Research and Reports on Mathematics

Short Communication

A SCITECHNOL JOURNAL

Two Algorithmic Problems in Group Theory

Alexander P Goryushkin*

Department of Mathematics and Physics, Kamchatka State University, Russia

***Corresponding author:** Alexander P Goryushkin, Professor, Department of Mathematics and Physics, Kamchatka State University, Petropavlovsk-Kamchatsky, Russia, E-mail: as2021@mail.ru

Received Date: August 16, 2018; **Accepted Date:** December 18, 2018; **Published Date:** December 25, 2018

Abstract

For individual classes of groups, a relationship is established between the existence of an algorithm for calculating the index of a subgroup and the algorithm for solving the problem of occurrence.

Keywords: Direct product; Almost free group; Algorithmic problem; Solvability; Occurrence problem; Index problem

Introduction

In recent years, difficult algorithmic problems in group theory have found practical application in cryptography. A difficult or even algorithmically unsolvable group-theoretic problem can be a reliable basis for cryptographic protection of the protocol. For cryptographic applications, the classical problems of Dan (the word problem, the conjugacy problem and the isomorphism problem) are of interest, and the algorithmic problems in group theory that are closely related to the classical ones. Such are the problem of the occurrence and the problem of the index.

The occurrence problem for a finitely presented group G consists in finding or proving the impossibility of an algorithm that for any finite set of elements *hi (i = 1, 2, ..., m)* and *w* would know whether or not the element w belongs to the subgroup *H = rp (h1 , h2, ..., hm)* generated by the elements *hi*. From the algorithmic solvability of the problem of occurrence follows the solvability of the problem of equality. Therefore, the problem of occurrence is also called the generalized equality problem.

The index problem for a finitely presented group *G* consists in finding an algorithm that, for any finite set of elements *hi (i = 1, 2, ..., m)* of *G*, would recognize that a finite or infinite index in *G* has a subgroup *H = gr (h1, h2 , ..., hm)* generated by this set.

A finitely generated group contains only a finite number of subgroups for every given finite index. Therefore, if the problem of occurrence and the index problem are solvable in *G*, then having obtained information that the index of the subgroup *H* in *G* is finite, it is possible to calculate this index in a finite number of steps by a simple search of subgroups of finite index (for a description of such an algorithm see, for example, [1]).

For a particular group *G*, computing its order is not a mass problem. However, if *G* is infinite, then there are subgroups of infinite and finite indices. Such indices have, for example, trivial subgroups, but it is possible that in *G* there are other subgroups, both finite and infinite index. If *G* is an infinite simple finitely presented group, then the solvability of the index problem follows from the solvability in *G* of the occurrence problem, since in this group only one subgroup of finite index is itself *G*.

However, the reverse situation with simple groups is more complicated. It was shown in [2] that every countable group is isomorphically embeddable in a two-generated simple group. In particular, a finitely presented group *S* with an unsolvable problem of equality (and hence an unsolvable entry problem) is also isomorphically imbedded in a simple two-generated group *G*. In each recursively defined simple group, the word problem is solvable [3]. This means that a two-generated simple group containing such a group *S* is not only not definite, it cannot even be recursively represented.

The classical Kronecker-Capelli theorem of linear algebra is essentially an algorithm for solving the problem of entering into a subspace of a finite-dimensional vector space. This algorithm consists in calculating the smallest possible number of elements in the generating system. This number - dimension - is found by means of a sequence of changes in the generating set of the subspace and its transformation into a basis.

To find the index of a finitely generated subgroup *H*, in the same way one can find a generating set *H* consisting of the smallest number of elements. The generating set of a subgroup is modified by means of elementary transformations analogous to elementary transformations of the generating set of a subspace of a vector space:

(1) replacing the element *x* by x^{-1};

(2) replacing the element *x* by an element *x y*, where $x \neq y$;

(3) removal of a single element.

If as a result of such transformations a single element appears, then this unit from the generating set can be deleted.

Let $H = gr(h_1, h_2, ..., h_m)$ be a finitely generated subgroup of the free group F_n. A system of free generators for a subgroup H is called a basis, and the number of elements in a basis is called a rank. This basis is the Nilsen set of generators see, for example, [4]. Let *R* be some set of elements from the free group F_r written in the reduced, that is, irreducible, form. Elements of the set *R* are words in the alphabet a_1, a_2, ..., a_r and their inverses, and abbreviations inside words are impossible. The symbol R^{-1} denotes all the inverse elements of *R*. A word *w* in F_r is said to be isolated with respect to the set *R* if there is at most one element *v* in $R \times R^{-1}$ such that w is an initial or terminal subword for *v*. The leading beginning of the word *v* is the initial subword s of the word *v* whose length satisfies the inequality

$$\frac{l(v)}{2} < l(s) \leq \frac{l(v)}{2} + 1.$$

Similarly, the leading end of the word *v* is defined.

The set *R* of non-unitary, incontractible words is said to be Nielsen if:

1) the older beginnings and the upper ends of all words from *R* are isolated;

2) for each word of even length, at least one of its halves - left or right - is isolated.

