EFFECTIVE RESULTS FOR DISCRIMINANT EQUATIONS OVER FINITELY GENERATED INTEGRAL DOMAINS

JAN-HENDRIK EVERTSE AND KÁLMÁN GYŐRY

To Professor Robert Tichy on the occasion of his 60th birthday

ABSTRACT. Let A be an integral domain with quotient field K of characteristic 0 that is finitely generated as a $\mathbb{Z}$-algebra. Denote by $D(F)$ the discriminant of a polynomial $F \in A[X]$. Further, given a finite étale K-algebra Ω, denote by $D_{\Omega/K}(\alpha)$ the discriminant of α over K. For non-zero $\delta \in A$, we consider equations

$$D(F) = \delta$$

to be solved in monic polynomials $F \in A[X]$ of given degree $n \geq 2$ having their zeros in a given finite extension field G of K, and

$$D_{\Omega/K}(\alpha) = \delta \quad \text{in } \alpha \in O,$$

where O is an A-order of Ω, i.e., a subring of the integral closure of A in Ω that contains A as well as a K-basis of Ω.

In the series of papers [6]–[11], Győry proved that when K is a number field, A the ring of integers or S-integers of K, and Ω a finite field extension of K, then up to natural notions of equivalence the above equations have, without fixing G, finitely many solutions, and that moreover, if K, S, Ω, O and δ are effectively given, a full system of representatives for the equivalence classes can be effectively determined. Later, Győry [12] generalized in an ineffective way the above-mentioned finiteness results to the case when A is an integrally closed integral domain with quotient field K of characteristic 0 which is finitely generated as a $\mathbb{Z}$-algebra and G is a finite extension of K. Further, in [13] he made these results effective for a special class of integral domains A containing transcendental elements. In [5, Chap. 10] we generalized in an effective form the results of [12] mentioned above to the case where A is an arbitrary integrally closed domain of characteristic 0 which is finitely generated as a $\mathbb{Z}$-algebra, Ω is a finite étale K-algebra, and A, δ and G, repsectively Ω, O are effectively given (in a well-defined sense described below).

In the present paper, we extend these effective results further to integral domains A that are not necessarily integrally closed.

August 29, 2016.
2010 Mathematics Subject Classification: Primary 11D99; Secondary 11D41.
Keywords and Phrases: Discriminant equation, effective finiteness theorems.

1. Introduction

We define the discriminant of a monic polynomial $F = X^n + a_1X^{n-1} + \cdots + a_n = (X - \alpha_1)\cdots(X - \alpha_n)$ of degree $n \geq 2$ by

$$D(F) := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Recall that $D(F) \in \mathbb{Z}[a_1, \ldots, a_n]$; in fact, it is a polynomial of total degree $2n-2$ in $a_1, \ldots, a_n$.

In this paper we consider discriminant equations over integral domains of characteristic 0 that are finitely generated as a $\mathbb{Z}$-algebra. Let A be such a domain, with quotient field K, let n be an integer with $n \geq 2$, let δ be a non-zero element of A, and let G be a finite extension of K. We consider the equation

$$D(F) = \delta \quad \text{in monic polynomials } F \in A[X] \text{ of degree } n \text{ having all their zeros in } G. \tag{1.1}$$

Two monic polynomials $F_1, F_2 \in A[X]$ are called *A-equivalent* if there is $a \in A$ such that $F_2(X) = F_1(X + a)$. Clearly, A-equivalent polynomials have the same discriminant, and so the solutions of equation (1.1) can be divided into A-equivalence classes. We proved [5, Thm. 10.1.1] the following result:

Theorem A. *Assume in addition to the above that A is integrally closed. Then the solutions of equation* (1.1) *lie in finitely many A-equivalence classes. If moreover A, δ and G are effectively given (in a sense defined in the next section), then a full system of representatives of these A-equivalence classes can be determined effectively.*

The ineffective finiteness statement of this is a consequence of [12, Thm. 4]. The effective part is a culmination of Győry's earlier results, mentioned in the abstract.

In the present paper we prove a generalization of Theorem A, where instead of integrally closed domains we consider integral domains A such that

$$\left(\tfrac{1}{n}A^+ \cap A_K^+\right)/A^+ \text{ is finite}, \tag{1.2}$$

where again n is an integer with $n \geq 2$; see Theorem 2.1 below. Here B^+ denotes the additive group of a ring B, and A_K denotes the integral closure of A in K. The class of domains with (1.2) contains all integrally closed domains, the integral domains that contain n^{-1}, and also all finitely generated subrings of $\overline{\mathbb{Q}}$. We do not know if condition (1.2) is the weakest possible. We will give an example of an integral domain A and a field extension G for which the finiteness part of Theorem A is false. So some condition will have to be imposed on the domain A.

As suggested by one of the anonymous referees, there are various variations on equation (1.1) that are worth being considered. First of all, instead of (1.1) one

could consider the equation

$$D(F) \in \delta A^* \text{ in monic polynomials } F \in A[X] \text{ of degree } n$$

where A^* denotes the unit group of A and $\delta A^* := \{\delta u : u \in A^*\}$. Secondly, in equation (1.1) one could consider polynomials F that do not have their zeros in a prescribed finite extension G of K. For both variations one can, in certain special cases, prove certain sensible effective finiteness results, see Győry [10], [11]. But it may be hard to obtain such results in full generality. We will return to this at the end of the next section.

We also consider discriminant equations where the unknowns are elements of orders of finite étale K-algebras. Let for the moment K be any field of characteristic 0 and Ω a *finite étale K-algebra,* i.e., $\Omega = K[X]/(P) = K[\theta]$, where $P \in K[X]$ is some separable polynomial and $\theta := X \bmod P$. We write $[\Omega : K] := \dim_K \Omega$; then clearly $[\Omega : K] = \deg P$. Let $\overline{K}$ be an algebraic closure of K. By a *K-homomorphism* of Ω to $\overline{K}$ we mean a non-trivial K-algebra homomorphism. There are precisely $n := [\Omega : K]$ K-homomorphisms of Ω to $\overline{K}$, which map θ to the n distinct zeros of P in $\overline{K}$. We denote these by $x \mapsto x^{(i)}$ $(i = 1, \ldots, n)$. The *discriminant* of $\alpha \in \Omega$ over K is given by

$$D_{\Omega/K}(\alpha) := \prod_{1 \le i < j \le n} (\alpha^{(i)} - \alpha^{(j)})^2,$$

where $\alpha^{(i)}$ denotes the image of α under $x \mapsto x^{(i)}$. This is an element of K. It is not difficult to show that $D_{\Omega/K}(\alpha + a) = D_{\Omega/K}(\alpha)$ for $\alpha \in \Omega$, $a \in K$. Further, $D_{\Omega/K}(\alpha) \neq 0$ if and only if $\Omega = K[\alpha]$. For more details on finite étale K-algebras, we refer to [5, Chap. 1].

