



Soviet-era science, translated into English

Yu. L. Ershov

1964

SovietRxiv

View the original and related papers at <https://sovietrxiv.org/items/ru-196401.52517>

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.

Abstract

Full Text

Yu. L. Ershov

Undecidability of the Theories of Symmetric and Simple Finite Groups

(Presented by Academician A. I. Mal'cev on 4 V 1964)

1. In this paper it is proved that the elementary theories of the classes of symmetric finite groups, alternating finite groups, and finite simple groups are undecidable. As a corollary one obtains new proofs of the theorems on undecidability and inseparability for the theory of the class of finite groups.
2. To prove the assertions stated in item 1 it is sufficient to establish the following theorem.

Theorem. *The set of identically true sentences of UHP (of signature $\sigma = \langle 1, \cdot, {}^{-1} \rangle$) and the set of sentences of this signature refutable on the models of the class of groups $\{S_{3n+2}\}_{n=3,4,\dots}$ ($\{A_{3n+2}\}_{n=3,4,\dots}$) are recursively inseparable.**

We shall use the following simple lemma (well known):

Lemma. *Let a theory T be such that the set of sentences true in the theory T , and the set of sentences refutable on finite models of the theory T , are recursively inseparable. Let φ be an effective mapping of the set of sentences of the signature of the theory T into the set of sentences of the signature of a class K such that: a) if $\mathfrak{A} \in T$, then $\varphi(\mathfrak{A})$ is an identically true sentence of UHP; b) if \mathfrak{A} is refutable on a finite model of the theory T , then $\varphi(\mathfrak{A})$ is refutable on a model of the class K . Then the set of identically true sentences of UHP and the set of sentences refutable on models of the class K are recursively inseparable.*

As the theory T we take the theory of two equivalence relations. The fact that this theory satisfies the conditions of the lemma is proved in (3). The author knows a simple proof of this assertion.

For the construction of the mapping φ we introduce a number of abbreviations:

$$\mathfrak{A}_1(x) \stackrel{df}{\iff} \{x \neq 1 \ \& \ x^3 = 1 \ \& \ \forall y [(xy^{-1}xy)^{15} = 1 \rightarrow (xy^{-1}xy)^3 = 1 \vee (xy^{-1}xy)^5 = 1]\};$$

$$\mathfrak{A}_2(x_1, x_2, x_3, x_4) \stackrel{df}{\iff} \left\{ \bigwedge_{i=1}^4 \mathfrak{A}_1(x_i) \ \& \ \bigwedge_{1 \leq i < j \leq 4} [x_{ixj} \neq 1 \ \& \ (x_{ixj})^5 = 1] \ \& \ (x_1x_2x_3x_4)^3 \neq 1 \ \& \ (x_1x_2x_3x_4)^9 = 1 \right\}$$

A quadruple of elements (x_1, x_2, x_3, x_4) satisfying the formula \mathfrak{A}_2 will be denoted by \bar{x} ;

$$(\forall \bar{x}) \mathfrak{A}(\bar{x}) \stackrel{df}{\iff} (\forall x_1, x_2, x_3, x_4) (\mathfrak{A}_2(x_1, x_2, x_3, x_4) \rightarrow \mathfrak{A}(x_1, x_2, x_3, x_4));$$

$$(\exists \bar{x}) \mathfrak{A}(\bar{x}) \stackrel{df}{\iff} (\exists x_1, x_2, x_3, x_4) (\mathfrak{A}_2(x_1, x_2, x_3, x_4) \& \mathfrak{A}(x_1, x_2, x_3, x_4));$$

$$\bar{x} \cdot y \stackrel{df}{\iff} (y^{-1}x_1y, y^{-1}x_2y, y^{-1}x_3y, y^{-1}x_4y);$$

$$\mathfrak{A}_3(x_1, x_2, x_3, x_4; y_1, y_2, y_3, y_4) = \mathfrak{A}_3(\bar{x}, \bar{y}) \stackrel{df}{\iff} \bar{x} \sim \bar{y} \stackrel{df}{\iff}$$

