Vol. 101, No. 1 DUKE MATHEMATICAL JOURNAL © 2000

DEFINING INTEGRALITY AT PRIME SETS OF HIGH DENSITY IN NUMBER FIELDS

ALEXANDRA SHLAPENTOKH

1. Introduction. Interest in the questions of Diophantine definability and decidability goes back to a question that was posed by Hilbert: Given an arbitrary polynomial equation in several variables over $\mathbb{Z}$, is there a uniform algorithm to determine whether such an equation has solutions in $\mathbb{Z}$? This question, otherwise known as Hilbert's tenth problem, has been answered negatively in the work of M. Davis, H. Putnam, J. Robinson, and Yu. Matijasevich (see [2] and [3]). Since the time when this result was obtained, similar questions have been raised for other fields and rings. Arguably the two most interesting and difficult problems in the area are the questions of Diophantine decidability of $\mathbb{Q}$ and the rings of algebraic integers of arbitrary number fields. One way to resolve the question of Diophantine decidability negatively over a ring of characteristic zero is to construct a Diophantine definition of $\mathbb{Z}$ over such a ring. This notion is defined below.

Definition 1.1. Let R be a ring and let $A \subset R$. Then we say that A has a Diophantine definition over R if there exists a polynomial $f(t, x_1, \dots, x_n) \in R[t, x_1, \dots, x_n]$ such that for any $t \in R$,

$$\exists x_1, \dots, x_n \in R, \quad f(t, x_1, \dots, x_n) = 0 \Longleftrightarrow t \in A.$$

If the quotient field of R is not algebraically closed, it can be shown that we can allow the Diophantine definition to consist of several polynomials without changing the nature of the relationship (for more details see [3]). Such Diophantine definitions have been obtained for $\mathbb{Z}$ over the rings of algebraic integers of the following fields: totally real extensions of $\mathbb{Q}$, their extensions of degree 2, fields with exactly one pair of complex conjugate embeddings, and some fields of degree 4. For more details concerning these results see [4], [5], [6], [13], [15], and [16]. However, not much progress has been made towards resolving the Diophantine problem of $\mathbb{Q}$. Furthermore, one of the consequences of a series of conjectures by Mazur and Colliot-Thélène, Swinnerton-Dyer, and Skorobogatov is that $\mathbb{Z}$ does not have a Diophantine definition over $\mathbb{Q}$, and thus one would have to look to some other method for resolving the Diophantine problem of $\mathbb{Q}$. (Mazur's conjectures can be found in [10] and [11]. However, Colliot-Thélène, Swinnerton-Dyer, and Skorobogatov gave a counterexample to the strongest of the conjectures in the papers cited above. Their modification of Mazur's

Received 15 September 1998. Revision received 12 March 1999.
1991 *Mathematics Subject Classification.* Primary 11U05, 11R80; Secondary 11R04, 03D25.
Author's work partially supported by National Security Agency grant number MDA904-98-1-0510.