

# Constructive methods for assignment and building of finite groups

© 2004, V.P. Golikov\*

*Methods for assignment and building of finite groups based on effective permutations numeration were offered. Trivial resolvability of problems, which are connected with equivalence, identity and conjugation of words in finite group, was shown. Resolvability of isomorphism problem in finite groups was proved.*

## Introduction

Group theory is one of the most important branches in mathematics. Group theory was formed in the works of Galois as abstract science, first it was used only for mathematics and then its applied opportunities in mechanics, quantum physics and crystallography were discovered.

Group is defined as set of members (finite or infinite) with assigned binary operation and axiom of associative property and axioms about unit element and about inverse elements [1-3]. Group theory got rapid development in 19-20 centuries and now, perhaps, she passed its peak of development [1]. In this theory, a number of important problems were stated and solved. So, insolubility of words identity law [4] problem and its conjugation in group [5] were proved as well as problems of group isomorphism establishment [6].

One of the key questions in group theory are questions which are connected with assignment and building of concrete group or some group class. We can assign group [2] as the set of members with one binary operation, which satisfies axioms referred above with the help of multiplication table (Cayley table), formative and defining proportions and at last with the help of schematic model (net).

---

\* Golikov Vasilij Petrovich – doctor of science (Technical), senior researcher of 4th Central Institute of Russian Federation Defence ministry

Group, which is assigned with one of the methods, mentioned above, could be isomorphically presented by permutation group [1-3]. In fact, group theory itself was beginning with substitutions and today they took their “spare place in general theory”. Nevertheless, there is principal difference between assignments of finite group by group of substitutions and by generating and defining proportions. By assignment of finite group with the help of substitutions, it is not necessarily to assign defining proportions because they will arrive automatically. In this regard, permutation is “constructional” generator unlike to “abstract” (non-constructive) generator, which is assigned by letters of different alphabets. Abstract generators naturally appear in the context of “free” groups [1]. At that for assignment of finite group as quotient group of free group, accept abstract generators it necessarily to assign defining proportions. Just here, are beginning problems of finite groups because for the group, which is assigned with the system of generators and the system of defining proportions, it is impossible to determine if this group is finite or infinite, commutative or not and so on [1]. For practical using of finite group for example in informatics the problem of equivalence of words in the group imposes essential restrictions. It is not surprising that here constructions which are based on polynomials of different powers, prime numbers, etc. are dominated.

Finite group, in fact, as the group with spinning is the group of imaging, regardless of nature of its elements and the sort of its binary operation. Nevertheless, the traditional method of permutation forming which is based on transpositions is not perfect because it allows ambiguity of their presentation [2].

It is noted in monograph [1] that the final goal of group theory is the “problem of absolute description of all groups which are existed in nature or at least sufficient wide group classes”. However to present day there are no complete description of even finite groups, although there are series of suggestions for the ways of their cataloging: using of solvable and simple groups, description of groups of given order and so on.

The suspense of mentioned question conformably to finite groups is explained, from our point of view, by following main reasons. First, there is no standard method of finite groups description with using of constructive generators. Secondly, there is no

formal building method of the whole system of finite group elements on the basis of mentioned generators. And, at last, there are no constructive and effective enough finite groups isomorphism criterions and algorithms of their calculation. Although the idea of group isomorphism is quite concrete and for the finite groups there must be some method of accordance excess, but this procedure is not quite evident. So, speaking about the difficulties during the solving of isomorphism of two groups problem which are assigned with finite number of generators and proportions the author notes, “that the assignment of finite groups by Cayley tables leads to analogous isomorphism problem”.

Lower, on the basis of special system of calculation, effective numeration is made, and on the set of these numbers group is assigned. With using of two permutations numbers, which assign finite group, method of the formal building of all group elements is proposed. The trivial solvability of problems of equivalence, identity law, conjugation of words in finite group is shown. Solvability of problem of finite groups isomorphism is proved and criterions of their isomorphism are offered. Some considerations about building of finite groups catalogue are expressed.

### **Effective numeration of permutations**

Effective numeration of mathematical objects sometimes is called *gödelisation* [7] in the honor of Kurt Gödel, he was one of the first mathematicians who used this procedure during proving of incompetence of arithmetic axioms [8].

Method of effective numeration of permutations is mentioned in authors article [9], there the main attention is concentrated on numeration of combinations, which is used for predication screening of “zero” terms during calculation of exact value of  $\pi(n)$  function (Offered by author methods of effective numeration of combinations and permutations (with suggestion of using possibility of last ones for description of groups) were arranged as article manuscript “About some formalizable procedures of combinatorial theory”. This manuscript was sent “Journal of calculus mathematics and

mathematical physics” but the answer from editorial office was “editorial portfolio is overfill” and it was recommended to apply to another journal).

For effective numeration of permutations special system of calculation with arcwise growing from digit to digit base  $n(c)$  is introduced. In the system of calculation  $n(c)$  unity of the second digit is in accord with “1”, - unity of the third digit is in accord with  $1 \cdot 2$ ,  $i + 1$  – number  $i!$ . By this system of calculation maximum possible set of digit numbers (which is written further in base-ten system) is given by  $(n-1)-(n-2)\dots 2-1-0$ . Conversion of the number from  $n(c)$  system of calculation to base-ten system  $n(10)$  is given by

$$n(10) = a_n \cdot (n - 1)! + a_{n-1} \cdot (n - 2)! + \dots + a_3 \cdot 2! + a_2 \cdot 1 + 0, \quad (1)$$

there  $a_i$  – number on the  $i$  – digit of  $n(c)$  during counting from right to left.

For example number 4-0-1-1-0 is in accord with decimal number

$$n(10) = 4 \cdot 4! + 0 \cdot 3! + 1 \cdot 2! + 1 + 0 = 99.$$

Number building in  $n(c)$  system from number in base-ten system  $n(10)$  is realized in reverse order. First, maximum possible number  $n!(10)$  is selected, by which given number  $n(10)$  is divisible, and  $n!(10)$  unities divisible by it is written to high order digit  $n(c)$ . Then residue of division is calculated and in the same way its division by  $(n - 1)!(10)$  is realized and so on down to divisor “1”.

