TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 242, August 1978

THE DIOPHANTINE PROBLEM FOR POLYNOMIAL RINGS AND FIELDS OF RATIONAL FUNCTIONS[1]

BY

J. DENEF[2]

ABSTRACT. We prove that the diophantine problem for a ring of polynomials over an integral domain of characteristic zero or for a field of rational functions over a formally real field is unsolvable.

1. Introduction.[3] During the last thirty years much work has been done to prove that the elementary theory of various rings is undecidable; see J. Ax [1], Yu. Eršov [9], [10], A. Malcev [14], Yu. Penzin [15], J. Robinson [17]–[20], R. M. Robinson [21], [22] and A. Tarski [23].

After M. Davis, Yu. Matijasevič, H. Putnam and J. Robinson (see, e.g., [4], [6]) proved that the existential theory of **Z** is undecidable, it is natural to ask whether the existential theory of various other rings is undecidable too.

Let R be a commutative ring with unity and let R' be a subring of R. We say that *the diophantine problem for R with coefficients in R'* is *unsolvable* (*solvable*) if there exists no (an) algorithm to decide whether or not a polynomial equation (in several variables) with coefficients in R' has a solution in R.

In [7] we proved that the diophantine problem for the ring of algebraic integers in any quadratic extension of **Q** is unsolvable, and recently we have extended this to some more algebraic integer rings. For some very interesting related results, see L. Lipshitz [13].

The main results of this paper are:

THEOREM A. *Let R be an integral domain of characteristic zero; then the diophantine problem for $R[T]$ with coefficients in $\mathbf{Z}[T]$ is unsolvable. ($R[T]$ denotes the ring of polynomials over R, in one variable T.)*

THEOREM B. *Let K be a formally real field, i.e. -1 is not the sum of squares*

Received by the editors June 20, 1977.

AMS (MOS) subject classifications (1970). Primary 02G05, 10N05, 10B99.

Key words and phrases. Hilbert's tenth problem, unsolvable problems, diophantine equations.

[1]Dedicated to Professor L. P. Bouckaert on the occasion of his seventieth birthday.

[2]This work has been supported by the "Nationaal Fonds voor Wetenschappelijk Onderzoek". It was done at Harvard University, whose generous hospitality I greatly appreciate. I am also grateful to M. Boffa and R. M. Robinson for simplifying the proof of Lemma 2.1.

[3]We use the following notations: **N** is the set of natural numbers; **Z** is the ring of integers; **Q** is the field of rationals; **R** is the field of real numbers; and **C** is the field of complex numbers.

in K. Then the diophantine problem for $K(T)$ with coefficients in $\mathbf{Z}[T]$ is unsolvable. ($K(T)$ denotes the field of rational functions over K, in one variable T.)

We prove Theorem A in §2 and Theorem B in §3.

It is obvious that the diophantine problem for $R[T]$ with coefficients in $\mathbf{Z}$ is solvable if and only if the diophantine problem for R with coefficients in $\mathbf{Z}$ is solvable. And the same holds for $K(T)$. (An algebraic closed field, a real closed field, the ring of p-adic integers and the ring of formal power series over a decidable field of characteristic zero are examples of rings whose diophantine problem with coefficients in $\mathbf{Z}$ is solvable.)

R. M. Robinson [**21**] proved for any integral domain R that the elementary theory of $R[T]$ is undecidable. M. Davis and H. Putnam [**5**] proved that the diophantine problem for $\mathbf{Z}[T]$ with coefficients in $\mathbf{Z}[T]$ is unsolvable. But, after that the diophantine problem for $\mathbf{Z}$ was proved unsolvable, it becomes trivial that the diophantine problem for $\mathbf{Z}[T]$ with coefficients in $\mathbf{Z}$ is unsolvable.

A. Malcev [**14**] and A. Tarski [**23**] proved that the elementary theory of $K(T)$ is undecidable when K is a real closed field. A simpler proof of this result has been given by J. Robinson [**20**]. Later R. M. Robinson [**22**] extended this result to any formally real field K. Yu. Eršov [**9**] and Yu. Penzin [**15**] proved the undecidability of the elementary theory of $K(T)$ when K is a finite field.

