DIOPHANTINE SETS

BHARGAV BHATT AND BJORN POONEN

Abstract. Diophantine subsets of $\mathbb{Z}$ play a key role in the negative answer to Hilbert's tenth problem. The definition of diophantine set generalizes in several ways to other commutative rings. We compare these definitions. Along the way, we prove that for every finitely presented scheme Y over a ring R, there exists an *affine* R-scheme X with a finitely presented R-morphism $X \to Y$ such that $X(R') \to Y(R')$ is surjective for every R-algebra R'.

1. Introduction

A subset $A \subset \mathbb{Z}$ is **diophantine** if there exists $f \in \mathbb{Z}[t, x_1, \ldots, x_m]$ such that

$$A = \{a \in \mathbb{Z} : \exists x \in \mathbb{Z}^m \text{ such that } f(a, x) = 0\}.$$

In other words, if one thinks of t as a parameter, then f defines a 1-parameter family of diophantine equations, and A is the set of parameter values for which the specialized diophantine equation is solvable in the remaining variables. Diophantine sets play an essential role in the negative answer to Hilbert's tenth problem: the key step is proving that every computably enumerable subset of $\mathbb{Z}$ is diophantine; see [Mat93] for an exposition.

There are several ways to generalize the definition to ground rings other than $\mathbb{Z}$, and they are not always equivalent. The goal of this article is to sort out the relationships between various definitions; see Theorem 1.4.

Let R be a ring. (All rings in this paper are assumed commutative.)

- Call $A \subset R^n$ **existential** if $A = \{a \in R^n : \phi(a)\}$ for some existential first-order formula $\phi(t)$, that is, a formula $(\exists x_1) \cdots (\exists x_m)\ \psi(t, x)$, where $\psi(t, x)$ is a Boolean combination of polynomial equations in $t_1, \ldots, t_n, x_1, \ldots, x_m$.
- **Positive-existential** is the same except that the only logical operators allowed in the Boolean combination are $\wedge$ (and) and $\vee$ (or).
- **Many-polynomial-diophantine** is the same except that only $\wedge$ is allowed; in other words, there exist $r \in \mathbb{Z}_{\geq 0}$ and $f_1, \ldots, f_r \in R[t_1, \ldots, t_n, x_1, \ldots, x_m]$ such that

$$A = \{a \in R^n : \exists x \in R^m \text{ such that } f_1(a, x) = \cdots = f_r(a, x) = 0\}.$$

Date: January 14, 2026.

2020 *Mathematics Subject Classification.* Primary 11U05; Secondary 13G05, 14A15, 14G99.

Key words and phrases. Diophantine set, positive-existential set.

B.B. was partially supported by a fellowship from the Packard Foundation and grants from the Simons Foundations (MPS-SIM-00622511, MPS-PERF-00001529-02). B.P. was supported in part by Simons Foundation grant #402472. The research was partly carried out while B.P. was participating in the 2025 program "Definability, decidability, and computability" at the Hausdorff Research Institute in Bonn, funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2047/1 – 390685813.

- One-polynomial-diophantine is the same except that there is just one equation, with no Boolean operators; in other words, there exists $f \in R[t_1, \dots, t_n, x_1, \dots, x_m]$ such that

$$A = \{a \in R^n : \exists x \in R^m \text{ such that } f(a, x) = 0\}.$$

  See [Shl07, Definition 1.2.1].
- Let X be a finitely presented R-scheme. Call $A \subset X(R)$ morphism-diophantine if there exists an R-scheme Y and finitely presented R-morphism $\phi \colon Y \to X$ such that $A = \phi(Y(R))$.

Remark 1.1. If $f \in R[t_1, \dots, t_n]$, then the set of zeros of f in R^n is one-polynomial-diophantine (take $m = 0$ in the definition). Likewise, the common zero set of $f_1, \dots, f_r \in R[t_1, \dots, t_n]$ in R^n is many-polynomial-diophantine.

Remark 1.2. Any morphism of finitely presented R-schemes $X \to X'$ maps morphism-diophantine subsets of $X(R)$ to morphism-diophantine subsets of $X'(R)$ (use the same Y).

Remark 1.3. The notion of morphism-diophantine can be applied to $A \subset R^n$ by taking $X = \mathbb{A}^n_R$.

