that the set $F \times E$ with the action of the group G consists of three orbits, whose typical representatives are shown in Fig. 5.5.

Exercise 113. Find the number of orbits and indicate their representatives for the action of G on the following sets: (a) $V \times F$ (pairs vertex–face), (b) $D \times F$ (pairs diagonal–face), (c) $E \times E$ (ordered pairs of edges).

Let us now generalize the observations that we have made during the previous discussion. To do so, we will need the notion of the *stabilizer*, or *stable subgroup*, of a point.

Definition 24 *Given an action of a group G on the set X, the stabilizer of a point $x \in X$ is the set of all elements of G that preserve the point x:*

$$\mathrm{St}(x) = \{g \in G \mid T_g(x) = x\}.$$

The stabilizer is a subgroup in G. Indeed, if both g and h are in $\mathrm{St}(x)$, then we have: $T_{gh}(x) = T_g(T_h(x)) = T_g(x) = x$ and $T_{g^{-1}}(x) = T_g^{-1}(x) = x$.

The stabilizer of a fixed point coincides with all of the group G. For example, look at Fig. 5.1. The stabilizer of O is all group, the stabilizer of the point A consists of two elements (identity and reflection), while the stabilizer of the point B is trivial (contains only the identity).

You can here notice the same rule that we saw in Problem 44: the order of the stable subgroup multiplied by the length of the corresponding orbit always gives the order of the whole group:

$$|\mathcal{O}(x)| \cdot |\mathrm{St}(x)| = |G|. \tag{5.3}$$

To prove this fact, consider the left coset decomposition of the group G with respect to the subgroup $H = \mathrm{St}(x)$:

$$G = g_1H \cup g_2H \cup \ldots \cup g_kH.$$

All the elements of the same coset act on x in the same way: if $h \in H$, then $T_{gh}(x) = T_g(T_h(x)) = T_g(x)$, which does not depend on the specific choice of h. Vice versa, if two elements $g, k \in G$ move the point x to the same position, then they belong to one and the same coset. Indeed, there is an element $h \in G$ such that $k = gh$. Then

$$T_h(x) = T_{g^{-1}k}(x) = T_g^{-1}T_k(x) = x,$$

which means that $h \in \mathrm{St}(x)$. Therefore, the number of different points in the orbit of x is the same as the number of cosets in the decomposition $G/\mathrm{St}(x)$, and the assertion follows.

Formula 5.3 shows, in particular, that the stabilizers of all the points that belong to the same orbit have the same number of elements. In fact, these subgroups are always conjugate to each other in the group G and hence isomorphic.

To prove this fact, take two arbitrary points x and y that belong to one and the same orbit. Then there is a group element g such that $y = T_g(x)$. We claim that the subgroups $\mathrm{St}(x)$ and $\mathrm{St}(y)$ are conjugate by the element g. Indeed, if $h \in \mathrm{St}(x)$, then

$$T_{ghg^{-1}}(y) = T_g(T_h(T_g^{-1}(y))) = T_g(T_h(x)) = T_g(x) = y$$

which means that $ghg^{-1} \in \mathrm{St}(y)$ and, since h is arbitrary, this implies that $g\,\mathrm{St}(x)g^{-1} \subset \mathrm{St}(y)$. Interchanging the roles of x and y in the previous argument proves the inverse inclusion, thus $g\,\mathrm{St}(x)g^{-1} = \mathrm{St}(y)$, and the two subgroups are indeed conjugate.

Problem 46 *How many different ways are there to paint the disk divided into p equal parts using n colours? The number p is supposed to be prime. Two colourings are considered to be the same, if one of them goes into another by a rotation of the disk.*

> **Solution.** We deal with the action of the cyclic group C_p on the set of all possible n^p colourings of the disk, and we are asked to find the number of orbits of this action. The length of the orbit, which is always a divisor of the order of the group, in this example can take only two values: 1 and p, because p is prime. An orbit of length 1 corresponds to a colouring which is invariant under all rotations, i.e. a colouring where the whole disk is coloured with one colour. The total number of such colourings is n. The remaining colourings, whose total number is $n^p - n$, split into orbits of cardinality p, and the number of the orbits is $(n^p - n)/p$. The total number of orbits, i. e the number of different ways to colour the disk, is thus $(n^p - n)/p + n$.

Note that we have proved, as a byproduct, that the number $n^p - n$ is always divisible by p, if p is prime. This is yet another proof of Fermat's little theorem 4.6.

Exercise 114. Try to solve the same problem in the case when p is not necessarily prime.

