DIOPHANTINE SETS OVER POLYNOMINAL RINGS[1]

BY

MARTIN DAVIS AND HILARY PUTNAM

Recent work (cf. [1], [2]) on decision problems for Diophantine equations can be generalized to various rings other than the integers. In this paper, we shall prove the recursive unsolvability of the analogue of Hilbert's tenth problem (cf. [2]) for the ring $J[\xi]$ of formal polynomials with integer coefficients.

1. Principal results

We begin with the following notational conventions:

J is the ring of rational integers, R is a *recursive ring* (in the sense of [3]) such that $J \subset R$. The letter ξ with or without a numerical subscript is an indeterminate. Where the contrary is not explicitly stated, capital Latin letters stand for elements of R, lower case Latin letters stand for positive integers, capital Greek letters stand for sets.

DEFINITION. A set Σ is called *Diophantine over* R if for some polynomial form $P(\xi_0, \xi_1, \cdots, \xi_n)$ in the polynomial ring $R[\xi_0, \xi_1, \cdots, \xi_n]$, we have

$$X \in \Sigma \leftrightarrow \bigvee_{Y_1,\ldots,Y_n} P(X, Y_1, \cdots, Y_n) = 0.$$

A similar definition may be given for predicates $R(X_1, \cdots, X_n)$. We have at once

COROLLARY 1.1. *If Σ is Diophantine over R, then Σ is a recursively enumerable[2] set.*

We shall be concerned with the following decision problem which we call the *Diophantine problem over* R:

To determine of a given polynomial form $P(\xi_1, \cdots, \xi_m) \in R[\xi_1, \cdots, \xi_m]$ whether or not the equation $P(\xi_1, \cdots, \xi_m) = 0$ has a solution in R.

For $R = J$, the ring of integers, this is exactly Hilbert's tenth problem.

Invoking the Church-Turing identification of recursiveness with effective calculability, and using the fact that there exists a recursively enumerable set which is not recursive, we have at once

COROLLARY 1.2. *If every recursively enumerable set of positive integers is Diophantine over R, then the Diophantine problem over R is unsolvable.*

The main result of the present paper, whose proof we postpone, is

Received November 22, 1961.

[1] This research was supported by the United States Air Force through the Air Force Office of Scientific Research of the Air Research and Development Command.

[2] Note that R is recursive, so this concept is defined for sets of elements of R.