# Yu. L. Ershov

1965

## Abstract

## Full Text


# Yu. L. Ershov


# THE UNDECIDABILITY OF CERTAIN FIELDS

*(Presented by Academician A. I. Mal' cev on 1 X 1964)*

1. The present note arose in connection with A. I. Mal' cev' s conjecture on the undecidability of fields of rational functions and fields of formal power series over an arbitrary field ([2]).

**Theorem 1.** *The field of rational functions in one variable over any finite field of characteristic not equal to 2 has an undecidable theory.*

**Theorem 2.** *The theory of all fields of any fixed finite characteristic not equal to 2 is undecidable.*

**Theorem 3.** *The field of formal power series in one variable over a field with an undecidable theory has an undecidable theory.*

2. We shall formulate a simple proposition on the possibility of proving the undecidability of various theories, which will be needed in the proof of Theorems 1 and 2.

Let $K_1$ and $K_2$ be classes of models of signatures $\sigma_1 = \langle P_1^{n_1}, \dots, P_k^{n_k} \rangle$ and $\sigma_2$. We shall say that the class of models $K_1$ is **relatively elementarily definable** (r.e.d.) in the class $K_2$ if there exist formulas

$$\mathfrak{A}(x_1, \dots, x_n;\ y_1, \dots, y_m)$$

(abbreviated $\mathfrak{A}(\bar{x}; \bar{y})$),

$$\mathfrak{B}(x; \bar{y}^1; \bar{y}^2)$$

$$(\mathfrak{B}(x_1, \dots, x_n;\ y_1^1, \dots, y_m^1;\ y_1^2, \dots, y_m^2)),$$

$$\mathfrak{C}_1(\bar{x}; \bar{y}^1, \dots, \bar{y}^{n_1}), \dots, \mathfrak{C}_k(\bar{x}; \bar{y}^1, \dots, \bar{y}^{n_k})$$

of signature $\sigma_2$, such that the following conditions are satisfied: 1) for every model $\mathfrak{M} \in K_1$ there exists a model $\mathfrak{N} \in K_2$ and elements $a_1, \dots, a_n \in \mathfrak{N}$ such that the set $L$ of $m$-tuples $\langle b_1, \dots, b_m \rangle$ such that $\mathfrak{A}(\bar{a}; \bar{b})$ is true in $\mathfrak{N}$, is nonempty; 2) the formula $\mathfrak{B}(\bar{a}; \bar{y}^1; \bar{y}^2)$ defines a congruence relation $\sim$ on the model of signature $\sigma_1$ obtained from the set $L$ by defining the predicate $P_i^{n_i}$ with the aid of the formula

$$\mathfrak{C}_i(\bar{a}; \bar{y}^1, \dots, \bar{y}^{n_i});$$

3) the model

$$\langle L/\sim,\ P_1^{n_1}, \dots, P_k^{n_k} \rangle,$$

where $L/\sim$ is the set of equivalence classes of $m$-tuples from the set $L$, and the predicates $P_i^{n_i}$ are induced by the predicates defined above on $L$, is isomorphic to the model $\mathfrak{M}$.

**Remark.** It is clear that if $K_1$ is r.e.d. in the class $K_2$, and $K_2$ is r.e.d. in the class $K_3$, then $K_1$ is r.e.d. in the class $K_3$.

The class $K_1$ has a **hereditarily undecidable** theory if every class $K_1' \supseteq K_1$ of signature $\sigma_1$ has an undecidable theory (see ([6])). It is known ([6]) that the class $K_1$, consisting of the single model

$$N = \langle \{0, 1, ...\},\ S^3,\ P^3 \rangle$$

—the natural numbers with the predicates of addition and multiplication—has a hereditarily undecidable theory.

**Proposition 1.** *If the class $K_1$ has a hereditarily undecidable theory and is r.e.d. in the class $K_2$, then $K_2$ also has a hereditarily undecidable theory.*

3. Let $\Omega$ be a finite field of characteristic not equal to 2. Let $\Omega(x)$ and $\Omega[x]$ be the field of rational functions and the ring of polynomials in $x$ over the field $\Omega$. The proof of Theorem 1 is analogous to D. Robinson' s proof ([4]) of the undecidability of fields of algebraic numbers and uses Hasse' s theorem on quadratic forms.

The local conditions for the representability of zero by a nondegenerate quadratic form in 4 variables can be formulated by means of the Hilbert symbol $(a, b)_p$ ($p$ is a point of the field $\Omega(x)$): $(a, b)_p = 1$, $a, b \in \Omega(x)$, if the equation $ax_1^2 + bx_2^2 = 1$ is solvable in the $p$-adic completion of the field $\Omega(x)$; $(a, b)_p = -1$ otherwise.