If K is a formally real field then so is $K(T)$; thus Theorem B is also true for fields of rational functions in several variables.

It is interesting to compare our work with a result of J. Becker and L. Lipshitz [**2**]: The diophantine problem for $\mathbf{C}[[T_1, T_2]]$ (i.e. the ring of formal power series over $\mathbf{C}$, in the variables T_1 and T_2) with coefficients in $\mathbf{Z}[T_1, T_2]$ is solvable, although the elementary theory of $\mathbf{C}[[T_1, T_2]]$ is undecidable (see Eršov [**10**]).

Let R be a commutative ring with unity and let $D(x_1, \ldots, x_n)$ be a realtion in R. We say that $D(x_1, \ldots, x_n)$ is *diophantine over R* if there exists a polynomial $P(x_1, \ldots, x_n, y_1, \ldots, y_m)$ over R such that for all $x_1, \ldots, x_n$ in R:

$$D(x_1, \ldots, x_n) \leftrightarrow \exists y_1, \ldots, y_m \in R: P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

We have the same definition for subsets of R by regarding them as 1-ary relations. Let R' be a subring of R and suppose P can be chosen such that its coefficients lay in R', then we say that $D(x_1, \ldots, x_n)$ is *diophantine over R with coefficients in R'*.

If R is an integral domain and if D_1 and D_2 are diophantine over $R[T]$ with coefficients in $\mathbf{Z}[T]$, then also $D_1 \vee D_2$ and $D_1 \wedge D_2$ are diophantine

over $R[T]$ with coefficients in $\mathbf{Z}[T]$; indeed,

$$P_1 = 0 \vee P_2 = 0 \leftrightarrow P_1 P_2 = 0 \quad \text{and} \quad P_1 = 0 \wedge P_2 = 0 \leftrightarrow P_1^2 + TP_2^2 = 0.$$

Moreover, the same holds for $K(T)$.

In this paper we prove also:

PROPOSITION 1. *Let R be an integral domain of characteristic zero. Suppose there exists a subset S of R which contains $\mathbf{Z}$ and which is diophantine over $R[T]$; then $\mathbf{Z}$ is diophantine over $R[T]$. In particular, this is true when R contains $\mathbf{Q}$.*

PROPOSITION 2. *Let K be a formally real field. Suppose there exists a subset S of K which contains $\mathbf{Z}$ and which is diophantine over $K(T)$; then $\mathbf{Z}$ is diophantine over $K(T)$. In particular, this is true when K contains the real closure of $\mathbf{Q}$.*

In [8] we have proved that a relation is diophantine over $\mathbf{Z}[T]$ if and only if it is recursively enumerable. M. Boffa noticed that for a nondenumerable language the situation can be very different:

COROLLARY (M. BOFFA). *Every subset D of $\mathbf{N}$ is diophantine over $\mathbf{R}[T]$.*

PROOF. Let r be the real number $r = \sum_{n=0}^{\infty} a_n/10^{n+1}$, where $a_n = 0$ for $n \in D$ and $a_n = 1$ for $n \notin D$. Then we have

$$n \in D \leftrightarrow n \in \mathbf{N} \wedge \exists p, m \in \mathbf{N}: \left(m = 10^n \wedge 0 \leqslant mr - p < \tfrac{1}{10}\right).$$

But $\mathbf{Z}$ is diophantine over $\mathbf{R}[T]$ by Proposition 1, and every recursively enumerable relation in $\mathbf{Z}$ is diophantine over $\mathbf{Z}$ (see, e.g., [4], [6]). Thus, using elementary algebra, we see that D is diophantine over $\mathbf{R}[T]$. Q.E.D.

