On the decidability of some problems in special classes of groups

by

A. Włodzimierz Mostowski (Warszawa)

1. Introduction.

1.1. Problems considered. In the group theory almost every problem is undecidable. A very large list of undecidable problems is given in Baumslag, Boone, and Neumann's paper [3]. The undecidability of most of those problems follows from the undecidability of the word problem, which was proved by Novikov [14], cf. also Britton [6] and others.

The aim of this paper is to construct algorithms to decide various problems, for wide classes of groups, in which those problems are decidable. We shall investigate the class of residually finite groups, and similar classes. Algorithms are given to decide the word problem, the inclusion problem, and the conjugacy problem, in some classes of groups. The algorithms are based on the residual properties of groups in those classes.

The idea of the paper is based on McKinsey's method presented in [13]. Some results announced by Malcev in [11] are proved. Some further results are obtained. One of them is a positive solution of the conjugacy problem for nilpotent groups—a problem which was first posed by Malcev. The other new result is the decidability of the problem of isomorphism with a given finite group, in the class of all groups with decidable word problem.

1.2. Notions and notation. Proving the decidability of group-theoretical questions lies in proving that some sets of words are recursive. The notion of recursivity and recursive enumerability, and theorems on recursive functions are used. For those theorems, cf. Kleene [9]. Various results concerning the decidability or undecidability problems, investigated in Tarski, Robinson, and Mostowski's book [16], are also used.

In order not to make the proofs too long and boring, the treatment of metamathematical notions is mostly informal and intuitive. Only the

formulations of the results, and the most difficult steps of the proofs are a little more formalized.

At the end of this introduction the author wishes to express his gratitude to his tutor professor Jerzy Łoś, for sympathetic interest and helpful and stimulating suggestions during the preparation of this paper.

2. Presentations and classes of groups.

2.1. Finite presentations of groups. For any set of objects X, we shall denote by $F(X)$ the free group which is generated by elements of X. For any subset $R \leqslant F(X)$ we shall denote by $N(R)$ the *normal closure* of R in $F(X)$. We shall say that the pair $P=(X, R)$ is a *presentation* of a group $G = G(X, R)$ iff G is isomorphic to the factor group $F(X)/N(R)$. Then the group G is a group with defining relations $r(x_1, \ldots, x_n) = 1$ for $r \in R$ and generators $x_1, \ldots, x_n \in X$. We shall say that a group is *finitely presented* (briefly an *f.p. group*) iff there exists a presentation $P = (X, R)$ of the group such that both X and R are finite.

When presenting a group, it is sometimes convenient to distinguish among the relations, those which hold identically in the group. Then as a presentation we have a triple $P = (X, R, V)$, where $R \leqslant F(X)$ and V is a set of words consisting of other symbols [1]. Then we shall say that the presentation P is a presentation of a group $G = G(X, R, V)$ with identical relations V iff the group G is isomorphic to the factor group $F(X)/N(R)\cdot V^{F(X)}$ [2]. Here $V^{F(X)}$ denotes the word subgroup of $F(X)$ defined by V. It is the subgroup of $F(X)$ (necessarily fully invariant) generated by elements which are obtained by substituting any elements of $F(X)$ on the variables in the words belonging to V.

Then for $v(y_1, \ldots, y_m) \in V$ the relation

$$v(y_1, \ldots, y_m) = 1 \tag{2.1.1}$$

holds identically in G. The set of relations: $r(x_1, \ldots, x_n) = 1$ for $r \in R$ complemented by those which follow from identities (2.1.1) is a set of defining relations for G.

When V is finite, then there exists a single word v generating the same word subgroup as V. E.g. when $V = \{v_1(y_1, \ldots, y_n), v_2(y_1, \ldots, y_n)\}$ then the word v is

$$v(y_1, \ldots, y_{2n}) = v_1(y_1, \ldots, y_n)\cdot v_2(y_{n+1}, \ldots, y_{2n}) .$$

[1] The elements of V need not be words in X. They are treated in the sequel as group-theoretic functions in some variables. They change into words from $F(X)$ when a substitution of elements from $F(X)$ on the variables is made.

[2] There $A\cdot B$ denotes the set of products $a\cdot b$ for $a \in A$ and $b \in B$. If A and B are subgroups, one of them normal, then $A\cdot B$ is a group.