The following properties of the Hilbert symbol are valid:

1) $(a, b)_p = (a, -ab)_p$.
2) $(a, -a)_p = 1$.
3) $(a, b)_p = (a', b)_p$, if $aa'$ is a $p$-adic square.
4) If $a, b \in \Omega[x]$, $p = 1/x$, $p \in \Omega[x]$, $p^2 \nmid ab$, then

$$(a, b)_p = \begin{cases} (a/p), & \text{if } p \nmid a, \quad p \mid b, \\ (b/p), & \text{if } p \mid a, \quad p \nmid b, \\ 1, & \text{if } p \nmid a, \quad p \nmid b, \end{cases}$$

where $(a/p)$ is the Legendre symbol (see (3), where the reciprocity law is also given).

5) $(a, b)_p = (b, a)_p$.
6) $\prod_p (a, b)_p = 1$.

If $a, b \in \Omega[x]$ and the coefficients of the highest powers of $x$ are equal to 1 (in what follows, when polynomials are discussed, this condition is assumed to be fulfilled), then $(a,b)_{1/x} = (-1)^{\mu\mu'(q-1)/2}$, where $q$ is the number of elements of the field $\Omega$, and $\mu$ and $\mu'$ are the degrees of the polynomials $a$ and $b$; in particular, if $a$ or $b$ has even degree, then $(a,b)_{1/x} = 1$.

**Lemma 1.** The form $f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ is not zero in the $p$-adic completion of the field $\Omega(x)$ only in the case when $a_1a_2a_3a_4$ is a $p$-adic square and $(-a_1a_2, -a_1a_3)_p = -1$.

From the condition of local representability of zero (Lemma 1) and Hasse' s theorem it follows immediately that

**Lemma 2.** An element $h$ of the field $\Omega(x)$ can be represented by the ternary quadratic form $x_1^2 - ax_2^2 - bx_3^2$ in $\Omega(x)$ if and only if, for every point $p$ such that $(a,b)_p = 1$, $-abh$ is not a $p$-adic square.

**Lemma 3.** Let $p$ be an irreducible polynomial in $\Omega[x]$; then there exist two relatively prime polynomials $a$ and $b$, without multiple factors, such that $(a,b)_p = -1$, and at least one of them has even degree. (We note that then $(a,b)_{1/x} = 1$.)

**Proof.** Find an irreducible polynomial $b$ such that $(b/p) = -1$. If $p$ or $b$ has even degree, then one may take $a = p$; if $p$ and $b$ have odd degree, then let $a = pq$, where $q \neq p$ is an irreducible polynomial of odd degree. By property 4, $(a,b)_p = (b/p) = -1$. Lemma 4 and Proposition 2 are proved as in (4).

**Lemma 4.** Let $a$ and $b$ be relatively prime polynomials without multiple factors, the degree of at least one of them even, and let $p_1, p_2, \ldots, p_k$ be all irreducible polynomials dividing $ab$ such that $(a,b)_{p_i} = -1$ for $i = 1, \ldots, k$. Then, for an element $c \in \Omega(x)$, there exist $x_1, x_2$ and $x_3$ such that $1 - abc^2 = x_1^2 - ax_2^2 - bx_3^2$, if and only if $c$ is a $p_i$-adic integer for all $i = 1, \ldots, k$.

**Proposition 2.** Let

$$\Phi(a_1, b, c) \Longleftrightarrow (\exists x_1, x_2, x_3)\,(1 - abc^2 = x_1^2 - ax_2^2 - bx_3^2),$$

$$\mathfrak{A}(s,t) \Longleftrightarrow (\forall a, b)\{[(\forall c)(\Phi(a,b,c)) \to {}_{\alpha\in\Omega}\& \,\Phi(a,b,c+\alpha)\&$$

$$\& \,\Phi(a,b,s\cdot c)] \to \Phi(a,b,t)\}.$$

Then the set of those $t$ for which the formula $\mathfrak{A}(x,t)$ is true in $\Omega(x)$ is exactly the ring of polynomials $\Omega[x]$.

Thus, the ring of polynomials $\Omega[x]$ is e.d. in $\Omega(x)$; R. Robinson in (5) showed that $N$ is e.d. in the ring of polynomials over any field. From the remark and Proposition 1 follows Theorem 1. Since among all fields of fixed characteristic not equal to 2 there are fields of rational functions over finite fields of

this characteristic, Theorem 2 follows from the hereditary undecidability of the latter.

4. **Proposition 3.** Let $\Omega(x)$ be the field of formal power series in the variable $x$ over the field $\Omega$. Then the ring of formal power series without negative powers of $x$ is formally distinguishable.