It is rather difficult to solve this exercise by a direct argument, like the one we used in the previous problem. However, there exists a general formula that computes the number of orbits for any group action — the so called *Burnside formula*, which we shall now state and prove.

If $g \in G$ is an element of the group acting on a set X, then we denote by $N(g)$ the number of fixed points of the corresponding transformation T_g, i.e. the number of points $x \in M$ such that $T_g(x) = x$.

Exercise 115. Under the central symmetry (rotation through 180°) digits 0, 1 and 8 are preserved, digits 6 and 9 change places, while all the remaining digits lose their meaning. How many 5-digit numbers are centrally symmetric?

Theorem 11 (Burnside's formula) *The number of orbits r is "the arithmetic mean of the number of fixed points for all elements of the group":*

$$r = \frac{1}{|G|} \sum_{g \in G} N(g),$$

or, in other words, the sum of numbers $N(g)$ for all the elements of the group is $|G|$ times the number of orbits.

Proof To prove the formula, let us think for a while over the following question: *how many times does a given point $x \in M$ participate in the total sum $\sum_{g \in G} N(g)$?*. Evidently, it comes up every time when an element g preserves x. The answer to the question is thus $|\operatorname{St}(x)|$. Other points belonging to the orbit $\mathcal{O}(x)$ appear in the total sum the same number of times, because all the stabilizers have the same cardinality. Therefore, the contribution of this orbit is $|\operatorname{St}(x)| \cdot |\mathcal{O}(x)|$ which, as we know, is equal to $|G|$, the order of the group. Since every orbit gives the same contribution $|G|$, the whole sum is $|G|$ times the number of the orbits, and this is exactly what we wanted to prove.

Let us use Burnside's formula to solve once again Problem 46. Here the identical transformation has n^p fixed points while every non-identical transformation has n fixed points. Therefore, the number of orbits is $r = (n^p + (p-1)n)/p$. It is easy to see that this result does not differ from the one obtained before.

Problem 47 *Find the number of different necklaces made of 7 white and 3 black beads.*

Solution. It is natural to treat two necklaces as equal, if they differ only by a rotation or a reflection of the circle. Therefore, we have to consider the set X whose elements are all possible dispositions of 7 white and 3 black beads in the vertices of a fixed regular 10-gon and the action of the dihedral group D_{10} on X. The problem is to find the number of orbits of this action.

Having in mind Burnside's formula, let us calculate the number of fixed points in X for every element of the group D_{10}. For the identical transformation, all $\binom{10}{3} = 120$ points of the set X are fixed.

A nontrivial rotation cannot leave any necklace invariant. The same is true for the reflections of type (a) (see Fig. 5.6), because the number of beads of each colour is odd. But the reflections of type (b) do have invariant necklaces. For every such reflection there are $2 \cdot 4 = 8$ such necklaces: first, one of the beads on the symmetry axes must be white and another one black, second, one of the four symmetrical pairs of beads must be black. The number of reflections of type (b) is 5, and by Burnside's formula we get: $r = (120 + 5 \cdot 8)/20 = 8$.

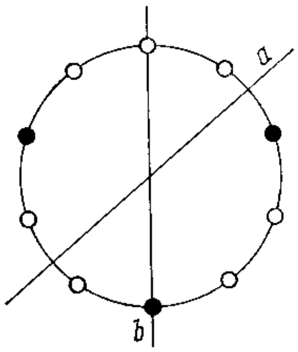


Figure 5.6: A necklace of type 3-7

Exercise 116. Solve the last problem in the case of 6 white and 4 black beads.

Exercise 117. A *dice* is a cube marked on each side with numbers 1 through 6. How many different dice are there? (Two dice are regarded as the same, of they can be so rotated in space that the numbers on corresponding sides become equal.)

Exercise 118. How many different ways are there to paint (a) the vertices, (b) the edges of a cube by two colours (i.e. using no more than two given colours)? (Here, like in the previous exercise, only proper rotations should be considered.)

Exercise 119. How many different hexagons can be inscribed into a given 15-gon? (Two figures are equal, if they coincide after a plane movement, not necessarily proper.)

5.6 Invariants

The problem about necklaces can be solved by a simple direct argument, without referring to group theory and Burnside's formula. The most natural solution can be stated as follows.

The three black beads break the circle into three parts, which contain m, n and k white beads. The integers m, n and k are between 0 and 7, inclusive, and satisfy $m + n + k = 7$. Note that the order in which these three numbers appear is in our case irrelevant, because rotations and reflections produce any of the 6 possible permutations. (For the case of 4 black beads this observation would no longer be true!) Therefore, we can assume that $m \leq n \leq k$ and the problem is reduced to the enumeration of all triples of integers that satisfy all the stated restrictions. All such triples can be found directly. Here they are, in lexicographic order: $(0, 0, 7)$, $(0, 1, 6)$, $(0, 2, 5)$, $(0, 3, 4)$, $(1, 1, 5)$, $(1, 2, 4)$, $(1, 3, 3)$, $(2, 2, 3)$.

