Automorphisms mapping a point into a subvariety

AUTOMORPHISMS MAPPING A POINT INTO A SUBVARIETY

BJORN POONEN

(with an appendix by Matthias Aschenbrenner*)*

Abstract. The problem of deciding, given a complex variety X, a point $x \in X$, and a subvariety $Z \subseteq X$, whether there is an automorphism of X mapping x into Z is proved undecidable. Along the way, we prove the undecidability of a version of Hilbert's tenth problem for systems of polynomials over $\mathbb{Z}$ defining an affine $\mathbb{Q}$-variety whose projective closure is smooth.

1. Introduction

Theorem 1.1. *There is no algorithm that, given a nice complex variety X, a closed point $x \in X$, and a nice subvariety $Z \subseteq X$, decides whether or not there is an automorphism of X mapping x into Z.*

Variety means separated scheme of finite type over a field. Nice means smooth, projective, and geometrically integral (we will eventually apply this adjective also to varieties over fields that are not algebraically closed). Algorithm means Turing machine. So that the input admits a finite description, we assume that the input includes a description of a finitely generated subfield K of $\mathbb{C}$ and that the coefficients of the equations defining X, x, Z are elements of K. More precisely, we assume that we are given $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$ such that $\mathbb{Z}[x_1, \dots, x_n]/(f_1, \dots, f_m)$ is a domain with fraction field K, and that elements of K are presented as rational expressions in the generators.

Actually, we show that the problem is undecidable even if X, x, Z are base extensions of $\mathbb{Q}$-varieties. In fact, we prove a strong form of Theorem 1.1:

Theorem 1.2. *There is a* fixed *nice $\mathbb{Q}$-variety X and a fixed rational point x on X such that it is impossible to decide which nice $\mathbb{Q}$-subvarieties Z of X meet $\{\sigma x : \sigma \in \operatorname{Aut} X\}$.*

That is, there is no algorithm that takes Z as input and decides whether there exists an automorphism of X mapping x into Z.

Finally, our X in Theorem 1.2 will have $\operatorname{Aut} X = \operatorname{Aut} X_{\mathbb{C}}$, where $X_{\mathbb{C}}$ is the base extension $X \underset{\operatorname{Spec} \mathbb{Q}}{\times} \operatorname{Spec} \mathbb{C}$, so it does not matter whether we consider only automorphisms defined over $\mathbb{Q}$ or also automorphisms over $\mathbb{C}$.

These problems are proved undecidable by relating them to Hilbert's tenth problem. Hilbert asked for an algorithm to decide, given a multivariable polynomial equation with

Date: February 22, 2011.

2000 *Mathematics Subject Classification.* Primary 14Q20; Secondary 11U05.

Key words and phrases. automorphism, Hilbert's tenth problem, undecidability.

M. A. and B. P. were partially supported by NSF grants DMS-0556197 and DMS-0841321, respectively.

integer coefficients, whether or not it was solvable in integers. Matiyasevich [Mat70], building on earlier work of Davis, Putnam, and Robinson [DPR61], proved that no such algorithm exists.

Remark 1.3. If X is a nice variety of general type, the problems above are *decidable* because $\operatorname{Aut} X$ is finite and computable as a subgroup of some PGL_n acting on some pluricanonical image of X.

Remark 1.4. This is not the first time that a problem in algebraic geometry has been proved undecidable. The problem of deciding whether a rational map of complex varieties $X \dashrightarrow \mathbb{P}^2$ admits a rational section is undecidable [KR92] (this is equivalent to the analogue of Hilbert's tenth problem for $\mathbb{C}(T_1, T_2)$). The generalization with $\mathbb{P}^2$ replaced by any fixed complex variety of dimension at least 2 is undecidable too [Eis04]. (But the analogue for $\mathbb{P}^1$ is still open, as is the analogue for any other fixed curve.)

Remark 1.5. Burt Totaro asked the author in 2007 whether the problem of deciding whether two varieties are isomorphic is undecidable.

2. Lattice automorphisms preserving a finite subset

The group of affine linear automorphisms of $\mathbb{Z}^n$ is the semidirect product $\mathrm{GL}_n(\mathbb{Z}) \ltimes \mathbb{Z}^n$, with $(A, \vec{b})$ acting as $\vec{x} \mapsto A\vec{x} + \vec{b}$.