$$\bigwedge_{i,j=1}^4 [(x_{iyj})^2 = 1 \vee (x_{iyj})^5 = 1 \vee \mathfrak{A}_1(x_{iyj})];$$

$$x \leq y \stackrel{df}{\iff} (\forall \bar{z}) [(\bar{z} \cdot x \sim \bar{z}) \vee (\bar{z} \cdot x \sim \bar{z} \cdot y)];$$

$$\begin{aligned} \bar{x} \sim_z \bar{y} &\stackrel{df}{\iff} \bar{x} \sim \bar{y} \vee (\exists u)(u \ll z \& (\forall v)(v \ll u \rightarrow v = \\ &= u \vee v = 1) \& \bar{x} \cdot u \approx \bar{x} \& \bar{y} \cdot u \approx \bar{y}); \end{aligned}$$

$$\begin{aligned} \mathfrak{B} &\stackrel{df}{\iff} (\exists x_1, x_2, x_3, x_4) \mathfrak{A}_2(x_1, x_2, x_3, x_4) \& (\forall \bar{x}, \bar{y}, \bar{z}) [\bar{x} \sim \\ &\sim \bar{x} \& (\bar{x} \sim \bar{y} \rightarrow \bar{y} \sim \bar{x}) \& \\ &\& (\bar{x} \sim \bar{y} \& \bar{y} \sim \bar{z} \rightarrow \bar{x} \sim \bar{z})] \& (\forall t)(\forall \bar{x}, \bar{y}, \bar{z}) [(\bar{x} \sim_t \bar{y} \rightarrow \bar{y} \sim_t \bar{x}) \& \\ &\& [\bar{x} \sim_t \bar{y} \& \bar{y} \sim_t \bar{z} \rightarrow \bar{x} \sim_t \bar{z}]. \end{aligned}$$

It is not hard to verify that the formula \mathfrak{A}_1 is true on precisely those elements of the groups S_{3n+2}, A_{3n+2} , $n = 3, \dots$, which in their canonical representation as a product of cycles have altogether one cycle, and moreover of third order. The formula \mathfrak{A}_2 singles out those quadruples of three-element cycles which all have one common element (the center of the quadruple), and any two of these cycles have only this element in common. The quadruple $\bar{x} \cdot y$ has as its center the element to which the substitution y sends the center of the quadruple \bar{x} . $\bar{x} \sim \bar{y}$ means that these two quadruples have the same center; $x \ll y$ means (in the group S_{3n+2}) that x is a product of cycles which occur in the canonical

representation of the element y ; $\bar{x} \underset{z}{\sim} \bar{y}$ means (in the group S_{3n+2}) that the centers of the quadruples \bar{x} and \bar{y} are moved by one cycle from the canonical representation of the element z , or else these centers simply coincide. The formula \mathfrak{B} is true on the groups S_{3n+2} ($n = 3, 4, \dots$).

Let $\sigma_1 = \langle \sim_1, \sim_2 \rangle$ be the signature of the theory T . The mapping $\varphi_{x,y}^*$ is defined inductively:

1. $\varphi_{x,y}^*(a \sim_1 b) = \bar{a} \underset{x}{\sim} \bar{b}$, $\varphi_{x,y}^*(a \sim_2 b) = \bar{a} \underset{y}{\sim} \bar{b}$.
2. $\varphi_{x,y}^*(\mathfrak{A} \& \mathfrak{B}) = \varphi_{x,y}^*(\mathfrak{A}) \& \varphi_{x,y}^*(\mathfrak{B})$, $\varphi_{x,y}^*(\mathfrak{A} \vee \mathfrak{B}) = \varphi_{x,y}^*(\mathfrak{A}) \vee \varphi_{x,y}^*(\mathfrak{B})$,
 $\varphi_{x,y}^*(\neg \mathfrak{A}) = \neg \varphi_{x,y}^*(\mathfrak{A})$, $\varphi_{x,y}^*(\mathfrak{A} \rightarrow \mathfrak{B}) = \varphi_{x,y}^*(\mathfrak{A}) \rightarrow \varphi_{x,y}^*(\mathfrak{B})$.
3. $\varphi_{x,y}^*(\forall a \mathfrak{A}(a)) = (\forall \bar{a}) \varphi_{x,y}^*(\mathfrak{A}(a))$, $\varphi_{x,y}^*(\exists a \mathfrak{A}(a)) = (\exists \bar{a}) \varphi_{x,y}^*(\mathfrak{A}(a))$.