Theorem 1.4. *Let R be a ring.*

(a) *For $A \subset R^n$, one-polynomial-diophantine implies many-polynomial-diophantine.*
(b) *The converse holds for all n and all $A \subset R^n$ if and only if*

$$\text{there exists } g \in R[x, y] \text{ whose zero set in } R^2 \text{ is } \{(0, 0)\}. \tag{1}$$

(c) *For $A \subset R^n$, many-polynomial-diophantine implies positive-existential.*
(d) *The converse holds if and only if $(R \times \{0\}) \cup (\{0\} \times R)$ is many-polynomial-diophantine.*
(e) *For $A \subset R^n$, positive-existential implies existential.*
(f) *The converse holds if and only if $R - \{0\}$ is positive-existential.*
(g) *For $A \subset R^n$, many-polynomial-diophantine is equivalent to morphism-diophantine.*

Given (g), we propose that, going forward, diophantine should be defined as morphism-diophantine (or equivalently, for $A \subset R^n$, many-polynomial-diophantine).

Most of Theorem 1.4 is easy and well known. The only complicated part is (g), which will be deduced from Theorem 2.1.

Finally, in Sections 4–6, we explore for which rings the conditions in (b), (d), and (f) hold. The most substantial new result in these sections is Theorem 4.3, which states that if K is a field that is not an algebraic closure of a finite field, then there exists R with $\operatorname{Frac} R = K$ such that (1) holds.

Here is one application of all of the above, which we record for convenience of use:

Corollary 1.5. *Suppose that R is a domain satisfying any of the following:*

(i) *R is a finitely generated $\mathbb{Z}$-algebra.*
(ii) *R is a finitely generated algebra over a field k, but R is not an algebraically closed field.*
(iii) *R is a localization of one of the above.*

Then all five notions (existential, positive existential, many-polynomial-diophantine, one-polynomial-diophantine, and morphism-diophantine) are equivalent.

Proof. We check that the conditions for all the converses in Theorem 1.4 are satisfied:

(b) If the domain R is a finitely generated $\mathbb{Z}$-algebra, or a localization thereof, then $\operatorname{Frac} R$ is not algebraically closed. If the domain R is a finitely generated k-algebra with $\dim R > 0$, or a localization thereof, then $\operatorname{Frac} R$ is not algebraically closed. If the domain R is a finitely generated k-algebra and $\dim R = 0$, then R is a field, and by assumption it is not algebraically closed. Thus in all three cases, $\operatorname{Frac} R$ is not algebraically closed. By Proposition 4.1, (1) holds.

(d) Since R is a domain, $(R \times \{0\}) \cup (\{0\} \times R)$ is the zero set of xy, hence one-polynomial-diophantine, hence many-polynomial-diophantine.

(f) If $\dim R = 0$, then R is a field, so $R - \{0\}$ is defined by $(\exists x)\ tx = 1$, hence positive-existential. If $\dim R > 0$, then the function field $\operatorname{Frac} R$ cannot carry a nontrivial henselian valuation, so $R - \{0\}$ is positive-existential by work of Moret-Bailly; see Theorem 5.1(a). □

2. Covering by an affine scheme

Theorem 2.1. *Let R be a ring. Let Y be a finitely presented R-scheme. Then there exists an* affine *R-scheme X with a finitely presented R-morphism $X \to Y$ such that $X(R) \to Y(R)$ is surjective.*

Remark 2.2. Let $Y_1, \ldots, Y_n$ be an affine open cover of Y. If R is local, then the disjoint union $X := \sqcup Y_i$ works. But if R is not local, $Y(R)$ need not equal $\bigcup Y_i(R)$: a morphism $\operatorname{Spec} R \to Y$ does not necessarily have image contained in a single Y_i.

Remark 2.3. If Y is quasi-projective over R (or more generally Y has an ample family of line bundles), then Jouanolou's trick (as generalized by Thomason [Wei89, Proposition 4.4]) produces a vector bundle $E \to Y$ and an E-torsor $X \to Y$ with X affine, and then $X(R) \to Y(R)$ is surjective since vector bundles over affine schemes have no nontrivial torsors.

