THE DIOPHANTINE PROBLEM FOR POLYNOMIAL RINGS AND FIELDS OF RATIONAL FUNCTIONS

BY

J. DENEF

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. 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 $\mathbb{Z}$ 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 $\mathbb{Q}$ 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 $\mathbb{Z}[T]$ 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.
in $K$. Then the diophantine problem for $K(T)$ with coefficients in $\mathbb{Z}[T]$ 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 $\mathbb{Z}$ is solvable if and only if the diophantine problem for $R$ with coefficients in $\mathbb{Z}$ 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 $\mathbb{Z}$ 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 $\mathbb{Z}[T]$ with coefficients in $\mathbb{Z}[T]$ is unsolvable. But, after that the diophantine problem for $\mathbb{Z}$ was proved unsolvable, it becomes trivial that the diophantine problem for $\mathbb{Z}[T]$ with coefficients in $\mathbb{Z}$ 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 $\mathbb{C}[[T_1, T_2]]$ (i.e. the ring of formal power series over $\mathbb{C}$, in the variables $T_1$ and $T_2$) with coefficients in $\mathbb{Z}[T_1, T_2]$ is solvable, although the elementary theory of $\mathbb{C}[[T_1, T_2]]$ is undecidable (see Eršov [10]).

Let $R$ be a commutative ring with unity and let $D(x_1, \ldots, x_n)$ be a relation 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 $R$:

$$D(x_1, \ldots, x_n) \iff \exists y_1, \ldots, y_m \in R: P(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$
over \( R[T] \) with coefficients in \( Z[T] \); indeed,

\[
P_1 = 0 \vee P_2 = 0 \iff P_1P_2 = 0 \quad \text{and} \quad P_1 = 0 \wedge P_2 = 0 \iff P_1^2 + TP_2^2 = 0.
\]

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 \( Z \) and which is diophantine over \( R[T] \); then \( Z \) is diophantine over \( R[T] \). In particular, this is true when \( R \) contains \( Q \).

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

In [8] we have proved that a relation is diophantine over \( Z[T] \) 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 \( N \) is diophantine over \( R[T] \).

**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

\[
n \in D \iff n \in N \land \exists p, m \in N: (m = 10^n \land 0 < mr - p < \frac{1}{10}).
\]

But \( Z \) is diophantine over \( R[T] \) by Proposition 1, and every recursively enumerable relation in \( Z \) is diophantine over \( Z \) (see, e.g., [4], [6]). Thus, using elementary algebra, we see that \( D \) is diophantine over \( R[T] \). 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 \( Z[T] \), 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 \( Z \) 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
\[(X - UY)(X + UY) = (T - U)^n = (T + U)^-n.\]
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
\[X + UY = c(t + U)^m, \quad c \in R, m \in Z.\]
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 \(Z[T]\), indeed
\[Z \sim 0 \iff \exists X \in R[T]: Z = (T - 1)X.\]
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
\[Y_n = \sum_{i=1}^{n} \binom{n}{i} (T^2 - 1)^{(i-1)/2} T^n - i.\]
Substitute now \(T = 1\). Q.E.D.
Let us define the 1-ary relation \(\text{Imt}(Y)\) in \(R[T]\) by
\[\text{Imt}(Y) \leftrightarrow Y \in R[T] \land \exists X \in R[T]: X^2 - (T^2 - 1)Y^2 = 1.\]

Lemma 2.3. We have:
(i) The relation \(\text{Imt}(Y)\) is diophantine over \(R[T]\) with coefficients in \(Z[T]\).
(ii) If \(Y\) satisfies \(\text{Imt}(Y)\), then there exists an integer \(m\) such that \(Y \sim m\).
(iii) For every integer \(m\) there exists a polynomial \(Y\) satisfying \(\text{Imt}(Y)\) 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 $\mathbb{Z}$, a polynomial $P^*(Z_1, \ldots, Z_m)$ over $\mathbb{Z}[T]$ such that
\[
\exists z_1, \ldots, z_n \in \mathbb{Z}: P(z_1, \ldots, z_n) = 0 \\
\iff \exists Z_1, \ldots, Z_m \in \mathbb{R}[T]: P^*(Z_1, \ldots, Z_m) = 0. \tag{5}
\]
Indeed by Lemma 2.3 we have
\[
\exists z_1, \ldots, z_n \in \mathbb{Z}: P(z_1, \ldots, z_n) = 0 \iff \exists Z_1, \ldots, Z_n \in \mathbb{R}[T]: \\
(\text{Imt}(Z_1) \land \cdots \land \text{Imt}(Z_n) \land P(Z_1, \ldots, Z_n) \sim 0).
\]
Since $\text{Imt}$ and $\sim$ are diophantine over $\mathbb{R}[T]$ with coefficients in $\mathbb{Z}[T]$, we easily obtain a polynomial $P^*$ satisfying (5). Hence if the diophantine problem for $\mathbb{R}[T]$ with coefficients in $\mathbb{Z}[T]$ would be solvable, then the diophantine problem for $\mathbb{Z}$ would be solvable. Q.E.D.