Now let as above A be an integral domain with quotient field K of characteristic 0 that is finitely generated over $\mathbb{Z}$. We denote by A_Ω the integral closure of A in Ω. An *A-order* is a subring of A_Ω that contains A as well as a K-basis of Ω. In particular A_Ω itself is an A-order of Ω. We consider equations of the type

$$D_{\Omega/K}(\alpha) = \delta \text{ in } \alpha \in O \tag{1.3}$$

where δ is a non-zero element of A, and O is an A-order of Ω. We call $\alpha_1, \alpha_2 \in O$ *A-equivalent* if $\alpha_1 - \alpha_2 \in A$. Then the solutions of (1.3) can be divided into A-equivalence classes. We recall Theorem 10.1.3 of [5]:

Theorem B. *Assume in addition to the above that A is integrally closed. Then the solutions of equation* (1.3) *lie in finitely many A-equivalence classes. If moreover A, δ and Ω are effectively given as defined in the next section then a full system of representatives for these A-equivalence classes can be determined effectively.*

The ineffective part of this theorem is a consequence of[12, Thm. 5]. The effective part was proved in [7]–[13] in the special cases mentioned in the abstract, in more precise, explicit forms.

In this paper we extend Theorem B to integral domains A such that

$$(O \cap K)^+/A^+ \text{ is finite,} \tag{1.4}$$

see Theorem 2.2 below. Notice that $O \cap K = A$ if A is integrally closed. It is shown that the finiteness result becomes false if we weaken condition (1.4).

In Section 2 we give the precise statements of our results. Section 3 contains some tools from effective commutative algebra. Much of them have been taken from [5, §10.7]. In Section 4 we recall from [5, Chap. 10] a central proposition, which is the basis of the proofs of the results in the present paper. The main tool in the proof of that proposition is Corollary 1.2 of [4] on unit equations over finitely generated integral domains. In the remaining sections we deduce our theorems.

Acknowledgement. We would like to thank the two anonymous referees for their careful scrutiny of our paper and their valuable comments and corrections.

2. Statements of the results

We start with the necessary definitions. Let A be an integral domain of characteristic 0 which is finitely generated over $\mathbb{Z}$ (i.e., finitely generated as a $\mathbb{Z}$-algebra). Let K be its quotient field. Suppose $A = \mathbb{Z}[x_1, \ldots, x_r]$ and define the ideal

$$I := \{f \in \mathbb{Z}[X_1, \ldots, X_r] : f(x_1, \ldots, x_r) = 0\}.$$

Thus, A is isomorphic to $\mathbb{Z}[X_1, \ldots, X_r]/I$ and x_i corresponds to the residue class of X_i mod I. Following [5, §10.7], we say that A is *given effectively* if a finite set of generators for the ideal I is given. We call such a set of generators for I an *ideal representation* for A. For A to be an integral domain of characteristic 0 it is necessary and sufficient that I be a prime ideal of $\mathbb{Z}[X_1, \ldots, X_r]$ with $1 \notin \mathbb{Q}I$. This can be checked for instance by means of [1, Proposition 4.10] and [20, §4]. By a representation for an element y of A we mean an polynomial $f \in \mathbb{Z}[X_1, \ldots, X_r]$ such that $y = f(x_1, \ldots, x_r)$ and we say that y is *effectively given/computable* if such f is given/can be computed. We can check whether two polynomials $f, g \in \mathbb{Z}[X_1, \ldots, X_r]$ represent the same element of A by checking whether their difference $f - g$ is in I, using an ideal membership algorithm for I (see e.g., [1]). By a representation for $y \in K$ we mean a pair (f, g) with $f, g \in \mathbb{Z}[X_1, \ldots, X_r]$ and $g \notin I$ such that $y = f(x_1, \ldots, x_r)/g(x_1, \ldots, x_r)$. By saying that a polynomial with coefficients in A or K is given/can be determined effectively we mean that its coefficients are given/can be determined effectively. We say that a finite extension G of K is effectively given, if it is given in the form $K[X]/(P)$, where P is an effectively given monic, irreducible polynomial in $K[X]$. We should mention here that for a given polynomial $P \in K[X]$ it can be decided effectively whether it is irreducible, see for instance [20, §§33-35].

In what follows, A is an integral domain finitely generated over $\mathbb{Z}$, K its quotient field and G a finite extension of K. Further, δ is a non-zero element of A

and n an integer with $n \geq 2$. Consider the equation

$$D(F) = \delta \quad \text{in monic polynomials } F \in A[X] \text{ of degree } n \text{ having all their zeros in } G. \tag{1.1}$$

Our first result is as follows.

Theorem 2.1. *Let n be an integer ≥ 2 and A an integral domain finitely generated over $\mathbb{Z}$ with quotient field K such that*

$$\left(\tfrac{1}{n}A^+ \cap A_K^+\right)/A^+ \text{ is finite.} \tag{1.2}$$

Further, let G be a finite extension of K and δ a non-zero element of A.

Then the set of monic polynomials $F \in A[X]$ with (1.1) is a union of finitely many A-equivalence classes. Moreover, for any effectively given n, A, G, δ as above, a full system of representatives for these equivalence classes can be determined effectively.

By Corollary 3.9 in Section 3 below, for any effectively given integral domain A finitely generated over $\mathbb{Z}$ it can be decided effectively whether it satisfies (1.2). As said in the introduction, we do not know whether condition (1.2) can be relaxed. Below, we show that Theorem 2.1 is not true for arbitrary finitely generated domains of characteristic 0.

We now turn to elements of orders in finite étale algebras. We start again with some definitions. Let again A be an integral domain finitely generated over $\mathbb{Z}$ and K its quotient field. We say that a finite étale K-algebra Ω is given effectively, if it is given in the form $K[X]/(P)$, where $P \in K[X]$ is an effectively given monic polynomial without multiple zeros. Elements of Ω can be expressed uniquely as $\sum_{i=0}^{n-1} a_i\theta^i$ with $a_0, \ldots, a_{n-1} \in K$, where $\theta := X \bmod P$. We say that an element of Ω is given/can be determined effectively effectively if $a_0, \ldots, a_{n-1}$ are given/can be determined effectively.

Recall that an A-order of Ω is an A-subalgebra of the integral closure of A in Ω, which spans Ω as a K-vector space. By a result of Nagata [18], the integral closure of A in Ω is finitely generated as an A-module. Since the integral domain A is Noetherian, any A-order of Ω is finitely generated as an A-module as well. We say that an A-order O of Ω is given effectively if a finite set of A-module generators $\{\omega_1 = 1, \omega_2, \ldots, \omega_m\}$ of O is given effectively. We say that an element α of O is given/can be determined effectively, if $a_1, \ldots, a_m \in A$ are given/can be determined effectively such that $\alpha = \sum_{i=1}^{m} a_i\omega_i$. Using Corollary 3.10 (i) below one can verify that $\omega_1, \ldots, \omega_m$ do indeed generate an A-order of Ω.

Let Ω be a finite étale K-algebra with $[\Omega : K] =: n \geq 2$, let O be an A-order in Ω, and let δ be a non-zero element of A. We consider the equation

$$D_{\Omega/K}(\alpha) = \delta \text{ in } \alpha \in O. \tag{1.3}$$

We prove the following result.

Theorem 2.2. *Let A be an integral domain finitely generated over $\mathbb{Z}$ with quotient field K, Ω a finite étale K-algebra, O an A-order in Ω, and $\delta \in A$, $\delta \neq 0$. Assume that*

$$(O \cap K)^+/A^+ \text{ is finite.} \tag{1.4}$$

Then the set of $\alpha \in O$ with (1.3) is a union of finitely many A-equivalence classes. Further, for any effectively given A, Ω, O, δ as above, a full system of representatives for these classes can be determined effectively.