**Proof.** Let $\Omega$ be a field of characteristic not equal to 2. Consider the formula

$$\mathfrak{A}(y) \Longleftrightarrow (\exists t)\{(\forall w)(t \neq w^2)\ \&\ (\forall u, v)[(\exists z)(1 + tu^2 = z^2)\ \&$$

$$\&\ (\exists z)(1 + tv^2 = z^2) \to (\exists z)(1 + tu^2v^2 = z^2)]\ \&\ (\exists z)(1 + ty^2 = z^2)\}.$$

We shall show that the elements $y$ satisfying the formula $\mathfrak{A}$ in $\Omega\{x\}$ are precisely the formal power series without negative powers of $x$, i.e.

$$y = x^m(\beta_0 + \beta_1 x + ...), \qquad \beta_i \in \Omega, \quad \beta_0 \neq 0, \quad m \geqslant 0. \tag{*}$$

Let us note that $t = x^n(\alpha_0 + \alpha_1 x + ...)$, $\alpha_i \in \Omega$, $\alpha_0 \neq 0$, is a square in $\Omega\{x\}$ if and only if $n$ is even and $\alpha_0$ is a square in $\Omega$. This follows immediately from Hensel' s lemma.

A. Take $x$ as the element $t$; then $x$ is not a square, and the set of elements $y$ such that $(\exists z)(1+xy^2 = z^2)$ is precisely the set of elements of the form $(*)$, and, consequently, is closed under multiplication. Indeed, if $m < 0$, then

$$1 + xy^2 = 1 + x^{2m+1}(\beta_0 + \beta_1 x + ...) = x^{2m+1}(\beta_0 + \beta_1' x + ...),$$

and since $2m + 1$ is odd, this element is not a square. If, however, $m \geqslant 0$, then

$$1 + xy^2 = 1 + \beta_0 x^{2m+1} + \beta_1 x^{2m+2} + \dots,$$

and, consequently, is a square. Thus, if $y = x^m(\beta_0 + \beta_1 x + ...)$, $\beta_i \in \Omega$, $\beta_0 \neq 0$, $m \geqslant 0$, then $\mathfrak{A}(y)$ is true.

B. Let $y = x^m(\beta_0 + \beta_1 x + ...)$, $\beta_i \in \Omega$, $\beta_0 \neq 0$, $m < 0$. Suppose that $\mathfrak{A}(y)$ is true; then there exists

$$t = x^k(\gamma_0 + \gamma_1 x + ...), \qquad \gamma_i \in \Omega, \quad \gamma_0 \neq 0,$$

such that $t$ is not a square, the set of elements $u$ for which $(\exists z)(1 - tu^2 = z^2)$ is closed under multiplication, and this set contains the element $y$. Consequently, this set contains every positive power of $y$. Let $l > 0$ be such that $2lm + k < 0$. The element $1 + t(y^l)^2$ must be a square. We shall show that this is impossible.

$$1 + t(y^l)^2 = 1 + x^{k+2lm}(\gamma_0\beta_0^{2l} + \delta_1 x + ...), \qquad \delta_i \in \Omega.$$

Since $k + 2lm < 0$, we have

$$1 + t(y^l)^2 = x^{k+2lm}(\gamma_0\beta_0^{2l} + \delta_1' x + ...).$$

If $k$ is odd, then $k + 2lm$ is also odd, and therefore this element is not a square; if $k$ is even, then $\gamma_0$ is not a square in $\Omega$, since otherwise

$$t = x^k(\gamma_0 + \gamma_1 x + ...)$$

would be a square, but then $\gamma_0\beta_0^{2l}$ is not a square in $\Omega$. Thus, in all cases the element $1 + t(y^l)^2$ is not a square in $\Omega\{x\}$. The contradiction obtained proves the assertion.

If the field $\Omega$ has characteristic 2, then the formula

$$\mathfrak{B}(y) \Leftrightarrow (\exists t)\{(\forall w)(t \neq w^3) \;\&\; (\forall u, v)[(\exists z)(1 + tu^3 = z^3) \;\&$$

$$\&\; (\exists z)(1 + tv^3 = z^3) \rightarrow$$

$$(\exists z)(1 + tu^3v^3 = z^3)] \;\&\; (\exists z)(1 + ty^2 = z^3)\}$$

is true for exactly those elements of the field $\Omega\{x\}$ which are formal power series without negative powers of $x$. The proof is entirely analogous. The proposition is proved.

Theorem 3 now follows from the fact that the ring of formal power series in the variable $x$ without negative powers of $x$ over an undecidable field is undecidable. This follows directly from the formal definability in such a ring of the ideal of noninvertible elements. The quotient ring by this ideal is isomorphic to the coefficient field (see, for example, (5)).

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

Received
27 IX 1964

## References

1. A. Weil, *Collected Works*, trans. Mathematics, **8**, 4, 3 (1964).
2. A. I. Maltsev, *Sibirsk. Mat. Zh.*, **1**, 71 (1960).
3. N. Hasse, *Zahlentheorie*, Berlin, 1963.
4. J. Robinson, *Proc. Am. Math. Soc.*, **10**, 950 (1959).

5. R. Robinson, *Trans. Am. Math. Soc.*, **70**, 137 (1951).

6. A. Tarski, A. Mostowski, R. Robinson, *Undecidable Theories*, Amsterdam, 1953.

7. E. Witt, *J. reine u. angew. Math.*, **176**, 31 (1936).

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