Chapter 4

Arbitrary groups

In this chapter we will introduce the general notion of a group, which includes transformation groups as a particular case. We will discuss the basic properties of groups in this general setting and consider some applications of groups in arithmetic.

4.1 The general notion of a group

In our study of transformation groups, it often did not matter that we dealt with *movements* or *transformations*. What mattered was the *properties* of the group G expressed as the following four requirements imposed on the *composition* defined for any pair of elements of G:

1. the composition of two movements belonging to G also belongs to G;
2. the composition of movements is associative;
3. the group contains the identical transformation which is characterized by the property that its composition with any movement f is equal to f;
4. together with every movement the group contains the inverse movement.

We will arrive to the general notion of a group, if we consider an arbitrary set, supplied with an operation which associates an element of this set with any pair of its elements and which enjoys a similar set of properties. For example, the set of all real numbers with the operation of addition $(\mathbb{R}, +)$ possesses all the listed properties and in this sense constitutes a group. We should like to draw the reader's attention to the fact that already in Chapter 1 (Problems 1, 7 etc.) we have used these properties for elements of various nature (numbers, points, vectors) and different operations (addition, multiplication). The analogy between Problem 32 and Exercise 67 is also noteworthy. All these facts testify that the notion of a group ought to be stated in a general setting. And here we go.

Definition 13 *A group is a set G with the following properties:*

1. *there is a rule (a (binary) operation), according to which for any ordered pair (a, b) of elements of the set G a certain element $a * b \in G$ is defined;*

2. *the operation $*$ is associative, i.e. for any three elements $a, b, c \in G$ the following equality holds: $(a * b) * c = a * (b * c)$;*

3. *in G, there is a neutral element, i.e. such an element e that $a * e = e * a = a$ for any $a \in G$;*

4. *for every element $a \in G$ there is a symmetric element $a' \in G$ which satisfies $a * a' = a' * a = e$.*

The four properties 1–4 are also referred to as the *group axioms*. Note that any transformation group is a group in this general sense, although the definition of a transformation group (p. 59) consists of only two out of the four group axioms: number 1 and number 4. The reason is that axiom 2 always holds for the composition of transformations (p. 54), and axiom 3 follows from axioms 1 and 4, because the neutral element with respect to the composition of transformations is the identity transformation, and the question is only whether it belongs to the given set G.

Exercise 70. Prove that for a finite set G consisting of transformations axiom 4 follows from axioms 1–3.

Instead of the symbols $*$ (*asterisk*), $'$ (*prime*) and the terms 'neutral', 'symmetric', whose meaning is explained in the definition of a group, other symbols and words are used in various specific circumstances:

- In case of transformation groups the group operation (composition) is denoted by a small circle ($\circ$), the neutral element is denoted by id (identical transformation) and the role of a symmetric element f' is played by the inverse transformation f^{-1}.

- For the group of numbers (integer, rational, real or complex) with the operation of addition the neutral element is 0 (zero), and the element, symmetric to a given number a, is the opposite number $-a$. (When we considered complex numbers as points in the plane, we called the neutral element the *pole* and denoted it by P.)

- For numeric groups with the operation of multiplication (for example, the set of all positive real numbers), the symbol of the operation is usually omitted, i.e. one writes ab instead of $a * b$, the neutral element is 1, and the symmetric element is the inverse number a^{-1}.

Groups that consist of numbers, vectors etc. with the operation of addition, are referred to as *additive groups*. If the group operation is multiplication, then the group is called *multiplicative*.

The system of notation adopted for the multiplication of numbers is the most convenient, so it is often used for arbitrary groups. We shall also use it by default. The only thing that has to be kept in mind is that group multiplication, in distinction with the numeric multiplication, is not in general commutative, hence ab and ba need not be the same element of the group.

Problem 33 *For each of the following sets with binary operations determine whether it is a group:*

1. *all even integers with the operation of addition;*
2. *all odd integers with the operation of addition;*
3. *all real numbers with the operation of subtraction;*
4. *all natural numbers with the operation of addition;*
5. *all non-negative integers with the operation of addition;*
6. *all real numbers with the operation* $x * y = x + y - 1$.

Solution. In example 1 all the group axioms are obviously satisfied.

In example 2 the first axiom fails: the sum of two odd numbers is not an odd number.

In the third example the first axiom holds, but the second fails, because subtraction is not associative: $(6 - 5) - 3 \neq 6 - (5 - 3)$.

In the next example the first two axioms are fulfilled, but the operation does not have the neutral element: the only number that could play the role of the neutral element with respect to the addition is zero, but it does not belong to the given set.

Example 5 differs from the previous one in only that the number 0 is added to the set, so that now the neutral element exists. But axiom 4 is not valid, because positive numbers do not have the inverse in this set.

The last example requires more attention, because the operation is unusual. Let us check all group axioms one by one. It is clear that for an arbitrary pair (x, y) of real numbers $x + y - 1$ is also a real number, so that the first axiom holds. To verify the associativity, we have to calculate the two expressions $(x * y) * z$ and $x * (y * z)$, using the definition of $*$. We have:

$$\begin{aligned}(x * y) * z &= (x + y - 1) * z = x + y - 1 + z - 1 = x + y + z - 2,\\ x * (y * z) &= x * (y + z - 1) = x + y + z - 1 - 1 = x + y + z - 2.\end{aligned}$$

We pass to the third axiom. The neutral element e must satisfy the identity $x + e - 1 = x$ for any x. This is true if and only if $e = 1$. Finally, since the operation $*$ is commutative, to determine the number, symmetric to the given number x with respect to $*$, we have only one equation instead of two: $x * x' = 1$, i.e. $x + x' - 1 = 1$, whence $x' = 2 - x$. All the four axioms are thus satisfied, and the given set $(\mathbb{R}, *)$ is a group.

Exercise 71. Check whether the given sets with binary operations are groups. In case of a negative answer, indicate which of the four axioms fails.

(1) the set of all irrational numbers with the operation of addition;

(2) the set of all real numbers $x > 2$ with the operation $x * y = xy - x - y + 2$;

(3) the set of all binary rational numbers (i.e. fractions whose denominator is a power of 2) with the operation of addition;

(4) the set of all non-zero binary rational numbers with the operation of multiplication;

(5) can you find a set of real numbers which forms a group with respect to the operation $x * y = (x + y)/(1 - xy)$?