Using Corollary 3.10 (ii) below, for given A, Ω, O it can be decided effectively whether condition (1.4) is satisfied. At the end of the present section we show that Theorem 2.2 becomes false if we relax condition (1.4).

We now show that Theorem 2.1 cannot be true for arbitrary finitely generated domains A. More precisely, we show that for every integer $n \geq 2$, there are an integral domain A finitely generated over $\mathbb{Z}$, a finite extension G of the quotient field of A, and a $\delta \in A \setminus \{0\}$, such that there are infinitely many A-equivalence classes of monic polynomials $F \in A[X]$ of degree n with $D(F) = \delta$ having all their roots in G.

Let n be an integer ≥ 2, let t be transcendental over $\mathbb{Q}$ and define the integral domain

$$A := \mathbb{Z}\left[nt, \tbinom{n}{2}t^2, \tbinom{n}{3}t^3, \ldots, t^n\right].$$

Notice that A is a subring of $\mathbb{Z}[t]$ and that A has quotient field $K := \mathbb{Q}(t)$. We can express elements of A as $\sum_{k=0}^{m} s_k t^k \in A$ with $s_k \in \mathbb{Z}$ for all k. We show that s_k is divisible by n if k is coprime with n. Indeed, assume that $\gcd(k, n) = 1$. Notice that s_k is a $\mathbb{Z}$-linear combination of terms

$$\prod_{j=1}^{n} \tbinom{n}{j}^{l_j} \quad \text{with } l_1, \ldots, l_n \in \mathbb{Z}_{\geq 0},\ \ l_1 + 2l_2 + \cdots + nl_n = k. \tag{2.1}$$

Let p^r be a prime power occurring in the prime factorization of n. For each term in (2.1), there is $j \in \{1, \ldots, n-1\}$ such that j is coprime with p and $l_j > 0$, since k is not divisible by p. From well-known divisibility properties of binomial coefficients, it follows that $\binom{n}{j}$ is divisible by p^r. Hence all terms in (2.1) are divisible by p^r. Consequently, s_k is divisible by each of the prime powers p^r in the factorization of n, hence it is divisible by n.

Now fix a non-zero $c \in A$, let δ be the discriminant of $X^n - c$, and let G be the splitting field of $X^n - c$ over K. Consider the polynomials

$$F_m := (X + t^{mn+1})^n - c = \sum_{j=0}^{n} \tbinom{n}{j} t^j \cdot (t^n)^{mj} X^{n-j} - c$$

where m runs through the positive integers. Clearly, for every m we have $F_m \in A[X]$, F_m has splitting field G over K, and $D(F_m) = \delta$. We show that the polynomials F_m lie in distinct A-equivalence classes; it then follows that (1.1)

has infinitely many A-equivalence classes of solutions. Let m, m' be two distinct positive integers. Suppose that $F_m, F_{m'}$ are A-equivalent; then there is $a \in A$ such that $F_{m'}(X) = F_m(X+a)$. It follows that there is an n-th root of unity ρ such that $X + t^{m'n+1} = \rho(X + t^{mn+1} + a)$. Consequently, $\rho = 1$ and $t^{m'n+1} - t^{mn+1} \in A$. But this is impossible, since the exponents of both terms are coprime with n, while the coefficients are not divisible by n.

We next show that if, with the notation of Theorem 2.2, the integral domain A and the A-order O of Ω do not satisfy (1.4), then there is a non-zero $\delta \in A$ such that (1.3) has infinitely many A-equivalence classes of solutions. Indeed, suppose (1.4) does not hold. Then there is an infinite sequence $b_1, b_2, \ldots$ of elements of $O \cap K$ such that none of the differences $b_i - b_j$ $(i > j \geq 1)$ belongs to A. Pick $\alpha \in O$ such that $\Omega = K[\alpha]$ and put $\delta := D_{\Omega/K}(\alpha)$. Then $D_{\Omega/K}(\alpha + b_i) = \delta$ and $\alpha + b_i \in O$ for $i = 1, 2, \ldots$, and the elements $\alpha + b_i$ $(i = 1, 2, \ldots)$ lie in different A-equivalence classes.

We finish this section with some remarks on certain variations on equation (1.1), following a suggestion of one of the referees.

Remark 2.3. Let A, K, n, δ, G be as in Theorem 2.1. Instead of (1.1) we consider the equation

$$D(F) \in \delta A^* \quad \text{in monic polynomials } F \in A[X] \text{ of degree } n \text{ having all their zeros in } G, \tag{2.2}$$

where A^* denotes the unit group of A and $\delta A^* := \{\delta u : u \in A^*\}$. We can partition the solutions of (2.2) into so-called *weak A-equivalence classes*, where two monic polynomials $F_1, F_2 \in A[X]$ of degree n are called weakly A-equivalent if $F_2(X) = u^{-n}F_1(uX + a)$ for some $u \in A^*$, $a \in A$.

By a theorem of Roquette [19], any integral domain that is finitely generated over $\mathbb{Z}$ has a finitely generated unit group. Hence for every positive integer m there is a finite subset $\mathcal{W}_m$ of A^* such that every element of A^* can be expressed as wv^m with $w \in \mathcal{W}_m$ and $v \in A^*$. Let $F \in A[X]$ be a solution of (2.2). Thus, $D(F) = \delta u$ with $v \in A^*$. Write $u = wv^{n(n-1)}$, with $w \in \mathcal{W}_{n(n-1)}$ and $v \in A^*$. Then the polynomial $F_v(X) := v^{-n}F(vX)$ has discriminant $D(F_v) = \delta w$. By Theorem 2.1 and the finiteness of $\mathcal{W}_{n(n-1)}$, the polynomials F_v lie in only finitely many A-equivalence classes, hence the polynomials F with (2.2) lie in only finitely many weak A-equivalence classes. In case of integrally closed domains A, this was proved in [12].

In certain special cases, for instance when A is the ring of S-integers of a number field K for some finite set of places S of K, we can effectively compute sets $\mathcal{W}_m$ as above, but we do not know of an algorithm that computes such sets $\mathcal{W}_m$ for *arbitrary* effectively given integral domains A that are finitely generated over $\mathbb{Z}$. So at least with the above argument, we cannot in general effectively

determine a full system of representatives for the weak A-equivalence classes of polynomials F with (2.2).

Remark 2.4. Let again A, K, n, δ, G be as in Theorem 2.1. We consider again equation (1.1) but for polynomials not necessarily having their zeros in a prescribed extension G of K, i.e., we consider

$$D(F) = \delta \quad \text{in monic polynomials } F \in A[X] \text{ of degree } n. \tag{2.3}$$

Let A be the ring of S-integers of an algebraic number field K, where S is a finite set of places of K. If F is a polynomial satisfying (2.3), then the discriminant of its splitting field G over K is composed of prime ideals from S and those occurring in the prime ideal factorization of δ. By a consequence of the Hermite-Minkowski Theorem, there are only finitely many possibilities for G, and these can be determined effectively. Together with Theorem 2.1, or with the results of Győry from [10], [11] or [13], this implies that the polynomials F with (2.3) lie in only finitely many A-equivalence classes, a full system of representatives of which can be determined effectively. Perhaps this effective results can be extended to certain finitely generated integral domains of low transcendence degree. But extending this to arbitrary domains that are finitely generated over $\mathbb{Z}$ seems to be very hard and beyond the scope of this paper.