Proof of Theorem 2.1. Let $I = Y(R)$. Let $X' = \sqcup_I \operatorname{Spec} R$ and $X'' = \operatorname{Spec}(\prod_I R)$. There is an obvious R-morphism $X' \to Y$ with $X'(R) \to Y(R)$ surjective by construction. Since Y is finitely presented over a ring, Y is quasi-compact and quasi-separated, so [Bha16, Theorem 1.3] implies that $X' \to Y$ factors uniquely as $X' \to X'' \to Y$. By writing $\prod_I R$ as a filtered colimit of finitely presented R-algebras and using the finite presentation property of Y, we find a further factorization $X' \to X'' \to X \to Y$, where X is an affine, finitely presented R-scheme. The composite morphism was surjective on R-points, so $X \to Y$ is too. □

Although we do not need it for our application, we can also prove the following strengthening:

Theorem 2.4. *Let R be a ring. Let Y be a finitely presented R-scheme. Then there exists an affine R-scheme X with a finitely presented R-morphism $X \to Y$ such that $X(R') \to Y(R')$ is surjective* for every *R-algebra R'.*

Proof. Since Y is finitely presented over R, for each R', each element of $Y(R')$ comes from an element of $Y(R_0)$ for some finitely presented R-algebra R_0. Thus it suffices to find X such that $X(R_0) \to Y(R_0)$ is surjective for every finitely presented R-algebra R_0. Let $\mathscr{R}$ be a set of representatives of the isomorphism classes of finitely presented R-algebras. Let $X' = \sqcup_{R_0 \in \mathscr{R}} \sqcup_{y \in Y(R_0)} \operatorname{Spec} R_0$ and $X'' = \operatorname{Spec}\left(\prod_{R_0 \in \mathscr{R}} \prod_{y \in Y(R_0)} R_0\right)$. Produce a factorization

$X' \to X'' \to X \to Y$ as before. For every R_0, the morphism $X' \to Y$ is surjective on R_0-points, so $X \to Y$ is too. □

Remark 2.5. Theorem 2.4 says that if Y is a finitely presented scheme over a ring, then the category of affine schemes equipped with a morphism to Y has a *weak terminal object* X (every object maps to X, but not necessarily uniquely), and X can be taken to be finitely presented over Y.

Remark 2.6. The proofs of Theorems 2.1 and 2.4 generalize to the situation where Y is an *algebraic space* that is finitely presented over R.

3. Comparing the definitions

Proof of Theorem 1.4.

(a) Trivial.

(b) $\Rightarrow$: Suppose that every many-polynomial-diophantine set is one-polynomial-diophantine. Then the many-polynomial-diophantine subset $\{(0,0)\} \subset R^2$ defined by $t_1 = t_2 = 0$ is one-polynomial-diophantine. That is, there exists $f(t_1, t_2, x_1, \ldots, x_m)$ whose zero set contains $(0, 0, u)$ for some $u \in R^m$ but contains no points with $(t_1, t_2) \neq (0, 0)$. Then $g(t_1, t_2) := f(t_1, t_2, u)$ has zero set $\{(0, 0)\}$.
$\Leftarrow$: Suppose that $g(x, y)$ has zero set $\{(0, 0)\}$. We prove by induction on r that the common zero set of any r polynomials $f_1, \ldots, f_r$ is the zero set of a single polynomial f. If $r = 0$, take $f = 0$. If $r = 1$, take $f = f_1$. If $r \geq 2$, apply the inductive hypothesis to $g(f_1, f_2), f_3, \ldots, f_r$.

(c) Trivial.

(d) $\Rightarrow$: The $(R \times \{0\}) \cup (\{0\} \cup R) = \{(x, y) \in R^2 : x = 0 \vee y = 0\}$ is positive-existential. If positive-existential implies many-polynomial-diophantine, then it is many-polynomial-diophantine too.
$\Leftarrow$: In $\phi(t)$, convert each expression $f(t, x) = 0 \vee g(t, x) = 0$ to $f(t, x) = z \wedge g(t, x) = w \wedge (z = 0 \vee w = 0)$ and replace $z = 0 \vee w = 0$ with its many-polynomial-diophantine definition. Eventually, we rewrite $\phi(t)$ in the form $(\exists x_1) \cdots (\exists x_m)\psi(t, x)$ for some new m and ψ such that ψ is a finite conjunction of polynomial equations.

(e) Trivial.