Proof of Proposition 1. If $S$ satisfies the conditions of the proposition, then
\[
z \in \mathbb{Z} \iff \exists Z \in \mathbb{R}[T]: (\text{Imt}(Z) \land z \sim Z \land \in S).
\]
Moreover, if $R$ contains $\mathbb{Q}$, then we define $S$ by:
\[
x \in S \iff x \in \mathbb{R}[T] \land (x = 0 \lor \exists y \in \mathbb{R}[T]: xy = 1). \quad \text{Q.E.D.}
\]

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 $0$ 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 $\mathbb{Q}$ whose $j$ invariant $(j = \frac{2^83^2a^3}{(4a^3 + 27b^2)})$ is not integral has no complex multiplication, i.e. the only $\mathbb{C}$-rational maps from $E$ into itself which fix $0$ are the maps $P \mapsto m \cdot P = P + P + \cdots + P$ ($m$ times), $m \in \mathbb{Z}$. (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 $\mathbb{Q}$, 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 $\mathbb{Q}(T)$, which we denote from now on by $E$. Obviously the point $P_1$ with coordinates $(T, 1)$ lies on $E(\mathbb{Q}(T))$.  

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
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 $\psi_1$ be the $F$-rational map

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

Notice that $\psi_1$ is a group homomorphism since it is rational and $\psi_1(0) = 0$. We denote the group of $K$-rational maps from $E_0$ into $E_0$ by $\text{Rat}_K(E_0, E_0)$. Let $\psi_2$ be the map

$$\psi_2: E_0(F) \rightarrow \text{Rat}_K(E_0, E_0)$$

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

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

Obviously $\psi_2$ is a homomorphism. Consider the group homomorphism

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

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

$$T \circ \psi(X, Y) = X, \quad (3)$$

$$U \circ \psi(X, Y) = UY. \quad (4)$$

Hence $\psi$ is injective. Since $E_0$ has no complex multiplication, we have

$$\text{Rat}_K(E_0, E_0) \cong \{ \alpha_m | m \in \mathbb{Z} \} \oplus E_0(K), \quad (5)$$

where $\alpha_m$ 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 $\mathbb{Q}(T)$. 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 $0$, hence
\( \left\{ \frac{(T/U) \circ \alpha_m}{T/U} \right\}(0) = m. \)

(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 \( \text{Imt}(Z) \) in \( K(T) \) by

\[
\text{Imt}(Z) \leftrightarrow Z \in K(T)
\]

\[
\land \{ Z = 0 \lor \exists X, Y \in K(T): ((X, Y) \in 2 \cdot E(K(T)) \land 2TYZ = X) \}.
\]

**Lemma 3.3.** (i) The relation \( \text{Imt}(Z) \) is diophantine over \( K(T) \) with coefficients in \( \mathbb{Z} \).

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

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

**Proof.** This follows at once from Lemmas 3.1 and 3.2.

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

\[
\text{Com}(y) \leftrightarrow y \in K(T) \land \exists x \in K(T): y^2 = x^3 - 4.
\]

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

**Lemma 3.4.** (i) The relation \( \text{Com}(y) \) is diophantine over \( K(T) \) with coefficients in \( \mathbb{Z} \).

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

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

(iv) If \( K \) contains the real closure of \( \mathbb{Q} \), then every integer \( y \) satisfies \( \text{Com}(y) \).

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

(ii) If the field $K$ is formally real and if $Z \sim 0$, then $Z \sim 0$.

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

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 $\deg Z > 0$ (where $\deg Z$ denotes the degree of the rational function $Z$). From (6) and Lemma 3.4(ii) follows

$$\forall a \in A, B \in B : (\forall y \in A, B : (y - T)^2 + 1 = X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2).$$

$$\text{(7)}$$

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

$$\left| (TZ^2)(r) \right| < \frac{1}{2} \quad \text{when } r \in \mathbb{R} \text{ and } |r| > z.$$

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

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

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

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

$$\exists z_1, \ldots, z_n \in \mathbb{Z} : P(z_1, \ldots, z_n) = 0$$

$$\iff \exists Z_1, \ldots, Z_m \in K(T) : P^*(Z_1, \ldots, Z_m) = 0.$$

Indeed, by Lemmas 3.3 and 3.5 we have

$$\exists z_1, \ldots, z_n \in \mathbb{Z} : P(z_1, \ldots, z_n) = 0 \iff \exists Z_1, \ldots, Z_n \in K(T) : (\text{Im}(Z_1) \wedge \cdots \wedge \text{Im}(Z_n) \wedge P(Z_1, \ldots, Z_n) \sim 0).$$

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

$$z \in \mathbb{Z} \iff \exists Z \in K(T) : (\text{Im}(Z) \wedge Z - z \sim 0 \wedge z \in S).$$
Moreover, the last assertion of the proposition follows from Lemma 3.4(iv).
Q.E.D.

REFERENCES


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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use