We shall say that a group is an *almost finitely presented group* (briefly an a.f.p. group) iff among all presentations of the group there exists such a presentation $P = (X, R, V)$ that X, R and V are finite. The finitely presented groups are a.f.p. groups; we can take as V a set composed of an empty word.

2.2. Residually finite groups. A group G is called *residually finite* (briefly an r.f. group) iff for any element $g \in G$, $g \neq 1$, there exists a homomorphism φ_g of G such that $\varphi_g(G)$ is finite and, moreover, $\varphi_g(g) \neq 1$. An equivalent definition is that a group is an r.f. group iff it can be imbedded in an unrestricted direct product of finite groups. From this definition one can easily see that the class of r.f. groups is closed under subgroup and direct product operations. The examples in the sequel show that this class is not closed under homomorphic images.

The class of r.f. groups is large. It contains free groups, solvable free groups, nilpotent free groups (cf. Gruenberg [8]), and finitely generated nilpotent groups (see the next section).

2.3. Separation of subgroups. We shall say that a group G is a *group with separable subgroups* (briefly an *s.s. group*) iff for any subgroup H of G, and any element $g \notin H$, there exists a homomorphism φ such that $\varphi(G)$ is finite, and $\varphi(g) \notin \varphi(H)$. Any s.s. group is an r.f. group, because the former definition is a special case of the latter when $H = \{1\}$. The notion of s.s. algebras was introduced and investigated by Malcev [11]. The class of s.s. groups is closed under subgroup and finite direct product operations. In Malcev's paper mentioned above a criterion is given for a solvable group to be an s.s. group, which is a necessary and sufficient condition in the case of torsion-free solvable groups. From this criterion it follows that finitely generated nilpotent groups are s.s. groups, but, say, the solvable free groups (non-abelian) are not.

2.4. Conjugacy separable groups. A group G is called a *conjugacy separable group* (briefly a *c.s. group*) if for any two elements $g_1, g_2 \in G$, which are non-conjugate in G, there exists a homomorphism φ of G onto a finite group G_1 such that the images $\varphi(g_1)$ and $\varphi(g_2)$ remains non-conjugate in G_1.

One can easily observe that c.s. groups are closed under a finite direct product. An important result concerning the question of the magnitude of the class of c.s. groups is Blackburn's result [4], stating that finitely generated nilpotent groups are c.s. groups.

3. Recursivity and decidability.

3.1. Lemmas for recursively enumerable sets of words. For a finite or a countable set X of any symbols, the set of all words in X, i.e. the group $F(X)$ is countable. It can be effectively mapped

one to one onto the set of natural numbers such that the function leading from a pair of numbers of words f and g to the number of the word $f.g$ is a recursive function (3).

The question whether or not the word problem is decidable in a class $\mathfrak{T}$ of presentations is the question whether or not for any $P(X, R, V)$ from $\mathfrak{T}$ the normal subgroup $U = N(R) \cdot V^{F(X)}$ is a recursive subset of $F(X)$. This is because $f(x_1, \ldots, x_n) = 1$ holds in the group $G(X, R, V)$ iff $f(x_1, \ldots, x_n) \in U$.

A useful method of proving that a set $U \in F(X)$ is recursive is to prove that both U and $F(X) \setminus U$ are recursively enumerable.

In this paragraph we shall prove some useful lemmas concerning recursively enumerable subsets of $F(X)$. These are the following:

LEMMA 1. *For any recursively enumerable subset R of $F(X)$ and a recursively enumerable set V of words in other symbols, the subgroups*

$$\{R\},\ N(R),\ \text{and}\ V^{F(X)}$$

are recursively enumerable.

LEMMA 2. *For any recursively enumerable subsets U and W of $F(X)$ the set $U \cdot W$ of products $u \cdot v$, where $u \in U$ and $w \in W$, is recursively enumerable.*

Both lemmas are almost trivial, even in the case where X is countable.

For $U = (u_1, u_2, \ldots)$ and $W = (w_1, w_2, \ldots)$, both of which are recursively enumerable sets, we order the products $u_i \cdot w_j$ (i.e. the couples of indices i, j) as is done in Cantor's proof that $\aleph_0 \cdot \aleph_0 = \aleph_0$, make the reductions in the strings $u_i \cdot w_j$, then by omitting the repetent words we obtain a recursively enumerable sequence of all elements of $U \cdot W$. The proof of lemma 2 is completed (4).

