Mathematics

Academician A. I. MAL' TSEV

1961

SovietRxiv

Abstract

Full Text

Mathematics

Academician A. I. MAL' TSEV

THE UNDECIDABILITY OF THE ELEMENTARY THEORY OF FINITE GROUPS

In connection with the study of elementary theories of various classes of algebras, the question naturally arose of the algorithmic decidability of the elementary theory of the class of all finite groups. This question is mentioned as an open problem in the well-known book by A. Tarski, A. Mostowski, and R. Robinson ([1]). In the present note it is proved that the elementary theory of the class of all finite groups is undecidable. In the course of the proof, and as corollaries, the undecidability of the elementary theories of some other classes of finite groups, and also of some classes of rings and semigroups, is established.

No. 1. Let K be an arbitrary fixed field. Denote by $\mathfrak{R}$ the class of all (nonassociative) rings that are finite-dimensional algebras over K. By *formulas* we shall mean formulas of the narrow predicate calculus whose only nonlogical symbols are the symbol of equality of elements and the symbol of multiplication. The formula $ax = x \;\&\; x^2 = x \;\&\; x \neq 0$ will be abbreviated by (a, x). The individual object symbols a, b will play a special role below. A formula $\mathfrak{A}(a, b)$ with individual object symbols a, b will be called *normal* if $\mathfrak{A}$ is the conjunction of some formula $\mathfrak{A}_1$ with the same individual object symbols and of the formulas

a1) $(x)(y)(x \neq y \;\&\; (a, x) \;\&\; (a, y) \to xy = x \vee yx = y \;\&\; xy \neq 0 \vee yx = 0)$,

a2) $(x)(y)(z)((a, x) \;\&\; (a, y) \;\&\; (a, z) \;\&\; xy \neq 0 \;\&\; yz \neq 0 \to xz \neq 0)$,

a3) $a^2 = 0 \;\&\; (x)((a, x) \to xa = 0)$,

a4) $ab = 0 \;\&\; (x)(y)((a, x) \;\&\; (b, y) \to xy = 0) \;\&\; ba = a$

and the formulas b1, b2, b3, obtained from a1, a2, a3 by replacing the symbol a by the symbol b. A ring $R \in \mathfrak{R}$ will be called an $\mathfrak{A}$-ring if in it there are distinguished elements a, b for which $\mathfrak{A}(a, b)$ is a true sentence in R, i.e., if the closed formula $(\exists a)(\exists b)\mathfrak{A}(a, b)$ is true in R. An element x of an $\mathfrak{A}$-ring R will be called an a-element if the formula (a, x) is true.

Modifying the basic definition from ([2]), we shall say that a formula $\mathfrak{A}$ *represents a function* $f(m)$ in the class $\mathfrak{R}$, if the following conditions are satisfied: 1) the formula $\mathfrak{A}$ is normal; 2) in every $\mathfrak{A}$-ring from the class $\mathfrak{R}$ that contains m a-elements, there are exactly $f(m)$ b-elements ($m = 0, 1, 2, ...$); 3) for every $m = 0, 1, 2, ...$, there exists in $\mathfrak{R}$ an $\mathfrak{A}$-ring having m a-elements.

Theorem 1. *For every normally given general recursive function $f(m)$, one can effectively construct a formula $\mathfrak{A}$ representing this function in the class $\mathfrak{R}$.*

By J. Robinson's theorem ([3]), Theorem 1 will be proved if formulas representing the functions $\lambda(m) = m + 1$, $\rho(m) = m - [\sqrt{m}]^2$, are constructed, and if an effective method is indicated for constructing formulas,

representing the functions $g(x) + h(x)$, $g(h(x))$, $g^{-1}(x)$, under the condition that formulas representing the functions $g(x)$, $h(x)$ are given. Here we shall construct only formulas for the functions $m+1$ and $g^{-1}(x)$, since the others are constructed analogously.