We will indicate several simple, but important corollaries of the group axioms.

1. The neutral element in a group is unique, i.e. there is only one element e that satisfies the requirements of the group axiom 3. Indeed, suppose that we have two elements e_1 and e_2 such that for every $a \in G$ the following relation holds:

$$ae_1 = e_1 a = ae_2 = e_2 a = a.$$

Setting successively $a = e_1$ and $a = e_2$, we derive that $e_1 = e_1 e_2 = e_2$.

2. Any equation $ax = b$ is uniquely solvable in a group. This means that for any $a, b \in G$ there is a unique element $x \in G$ such that $ax = b$. Indeed, using group axioms 2 and 4, we can multiply the given equation by a^{-1} on the left and get: $x = a^{-1}b$.

Exercise 72. Find a solution of the equation $xa = b$ and prove that it is unique.

3. The previous assertions imply that:

   - The inverse element for a given $a \in G$, defined by axiom 4, is unique.
   - In every row and every column of the multiplication table of a group each element of the group appears exactly once. One of these facts follows from the unique solvability of equations $ax = b$, the other — from the unique solvability of equations $xa = b$.

4. Group elements imply that the element $(a^{-1})^n$ is inverse to a^n. Therefore, like in the case of transformation groups, we can define zeroth and negative powers of the given element by setting $a^0 = e$, $a^{-n} = (a^{-1})^n$ for $n > 0$. Then, for arbitrary integer values of k and l we will have:

$$a^k a^l = a^{k+l}. \tag{4.1}$$

5. The last relation implies that the set of all integer powers of an element a forms a group. Such a group is called *cyclic* and the element a, its *generator*. The *order* of the element a is defined as the smallest positive integer n such that $a^n = e$. If $a = e$, the order is 1 by definition; if a^n is different from e for any $n > 0$, we say that the order of a is infinite. In the latter case the subgroup generated by a is an *infinite cyclic group*. Note that the order (the number of elements) of the group generated by a is equal to the order of the element a.

6. The axiom of associativity means that the product of three elements of a group, which involves two multiplications, does not depend on the order in which these multiplications are computed. Using induction, one can prove that this property is also true for any number of multiplications: any bracketing of the product $a_1a_2\dots a_n$ gives one and the same result. For example, $(a_1(a_2a_3))a_4 = ((a_1a_2)a_3)a_4 = (a_1a_2)(a_3a_4) = a_1(a_2(a_3a_4)) = a_1((a_2a_3)a_4)$.

So far, we have dealt with groups consisting of either transformations (transformation groups) or numbers (numeric groups). Now we will give an example of a group whose elements have quite a different nature.

Problem 34 *Let us call a 3-switch an electric circuit with three inputs and three outputs connected by wires in such a way that every input corresponds to a certain output. The total number of 3-switches is six, and they are all displayed in Figure 4.1. The problem is to define a natural operation on the set of 3-switches which turns this set into a group.*

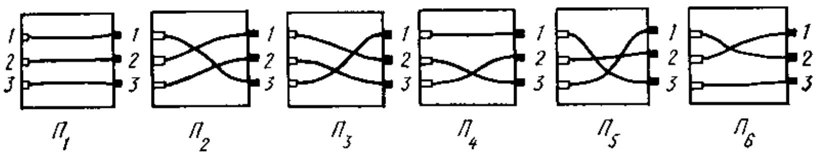


Figure 4.1: 3-switches

Solution. A natural operation on the set of switches is *concatenation*. To concatenate two switches means to connect the inputs of one of them to the outputs of another. For example, if we concatenate the switches Π_2 and Π_4, input number 1 of Π_2 will go through the input number 3 of Π_4 to the output number 2, so that in the result we have that input 1 is connected to output 2. Similarly, input 2 goes into output 1 and input 3 — into output 3. This is the same pattern that we have for the switch Π_6. In this sense we can write that $\Pi_2\Pi_4 = \Pi_6$. Note that this operation is not commutative, for example, $\Pi_4\Pi_2 = \Pi_5$.

The complete multiplication (or, more exactly, concatenation) table for the set of 3-switches looks as follows:

	Π_1	Π_2	Π_3	Π_4	Π_5	Π_6
Π_1	Π_1	Π_2	Π_3	Π_4	Π_5	Π_6
Π_2	Π_2	Π_3	Π_1	Π_6	Π_4	Π_5
Π_3	Π_3	Π_1	Π_2	Π_5	Π_6	Π_4
Π_4	Π_4	Π_5	Π_6	Π_1	Π_2	Π_3
Π_5	Π_5	Π_6	Π_4	Π_3	Π_1	Π_2
Π_6	Π_6	Π_4	Π_5	Π_2	Π_3	Π_1

It turns out that the set of switches with this multiplication table forms a group. But how can one prove this? Using a direct procedure of verifying all the group axioms, already for one axiom number 2 (associativity) one has to check $6^3 = 216$ equalities $\Pi_i(\Pi_j\Pi_k) = (\Pi_i\Pi_j)\Pi_k$. Fortunately, there is a less tedious way to do all these checks. Note that if you replace the letters Π_1, Π_2, Π_3, Π_4, Π_5, Π_6 in the multiplication table of the switches by id, R, R^2, S_a, S_c, S_b respectively and swap the two last rows and the two last columns of the table obtained, then you will get the multiplication table for the group D_3 (see p. 70). This means that the concatenation of 3-switches and the composition of the movements in the group D_3 establish exactly the same relations between the elements of the respective sets. Therefore, the operation of concatenation in the set of switches has all the properties that the composition of transformations has: it is associative, there is a neutral element (the switch Π_1) and every switch has an inverse. This implies that the set of 3-switches forms a group with respect to concatenation.

The mathematical content of the previous example consists in the description of all possible one-to-one mappings of the set $\{1, 2, 3\}$ into itself, or, in another terminology, all *transformations* of this set.

A transformation of the set $\{1, 2, \ldots, n\}$ is called a *permutation* of n elements, or a *permutation of degree* n. A permutation that takes 1 into i_1, 2 into i_2, $\ldots$, n into i_n, is denoted as $\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$. There are $n!$ permutations of degree n all in all, and they form a group, denoted by S_n.