2. Polynomial rings. Let R be any integral domain of characteristic zero. We consider the Pell equation

$$X^2 - (T^2 - 1)Y^2 = 1 \tag{1}$$

over $R[T]$. Let U be an element in the algebraic closure of $R[T]$ satisfying

$$U^2 = T^2 - 1. \tag{2}$$

Define two sequences X_n, Y_n, $n = 0, 1, 2, \ldots$, of polynomials in $\mathbf{Z}[T]$, by setting

$$X_n + UY_n = (T + U)^n. \tag{3}$$

We prove that Lemma 2.2 of M. Davis and H. Putnam [5] remains true when $\mathbf{Z}$ is replaced by R:

LEMMA 2.1. *The solutions of (1) in $R[T]$ are given precisely by*

$$X = \pm X_n, \quad Y = \pm Y_n, \quad n = 0, 1, 2, \ldots.$$

PROOF. (1) is equivalent to

$$(X - UY)(X + UV)^{-1} \tag{4}$$

From (3) and (2) follows

$$X_n - UY_n = (T - U)^n = (T + U)^{-n}.$$

Hence the X_n, Y_n are solutions of (1).

Conversely, suppose X and Y in $R[T]$ satisfy (1). Let us parametrise the curve (2) by

$$T = \frac{t^2 + 1}{t^2 - 1}, \quad U = \frac{2t}{t^2 - 1}.$$

The rational functions $X + UY$ and $X - UY$ in t have poles only at $t = \pm 1$. Moreover (4) implies they have zeroes only at $t = \pm 1$. Hence

$$X + UY = c\left(\frac{t+1}{t-1}\right)^m = c(T + U)^m, \qquad c \in R, m \in \mathbf{Z}.$$

Thus also $X - UY = c(T - U)^m$. But substituting this in (4) gives $c^2 = 1$, which proves the lemma by (3). Q.E.D.

Throughout this section we write $V \sim W$ to denote that the polynomials V and W in $R[T]$ take the same value at $T = 1$. Notice that the relation $Z \sim 0$ is diophantine over $R[T]$ with coefficients in $\mathbf{Z}[T]$, indeed

$$Z \sim 0 \leftrightarrow \exists X \in R[T]: Z = (T - 1)X.$$

The following lemma was used by M. Davis and H. Putnam [5, Lemma 2.3] too:

LEMMA 2.2. *We have* $Y_n \sim n$, *for* $n = 0, 1, 2, \ldots$.

PROOF. From (3) and (2) follows

$$Y_n = \sum_{\substack{i=1 \\ i \text{ odd}}}^{n} \binom{n}{i} (T^2 - 1)^{(i-1)/2} T^{n-i}.$$

Substitute now $T = 1$. Q.E.D.

Let us define the 1-ary relation $\mathrm{Imt}(Y)$ in $R[T]$ by

$$\mathrm{Imt}(Y) \leftrightarrow Y \in R[T] \wedge \exists X \in R[T]: X^2 - (T^2 - 1)Y^2 = 1.$$

LEMMA 2.3. *We have*:

(i) *The relation* $\mathrm{Imt}(Y)$ *is diophantine over* $R[T]$ *with coefficients in* $\mathbf{Z}[T]$.

(ii) *If* Y *satisfies* $\mathrm{Imt}(Y)$, *then there exists an integer* m *such that* $Y \sim m$.

(iii) *For every integer* m *there exists a polynomial* Y *satisfying* $\mathrm{Imt}(Y)$ *and* $Y \sim m$.

PROOF. This follows at once from Lemmas 2.1 and 2.2.