Denote by $\mathfrak{A}(a, b, c)$ the conjunction of formulas a1—a4, b1—b3 and the formulas

$$(x)((a, x) \to (b, cx)); \tag{1}$$

$$(x)(y)((a, x)\ \&\ (a, y)\ \&\ cx = cy \to x = y); \tag{2}$$

$$\begin{aligned}(\exists z)[(b, z)\ \&\ (x)((a, x) \leftrightarrow cx \neq z)\ \&\ (y)(y \neq z\ \&\ (b, y) \to \\ \to (\exists x)((a, x)\ \&\ y = cx))].\end{aligned} \tag{3}$$

The formula $(\exists c)\mathfrak{A}$ represents the function $m + 1$. Indeed, suppose that in some ring $R \in \mathfrak{R}$ there exist elements a, b, c possessing properties (1), (2), (3). According to (3), the set of b-elements of R consists of the element z, determined by requirement (3), and all a-elements multiplied by c. Since by virtue of (2) the multiplication of distinct a-elements by c gives distinct b-elements, the number of b-elements in R is greater by 1 than the number of a-elements.

To construct an $\mathfrak{R}$-ring having a prescribed number m of a-elements, take an algebra over K with basis $a, b, c, x_1, \dots, x_m, y_1, \dots, y_{m+1}$ and introduce for the basis elements the relations

$$ba = a, \quad ax_i = x_i = x_{ix}i; \quad cx_i = y_i; \quad by_j = y_j = y_{jy}j\ (i \leq j;\ i, j = 1, 2, \dots).$$

All remaining pairwise products of basis elements are set equal to 0. It is clear that the algebra obtained will be an $\mathfrak{R}$-ring in which the a-elements are $x_1, \dots, x_m$.

No. 2. Let some function $g(m)$ be represented by the formula $\mathfrak{A}(a, b)$, and suppose that the equation $g(x) = m$ is solvable for every $m = 0, 1, 2, \dots$. By definition, the symbol $g^{-1}(m)$ denotes the least solution of the indicated equation. Introduce a formula $\mathfrak{A}(a, b; p)$, expressing the following requirements: a) the totality R_p of elements x satisfying the condition $px = x$ is a subring; b) the elements a, b belong to R_p; c) in R_p the formula $\mathfrak{A}(a, b)$ is true. In other words, $\mathfrak{A}(a, b; p)$ is the conjunction of the formula

$$(x)(y)(px = x \ \& \ py = y \to p(xy) = xy) \ \& \ pa = a \ \& \ pb = b$$

and the relativization of the formula $\mathfrak{A}(a, b)$ to the set of elements x satisfying the condition $px = x$.

Denote by $\mathfrak{B}(a, b, a', b', p)$ the conjunction of the formula $\mathfrak{A}(a', b'; p)$ and the formula

$$(x)\{px = x \ \& \ (a', x) \to (\exists uvde)[\mathfrak{A}(u, v; d) \ \& \tag{4}$$

$$\& \ (y)((a', y) \ \& \ py = y \ \& \ yx = y \ \& \ y \neq x \to d \cdot ey = ey \ \& \ (u, ey)) \ \& \tag{5}$$

$$\& \ (y)(z)((a', y) \ \& \ py = y \ \& \ pz = z \ \& \ (a', z) \ \& \ y \neq z \to ey \neq ez) \ \& \tag{6}$$

$$\& \ (y)((u, y) \ \& \ dy = y \to (\exists z)(pz = z \ \& \ (a', z) \ \& \ xz = 0 \ \& \ y = ez)) \ \& \tag{7}$$

$$\& \ (\exists f)(y)(y')(py = y \ \& \ (b', y) \ \& \ (b', y') \ \& \ py' = y' \ \& \ fy = fy' \to y = y' \ \& \tag{8}$$

$$\& \ d \cdot fy = fy \ \& \ (v, fy) \ \& \ (\exists z)(dz = z \ \& \ (v, z) \ \& \ fy \cdot z \neq fy) \ \vee$$

$$\vee \ (\exists f)(y)(y')(dy = y \ \& \ (v, y) \ \& \ (v, y') \ \& \ dy' = y' \ \& \ fy = fy' \to y = y' \ \&$$

$$\& \ p \cdot fy = fy \ \& \ (b', fy) \ \& \ (\exists z)(pz = z \ \& \ (b', z) \ \& \ fy \cdot z \neq fy)) \ \&$$

$$\& \ (x)((a', x) \leftrightarrow px = x \ \& \ (b', x) \ \& \ (x)((b, x) \leftrightarrow px = x \ \& \ (d', x)))\}. \tag{9}$$