Lemma 2.1. *For each $n \geq 3$, there exists a finite subset S of $\mathbb{Z}^n$ containing $\vec{0} := (0, 0, \ldots, 0)$ such that the subgroup of $\mathrm{GL}_n(\mathbb{Z}) \ltimes \mathbb{Z}^n$ mapping S to S equals the subgroup G of linear maps given by matrices*

$$\begin{pmatrix} 1 & & & & a_1 \\ & 1 & & & a_2 \\ & & \ddots & & \vdots \\ & & & 1 & a_{n-1} \\ & & & & a_n \end{pmatrix}$$

with $a_i \in \mathbb{Z}$ for all i and $a_n = \pm 1$.

Proof. Let p_i be the i^{th} prime. For $1 \leq i \leq n-1$, let $v_i \in \mathbb{Z}^n$ be the vector with p_i in the i^{th} coordinate and 0 elsewhere. Let $S = \{\vec{0}, v_1, \ldots, v_{n-1}\}$. Let G' be the subgroup of $\mathrm{GL}_n(\mathbb{Z}) \ltimes \mathbb{Z}^n$ mapping S to itself. Suppose that $g \in G'$. Then g fixes $\vec{0}$ since each other vector in S differs from some other vector by a primitive vector. Also g fixes v_i for each i, since v_i is distinguished from the other v_j by being divisible by p_i. So g fixes S pointwise. It hence acts trivially on the real affine linear span of S, so it acts trivially on $\mathbb{Z}^{n-1} \times 0$. Thus $G' \subseteq G$. Conversely, elements of G map S to S. So $G' = G$. □

Remark 2.2. In fact, Lemma 2.1 holds for all $n \geq 1$.

3. Blow-ups of powers of an elliptic curve

In this section, we prove a weak version of Theorem 1.1 in which Z is not required to be smooth or integral.

Fix an elliptic curve E over $\mathbb{Q}$ such that $\operatorname{End} E \simeq \mathbb{Z}$ and such that $E(\mathbb{Q})$ contains a point P of infinite order. For instance, E could be the curve labelled 37A1 in [Cre97], with equation $y^2 + y = x^3 - x$, and P could be $(0, 0)$. Let $n \geq 3$. Let X be the blow-up of E^n at the subset

$S' \subset (\mathbb{Z} \cdot P)^n$ corresponding to the subset $S \subset \mathbb{Z}^n$ given by Lemma 2.1. For a variety V, we write $\operatorname{Aut} V$ for the group of automorphisms of V *as a variety without extra structure*, even if V is an abelian variety. The birational morphism $X \to E^n$ is the map from X to its Albanese torsor, so there is an injective homomorphism $\operatorname{Aut} X \to \operatorname{Aut} E^n$ whose image equals the subgroup of $\operatorname{Aut} E^n$ mapping S' to itself. Any such automorphism of E^n must be of the form $\vec{x} \mapsto A\vec{x}+\vec{b}$ for some $A \in \mathrm{GL}_n(\mathbb{Z})$ and $\vec{b} \in E^n$, but $S' \subset (\mathbb{Z}\cdot P)^n$ so $\vec{b} \in (\mathbb{Z}\cdot P)^n$. It follows that $\operatorname{Aut} X$ is isomorphic to the group G in Lemma 2.1. Identify the exceptional divisor D above $\vec{0} \in E^n$ with $\mathbb{P}^{n-1}$ in the natural way. Let $x = (0 : \cdots : 0 : 1) \in \mathbb{P}^{n-1} = D \subseteq X$. If $\sigma \in \operatorname{Aut} X$ corresponds to

$$\begin{pmatrix} 1 & & & & a_1 \\ & 1 & & & a_2 \\ & & \ddots & & \vdots \\ & & & 1 & a_{n-1} \\ & & & & a_n \end{pmatrix} \in G,$$

then $\sigma x = (a_1 : \cdots : a_n) \in \mathbb{P}^{n-1}$.

