PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 102, Number 2, February 1988

DECIDABLE SENTENCES OVER POLYNOMIAL RINGS

SHIH-PING TUNG

(Communicated by Thomas J. Jech)

ABSTRACT. Let R be an algebraic number field or an algebraic integer ring. We prove that there is an algorithm to determine whether the sentence $\forall x\ \exists y\ \phi(x,y)$, with $\phi(x,y)$ a quantifier free formula over $R[T]$, is true in the polynomial ring $R[T]$ or not.

1. Introduction. R. M. Robinson [**7**] proved for any integral domain R that the elementary theory of $R[T]$ is undecidable. J. Denef [**2**] proved for any integral domain R of characteristic zero that the diophantine problem for $R[T]$ with coefficients in $Z[T]$ is undecidable. It thus makes sense to investigate subclasses of arithmetical sentences which are decidable. We study the arithmetical sentences over polynomial rings from this point of view.

There is an algorithm for solving equations with one unknown in any algebraic number field K. Hence there is an algorithm to decide whether sentences over $K[T]$ with a single existential quantifier (or a single universal quantifier), are true in $K[T]$ (see Lemma 2.2 below). The decidability of sentences with two existential quantifiers is very much an open problem; deciding which equations with two unknowns are solvable is tantalizingly difficult. However, over the rational number field Q or integer ring Z there are algorithms to decide the truth of sentences with one universal quantifier and one existential quantifier [**10**]. In this paper we show that there are also such algorithms for polynomial rings over an algebraic number field K or algebraic integer ring I respectively.

Our main theorems are the following:

THEOREM 3.4. *There is an algorithm to determine whether the sentence* $\forall x\ \exists y\ \phi(x,y)$ *(or* $\exists x \forall y\ \phi(x,y)$ *respectively), with* $\phi(x,y)$ *a quantifier free formula over* $K[T]$, *is true in* $K[T]$ *or not.*

THEOREM 4.3. *There is an algorithm to determine whether the sentence* $\forall x\ \exists y\ \phi(x,y)$ *(or* $\exists x \forall y\ \phi(x,y)$ *respectively), with* $\phi(x,y)$ *a quantifier free formula over* $K[T]$, *is true in* $I[T]$ *or not.*

Our main tools are theorems of Schinzel [**9**] on diophantine equations with parameters. Along the proofs, we give necessary and sufficient conditions for the solvability of diophantine equations with parameters in $K[T]$ and $I[T]$ respectively. We then obtain that the solvability of diophantine equations with parameters in $K[T]$ or $I[T]$ is decidable. That is, there is an algorithm to determine whether the

Received by the editors August 21, 1986 and, in revised form, October 31, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 03B25.
The author would like to express his thanks to the referee. This paper is much improved by his suggestions.

sentences of the form

$$\forall x_1 \cdots \forall x_n \, \exists y \; f(x_1, \ldots, x_n, y) = 0,$$

where f is a polynomial over $K[T]$, is true in $K[T]$ (or $I[T]$ respectively) or not.

The diophantine problem for $I[T]$ with coefficients in Z is decidable if and only if the diophantine problem for I with coefficients in Z is decidable. In [**1**, **3**, **4**], the diophantine problems for some algebraic integer rings (with coefficients in Z) were shown to be undecidable. We obtain that for some polynomial rings $I[T]$, for example $Z[T]$, sentences of the form

$$\forall x_1 \cdots \forall x_n \; f(x_1, \ldots, x_n) \neq 0,$$

where f is a polynomial over Z, are undecidable. It is well known [**4**] that in I,

$$x \neq 0 \Leftrightarrow \exists y \, \exists z \; xy = (2z - 1)(3z - 1).$$

This is also true in $I[T]$. We obtain that there is no algorithm to determine whether the sentences of the form

$$\forall x_1 \cdots \forall x_n \, \exists y \exists z \; f(x_1, \ldots, x_n, y, z) = 0$$

is true in $I[T]$ or not.

2. Preliminaries. In this paper, K denotes a finite extension field of the rational number field Q and I denotes the ring of integers of K. We call K or I an algebraic number field or an algebraic integer ring respectively. All formulas are assumed to be in the language of rings augmented by constants denoting the elements of $K[T]$. Let $R[T]$ be the ring of polynomials over R in one variable T. In this paper, we study the sentences true in $K[T]$ or $I[T]$. In fact, all the results proved in this paper are also true for polynomial rings in more than one variable. The proofs are the same. For simplicity, we do the case of the polynomials in one variable.