To prove that $\{R\}$ is recursively enumerable for R recursively enumerable, we note that $R^* = R \cup R^{-1}$ is recursively enumerable. Now by lemma 2 the sets R_i^*, where $R_1^* = R^*$, $R_{i+1}^* = R_i^* \cdot R^*$, are recursively enumerable. Then the sum

$$\bigcup_{i=1}^{\infty} R_i^* = \{R\}$$

is recursively enumerable.

In the case of $N(R)$, we define the recursively enumerable sets R_i^* for $i = 1, 2, \ldots$ as follows: $R_1^* = R^* \cup \{1\}$, and for $i > 1$,

$$R_i^* = \bigcup_{\lambda_1 \leqslant i, \ldots, \lambda_l \leqslant i} f_{\lambda_1}^{-1} R_1^* f_{\lambda_1} \ldots f_{\lambda_l}^{-1} R_1^* f_{\lambda_l}$$

(3) "Recursive" here always means "general recursive".

(4) Note that we cannot state that $U \cdot W$ is recursive for recursive U and W, since reductions in strings have been made.

where $f_1 = 1, f_2, \ldots, f_i, \ldots$ is a recursive sequence of all words from $F(X)$. The conclusion of the lemma follows from the fact that

$$\bigcup_{i=1}^{\infty} R_i^* = N(R).$$

In the case of $V^{F(X)}$, let us note that by making in a word $v(y_1, \ldots, y_k)$ from V all possible substitutions of elements from $F(X)$ for the variables $y_1, \ldots, y_k$ and then making reductions, we obtain a recursively enumerable set of words. Let us denote this set by $R(v)$. Then if $V = (v_1, v_2, \ldots)$ is a recursively enumerable set, then the set $V^* = \bigcup_{i=1}^{\infty} R(v_i)$ is recursively enumerable. Since $V^{F(X)} = \{V^*\}$, the proof is reduced to the proof of the first case of the lemma. This completes the proof.

As a corrollary to lemmas 1 and 2 we obtain:

LEMMA 3. *For any recursively enumerable U, R, and V, the subgroups $\{U\} \cdot N(R)$ and $\{U\} \cdot N(R) V^{F(X)}$, as well as the normal subgroup $N(R) \cdot V^{F(X)}$ of $F(X)$, are recursively enumerable. The set X is supposed to be finite or countable.*

3.2. A recursive sequence of homomorphisms. The aim of this paragraph is to describe all homomorphisms of a group $G(X, R, V)$ into finite groups.

Let X be a finite set of any objects $X = (x_1, x_2, \ldots, x_t)$; the set X can be turned into a finite group of order t if we define a multiplication table

$T =$

	x_1	x_2	$\ldots$	x_t
x_1	x_{1_1}	x_{1_2}	$\ldots$	x_{1_t}
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
x_t	x_{t_1}	x_{t_2}	$\ldots$	x_{t_t}

such that each row and column is a permutation of symbols from X, and the operation $x_i \cdot x_j = x_{i_j}$, defined by the table, is associative. Then the table T gives a presentation $P(T) = (X, R)$, where R is a set of words $x_i \cdot x_j \cdot x_{i_j}^{-1}$ for $i, j = 1, 2, \ldots, t$ of the group X with multiplication defined by the table.

For any t there is a finite number of non-isomorphic group tables, and thus a finite number of presentations $P(T)$ of non-isomorphic groups of order t. By ordering the presentations in a sequence

$$P_1, P_2, P_3, \ldots \tag{3.2.1}$$

first one presentation of the trivial group of order 1, then all presentations of the groups of order 2 (there is only one), and so on, we obtain

a recursive sequence of some special presentations of all finite groups, up to isomorphism. For any presentation $P = (X, R)$ with finite X and finite R, there is a method of deciding whether or not P is in the sequence (3.2.1), and to compute its position in the sequence.

Note that no sequence of all presentations of finite groups is recursive; cf. Adjan [1] or Rabin [15].