3. Tools from effective commutative algebra

For the definitions of a domain, étale algebra, order, etc. and elements of those being effectively given/computable we refer to Section 2. We start with some effective results on systems of linear equations in polynomials.

Proposition 3.1. *Let $\mathbf{k} = \mathbb{Q}$ or $\mathbb{F}_p$ for some prime p. Then for any given positive integer r and any given polynomials $f_1, \dots, f_s \in \mathbf{k}[X_1, \dots, X_r]$ we can:*
(i) determine effectively whether a given polynomial g from $\mathbf{k}[X_1, \dots, X_r]$ belongs to the ideal $I = (f_1, \dots, f_s)$ and if so, determine effectively polynomials $g_1, \dots, g_s$ such that $g = g_1 f_1 + \cdots + g_s f_s$ (ideal membership problem);
(ii) determine effectively whether I is a prime ideal.

Proof. See Seidenberg [20]: §4, p. 277 for (i) and §46, p. 293 for (ii) (in fact Seidenberg gives a method to determine the prime ideals associated to a given ideal I, which certainly enables one to decide whether I is a prime ideal). The main ideas in the proofs of these results originate from Hermann [14] but her arguments contain gaps. □

For a polynomial f with integer coefficients, we denote by $H(f)$ its height (maximum of the absolute values of its coefficients) and by $\mathrm{Deg}\, f$ its total degree. Further, we define the polynomial ring $R := \mathbb{Z}[X_1, \dots, X_r]$.

Proposition 3.2. *Let M be an $m \times n$-matrix with entries from R, and $\mathbf{b}$ a vector from R^m, such that the entries of M and $\mathbf{b}$ have total degrees at most d and heights at most H.*

(i) The R-module

$$\{\mathbf{x} \in R^n : M\mathbf{x} = \mathbf{0}\}$$

is generated by vectors, of which the coordinates are polynomials, whose total degrees are bounded above by an effectively computable number C_1 depending only on m, n, d, r and whose heights are bounded above by an effectively computable number C_2 depending only on m, n, d, r and H.

(ii) Suppose that the system

$$M\mathbf{x} = \mathbf{b}$$

is solvable in $\mathbf{x} \in R^n$. Then this system has a solution $\mathbf{x}_0 \in R^n$ whose coordinates have total degrees bounded above by C_3 and heights bounded above by C_4, where both C_3, C_4 are effectively computable numbers depending only on m, n, d, r and H.

Proof. Aschenbrenner [1] proved the above with $C_1 = (2md)^{2^{c_1 r \log 2r}}$, $C_2 = \exp\left((2m(d+1))^{2^{c_2(1+r\log 2r)}}(1+\log H)\right)$ (cf. his Proposition 5.2) and $C_3 = (2md)^{2^{c_3 r \log 2r}}(1+\log H)$ (cf. his Theorem 6.5), where c_1, c_2, c_3 are effectively computable absolute constants. In (ii), thanks to our upper bound for the total degrees, the problem to find a solution to $M\mathbf{x} = \mathbf{b}$ reduces to solving a finite system of inhomogeneous linear equations over $\mathbb{Z}$, and then we obtain a value for C_4 for instance by invoking for instance a result from [2]. □

Corollary 3.3 (Ideal membership over $\mathbb{Z}$)**.** *Let $I = (f_1, \dots, f_s)$ be an ideal in R and $g \in R$. Suppose that $f_1, \dots, f_s$ and g have total degrees at most d and heights at most H. If $g \in I$, there exist $g_1, \dots, g_s \in R$ of total degrees and heights bounded above by effectively computable numbers depending only on r, d, s and H, such that $g = \sum_{i=1}^{s} g_i f_i$.*

Proof. Apply part (ii) of Proposition 3.2 with $m = 1$, $n = s$. □

In what follows, A is an integral domain with quotient field K of characteristic 0 that is finitely generated over $\mathbb{Z}$. We assume that A is effectively given, i.e., we have $A = \mathbb{Z}[x_1, \dots, x_r]$, and we are given a finite set of generators $f_1, \dots, f_s$ of the ideal

$$I = \{f \in \mathbb{Z}[X_1, \dots, X_r] : f(x_1, \dots, x_r) = 0\}.$$

Corollary 3.4. *Given an $m \times n$-matrix M with entries in K and $\mathbf{b} \in K^m$ one can:*

(i) effectively determine a finite set of A-module generators $\mathbf{a}_1, \dots, \mathbf{a}_t$ for the A-module of $\mathbf{x} \in A^n$ with $M\mathbf{x} = \mathbf{0}$;

(ii) decide effectively whether $M\mathbf{x} = \mathbf{b}$ has a solution $\mathbf{x} \in A^n$ and if so, find a solution.

Proof. (i) After clearing denominators, one may assume that the entries of M and the coordinates of $\mathbf{b}$ lie in A. Let $m_{ij} \in R$ $(i = 1, \ldots, m,\ j = 1, \ldots, n$ be representatives for the elements of M. Writing $y_1, \ldots, y_n$ for representatives in R for the coordinates of $\mathbf{x}$ we can rewrite the system $M\mathbf{x} = \mathbf{0}$ as

$$m_{i1}y_1 + \cdots + m_{in}y_n \in I \quad (i = 1, \ldots, m)$$

or as

$$m_{i1}y_1 + \cdots + m_{in}y_n = f_1 y_{i1} + \cdots + f_s y_{is} \quad (i = 1, \ldots, m)$$

in $y_i, y_{ij} \in R$, which is a system of equations as in part (i) of Proposition 3.2. Likewise $M\mathbf{x} = \mathbf{b}$ can be rewritten as a system of equations as in part (ii) of Proposition 3.2. Now one simply has to apply Proposition 3.2 to these systems. □

We say that a finitely generated A-module $\mathcal{M} \subset K$ is effectively given if a finite set of A-module generators for $\mathcal{M}$ is effectively given. We denote the A-module generated by $a_1, \ldots, a_u$ by $(a_1, \ldots, a_u)$.

Corollary 3.5. *For any two effectively given A-submodules $\mathcal{M}_1$, $\mathcal{M}_2$ of K, one can*

(i) effectively decide whether $\mathcal{M}_1 \subseteq \mathcal{M}_2$;

(ii) effectively compute a finite set of A-module generators for $\mathcal{M}_1 \cap \mathcal{M}_2$.

Proof. Let $\mathcal{M}_1 = (a_1, \ldots, a_u)$, $\mathcal{M}_2 = (b_1, \ldots, b_v)$ with the $a_i, b_j \in K$ effectively given. Then (i) comes down to checking whether $a_1, \ldots, a_u \in \mathcal{M}_2$, which is a special case of part (ii) of Corollary 3.4. To determine a finite set of A-module generators for $\mathcal{M}_1 \cap \mathcal{M}_2$, one first determines a finite set of A-module generators for the solution set of $(x_1, \ldots, x_u, y_1, \ldots, y_v) \in A^{u+v}$ of $\sum_{i=1}^{u} x_i a_i = \sum_{j=1}^{v} y_j b_j$ and then for each generator one takes the coordinates $x_1, \ldots, x_u$. □

Probably the following results is well-known but we could not find a proof for it.