Now we introduce a convention which will be used throughout this paper. Let $f(x_1, \ldots, x_n)$ be a polynomial with coefficients in $K[T]$. We may view this polynomial as a polynomial in $n + 1$ variables with coefficients in K and denote this polynomial by $f(T, x_1, \ldots, x_n)$.

In K we may find a polynomial $p(x)$ of degree $d > 0$ with no roots in K. Let $B(x, y)$ be its homogenization $y^d p(x/y)$. Then over $K[T]$, $B(a, b) = 0$ if and only if $a = 0 \wedge b = 0$. With this fact, now we may give a syntactical transformation for quantifier free formulas. This transformation will simplify our proofs later.

LEMMA 2.1. *If $\phi(x, y)$ is a formula containing no quantifiers and no free variables other than x and y then we may reduce $\phi(x, y)$ to the form $\bigvee_{i=1}^{n} [f_i(x, y) = 0 \wedge g_i(x, y) \neq 0]$ where $f_i(x, y)$ and $g_i(x, y)$ are relatively prime polynomials over $K[T]$ for every i, $1 \leq i \leq n$.*

PROOF. Cf. [**8**, Theorem 3].

LEMMA 2.2. *There is an algorithm to determine whether a given sentence with a single quantifier is true in $K[T]$ (or $I[T]$ respectively) or not.*

PROOF. It suffices to show the case of sentences with a single existential quantifier. Let $\exists x \; \phi(x)$ be such a sentence. By Lemma 2.1, we may write $\phi(x)$ in the

form $\bigvee_{i=1}^{n}[f_i(x) = 0 \wedge g_i(x) \neq 0]$. There is an algorithm [**5**] for solving equations in $K[T]$ by factorization; $a = h(T)$ is a root of the equation $f(x) = 0$ in $K[T]$ if and only if $x - h(T)$ is a factor of the polynomial $f(T, x)$. Therefore, if there exist an i and an element a of $K[T]$ such that $f_i(a) = 0$ but $g_i(a) \neq 0$ then $\exists x\ \phi(x)$ is true in $K[T]$. Otherwise, $\exists x\ \phi(x)$ is false in $K[T]$.

Given an algebraic number b in K, there is an algorithm to check whether b is an algebraic integer or not [**6**, p. 11]. The proof for the case of $I[T]$ is similar.

3. Sentences in $K[T]$. Given a polynomial $f(x_1, \ldots, x_n, y)$, we may ask whether for any numbers $x_1', \ldots, x_n'$ the equation $f(x_1', \ldots, x_n', y) = 0$ is solvable. Problems of this type are called diophantine equations with parameters in number theory. We apply a theorem of Schinzel over K to obtain a necessary and sufficient condition for a diophantine equation with parameters to be solvable in $K[T]$. Now we state the theorem of Schinzel [**9**, p. 192].

THEOREM A. *Let $F(x, t_1, \ldots, t_r)$ be a polynomial over an algebraic number field K. If for every r arithmetic progressions $P_1, \ldots, P_r$ in Z there exist integers t_i' of P_i $(i \leq r)$ and an x' of K such that $F(x', t_1', \ldots, t_r') = 0$ then there exists a rational function $x(t_1, \ldots, t_r)$ over K such that*

$$F(x(t_1, \ldots, t_r),\ t_1, \ldots, t_r) \equiv 0.$$

We now prove a necessary lemma before we give the necessary and sufficient condition over $K[T]$.

LEMMA 3.1. *Let $r_j(t, x_1, \ldots, x_n)$ $(j \leq m)$ be rational functions, but not polynomials over K. There exist elements $x_1', \ldots, x_n'$ in $Z[T]$ such that $r_j(T, x_1', \ldots, x_n')$ $(j \leq m)$ are not elements of $K[T]$.*