Numbers  $n(c)$  are used only for recording of whole positive numbers. Then they are called *permutations codes* and denoted as  $K_i$ . The “ $i$ ” value in  $K_i$  equals  $n(10)$  number which is increased by one and which is calculated by (1). The quantity of digits, which contain code of  $K_i$ . permutation we call further code *rank*.

Further all permutations are formed from natural numbers  $1, 2, \dots, n$ . Biunivocal mapping between permutations codes and permutations themselves can be established. The validity of this statement is evident from the following theorem.

**Theorem1.** The number of permutations, which is formed from  $n$  elements equals to quantity of numbers in the interval from 0-0-...0 to  $(n-1) - (n-2) - \dots - 2 - 1 - 0$  in the  $n(c)$  system of calculation.

Proof.

Since the number of permutations from  $n$  elements equals  $n!$  then, for proving of Theorem1 statement, first let us present this numbers as the sum of two items:  $(n-1)!(n-1)+(n-1)!$ . Then let us take second component  $(n-1)!$  of acquired sum and also present it as the sum of two items and so on till, finally, we get item:  $1+1$ . Let us write down stated reforming as the following array:

$$\begin{aligned}
 n! &= (n-1)!(n-1)+(n-1)! \\
 (n-1)! &= (n-2)!(n-2)+(n-2)! \\
 (n-2)! &= (n-3)!(n-3)+(n-3)! \\
 &\dots\dots\dots \\
 (n-(n-2))! &= 1! \cdot 1 + 1!
 \end{aligned}
 \tag{1a}$$

Let us present the value of  $n!$  according to (1a) as the sum of items and compare this sum with sum (1) by  $a_{i_{\max}} = i - 1$ . It can be seen from this comparison that these sums differ from each other only by last pair of items: in expression (1a) this pair equals  $1+1$ , and in (1) –  $1+0$ . If we take “0” of the last pair as the first member of consequence (1), then we get proving of theorem1.

Each  $K_i$  code of  $l$  rank and further is in accord with  $M_i$  permutation from  $l$  natural numbers.  $K_1$  0-0-...-0 code is in accord with  $M_1 = 1,2,\dots,n$  permutation.  $M_i$  permutation is formed regarding  $K_i$  code by enclosed in each other cyclic shifts of  $M_1$  permutation by following rule.

Number which is on the  $i$  position of permutation code (during counting from left to right), shows for how many digits it is necessary to move elements of already formed intermediate permutation, beginning with element on the  $i+1$  position. All the process of moving begins from the very high-order digit, first left digit. The last, the very lower-order zero digit of  $K_j$  code, doesn't take part in cyclic shifts.

For example, let us form permutation  $M_j$  by code  $K_j = 3-1-2-1-0$ . After consistent cyclic shifts of  $M_j$  permutation we will get:

$$\begin{aligned}
 K_1 &= 0-0-0-0-0 & M_1 &= 1-2-3-4-5. \\
 K_{j1} &= 3-0-0-0-0 & M_{j1} &= 4-5-1-2-3.
 \end{aligned}$$

$$\begin{array}{ll}
K_{j_2} = 3-1-0-0-0 & M_{j_2} = 4-1-2-3-5. \\
K_{j_3} = 3-1-2-0-0 & M_{j_3} = 4-1-5-2-3. \\
K_{j_4} = 3-1-2-1-0 & M_{j_4} = 4-1-5-3-2.
\end{array}$$

As the result  $K_j = 3-1-2-1-0$  code is in accord with permutation  $M_j = 4-1-5-3-2$ . Conversion from permutation  $M_j$  to  $K_j$  code is made in reverse order. First, we take first number of the first position in permutation  $M_i$  and find it in permutation  $M_1$ . Then we calculate for how many positions it is necessary to move this number in  $M_1$  in order this number to be on the first (left) position. The received number of positions is carried instead of zero to high-order digit  $K_1$  and so we get  $K_{i1}$  code. After that we form permutation  $M_{i1}$  from permutation  $M_1$  by  $K_{i1}$  code. Then we choose number of the second  $M_i$  position and find in  $M_{i1}$  and calculate, as before, for how many positions it is necessary to move it in order to be on the second position of  $M_{i1}$ . The calculated number of positions is carried to second position of  $K_{i1}$  and so we get  $K_{i2}$  code and so on until we form the whole  $K_i$  code.

For example, it is necessary to form code of  $M_i = 5-1-3-2-4$  permutation. By carrying out operations given above we will get:

$$\begin{array}{ll}
M_1 = 1-2-3-4-5 & K_1 = 0-0-0-0-0 \\
M_{i1} = 5-1-2-3-4 & K_{i1} = 4-0-0-0-0 \\
M_{i2} = 5-1-2-3-4 & K_{i2} = 4-0-0-0-0 \\
M_{i3} = 5-1-3-4-2 & K_{i3} = 4-0-1-0-0 \\
M_{i4} = 5-1-3-2-4 & K_{i4} = 4-0-1-1-0.
\end{array}$$

As a result  $M_i = 5-1-3-2-4$  permutation is in accord with  $K_{i4} = 3-1-2-1-0$  code. Coincidence of  $K_{i1}$  and  $K_{i2}$  codes is explained by the absence necessity of any shifts in  $M_{i1}$  permutations.

### **Method for assignment of finite group**

Let us assign binary operation, which is used for building of finite group on the codes of permutations of the same rank, in the following way: product of  $K_i$  code by  $K_j$

code is in accord with  $K_l$  code, which is result of cyclic shift of  $M_i$  permutation by  $K_j$  code.

Let us write down stated operation in detailed way:

$$K_i \cdot K_j = (K_i \rightarrow M_i) \cdot K_j = M_l \rightarrow K_l \quad (2)$$

where “•” - binary operation symbol and “→” means procedure of conversion of code to permutation and vice versa.