Proposition 3.6. *Assume that A is effectively given and let $\mathcal{M}_1, \mathcal{M}_2$ be two effectively given finitely generated A-submodules of K with $\mathcal{M}_1 \subset \mathcal{M}_2$. Then it can be decided effectively whether $\mathcal{M}_2/\mathcal{M}_1$ is finite. If this is the case, a full system of representatives for $\mathcal{M}_2/\mathcal{M}_1$ can be determined effectively.*

We use the following simple lemma.

Lemma 3.7. *Suppose we are given a sequence $\mathcal{N}_1 \subseteq \cdots \subseteq \mathcal{N}_r$ of finitely generated A-modules contained in K. Then $\mathcal{N}_r/\mathcal{N}_1$ is finite if and only if for $i = 1, \ldots, r-1$, the quotient $\mathcal{N}_{i+1}/\mathcal{N}_i$ is finite. Further, if this is the case, we obtain a full system*

of representatives for $\mathcal{N}_r/\mathcal{N}_1$ by taking all sums $a_1 + \cdots + a_{r-1}$ where a_i runs through a full system of representatives for $\mathcal{N}_{i+1}/\mathcal{N}_i$ for $i = 1, \ldots, r-1$.

Proof. Obvious. □

Proof of Proposition 3.6. We may assume that A is given in the form

$$\mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_s),$$

with given polynomials $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_r]$, and that x_i is the residue class of X_i modulo $(f_1, \ldots, f_s)$, for $i = 1, \ldots, r$. Then the elements of K may be represented as quotients $g(x_1, \ldots, x_r)/h(x_1, \ldots, x_r)$, where $g, h \in \mathbb{Z}[X_1, \ldots, X_r]$ and $h \notin (f_1, \ldots, f_s)$. After multiplying the given generators of $\mathcal{M}_1$ and $\mathcal{M}_2$ with the product of their denominators, we may assume that $\mathcal{M}_1, \mathcal{M}_2 \subseteq A$. There is clearly no loss of generality to assume that $\mathcal{M}_1, \mathcal{M}_2$ are given as $\mathcal{M}_1 = (a_1, \ldots, a_u)$, $\mathcal{M}_2 = (a_1, \ldots, a_v)$ with $v > u$. In fact, it suffices to prove our Theorem in the special case $v = u + 1$. Then the general case with arbitrary v can be deduced from Lemma 3.7.

So we assume henceforth that $v = u + 1$. Let

$$J := \{x \in A : x \cdot a_{u+1} \in \mathcal{M}_1\} = A \cap a_{u+1}^{-1}\mathcal{M}_1;$$

then $\mathcal{M}_2/\mathcal{M}_1$ is isomorphic to the additive group of A/J. By Corollary 3.5 we can compute a finite set of generators for J, which we may represent as residue classes modulo $(f_1, \ldots, f_s)$ of polynomials $f_{s+1}, \ldots, f_t$ from $\mathbb{Z}[X_1, \ldots, X_r]$. Then

$$\mathcal{M}_2/\mathcal{M}_1 \cong \mathbb{Z}[X_1, \ldots, X_r]/I,$$

where $I = (f_1, \ldots, f_s, \ldots, f_t)$. So it suffices to prove that it can be decided effectively whether $\mathbb{Z}[X_1, \ldots, X_r]/I$ is finite and that in this case a full system of representatives can be computed effectively.

A necessary condition for $\mathbb{Z}[X_1, \ldots, X_r]/I$ to be finite is that $I \cap \mathbb{Z} \neq (0)$. This in turn is equivalent to the existence of $g_1, \ldots, g_t \in \mathbb{Q}[X_1, \ldots, X_r]$ such that $g_1 f_1 + \cdots + g_t f_t = 1$. By Proposition 3.1 it can be decided effectively whether such $g_1, \ldots, g_t$ exist and if so, they can be computed. Supposing such $g_1, \ldots, g_t$ exist, by clearing the denominators of their coefficients we find non-zero $b \in \mathbb{Z}$ in $I \cap \mathbb{Z}$. Using Corollary 3.3 we can check, for every divisor $a \in \mathbb{Z}$ of b whether $a \in I$. In this manner we eventually find a with $I \cap \mathbb{Z} = (a)$.

If $a = 1$ then $I = \mathbb{Z}[X_1, \ldots, X_r]$ and we are done. Suppose that $a \neq 1$. We make a reduction to the case that $a = p$ is a prime number. Suppose that $a = p_1 \cdots p_k$ where $p_1, \ldots, p_k$ are not necessarily distinct prime numbers. We may write $I = (p_1 \cdots p_k, f_1, \ldots, f_t)$. For $i = 1, \ldots, k$, put $I_i := (p_1 \cdots p_i, f_1, \ldots, f_t)$ and for $i \in \{1, \ldots, k-1\}$ define

$$J_i := \{f \in \mathbb{Z}[X_1, \ldots, X_r] : p_1 \cdots p_i f \in I_{i+1}\}.$$

Then I_i/I_{i+1} is isomorphic to the additive group of $\mathbb{Z}[X_1,\dots,X_r]/J_i$. Now if we are able to decide, for $i=1,\dots,k-1$, whether $\mathbb{Z}[X_1,\dots,X_r]/J_i$ is finite and find a full system of representatives for this quotient, we can do the same for I_i/I_{i+1} and then, thanks to Lemma 3.7, for $\mathbb{Z}[X_1,\dots,X_r]/I$.

Using Proposition 3.2 we find a set of generators for J_i. By what has been explained above, from this we can compute $b_i \in \mathbb{Z}$ with $J_i \cap \mathbb{Z} = (b_i)$. Clearly, $p_{i+1} \in J_i$; hence $J_i \cap \mathbb{Z} = (1)$ or (p_{i+1}). The case $J_i = (1)$ being obvious, it remains to check whether $\mathbb{Z}[X_1,\dots,X_r]/J_i$ is finite if $J_i \cap \mathbb{Z} = (p_{i+1})$.

Changing notation, we see that it suffices to show, for any given ideal I of $\mathbb{Z}[X_1,\dots,X_r]$ with $I \cap \mathbb{Z} = (p)$ for some prime p, whether $\mathbb{Z}[X_1,\dots,X_r]/I$ is finite and if so, to compute a full system of representatives for $\mathbb{Z}[X_1,\dots,X_r]$ modulo I. We may assume that I is given in the form $I = (p, f_1,\dots,f_t)$, with $f_1,\dots,f_t \in \mathbb{Z}[X_1,\dots,X_r]$. Given $f \in \mathbb{Z}[X_1,\dots,X_r]$, denote by $\overline{f}$ its reduction modulo p, and put $\overline{I} = (\overline{f}_1,\dots,\overline{f}_t)$. Then $\mathbb{Z}[X_1,\dots,X_r]/I \cong \mathbb{F}_p[X_1,\dots,X_r]/\overline{I}$. So we have to decide whether this latter residue class ring is finite and if so, to compute a full system of representatives for the residue classes.