PROOF. Let $r_j = G_j/H_j$ where $G_j \in K[t, x_1, \ldots, x_n]$, $H_j \in K[t, x_1, \ldots, x_n] - K$ and G_j, H_j are relatively prime over $K[t, x_1, \ldots, x_n]$ for each j. We first assume that G_j and H_j all contain variable t except for some G_j which may be elements of K. If the polynomial H_i does not contain the variable t, then H_i must contain another variable, say x_1. Then we can choose a suitable b of Z such that $H_i(x_1 + bt,\ x_2, \ldots, x_n)$ contains variable t. Also all other polynomials G_j, H_j still contain variable t after substituting x_1 by $x_1 + bt$ if they contain t originally. After at most $2m$ substitutions all polynomials contain variable t except for some polynomials G_j which are elements of K. We also assume that G_j and H_j are all irreducible or we factor G_j and H_j into irreducible factors and set them into rational functions to satisfy the assumption. For example, if $H_j = h_1 \cdot h_2$ and $G_j = g_1 \cdot g_2$ where h_1, h_2, g_1 and g_2 are irreducible, then we set $r_j^1 = h_1/g_1$, $r_j^2 = h_2/g_1$, $r_j^3 = h_1/g_2$ and $r_j^4 = h_2/g_2$. Now we want to choose $x_1', \ldots, x_n'$ of Z such that $G_j(t, x_1', \ldots, x_n')$ and $H_j(t, x_1', \ldots, x_n')$ are irreducible for every $j \leq m$ and $G_j(t, x_1', \ldots, x_n') \neq k \cdot H_j(t, x_1', \ldots, x_n')$ for every k of K. Then $r_j(T, x_1', \ldots, x_n')$ are not elements of $K[T]$ for $j \leq m$. For simplicity, we do the case $m = 2$. Let

$$G_1 = \sum_{i=0}^{s} g_i \cdot t^i, \quad G_2 = \sum_{j=0}^{t} g_j' \cdot t^j, \quad H_1 = \sum_{k=0}^{p} h_k \cdot t^k, \quad H_2 = \sum_{l=0}^{q} h'^l \cdot t^l,$$

where g_i, g_j', h_k, h_l' are elements of $K[x_1, \ldots, x_n]$. Since G_i and H_i are relatively prime for $i = 1, 2$ we may choose suitable i, j, k, l such that $p_1 = g_i \cdot h_k - g_k \cdot h_i$,

$p_2 = g'_j \cdot h'_l - g'_l \cdot h'_j$ and $p = p_1 \cdot p_2 \not\equiv 0$. By Hilbert's irreducibility theorem [**9**, p. 179], there are integers $x'_1, \ldots, x'_n$ of Z such that $G_j(t, x'_1, \ldots, x'_n)$, $H_j(t, x'_1, \ldots, x'_n)$ are irreducible and $p(x'_1, \ldots, x'_n) \neq 0$. This completes the proof.

THEOREM 3.2. *Let $f(x_1, \ldots, x_n, y)$ be a polynomial over $K[T]$. For every $x'_1, \ldots, x'_n$ of $K[T]$ there is a y' of $K[T]$ such that $f(x'_1, \ldots, x'_n, y') = 0$ if and only if $f(x_1, \ldots, x_n, y)$ has a factor of the form $y - F(x_1, \ldots, x_n)$ with $F(x_1, \ldots, x_n)$ a polynomial over $K[T]$.*

PROOF. One direction is trivial. Now we assume that for every $x'_1, \ldots, x'_n$ of $K[T]$ there is a y' of $K[T]$ such that $f(x'_1, \ldots, x'_n, y') = 0$. Then for every $t, a_1, \ldots, a_n$ of K there is a number b of K such that $f(t, a_1, \ldots, a_n, b) = 0$. By Theorem A and the Factor Theorem, $f(T, x_1, \ldots, x_n, y)$ has factors of the form $y - r(T, x_1, \ldots, x_n)$ where $r(T, x_1, \ldots, x_n)$ are rational functions over K. Let

$$r_i(T, x_1, \ldots, x_n) = F_i(T, x_1, \ldots, x_n)/G_i(T, x_1, \ldots, x_n)$$

with F_i, G_i relatively prime. Since K is a unique factorization domain, we may write that

$$f(T, x_1, \ldots, x_n, y) = f_0(T, x_1, \ldots, x_n, y) \cdot \prod_{i=1}^{s} (G_i(T, x_1, \ldots, x_n)y - F_i(T, x_1, \ldots, x_n)), \qquad s \neq 0,$$