Since rank of all codes and permutations, used below, is less than nine then, for short recording of  $M_i$  and  $K_j$  let us turn down hyphens (“-”) below. At that recording of permutation differs from code only by the zero on the end of the code.

For example, let us calculate the product of  $K_i = 0210$  and  $K_j = 3210$  codes. We have:

$$K_l = (0210)(3210) = (0210 \rightarrow 1432) \cdot 3210 = 2341 \rightarrow 1000.$$

Let us show that the set of codes of permutations of the finite rank  $n$  with given binary operation, assigned above, form group.

Indeed, as a unit  $I$  of the group we can take code  $K_1 = 00\dots0$ . For any  $K_i$  code there is the only one inverse unit  $K_i^{-1}$  and:

$$K_i \cdot K_i^{-1} = K_i^{-1} \cdot K_i = K_1.$$

The order of  $K_i^{-1}$  code forming differs from calculation of  $K_j$  code by permutation  $M_j$  only by that on the first stage of determination of  $K_{i1}^{-1}$  code the value of  $M_{i1}^{-1}$  is calculated not by permutation  $M_1$ , but by permutation  $M_i$  which is in accord with  $K_i$ . On each following calculation stage of  $K_{il}^{-1}$  we use accordingly permutation  $M_{i(l-1)}^{-1}$ , which was formulated earlier.

At that, during the process of consistent calculation of  $K_{il}^{-1}$  from initial permutation  $M_i$  we are building permutation  $M_1$ .

For example, it is necessary to calculate inverse code  $K_i^{-1}$  for  $K_i = 23110$  code. Given code is in accord with permutation  $M_i = 32541$ . During calculations we have:

$$\begin{aligned} K_{i1}^{-1} &= 40000 & M_{i1}^{-1} &= M_i \cdot K_{i1}^{-1} = 13254 \\ K_{i2}^{-1} &= 01000 & M_{i2}^{-1} &= M_{i1}^{-1} \cdot K_{i2}^{-1} = 12543 \end{aligned}$$

$$K_{i3}^{-1} = 00200 \qquad M_{i3}^{-1} = M_{i2}^{-1} \cdot K_{i3}^{-1} = 12354$$

$$K_{i4}^{-1} = 00010 \qquad M_{i4}^{-1} = M_{i3}^{-1} \cdot K_{i4}^{-1} = 12345.$$

So, we have  $K_i^{-1} = 41210$ , which is in accord with permutation  $M_i^{-1} = 52143$ . It is easy to see that  $K_i \cdot K_i^{-1} = K_i^{-1} \cdot K_i = K_1 = 00000$ .

Binary operation, which is assigned by (2) is associative because it unambiguously reflects all codes multitude of permutations into itself.

So, the multitude of all permutations codes with binary operation (2) is a group because it satisfies all group axioms.

During group assignment permutation codes are its generators.

Let us interpret *code  $K_i$  order* as the power, to which we have to raise this code in order to get  $K_1$  code (group unit). Further we designate group unit by zeroes ( $K_1$  code) or, for shot, by symbol “ $P$ ”.

We have following Theorem.

**Theorem 2.** Two permutations codes  $K_i$  and  $K_j$  of the same rank  $n$  with binary operation (2) assign concrete finite group and for any, assigned by some way finite group, there is at least one pair of permutations codes by which it is defined.

First, let us realize proof of the first part of theorem. Indeed, two generators can define any finite group as sub-group of symmetrical group [1]. By assignment of two permutations codes it is not necessary to assign determinative proportions of the group, because by virtue of constructiveness of generators we can get all of them automatically by multiplication of different powers of  $K_i$  and  $K_j$  codes in compliance with operation (2). So, we can formally examine all possible products  $K_i$  and  $K_j$  as determinative proportions of the group. Since binary operation (2) satisfies the axioms of the group and the number of codes is finite and is less or equal  $n!$  for the rank “ $n$ ” then all products of possible powers of  $K_i$  and  $K_j$  codes assign finite group. At that, if both codes  $K_i$  and  $K_j$  equal  $K_1$ , then the group is presented by one unit element. If even one of the codes equals  $K_1$ , then group is cyclic.

Let us prove the second part of the theorem.

Any sub-group of symmetrical group can be generated by two substitutions, which are presented as classical transpositions. Between procedure of transposition and procedure of generating of permutations with using of operation (2) it is possible to establish correspondence, which gives the same permutation. Therefore any sub-group of symmetrical group can be assigned by two codes. Since group, which generated by some way is finite, then we can find symmetrical group of finite order, in which this group is sub-group.

So theorem 2 is proved completely.

It is obvious that in theorem1 wording we can replace phrase “two codes of permutation” by the words “two whole positive numbers”.

As easy to see that requirement of codes ranks coincidence in theorem wording is fundamental. For example, it is impossible to multiply code 010 and code 1000, but it is possible to multiply 0010 and 1000. This is due to the fact that we have to use the same set of natural numbers for permutations. We can exclude this requirement, if only we examine cyclic shifts in some unlimited natural numbers sequence. However we have some difficulties during writing from left to right, which are connected with necessity to make shift from right to left or to write numbers from right to left. In the first case code 1000 is in accord with permutation 4-1-2-3-5-6, and in the second 6-5-3-2-1-4. Further we use constructions, which were described earlier. At that we can we can turn down unnecessary left zeroes in codes pair, for example instead of 0100 and 0200 we can use codes 100 and 200 because the result of the multiplication will not change.

It is reasonable that different codes pair can assign the same group and we will see that it is true in the context of the same symmetrical group.