Why is it that the triple (m, n, k) can serve for the enumeration of orbits? Because it satisfies the following two properties:

- first, if two necklaces are the same (belong to the same orbit), then the corresponding triples are equal,
- second, if the triples of two necklaces are equal, then the necklaces themselves are equivalent.

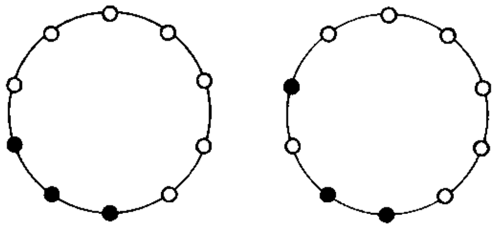


Figure 5.7: Invariant of a necklace

The first property can also be expressed in the following way: the values of m, n and k are constant on the orbits of the action.

Consider the general situation. Suppose that the group G acts on the set X.

Definition 25 *A mapping φ from X into a certain set N is called an invariant of the action, if the values it takes on the elements of the same orbit are always equal.*

Invariants may take values in arbitrary sets. In the previous example, the set N consisted of unordered triples of integers. The least of these three numbers (denoted above by m) is also an invariant of the group action under study. However, this invariant does not possess the second property: for example, the two necklaces shown in Fig. 5.7, are different, but the values of m for them are the same. Such an invariant cannot be used to distinguish different orbits.

Definition 26 *An invariant $\varphi : X \to N$ is said to be complete, if it takes different values on different orbits.*

Exercise 120. Construct a complete invariant for necklaces with 4 black and 6 white beads.

Let $\mathcal{M}$ be the group of all plane movements. This group acts on the plane in a natural way. This action is transitive, thus the plane is a homogeneous space of the group $\mathcal{M}$. Invariants of this action present no interest: these are only constant mappings.

The group $\mathcal{M}$ also acts on the set of all straightline segments in the plane. This action is not trivial. Two segments belong to one orbit, if and only if their lengths are equal. The length of the segment is thus a complete invariant of this action.

Exercise 121. Indicate some complete invariants for the action of the group G of plane movements on the set of (a) all triangles, (b) all quadrangles.

If $H \subset G$ is a subgroup, then it also acts on the plane. If H is small enough, then its orbits cannot be big and therefore the action might have nontrivial invariants. For example, if H is the group of rotations around a point A, then its orbits are circles centred at A. The distance of a point from A is the complete invariant of this action. In the polar system of coordinates with centre A (see p.26), the distance is the polar coordinate r, and every invariant has the form $f(r)$, i.e. is a function of the complete invariant.

Consider the action of the dihedral group D_3 on the plane (see Fig. 5.1). Let O be the polar centre and OM the polar axis. The polar distance r is an invariant of this action. But it is not a complete invariant. To make it complete, we will add one more function to r. Note that the function $\cos\varphi$ is an invariant of the group D_3. Indeed, the group is generated by the reflection $\varphi \mapsto -\varphi$ and the rotation $\varphi \mapsto \varphi + 120^\circ$, and the expression $\cos 3\varphi$ does not change under these transformations. The pair of numbers $(r, \cos 3\varphi)$ makes a complete invariant of the action. Indeed, it is easy to check that the simultaneous equations

$$\begin{aligned} \cos 3\varphi &= b, \\ r &= c \end{aligned}$$

for any real $c > 0$ and $|b| \leq 1$ may have 3 or 6 solutions that correspond to the points of one orbit.

5.7 Crystallographic groups

We now have all the techniques necessary to revisit the question about the symmetry of ornaments posed in the introduction (see page 5). The symmetry of ornaments — plane patterns infinitely repeated in two different directions — is described by the so called *plane crystallographic groups*. An example of such a group is the rolling group of the regular triangle studied in Problem 27 — it describes the symmetry of the ornament shown in Fig. 3.1b. Crystallographic groups are also referred to as *wallpaper groups*.

The exact definition reads as follows.

Definition 27 *A crystallographic group is a discrete group of plane movements that has a bounded fundamental domain.*

We will explain the two terms that appear in this definition.

Definition 28 *A group of plane movements G is said to be discrete, if every orbit is a discrete set in the plane, i.e. for every point A there is a disk centred at A and containing no other point of the same orbit.*

A simple example of a discrete group is provided by the cyclic group generated by one translation. On the contrary, the group containing two translations with collinear vectors of incommensurable lengths is not discrete, because the orbit of every point A is a dense subset of the line passing through A in the direction of the translations.