For any positive integer m, denote by V_m the set of residue classes modulo $\overline{I}$ of all polynomials of degree $\le m$ in $\mathbb{F}_p[X_1,\dots,X_r]$. This is a finite dimensional $\mathbb{F}_p$-vector space. Recall that the *Hilbert function* $H_{\overline{I}}$ of $\overline{I}$ is defined by $H_{\overline{I}}(m) := \dim_{\mathbb{F}_p} V_m$. It is known that there are an integer $m_{\overline{I}}$, and a polynomial $p_{\overline{I}} \in \mathbb{Q}[X]$, called the *Hilbert polynomial* of $\overline{I}$, such that $H_{\overline{I}}(m) = p_{\overline{I}}(m)$ for $m \ge m_{\overline{I}}$. Now $\mathbb{F}_p[X_1,\dots,X_r]/\overline{I}$ is finite if and only if $p_{\overline{I}}$ is constant, and this being the case, every residue class of $\mathbb{F}_p[X_1,\dots,X_r]$ modulo $\overline{I}$ is represented by a polynomial of degree at most $m_{\overline{I}}$. There is a general procedure, based on Gröbner basis theory, to compute $m_{\overline{I}}$ and $p_{\overline{I}}$, given a set of generators for $\overline{I}$, see [3, §§15.1.1, 15.10.2]. With this procedure one can decide whether $\mathbb{F}_p[X_1,\dots,X_r]/\overline{I}$ is finite. Subsequently, using Proposition 3.1, one can select a full system of representatives modulo $\overline{I}$ from the polynomials of degree $\le m_{\overline{I}}$.

This completes the proof of Proposition 3.6. □

For a finite extension G of K, we denote by A_G the integral closure of A in G. In particular, A_K is the integral closure of A in its quotient field K.

Proposition 3.8. *Assume that A and a finite extension G of K are effectively given. Then one can effectively compute a finite set of A-module generators for A_G. Moreover, one can compute an ideal representation for A_G.*

Proof. Computing a finite set of A-module generators for A_G follows from results of Nagata [18], de Jong [15], Matsumura [17] and Matsumoto [16]. For more details, see [5, Cor. 10.7.18]. Then an ideal representation for A_G can be computed using [5, Thms. 10.7.13, 10.7.16]. □

Corollary 3.9. *Assume that A is effectively given. Then one can can effectively decide whether $(\frac{1}{n}A^+ \cap A_K^+)/A^+$ is finite and if so, compute a full system of representatives for $(\frac{1}{n}A^+ \cap A_K^+)/A^+$.*

Proof. Immediate consequence of Proposition 3.8, Corollary 3.5, (ii) and Proposition 3.6. □

Corollary 3.10. *Assume that A and a finite étale K-algebra Ω are effectively given. Further, let $\omega_2, \dots, \omega_u \in \Omega$ be effectively given and let O be the A-module generated by $1, \omega_2, \dots, \omega_u$.*

(i) It can be effectively decided whether O is an A-order of Ω.

(ii) If O is an A-order of Ω, one can effectively decide whether $(O \cap K)^+/A^+$ is finite, and if so, compute a full system of representatives for $(O \cap K)^+/A^+$.

Proof. We assume that $\Omega = K[X]/(P)$ where $P \in K[X]$ is an effectively given, separable monic polynomial. Let $n := [\Omega : K] = \deg P$ and $\theta := X \bmod P$. Then $\{1, \theta, \dots, \theta^{n-1}\}$ is a K-basis of Ω. Further, we assume that $\omega_2, \dots, \omega_u$ are effectively given as K-linear combinations of $1, \theta, \dots, \theta^{n-1}$. Then we may express elements of O as $\sum_{k=0}^{n-1} l_k(\mathbf{x})\theta^k$ with $\mathbf{x} \in A^u$, where $l_0, \dots, l_{n-1}$ are linear forms from $K[X_1, \dots, X_u]$.

(i) We first verify that the linear forms $l_0, \dots, l_{n-1}$ have rank n over K, to make sure that O contains a K-basis of Ω. The next thing to verify is whether $\omega_i\omega_j$ is an A-linear combination of $1, \omega_2, \dots, \omega_u$ for $i, j = 2, \dots, u$. Compute $b_{ij} \in K$ such that $\omega_i\omega_j = \sum_{k=0}^{n-1} b_{ijk}\theta^k$. Then we have to verify whether the system $l_k(\mathbf{x}) = b_{ijk}$ $(k = 0, \dots, n-1)$ is solvable in $\mathbf{x} \in A^u$, for $i, j = 2, \dots, u$, and this can be done by means of Corollary 3.4 (ii). Lastly, it is a standard fact from algebra, that if A is a subring of a commutative ring B that is finitely generated as an A-module, then B is in fact integral over A. So in particular, if we have verified that O is closed under multiplication then it is automatically contained in A_Ω.

(ii) Using Corollary 3.4 (i) we can compute a finite set of A-module generators, say $\mathbf{x}_1, \dots, \mathbf{x}_v$ for the A-module of $\mathbf{x} \in A^u$ with $l_i(\mathbf{x}) = 0$ for $i = 1, \dots, n-1$. Then $(O \cap K)^+$ is generated as an A-module by $l_0(\mathbf{x}_1), \dots, l_0(\mathbf{x}_v)$. With these generators for $(O \cap K)^+$ and Proposition 3.6, we can check whether $(O \cap K)^+/A^+$ is finite, and if so, compute a full system of representatives. □

4. The main proposition

We recall from [5] a central proposition from which Theorems 2.1 and 2.2 are deduced. We keep the notation from Section 2.

Proposition 4.1. *For any integral domain A of characteristic 0 that is finitely generated over $\mathbb{Z}$, any finite extension G of the quotient field of A, any non-zero $\delta \in A$, and any integer $n \geq 2$, all effectively given, one can determine effectively*

a finite subset $\mathscr{F} = \mathscr{F}_{A,G,n,\delta}$ of G with the following property: if F is any monic polynomial from $A[X]$ of degree n and discriminant δ having all its zeros, say $\alpha_1, \ldots, \alpha_n$, in G, then

$$\alpha_i - \alpha_j \in \mathscr{F} \text{ for } i, j \in \{1, \ldots, n\}, i \neq j. \tag{4.1}$$

Proof. This is Proposition 10.2.1 of [5]. Its proof is based on Corollary 1.2 of [4] on unit equations over finitely generated integral domains. □

5. Proof of Theorem 2.1

We start with a preliminary lemma.

Lemma 5.1. *For every integral domain A finitely generated over $\mathbb{Z}$ and every two monic polynomials F_1, $F_2 \in A[X]$, all effectively given, we can determine effectively whether F_1, F_2 are A-equivalent.*

Proof. It suffices to consider the case when F_1, F_2 have equal degrees. Write $F_1(X) = X^n + a_1X^{n-1} + \cdots$, $F_2(X) = X^n + b_1X^{n-1} + \cdots$. We have to check whether there exists $a \in A$ with $F_2(X) = F_1(X + a)$. Comparing the coefficients of X^{n-1} we see that for such a we must have $na = b_1 - a_1$. Using Corollary 3.4 (ii) we can check whether $a \in A$ and then whether indeed $F_2(X) = F_1(X + a)$. □

Henceforth, the integral domain A is given effectively in the form

$$\mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_s) = \mathbb{Z}[x_1, \ldots, x_r]$$

where x_i is the residue class of X_i mod $(f_1, \ldots, f_s)$ for $i = 1, \ldots, r$. Further the finite extension G of the quotient field K of A is given in the form $K[X]/(P)$ or $K(w)$, where w is the residue class of X mod P. The polynomial P may be represented as $b_0^{-1} \sum_{i=0}^{d} b_i X^{d-i}$ with $b_0, \ldots, b_d$ given as polynomials in $x_1, \ldots, x_r$ with integer coefficients. Define

$$u := b_0 w.$$

Then u has minimal polynomial

$$Q = X^d + \sum_{i=1}^{d} b_i b_0^{d-1-i} X^{d-i} =: X^d + \sum_{i=1}^{d} c_i X^{d-i} \in A[X] \tag{5.1}$$

over K. Now clearly, $G = K(u)$, u is integral over A, and every element of G can be expressed in the form $\sum_{i=0}^{d-1} (a_i/b) u^i$ with $a_0, \ldots, a_{d-1}, b \in A$, given as polynomials with integer coefficients in $x_1, \ldots, x_r$.

