Defining constant polynomials

Mihai Prunescu*

Abstract

We define diophantinely rings of algebraic integers O inside their polynomial rings $O[T]$ using only constant coefficients from $\mathbb{Z}$. The result is motivated by minimizing the number of occurrences of T and its exponent in a diophantine definition for the predicate $t \neq 0$ in $O[T]$. Primary 03B99, Secondary 11D99.

1 Introduction

In this paper we will consider some issues of diophantine definability over rings. We concentrate on rings of algebraic integers and their polynomial rings, and we hope to show some useful tricks.
Definition: For an abstract set of constants C, we call the language $L = \{+, -, \cdot, \{0,1\} \cup C\}$ **extension** with constants of the formal language of rings. We say that the constants are interpreted over some ring R if there is an interpretation of the language over R such that the arithmetical operations keep their usual meaning and every constant become the name of a fixed element of R. We say that a relation $D \subset R^k$ is L**-definabile** iff there is a first order formula $\phi(x_1, \dots, x_k)$ with k free variables in the language L such that $D = \{(x_1, \dots, x_k) \in R^k \mid$ there is an extension with new constants $a_1, \dots, a_k \notin C$ of L so that according to the interpretation $a_i^R := x_i$ holds $R \models \phi(a_1, \dots, a_n)$ $\}$. If the formal definition ϕ is quantifier-free or contains only existential quantifiers, we say that D is **existentially** L-definable. If ϕ is existential and, moreover, does not contain any negation, we say that D is L**-diophantine**.
We start with a simple observation about the importance of the complement of 0.

Lemma 1.1 *Let R be a ring and L be an extension with constants of the formal language of rings, interpreted over R, such that the unary relation $t \in R \setminus \{0\}$, shortly denoted $t \neq 0$, is L-diophantine. Then every existentially L-definable relation is L-diophantine.*

2 Adequacy

The remark above justifies the following:
Definition: A ring R will be called **adequate** with respect to a language L iff all existentially L-definable relations over R are L-diophantine over R.
A ring R is adequate with respect to L iff the relation $t \neq 0$ is L-diophantine, because the empty prefix is also existential.
The following results show that the adequacy is strongly dependent on the interpretation of the constants occurring in L.

Theorem 2.1 *Let Δ be a commutative ring not necessarily with* 1.

1. *Let L be an extension with constants of the formal language of rings interpreted over Δ. Let T be transcendental over Δ. Then the polynomial ring $\Delta[T]$ is not adequate with respect to L.*

[*] Institut für Mathematik und Informatik, Universität Greifswald, Germany. These results occurred as technical lemmata in author's dissertation [P] at the University of Konstanz, Germany. During this dissertation the author was partially supported by D.A.A.D. and by the University of Konstanz. The author kindly thanks his advisor, Prof. Alexander Prestel, for all support.

2. *Let $\Omega = \Delta[T_1, T_2, \dots, T_n, \dots]$ be the polynomial ring in $\aleph_0$ variables over Δ. Then there is no extension with constants L of the formal language of rings such that Ω is adequate with respect to L.*

Proof of 1: Let $L = \{+, -, \cdot, (\underline{a})_{a\in\Delta}\}$ be a new language which contains a name (constant) for every element of Δ. For $\Delta[T]$ we define the language $LT = L \cup \{\underline{T}\}$, with $\underline{T}$ interpreted as T. Suppose now that the subset $\Delta[T] \setminus \{0\}$ is L-diophantine in $\Delta[T]$. Its positive existential definition can be put in the normal form:

$$\Delta[T] \models\ [\, t \neq \underline{0} \Longleftrightarrow \exists X_1, \dots, X_n \ \bigvee_i \bigwedge_j P_{ij}(t, X_1, \dots, X_n) = \underline{0}\,],$$

where $P_{ij} \in \Delta[t, X_1, \dots, X_n]$ have coefficients which are constant terms over L and do not contain $\underline{T}$.