Exercise 122. Prove that the group generated by a rotation through α degrees is discrete if and only if the number α is rational.

Exercise 123. Prove that the stabilizer of any point with respect to a discrete group of plane movements is finite.

The second notion that needs explanation is that of a *fundamental domain*.

Definition 29 *A domain*[1] *F is said to be fundamental for the group G, if*

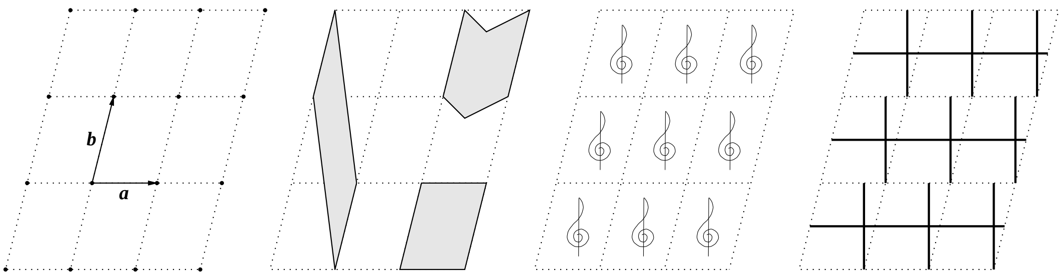
- *Any point in the plane belongs to the orbit of some point $x \in F$ (which can also be a boundary point).*
- *No two different inner points of F belong to the same orbit.*

These two properties mean that the images of the domain F under the group transformations are all distinct (with the exception of boundary points) and fill the plane without overlapping. Another wording is that we have a *tiling*, or *tessalation*, of the plane by the copies of the figure F. For example, the rolling group of the regular triangle (Problem 27) is crystallographic, and the initial triangle can be chosen as its fundamental domain. The assertion claimed in the statement of this problem, is exactly the second property in the definition of a fundamental domain.

Exercise 124. Find the fundamental domains for the groups C_n and D_n.

The term "crystallographic" has its origin in the fact that discrete groups of *space* movements are used to describe the symmetry of natural crystals. There exists a special universal system of notations for the crystallographic groups, both plane, and spacious. For example, the rolling group of the regular triangle is traditionally denoted by $p3m1$. We will give some more examples of crystallographic groups and corresponding ornaments.

The simplest such group, denoted by $p1$, is the group generated by two translations by non-collinear vectors **a** and **b**. Fig. 5.8a shows the generators of the group and the orbit of a point.



a b c d

Figure 5.8: The simplest crystallographic group

As a fundamental domain, one can take the parallelogram with sides **a** and **b**. The fundamental domain can be chosen in a variety of ways. Figure 5.8b shows several different fundamental domains for the same group $p1$. Two of these domains are parallelograms, while the third one is a hexagon. The sides of the parallelogram 1 are $\mathbf{b} - \mathbf{a}$ and $\mathbf{b}$; the sides of the parallelogram 2 are $\mathbf{a} + 2\mathbf{b}$ and $2\mathbf{a} + 3\mathbf{b}$.

[1]It would take some effort to give an exact meaning of the notion of domain. However, it is safe to substitute everywhere in this section the word "domain" by the word "polygon".

Exercise 125. Prove that the parallelogram with sides $k\mathbf{a} + l\mathbf{b}$ and $m\mathbf{a} + n\mathbf{b}$, where k, l, m, n are integers, is a fundamental domain if and only if $|kn - lm| = 1$.

The group $p1$, simplest among all ornamental groups, describes the purely translational symmetry of an ornament. An ornament has symmetry $p1$, if it has no other symmetries other than translations. It is very easy to invent such an ornament. All you have to do is draw an arbitrary figure with a trivial symmetry group, lying inside the fundamental parallelogram, and consider the union of all the copies of this figure obtained by parallel translations of the given group (Fig. 5.8c).

If the chosen figure lies strictly inside the parallelogram, then the ornament obtained has symmetry group exactly equal to $p1$. However, if you allow the figure to touch the border, then it may happen that the obtained ornament may have a wider symmetry group. An example of this phenomenon is shown in Fig. 5.8d.

The group $p1$ is important not only because it is the simplest crystallographic group in the plane, but also because of the following fact.

Lemma 1. *Every plane crystallographic group contains a subgroup of type $p1$, i.e. generated by two non-collinear translations.*

Proof A crystallographic group must contain at least one translation, otherwise it will reduce to a finite group.