(f) $\Rightarrow$: The set $R - \{0\} = \{x \in R : x \neq 0\}$ is existential. If existential implies positive-existential, then it is positive-existential too.
$\Leftarrow$: In $\phi(t)$, convert each expression $f(t, x) \neq 0$ to $f(t, x) = z \wedge z \neq 0$ and replace $z \neq 0$ with the equivalent positive-existential formula.

(g) $\Rightarrow$: To say that $A \subset R^n$ is many-polynomial-diophantine is to say that A is the image of the R-points under the projection morphism

$$\operatorname{Spec} \frac{R[t_1, \ldots, t_n, x_1, \ldots, x_m]}{(f_1, \ldots, f_r)} \longrightarrow \operatorname{Spec} R[t_1, \ldots, t_n] = \mathbb{A}^n_R$$

for some m and r and $f_1, \ldots, f_r \in R[t_1, \ldots, t_n, x_1, \ldots, x_m]$.
$\Leftarrow$: Suppose that $A \subset R^n$ is morphism-diophantine. By definition, $A = \phi(Y(R))$ for some morphism $\phi \colon Y \to \mathbb{A}^n_R$ of finitely presented R-schemes. Theorem 2.1 provides a morphism $\psi \colon X \to Y$ of finitely presented R-schemes such that $\psi(X(R)) = Y(R)$. Then $A = (\phi\psi)(X(R))$ and X is affine and finitely presented, so A is many-polynomial-diophantine. □

Remark 3.1. In the definition of morphism-diophantine for $A \subset X(R)$, we required the Y mapping to X to be a scheme. Remark 2.6 implies that allowing Y to be an algebraic space would yield an equivalent definition. One could also define morphism-diophantine for $A \subset X(R)$ with X a finitely presented R-algebraic space.

4. Two-variable polynomials vanishing only at $(0,0)$

Recall that (1) is the property that there exists $g \in R[x,y]$ whose zero set is $\{(0,0)\}$.

Proposition 4.1 (cf. [Shl07, Lemma 1.2.3])**.** *If R is a domain whose fraction field* $\operatorname{Frac} R$ *is not algebraically closed, then* (1) *holds.*

Proof. Let $K = \operatorname{Frac} R$. Since K is not algebraically closed, there is a nontrivial finite extension L/K. Let $\alpha \in L - K$. Let $h(x,y)$ be the norm form $\mathrm{N}_{L/K}(x + y\alpha) \in K[x,y]$. The only zero of h in K^2 is $(0,0)$. Let $g = rh$ where $r \in R - \{0\}$ is chosen so that $g \in R[x,y]$. Then the only zero of g in R^2 is $(0,0)$. □

For domains whose fraction field K is algebraically closed, the answer is sometimes yes, sometimes no, as the next two propositions show.

Proposition 4.2. *If K is an algebraically closed field, then* (1) *fails.*

Proof. If the zero set of $g \in K[x,y]$ is nonempty, its Krull dimension is at least $2 - 1 > 0$. □

If K is algebraic over a finite field, then any domain R with fraction field K equals K, and Proposition 4.2 applies. Otherwise, we have the following:

Theorem 4.3. *If K is a field that is not an algebraic closure of a finite field, there exists a domain R with fraction field K for which* (1) *holds.*

Proof. Because of Proposition 4.1, we may assume that K is algebraically closed.

First suppose that K is countable. If $\operatorname{char} K = 0$, let $A_0 = \mathbb{Z}$ and $F_0 = \mathbb{Q}$. If $\operatorname{char} K = p > 0$, let $A_0 = \mathbb{F}_p[t]$ and $F_0 = \mathbb{F}_p(t)$. Since K is not an algebraic closure of a finite field, we may view K as an extension of F_0. Let C be a smooth plane quartic in $\mathbb{P}^2_{F_0}$ passing through $(1:0:0)$; if $\operatorname{char} K > 0$, assume moreover that C is not isotrivial. The genus of C is at least 2 (it is 3), so the Mordell conjecture [Fal83] and its function field analogues [Gra65, Sam66] imply that $C(F)$ is finite for any finitely generated extension $F \supset F_0$.