We remark that for an element $a \in \Delta \setminus \{0\}$ is $aT \in \Delta[T] \setminus \{0\}$. (This is a precaution for the case that the ring has no 1. Normally we work with the polynomial T.) We fix a choice of polynomials $Y_1(T), \dots, Y_n(T)$ and an index i_0 such that

$$\Delta[T] \models \bigwedge_j P_{i_0,j}(\underline{aT}, Y_1(\underline{T}), \dots, Y_n(\underline{T})) = \underline{0}.$$

For the ring Δ with respect to L this is a conjunction of true polynomial identities in a new constant $\underline{T}$. The new constant may be substituted with every constant from L, leading to true sentences. This is possible because T is transcendental over Δ. We substitute $\underline{T}$ with $\underline{0}$. From an algebraic point of view this is the evaluation in $T = 0$ of a polynomial function. We get:

$$\Delta \text{ and } \Delta[T] \models \bigwedge_j P_{i_0,j}(\underline{0}, Y_1(\underline{0}), \dots, Y_n(\underline{0})) = \underline{0}.$$

We remark that $\forall k\ X_k := Y_k(0) \in \Delta \subset \Delta[T]$. X_k are again constant L-terms. The crucial fact that $\underline{T}$ did not occur in the coefficients of P_{ij} allowed us to keep and get back these polynomials after the evaluation. Now:

$$\Delta[T] \models\ \exists X_1, \dots, X_n \quad \bigwedge_j P_{i_0,j}(\underline{0}, X_1, \dots, X_n) = \underline{0},$$

$$\Delta[T] \models\ \exists X_1, \dots, X_n \quad \bigvee_i \bigwedge_j P_{ij}(\underline{0}, X_1, \dots, X_n) = \underline{0}.$$

If we remember the way in which we have defined $t \neq 0$, we get finally:

$$\Delta[T] \models\ \underline{0} \neq \underline{0}.$$

This is a contradiction. □

Proof of 2: We are following the proof of 2.1.1 insisting on some differences. We introduce the language $LT_\infty = L \cup \{\underline{T_1}, \underline{T_2}, \dots\}$. It is the strongest extension with constants of the formal language of rings for Ω, in the sense that all elements of Ω can be represented as constant LT_∞-terms. We prove that the subset $\Omega \setminus \{0\}$ is not LT_∞-diophantine in Ω, and it is sufficient for our conclusion.

As before suppose that $\Omega \setminus \{0\}$ was LT_∞-diophantine and had a positive existential definition in prenex normal form given by $P_{ij} \in \Omega[t, X_1, \dots, X_n]$. Only a finite set of variable-names may occur in the P_{ij}'s, say without restricting the generality $\underline{T_1}, \underline{T_2}, \dots, \underline{T_m}$. These are the constants which will not be subjected to any substitution. We write also $\Delta_m := \Delta[T_1, T_2, \dots, T_m]$ and $LT_m = L \cup \{\underline{T_1}, \underline{T_2}, \dots, \underline{T_m}\}$.

Now for $a \in \Delta \setminus \{0\}$ is again $aT_{m+1} \in \Omega \setminus \{0\}$. We choose and fix elements $Y_1, \dots, Y_n \in \Omega$ and one index i_0 such that:

$$\Omega \models \bigwedge_j P_{i_0,j}(\underline{aT_{m+1}}, Y_1, \dots, Y_n) = \underline{0}.$$

Only a finite number of variable-names can occur in the Y_k's, say $\underline{T_1}, \underline{T_2}, \dots, \underline{T_m}$, $\underline{T_{m+1}}, \dots, \underline{T_{m+p}}$. It might happen that the Y_k's are already elements in Δ_m, but then this is anyway true for some $p \geq 1$.
$\underline{T_{m+1}}, \dots, \underline{T_{m+p}}$ are new constants over (Δ_m, LT_m) and may be substituted with any other constants. We substitute $\underline{T_{m+1}}$ with $\underline{0}$ and $\underline{T_{m+2}}, \dots,$ $\underline{T_{m+p}}$ with arbitrary other constants from L, say $\underline{a_{m+2}}, \dots, \underline{a_{m+p}}$. If we denote now by $X_k := Y_k(T_1, \dots, T_m, 0, a_{m+2}, \dots, a_{m+p}) \in \Delta_m \subset \Omega$, we get:

$$\Delta_m \text{ and } \Omega \models \exists X_1, \dots, X_n \bigwedge_j P_{i_0,j}(\underline{0}, X_1, \dots, X_n) = \underline{0},$$

which means the contradiction $\Omega \models \underline{0} \neq \underline{0}$. The crucial facts were the following: First $\underline{T_1}, \underline{T_2}$, $\dots, \underline{T_m}$ have not been substituted, permitting us to get back the P_{ij}'s and the diophantine definition. Second, no possible formal definition could use infinitely many constants (in our case, variable-names). □□
Using the same procedure we can prove the following:

Remark 2.2 *If Δ is a commutative ring with 1 and L an extension with constants of the formal language of rings interpreted over Δ, then the unary singleton relation $\{T\}$ is not L-diophantine over $\Delta[T]$.*

Fortunately for proving that the rings of algebraic integers are adequate a very simple idea does work, see for example [Sauerland]:

$$O \models \ [\, t \neq 0 \Longleftrightarrow \exists s \in O \ t \,|\, (2s-1)(3s-1)\,].$$

Indeed, if the divisibility takes place, t may not be 0 because $\frac{1}{2}$ and $\frac{1}{3}$ do not belong to O. If t is any nonzero element of O, it is enough to find a natural number s such that the norm $N_{K/\mathbb{Q}}(t) \,|\, (2s-1)(3s-1)$ in $\mathbb{Z}$, because $t \,|\, N_{K/\mathbb{Q}}(t)$ already in O and $t = 0 \Leftrightarrow N_{K/\mathbb{Q}}(t) = 0$. Let $\pm N_{K/\mathbb{Q}}(t)$ be a natural number whose decomposition in primes looks like $2^n 3^m q$ where 2 and 3 do not divide q. Using the Chinese Remainder Theorem for 2^n and $3^m q$ and the fact that 2 and 3 are units in the rings $\mathbb{Z}/3^m q\mathbb{Z}$ and $\mathbb{Z}/2^n\mathbb{Z}$, we get a natural number s such that

$$\begin{aligned} 2s &\equiv 1 \mod (3^m q), \\ 3s &\equiv 1 \mod (2^n). \end{aligned}$$

This means that $\pm N_{K/\mathbb{Q}}(t) = 2^n 3^m q \,|\, (2s-1)(3s-1)$, and we are done. □

3 Main result

Theorem 3.1 *If O is the ring of algebraic integers in a number field K, then the relation $x \in O$ is diophantine in the polynomial ring $O[T]$ due to a diophantine formula whose coefficients are constant polynomials of $O[T]$. Moreover, we can choose them to be elements of $\mathbb{Z}$.*

Proof: Before starting with the proof of this theorem, I will shortly comment on its history. For $O = \mathbb{Z}$ this was known by Putnam and Davis, see [Davis-Putnam]. Their defining equation has coefficients in $\mathbb{Z}$ and has been one of the first applications of the Pell equation for defining $\mathbb{Z}$. On the other hand Alexandra Shlapentokh diophantinely defined $\mathbb{Z}$ in $R[T]$ in a uniform manner for all domains R of characteristic 0. Using her result and the appropriate language for O it is quite trivial to define O. But the resulting definition would have not constant coefficients because her definition displays T explicitly by using Pell equations with transcendental coefficients, like $X^2 - (T^2-1)Y^2 = 1$.
Recently Zahidi made such definitions for rings of algebraic integers in formally real number fields, see [Zahidi]. Our method works more generally because uses valuations instead of orderings.

Let K =Quot(O) be the corresponding number field and $\mathfrak{p}$ any prime of K. After [Rumely] the valuation ring $O_{\mathfrak{p}}$ is L-diophantine in K. We can choose a valuation ring $O_{\mathfrak{p}}$ which accepts a definition with coefficients in $\mathbb{Z}$.

$$K \models \ (x \in O_{\mathfrak{p}} \Longleftrightarrow \exists x_1, \ldots, x_n \ P(x, x_1, \ldots, x_n) = 0).$$

We introduce new variables $y_1, \ldots, y_n$ and z which are interpreted as elements in O such that for all i one has $x_i = \frac{y_i}{z}$. Multiplying $P(x, \frac{x_1}{z}, \ldots, \frac{x_n}{z})$ with a suitable power of z we obtain the partially homogenized polynomial $Q(x, x_1, \ldots, x_n, z)$. Now we claim:

$$O[T] \models \ (x \in O \Longleftrightarrow \exists x_1, \ldots, x_n, z \ Q(x, x_1, \ldots, x_n, z) = 0 \wedge z \neq 0).$$