Using the transformations (1) - (3) of the generating set in a finite number of steps, one can obtain the Nilsen generators for the subgroup H, and thus find the rank of H. This method of obtaining free generating subgroups of free is usually called the Nielsen method.

Using the Nielsen method, it is possible in a finite number of steps to find out whether an element of the free group enters or does not belong to a given finite generated subgroup, that is, the occurrence problem for free groups is algorithmically solvable.

Otto Schreyer, using not only the generating elements of a subgroup, but also representatives of adjacent classes, established a connection between the index of a subgroup of a free group, the rank of this subgroup, and the rank of the original free group, see, for example, [4]. If a subgroup H of rank k has finite index in a free non-cyclic group of rank r, then this index is equal to

$$\frac{k-1}{r-1}.$$

Using the Schreier formula, the index problem of a subgroup of a free group reduces to calculating the rank of a subgroup, which can be found using the Nielsen method.

Thus, the index problem for a free group is also algorithmically solvable.

We call a group G almost free if it contains as a subgroup of finite index a free non-cyclic group F. If a finitely presented group G is almost free, then its free subgroup F has finite rank; in addition, we can assume that F is normal in G.

The solution of both problems under discussion for an almost free group is reduced to solving this problem for the free part F.

In an almost free group, both the index problem and the problem of occurrence are solvable.

A free group is a free product of infinite cyclic groups. In an infinite cyclic group, both problems were algorithmically solvable, and both of them were inherited under a free product.

Let us now consider another important group-theoretic construction-the direct product.

Each element of the direct product A × B has a representation in the form of the product ab, where a × A and b × B.

The element ab is equal to one if and only if a and b are both single. This means that if the equality problem is algorithmically solvable in groups A, B, then this problem is solvable in the direct product A×B. In other words, the solvability of the equality problem is inherited by the direct product. The solvability of the index problem in such a construction may not be inherited.

Theorem

In the direct product of two almost free groups, the index problem is algorithmically unsolvable.

Evidence

Let groups A and B be two almost free groups. The group A contains, as a normal subgroup of finite index, a free subgroup A1 of rank m; and the elements a1, a2, ..., am are free generators for A1. Similarly, the group B contains a normal subgroup B1, where B1 is free of rank m and b1, b2, ..., bm-ee are its free generators. In addition, both indices are $[A : A_1]$ and $[B : B_1]$ finite.

If the group $G = A \times B$ is a direct product of the groups A and B, then its subgroup G_1 generated by the subgroups A_1 and B_1 forms a direct product:

$G_1 = A_1 \times B_1$.

The index G1 in G is equal to $[A : A_1]\ [B : B_1]$, and is therefore finite.

We now consider an arbitrary finitely presented group R given by the representation

$R = \langle r_1, r_2, \ldots, r_k; w_1(r_i), \ldots, w_n(r_i) \rangle$.,

where r1, r2, ..., rk are generating elements, and w1 (ri), ..., wn (ri) are defining relations. Recall that the defining relation is a word in the alphabet r1, r2, ..., rk, $r_1^{-1}, r_2^{-1}, \ldots, r_k^{-1}$...., In the group A1 we choose a subgroup P of index s in A1 such that inequality $s \geq \frac{k-1}{m-1}$.

Then by the Schreier formula the rank of the subgroup P is equal to $s(m-1)+1$, and this number is not less than k. If the rank of the subgroup P turns out to be strictly greater than k, then the representation of the group R is supplemented by s-k generators and equates these elements to unity. Without loss of generality, we can assume that this has already been done, that is, s = k.

Let the elements $p_1, p_2, \ldots, p_k$ freely generate the subgroup P. In the group B_1 we choose a subgroup Q of rank k, of index s in $B1$ and with free generators $q_1, q_2, \ldots, q_k$.

We now consider two normal subgroups, one in the group P and the other in Q. In the group P, the normal subgroup N_1 generated by the elements $w_1(r_i), \ldots, w_n(r_i)$, and in the group Q the normal subgroup $N2$ generated by the elements $w1(q_i), \ldots, w_n(q_i)$. More precisely,

$N_1 = \langle w_1(r_i), \ldots, w_n(r_i) \rangle P$;

$N_2 = \langle w_1(q_i), \ldots, w_n(q_i) \rangle Q$.

In the group G_1 we take two subgroups:

$H_1 = rp(w_1(q_i), \ldots, w_n(q_i), p_1q_1, \ldots, p_kq_k)$;

$H_2 = rp(w_1(p_i), \ldots, w_n(p_i), p_1q_1, \ldots, p_kq_k)$.

The elements r_i, q_i lie in different direct factors of G_1, therefore they commute:

$r_i\, q_i = qi\, r_i$.

This means that for any word ϕ the equality

$\phi(p_iq_i) = \phi(p_i)\, \phi(q_i)$.

The conjugation of the element $w_j(p_i)$ by means of an element of H_1 is equal to the corresponding conjugation by means of an element of the subgroup A. Hence it follows that the subgroup H_1 contains N_1. Similarly, H_2 includes N_2.

In addition, the subgroups H_1 and H_2 themselves coincide. Let $H = H_1 = H_2$; then:

$H \cap P = N_1$;

$H \cap Q = N_2$.