PROOF OF THEOREM A. There exists an algorithm to find for any polynomial $P(z_1, \ldots, z_n)$ over $\mathbf{Z}$, a polynomial $P^*(Z_1, \ldots, Z_m)$ over $\mathbf{Z}[T]$ such that

$$\exists z_1, \ldots, z_n \in \mathbf{Z}\colon P(z_1, \ldots, z_n) = 0$$
$$\leftrightarrow \exists Z_1, \ldots, Z_m \in R[T]\colon P^*(Z_1, \ldots, Z_m) = 0. \tag{5}$$

Indeed by Lemma 2.3 we have

$$\exists z_1, \ldots, z_n \in \mathbf{Z}\colon P(z_1, \ldots, z_n) = 0 \leftrightarrow \exists Z_1, \ldots, Z_n \in R[T]\colon$$
$$(\mathrm{Imt}(Z_1) \wedge \ldots \wedge \mathrm{Imt}(Z_n) \wedge P(Z_1, \ldots, Z_n) \sim 0).$$

Since Imt and $\sim$ are diophantine over $R[T]$ with coefficients in $\mathbf{Z}[T]$, we easily obtain a polynomial P^* satisfying (5). Hence if the diophantine problem for $R[T]$ with coefficients in $\mathbf{Z}[T]$ would be solvable, then the diophantine problem for $\mathbf{Z}$ would be solvable. Q.E.D.

PROOF OF PROPOSITION 1. If S satisfies the conditions of the proposition, then

$$z \in \mathbf{Z} \leftrightarrow \exists Z \in R[T]\colon (\mathrm{Imt}(Z) \wedge Z \sim z \wedge \in S).$$

Moreover, if R contains $\mathbf{Q}$, then we define S by:

$$x \in S \leftrightarrow x \in R[T] \wedge (x = 0 \vee \exists y \in R[T]\colon xy = 1). \quad \text{Q.E.D.}$$

3. Fields of rational functions. Let F be a field. A projective curve E, given by the affine equation $cy^2 = x^3 + ax + b$, is called an *elliptic curve defined over* F if it is nonsingular and if a, b and c are in F. One defines (see, e.g., Cassels [3, §7], Fulton [11, Chapter 5, §6] or Lang [12, Chapter 1, §§3, 4]) a commutative group law "+" on the set $E(F)$ of points on the elliptic curve E which are rational over F. The neutral element of this group is the unique point $\underline{0}$ at infinity on E. We shall denote by (v, w) the point with affine coordinates $x = v, y = w$.

Every elliptic curve E defined over $\mathbf{Q}$ whose j invariant ($j = 2^8 3^3 a^3/(4a^3 + 27b^2)$) is not integral has no complex multiplication, i.e. the only $\mathbf{C}$-rational maps from E into itself which fix $\underline{0}$ are the maps $P \mapsto m \cdot P = P + P + \cdots + P$ (m times), $m \in \mathbf{Z}$. (See, e.g., Lang [12, Chapter 1, §5 and Chapter 5, §2, Theorem 4].)

From now on we fix an elliptic curve E_0 defined over $\mathbf{Q}$, without complex multiplication and with equation

$$y^2 = x^3 + ax + b. \tag{1}$$

To E_0 we associate the elliptic curve

$$(T^3 + aT + b)Y^2 = X^3 + aX + b, \tag{2}$$

defined over $\mathbf{Q}(T)$, which we denote from now on by E. Obviously the point P_1 with coordinates $(T, 1)$ lies on $E(\mathbf{Q}(T))$.

Let K be any field of characteristic zero; then we have

LEMMA 3.1. *The point P_1 is of infinite order and generates the group $E(K(T))$ modulo points of order two.*

PROOF. We identify T with the rational function $(x, y) \mapsto x$ on E_0 and we denote the rational function $(x, y) \mapsto y$ on E_0 by U. The function field F of E_0 over K is thus $F = K(T, U)$, where $U^2 = T^3 + aT + b$. Let ψ_1 be the F-rational map

$$\psi_1 : E \to E_0 : (X, Y) \mapsto (X, UY).$$

Notice that ψ_1 is a group homomorphism since it is rational and $\psi_1(\underline{0}) = \underline{0}$. We denote the group of K-rational maps from E_0 into E_0 by $\mathrm{Rat}_K(E_0, E_0)$. Let ψ_2 be the map