Suppose that G is a discrete group of plane movements such that all the translations belonging to G have the same direction (say, parallel to the line l). We are going to prove that the fundamental domain of the group G cannot be bounded in this case.

Let us think a little while what movements, other than rotations, can belong to the group G. Note first that the axes of all glide symmetries that belong to G must also be parallel to the line l — because the square of a glide symmetry is a translation. The rotations that belong to the group can only be rotations through 180°, because, if $R_\varphi \in G$ and $\varphi \neq 180°$, then, together with every translation $T_\mathbf{a} \in G$ the group also contains the translation $R^\varphi \circ T_\mathbf{a} \circ R^{-\varphi}$, non-collinear with $T_\mathbf{a}$ (see the answer to Exercise 58). The composition of two rotations by 180° is a translation along the line that connects their centres. Therefore, the centres of all rotations that belong to G must lie on one line parallel to l. Without loss of generality, we can assume that l is the line that passes through the centres of all rotations. Finally, we leave it to the reader as an exercise to find out what kind of reflections our group may contain.

Exercise 126. Prove that the group G may contain only the reflections whose axis are perpendicular to l or coincide with l.

From all the observations made, we can conclude that two points can belong to one orbit only if their distances from the line l are equal. The fundamental domain must contain one point of each orbit, therefore it cannot be bounded, and the group G is non-crystallographic.

We have thus proved that every ornamental group G contains two non-collinear translations and hence a subgroup of type $p1$ that they generate. In fact, a stronger assertion holds.

Lemma 2. *The set of all translations belonging to G is a group of type $p1$.*

This lemma is an immediate consequence of the following exercise.

Exercise 127. Prove that every ornamental group that consists only of translations is generated by two non-collinear translations.

In a certain sense, any ornamental group is reduced to the group $p1$ and a finite group of plane movements. We will explain how. Let G be an arbitrary ornamental group. Denote by H its subgroup of translations (we already know that it is of type $p1$). The subgroup H is normal in G, because the conjugate of a translation by any movement is always a translation (see page 177).

Lemma 3. *For any crystallographic group G, the quotient group G/H is finite and may only belong to one of the ten types C_n, D_n, where $n = 1, 2, 3, 4, 6$.*

We are not going to prove this fact now. The reader will verify it later, using the table of plane crystallographic groups (Exercise 130). The type of the group G/H is referred to as the *ornamental class* of G.

Let us now discuss the relation between the groups G and H and their fundamental domains in more detail.

If Φ is a fundamental domain of G and g_1, ..., g_k is the complete set of representatives of the coset decomposition G/H, then the union

$$\Pi = \bigcup_{i=1}^{k} g_i \Phi$$

forms a fundamental domain for H. The domain Φ is called the *motif* of the ornament, and the domain Π, its *elementary cell*. In principle, Φ and g_i can always be chosen in such a way that Π becomes a parallelogram, but sometimes it is more convenient to use polygons of another shape, notably, regular hexagons, as the elementary cell.

The ratio of the area of Π to the area of Φ is equal to the index of H in G, i.e. the number of cosets in G/H. The bigger is G/H, the smaller is the fundamental domain Φ in Π.

Problem 48 *Find the motif and the elementary cell of the ornament that has symmetry group of type $p3m1$. Describe the cosets of G with respect to its subgroup of translations H.*

Solution.

Look at Fig. 5.9a which shows an ornament with symmetry group $p3m1$, i.e. the group generated by three reflections in the sides of a regular triangle. (Instead of Fig. 5.9a, we could as well use Fig. 3.1b.) The ornament is obtained by rolling over the triangle MNB (the *motif*) on the plane. You can see from the picture that the ornament admits translations by vectors that connect the points A, B and D. As the elementary cell we can choose, for example, the parallelogram $ABCD$, whose sides $\overrightarrow{AB}$ and $\overrightarrow{AD}$ generate the subgroup of translations H. It is easy to see that $S_{ABCD} : S_{MNB} = 6 : 1$. It is impossible to divide the parallelogram $ABCD$ into six

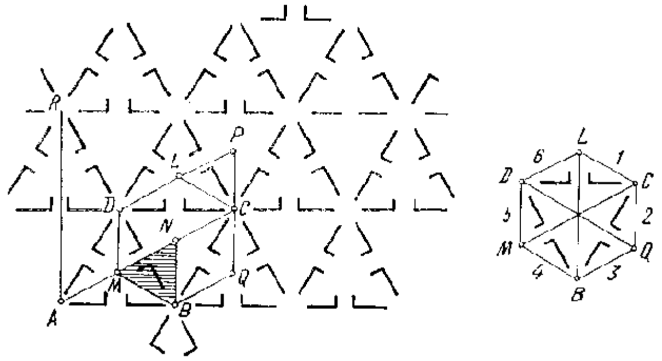


Figure 5.9: An ornament with symmetry group $p3m1$

regular triangles which are the fundamental domains of the ornament (although it is possible to divide it into six fundamental domains of another type — try to do this!). In this case, it is more convenient to choose the fundamental domain for H having the shape of a hexagon, for example $BQCLDM$, which is naturally divided into six fundamental triangles.