There are even two different natural ways to define the group structure in the set of all permutations of a given degree. The first one is to treat permutations exactly like transformations and define the product $\sigma_1\sigma_2$ of the two permutations σ_1 and σ_2 as the composition $\sigma_1 \circ \sigma_2$ of the two mappings. We remind that the composition $\sigma_1 \circ \sigma_2$ is obtained by first performing the transformation s_2 and then the transformation s_1. According to this definition, we will have:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Another way to define the product of the two permutations σ_1 and σ_2 is to first perform σ_1 and then σ_2 — exactly like we defined the concatenation of switches in Problem 34.

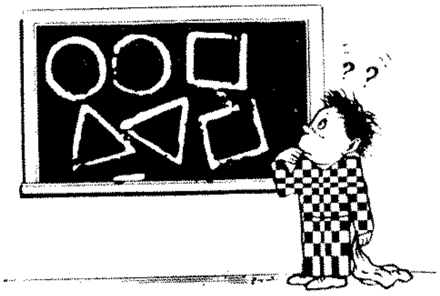
There are two schools of mathematicians: one maintains that the product of permutations should be defined as $\sigma_1 \circ \sigma_2$, another — that it should be defined as $\sigma_2 \circ \sigma_1$. Multiplication tables for S_n adopted by the two schools differ by a reflection in the main diagonal. Actually, both viewpoints are not so far apart: after studying section 14 you will be able to prove that the two permutation groups resulting from the two definitions are in fact *isomorphic*.

Here are some more problems where different groups appear, implicitly or explicitly.

Exercise 73. On a blackboard, several circles, squares and triangles are drawn. It is allowed to erase any two figures and replace them by a new figure following the rule:

— two circles make a circle;
— two squares make a triangle;
— two triangles make a square;
— a circle and a square make a square;
— a circle and a triangle make a triangle;
— a square and a triangle make a circle;

Prove that the shape of the last figure that will remain does not depend on the order in which the replacements are made.



Exercise 74. Consider the rational algebraic expressions in one variable, i.e. quotients of two polynomials in x with real coefficients. If A and B are two such expressions, then we can form the *superposition* $A * B$ by substituting B instead of x into A. Prove that the set Φ of all expressions that can be obtained by substitutions from $A_1 = 1 - x$ and $A_2 = 1/x$, forms a group, find its order, the list of elements and the multiplication table.

Exercise 75. Find a rational expression B, different from a constant, such that $B * A_1 = B * A_2 = B$, where $A_1 = 1 - x$, $A_2 = 1/x$.

4.2 Isomorphism

When working on Problem 34, we have deduced all the properties of the concatenation from the similar properties of the composition of transformations, using the fact that both operations have the same inner structure. The precise notion suited to characterize such situations is *isomorphism.*

Definition 14 *Two groups G and H are said to be isomorphic, if there is a one-to-one correspondence, denoted by '$\leftrightarrow$', between the elements of G and the elements of H, such that $g_1 \leftrightarrow h_1$ and $g_2 \leftrightarrow h_2$ always imply $g_1g_2 \leftrightarrow h_1h_2$. One can also say that this correspondence respects, or agrees with the group operations in both groups.*

A more exact way to state the definition of an isomorphism is: the groups G and H are isomorphic, if there exists a one-to-one mapping $\varphi : G \to H$ such that

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) \tag{4.2}$$

for any elements g_1 and g_2 of G. One can also say that φ is an *isomorphism* of the group G onto the group H.

At first sight it seems that the second version of the definition is different from the first one, because the two groups do not enter symmetrically. In reality, however, both groups have equal rights, because, if φ is an isomorphism of G onto H, then φ^{-1} will be an isomorphism of H onto G. Indeed, denoting $h_1 = \varphi(g_1)$, $h_2 = \varphi(g_2)$ and applying φ^{-1} to both sides of equation 4.2, we get $\varphi^{-1}(h_1)\varphi^{-1}(h_2) = \varphi^{-1}(h_1 h_2)$.

The most direct way to establish the isomorphism, especially for finite groups, is to explicitly indicate all pairs of corresponding elements and then check that, after all elements of one group in its multiplication table are replaced by their counterparts from another group, we will obtain the multiplication table of the second group. Of course, it might be necessary to change the order of columns and rows in the table obtained to make it literally coincide with the multiplication table of the second group that was given. Note that we have followed this procedure in Problem 34.

Exercise 76. Check whether the following correspondence is an isomorphism between the group of 3-switches and the symmetry group of the regular triangle D_3: id $\leftrightarrow \Pi_1$, $R^2 \leftrightarrow \Pi_2$, $R \leftrightarrow \Pi_3$, $S_b \leftrightarrow \Pi_4$, $S_c \leftrightarrow \Pi_5$, $S_a \leftrightarrow \Pi_6$.

This exercise leads to an important observation: of two groups G and H are isomorphic, the isomorphism $\varphi : G \to H$ is not in general unique. In particular, there might exist isomorphisms of a group onto itself, different from the identity transformation.

Exercise 77. Find all isomorphisms of the group D_3 onto itself.

The notion of an isomorphism illuminates the meaning of some analogies that an industrious reader might have noticed in the material of the previous chapters. We can now state them as clear-cut problems.

Exercise 78. Prove that the set of all points of the plane with the operation of addition over a fixed pole (see p. 9) forms a group isomorphic to the additive group of plane vectors. Also prove that assigning to a point (or a vector) the pair of its coordinates in a certain basis establishes an isomorphism of the respective group and the group of pairs of real numbers with the operation defined by the rule

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2).$$

Exercise 79. Prove that the set of vertices of a regular hexagon with the multiplication described in Problem 7 (p. 21) forms a cyclic group isomorphic to the group C_6 of rotations with a common centre through angles which are multiples of 60°.

Exercise 80. Prove that the set {circle, triangle, square} with the operation defined in Exercise 73, is a group isomorphic to the cyclic group C_3. How many different isomorphisms between these groups are there?

Exercise 81. Prove that the group of rational algebraic expressions defined in Exercise 74, is isomorphic to the dihedral group D_3.