where f_0, $F_i, G_i \not\equiv 0$ are polynomials over K, F_i and G_i are relatively prime and f_0 has no factors of the form $G(T, x_1, \ldots, x_n)y - F(T, x_1, \ldots, x_n)$. Now suppose that for every i, $G_i(T, x_1, \ldots, x_n)$ is an element of $K[T, x_1, \ldots, x_n] - K$. We want to choose $x'_1, \ldots, x'_n$ of $K[T]$ such that $f(x'_1, \ldots, x'_n, y) \neq 0$ for every y of $K[T]$. The polynomial f_0 has no factor of the form $G(T, x_1, \ldots, x_n)y - F(T, x_1, \ldots, x_n)$; by Theorem A again, there exist arithmetic progressions $P_i = \{b_i z + m_i | \ z \in Z\}$ in Z, $0 \leq i \leq n$, such that for every a_i of P_i the equation $f_0(a_0, a_1, \ldots, a_n, y) = 0$ has no solutions in K. Notice that $r_i(b_0 T + m_0, b_1 x_1 + m_1, \ldots, b_n x_n + m_n)$ are rational functions but not polynomials over K. By Lemma 3.1, we may choose $x'_1, \ldots, x'_n$ of $Z[T]$ such that $r_i(b_0 T + m_0, b_1 x'_1 + m_1, \ldots, b_n x'_n + m_n)$ are not elements of $K[T]$. We also obtain that $f_0(b_0 T + m_0, b_1 x'_1 + m_1, \ldots, b_n x'_n + m_n, y) = 0$ is not solvable in $K[T]$. Suppose that there is a solution y' in $K[T]$. Substituting $T = 1$, this contradicts the choices of arithmetic progressions.

COROLLARY 3.3. *There is an algorithm to determine whether the sentences of the form*

$$\forall x_1 \cdots \forall x_n \, \exists y \; f(x_1, \ldots, x_n, y) = 0,$$

where f is a polynomial over $K[T]$, is true in $K[T]$ or not.

PROOF. By Theorem 3.2, we only need to apply the algorithm in [**5**] to factor the polynomial $f(T, x_1, \ldots, x_n, y)$ over K, then check whether f has a factor of the form $y - F(T, x_1, \ldots, x_n)$ or not.

THEOREM 3.4. *There is an algorithm to determine whether the sentence $\forall x \, \exists y \; \phi(x, y)$ (or $\exists x \forall y \; \phi(x, y)$ respectively), with $\phi(x, y)$ a quantifier free formula over $K[T]$, is true in $K[T]$ or not.*

PROOF. It suffices to prove the case for sentences of the form $\forall x \, \exists y \; \phi(x, y)$. By Lemma 2.1, we may write that $\phi(x, y) \Leftrightarrow \bigvee_{i=1}^{n} [f_i(x, y) = 0 \wedge g_i(x, y) \neq 0]$.

In order for the sentence $\forall x \exists y\ \phi(x,y)$ to be true in $K[T]$, it is necessary that $\forall x \exists y\ [\bigvee_i f_i(x,y) = 0]$ or $\forall x \exists y\ [\prod_i f_i(x,y) = 0]$ be true in $K[T]$. Now we apply the algorithm in [**5**] to factor the polynomial $\prod_i f_i(T,x,y)$ over K. If $\prod_i f_i(T,x,y)$ does not have any factor of the form $y - F(T,x)$ with $F(T,x)$ a polynomial over K, then $\forall x \exists y\ [\prod_i f_i(x,y) = 0]$ is false in $K[T]$ by Theorem 3.2. Then $\forall x \exists y\ \phi(x,y)$ is false in $K[T]$. Now we suppose that $\prod_i f_i(T,x,y)$ has such a factor $y - F(T,x)$. Since $y - F(T,x)$ is irreducible, there is an i such that $y - F(T,x)$ is a factor of $f_i(T,x,y)$. For every element a of $K[T]$, $F(T,a)$ is an element of $K[T]$. Hence if $\exists y\ \phi(a,y)$ is false in $K[T]$ then a must be a root of the equation $g_i(x,F(x)) = 0$ in $K[T]$ where $g_i(x,F(x)) \not\equiv 0$. Now we solve the equation $g_i(x,F(x)) = 0$ in $K[T]$ and let $\{a_1,\ldots,a_r\}$ be the roots of this equation. We check the truth of the sentence $\exists y\ \phi(a_i,y)$ in $K[T]$ for every $i \leq r$ by the algorithm of Lemma 2.2. If there is an i such that $\exists y\ \phi(a_i,y)$ is false in $K[T]$ then $\forall x \exists y\ \phi(x,y)$ is false in $K[T]$. Otherwise, $\forall x \exists y\ \phi(x,y)$ is true in $K[T]$.

4. Sentences in $I[T]$. In this section we study the sentences in $I[T]$. We apply another theorem of Schinzel to obtain similar results to those in §3. The ideas of the proofs are similar. Only in certain places do we need to check whether an algebraic number is an algebraic integer or not. We sketch or even omit the proofs in this section. We first state the theorem of Schinzel [**9**, p. 195].