To find the number of cosets in G/H let us note that the elements of the subgroup H do not change the relative position of the motif in the plane (the direction and the orientation of the "leg"). Different movements that belong to the same coset, say $g \circ h_1$ and $g \circ h_2$, $h_1, h_2 \in H$, change the relative position of the motif in the same way, because h_1 and h_2 do not change it at all. In the picture, you can see six different positions of the motif, hence the number of the cosets in G/H is six. We can number them from 1 to 6, as in Fig. 5.9b. Then, for example, all the movements belonging to the coset gH, where $g \in G$ is the reflection in a vertical line, induce the following permutation of these numbers: $1 \leftrightarrow 6$, $2 \leftrightarrow 5$, $3 \leftrightarrow 4$.

We have thus arrived at the following conclusion: the quotient group G/H acts on the set of motifs contained in the elementary cell in the same way as the group D_3 acts on the set of vertices of a regular triangle: there are three rotations, including the identity, and three reflections. We can write the result as follows: $G/H \cong D_3$. In the terminology introduced above, this fact can also be stated as follows: the ornamental class of G is D_3.

Note, finally, that writing $p3m1/p1 \cong D_3$ is not correct, because there are many subgroups of type $p1$ contained in the group of type $p3m1$.

Exercise 128. What is the order of the quotient group G/K, where G is the group just studied, and $K \subset H$ is the subgroup of translations generated by $\overrightarrow{AC}$ and $\overrightarrow{AR}$ (see Fig. 5.9a). Describe the structure of this group, in particular find whether it is isomorphic to one of the groups C_n, D_n.

How many different subgroups of types $p1$ are there in the group of plane movements $\mathcal{M}$? Of course, an infinite number: the choice of a specific group is determined by two basic vectors $\mathbf{a}$ and $\mathbf{b}$. However, any two such groups are isomorphic. In fact, a stronger assertion holds: any two such groups are conjugate to each other via a suitable linear transformation (see page 127) of the plane: if H is generated by translations $T_{\mathbf{a}}$ and $T_{\mathbf{b}}$ and K by translations $T_{\mathbf{c}}$ and $T_{\mathbf{d}}$, then $LHL^{-1} = K$, where L is a linear transformation such that $L(\mathbf{a}) = \mathbf{c}$ and $L(\mathbf{b}) = \mathbf{d}$.

Definition 30 *Two groups of plane movements are said to be equivalent, if they are conjugate to each other by a suitable linear transformation.*

We can now state the theorem that gives the exact meaning to the phrase that there are 17 types of wallpaper symmetry.

Theorem 12 (Fedorov–Schönfliess) *Up to the equivalence formulated above, any plane crystallographic group is equivalent to one of the 17 groups given in the table below. These 17 groups are not isomorphic to each other.*

Outline of the proof The proof is not very difficult, but rather lengthy. We are only giving an outline, leaving the details to the industrious reader.

1. Prove that only possible rotations in a crystallographic group are of order 2, 3, 4 or 6.

2. Let $G^+ \subset G$ be the subgroup of all proper (orientation preserving) movements in the group G. Then G^+ is a normal subgroup of index 1 or 2, i.e. the order of G/G^+ is 1 or 2.

3. If $G^+ = G$, i.e. the group consists only of translations and rotations, then it is equivalent to one of the groups $p1$, $p2$, $p3$, $p4$, $p6$, depending on the biggest order of a rotation it contains.

4. If $G^+ \neq G$, then G is generated by the subgroup G^+, which belongs to one of the five types listed above, and one movement f from $G \setminus G^+$. Considering the various possibilities that may arise (f is either a reflection or a glide reflection, its axis may pass or not pass through the centres of rotations etc.), we establish that

   (a) If $G^+ = p1$, then $G = pm$, pg or cm.

   (b) If $G^+ = p2$, then $G = pmm$, pmg, pgg or cmm.

   (c) If $G^+ = p3$, then $G = p31m$ or $p3m1$.

   (d) If $G^+ = p4$, then $G = p4m$ or $p4g$.

   (e) If $G^+ = p6$, then $G = p6m$.