Proof of Theorem 2.1. Let A, G, n, δ be effectively given and satisfy the conditions of Theorem 2.1. Further, let $\mathscr{F}$ be the finite effectively determinable set from Proposition 4.1.

Take a monic polynomial F from $A[X]$ with (1.1). Then F has all its zeros in G, say $F(X) = (X - \alpha_1) \cdots (X - \alpha_n)$, with $\alpha_1, \ldots, \alpha_n \in G$. By Proposition 4.1 we have

$$\alpha_i - \alpha_j \in \mathscr{F} \text{ for } i, j \in \{1, \ldots, n\} \text{ with } i \neq j.$$

Recall that $\mathscr{F}$ is finite, and effectively determinable in terms of A, G, n, δ. For each tuple $(\gamma_{ij} : i, j \in \{1, \ldots, n\}, i \neq j)$ with elements from $\mathscr{F}$ we consider the polynomials F with (1.1) and with $\alpha_i - \alpha_j = \gamma_{ij}$ for $i, j \in \{1, \ldots, n\}$, $i \neq j$. That is, we consider polynomials F such that

$$\text{(5.2)} \qquad \begin{cases} F \in A[X], F \text{ monic }, \deg F = n, D(F) = \delta, \\ F = (X - \alpha_1) \cdots (X - \alpha_n) \text{ for some } \alpha_1, \ldots, \alpha_n \in G \\ \text{such that } \alpha_i - \alpha_j = \gamma_{ij} \text{ for } i, j \in \{1, \ldots, n\}, i \neq j. \end{cases}$$

Our proof will be completed as follows. We show that for each tuple $\{\gamma_{ij}\}$ it can be decided effectively whether a polynomial F with (5.2) exists. If so, we show that the polynomials with (5.2) lie in finitely many A-equivalence classes, and determine effectively a full system of representatives for them. Then from the union of these systems, we extract a full system of representatives for the A-equivalence classes of solutions of (1.1).

Fix elements γ_{ij} from $\mathscr{F}$ $(1 \leq i, j \leq n, i \neq j)$. Suppose there is a polynomial F with (5.2). For this polynomial we have

$$\text{(5.3)} \qquad n\alpha_i = y + \gamma_i \text{ for } i = 1, \ldots, n,$$

with $y = \alpha_1 + \cdots + \alpha_n$, $\gamma_i = \sum_{j=1}^{n} \gamma_{ij}$ for $i = 1, \ldots, n$, where we have put $\gamma_{ii} := 0$ for $i = 1, \ldots, n$. Here $\gamma_1, \ldots, \gamma_n$ are fixed and $y, \alpha_1, \ldots, \alpha_n$ are unknowns. The number y is a coefficient of F, so $y \in A$. Further, if there is a polynomial F with (5.2), then

$$\text{(5.4)} \qquad (X - \gamma_1) \cdots (X - \gamma_n) = n^n F\left(\frac{X + y}{n}\right) \in A[X].$$

The coefficients of $(X - \gamma_1) \cdots (X - \gamma_n)$ belong to G. It can be checked whether they belong to K, and then by means of and by Corollary 3.4 (ii), it can be checked whether they belong to A. If not so, there is no polynomial with (5.2). So we assume henceforth that $(X - \gamma_1) \cdots (X - \gamma_n) \in A[X]$. Then $\gamma_1, \ldots, \gamma_n \in A_G$.

Using Proposition 3.8, we compute a finite set of A-module generators for A_G. From this, we deduce a system $\{\mathbf{a}_1, \ldots, \mathbf{a}_t\}$ of A-module generators for A_G^n. The numbers $\alpha_1, \ldots, \alpha_n$ from (5.2) are in A_G. So there are $x_1, \ldots, x_t \in A$ such that

$$\text{(5.5)} \qquad \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = x_1\mathbf{a}_1 + \cdots + x_t\mathbf{a}_t,$$

and we can rewrite (5.3) as

$$x_1(n\mathbf{a}_1)+\cdots+x_t(n\mathbf{a}_t)=y\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}+\begin{pmatrix}\gamma_1\\ \vdots\\ \gamma_n\end{pmatrix}. \tag{5.6}$$

By linear algebra, we can determine a maximal K-linearly-independent subset of $\{n\mathbf{a}_1,\dots,n\mathbf{a}_t,(1,\dots,1)^T,(\gamma_1,\dots,\gamma_n)^T\}$, say $\{\mathbf{b}_1,\dots,\mathbf{b}_m\}$. Further, we can compute expressions for $n\mathbf{a}_1,\dots,n\mathbf{a}_t,(1,\dots,1)^T,(\gamma_1,\dots,\gamma_n)^T$ as K-linear combinations of $\mathbf{b}_1,\dots,\mathbf{b}_m$. By substituting these into (5.6) and equating the coordinates of (5.6), we obtain a system of inhomogeneous linear equations:

$$M\mathbf{x}=\mathbf{b}\ \text{ in }\mathbf{x}=(x_1,\dots,x_t,y)^T\in A^{t+1} \tag{5.7}$$

where the matrix M and vector $\mathbf{b}$ have their entries in K. Then using Corollary 3.4 we can decide whether (5.7) is solvable and if so, compute a solution. Translating this back to (5.6), we can decide whether (5.6) is solvable and if so, compute a solution.

If (5.6) is unsolvable, then there is no polynomial F satisfying (5.2). Assume (5.6) is solvable and compute a solution, say $(x_{10},\dots,x_{t0},y_0)\in A^{t+1}$. Thus, $\sum_{i=1}^t x_{i0}(n\mathbf{a}_i)-y_0(1,\dots,1)^T=(\gamma_1,\dots,\gamma_n)^T$. Put

$$\begin{pmatrix}\alpha_{10}\\ \vdots\\ \alpha_{n0}\end{pmatrix}:=x_{10}\mathbf{a}_1+\cdots+x_{n0}\mathbf{a}_t. \tag{5.8}$$

Then

$$n\alpha_{i0}=y_0+\gamma_i\ \text{ for } i=1,\dots,n\ \text{ with } y_0\in A. \tag{5.9}$$

Now let again F be an arbitrary polynomial with (5.2) and let y be as in (5.3). From (5.3), (5.9) we infer that

$$\alpha_i-\alpha_{i0}=\frac{y-y_0}{n}=:a\ \text{ for } i=1,\dots,n. \tag{5.10}$$

Clearly, $a\in\frac{1}{n}A$. Identity (5.8) implies that $\alpha_{10},\dots,\alpha_{n0}\in A_G$. Hence a is integral over A. So in fact, $a\in\frac{1}{n}A\cap A_K$.