The Hasse diagram for the inclusion of subgroups [Figure 1] represents all the links between all these groups. If the subgroup H has a finite index in the direct product $A \times B$, then the index H in the subgroup $A_1 \times B_1$ is also finite, which means that the indices N_1 and N_2 are finite in the subgroups P and Q, respectively. This means that the group R is finite. Conversely, if the group R is finite, then the indices N_1 and N_2 in the subgroups P and Q are also finite; but P and Q are subgroups of finite index in direct factors, and hence the index is $[G_1 : H]$ finite, and $[G : H]$ therefore also finite.

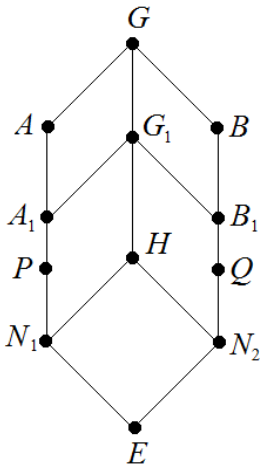

Figure 1: Hasse Diagram, representing the groups.

In other words, the index problem in the group G is equivalent to the finiteness problem in the class of all finitely presented groups.

The finiteness problem for groups is algorithmically unsolvable [5], and, hence, the index problem for a finitely determined group is also algorithmically undecidable.

The assertion is proved.

Algorithmic unsolvability of the problem means that there is no machine solution for such a problem. For example, no technique will ever be able to answer the question, whether a finite or infinite index of an arbitrarily chosen finitely generated subgroup in the group $F_2 \times F_2$, given by the representation

$< a, b, c, d; aca^{-1}c^{-1}, ada^{-1}d^{-1}, bcb^{-1}c^{-1}, bdb^{-1}d^{-1} >.$

We note that in some cases the calculation of the index of a finitely generated subgroup in a finitely determined group can be entrusted to the technique. True, the result can be obtained, as a rule, only in the case of a finite (and relatively small) index of the subgroup. Computer calculations of this kind associated with the solution of specific problems in group theory are presented in [6-9].

For the direct product of two free groups of the second rank, the problem of occurrence is also unsolvable [10]. The proof of this assertion in [9], carried out for only one group $F_2 \times F_2$, is also carried over to the general case of a direct product of almost free non-cyclic groups.

Thus, there arises an infinite series of finitely presented groups for which the occurrence problem and the index problem turn out to be equivalent - both are undecidable.

On the other hand, in an almost free group both problems: both the problem of occurrence and the index problem are algorithmically solvable. It is known that a free product inherits the solvability of the problem of occurrence [11].

Using Nielsen's method, which was improved by the Moldovan method [12], it can be shown (see, for example, [1]) that for the solvability of the index problem in the free product $A \times B$, the solvability of the occurrence problem in groups is sufficient.

This sufficient condition for the existence of an algorithm that computes the index of a subgroup is also necessary: If the index problem is solvable in a nontrivial free product $A \times B$, then the occurrence problem is solvable in the free factors A and B.

The algorithm from [1] that solves the index problem in the free product $A \times B$ does not use the solvability of the index problem in the factors A and B. Therefore, the natural question arises: is it true that the decidability of the index problem in free factors follows the solvability of the index problem in the free product ?

The converse is also interesting: is it true that the decidability of the index problem in a free product implies the solvability of the index problem in free multipliers?

From positive answers to both questions, the following statement would follow: in the class of finitely presented groups the problem of occurrence is algorithmically equivalent to the index problem.

References

1. Goryushkin A (2012) Amalgamated free products of groups. Fed University, Vladivostok: Publishing house Dalnevost, Russia.
2. Goryushkin AP (1974) Imbedding of countable groups in 2-generated simple groups. Mathematical Notes. 16: 725-727.
3. Kuznetsov AV (1958) Algorithms as operations in algebraic systems. Uspekhi Mat. Nauk 13: 240-241.
4. Lyndon RC, Shupp PE (1980) Combinatorial group theory Mir 12: 448.
5. Adyan SI (1955) Algorithmic unsolvability of recognition problems for certain properties of groups, Dokl. Academy of Sciences of the USSR 103: 533-535.
6. Goriushkin AP (2013) Features of computer research of discrete group. Ser Phys Math Science 1: 43-55.
7. Goryushkin A (2011) The machine solution of problems of discrete mathematics. Ser Phys Math Science 2: 58-68.
8. Goryushkin AP (2010) On groups with the representation. Ser Fiz Mat Science 1: 8-11.
9. Goryushkin A (2011) Elements of Abstract and Computer Algebra: A Tutorial. Petropavlovsk-Kamchatsky: KamSU them Vitus Bering.
10. Mikhailova KA (1968) The occurrence problem for free products of groups. Matematicheskii Sbornik 117: 199-210.
11. Mikhailova SA (1968) The problem of occurrence for free products of groups. Mat Coll 2: 199-210.
12. Moldavansky DI (1969) Nielsen's method for the free product of groups. Uch Zap Ivanov state ped Institute 61: 170-182.