Let $P = (X, R, V)$ be a presentation of a group $G = G(X, R, V)$ and $\bar{G}$ a group with a presentation $\bar{P} = (\bar{X}, \bar{R})$ in the sequence (3.2.1). A necessary and sufficient condition for a mapping μ of X into $\bar{X}$ to be extendable (uniquely) to a homomorphism of G into $\bar{G}$, is:

(*) *For any* $r(x_1, \ldots, x_n)$ *from* R: $r(\mu(x_1), \ldots, \mu(x_n)) = 1$ *in* $\bar{G}$, *and moreover* $V^{\bar{G}} = \{1\}$.

Since the set of elements of the group $\bar{G}$ equals $\bar{X}$, a homomorphism φ of G into $\bar{G}$ is uniquely described by a mapping μ of X into $\bar{X}$, which satisfies condition (*). This proves that for a finite X the set of all homomorphisms of G into $\bar{G}$ is finite, since the set of all mappings from a finite set X to a finite set $\bar{X}$ is finite. More interesting is the fact that in the case where R and V are finite, one can effectively check whether or not a mapping μ of X into $\bar{X}$ can be extended to a homomorphism of G into $\bar{G}$. That is so by a special form of the presentation of $\bar{G}$ by a table T.

For any mapping μ of X into $\bar{X}$, the elements $\mu(x_1)\cdot\mu(x_2)$ or $\mu(x_1)^{-1}$ belong to $\bar{X}$, and can be computed for any x_1, x_2 from X by using the table T (or relations from $\bar{R}$). Thus it can be effectively checked whether or not a relation $r(\mu(x_1), \ldots, \mu(x_n))$ holds, for any r from R. In a quite similar way it can be effectively checked for any v from V whether or not $v = 1$ holds identically in the group $\bar{G}$.

Note that from the above considerations it follows that one can effectively check whether or not a mapping μ of X into $\bar{X}$ can be extended to a homomorphism of G onto $\bar{G}$. We need only to check in addition whether or not $\mu(X)$ generates $\bar{X}$, which can be done effectively by a special form of the presentation $\bar{P}$.

Now we shall deduce some conclusions from the given method of descriptions of homomorphisms of G into $\bar{G}$ by some mappings of X into $\bar{X}$.

Let us form for a sequence (3.2.1) of presentations $P_1, P_2, \ldots$, a sequence of homomorphisms of $G = G(X, R, V)$

$$\varphi_1, \varphi_2, \varphi_3, \ldots, \tag{3.2.2}$$

each homomorphism φ_i being described by a mapping of X into a set X_{i_j} of generators in a presentation P_{i_j}. The method of forming (3.2.2) is the following: First we set all homomorphisms of G into $G_1 = G(P_1)$, then all homomorphisms into $G_2 = G(P_2)$, and so on.

Thus we have proved that the sequence (3.2.2) is a recursive sequence of homomorphisms since for any mapping μ of X into some X_j we can effectively check whether or not μ determines a homomorphism of G into $G_j = G(P_j)$. Moreover, in the case where μ determines a homomorphism we can compute its position in sequence (3.2.2).

This gives the following

LEMMA 4. *There exists a recursive sequence* (3.2.1) *of some finite presentations of all finite groups and for any a.f. presentation of a group a sequence of suitably described homomorphisms of the group such that it is a recursive sequence of all homomorphisms* (*up to isomorphism*) *of the group into finite groups.*

The case where a presentation is finitely generated but infinitely related by a recursive set of relations, i.e. X is finite and R infinite but recursive is still an open problem. In this case there is a finite number of mappings μ of X into $\bar{X}$, but to check whether or not a mapping μ can be extended to a homomorphism we have to check an infinite number of relations in the group $\bar{G}$. In this case, is the sequence (3.2.2) a recursive one or not?

4. Decidability of some problems.

In this section we shall give some proofs concerning the decidability of some questions, basing ourselves on the results given in section 3.

4.1. The word problem. By using the results of section 3.2 it is easy to prove McKinsey's result (cf. [13]) stating that the word problem is decidable in the class of all r.f. groups.

For the proof we have to show that for any a.f. presentation $P = (X, R, V)$ of a r.f. group there is an effective method of deciding for any word $f(x_1, \ldots, x_n)$, $x_1, \ldots, x_n \in X$, whether or not

$$f(x_1, \ldots, x_n) = 1$$

in the group $G(P)$.