Given a polynomial $f(t_1, \ldots, t_{n-1}) \in \mathbb{Z}[t_1, \ldots, t_{n-1}]$, let $F(t_1, \ldots, t_n) \in \mathbb{Z}[t_1, \ldots, t_n]$ be its homogenization, and let Z be the zero locus of F in $\mathbb{P}^{n-1} = D \subseteq X$. Then f has a zero in $\mathbb{Z}^{n-1}$ if and only if F has a zero in $\mathbb{Z}^{n-1} \times \{\pm 1\}$, which holds if and only if $\sigma x \in Z$ for some $\sigma \in \operatorname{Aut} X$.

Since the general problem of deciding whether a polynomial in $\mathbb{Z}[t_1, \ldots, t_{n-1}]$ has an zero in $\mathbb{Z}^{n-1}$ is undecidable, the general problem of deciding whether $\sigma x \in Z$ for some $\sigma \in \operatorname{Aut} X$ is undecidable too.

4. Making the subvariety smooth

Lemma 4.1. *There is an algorithm that, given a nonconstant $f \in \mathbb{Z}[x_1, \ldots, x_n]$, constructs a polynomial $F \in \mathbb{Z}[x_1, \ldots, x_{n+1}]$ such that*

(i) *The equation $f(\vec{a}) = 0$ has a solution $\vec{a} \in \mathbb{Z}^n$ if and only if $F(\vec{b}) = 0$ has a solution $\vec{b} \in \mathbb{Z}^{n+1}$.*
(ii) *The affine variety $X := \operatorname{Spec} \mathbb{Q}[x_1, \ldots, x_{n+1}]/(F)$ is smooth and geometrically integral.*
(iii) *We have $\deg F = 2 \deg f$. (Here* deg *denotes total degree.)*

Proof. Consider $F(x_1, \ldots, x_n, y) = c(y^2 - y) + f(x_1, \ldots, x_n)^2$ for some $c \in \mathbb{Z}_{>0}$. The values of $y^2 - y$ and $f(x_1, \ldots, x_n)^2$ on integer inputs are nonnegative, so (i) is satisfied. The singular locus S of X is contained in the locus where $\partial F/\partial y = 0$, which is $2y - 1 = 0$ in $\mathbb{A}^N$. On the other hand, Bertini's theorem ([Har77, Remark III.10.9.2]) shows that S is contained in $y^2 - y = 0$ for all but finitely many c. In this case $S = \emptyset$, so X is smooth over $\mathbb{Q}$. By testing $c = 1, 2, \ldots$ in turn, we can effectively find the first c for which X is smooth over $\mathbb{Q}$.

This X is also geometrically integral: since X is isomorphic to a variety of the form $z^2 - g = 0$ for some nonconstant $g \in \mathbb{Z}[x_1, \ldots, x_n]$, if it were not geometrically integral, $z^2 - g$ would factor as $(z + h)(z - h)$ for some nonconstant $h \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$, but then X would have to be singular at the common zeros of z and h, a contradiction. □

Lemma 4.2. *There is an algorithm that, given an affine scheme U of finite type over $\mathbb{Z}$ whose generic fiber $U_{\mathbb{Q}}$ is smooth over $\mathbb{Q}$, constructs $N \in \mathbb{Z}_{>0}$ and a closed immersion $U \hookrightarrow \mathbb{A}^N_{\mathbb{Z}}$*

such that the projective closure of the generic fiber $U_{\mathbb{Q}}$ in $\mathbb{P}^N_{\mathbb{Q}}$ is smooth. Moreover, N can be bounded in terms of the degree and number of variables of the equations defining U.

Proof. Embed U as a closed subscheme of some $\mathbb{A}^m_{\mathbb{Z}}$. Identify $\mathbb{A}^m_{\mathbb{Z}}$ with the locus in $\mathbb{P}^m_{\mathbb{Z}} = \operatorname{Proj}\mathbb{Z}[x_0, \ldots, x_m]$ where $x_0 \neq 0$. Let X be the closure of U in $\mathbb{P}^m_{\mathbb{Z}}$. Let $H = X - U$.