Denote the subset of $O[T]$ defined on the right above by S; $S \subseteq O[T]$. We prove $S = O$:
$\underline{O \subseteq S}$: If $x \in O$ then as element of K is $x \in O_{\mathfrak{p}}$ and thus x trivially satisfies the definition of S.
$\underline{S \subseteq O}$: Suppose $x \in S \setminus O$ and look at x as nonconstant polynomial function on K. Choose polynomials $y_1, \ldots, y_n, z$ with $Q(x, y_1, \ldots, y_n, z) = 0$ and $z \neq 0$. As polynomial z is not identical 0, so the set of elements of K which are zeros for z is at most finite.
Let $v_{\mathfrak{p}}$ be the valuation on K corresponding to $\mathfrak{p}$. For all nonconstant polynomials x the set

$$\{u \in K \mid v_{\mathfrak{p}}(x(u)) < 0\}$$

is infinite, so we choose an $u \in K$ such that $v_{\mathfrak{p}}(x(u)) < 0$ and $z(u) \neq 0$.
But $P(x(u), \frac{y_1(u)}{z(u)}, \ldots, \frac{y_n(u)}{z(u)}) = 0$ implies $v_{\mathfrak{p}}(x(u)) \geq 0$. Contradiction.
In order to prove the diophantine character of this definition we must now eliminate the negation. Without being able to define diophantinely $z \neq 0$ in $O[T]$ using only constant coefficients (see 2.1), we find a tricky way for this particular situation. We claim that in $O[T] \models$:

$$(x \in O \Longleftrightarrow \exists x_1, \ldots, x_n, z, s \ Q(x, x_1, \ldots, x_n, z) = 0 \ \wedge \ z \,|\, (2s-1)(3s-1)).$$

Suppose $x \in O$ and $x_1, \ldots, x_n \in K$ such that $P(x, x_1, \ldots, x_n) = 0$. K being in fact $\frac{O}{\mathbb{N} \setminus \{0\}}$ one can find a common denominator $z \in \mathbb{N} \setminus \{0\}$ such that all $x_i = \frac{y_i}{z}$ and depending on z find $s \in \mathbb{N}$ as discussed before for the rings O.
On the other side if $(x, \vec{y}, z, s) \subset O[T]$ is any solution of the system, we must have $z \neq 0$ because $\frac{1}{2}$ and $\frac{1}{3}$ do not belong to $O[T]$, and we may repeat the proof to conclude that $x \in O$. □□

4 One application

Corollary 4.1 *The polynomial rings over the rings of algebraic integers are adequate with respect to the formal language $LT = \{+, -, \cdot, 0, 1, \underline{T}\}$.*

Proof: We see that:

$$O[T] \models \ (t \neq 0 \Longleftrightarrow \exists a, b \ \ a \in O \wedge b \in O \setminus \{0\} \wedge \underline{T} - a \mid t - b\,).$$

Indeed O is a diophantine subset in $O[T]$ as already proven in 3.1 and $O \setminus \{0\}$ is a diophantine subset in O because O is adequate. The definition of $O \setminus \{0\}$ should be relativized to the definition of O in $O[T]$ using new variables. The resulting definition is hence diophantine and says that a polynomial is not the null polynomial iff its associate polynomial function takes at least one nonzero value. We can choose a diophantine definition of O in $O[T]$ which contains only coefficients in $\mathbb{Z}$. It leads to a definition of $O[T] \setminus \{0\}$ using just the formal language of rings and no other constants, excepting $\underline{T}$. □
We used the new constant $\underline{T}$ for only one occurrence in the defining formula. Because of Theorem 2.1, we could not avoid this.

References

[Davis-Putnam] **Martin Davis, Hilary Putnam**: *Diophantine Sets over Polynomial Rings* Illinois Journal of Mathematics 7, 1963

[P] **Mihai Prunescu**: *A structural approach to diophantine definability* Reihe Konstanzer Dissertationen, Hartung-Gorre Verlag, Konstanz 1999

[Rumely] **Robert S. Rumely**: *Undecidability and Definability for the Theory of Global Fields* Transactions of the A.M.S. 262(1), 1980

[Sauerland] **Ulrich Sauerland**: *Entscheidbarkeitsprobleme in Ringen algebraischer Zahlkörper* Diplomarbeit Universität Konstanz, 1993

[Shlapentokh] **Alexandra Shlapentokh**: *Diophantine Definitions for Some Polynomial Rings* Communications of Pure and Applied Mathematics, Vol. XLIII, 1990; 1055-1066

[Zahidi] **Karim Zahidi** Doctoral Dissertation at the University of Gent, 1999