Let us give an example of finite groups assignment with the help of codes. Any symmetrical group can be assigned by pair of codes 000...010 and 100...00. Quaternion group – by codes 10041000 and 42542210, and icosahedrons group – by 10000 and 01210. It is easy to check that given assignment of stated groups corresponds with the following assignment of the same groups in abstract generators:

$$a^n = b^2 = (ab)^{(n-1)} = I. \quad (3)$$

$$a^4 = b^4 = (ab)^4 = I. \quad (4)$$

$$r^5 = f^2 = (rf)^3 = I. \quad (5)$$

### Method for building of finite group

Let some finite group, which is assigned by to abstract generators  $f$  and  $r$ , be assigned in the form of multiplication table. At that we consider inner elements are written in incomplete way after using of defining proportions but in the form of products of the elements of upper line and left column. In this case proportions of such kind are used:

$$f^\alpha = I, r^\beta = I. \quad (6)$$

We identify further stated group multiplication table as *prototypal group table*. Prototypal table except elements of the upper line contains finite words, which are composed from different powers of generators  $f$  and  $r$ .

Let us make blank for three upper lines of prototypal multiplication table in the form of rectangular table 1.

Table 1.

Blank for three upper lines of group prototypal table

|     |     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|-----|
| $I$ | $f$ | $r$ | ... | ... | ... | ... | ... |
| $f$ | ... | ... | ... | ... | ... | ... | ... |
| $r$ | ... | ... | ... | ... | ... | ... | ... |

In the left upper corner of the table 1 stands one, in the second and third position of the first line and first column group generators are written.

Then by multiplication of the first generator  $f$  by the elements of the upper line we begin filling of the second line of table 1. Elements, which were got after multiplication with using proportion (6) and elements, which are absent in the upper line of the table 1 are carried in this line. At that process, of filling of the second line of the table, generator  $f$  is multiplied also by anew-appeared elements in the upper line,

until the process of new elements formation will end. This moment will necessarily come because we use proportions (6) and in this case upper line come up with in the second line by the number of filled squares.

After that in the similar manner we fill the line of the generator  $r$  and carry in it anew received and absent in the upper line elements. After ending of new elements formation we realize return to the line with generator  $f$  and so on until fulfillment of some restrictive condition.

This operation of fulfillment of stated lines of prototypal table we call generators *unfolding*. Let us identify fulfillment of one of the lines for  $f$  or  $r$  of table 1 as *unfolding step*.

Let us prove the following lemma.

**Lemma 1.** Totality of all elements of finite group prototypal multiplication table, which is assigned by two generators, can be derived after finite number of unfolding steps.

Indeed, since generators  $f$  and  $r$  (raised to a power one) are in turn multiplicands and we use proportions (6) then we form the word of any given structure after large enough number of unfolding steps. Naturally, that in the process of unfolding we will get other excess words.

For example, let us build generators unfolding table of dihedral group  $D_3$ . For this group:

$$f^2 = I, r^3 = I. \quad (7)$$

Prototypal table of  $D_3$ , which is built in [2], includes eighteen elements:  $I, r, r^2, f, fr, fr^2, rf, rfr, rfr^2, r^2f, r^2fr, r^2fr^2, ffr, ffr^2, ffr^2f, fr^2fr, fr^2fr^2$ .

$D_3$  generator unfolding table is given by table 2.

Table 2.

 $D_3$  generator unfolding table

|     |      |       |       |        |        |         |         |          |        |         |         |
|-----|------|-------|-------|--------|--------|---------|---------|----------|--------|---------|---------|
| $I$ | $f$  | $r$   | $fr$  | $rf$   | $r^2$  | $rfr$   | $r^2f$  | $r^2fr$  | $frf$  | $fr^2$  | $frfr$  |
| $f$ | $I$  | $fr$  | $r$   | $frf$  | $fr^2$ | $frfr$  | $fr^2f$ | $fr^2fr$ | $rf$   | $r^2$   | $rfr$   |
| $r$ | $rf$ | $r^2$ | $rfr$ | $r^2f$ | $I$    | $r^2fr$ | $f$     | $fr$     | $rfrf$ | $rfr^2$ | $rfrfr$ |

|          |           |     |           |     |             |     |           |     |            |
|----------|-----------|-----|-----------|-----|-------------|-----|-----------|-----|------------|
| $fr^2f$  | $fr^2fr$  | ... | $rfr^2$   | ... | $r^2fr^2$   | ... | $frfr^2$  | ... | $fr^2fr^2$ |
| $r^2f$   | $r^2fr$   | ... | $frfr^2$  | ... | $fr^2fr^2$  | ... | $rfr^2$   | ... | $r^2fr^2$  |
| $rfr^2f$ | $rfr^2fr$ | ... | $r^2fr^2$ | ... | $rfr^2fr^2$ | ... | $rfrfr^2$ | ... | $fr^2$     |

With the object of decreasing of table 2 size, unfolding of its generators is made only until the moment then all eighteen elements, which are stated above appear in upper line of the table.

Let us prove the following theorem.

**Theorem 3.** All elements of finite group, which is assigned by two permutations codes, can be derived with using of binary operation (2) after finite number of unfolding steps.

Proof. Since all codes are assigned then generative proportions (6) are assigned unambiguously, which are derived by codes involution. In accordance with theorem 2 pair of codes assign finite group and so there is prototypal group table for it. By cited above lemma 1 and using operation of codes (generators) unfolding we can derive all elements of prototypal table after finite number of steps. If at once we use binary operation (2) in the process of generators unfolding not only to proportions (6) but by all derived codes then we at once derive in final form first three lines of Cayley table, each of these lines contains totality of group elements.

Theorem is proved.

Further we use understandable phrase *group unfolding* and *group unfolding table*. For example, let us realize unfolding of  $D_3$  group. This group is assigned by two codes: 010 and 100. Unfolding table of this group is presented by table 3.

Table 3.

 $D_3$  group unfolding table

|     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|
| 000 | 010 | 100 | 210 | 110 | 200 |
| 010 | 000 | 210 | 100 | 200 | 110 |
| 100 | 110 | 200 | 010 | 210 | 000 |

Analysis of this table shows that totality of  $D_3$  group elements is present at all three lines of this table.

It is easy to see that all constructions cited above can be successfully used conformably to first three columns of multiplication group table. Let us note that in spite of “constructiveness” of the ways of assignment and construction of finite groups, nevertheless, constructed groups keep all properties of abstract groups.