Let $\mathbb{A}^2_{F_0} \subset \mathbb{P}^2_{F_0}$ be the standard affine patch containing $(1:0:0)$. Let $C' = C \cap \mathbb{A}^2_{F_0}$, which has an equation $g(x,y) = 0$. Then $C'(F_0)$ consists of $(0,0)$ and finitely many other points in F_0^2. By scaling coordinates, we may assume none of these other points lie in A_0^2. Let C' denote also the hypersurface in $\mathbb{A}^2_{A_0}$ defined by $g(x,y) = 0$. Thus $C'(A_0) = \{(0,0)\}$.

Write $K = \{\alpha_1, \alpha_2, \ldots\}$. Let $F_n = F_0(\alpha_1, \ldots, \alpha_n)$. By induction, we will construct finitely generated subrings $A_0 \subset A_1 \subset \cdots$ such that $\operatorname{Frac} A_n = F_n$ and $C'(A_n) = \{(0,0)\}$. Suppose that A_n has been constructed. Write $A = A_n$, $F = F_n$, $\alpha = \alpha_{n+1}$, so $F_{n+1} = F(\alpha)$.

Case 1: α is algebraic over F. Since F_{n+1} is finitely generated, $C(F_{n+1})$ is finite. By scaling α, we may assume that α is integral over A. We will let $A_{n+1} = A + cA[\alpha]$ for a suitable $c \in A - \{0\}$. We have $\bigcap_{c \in A - \{0\}} (A + cA[\alpha]) = A \subset F$, so for each of the finitely many $P \in C'(F_{n+1}) - C'(F)$, we can find c_P such that $P \notin (A + c_P A[\alpha])^2$. Let $c = \prod_P c_P$. Let $A_{n+1} = A + cA[\alpha]$. Then $P \notin A_{n+1}^2$ for all P. Hence $C'(A_{n+1}) - C'(F) = \emptyset$, so

$$C'(A_{n+1}) = C'(A_{n+1}) \cap C'(F) = C'(A_{n+1} \cap F) = C'(A) = \{(0,0)\}.$$

Case 2: α is transcendental over F. Every rational map $\mathbb{P}^1 \to C'$ is constant, so $C'(F(\alpha)) = C'(F)$. Thus if $A_{n+1} := A[\alpha]$, then $C'(A_{n+1}) = C'(A) = \{(0,0)\}$.

Now that we have all the A_n, let $R = \bigcup_{n \geq 0} A_n$. Then $\operatorname{Frac} R = \bigcup_{n\geq 0} F_n = K$, and $C'(R) = \bigcup_{n \geq 0} C'(A_n) = \{(0,0)\}$. This completes the proof when K is countable.

It remains to prove the result for one algebraically closed field of each characteristic and each uncountable cardinality κ. By taking an ultrapower of a countable field (for which we already know the result), we find K with $\#K \geq \kappa$ for which R and g exist. By the theory of transcendence bases, we can find an algebraically closed subfield $K_0 \subset K$ of the desired cardinality κ, and we may assume that K_0 contains the coefficients of g. Unfortunately, $R_0 := R \cap K_0$ might have fraction field smaller than K_0. To deal with this, we will enlarge R_0 and K_0. Represent each element of K as a quotient of elements of R, so that we can speak of its numerator and denominator. Given any subfield $L \subset K$, let L' be the extension of L generated by the numerators and denominators of all the elements of L, and let $\phi(L)$ be the algebraic closure of L' in K. For $n \in \mathbb{Z}_{\geq 0}$, let $K_{n+1} = \phi(K_n)$. By induction, $\#K_n = \kappa$ for all n. Let $K_\omega = \bigcup K_n$, so $\#K_\omega = \kappa$. Let $R_\omega = R \cap K_\omega$. Each $a \in K_\omega$ lies in K_n for some n, so its numerator and denominator lie in $K_{n+1} \subset K_\omega$, hence in R_ω. Thus $\operatorname{Frac} R_\omega = K_\omega$. Also, the only solution to $g(x,y) = 0$ in R^2 is $(0,0)$, so the same is true in R_ω^2. In other words, the result holds for K_ω. □

Proposition 4.4. *Let R be a normal domain with* $\operatorname{Frac} R$ *isomorphic to $\overline{\mathbb{Q}}$ or $\overline{\mathbb{F}_p(t)}$. Then* (1) *fails for R.*

Proof. This is a consequence of work of Rumely [Rum86], extended by Moret-Bailly [MB89]. Let $g \in R[x,y]$ be such that $g(0,0) = 0$. We will show that $g(x,y) = 0$ has infinitely many solutions over R.