The formula $\mathfrak{B}(a, b, a', b'; p)$, together with the formulas a1–a4, b1–b3, defines the function $g^{-1}(m)$. Indeed, suppose that in the ring $R \in \mathfrak{R}$ there are elements a, b, a', b', p such that in R the formula $\mathfrak{B}$ is true and the number of a-elements in R is equal to m. The formula $\mathfrak{A}(a', b')$ is true in R_p, and R_p is

subring, the set of b'-elements of which coincides with the set of a-elements of the ring R, while the set of a'-elements of R_p, by virtue of (9), coincides with the set of b-elements of R. Therefore $m = g(n)$, where n is the number of b-elements

in R. By a1—a3, the a'-elements of R_p can be denoted by the symbols $x, \dots, x_n$ so that the relations $x_i x_j = x_i x_i = x_i,\ x_{jx} i = 0\ (i < j)$ will hold for them. According to (4), for each $x_i,\ 1 \leq i \leq n$, there will be found in R elements u, v, d, e such that the aggregate R_d will be an $\mathfrak{A}$-subring with distinguished elements u, v. Conditions (5)—(8) guarantee that the number of u-elements in R_d is equal to $i-1$, while the number of v-elements in R_d is different from m, i.e. $g(i-1) \neq m$.

Thus, if in some $\mathfrak{B}$-ring R the number of a-elements is equal to m and the number of b-elements is equal to n, then $g(n) = m$ and, simultaneously, $g(i) \neq m$ for $0 \leq i < n$, i.e. $n = g^{-1}(m)$.

It remains to check 3). Let m be given. Put $n = g^{-1}(m)$. By assumption, for each $i = 0, 1, \dots, n$ there exists an $\mathfrak{A}$-ring R_i with distinguished elements a_i, b_i, having i a_i-elements $x_{i1}, \dots, x_{ii}$ and $g(i)$ b_i-elements $y_{i1}, \dots, y_{ig(i)}$, connected by the relations $a_i x_{i\alpha} = x_{i\alpha} x_{i\beta} = x_{i\alpha} x_{i\alpha} = x_{i\alpha},\ x_{i\beta} x_{i\alpha} = 0,\ b_i y_{i\alpha} = y_{i\alpha} y_{i\beta} = y_{i\alpha} y_{i\alpha} = y_{i\alpha},\ y_{i\beta} y_{i\alpha} = 0,\ a_i b_i = a_i^2 = b_i^2 = 0,\ b_i a_i = a_i\ (\alpha < \beta)$. From these relations it follows that the a_i-elements, the b_i-elements and a_i, b_i are linearly independent in their aggregate. Therefore they can be supplemented by suitable elements $z_{i1}, \dots, z_{i\alpha_i}$ to a basis of R_i. Assuming the algebras R_i to have no common elements, we formally construct a new algebra R. The basis of R is formed by the basis elements of all R_i and by new elements $d_i, e_i, f_i, a, b\ (i = 1, \dots, n)$. Multiplication of basis elements belonging to R_i is performed according to the rules of R_i, and we put $d_i x = x\ (x \in R_i),\ e_i x_{nj} = x_{ij}\ (i > j),\ fa = a,\ a x_{ni} = x_{ni},\ b y_{ni} = y_{ni},\ f_i x_{nj} = y_{ij}$ for $g(i) > m,\ f_i y_{ij} = x_{nj}$ for $g(i) < m$. The remaining products are regarded as equal to 0. The algebra R satisfies the requirements a1—a4, b1—b3 and $\mathfrak{B}(a, b, a', b', p)$ with $a' = a_n,\ b' = b_n,\ p = d_n$. Thus theorem 1 is proved.

No. 3. From theorem 1 it is easy to obtain the

Corollary. *For each normally given general recursive function $f(m)$, one can effectively construct a formula $\mathfrak{B}(a, b)$ representing this function in the class $\mathfrak{R}_1$ of finite-dimensional algebras over K possessing a unit.*

Let $\mathfrak{A}(a, b)$ be a formula representing $f(m)$ in $\mathfrak{R}$, and let R be an $\mathfrak{A}$-ring from $\mathfrak{R}$ having m a-elements. Denote by $\mathfrak{B}(a', b', a, b, p)$ the conjunction of the formulas $a'1$—$a'4$, $b'1$—$b'3$, the formula $\mathfrak{A}(a, b; p)$, and the formula

$$(x)((a', x) \leftrightarrow px = x\ \&\ (a, x))\ \&\ (x)((b', x) \leftrightarrow px = x\ \&\ (b, x)).$$

The formula $\mathfrak{B}(a', b', a, b, p)$ with distinguished elements a', b' represents the function $f(m)$ in the class $\mathfrak{R}_1$. Indeed, $\mathfrak{B}$ obviously possesses properties 1), 2). On the other hand, adjoining to the basis of R new elements a', b', p, e and putting $eu = ue = pu = u,\ up = 0$ for $u \in R,\ a'x = x,\ b'y = y$, if x is an a-element and y is a b-element of R, and $b'a' = a',\ a'^2 = b'^2 = 0$, we obtain a $\mathfrak{B}$-ring having m a'-elements and possessing a unit e.