### **Solvability of the main problems of group theory in finite groups**

Insolubility of stated in introduction problems is proved by means of group building with using of finite number of abstract generators and determinative proportions, for these proportions corresponding problems are insoluble. At that Post result is used, in which it is affirmed that the systems of “productions” is existed, for which there are no algorithm, which allows to indicate for any two words if they are equal or not.

The main group theory problem for finite groups, which are assigned by permutations codes, like problems of equivalence (equality), identity of words and conjugate words in group are trivial solvable. Let us formulate their solvability as consequences from proportions (2) and theorems 2 and 3.

Words  $W_1$  and  $W_2$  of group  $G$  are equivalent (equal) if they are differing by recording and present the same element. The problem of words equivalence consists in finding of algorithm, which after finite number of steps determines if any of two words

from the group are equivalent or not. By this wording of the problem there are no restrictions on the algorithm itself. We have

**Consequence 1.** The problem of words equivalence in finite group is solvable.

Indeed, after using in series of operation (2) for the words, which are made from the codes (generators) after all we will derive the answer on the stated question.

The problem of words identity is the particular case of the problem of equivalence and is formulated in the following way [1]: it is necessary to find algorithm, which allows for any group, which is assigned by finite number of generators and proportions, after finite number of steps to answer the question if some given word in this generators equals one or not, or to prove that this algorithm doesn't exist.

The problem itself appeared apparently because it was offered to solve the problem of equivalence by conversion of word  $W_2$  to  $W_1$  by deletion of the word, which equals  $I$  in the first of them.

**Consequence 2.** The problem of words identity in finite group is solvable.

Algorithm of problem solving remains the same as during establishment of words equivalence.

Because of consequence 1 the problem of conjugate words can be reduced to problem of conjugate group elements.

Group  $G$  elements  $a$  and  $b$  are conjugate in this group if we can find in  $G$  even one element  $g$ :

$$b = g^{-1}ag. \quad (8)$$

By multiplication of both parts of (8) by  $g$  from left, we will get

$$gb = ag. \quad (9)$$

Therefore the problem of conjugate group elements is reduced to the answer on such question: if we can find for these two elements  $a$  and  $b$  such element  $g$  in order to fulfill equality (9).

**Consequence 3.** The problem of conjugate elements in finite group is solvable.

Indeed, if the finite group is assigned by two codes, then by formulating by means of unfolding of its elements and substitution in (9) instead of element  $g$  all other elements except elements  $a$  and  $b$ , after finite number of steps we will derive the answer on stated question.

The group is considered as simple if it doesn't have own normal sub-groups. The problem of ascertainment of simplicity is reduced to finding of algorithm, which can after the finite number of steps to answer the question if even one of sub-groups of the group is normal divisor or not.

**Consequence 4.** If all sub-groups of the group  $G$  are known, then the problem of ascertainment of group simplicity is solvable.

To answer the question about simplicity of group it is enough for each of sub-groups, using operation (2), to formulate its left and right cosets. If these cosets mismatch for any of sub-groups, then the group is simple.

Other special problems can be solved by direct calculations. For example, in order to calculate left and right unknown multiplier in equations of such type:

$$xa = b, ax = b$$

it is enough to present them by the way of

$$x = ba^{-1}, x = a^{-1}b$$

and then in compliance with algorithm, which is stated above, it is necessary to calculate inverse element  $a^{-1}$  and to realize calculations.

The problem of isomorphism of two groups is also reduced to finding of algorithm, which allows to determine if these groups are isomorphous or not after finite number of steps. For finite groups this problem is solvable.

**Theorem 4.** The problem of isomorphism of two groups is solvable.

Let us present algorithm, which allows, after finite number of steps, to determine if these two groups, which are assigned by Cayley tables with the help of abstract generators, are isomorphous or not.

We consider further two groups  $G$  and  $G'$ , which have the same number of elements with assigned on them binary operations  $f$  and  $f'$ , isomorphous if one-to-one mapping of  $G$  group elements on  $G'$  group elements and such that for any elements of group  $G$   $a, b, c, d$ , the following equalities are fulfilled  $f(ab) = c, f(ba) = d$ , is existed, then for the four elements  $a', b', c'$  and  $d'$  from the group  $G'$ , which are in accord with them the following equalities are fulfilled  $f'(a'b') = c'$  and  $f'(b'a') = d'$ . At that if  $c = d$ , then  $c' = d'$ .

Let for groups  $G$  and  $G'$  of the  $n$  order Cayley tables are assigned. If group unit  $I$ , of the first line, occupies not the very left position, then, by means of table transformation, we move it on this position.

Let us number the elements of the upper line and first column of group  $G'$  table by natural numbers  $1, 2, \dots, n$ . By using further group  $G'$  multiplication table we will formulate for it Latin square in standard (reduced) form [10] and identify it as  $L_0'$ . All positions of this square will be filled by numbers from the interval  $1, 2, \dots, n$ . For isomorphism establishment between  $G$  and  $G'$  groups further we begin to form every possible Latin squares  $L_i$  of standard form for group  $G$  and compare them with the square  $L_0'$ . The maximum number of such squares equals  $(n - 1)!$ . All of them are formed on the basis of ordered set of elements of the upper line of  $G$  group table, which is taken as initial first permutation. Forming of all set of permutations is realized with the help of ascending sequence of permutation codes  $000\dots00, 000\dots010, 00\dots100, \dots, (n - 1)(n - 2)\dots210$  and it doesn't differ from above-stated. Each permutation is in accord with its Latin square of  $G'$  group. It is obvious that  $G$  and  $G'$  groups are isomorphous only in case when we can find Latin square  $L_j$ , which identical equals (i.e. is the copy) square  $L_0'$ . Otherwise groups are not isomorphous.

In other words, sufficient criterion of isomorphism of two groups  $G$  and  $G'$  of the same order is the presence of correspondence between group elements when their standard Latin squares identical equal each other. Existence of algorithm of Latin squares forming stated above proves theorem 4.

Fundamental idea in stated algorithm is the procedure of permutations forming, although isomorphism criterion (identity of Latin squares) is quite natural.