The results of Exercises 79 and 80 are generalized by the following assertion: *any two cyclic groups of the same order are isomorphic*. Indeed, let g be the generator of the first group G and h be the generator of the second group H. Define the mapping $\varphi : G \to H$ by the rule $\varphi(g^k) = h^k$. The law of multiplication of powers 4.1 holds in either group and implies that φ is an isomorphism:

$$\varphi(g^k g^l) = \varphi(g^{k+l}) = h^{k+l} = h^k h^l = \varphi(g^k)\varphi(g^l).$$

It is likewise clear that a group isomorphic to a cyclic group, is itself cyclic, because the image of a generator under an isomorphism will also be a generator.

If we are interested in the inner structure of a group, we can forget about the nature of elements it consists of, keeping track only of the properties of the group operation.

Definition 15 *An abstract group is a class of all groups which are isomorphic between themselves.*

For example, all cyclic groups of order n, such as the group of rotations C_n or the group of complex n-th root of unity, are representatives or, in Buddhist terminology, *incarnations*, of one and the same abstract cyclic group of order n. In the same way, the dihedral group D_3, the permutation group S_3, the group of switches (Problem 34) and the group of rational expressions (Exercise 74) are all representatives of one and the same abstract group. Later (page 103) we will explain how to define an abstract group with a given structure (set of relations between generators).

We now pass to the following general problem: *given two groups, decide whether they are isomorphic or not.* Usually, it takes more efforts to establish the isomorphism than to establish the non-isomorphism, because, in the first case, one normally has to *construct* the isomorphism, while in the second case, it is often enough to find some property which must be preserved by an isomorphism and which, however, distinguishes the groups under study. Here is a short list of some simple properties whose coincidence for the two groups is a necessary condition of the isomorphism:

1. *The order of the group.* Groups that have a different number of elements cannot be isomorphic.

   Exercise 82. Is the group of all integers with addition isomorphic to the group of all even numbers with addition?

2. *Commutativity.* A commutative group cannot be isomorphic to a non-commutative.

3. *Cyclicity.* A cyclic group cannot be isomorphic to a non-cyclic.

   Exercise 83. Are there any pairs of isomorphic groups in the list C_1, D_1, C_2, D_2, C_3, D_3, ...?

4. *The orders of elements.* The number of elements of order n in one group must be equal to the number of elements of order n in the other group, because the orders of the corresponding elements are the same.

We will only prove the last item, because it is somewhat more complicated than the previous ones.

To begin with, note that under an isomorphism, the unit elements of the groups correspond to each other. In fact, if e is the unit of the group G and $\varphi : G \to H$ is an isomorphism, then $ee = e$ implies $\varphi(e)\varphi(e) = \varphi(e)$, which, upon multiplication by the element of H, inverse to $\varphi(e)$, leads to the equality $\varphi(e) = e'$, where e' is the unit of H. Now let g be an element of G that has order n in G. By definition, $g^n = e$, whence $\varphi(g)^n = e'$, i.e. the order of $h = \varphi(g)$ does not exceed n. An inverse argument shows that the order of g cannot exceed the order of h. Therefore, both orders are equal.

For example, to distinguish between the groups C_6 and D_3, it is enough to use any of the three criteria 2–4. First of all, one group is commutative, another is not. Then, one group is cyclic, another is non-cyclic. Finally, the group C_6 has one element of order 1, one element of order 2, two elements of order 3 and two elements of order 6, while the group D_3 has one element of order 1, three elements of order 2 and two elements of order 3.

The list of properties that are necessary for two groups to be isomorphic, is virtually infinite, because it contains any property of the group which can be formulated in terms of the group operation, without referring to the specific nature of the elements of the group. We will, however, pass to the second half of the isomorphism problem. Suppose that we are given two groups G and H and we cannot find any intrinsic property that distinguishes one of them from another. Then the conjecture arises that the groups are isomorphic. To prove this, one must construct an isomorphism $f : G \to H$ between G and H. How can this be done?

First we recall that, if e and e' are the unit elements in G and H respectively, then we have $\varphi(e) = e'$. Further, if $f(g) = h$ for a certain pair of of elements $g \in G$ and $h \in H$, then by repeated application of identity 4.2 we can derive that $\varphi(g^k) = h^k$ for any natural k.

Exercise 84. Prove the equality $\varphi(g^k) = h^k$ for negative values of k.

We thus see that, if the mapping φ is defined on a certain element g of the group G, then it is also uniquely defined on the whole subgroup generated by g. Quite similarly, if the images of *several* elements $g_1, \dots, g_n$ of the group G are known, then one can uniquely determine the image of any element expressible through $g_1, \dots, g_n$. If these elements are *generators* of G, then the values $\varphi(g_1) = h_1, \dots, \varphi(g_n) = h_n$ completely determine the mapping φ. In the case of two generators we can write the corresponding formula as follows:

$$\varphi(g_1^{k_1} g_2^{l_1} \dots g_1^{k_s} g_2^{l_s}) = h_1^{k_1} h_2^{l_1} \dots h_1^{k_s} h_2^{l_s}. \tag{4.3}$$

Thus, if the group G is generated by two elements g_1 and g_2, then, to construct an isomorphism $\varphi : G \to H$, we must define its values $\varphi(g_1) = h_1$, $\varphi(g_2) = h_2$ and then extend the mapping to all of G according to relation 4.3. But how should the elements h_1, h_2 be chosen? It is clear that they ought to be a set of generators of the group H, they must have the same respective orders as g_1 and g_2 and must satisfy all the relations that g_1 and g_2 satisfy. For example, if $g_1^2 g_2^3 = e$, then we must have $h_1^2 h_2^3 = e'$. These observations allow to guess a 'candidate' for the isomorphism φ. After the mapping is constructed, one has to verify that it is really an isomorphism.