Effective resolution of singularities [Vil89, Vil92, BM91, BM97, BS00] lets us construct a coherent sheaf of ideals $\mathcal{I}_{\mathbb{Q}}$ on $X_{\mathbb{Q}}$ with support contained in $H_{\mathbb{Q}}$ such that blowing up $X_{\mathbb{Q}}$ along $\mathcal{I}_{\mathbb{Q}}$ yields a smooth $\mathbb{Q}$-scheme. Moreover, resolution of singularities has computably bounded complexity as one varies the variety in an algebraic family, by Noetherian induction: namely, reduce to the case of an irreducible base B, compute the blow-ups needed to resolve the generic fiber, examine the denominators in the rational functions on B that arise in the coefficients, define the open subscheme V of B on which these denominators are invertible so that the same sequence of blow-ups specializes to give a resolution for any fiber above a point of V, and finally apply the inductive hypothesis to the family over $B - V$, which has lower dimension. Therefore the degrees of the homogeneous polynomials that locally generate $\mathcal{I}_{\mathbb{Q}}$ can be bounded (in terms of the degree and number of variables of the equations defining U). Let $I_{\mathbb{Q}}$ be the homogeneous ideal of $\mathbb{Q}[x_0, \ldots, x_m]$ generated by these polynomials. Since the support of $\mathcal{I}_{\mathbb{Q}}$ is contained in $H_{\mathbb{Q}}$, the Nullstellensatz shows that there is a positive integer r such that $x_0^r \in I_{\mathbb{Q}}$. By Noetherian induction again, r is bounded. We have $x_0^r \in I$.

By the appendix to this article, we can compute $I := I_{\mathbb{Q}} \cap \mathbb{Z}[x_0, \ldots, x_m]$. Moreover, the degrees of the generators of I can be bounded in terms of those of $I_{\mathbb{Q}}$, as explained in the remarks at the end of the appendix. Choose d larger than all these degrees and larger than r. Blowing up the coherent sheaf of ideals on X defined by I yields $X' \xrightarrow{\pi} X$ with $X'_{\mathbb{Q}}$ smooth over $\mathbb{Q}$. Let E be the exceptional divisor on X'.

A basis for the degree-d part I_d of I determines a projective embedding of X' in some $\mathbb{P}^N_{\mathbb{Z}}$ (cf. the proofs of [Har77, II.7.10(b) and II.7.16(c)]), and N is bounded. We have $x_0^d \in I_d$, and the corresponding hyperplane section of X' is the Cartier divisor $d\pi^*H - E$, which has the same support as π^*H, since $d > r$. Let $\mathbb{A}^N_{\mathbb{Z}}$ be the complement in $\mathbb{P}^N_{\mathbb{Z}}$ of the hyperplane defined by the coordinate corresponding to $x_0^d \in I_d$. Then $X' \cap \mathbb{A}^N_{\mathbb{Z}} = X' - \pi^{-1}(H) = \pi^{-1}(U) \simeq U$. In other words, U is isomorphic to a closed subscheme of $\mathbb{A}^N_{\mathbb{Z}}$ whose projective closure is X', and the generic fiber $X'_{\mathbb{Q}}$ of X' is smooth. □

Combining the previous two lemmas with the negative solution to Hilbert's tenth problem yields:

Corollary 4.3. *There is no algorithm that, given $f_1, \ldots, f_m \in \mathbb{Z}[x_1, \ldots, x_n]$ such that the projective closure of* $\operatorname{Spec}\mathbb{Q}[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ *in $\mathbb{P}^n_{\mathbb{Q}}$ is smooth and geometrically integral over $\mathbb{Q}$, decides whether $f_1(\vec{a}) = \cdots = f_m(\vec{a}) = 0$ has a solution $\vec{a} \in \mathbb{Z}^n$.*

Applying the construction of Section 3 to the smooth projective geometrically integral $\mathbb{Q}$-variety Z arising as the projective closure in Corollary 4.3 proves Theorem 1.1.

5. Uniformity

In this section we prove Theorem 1.2. In our proof of Theorem 1.1, the variety X and the point x depend only on the integer n chosen at the beginning of Section 3.

The negative solution of Hilbert's tenth problem shows that there are fixed m and d such that the problem of deciding whether an m-variable polynomial of total degree d is solvable

in natural numbers is undecidable [Mat70]. Replacing each variable by a sum of squares of four new variables and applying Lagrange's theorem that every nonnegative integer is a sum of four squares shows that the same uniform undecidability holds for solvability in integers, provided that we replace (m, d) by $(4m, 2d)$. Combining this with Lemma 4.1 yields undecidability even if we restrict to polynomials defining a smooth affine hypersurface over $\mathbb{Q}$, provided that we replace (m, d) by $(m+1, 2d)$. Lemma 4.2 re-embeds these hypersurfaces in a projective space of bounded dimension, which can then be embedded in a larger projective space of *fixed* dimension D. Finally we may take $n = D + 1$ in Section 3. This completes the proof of Theorem 1.2.