Factor g over the algebraically closed field $\operatorname{Frac} R$; some factor vanishes at $(0,0)$ and may be scaled to assume that it has coefficients in R. Without loss of generality, replace g by this factor. Now g is geometrically irreducible.

Let R_0 be the ring generated by the coefficients of g, together with one transcendental element of R if $\operatorname{Frac} R = \overline{\mathbb{F}_p(t)}$. Let R_1 and $\overline{R}_1$ be the integral closures of R_0 in $\operatorname{Frac} R_0$ and $\operatorname{Frac} R$, respectively, so $R_0 \subset R_1 \subset \overline{R}_1 \subset R$. Then R_1 is an excellent Dedekind domain satisfying condition (**T**) of [MB89]. The morphism $\operatorname{Spec} R_1[x,y]/(g) \to \operatorname{Spec} R_1$ is surjective because of the $(0,0)$ section. Applying [MB89, §6] to R_1 proves that $g(x,y) = 0$ has infinitely many solutions over $\overline{R}_1$, and hence also over R. □

Question 4.5. Does (1) hold for *some* normal domain with algebraically closed fraction field?

5. Defining the nonzero elements

Theorem 5.1 (Moret-Bailly)**.** *Let R be a noetherian ring.*

(a) *If R is a domain that is not local henselian, then $R - \{0\}$ is positive-existential.*
(b) *If R is a localization of a noetherian Jacobson ring, then $R - \{0\}$ is positive-existential.*
(c) *If R is a henselian excellent local ring and* $\dim R > 0$*, then $R - \{0\}$ is* not *positive-existential.*

Proof. For the ring of integers in a number field, see [DL78, Proposition 1(b)]. For the ring of S-integers in a global field (even when S is infinite), see [Shl07, Proposition 2.2.4]. The general case is [MB07]. $\square$

See [MB07] for further results along these lines.

6. Defining the union of two axes

If R is a domain, then $(R \times \{0\}) \cup (\{0\} \times R)$ is one-polynomial-diophantine, since it is the set of solutions to $xy = 0$. For non-domains, sometimes $(R \times \{0\}) \cup (\{0\} \times R)$ is many-polynomial-diophantine (necessarily via polynomials different from xy), and sometimes it is not:

Proposition 6.1. *For a ring R, the following are equivalent:*

(i) *R is not a product of two nonzero rings.*
(ii) $\operatorname{Spec} R$ *is connected or empty.*
(iii) *Any finite union of many-polynomial-diophantine sets is many-polynomial-diophantine.*
(iv) *The set $(R \times \{0\}) \cup (\{0\} \times R)$ is many-polynomial-diophantine.*

Proof.
(i)⇒(ii): (This is well-known.) We prove the contrapositive. Suppose that $\operatorname{Spec} R$ is the disjoint union of nonempty open sets U_0 and U_1. For $i = 0, 1$, let $r_i \in R$ be the element that is 1 on U_i and 0 on U_{1-i}. Thus r_0 and r_1 are idempotents summing to 1, so $R = r_0 R \times r_1 R$.

(ii)⇒(iii): If $\operatorname{Spec} R$ is empty, then $R = 0$ and (iii) holds.

Now assume that $\operatorname{Spec} R$ is connected. It suffices to consider the union of *two* many-polynomial-diophantine sets of R^n. Write the first as the image of $X_0(R)$ under the projection $\mathbb{A}^{n+m} \to \mathbb{A}^n$ for some finitely presented closed subscheme $X_0 \subset \mathbb{A}^{n+m}$. Similarly, write the second as the image of $X_1(R)$ for some $X_1 \subset \mathbb{A}^{n+m}$; we may assume that the m is the same, by enlarging the smaller m if necessary. Let Y be the (disjoint) union of $Y_0 := X_0 \times \{0\}$ and $Y_1 := X_1 \times \{1\}$ in $\mathbb{A}^{n+m+1}$. Since $\operatorname{Spec} R$ is connected, any morphism $\operatorname{Spec} R \to Y$ has image contained in either Y_0 or Y_1. That is, $Y(R) = Y_0(R) \cup Y_1(R)$. Thus the image of $Y(R)$ under the projection $\mathbb{A}^{n+m+1} \to \mathbb{A}^n$ is the union of the two given sets. Finally, Y is a finitely presented closed subscheme of $\mathbb{A}^{n+m+1}$, so the image of $Y(R)$ is many-polynomial-diophantine.