Problem 35 *Let ε be the complex number $-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ (note that $\varepsilon^3 = 1$). Consider two functions of a complex variable $F_1(z) = \varepsilon z$, $F_2(z) = \overline{z}$. Prove that the set of all functions that can be obtained from F_1 and F_2 by superposition, forms a group isomorphic to the dihedral group D_3.*

Solution. We successively find:

$$\begin{aligned}
F_3(z) &= F_1(F_2(z)) = F_1(\overline{z}) = \varepsilon\overline{z},\\
F_4(z) &= F_2(F_2(z)) = F_2(\overline{z}) = z,\\
F_5(z) &= F_1(F_1(z)) = F_1(\varepsilon z) = \varepsilon^2 z,\\
F_6(z) &= F_2(F_1(z)) = F_2(\varepsilon z) = \overline{\varepsilon z} = \varepsilon^2\overline{z}.
\end{aligned}$$

A straightforward check shows that further application of F_1 and F_2 to these expressions does not lead to any new functions. Thus, the set of six functions F_1, $\dots$, F_6 is closed under superposition. The inverse of every function belonging to this list also belongs to this list. This proves that what we have is a group. The neutral element is the identity function F_4, functions F_2, F_3, F_6 have order 2 and functions F_1, F_5 have order 3. The group is not commutative since, for example, $F_1(F_2(z)) = F_3(z)$, while $F_2(F_1(z)) = F_6(z)$. These observations suggest that our group G is likely to be isomorphic to the group D_3.

To construct an isomorphism $\varphi : G \to D_3$, note that the group G by definition has two generators F_1 and F_2, whose orders are 3 and 2. In the group D_3 we can also find a system of two generators with orders 3 and 2: a rotation and a reflection. For example, let us set $F_1 \leftrightarrow R$, $F_2 \leftrightarrow S_a$ (in the notation of p. 70). Then $F_3 \leftrightarrow S_c$, $F_4 \leftrightarrow \mathrm{id}$, $F_5 \leftrightarrow R^2$, $F_6 \leftrightarrow S_b$. Replacing every element of D_3 by the corresponding element of G in the multiplication table of D_3 (p. 70), we will obtain the following table:

	F_4	F_1	F_5	F_2	F_6	F_3
F_4	F_4	F_1	F_5	F_2	F_6	F_3
F_1	F_1	F_5	F_4	F_6	F_3	F_2
F_5	F_5	F_4	F_1	F_3	F_2	F_6
F_2	F_2	F_3	F_6	F_4	F_5	F_1
F_6	F_6	F_2	F_3	F_1	F_4	F_5
F_3	F_3	F_6	F_2	F_5	F_1	F_4

which, as one can easily check, is the correct multiplication table for the group G.

The isomorphism is thus established. There is, however, a more natural way to find an isomorphism between the two groups in question. Indeed, let us recall that the functions of a complex variable can be viewed as an analytical representation of plane transformations. In particular, the function $F_1(z) = \varepsilon z$ corresponds to the

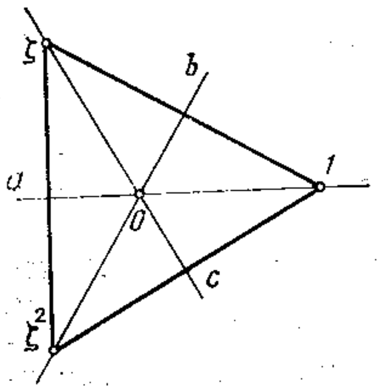


Figure 4.2: Regular triangle in the complex plane

rotations around 0 through 120°, while the function $F_2(z) = \overline{z}$, to a reflection in the real axis (axis a in Figure 4.2).

If we assign to every function obtained from F_1 and F_2 by superpositions, the corresponding plane transformation, we will obtain a group isomorphism.[1]

The isomorphism constructed by the second method is called *natural*. A natural isomorphism reveals the reason why the two groups are isomorphic.

Exercise 85. Indicate a natural isomorphism
(1) between the group of 3-switches (see Problem 34) and the group D_3;
(2) between the group of rational algebraic expressions of Exercise 76 and the group D_3.

We have to admit that the naturality we are talking about is by no means a strict mathematical notion, it rather bears a heuristic character. In a certain sense, any isomorphism is natural, but, in order to *understand* why is it natural, people often have to develop a special mathematical theory. A quest for natural isomorphisms that explain the reason why similar objects appear in different areas of mathematics is a powerful impetus that fosters the development of knowledge.

Here, we have used the general word 'knowledge' on purpose, to emphasize the fact that the notion of isomorphism is important not only in mathematics, but in any area of thinking. To get an idea of this general meaning of 'isomorphism', we invite the reader to contemplate over the following historical example.

In 1970, one of the problems of the entrance examination set for the Gelfand's Correspondence Mathematical School in Moscow was published by two major journals in different formulations.

One of the journals stated the problem like this:

[1]Note that the terms 'superposition' and 'composition' actually have the same meaning, only the first one is used in analysis for functions, while the second one in geometry for transformations.

> One of the three gangsters, known in the city M under the names of Archie, Boss and Wesley, has stolen a bag with money. Each of them made three declarations:
>
> - Archie:
>   - I did not steal the bag.
>   - On the day of the theft I was not in the city.
>   - Wesley stole the bag.
> - Boss:
>   - Wesley stole the bag.
>   - Even if I stole it, I would not confess.
>   - I have lots of money.
> - Wesley:
>   - I did not steal the bag.
>   - I've been long looking for a good bag.
>   - Archie told the truth that he was not in the city.
>
> During the investigation it was found that two declarations of each gangster were true and one false. Who stole the bag?

Another journal proposed the following problem (names mentioned belong to protagonists of Russian folk tales):

> The King learned that somebody has killed the ruthless Dragon. He knew that this could only be done by one of the three famous warriors: Ilya Muromets, Dobrynia Nikitich or Alyosha Popovich. They were summoned to the King and each of them spoke three times. Here is what they said.
>
> - I. M.:
>   - I did not kill the dragon.
>   - On that day I was travelling abroad.
>   - A. P. did that.
> - D. N.:
>   - A. P. did that.
>   - Even if I killed him, I would not confess.
>   - There are many evil spirits still alive.
> - A. P.:
>   - I did not kill the dragon.
>   - I've been long looking for a nice feat to do.
>   - It is true that I. M. was abroad.
>
> The King found out that each of the three warriors twice told the truth and once lied. Who killed the dragon?