THEOREM B. *Let $F(x,t_1,\ldots,t_r)$ be a polynomial over an algebraic number field K. If for every r arithmetic progressions $P_1,\ldots,P_r$ in Z there exist integers t_i' of P_i and an integer x' of K such that $F(x',t_1',\ldots,t'r) = 0$ then there exists a polynomial $X(t_1,\ldots,t_r)$ over K such that*

$$F(X(t_1,\ldots,t_r),\ t_1,\ldots,t_r) \equiv 0.$$

THEOREM 4.1. *Let $f(x_1,\ldots,x_n,y)$ be a polynomial over $K[T]$. For every $x_1',\ldots,x_n'$ of $I[T]$ there is a y' of $I[T]$ such that $f(x_1',\ldots,x_n',y') = 0$ if and only if $f(x_1,\ldots,x_n,y)$ has a factor of the form $y - F(x_1,\ldots,x_n)$ with $F(x_1,\ldots,x_n)$ a polynomial over $I[T]$.*

PROOF. By Theorem B, we may write that

$$f(T,x_1,\ldots,x_n,y) = f_0(T,x_1,\ldots,x_n,y) \cdot \prod_{i=1}^{s}(y - F_i(T,x_1,\ldots,x_n)), \qquad s \neq 0,$$

where f_0 and F_i are polynomials over K and f_0 has no factors of the form $y - F(T,x_1,\ldots,x_n)$. Now suppose that $F_i(T,x_1,\ldots,x_n)$ are not polynomials over I for every i. By Theorem B again, there exist arithmetic progressions $P_i = \{n_i z + m_i |\ z \in Z\}$ in Z such that for every a_i of P_i, $f_0(a_0,a_1,\ldots,a_n,y)$ has no solution in I. Now let d be a positive integer greater than the degree of the polynomial $f(T,x_1,\ldots,x_n,y)$ and $x_1' = T^d + m_1$, $x_2' = T^{d^2} + m_2,\ldots,x_n' = T^{d^n} + m_n$. Then $F_i(T,x_1',\ldots,x_n')$ cannot be an element of $I[T]$ and $f_0(x_1',\ldots,x_n',y) = 0$ is not solvable in $I[T]$. The latter can be seen by taking $T = \prod_i n_i$. This is a contradiction.

COROLLARY 4.2. *There is an algorithm to determine whether the sentences of the form*

$$\forall x_1 \cdots \forall x_n \exists y \ f(x_1, \ldots, x_n, y) = 0,$$

where f is a polynomial over $K[T]$, are true in $I[T]$ or not.

THEOREM 4.3. *There is an algorithm to determine whether the sentence $\forall x \exists y \ \phi(x, y)$ (or $\exists x \forall y \ \phi(x, y)$ respectively), with $\phi(x, y)$ a quantifier free formula over $K[T]$, is true in $I[T]$ or not.*

FINAL REMARK. Analyzing the algorithms in this paper more carefully, we find that all the algorithms are in deterministic polynomial time. In [**11**], we proved that the decision problem of deciding which sentences of the form $\exists x \forall y \ f(x, y) \neq 0$, where $f(x, y)$ is a polynomial over I, are true in I, is NP-complete. The reason why we have more efficient algorithms for $I[T]$ is that we have a simple criterion, i.e. Theorem 4.1, to tell whether a diophantine equation with parameters is solvable in $I[T]$.

REFERENCES

1. J. Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214–220.
2. ——, *The diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399.
3. ——, *Diophantine sets over algebraic integer rings*. II, Trans. Amer. Math. Soc. **257** (1980), 227–236.
4. J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), 385–391.
5. S. Landau, *Factoring polynomials over algebraic number fields*, SIAM J. Comput. **14** (1985), 184–195.
6. H. Mann, *Introduction to algebraic number theory*, Ohio State Univ. Press, Columbus, 1955.
7. R. M. Robinson, *Undecidable rings*, Trans. Amer. Math. Soc. **70** (1951), 137–159.
8. ——, *Arithmetical definitions in the ring of integers*, Proc. Amer. Math. Soc. **10** (1951), 279–284.
9. A. Schinzel, *Selected topics on polynomials*, Univ. of Michigan Press, Ann Arbor, Mich., 1982.
10. S. P. Tung, *Provability and decidability of arithmetical universal-existential sentences*, Bull. London Math. Soc. **18** (1986), 241–247.
11. ——, *Complexity of sentences over number rings*, preprint.

DEPARTMENT OF MATHEMATICS, CHUNG YUAN CHRISTIAN UNIVERSITY, CHUNG LI, TAIWAN 32023, REPUBLIC OF CHINA