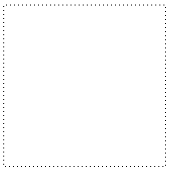
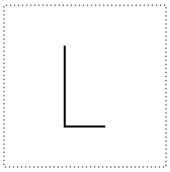
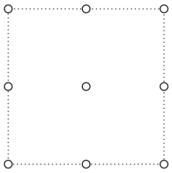
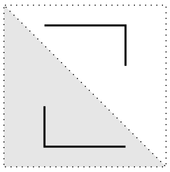
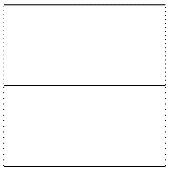
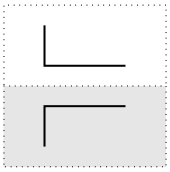
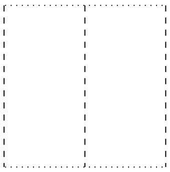
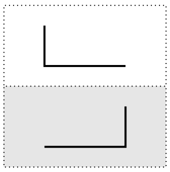
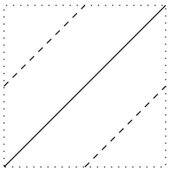
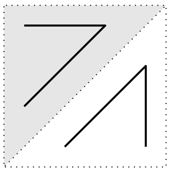
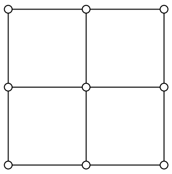
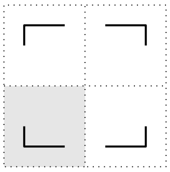
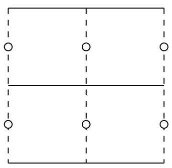
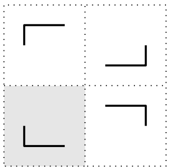
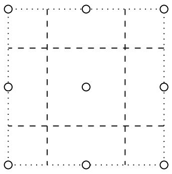
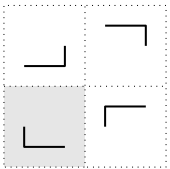
Now, the table. For every group, the table of plane crystallographic groups includes (left to right):

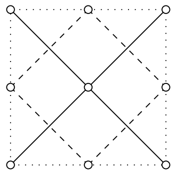
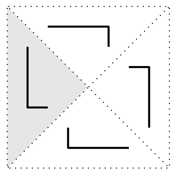
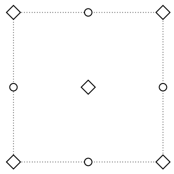
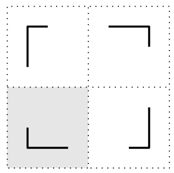
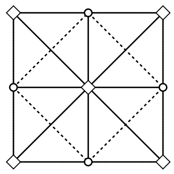
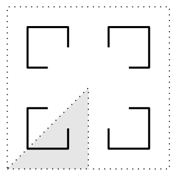
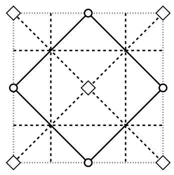
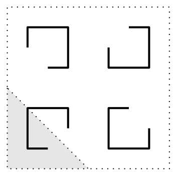
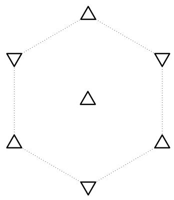
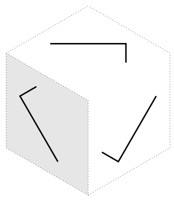
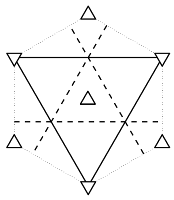
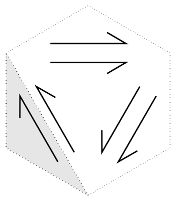
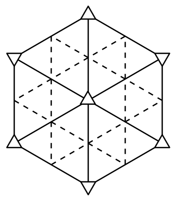
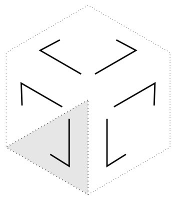
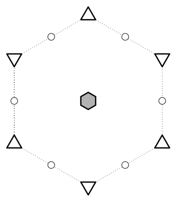
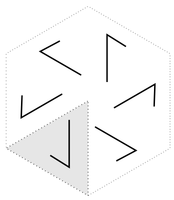
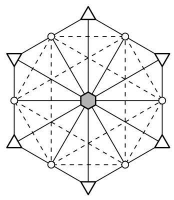
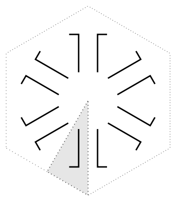
- *Smbl*: The canonical crystallographic notation of the group.
- *Symmetries*: An elementary cell (either a square or a regular hexagon) with the symbols for the movements contained in the group (a solid line means the axis of a reflection, a dashed line means the axis of a glide symmetry, the symbols ○, △, ◇, ⬣ designate the centres of rotation of orders 2, 3, 4 and 6).
- *Sample*: A sample ornament with this symmetry group. The sample shows only one cell of the ornament. The ornament is obtained from the elementary cell by translations in two non-collinear directions. Inside the elementary cell, a fundamental domain is hatched.
- *Generators and relations*: A set of generators and defining relations of the group.