Remark. $\bar{a} = (a_1, a_2, a_3, a_4)$, and in the successive construction of the mapping $\varphi_{x,y}^*$ for a complex formula one must ensure that there is no collision of variables (where necessary, rename variables, but not x and y).

If \mathfrak{A} is a sentence, then $\varphi_{x,y}^*(\mathfrak{A})$ is a formula with two free variables x and y . We define the mapping φ on sentences as follows: $\varphi(\mathfrak{A}) = \mathfrak{B} \rightarrow (\forall x, y) \varphi_{x,y}^*(\mathfrak{A})$. It is not hard to verify that this mapping, in the case of the class $\{S_{3n+2}\}_{n=3,4,\dots}$, satisfies the conditions of the lemma.

In the case of alternating groups we shall make the following changes. Fix two quadruples of variables $\bar{\alpha} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and $\bar{\beta} = (\beta_1, \beta_2, \beta_3, \beta_4)$:

$$(\forall \bar{x}) \mathfrak{A}(\bar{x}) \stackrel{df}{\iff} (\forall x_1, x_2, x_3, x_4) (\mathfrak{A}_2(\bar{x}) \& \bar{x} \sim \bar{\alpha} \& \bar{x} \sim \bar{\beta} \rightarrow \mathfrak{A}(\bar{x}));$$

$$(\exists \bar{x}) \mathfrak{A}(\bar{x}) \stackrel{df}{\iff} (\exists x_1, x_2, x_3, x_4) (\mathfrak{A}_2(\bar{x}) \& \bar{x} \sim \bar{\alpha} \& \bar{x} \sim \bar{\beta} \& \mathfrak{A}(\bar{x})).$$

In the formulas $x \ll y$ and \mathfrak{B} , the quantifiers $(\forall \bar{x}), (\forall \bar{y}), \dots$ will be understood only as just indicated. The mapping $\varphi_{x,y,\bar{\alpha},\bar{\beta}}^*$ is defined analogously to the mapping $\varphi_{x,y}^*$. We define the mapping $\hat{\varphi}$ on sentences as follows:

$$\begin{aligned} \hat{\varphi}(\mathfrak{A}) &= (\forall \alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta_1, \beta_2, \beta_3, \beta_4) (\mathfrak{A}_2(\bar{\alpha}) \& \mathfrak{A}_2(\bar{\beta}) \& \bar{\alpha} \sim \bar{\beta} \rightarrow \\ &\rightarrow (\mathfrak{B} \rightarrow (\forall x, y) \varphi_{x,y,\bar{\alpha},\bar{\beta}}^*(\mathfrak{A}))). \end{aligned}$$

The mapping $\hat{\varphi}$ also satisfies the conditions of the lemma. The theorem is proved.

Corollary. *The set of identically true sentences of UNP and the set of sentences refutable on models of the class of finite (and infinite) groups (symmetric, sign-alternating, simple) are recursively inseparable.*

The author expresses his gratitude to Academician A. I. Mal' tsev for posing the problem.

Institute of Mathematics
Siberian Branch of the Academy of Sciences of the USSR

Received
30 IV 1964

CITED LITERATURE

1. A. I. Mal' tsev, DAN, **138**, 1001 (1961).
2. A. I. Mal' tsev, DAN, **139**, 802 (1961).
3. I. A. Lavrov, Algebra and Logic, **2**, 1, 5 (1963).

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

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.