In an other formulation of that problem we have to prove that the subgroup $N(R)\cdot V^{F(X)}$ of $F(X)$ is recursive if X, R, and V are finite.

It has been proved (lemma 3) that $N(R)\cdot V^{F(X)}$ is recursively enumerable. It remains to prove that $F(X)\setminus N(R)\cdot V^{F(X)}$ is recursively enumerable in the case where the group $G(X, R, V)$ is an r.f. group. Then we shall obtain the following lemma:

LEMMA 5. *If a group with an a.f.p.* $P = (X, R, V)$ *is an r.f. group, then the subgroup* $N(R)\cdot V^{F(X)}$ *of* $F(X)$ *is a recursive set.*

Proof. Let $f(x_1, \ldots, x_n) \notin N(R)\cdot V^{F(X)}$. Then by the assumption of residual finiteness of the group $G = G(X, R, V)$, there exists a homomorphism φ_i of G onto a finite group $G_{j_i} = G(P_{j_i})$ such that $\varphi_i(f(x_1, \ldots, x_n))$

$\neq 1$. The homomorphism φ_i occurs in the sequence (3.2.2). There is an effective method of constructing the homomorphisms φ_i in the sequence and checking whether or not $\varphi_i(f(x_1, \ldots, x_n)) = 1$ in the group G_{j_i}, presented by a presentation P_{j_i} from the sequence (3.2.1) (since each G_{j_i} is finite with explicitly given elements and group multiplication given by a table; cf. section 3.2). This proves that the set of f which do not belong to $N(R)\cdot V^{F(X)}$ is a set of values of a certain recursive function. So $F(X)\setminus N(R)\cdot V^{F(X)}$ is a recursively enumerable set. This completes the proof of the lemma.

We shall state the result of lemma 5 as the following theorem.

THEOREM 1. *The word problem is decidable relative to the class of all r.f. groups.*

We now give some remarks concerning theorem 1.

The word problem is undecidable relatively to the class of all groups. There exists a finite presentation $P = (X, R)$ such that the subgroup $N(R)$ of $F(X)$ is not recursive. For this result, see Novikov [14], Britton [6], or others.

The question whether or not a finite presentation is a presentation of an r.f. group is undecidable. This is an easy result from Adjan [2], theorem 1, when we take as the property a_0 the property of being an r.f. group. For other results of this type, cf. Adjan [1] and Rabin [15].

Theorem 1 is well known. It is a special case of McKinsey's result [13] concerning the decidability of elementary sentences of special type for various classes of algebras. The theorem states that the word problem is decidable for a group when we know that the group in question is an r.f. group.

Now we shall list some consequences of theorem 1.

COROLLARY. *The word problem is decidable relatively to the class of*

(a) *finite groups*;

(b) *free groups*;

(c) *solvable free groups*;

(d) *nilpotent groups of any nil*;

For the proof cf. section 2.2.

Now we shall give some explanations of these results. In case (a) the result is that when we have a presentation of a group, and we know that the group is finite, then the word problem is decidable for the presentation. The result is well known, cf. McKinsey [13]. Let us note that the question whether or not the group is finite is undecidable, cf. Adjan, loc. cit. on the p. 8.

In case (c) the result can also be deduced from McKinsey's result, and is well known; many mathematicians have known it, but I could not find it in literature. Result (d) is one of the oldest; I believe it was first obtained by Malcev [10].

Now we shall make some remarks concerning result (b). The statement is: When we have a finite presentation $P = (X, R)$, and we know that $G(X, R)$ is a free group (a group which is free in the class of all groups), then there exists a decision method for the word problem for $G(X, R)$.

Remark. Statement (b) is false for infinite presentations. In Britton's paper [5], example 2, page 50, a presentation $P = (S, R)$ is given with an infinite set S of generators and a recursive set R of relations for which the word problem is undecidable. It is easy to observe that the group $G(S, R)$ from Britton's example is a free group of infinite rank. The idea of Britton's example is based on the existence of a recursive function with (recursively enumerable) non-recursive set of values.