Let us examine an example of two groups, which are assigned for simplicity by permutations codes, isomorphism establishment. Let group  $G$  is generated by six permutations codes, which are given in table 4 with their order numbers. Further we use lower codes indexes for forming of permutations from elements.

Table 4.

$G$  group elements

|                  |                  |                  |                  |                  |                  |
|------------------|------------------|------------------|------------------|------------------|------------------|
| 000 <sub>1</sub> | 110 <sub>2</sub> | 200 <sub>3</sub> | 100 <sub>4</sub> | 210 <sub>5</sub> | 010 <sub>6</sub> |
| 1                | 2                | 3                | 4                | 5                | 6                |

Table 5.

$G'$  group elements

|      |      |      |      |      |      |
|------|------|------|------|------|------|
| 0000 | 0110 | 1200 | 2100 | 1010 | 2210 |
| 1    | 2    | 3    | 4    | 5    | 6    |

$G'$  group elements are presented in table 5. Let form Cayley tables for stated groups by using of binary operation (2) and then in compliance with their order numbers in tables 4 and 5 build, by Cayley tables, standard Latin squares. Initial Latin squares  $L$  and  $L'$  for  $G$  and  $G'$  groups are presented with tables 6 and 7 accordingly.

Table 6.

Latin square  $L_1$  for group  $G$

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 1 | 5 | 6 | 3 | 4 |
| 3 | 6 | 4 | 1 | 2 | 5 |
| 4 | 6 | 4 | 1 | 2 | 5 |
| 5 | 4 | 6 | 2 | 1 | 3 |
| 6 | 3 | 2 | 5 | 4 | 1 |

Table 7.

Latin square  $L_1'$  for group  $G'$

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 1 | 4 | 3 | 6 | 5 |
| 3 | 5 | 1 | 6 | 2 | 4 |
| 4 | 6 | 2 | 5 | 1 | 3 |
| 5 | 3 | 6 | 1 | 4 | 2 |
| 6 | 4 | 5 | 2 | 3 | 1 |

It is easy to see from comparison of Latin squares  $L_1$  and  $L_1'$  that they are different. This means that if we reflect  $G$  group elements on  $G'$  group elements in compliance with tables 6 and 7, then isomorphism fails. For example, product of element 2 on element 3 in group  $G$  equals 5 and in group  $G' - 4$ .

For further checking of groups  $G$  and  $G'$  for the purpose of isomorphism we will make permutations of elements of  $G$  group table 4, form Latin squares and compare them with square  $L_1'$ . Let us suppose that code 040000, which is in accord with permutation 162345, is formed. This permutation is in accord with mapping of  $G$  group elements on numbers 1...6, which are presented by table 8.

Table 8.

Table of  $G$  group elements arrangement for code 040000

|                  |                  |                  |                  |                  |                  |
|------------------|------------------|------------------|------------------|------------------|------------------|
| 000 <sub>1</sub> | 010 <sub>6</sub> | 110 <sub>2</sub> | 200 <sub>3</sub> | 100 <sub>4</sub> | 210 <sub>5</sub> |
| 1                | 2                | 3                | 4                | 5                | 6                |

If now for accordance of elements, which are presented by table 8, we generate Latin square, then it exactly repeats Latin square  $L_1'$ , which is presented in table 7. Therefore  $G$  and  $G'$  groups are isomorphous. Of course this was designed isomorphous presentation, which was generated by beforehand set, though in another presentation of dihedral group  $D_3$  (table 3) by  $G'$  group, unfolding table of  $G'$  group is presented by table 9

Table 9.

Unfolding table of  $G'$  group

|      |      |      |      |      |      |
|------|------|------|------|------|------|
| 0000 | 0110 | 1200 | 2100 | 1010 | 2210 |
| 0110 | 0000 | 2100 | 1200 | 2210 | 1010 |
| 1200 | 1010 | 0000 | 2210 | 0110 | 2100 |

Practical using of isomorphism criterion in the form of identity of group Latin squares needs large amount of calculations. The question arises as to whether exist easier criterions. The answer on this question is affirmative.

Let some finite group is presented by its unfolding table. For it by analogy with Latin square we will talk about three-lined standard *Latin rectangle*. We will identify *expansion* of group Latin rectangle as lines of Latin square, which is generated from the same group as rectangle. Let us prove the following lemma.

**Lemma 2.**  $G$  and  $G'$  groups, which have identical equal standard Latin rectangles, have identical equal expansions.

Proof. Identity of group Latin squares means that in unfolding process of their tables each step of group  $G$  unfolding exactly repeats  $G'$  group unfolding step. After supplement of the first columns of group Latin rectangles symmetrically to first line and multiplication of these elements we will derive Cayley tables for groups. Further let us convert Cayley tables to Latin squares. It is necessary to prove, that for extra generated products of group elements  $a_i \cdot a_j$  (where  $i = \overline{4, n}, j = \overline{1, n}$   $n$  – order of the group) will be fulfilled identity of elements order numbers in group Latin squares. Indeed, by virtue of proved above lemma 1 during building of group unfolding table, when we use only generating proportions (6), all products of elements of  $a_i \cdot a_j$  type for  $i \geq 4$  are present in this table in an explicit form. If other group generating proportions are used, then stated products are present in group unfolding table in an inexplicit form. If the products of stated elements for  $i \geq 4$  generate different structures of unfolding steps in  $G$  and  $G'$  groups then Latin rectangles of these groups are differ from each other. By the terms they are identically equal to each other and this means that expansions of their Latin rectangles will identically equal to each other.

Lemma is proved.

**Theorem 5.** Finite groups  $G$  and  $G'$ , for which at least one pair of identically equal standard Latin rectangles can be found, are isomorphous.

Indeed, by virtue of Lemma 2, identically equal Latin rectangles have identically equal expansions and therefore  $G$  and  $G'$  groups, by virtue of identity criterion of Latin squares, are isomorphous.