It is easy to see that, although the two problems are about quite different things, their logical structure is the same. Here is a glossary of names, things and actions that correspond to each other in the two problems:

Archie	Ilya Muromets
Boss	Dobrynia Nikitich
Wesley	Alyosha Popovich
bag	dragon
to steal	to kill
to leave the city	to go abroad

If, in the statement of the first problem, all the significant words are replaced by their counterparts from the right-hand column, the result almost coincides with the statement of the second problem — with the exception of proposition number six, which is actually irrelevant for the solution of the problem. In this sense, the two problems are isomorphic.

This isomorphism can be used as follows. If you solve the first problem and find that the answer is 'Boss', then you do not have to solve the second problem: the correct answer is given by the word that corresponds to Boss in our glossary, namely 'Dobrynia Nikitich'.

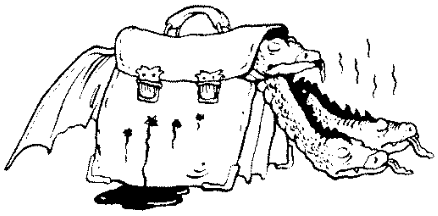


Figure 4.3: Isomorphism

In the same way one can use the isomorphism of groups: if G is isomorphic to H, then every assertion about G that can be stated in terms of the group operation, will also hold for the group H, after an appropriate translation.

Another, more simple and direct, application of the group isomorphism is the computation of the product of elements in one group, using the product in another, provided that the second multiplication is less difficult and time-consuming. More exactly, if $\varphi : G \to H$ is an isomorphism between the groups $(G, *)$ and $(H, \circ)$, then the $*$-product can be computed by the formula

$$g_1 * g_2 = \varphi^{-1}(\varphi(g_1) \circ \varphi(g_2)). \tag{4.4}$$

A classical example of this kind of computations is provided by *logarithms* invented by J. Napier[2] (early XVII century) who sought to replace the multiplication of numbers by a simpler operation — addition. Denoting the decimal logarithm of x by $\lg x$, we have the identity

$$x_1 x_2 = 10^{\lg x_1 + \lg x_2}, \tag{4.5}$$

[2]Actually, logarithms in the contemporary sense of the word were introduced and tabulated by his disciple G. Briggs; J. Napier himself used a function $y = A \lg x + B$ with some constants A and B.

being a particular case of the general relation 4.4. The isomorphism that makes possible the computations based on logarithms, is the isomorphism $\lg : (\mathbb{R}_+, \cdot) \to (\mathbb{R}, +)$ of the group of positive real numbers with multiplication onto the group of all real numbers with addition. The two basic properties of the logarithmic function:

1. it is on-to-one on the sets specified,
2. it satisfies the identity
$$\lg(x_1 x_2) = \lg x_1 + \lg x_2$$

— mean precisely that it establishes an isomorphism between the two groups.

Exercise 86. 1. Find the analog of formula 4.5, if the decimal logarithm $y = \lg x$ is replaced by the Napier function $y = A \lg x + B$.

2. Find a group operation $*$ on the set of all real numbers such that the Napier function gives an isomorphism of $(\mathbb{R}_+, \cdot)$ onto $(\mathbb{R}, *)$.

The second half of the last exercise is a particular case of the so called *transition of structure*. Here is what we mean by that.

Let G be a group with operation $\triangle$ and H a set with no operation. Suppose that a one-to-one mapping $\varphi : H \to G$ is given. Then it is possible to *carry the group operation from G to H along φ* by the formula

$$h_1 \triangledown h_2 = \varphi^{-1}(\varphi(h_1) \triangle \varphi(h_2)).$$

We have actually used this method:

- to derive the addition of points from the addition of vectors (Chapter 1);
- to define the unusual group operation over the real numbers $x * y = x + y - 1$ (Problem 33). This operation is obtained from the ordinary addition, which is carried over from one copy of $\mathbb{R}$ into another along the mapping $\varphi(x) = x - 1$. Indeed, $x * y = \varphi^{-1}(\varphi(x) + \varphi(y)) = ((x - 1) + (y - 1)) + 1 = x + y - 1$.

The operation $x * y = \dfrac{x + y}{1 - xy}$ that appeared in Exercise 71, has the same origin. We have tried to perform the transition of the group structure $(\mathbb{R}, +)$ along the mapping $\varphi(x) = \tan x$, but we were not quite successful, because this mapping is not one-to-one. However, for any set $M \subset \mathbb{R}$ which is an additive group and has the property that the values of the tangent in the points of M are all different, the set of these values forms a group with respect to operation $*$.

Exercise 87. Prove that:

1. As such set M one can take the set of all multiples of a real number α which is incommensurable with π.
2. A set M with the required properties cannot contain any open interval of the real axis.

Exercise 88. Find out:

1. what operation on real numbers is the result of transition of the addition along the mapping $x \mapsto x^3$?

2. how was the operation $x * y = xy - x - y + 2$ (Exercise 71) obtained?

In terms of the transition of structure the notion of isomorphism can be formulated as follows: the mapping $\varphi : G \to H$ is an isomorphism of groups, if the group operation of H carried over to G along φ coincides with the group operation of G.

4.3 The Lagrange theorem

In this section we will state and prove the very first theorem of group theory which was found by the French mathematician Lagrange in late XVIII century, even before the notion of group was explicitly introduced in mathematics in XIX century by E. Galois.

Theorem 7 (Lagrange) *The order of a subgroup of a finite group is always a divisor of the order of the whole group.*

Since every element of a group generates a cyclic subgroup whose order is equal to the order of this element, we obtain, in particular, that *the order of a finite group is divisible by the order of each element.* The reader might have noticed this law in the examples considered above (groups C_{12}, D_3 etc.)

To prove the theorem of Lagrange in the general setting, we shall use the important construction of the *coset decomposition* of a group over a subgroup.

Let G be a group of order n and H its subgroup of order m: $H = \{h_1, h_2, \ldots, h_m\}$. Since every subgroup contains the unit element of the group, we can assume that $h_1 = e$. Choose an arbitrary element g of the group G that does not belong to the subgroup H and consider the set

$$gH = \{gh_1, gh_2, \ldots, gh_m\}$$

obtained by multiplying all the elements of the subgroup by one and the same element g on the left. The set gH is called a *left coset of G over H*. It has two important properties:

1. $|gH| = |H|$, i.e. gH has the same number of elements as H;

2. $gH \cap H = \emptyset$, i.e. the sets gH and H do not have common elements.