$$\psi_2 : E_0(F) \to \mathrm{Rat}_K(E_0, E_0)$$

which sends the point (V, W) on $E_0(F)$ to the K-rational map

$$\psi_2(V, W) : E_0 \to E_0 : (x, y) \mapsto (V(x, y), W(x, y)).$$

Obviously ψ_2 is a homomorphism. Consider the group homomorphism

$$\psi = \psi_2 \circ \psi_1 : E(K(T)) \to \mathrm{Rat}_K(E_0, E_0).$$

For all points (X, Y) on $E(K(T))$ we have

$$T \circ \psi(X, Y) = X, \tag{3}$$

$$U \circ \psi(X, Y) = UY. \tag{4}$$

Hence ψ is injective. Since E_0 has no complex multiplication, we have

$$\mathrm{Rat}_K(E_0, E_0) \cong \{\alpha_m \mid m \in \mathbf{Z}\} \oplus E_0(K), \tag{5}$$

where α_m is the map $P \mapsto m \cdot P$, and where we identify a point on E_0 with the constant map from E_0 onto this point. Notice that $\psi(P_1) = \alpha_1$, and $\psi(m \cdot P_1) = \alpha_m$. Thus P_1 is of infinite order. Moreover, if $(X, Y) \in E(K(T))$ and $\psi(X, Y) \in E_0(K)$, then $X \in K$ by (3) and (2) yields $Y = 0$. This means that (X, Y) is a point of order two on $E(K(T))$. The lemma follows now from (5). Q.E.D.

We denote, for any nonzero integer m, the affine coordinates of $m \cdot P_1$ by (X_m, Y_m). Notice that X_m and Y_m are in $\mathbf{Q}(T)$. For any V and W in $K(T)$ we write $V \sim W$ to denote that $V - W$ (considered as a rational function on the projective line over K) takes the value zero at infinity.

LEMMA 3.2. *Using the above notation we have $X_m / TY_m \sim m$ for all nonzero integers m.*

PROOF. Notice that T/U is a local parameter on E_0 at $\underline{0}$, hence

$$\left\{ \frac{(T/U) \circ \alpha_m}{T/U} \right\}(\underline{0}) = m.$$

(See, e.g., Lang [12, Appendix 1, §3].) On the other hand, from (3) and (4) follows

$$\frac{X_m}{TY_m} = \frac{T \circ \psi(X_m, Y_m)}{(U \circ \psi(X_m, Y_m))T/U} = \frac{T \circ \alpha_m}{(U \circ \alpha_m)T/U} = \left(\frac{T}{U} \circ \alpha_m \right) / \frac{T}{U}.$$

Q.E.D.

Let us define the 1-ary relation $\mathrm{Imt}(Z)$ in $K(T)$ by

$$\mathrm{Imt}(Z) \leftrightarrow Z \in K(T)$$
$$\wedge \{ Z = 0 \vee \exists X, Y \in K(T): ((X, Y) \in 2 \cdot E(K(T)) \wedge 2TYZ = X) \}.$$

LEMMA 3.3. (i) *The relation* $\mathrm{Imt}(Z)$ *is diophantine over* $K(T)$ *with coefficients in* $\mathbf{Z}[T]$.

(ii) *If* Z *satisfies* $\mathrm{Imt}(Z)$, *then there exists an integer* m *such that* $Z \sim m$.

(iii) *For every integer* m, *there exists an element* Z *in* $\mathbf{Q}(T)$ *satisfying* $\mathrm{Imt}(Z)$ *and* $Z \sim m$.

PROOF. This follows at once from Lemmas 3.1 and 3.2.

We consider the relation $\mathrm{Com}(y)$ defined by

$$\mathrm{Com}(y) \leftrightarrow y \in K(T) \wedge \exists x \in K(T): y^2 = x^3 - 4.$$

The following lemma was used by R. M. Robinson [22, §4] too:

LEMMA 3.4. (i) *The relation* $\mathrm{Com}(y)$ *is diophantine over* $K(T)$ *with coefficients in* $\mathbf{Z}$.

(ii) *If* y *satisfies* $\mathrm{Com}(y)$, *then* y *lies in* K.