If we take into account that from two generators we can arrange only two permutations, then by using Latin rectangles as group isomorphism criterion it is necessary to construct  $2 \cdot C_{n-1}^2 = (n-1) \cdot (n-2)$  number of such rectangles.

However this number can be decreased. For that let us examine another isomorphism criterion for finite groups.

By assignment of finite groups by two abstract generators, for example  $a$  and  $b$  proportion of free group of such type:

$$(ab)^\gamma = I. \quad (10)$$

At that the group itself is assigned by such defining proportions:

$$a^\alpha = b^\beta = (ab)^\gamma = I. \quad (11)$$

Since during assignment of finite group by permutation codes it is enough to assign two generators  $a$  and  $b$  and all other elements of proportion (11) ( $ab, \alpha, \beta, \gamma$ ) are derived automatically, then we can use next isomorphism criterion of two finite groups – identity of “three powers  $\alpha\text{--}\beta\text{--}\gamma$ ”.

However here the question arises about uniqueness of assignment and unambiguity of presentation of concrete finite group. As a matter of fact such assignment of finite groups by proportions of (11) type is not only unique but can be ambiguous.

The fact that such assignment of group is not unique is easily confirmed by numerous examples with using permutation codes. So, for example, symmetrical group  $S_4$  can be assigned by two different proportions terms of (11) type

$$0010^2 = 1000^4 = 1110^3 = I. \quad (12)$$

$$2110^4 = 2100^3 = 3200^4 = I. \quad (13)$$

It is easy to check assignments equivalence of group  $S_4$  by proportions (12) and (13) by generating group unfolding tables.

It is remarkable here that different generators pairs generate the same group elements set. So unlike the problem of group isomorphism establishment here we have the problem of finding different group permutations codes pairs, which invariantly assign these groups. Finite solution, which differs from direct excess of codes pairs with the following generating of group unfolding table, is the interest here.

We can show ambiguity of group assignment by proportions of (11) type in such example.

For the groups, which are Cartesian product of cyclic groups  $C_2 \times C_4$  and with taking into account of group commutability ( $ab = ba$ ) the following defining proportions are presented in [2]

$$a^2 = b^4 = ab a^{-1} b^{-1} = I. \quad (14)$$

Taking into account, that  $a^{-1} = a$ ,  $b^{-1} = b^3$ ,  $b^{-2} = b^2$ , then it easy to reduce (14) to

$$a^2 = b^4 = (ab)^4 = I. \quad (15)$$

Let us assign in permutations codes the following two groups for three powers “2-4-4”

$$000010^2 = 100200^4 = 100210^4 = I. \quad (16)$$

$$20402000^2 = 76541210^4 = 56143210^4 = I. \quad (17)$$

It is easy to check with the help of group unfolding table that proportion (16) in fact is in accord with commutative group  $C_2 \times C_4$ , which contains 8 elements. Proportion (17) assigns cyclic group of the fourth order, which is sub-group of quaternion group. Element  $K_i = 76541210$ . is generator “ $a$ ” here. Analogous cyclic groups with terns “2-4-4” are derived in the context of symmetrical group  $S_4$  with generator  $K_i = 1100$  and  $K_j = 2010$ .

These examples show that we can apply isomorphism criterion of “power terns” identity only to two groups of the same type, i.e. to such groups, which are cyclic and no cyclic at the same time but commutative or, at last, not commutative. We can easily identify class of the groups by direct calculation, using two generating group permutations codes.

By using of the last groups isomorphism criterion the order of  $\alpha$ ,  $\beta$  and  $\gamma$  power sequence in proportion (11) is fundamental. However we should note, that some codes pairs, which are group generators, have the permutation property. For example icosahedral group can have the following defining proportions

$$1000^5 = 01210^2 = 11210^3 = I. \quad (18)$$

$$01210^2 = 11210^3 = 21110^5 = I. \quad (19)$$

$$11210^3 = 01210^2 = 10000^5 = I. \quad (20)$$

We can see from these proportions that power tern “5-2-3” can be reduced to power terns “2-3-5” and “3-2-5”.

However for group  $S_4$ , for example, which is assigned by proportion (12), during permutation of generators we derive

$$1110^3 = 1000^4 = 3200^4 = I. \quad (21)$$

As a result instead of power tern “2-4-3” in proportion (12) we derived tern “3-4-4” in proportion (21), i.e. tern powers turned to be not commutative.

Because of this, during using group isomorphism criterion by power tern it necessary check them for the purpose of commutation and constitution of new powers, at their lack of coincidence. It is necessary to use this criterion among the first and only then pass on to criterion of identity of Latin rectangles. At that, in the case of coincidence of elements in analyzed groups it is not of necessity to build all  $(n-1)(n-2)$  Latin rectangles. In this case for isomorphism establishment for two groups it is enough to take as initial two generating codes of one group and to find among the elements of another group two permutation codes, which could provide coincidence of power terns of both groups. If we can find such codes pair in the second group and by checking it turns out that groups are of the same type, then groups are isomorphous, and otherwise – not isomorphous.

### **Some considerations about building of finite groups catalogue**

Constructions, which are stated above, leave no fundamental difficulties for creation of catalogue of finite groups of some rational size. From our point of view it is reasonable to generate this catalogue by principle of symmetrical groups, which are unfolded in each other, beginning at  $S_1$  group. Since for each of the following symmetrical groups all previous are its sub-groups, then for creating of catalogue it is possible realize in the context of maximum possible symmetrical group  $S_n$ . The easiest, though very laborious method here is the method of generating of all groups on the basis of combinations of all possible codes pairs of group  $S_n$  permutation. Further, by using of isomorphism criterions in the form of power terns and Latin rectangles we can generate all sub-groups of  $S_n$  group. It is reasonable to put in catalogue left terns of proportions (11), which are separated by hyphen, number of group elements, information about it commutability, simplicity and so on. At that it is reasonable to

express groups, which are carried in catalogue, by the codes of minimum possible rank.

Let us demonstrate scheme of catalogue filling of finite groups by the example of  $S_4$  symmetrical group. Permutation codes of rank “4” their order and permutations themselves are presented in table 10.