To prove property (1), we have to show that all the elements of the list $gh_1, gh_2, \ldots, gh_m$ are distinct. Indeed, if we had $gh_i = gh_k$, then, after multiplying this equation by g^{-1} on the left, we would obtain $h_i = h_k$.

To prove (2), suppose that $h_i = gh_k$. This implies that g can be expressed as $h_i h_k^{-1}$ and must, therefore, belong to the subgroup H, contrary to the supposition.

The second property has the following generalization: *if g_1H is a coset and $g_2 \in G$ an element of the group that does not belong to g_1H, then the two cosets g_1H and g_2H do not have common elements* or, in other words, *two cosets either coincide or are disjoint.* In fact, if there was a common element, we would have $g_1h_i = g_2h_k$, hence $g_2 = g_1h_ih_k^{-1}$ and, since $h_ih_k^{-1} \in H$, this would imply that $g_2 \in g_1H$ and therefore $g_2H = g_1H$.

Now, the process of decomposing the group G into the left cosets over the subgroup H can be described as follows. If the subgroup H coincides with the entire group G, then the coset decomposition consists of only one set H. Otherwise, choose an element $g_1 \notin H$ and consider the coset g_1H. If $H \cup g_1H = G$, the process terminates. If not, we choose a $g_2 \in G$ which belongs neither to H nor to g_1H and thus obtain three pairwise disjoint cosets H, g_1H and g_2H.

Since the group is finite, this process sooner or later terminates and we obtain the required decomposition

$$G = H \cup g_1H \cup \ldots \cup g_kH,$$

where each of the listed subsets has m elements and they are all pairwise disjoint.

Therefore, the number of elements in the group, n, is divisible by the number of elements in the subgroup, m. The theorem is proved.

Let us remark that similar to the left coset decomposition, one can also consider the right coset decomposition. In general, these two decompositions do not coincide, and we will discuss this question in the next chapter.

Figures 4.4 and 4.5 show the left coset decompositions of the group D_3 over a subgroup of order 3 and a subgroup of order 2.

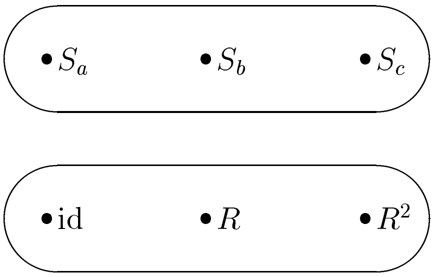


Figure 4.4: First coset decomposition of the group D_3

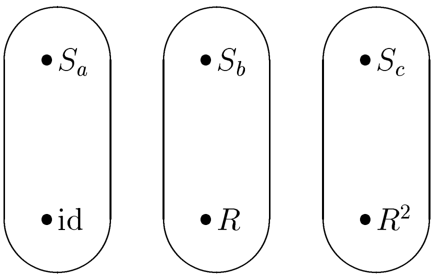


Figure 4.5: Second coset decomposition of the group D_3

Exercise 89. Find all subgroups of the group D_3.

The Lagrange theorem implies the following important fact.

Problem 36 *Prove that every finite group whose order is a prime number, is cyclic.*

> **Solution.** Let G be a group of prime order p and g an arbitrary element of G different from the unit element e. Denote by H the subgroup of G generated by g. The order of H is at least 2, since it contains e and g. The only divisor of the prime number p which is greater than 1, is p itself. Therefore, the order of H is p and $H = G$. The group G is thus generated by one element g.

As a direct consequence of the assertion just proved we obtain the following fact: *any group of prime order is commutative.*

We shall now discuss some applications of group theory, in particular, Lagrange's theorem, to arithmetic.

The simplest group that we come across in arithmetic is the group $\mathbb{Z}$ of all integers under addition. Since the group operation is addition, instead of powers of a certain element we will speak about its multiples, i.e. elements that are obtained by successively adding the given element to itself. The group $\mathbb{Z}$ is cyclic with generator 1, since every integer is a multiple of 1: $n = n \cdot 1$.

Exercise 90. Is there another generator in the group $\mathbb{Z}$?

Like in any group, every element n of $\mathbb{Z}$ generates a subgroup. This subgroup consists of all multiples of n, and we denote it by $n\mathbb{Z}$.

Exercise 91. Prove that *every* subgroup of the group $\mathbb{Z}$ has the form $n\mathbb{Z}$ for a suitable n.

This simple result already provides a basis for useful applications in number theory. As an example, we will give a short proof of the following well-known fact: *if a and b are mutually prime numbers, then there exist two integers x and y, such that $ax + by = 1$.*

Indeed, let H be the subgroup in $\mathbb{Z}$ generated by the two given numbers a and b. By definition, $H = \{ax + by \mid x, y \in Z\}$ (let us note that in multiplicative notations this expression would be written as $a^x b^y$). According to Exercise 91, we can find a natural n, such that $H = n\mathbb{Z}$. Since the subgroup H contains the elements a and b, both of them are divisible by n. But, since they are mutually prime, n must be equal to 1. Therefore, the number 1 belongs to H and hence can be written as $ax + by$.

Lagrange's theorem does not directly apply to the pair consisting of the group $\mathbb{Z}$ and the subgroup $n\mathbb{Z}$, because these groups are infinite. However, the construction of the coset decomposition of the group over the subgroup does make sense and leads to the important notions of residue classes and modular arithmetic.

Take, for example, $n = 3$. If we add 1 to all the elements of the subgroup $3\mathbb{Z}$ (i.e. multiples of 3), we get the set of all whole numbers that have remainder 1 in division by 3. Likewise, adding 2 to all the elements of the subgroup, we get the set of all numbers that have remainder 2 in division by 3. Since there are no other remainders in division by 3, we see that the set of all integers splits into 3 classes that we obtained. This is the *coset*

$\ldots, -6,\ -3,\ 0,\ 3,\ 6,\ \ldots$ $\quad 3\mathbb{Z}$

$\ldots, -5,\ -2,\ 1,\ 4,\ 7,\ \ldots$ $\quad 3\mathbb{Z}+1$

$\ldots, -4,\ -1,\ 2,\ 5,\ 8,\ \ldots$ $\quad 3\mathbb{Z}+2$

Figure 4.6: Coset decomposition of the group $\mathbb{Z}$ over $3\mathbb{Z}$

decomposition of $\mathbb{Z}$ *over* $3\mathbb{Z}$. A visual representation of this decomposition is shown in Fig. 4.6. Since the sets $3\mathbb{Z}$, $3\mathbb{Z}+1$ and $3\mathbb{Z}+2$ are infinite, only several elements of each coset are listed.