Acknowledgements

It was a discussion with Burt Totaro that inspired the research leading to this article. I thank Andrew Kresch, Florian Pop, and Yuri Tschinkel for a teatime discussion at the Hausdorff Institute for Mathematics that led to an outline of the proof of Lemma 4.2. I thank Matthias Aschenbrenner for permission to include his appendix. Finally, I thank Steven Dale Cutkosky, David Eisenbud, Herwig Hauser, and Laurent Moret-Bailly for suggestions regarding references.

Appendix: Algorithms for computing saturations of ideals in finitely generated commutative rings

by Matthias Aschenbrenner

Consider the following basic task:

> *Given a finitely generated commutative $\mathbb{Z}$-algebra A (specified by generators and relations) and a finite list of generators for an ideal I of A, compute a finite list of generators for the inverse image of the ideal $I \otimes \mathbb{Q}$ under the natural morphism $A \to A \otimes \mathbb{Q}$.*

The existence of such an algorithm is well-known [GTZ88, Corollary 3.8], and the purpose of this appendix is to briefly describe two different procedures for the task at hand, and to make some additional related remarks. Before this, we observe that representing the $\mathbb{Z}$-algebra A as a quotient $A = \mathbb{Z}[X]/J$ where J is an ideal of the polynomial ring $\mathbb{Z}[X] = \mathbb{Z}[X_1, \dots, X_N]$ (where N and generators for J are part of the input data) one sees that it suffices to consider the case where A is a polynomial ring over $\mathbb{Z}$. In this case, the pullback ideal in question may also simply be described as the *saturation* $I\mathbb{Q}[X] \cap \mathbb{Z}[X]$ of I with respect to the multiplicative subset $\mathbb{Z} \setminus \{0\}$ of $\mathbb{Z}[X]$. That is, we need to give an algorithm which does the following:

> *Given $N \in \mathbb{N}$ and generators $f_1, \dots, f_n$ for an ideal I of $\mathbb{Z}[X] = \mathbb{Z}[X_1, \dots, X_N]$, compute a finite list of generators for the ideal $I\mathbb{Q}[X] \cap \mathbb{Z}[X]$ of $\mathbb{Z}[X]$.*

In fact, both algorithms below compute a nonzero integer δ such that $(I : \delta) = I\mathbb{Q}[X] \cap \mathbb{Z}[X]$ as well as a finite list of generators for the ideal $(I : \delta)$.

Algorithm 1. This algorithm, from [GTZ88, §3], uses Gröbner bases in polynomial rings over $\mathbb{Z}$. For basic facts about Gröbner bases in this context, see [AL94]. One may proceed as follows:

(1) Compute a Gröbner basis G of I with respect to an arbitrary monomial ordering of the monomials in X. Let s be the least common multiple of the leading coefficients of the elements of G, with $s = 1$ if $I = \{0\}$ (and hence $G = \emptyset$). Then we have

$$I\mathbb{Q}[X] \cap \mathbb{Z}[X] = I\mathbb{Z}[\tfrac{1}{s}][X] \cap \mathbb{Z}[X]$$

by [AL94, Proposition 4.4.4]. (The integer s also has the property that $(\mathbb{Z}[X]/I)[\frac{1}{s}]$ is a free $\mathbb{Z}[\frac{1}{s}]$-module [Vas97, Theorem 2.1]; this is a particular instance of Grothendieck's "generic freeness lemma".)