Table 10.

Permutations and their codes of rank “4”

| $i$ | Permutation code and its order | Permutation | $i$ | Permutation code and its order | Permutation |
|-----|--------------------------------|-------------|-----|--------------------------------|-------------|
| 1   | 0000 <sup>1</sup>              | 1234        | 13  | 2000 <sup>2</sup>              | 3412        |
| 2   | 0010 <sup>2</sup>              | 1243        | 14  | 2010 <sup>4</sup>              | 3421        |
| 3   | 0100 <sup>3</sup>              | 1342        | 15  | 2100 <sup>3</sup>              | 3124        |
| 4   | 0110 <sup>2</sup>              | 1324        | 16  | 2110 <sup>4</sup>              | 3142        |
| 5   | 0200 <sup>3</sup>              | 1423        | 17  | 2200 <sup>3</sup>              | 3241        |
| 6   | 0210 <sup>2</sup>              | 1432        | 18  | 2210 <sup>2</sup>              | 3214        |
| 7   | 1000 <sup>4</sup>              | 2341        | 19  | 3000 <sup>4</sup>              | 4123        |
| 8   | 1010 <sup>3</sup>              | 2314        | 20  | 3010 <sup>3</sup>              | 4132        |
| 9   | 1100 <sup>4</sup>              | 2413        | 21  | 3100 <sup>2</sup>              | 4231        |
| 10  | 1110 <sup>3</sup>              | 2431        | 22  | 3110 <sup>3</sup>              | 4213        |
| 11  | 1200 <sup>2</sup>              | 2134        | 23  | 3200 <sup>4</sup>              | 4312        |
| 12  | 1210 <sup>2</sup>              | 2143        | 24  | 3210 <sup>2</sup>              | 4321        |

Possible beginning of modest enough by information, catalogue of finite groups can be such as it is shown in table 11.

Table 11.

Possible beginning of finite groups catalogue

| №  | Defining group proportions  | Number of elements in group | Group type |
|----|-----------------------------|-----------------------------|------------|
| 1. | $S_1$<br>$I - I - I$        | 1                           | $c$        |
| 2. | $S'_2$<br>$10^2 - I - 10^2$ | 2                           | $c$        |

|     |                            |        |     |
|-----|----------------------------|--------|-----|
|     | $S'_3$                     |        |     |
| 3.  | $010^2 - 100^3 - 210^2$    | $3!$   | $n$ |
| 4.  | $100^3 - 200^3 - I$        | $3$    | $c$ |
|     | $S'_4$                     |        |     |
| 5.  | $0010^2 - 1000^4 - 1110^3$ | $4!$   | $n$ |
| 6.  | $0100^3 - 1210^2 - 2100^3$ | $4!/2$ | $n$ |
| 7.  | $0010^2 - 2000^2 - 3200^4$ | $8$    | $n$ |
| 8.  | $1000^4 - 3000^4 - I$      | $4$    | $c$ |
| 9.  | $0010^2 - 1200^2 - 1210^2$ | $4$    | $a$ |
| ... | ...                        | ...    | ... |

In table 11 we identify  $S'_n$  as the set of group elements, which are not formed in previous groups. Letters  $c$ ,  $n$ ,  $a$  are correspondingly identified as cyclic, non-commutative and Abelian groups. Cyclic groups are presented by two generators in order to see the difference of their power terms from other groups, though it is not necessary. Groups №№ 1,2,3 and 5 from table 11 are symmetrical groups  $S_1$ ,  $S_2$ ,  $S_3$  and  $S_4$  and №4 and №6 – are correspondingly alternate groups  $A_2$  and  $A_4$ , though some of them have special name [2]. Group №7 is non-commutative group of the 8th order. Unlike quaternion group it contains forth group (№9) as sub-group. Group №8 is cyclic group of the forth order. Of course practically created catalogue must be much more informative and besides other group characteristics can contain about discoverers of single groups.

The created group catalogue can be taken as basic. Finite groups uses can create their own catalogues in which groups of the base catalogue can be isomorphly presented by permutation codes of higher rank. For example instead of forth group №9 in table 11 we can use isomorphous to it group with defining proportions

$$000010^2 = 140000^2 = 140010^2 = I. \quad (22)$$

Transition to permutation codes of higher rank raises, in a certain sense, informative superfluity of group elements. Using of abstract generators for assignment

of finite groups unites group as numerical construction. Therefore the problem of development of the method, which allows generating isomorphous groups to codes of different (higher or lower) ranks, has the right to exist. If we take into account that permutation code is original record of some whole positive number then in more general form the problem is formulated in such way: to find the method, which allows to form classes of isomorphous to each others in pairs finite groups from pairs of whole positive numbers. There can be particular, narrower, this target setting.

So, assignment of finite group by permutation codes makes from it numerical construction, which is definite enough and all main problems can be solved by direct calculation.

### References

1. Kurosh A.G. Group theory, M., 1967.
2. Grossman I., Magnus W. Groups and their graphs, Random house, The L.W. Singer company, 1964.
3. Kargapalov M.I., Merzlyakov Y.I. Fundamentals of group theory, "Science", M., 1977
4. Novikov P.S. About algorithmic insolvability of the problem of words identity in group theory, works math. Institute AS USSR 44(1955).
5. Novikov P.S. Insolvability of the problem of contingency in group theory, news. AS USSR, ser. Math. 18(1954).
6. Adyan S.I. Insolvability of some algorithmic problems of group theory, works. Moscow math. Soc. 6(1957).
7. Selecta Mathematica II, Herausgegeben von Konrad Jacobs, Springer-verlag, Berlin · Heidelberg · New-York, 1970.
8. Kleene S.C. Introduction to metamathematics, D. Van Nostrand company, inc., New-York, Toronto, 1952.

9. Golikov V.P. Rational algorithm for calculation of distribution of prime numbers function value, Double technologies №4, 2003.
10. Mathematical encyclopedia, volume 3, "Soviet encyclopedia", M., 1982.