The cosets of $\mathbb{Z}$ over $m\mathbb{Z}$ are called *residue classes over* m. The class of all integers with remainder k in division by m, is conventionally denoted by $\overline{k}$. There are m residue classes all in all; $\overline{0}$, $\overline{1}$,... $\overline{m-1}$. For example, there are 3 classes modulo 3: $\overline{0}$, $\overline{1}$, $\overline{2}$ (see Fig. 4.6).

Looking at the figure, one can observe that the sum of two numbers always belongs to one and the same class which is determined only by the classes of the two numbers under study and is independent on the particular choice of the representatives within the classes. For example, taking the representatives $1, -2, 7$ of the class $\overline{1}$ and representatives $-4, 5, 8$ of the class $\overline{2}$, we see that the three sums $1+(-4)=-3$, $(-2)+5=3$, $7+8=15$ get into one and the same class $\overline{0}$.

In general, the identity

$$(mx+k)+(my+l)=m(x+y)+(k+l)$$

allows to define the operation of addition of residue classes over m: the sum of the classes $\overline{k}$ and $\overline{l}$ is the class that contains all the sums $k+l$ where k is a representative of the class $\overline{k}$ and l is a representative of the class $\overline{l}$. For example, if $m=3$, we obtain the following addition table in the set of residues modulo 3:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

One can see from this table that the residue classes modulo 3 form a cyclic group of order 3.

Exercise 92. Prove that the residue classes over an arbitrary number m form a cyclic group of order m.

Can we also define the *multiplication* of residue classes in a similar way? Yes. Indeed, consider two classes $\overline{k}$, $\overline{l}$. The product of two arbitrary representatives $mx+k$ and $my+l$

of these two classes, equal to $m(mxy+xl+ky)+kl$, has the same remainder in division by m as the number kl. This remainder does not depend on the choice of the representatives. Therefore, the operation is correctly defined in the set of residue classes.

Here is the multiplication table of residue classes modulo 3:

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

It is evident that this multiplication does not satisfy group axioms because there is one row and one column that entirely consist of zeroes, whereas in the multiplication table of a group no two elements may coincide. However, the smaller table that remains after the zero row and column are deleted:

$\times$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{1}$

does obey all the group laws — it represents a cyclic group of order 2.

Exercise 93. Do all the nonzero residues modulo 6 form a multiplicative group?

This exercise suggests the following conclusion: *to form a multiplicative group out of residues over m it is reasonable to choose only numbers, mutually prime with m.* For example, if $m=6$, then the element $\overline{4}$ that has a common multiple 2 with the number 6, becomes $\overline{0}$ after multiplication by $\overline{3}$. But $\overline{0}$ cannot belong to a group, because it makes a whole row of zeroes in the multiplication table!

We shall now prove the following important fact: *the set of all residue classes $\overline{k}$ modulo m, such that the number k is mutually prime with m, forms a multiplicative group.*

Indeed, if two numbers are mutually prime with m, then their product is mutually prime, too; this means that the operation is closed on the given set. The associativity follows from the associativity of ordinary multiplication of numbers. The class $\overline{1}$ is mutually prime with m and plays the role of the unity. The only non-evident property that we must check is that every residue class in the set under study has an inverse. In other words, for every a, mutually prime with m, there must exist a number x, mutually prime with m and such that $ax \equiv 1 \pmod m$. The last formula is read aloud as '*numbers ax and 1 are congruent modulo m*', which means, by definition, that ax has remainder 1 in division by m. This can be rephrased as follows: *there exists an integer y such that $ax+my=1$.* Now recall that we have already proved this fact, stated in this form (as a corollary from Exercise 91). We only did not mention that x will be mutually with m, but this is evident.

Exercise 94. Consider the set of two residue classes $\{\overline{2},\overline{4}\}$ modulo 6. Does it make a group with respect to multiplication?

For any given m, we shall denote by $\mathbb{Z}_m^*$ the multiplicative group, constituted by all residue classes modulo m which are mutually prime with m. The order of this group, i.e. the number of all such residue classes, is equal to $\varphi(m)$, the Euler function of m. We have encountered this function when we discussed the number of generators of a cyclic group (see page 68). We are now ready to apply the Lagrange theorem.

Note that in any group the following identity holds: $g^m = e$, where m is the order of the group, g an arbitrary element and e the unity. Indeed, if k is the order of g, then by Lagrange's theorem $m = kl$ for an appropriate integer l, and we have: $g^m = (g^k)^l = e^l = e$. In the case of the group $\mathbb{Z}_m^*$ this implies the following theorem.

Theorem 8 **(Euler)** *If a is a number mutually prime with m, then*

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

where $\varphi(m)$ is the Euler's function of m, i.e. the number of integers between 1 and m mutually prime with m.

In the case when $m = p$ is a prime number, we have $\varphi(p) = p - 1$ and the Euler theorem takes the shape of the following fact known as *Fermat's little theorem.*

Theorem 9 *If p is a prime number, then*

$$a^{p-1} \equiv 1 \pmod{p} \tag{4.6}$$

for any integer a not divisible by p.

Historical remark. Neither Fermat, nor Euler used group theoretic considerations explicitly to prove their theorems. It was only in early 19th century that group theory came into being in the works of E. Galois. However, both Fermat and Euler *implicitly* did use such notions as, for example, coset decomposition of residue classes. These investigations became one of the sources from which group theory was born. The explicit application of group theory notions and theorems makes the arithmetical facts more clear and allows to devise far-going generalizations.

In the end of this chapter, we propose several problems in elementary number theory that can be solved using residues and the theorem of Euler.

Exercise 95. Prove that the equation $x^2 = 3y^2 + 8$ has no integer solutions.

Exercise 96. What are the two last digits of the number 2003^{2004}?