4.2. The inclusion problem. Now we shall investigate a non-elementary problem—the inclusion problem. It consists in recognizing for any words $f, h_1, \ldots, h_s$ with variables in $X = (x_1, \ldots, x_n)$ whether or not

$$f(x_1, \ldots, x_n) \in \{h_1(x_1, \ldots, x_n), \ldots, h_s(x_1, \ldots, x_n)\} \tag{4.2.1}$$

in a group with an almost finite presentation $P = (X, R, V)$.

The word problem is a special case of the inclusion problem in the case where the group generated by $h_1, \ldots, h_s$ is trivial. From this remark it follows that the inclusion problem is undecidable in the class of all groups. In this section we shall prove the result announced in Malcev's note [11]. The result is given by theorem 2.

THEOREM 2. *The inclusion problem is decidable relatively to the class of all subgroup separable groups.*

The proof given below is very similar to that of theorem 1. It is based on lemma 3, and on the recursivity of the sequence (3.2.2) of homomorphisms.

The theorem will be proved when we show that for any almost finite presentation $P = (X, R, V)$ of an s.s. group the subgroup $W = \{h_1, \ldots, h_s\}\cdot N(R)\cdot V^{F(X)}$ of $F(X)$ is recursive, since

$$f(x_1, \ldots, x_n) \in W \quad \text{in } F(X)$$

is equivalent to (4.2.1) in the group $G(X, R, V)$.

By lemma 3 the subgroup W is recursively enumerable. We shall prove that $F(X)\setminus W$ is recursively enumerable.

Let $f \notin W$. Then by the s.s. property of the group $G(X, R, V)$ there exists a homomorphism φ of G into a finite group $\bar{G}$ such that $\varphi(f) \notin \varphi\{h_1, \ldots, h_s\}$. The homomorphism φ is in the sequence (3.2.2). Since every $G(P_j) = G_j$ is explicitly given by the presentation $P_j = (X_j, R_j)$

in sequence (3.2.1), as the set X_j with multiplication defined by a table described by R_j we can decide for any j, in a finite number of steps, whether or not $\varphi_i(f) \in \varphi_i(\{h_1, \ldots, h_s\})$ in the group G_{j_i}, for $i = 1, 2, \ldots$ After a finite number of steps we find $\varphi_i = \varphi$ and $G_{j_i} = \bar{G}$. Thus we can decide in a finite number of steps, that $f \notin W$.

This completes the proof of the theorem.

4.3. The conjugacy problem. This problem consists in recognizing for any words f_1 and f_2 in variables in $X = (x_1, \ldots, x_n)$ whether or not:

(4.3.1) *there exists a word* $h(x_1, \ldots, x_n)$ *such that*

$$f_1(x_1, \ldots, x_n) = h(x_1, \ldots, x_n)^{-1} f_2(x_1, \ldots, x_n) h(x_1, \ldots, x_n)$$

holds in a group with an almost finite presentation $P = (X, R, V)$.

As before, we translate the problem to a problem concerning some inclusion questions in the group $F(X)$. Let S be the set of elements: $h(X)^{-1} \cdot f_1(X) \cdot h(X)$ for $h(X) \in F(X)$, and W the set $S \cdot N(R) \cdot V^{F(X)}$. The sentence (4.3.1) in the group $G(X, R, V)$ is equivalent to the sentence

$$f_2(x_1, \ldots, x_n) \in W$$

in the group $F(X)$. It differs from the sentence appearing in the inclusion problem only in the definition of the set W. In the definition we have, instead of a subgroup, a class of conjugates.

We shall prove that W is recursive. The set S is recursively enumerable and so by lemmas 2 and 3 the set W is recursively enumerable. It remains to prove that $F(X) \setminus W$ is recursively enumerable.

Suppose that f_2 does not belong to W. Then the elements f_1 and f_2 are non-conjugate in $G(X, R, V)$. By the c.s. property of the group, there exists a homomorphism φ of $G(X, R, V)$ onto a finite group $\bar{G}$, such that $\varphi(f_1)$ and $\varphi(f_2)$ are non-conjugate in $\bar{G}$.