(2) Next, let Y be a new indeterminate, distinct from $X_1, \ldots, X_N$. Then

$$I\mathbb{Z}[\tfrac{1}{s}][X] \cap \mathbb{Z}[X] = (I, Ys - 1) \cap \mathbb{Z}[X]$$

by [AL94, Proposition 4.4.1]. Fix an arbitrary monomial ordering $<_X$ of the monomials $X^\alpha = X_1^{\alpha_1} \cdots X_N^{\alpha_N}$ ($\alpha = (\alpha_1, \ldots, \alpha_N) \in \mathbb{N}^N$) in X. Compute a Gröbner basis G_s for the ideal $(I, Ys - 1)$ of $\mathbb{Z}[X, Y]$ with respect to the monomial ordering given by

$$X^\alpha Y^a < X^\beta Y^b \quad \Longleftrightarrow \quad a < b, \text{ or } a = b \text{ and } X^\alpha <_X X^\beta.$$

Then the finite set $G_s \cap \mathbb{Z}[X]$ is a Gröbner basis for $(I, Ys-1) \cap \mathbb{Z}[X] = I\mathbb{Q}[X] \cap \mathbb{Z}[X]$, by [AL94, Theorem 4.3.6].

As a bonus, if we choose a nonzero integer δ such that $\delta g \in I$ for all $g \in G_s \cap \mathbb{Z}[X]$, then $I\mathbb{Q}[X] \cap \mathbb{Z}[X] = (I : \delta)$. (We may take δ to be a power of s.)

Algorithm 2. This algorithm, implicit in [Asc04], uses the natural division of the problem posed into two subproblems:

(P1) Compute an integer δ such that $(I : \delta) = I\mathbb{Q}[X] \cap \mathbb{Z}[X]$.
(P2) Compute, given $g \in \mathbb{Z}[X]$, a finite list of generators for the ideal $(I : g)$.

First, as a byproduct of Hermann's classical algorithm [Her26] for deciding ideal membership in polynomial rings over fields, one obtains a procedure for computing a polynomial $P(C) \in \mathbb{Z}[C]$ in the coefficient tuple c of $f_1, \ldots, f_n$ such that $\delta = P(c)$ has the property in (P1); see [Asc04, Section 3]. Subproblem (P2) is approached by specifying an algorithm which accomplishes the following:

(P2′) Given $g_1, \ldots, g_m \in \mathbb{Z}[X]$, compute a finite generating set for the $\mathbb{Z}[X]$-submodule of $\mathbb{Z}[X]^m$ consisting of the solutions to the homogeneous linear equation $y_1 g_1 + \cdots + y_m g_m = 0$.

To see how this solves (P2), given $g \in \mathbb{Z}[X]$, consider the homogeneous linear equation

$$y_1 f_1 + \cdots + y_n f_n = y_{n+1} g.$$

Then the projection onto the $(n + 1)$st components of every generating set for the $\mathbb{Z}[X]$-module of solutions to this equation in $\mathbb{Z}[X]^{n+1}$ is a generating set for the ideal $(I : g)$. An algorithm for (P2′), based on an adaptation of Hermann's algorithm from $\mathbb{Q}[X]$ to $\mathbb{Z}[X]$, may be found in [Asc04, Section 4]. (Of course, (P2′) may also be solved using Gröbner bases: it suffices to note that given a Gröbner basis G for the ideal $(g_1, \ldots, g_m)$ of $\mathbb{Z}[X]$ with respect to an arbitrary monomial ordering, the representations of the S-polynomials of G in normal form with respect to G give rise to a finite generating set for the syzygies of $g_1, \ldots, g_m$; see [AL94, Theorem 4.3.16].)

Remarks. Algorithm 1 seems better suited for practical computations. However, unlike in the case of fields, the precise worst-case behavior of the analogue of Buchberger's algorithm for computing Gröbner bases over $\mathbb{Z}[X]$ is as of yet still unclear. (For very weak bounds see [GM94], and for further discussion the forthcoming [Asc09].) Algorithm 2 has the advantage of coming with explicit (doubly-exponential) complexity bounds: for example, suppose $d \in \mathbb{N}$ is an upper bound on the (total) degree of f_i for $i = 1, \ldots, n$; then $I\mathbb{Q}[X] \cap \mathbb{Z}[X] = (g_1, \ldots, g_m)$ where $\deg(g_j) \leq (2d)^{2^{N \log(N+1)}}$ for $j = 1, \ldots, m$, cf. [Asc04, Theorem B]. (Note that this bound only depends on the bound d on the degrees and not on the particular coefficients of the f_i.)