(iii) *For every rational number* z, *there exists a rational number* y *satisfying* $\mathrm{Com}(y)$ *and* $y > z$.

(iv) *If* K *contains the real closure of* $\mathbf{Q}$, *then every integer* y *satisfies* $\mathrm{Com}(y)$.

PROOF. (i) and (iv) are obvious.

(ii) Since $y^2 = x^3 - 4$ is a curve of genus 1, it admits no rational parametrization.

(iii) It is known (see, e.g., R. M. Robinson [22, §4]) that the group of rational points on the elliptic curve $y^2 = x^3 - 4$ is infinite. So the rational points are everywhere dense on the curve in the real plane. Indeed since the curve is connected in the real plane, its group of real points is a topological group isomorphic to the circle group. But every infinite subgroup of the circle group is everywhere dense. Q.E.D.

We define the 1-ary relation $Z \dot{\sim} 0$ in $K(T)$ by

$$Z \dot{\sim} 0 \leftrightarrow Z \in K(T) \wedge \exists X_1, X_2, X_3, X_4, X_5, y \in K(T):$$

$$(\mathrm{Com}\,(y) \wedge \tag{6}$$

$$(y - T)Z^2 + 1 = X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2). \tag{7}$$

LEMMA 3.5. (i) *The relation* $Z \dot{\sim} 0$ *is diophantine over* $K(T)$ *with coefficients in* $\mathbf{Z}[T]$.

(ii) *If the field* K *is formally real and if* $Z \dot{\sim} 0$, *then* $Z \sim 0$

(iii) *If* $Z \in \mathbf{Q}(T)$ *and* $Z \sim 0$, *then* $Z \dot{\sim} 0$.

PROOF. (i) is obvious.

(ii) Suppose there exist $X_1, \ldots, X_5$, y in $K(T)$ satisfying (6) and (7). Suppose we have not $Z \sim 0$, then $\deg Z \geqslant 0$ (where $\deg Z$ denotes the degree of the rational function Z). From (6) and Lemma 3.4(ii) follows $y \in K$. Hence $\deg((y - T)Z^2 + 1)$ is positive and odd. But $\deg(X_1^2 + X_2^2 + \cdots + X_5^2)$ is even. Indeed there is no cancellation of the coefficients of largest degree, since a sum of squares in a formally real field vanishes only if each term is zero. So we are in contradiction with (7), hence $Z \sim 0$.

(iii) Let $Z \in \mathbf{Q}(T)$ and $Z \sim 0$, then $TZ^2 \sim 0$ and there is a natural number z such that

$$|(TZ^2)(r)| \leqslant \tfrac{1}{2} \quad \text{when } r \in \mathbf{R} \text{ and } |r| > z.$$

By Lemma 3.4(iii) there exists a rational number y satisfying $\mathrm{Com}(y)$ and $y > z \geqslant 0$. Thus

$$((y - T)Z^2 + 1)(r) \geqslant 0 \quad \text{for all } r \text{ in } \mathbf{R}.$$

But a theorem of Y. Pourchet [**16**] states that every positive definite rational function over $\mathbf{Q}$ can be written as a sum of five squares in $\mathbf{Q}(T)$. Hence there exist $X_1, \ldots, X_5$ in $K(T)$ satisfying (7), whence $Z \dot{\sim} 0$. Q.E.D.

PROOF OF THEOREM B. There exists an algorithm to find for any polynomial $P(z_1, \ldots, z_n)$ over $\mathbf{Z}$, a polynomial $P^*(Z_1, \ldots, Z_m)$ over $\mathbf{Z}[T]$ such that

$$\exists z_1, \ldots, z_n \in \mathbf{Z}: P(z_1, \ldots, z_n) = 0$$
$$\leftrightarrow \exists Z_1, \ldots, Z_m \in K(T): P^*(Z_1, \ldots, Z_m) = 0.$$

Indeed, by Lemmas 3.3 and 3.5 we have

$$\exists z_1, \ldots, z_n \in \mathbf{Z}: P(z_1, \ldots, z_n) = 0 \leftrightarrow \exists Z_1, \ldots, Z_n \in K(T):$$
$$(\mathrm{Imt}(Z_1) \wedge \cdots \wedge \mathrm{Imt}(Z_n) \wedge P(Z_1, \ldots, Z_n) \dot{\sim} 0).$$

Proceed now as in the proof of Theorem A. Q.E.D.