For a φ_i of $G(X, R, V)$ into $G(P_{j_i})$, where φ_i is in sequence (3.2.2) and P_{j_i} in sequence (3.2.1), we can decide, in a finite number of steps, whether or not φ_i is a homomorphism onto. That is so by the special form of the presentation P_{j_i}, cf. section 3.2. In the case where φ_i maps $G(X, R, V)$ onto $G(P_{j_i})$ we can find in a finite number of steps the class of conjugates of $\varphi_i(f_2)$. That is so because by the special form of the presentation $P_{j_i} = (X_{j_i}, R_{j_i})$, where the multiplication of elements in X_{j_i} leads to an element of X_{j_i} given by the relation from R_{j_i}, both $\varphi_i(f_2)$ and the conjugates of $\varphi_i(f_1)$ are elements of X_{j_i}. Doing so for $i = 1, 2, \ldots$, we shall find after a finite number of steps the G_{j_i} isomorphic to $\bar{G}$, and φ_i equal to φ (up to isomorphism). Thus we can effectively check that $\varphi(f_1)$ and $\varphi(f_2)$ are non-conjugate. In other words, we can effectively check that f_2 does not belong to W. This proves that $F(X) \setminus W$ is recursively enumerable.

The only assumption we have made to prove that W is recursive was that the group $G(X, R, V)$ was a c.s. group. Thus we have proved the following theorem:

THEOREM 3. *The conjugacy problem is decidable relatively to the class of conjugacy separable groups.*

The theorem is strictly connected with Blackburn's result, which states that nilpotent groups are c.s. groups (cf. section 2.5, or [4]), and gives the answer to the question, posed by Malcev, whether or not the conjugacy problem is decidable for nilpotent groups. The answer is given by the following corollary.

COROLLARY. *The conjugacy problem is decidable relatively to the class of all nilpotent groups.*

As far as I know, there has been only one note concerning the decidability of the conjugacy problem for nilpotent groups. This is Goldina's note with a positive solution in the case of metabelian free groups (cf. [7], p. 530). Notwithstanding a few incorrect results announced in this note, this one is correct.

5. Groups with a decidable word problem.

5.1. Isomorphism problem. The isomorphism problem consists in deciding for any two finite presentations P and Q whether or not the groups $G(P)$ and $G(Q)$ are isomorphic. The problem is undecidable in the class of all finite presentations, even when we ask whether or not a group is isomorphic with a given group, e.g. a finite one (cf. loc. cit. [1] or [15]). We shall prove in this section the following theorem.

THEOREM 4. *The question whether or not a group is isomorphic with a given finite group is decidable relatively to a class of f.p. groups with the word problem decidable.*

The proof divides into two parts, which are very similar to each other.

First it must be proved that, having a presentation of a finite group, we can find the number i of the presentation P_i in sequence (3.2.1) of the group. Secondly it must be proved that for any finite presentation of a group with the word problem decidable and for any $i = 1, 2, \ldots$ we can decide whether or not the group is isomorphic to the group $G(P_i)$. Since any finite group is a group with the word problem decidable, it is quite obvious that the proof of the second part covers the proof of the first part.

Proof. Let $\bar{P} = (\bar{X}, \bar{R})$ be a presentation in the sequence (3.2.1), and φ a homomorphism from (3.2.2) for a group $G(X, R, V)$. Let $X = (x_1, \ldots, x_n)$ and $\bar{X} = (\bar{x}_1, \ldots, \bar{x}_t)$. Then $\varphi(x_i) = \bar{x}_{\alpha(i)}$ for $i = 1, \ldots, n$, where $\alpha(i)$ is a function from integers to integers $1, \ldots, t$. According to the remark on page 128, we can decide whether or not φ is a homo-

morphism onto $\bar{G}$. If φ is not a homomorphism onto, it is not an isomorphism either. When φ is onto, we can effectively find some words $f_1(x_1, \ldots, x_n), \ldots, f_t(x_1, \ldots, x_n)$ such that for $j = 1, \ldots, t$

$$\varphi\big(f_j(x_1, \ldots, x_n)\big) = \bar{x}_j .$$

In particular, we shall choose the words so that:

$$f_{\alpha(i)}(x_1, \ldots, x_n) = x_i \quad \text{for} \quad i = 1, \ldots, n . \tag{5.1.2}$$

Now φ is an isomorphism iff the mapping

$$\nu(\bar{x}_j) = f_j(x_1, \ldots, x_n) \quad \text{for} \quad j = 1, \ldots, t ,$$

can be extended to an homomorphism of G into $\bar{G}$. Indeed, if φ is an isomorphism, then φ^{-1} is an extension of ν to a homomorphism. Conversely, if there is an extension of ν to a homomorphism ψ, then by (5.1.2) we have

$$\psi\big(\varphi(x_i)\big) = x_i \quad \text{for} \quad i = 1, \ldots, n .$$

Then $\psi\varphi$ is an identity mapping and so by finiteness of $\bar{G}$, φ is an isomorphism.