(iii)⇒(iv): Both $R \times \{0\}$ and $\{0\} \times R$ are many-polynomial-diophantine (even one-polynomial diophantine). By (iii), their union is many-polynomial-diophantine.

(iv)⇒(i): We prove the contrapositive. Suppose that $R \simeq R_1 \times R_2$ with $R_1, R_2 \neq 0$. Call $A \subset R^n = R_1^n \times R_2^n$ a product set if it is $A_1 \times A_2$ for some sets $A_i \subset R_i^n$. Each $f \in R[x_1, \ldots, x_n]$ amounts to a pair of functions $f_i \in R_i[x_1, \ldots, x_n]$, so the zero set of f is a product set. Intersecting product sets yields a product set, and the image of a product set under a projection $R^{n+m} \to R^n$ is a product set. Thus every many-polynomial-diophantine subset of R^n is a product set. But $(R \times \{0\}) \cup (\{0\} \times R)$ is not a product set, because, viewed in $R_1^2 \times R_2^2$, it contains $((1,0),(1,0))$ and $((0,1),(0,1))$ but not $((1,0),(0,1))$. Thus $(R \times \{0\}) \cup (\{0\} \times R)$ is not many-polynomial-diophantine. $\square$

Acknowledgments

We thank Laurent Moret-Bailly for several comments and corrections, and in particular for pointing out Remark 2.3. We thank also Philip Dittmann.

References

[Bha16] Bhargav Bhatt, *Algebraization and Tannaka duality*, Camb. J. Math. **4** (2016), no. 4, 403–461. MR 3572635 3

[DL78] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391. MR 518221 7

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, English translation: Finiteness theorems for abelian varieties over number fields, 9–27 in *Arithmetic Geometry (Storrs, Conn., 1984)*, Springer, New York, 1986. Erratum in: Invent. Math. **75** (1984), 381. MR 718935 5

[Gra65] Hans Grauert, *Mordells Vermutung über rationale Punkte auf algebraischen Kurven und Funktionenkörper*, Inst. Hautes Études Sci. Publ. Math. (1965), no. 25, 131–149. MR 222087 5

[Mat93] Yuri V. Matiyasevich, *Hilbert's tenth problem*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1993, Translated from the 1993 Russian original by the author, With a foreword by Martin Davis. MR 1244324 1

[MB89] Laurent Moret-Bailly, *Groupes de Picard et problèmes de Skolem. I*, Ann. Sci. École Norm. Sup. (4) **22** (1989), no. 2, 161–179. MR 1005158 6

[MB07] ———, *Sur la définissabilité existentielle de la non-nullité dans les anneaux*, Algebra Number Theory **1** (2007), no. 3, 331–346. MR 2361937 7

[Rum86] Robert S. Rumely, *Arithmetic over the ring of all algebraic integers*, J. Reine Angew. Math. **368** (1986), 127–133. MR 850618 6

[Sam66] Pierre Samuel, *Compléments à un article de Hans Grauert sur la conjecture de Mordell*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 29, 55–62. MR 204430 5

[Shl07] Alexandra Shlapentokh, *Hilbert's tenth problem*, New Mathematical Monographs, vol. 7, Cambridge University Press, Cambridge, 2007, Diophantine classes and extensions to global fields. MR 2297245 2, 5, 7

[Wei89] Charles A. Weibel, *Homotopy algebraic K-theory*, Algebraic K-theory and algebraic number theory (Honolulu, HI, 1987), Contemp. Math., vol. 83, Amer. Math. Soc., Providence, RI, 1989, pp. 461–488. MR 991991 3

School of Mathematics, Institute for Advanced Study & Department of Mathematics, Princeton University

Email address: `bhargav.bhatt@gmail.com`

URL: `https://www.math.ias.edu/~bhatt/`

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

Email address: `poonen@math.mit.edu`

URL: `http://math.mit.edu/~poonen/`