PROOF OF PROPOSITION 2. If S satisfies the conditions of the proposition, then

$$z \in \mathbf{Z} \leftrightarrow \exists Z \in K(T): (\mathrm{Imt}(Z) \wedge Z - z \dot{\sim} 0 \wedge z \in S).$$

Moreover, the last assertion of the proposition follows from Lemma 3.4(iv). Q.E.D.

REFERENCES

1. J. Ax, *On the undecidability of power series fields*, Proc. Amer. Math. Soc. **16** (1965), 846.

2. J. Becker and L. Lipshitz, *Remarks on the elementary theories of formal and convergent power series*, Fund. Math. (to appear).

3. J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

4. M. Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), 233–269.

5. M. Davis and H. Putnam, *Diophantine sets over polynomial rings*, Illinois J. Math. **7** (1963), 251–256.

6. M. Davis, Yu. Matijasevič and J. Robinson, *Diophantine equations: Positive aspects of a negative solution*, Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, R.I., 1976, pp. 323–378.

7. J. Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214–220.

8. _____, *Diophantine sets over* $\mathbf{Z}[T]$, Proc. Amer. Math. Soc. **69** (1978), 148–150.

9. Yu. Eršov, *Undecidability of certain fields*, Dokl. Akad. Nauk SSSR **161** (1965), 349–352.

10. _____, *New examples of undecidable theories*, Algebra i. Logika **5** (1966), 37–47.

11. W. Fulton, *Algebraic curves*, Benjamin, New York, 1969.

12. S. Lang, *Elliptic functions*, Addison-Wesley, London, 1973.

13. L. Lipshitz, *Undecidable problems for addition and divisibility in algebraic number rings*. II, Proc. Amer. Math. Soc. **64** (1977), 122–128.

14. A. I. Malcev, *On the undecidability of the elementary theories of certain fields*, Sibirsk Mat. Ž. **1** (1960), 71–77; ibid **2** (1961), 639; English transl., Amer. Math. Soc. Transl. (2) **48** (1965).

15. Yu. Penzin, *Undecidability of fields of rational functions over fields of characteristic* 2, Algebra i. Logika **12** (1973), 205–210; 244.

16. Y. Pourchet, *Sur la représentation en somme de carrés des polynômes à une indéterminé sur un corps de nombres algébriques*, Acta Arith. **19** (1971), 89–104.

17. J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114.

18. _____, *The undecidability of algebraic rings and fields*,Proc. Amer. Math. Soc. **10** (1959), 950–957.

19. _____, *On the decision problem for algebraic rings*, Studies in Math. Anal. and Related Topics, Stanford, 1962, pp. 297–304.

20. _____, *The decision problem for fields*, Sympos. on the Theory of Models, North-Holland, Amsterdam, 1965, pp. 299–311.

21. R. M. Robinson, *Undecidable rings*, Trans. Amer. Math. Soc. **70** (1951), 137–159.

22. _____, *The undecidability of pure transcendental extensions of real fields*, Z. Math. Logik Grundlagen Math. **10** (1964), 275–282.

23. A. Tarski, *The elementary undecidability of pure transcendental extensions of real closed fields*, Notices Amer. Math. Soc. **10** (1963), A-355.

UNIVERSITY OF LEUVEN, DEPARTMENT OF MATHEMATICS, CELESTIJNENLAAN 200B, 3030 HEVERLEE, BELGIUM

Current address: Department of Mathematics, Princeton University, Fine Hall, Box 37, Princeton, New Jersey 08540