No. 4. From theorem 1 and the indicated corollary, in the usual way one obtains:

Theorem 2. *The class $\mathfrak{R}$ of all rings that are finite-dimensional algebras over an arbitrary fixed field K, and the class $\mathfrak{R}_1$ of all $\mathfrak{R}$-rings having a unit, have undecidable elementary theories.*

For the proof it is enough to take a general recursive function $f(m)$ with a nonrecursive set of values and to construct, representing it in $\mathfrak{R}_1$, a formula $\mathfrak{A}(a, b)$. Then the falsity of the formula

$$\mathfrak{A}(a,b)\ \&\ (\exists x_1 \dots x_n)\left(\bigwedge_{i\neq j}(x_i \neq x_j\ \&\ (b,x_i))\ \&\ (y)\left((b,y)\to\bigvee_i y = x_i\right)\right)$$

in every $\mathfrak{R}_1$-ring will be equivalent to the unsolvability of the equation $f(x) = n$.

Corollary. *The elementary theories of the class of all finite rings with the identity $px = 0$ (p fixed prime) and of the class of all finite rings are undecidable.*

The first assertion is obtained from Theorem 2 in the case where K is a prime field of characteristic p, and the second follows from the first, since $\mathfrak{R}_0$ is a finitely axiomatizable subclass in $\mathfrak{R}$.

No. 5. In paper ([4]) a correspondence was established between rings with identity and metabelian groups of a special finitely axiomatizable class. Under this correspondence, to the class of rings with identity of prime odd characteristic p there corresponds a finitely axiomatizable subclass of the class of all metabelian groups with the identity $x^p = 1$. There an effective method is also indicated which makes it possible, for each closed formula concerning rings with identity, to obtain a formula for groups such that the truth of the first formula on a ring is equivalent to the truth of the second formula on the corresponding group. Since finite rings are thereby transformed into finite groups, it follows immediately from the corollary to Theorem 2 that:

Theorem 3. *The elementary theory of the class of all finite metabelian groups with the identity $x^p = 1$ (p odd prime) is undecidable.*

The class of groups indicated in this theorem is a finitely axiomatizable subclass of the class of all finite groups, of the class of all finite metabelian groups, of the class of all finite semigroups, etc. Therefore the elementary theories of all the classes mentioned are undecidable.

Let $\mathfrak{L}$ be a metabelian Lie ring of odd prime characteristic p. Defining in $\mathfrak{L}$ a new multiplication operation by the formula $xy = x + y + \frac{1}{2}[xy]$, we turn $\mathfrak{L}$ into a metabelian p-group, and we have $[xy] = xyx^{-1}y^{-1}$, $x + y = xy[yx]^{1/2}$. Conversely, introducing into an arbitrary metabelian p-group the operations $[xy]$ and $x + y$ by means of the indicated formulas, we obtain a metabelian Lie ring of characteristic p. Therefore the elementary theory of finite metabelian

Lie rings of odd prime characteristic p is equivalent to the elementary theory of finite metabelian p-groups and, together with the latter, is undecidable.

A metabelian Lie ring is also associative. Hence it follows that the elementary theories of the class of finite two-step nilpotent rings and of the class of all finite associative rings are undecidable.

Received
27 II 1961

CITED LITERATURE

[1] A. Tarski, A. Mostowski, R. Robinson, *Undecidable Theories*, Amsterdam, 1953, p. 85.
[2] B. A. Trakhtenbrot, DAN, 70, No. 4, 569 (1950).
[3] J. Robinson, Proc. Am. Math. Soc., 1, 703 (1951).
[4] A. I. Mal' cev, Matem. sborn., 50, No. 3, 257 (1960).

Note: Figure translations are in progress. See original paper for figures.