In the table, for the first twelve groups, we give a representative with an elementary cell in the form of a square, and for the remaining five groups, in the form of a regular hexagon. Note that the cell can be an arbitrary parallelogram for groups $p1$ and $p2$, an arbitrary rectangle for groups pm, pg, pmm, pmg, and pgg, and an arbitrary rhombus for groups cm, cmm.

Using this table, the reader can determine the symmetry type of any ornament, starting from the wallpaper design on the walls of his room.

Table of plane crystallographic groups

Smbl	*Symmetries*	*Sample*	*Generators and relations*
p1			Non-collinear translations T_1, T_2 $T_1T_2 = T_2T_1$
p2			Half turns R_1, R_2, R_3 $R_1^2 = R_2^2 = R_3^3 = \mathrm{id}$, $(R_1R_2R_3)^2 = \mathrm{id}$
pm			Reflections S_1, S_2 and translation T $S_1T = TS_1$, $S_2T = TS_2$, $S_1^2 = S_2^2 = \mathrm{id}$
pg			Parallel glide reflections U_1, U_2 $U_1^2 = U_2^2$
cm			Reflection S and glide reflection U $S^2 = \mathrm{id}$, $SU^2 = U^2S$
pmm			Reflections in the sides of a rectangle S_1, S_2, S_3, S_4 $S_1^2 = S_2^2 = S_3^2 = S_4^2 = \mathrm{id}$, $(S_1S_2)^2 = (S_2S_3)^2 = (S_3S_4)^2 = (S_4S_1)^2 = \mathrm{id}$
pmg			Reflection S and central symmetries R_1, R_2 $S^2 = R_1^2 = R_2^2 = \mathrm{id}$, $R_1SR_1 = R_2SR_2$
pgg			Perpendicular glide reflections U_1, U_2 $(U_1U_2)^2 = (U_1^{-1}U_2)^2 = \mathrm{id}$

cmm			Reflections S_1, S_2 and central symmetry R $S_1^2 = S_2^2 = R^2 = \mathrm{id}$, $(S_1S_2)^2 = (S_1RS_2R)^2 = \mathrm{id}$
p4			Central symmetry R and 90° rotation R_1 $R^2 = R_1^4 = (R_1R)^4 = \mathrm{id}$
p4m			Reflections S_1, S_2, S_3 in the sides of an isosceles right triangle $S_1^2 = S_2^2 = S_3^2 = \mathrm{id}$, $(S_1S_2)^2 = (S_2S_3)^4 = (S_3S_1)^4 = \mathrm{id}$
p4g			Reflection S and 90° rotation R $S^2 = R^4 = (R^{-1}SRS)^2 = \mathrm{id}$
p3			Three rotations R_1, R_2, R_3 through 120° $R_1^3 = R_2^3 = R_3^3 = R_1R_2R_3 = \mathrm{id}$
p31m			Reflection R and rotation R through 120° $R^3 = S^2 = (R^{-1}SRS)^3 = \mathrm{id}$
p3m1			Reflections S_1, S_2, S_3 in the sides of a regular triangle $S_1^2 = S_2^2 = S_3^2 = \mathrm{id}$, $(S_1S_2)^3 = (S_2S_3)^3 = (S_3S_1)^3 = \mathrm{id}$
p6			Half turn R and 120° rotation R_1 $R^2 = R_1^3 = (R_1R)^6 = \mathrm{id}$
p6m			Reflections S_1, S_2, S_3 in the sides of a $(30°, 60°, 90°)$ triangle $S_1^2 = S_2^2 = S_3^2 = \mathrm{id}$, $(S_1S_2)^2 = (S_2S_3)^3 = (S_3S_1)^6 = \mathrm{id}$

Exercise 129. Find the symmetry groups of the ornaments shown in Fig. 4 and Fig. 5.8d.

Exercise 130. Determine the ornamental class of every group in the table and thus prove Lemma 3 (p. 117).

Exercise 131. Try to guess the meaning of the letters and numbers used in the notation of crystallographic groups.