The group $\bar{G}$ has a finite number of explicitly given relations. To check whether or not ν can be extended to a homomorphism, we need only to check, for a finite number of $\bar{r} \in \bar{R}$, whether or not

$$\bar{r}\big(f_1(x_1, \ldots, x_n), \ldots, f_t(x_1, \ldots, x_n)\big) = 1$$

holds in G. Since G is a group with a decidable word problem, that question is decidable.

This ends the second part of the proof, and by previous remarks the proof of the theorem.

5.2. Determination of nilpotency. The question whether or not the group is nilpotent is undecidable in the class of all groups. This is an easy result from Adjan's paper [2] cited on p. 130 when we take as the property α_0 the property: a group is nilpotent. But we have the following theorem:

THEOREM 5. *The problem whether or not a group is nilpotent of a given nil is decidable relatively to the class of all groups with the word problem decidable.*

The proof is an immediate consequence of the fact that by lemma 3 from paper [12] the nilpotency of a given nil, for a finitely generated group with given generators, follows from the finite number of explicitly given relations in generators.

Let us note that from theorem 5 it does not follow that the problem whether or not a group is nilpotent (of any nil) is decidable relatively to all groups with the word problem decidable.

A note added in proof. Theorem 1 on p. 130 with an outline of the proof, was announced in the abstract: V. Huber Dyson, *The word problem and residually finite groups*, AMNS 11 (1964), 666-7, p. 743.

References

[1] S. I. Adjan, *Algorifmičeskaja nierazrešimost' problem rozpoznavanija niekotoryh svoistv grupp* (in Russian), DAN 103, pp. 533-535.

[2] — *Koniečno opredelennye gruppy i algorifmy* (in Russian), Uspiehi Mat. Nauk 12 (1957), pp. 248-249.

[3] G. Baumslag, W. W. Boone, B. H. Neumann, *Some unsolvable problems about elements and subgroups of groups*, Math. Scand. 7 (1955), pp. 191-201.

[4] N. Blackburn, *Conjugacy in nilpotent groups*, Proc. Amer. Math. Soc. 16 (1965), pp. 143-148.

[5] J. L. Britton, *Solution of the word problem for certain types of groups, I*, Proc. Glasgow Math. Ass. 3 (1956), pp. 45-54.

[6] — *The word problem for groups*, Proc. London Math. Soc. 8 (1958) pp. 493-506.

[7] N. P. Goldina, *Svobodnyje nilpotentnye gruppy* (in Russian), DAN 111 (1956), pp. 528-530.

[8] K. W. Gruenberg, *Residual properties of infinite soluble groups*, Proc. London Math. Soc. 7 (1957), pp. 29-62.

[9] S. C. Kleene, *Introduction to metamathematics*, Van Nostrand 1952.

[10] A. I. Malcev, *Dva zamiečania ob nilpotientnych gruppah* (in Russian), Mat. Sbornik 37 (1955), pp. 567-572.

[11] — *O homomorfizmah na koniečnye gruppy* (in Russian), Uspiehy Matičeskich Nauk 13 (1958), pp. 237-238.

[12] A. W. Mostowski, *Computational algorithms for deciding some problems for nilpotent groups*, Fund. Math. this volume, pp. 137—152.

[13] J. C. C. McKinsey, *The decision problem for some classes of sentences*, J. Symb. Logic 8 (1943), pp. 61-76.

[14] P. S. Novikov, *On the algorithmic unsolvability of the word problem in group theory*, Trudy Inst. im. Stieklowa 44 (1955), also in American Math. Soc. Transactions.

[15] M. O. Rabin, *Recursive unsolvability of group theoretic problems*, Ann. of Math. 67 (1958), pp. 172-194.

[16] A. Tarski, A. Mostowski, R. M. Robinson, *Undecidable theories*, North Holland 1953.

Reçu par la Rédaction le 19. 6. 1965