In connection with (P1), we remark that the *smallest* positive integer δ such that $(I : \delta) = I\mathbb{Q}[X] \cap \mathbb{Z}[X]$ agrees with the exponent of the torsion subgroup of the additive group of $\mathbb{Z}[X]/I$. (The torsion subgroup of the additive group of a Noetherian ring always has finite exponent.) The algorithms indicated above, together with a procedure for deciding equality of ideals in $\mathbb{Z}[X]$ (found in [GTZ88, Asc04]), give rise to a procedure for computing this exponent in an obvious way; another algorithm was given by Clivio [Cli90] (based on earlier work of Ayoub [Ayo83]).

References

[AL94] William W. Adams and Philippe Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994. MR **1287608 (95g:**13025) ↑5, 1, 2, 5

[Asc04] Matthias Aschenbrenner, *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. **17** (2004), no. 2, 407–441 (electronic). MR **2051617 (2005c:**13032) ↑5, 5

[Asc09] ———, *Uniform degree bounds for Gröbner bases*, 2009. In preparation. ↑5

[Ayo83] Christine W. Ayoub, *On constructing bases for ideals in polynomial rings over the integers*, J. Number Theory **17** (1983), no. 2, 204–225, DOI 10.1016/0022-314X(83)90021-5. MR **716943 (85m:**13017) ↑5

[BM91] Edward Bierstone and Pierre D. Milman, *A simple constructive proof of canonical resolution of singularities*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 11–30. MR **1106412 (92h:**32053) ↑4

[BM97] ———, *Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant*, Invent. Math. **128** (1997), no. 2, 207–302. MR **1440306 (98e:**14010) ↑4

[BS00] Gábor Bodnár and Josef Schicho, *Automated resolution of singularities for hypersurfaces*, J. Symbolic Comput. **30** (2000), no. 4, 401–428. MR **1784750 (2001i:**14083) ↑4

[Cli90] A. Clivio, *Algorithmic aspects of* $\mathbf{Z}[x_1, \cdots, x_n]$ *with applications to tiling problems*, Z. Math. Logik Grundlag. Math. **36** (1990), no. 6, 493–515. MR **1114102 (92j:**13024) ↑5

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. MR **1628193 (99e:**11068) ↑3

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR 0133227 (24 #A3061) ↑1

[Eis04] Kirsten Eisenträger, *Hilbert's tenth problem for function fields of varieties over* $\mathbb{C}$, Int. Math. Res. Not. (2004), no. 59, 3191–3205. MR **2097039 (2005h:**11273) ↑1.4

[GTZ88] Patrizia Gianni, Barry Trager, and Gail Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symbolic Comput. **6** (1988), no. 2-3, 149–167. Computational aspects of commutative algebra. MR **988410 (90f:**68091) ↑5, 5, 5

[GM94] Giovanni Gallo and Bhubaneswar Mishra, *A solution to Kronecker's problem*, Appl. Algebra Engrg. Comm. Comput. **5** (1994), no. 6, 343–370, DOI 10.1007/BF01188747. MR **1302282 (95i:**13026) ↑5

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. MR 0463157 (57 #3116) ↑4, 4

[Her26] Grete Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), no. 1, 736–788, DOI 10.1007/BF01206635 (German). MR 1512302 ↑5

[KR92] K. H. Kim and F. W. Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, J. Algebra **150** (1992), no. 1, 35–44. MR **1174886 (93h:**03062) ↑1.4

[Mat70] Yu. Matiyasevich, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 (Russian). MR 0258744 (41 #3390) ↑1, 5

[Vas97] Wolmer V. Vasconcelos, *Flatness testing and torsionfree morphisms*, J. Pure Appl. Algebra **122** (1997), no. 3, 313–321, DOI 10.1016/S0022-4049(97)00062-5. MR **1481094 (98i:**13013) ↑1

[Vil89] Orlando Villamayor, *Constructiveness of Hironaka's resolution*, Ann. Sci. École Norm. Sup. (4) **22** (1989), no. 1, 1–32. MR **985852 (90b:**14014) ↑4

[Vil92] O. E. Villamayor U., *Patching local uniformizations*, Ann. Sci. École Norm. Sup. (4) **25** (1992), no. 6, 629–677. MR **1198092 (93m:**14012) ↑4

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

E-mail address: poonen@math.mit.edu

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