By Corollary 3.9, we can compute a full system of representatives, say $\{\theta_1,\dots,\theta_h\}$ for $\big(\frac{1}{n}A^+\cap\overline{A}^+\big)/A^+$. For $j=1,\dots,h$, put

$$F_j(X):=(X-\alpha_{10}-\theta_j)\cdots(X-\alpha_{n0}-\theta_j).$$

For some $j\in\{1,\dots,h\}$ we have $a=\theta_j+c$ for some $c\in A$. Then (5.10) implies that $\alpha_i=\alpha_{i0}+\theta_j+c$ for $i=1,\dots,n$, and so $F(X)=F_j(X-c)$. Hence F is A-equivalent to F_j.

The polynomials $F_1,\dots,F_h$ can be determined effectively. Their coefficients belong to K and using Corollary 3.4 we can select those polynomials that have their coefficients in A. Thus, for each tuple $\{\gamma_{ij}\}$ with $\gamma_{ij}\in\mathscr{F}$ we can compute a

finite system of polynomials from $A[X]$ such that every polynomial with (5.2) is A-equivalent to one of them. By taking the union of these systems for all tuples $\{\gamma_{ij}\}$, we effectively determine a finite list of polynomials from $A[X]$ such that every polynomial with (1.1) is A-equivalent to at least one of them. For each polynomial from the list we can effectively decide whether it satisfies (1.1) and if not so, remove it. Finally, assuming the list is ordered, by means of Lemma 5.1 we can effectively decide whether a polynomial from the list is A-equivalent to an earlier polynomial in the list and if so, remove it. This leaves us with a full system of representatives for the A-equivalence classes of polynomials with (1.1). This completes the proof of Theorem 2.1. □

6. Proof of Theorem 2.2

Let A be an integral domain finitely generated over $\mathbb{Z}$, effectively given as usual in the form $\mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_s) = \mathbb{Z}[x_1, \ldots, x_r]$, where $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_r]$ and where x_i is the residue class of X_i mod $(f_1, \ldots, f_s)$ for $i = 1, \ldots, r$. Denote by K the quotient field of A. Let Ω be a finite étale K-algebra, effectively given in the form $K[X]/(P) = K[\theta]$, where $P \in K[X]$ is a monic polynomial without multiple zeros, and $\theta = \bmod P$.

We need some results from [5, §10.7]. Using [5, Cor. 10.7.7] we can construct the splitting field of P over K; call this G. By means of [5, Cor. 10.7.8] we can compute w such that $G = K(w)$, together with the minimal polynomial of w over K. As was explained in Section 5, we can compute from this another representation for G of the form $K(u)$, where u is integral over A, together with the monic minimal polynomial Q of u over K. Elements of G are always given in the form $\sum_{i=0}^{d-1}(a_i/b)u^i$ where $d = [G : K]$ and $a_0, \ldots, a_{d-1}, b$ are elements of A.

The polynomial P factorizes as $(X - \theta^{(1)}) \cdots (X - \theta^{(n)})$ in G, and by [5, Cor. 10.7.8] we can compute expressions of $\theta^{(1)}, \ldots, \theta^{(n)}$ as K-linear combinations of $1, u, \ldots, u^{d-1}$. With these expressions we can compute, for any element $\alpha = \sum_{i=0}^{n-1} c_i\theta^i \in \Omega$ with $c_0, \ldots, c_{n-1} \in K$, its images $\alpha^{(j)} = \sum_{i=0}^{n-1} c_i(\theta^{(j)})^i$ $(j = 1, \ldots, n)$ under the K-homomorphisms of Ω to G.

We start with a lemma.

Lemma 6.1. *For any two effectively given $\alpha_1, \alpha_2 \in O$ with $K[\alpha_1] = K[\alpha_2] = \Omega$, we can decide effectively whether α_1, α_2 are A-equivalent.*

Proof. Compute expressions $\alpha_1 = \sum_{i=0}^{n-1} c_i\theta^i$, $\alpha_2 = \sum_{i=0}^{n-1} d_i\theta^i$ with $c_i, d_i \in K$, and check if $c_0 - d_0 \in A$, $c_i = d_i$ for $i = 1, \ldots, n-1$. □

Proof of Theorem 2.2. Let A, Ω, O be the effectively given integral domain, finite étale K-algebra, and A-order in Ω. Assume that $(O \cap K)^+/A^+$ is finite. Let $\{\omega_1 = 1, \ldots, \omega_m\}$ be the effectively given system of A-module generators for O.

Further, let $n = [\Omega : K]$, $n \geq 2$ and let δ be the given element of A. Lastly, let G be the field defined above, given in the form $K(u)$ with u integral over A.

Recall that by Proposition 3.6, we can compute an ideal representation for the integral closure A_K of A, i.e., A_K is effectively given as an integral domain in the usual sense. So we can apply Proposition 4.1 with A_K instead of A. Let $\mathscr{F}'$ be the finite set $\mathscr{F}$ from Proposition 4.1 but taken with A_K instead of A. This set can be computed effectively in terms of A_K, G, δ, hence in terms of A, Ω, δ. Now if α is an element of O with (1.3), i.e., $D_{\Omega/K}(\alpha) = \delta$, then $\alpha \in A_\Omega$, hence $F_\alpha(X) := (X - \alpha^{(1)}) \cdots (X - \alpha^{(n)})$ has its coefficients in A_K, we have $D(F_\alpha) = \delta$, and F_α has its zeros in G. Hence

$$\alpha^{(i)} - \alpha^{(j)} \in \mathscr{F}' \text{ for } i, j \in \{1, \ldots, n\}, i \neq j.$$

We now pick elements γ_{ij} from $\mathscr{F}'$ and consider the elements α with

$$\left\{ \begin{array}{l} \alpha \in O,\ D_{\Omega/K}(\alpha) = \delta, \\ \alpha^{(i)} - \alpha^{(j)} \in \gamma_{ij} \text{ for } i, j \in \{1, \ldots, n\}, i \neq j. \end{array} \right. \tag{6.1}$$

We show that it can be decided effectively whether (6.1) is solvable and if so, compute a solution of (6.1). Notice that (6.1) is certainly unsolvable if $\prod_{1 \leq i < j \leq n} \gamma_{ij}^2 \neq \delta$. Assume that $\prod_{1 \leq i < j \leq n} \gamma_{ij}^2 = \delta$. Then the condition $D_{\Omega/K}(\alpha) = \delta$ can be dropped. Writing α as $\sum_{k=1}^m x_k \omega_k$ with $x_1, \ldots, x_m \in A$, we can rewrite (6.1) as

$$\sum_{k=1}^m x_k \left(\omega_k^{(i)} - \omega_k^{(j)} \right) = \gamma_{ij} \text{ for } i, j \in \{1, \ldots, n\}, i \neq j. \tag{6.2}$$

Clearly, $(x_1, \ldots, x_m)$ is a solution of (6.2) in A^m if and only if $\alpha := \sum_{k=1}^m x_k \omega_k$ is a solution of (6.1).

By expressing $\omega_k^{(i)} - \omega_k^{(j)}$ and the numbers γ_{ij} as K-linear combinations of $1, u, \ldots, u^{d-1}$ where $d = [G : K]$ and u is the generating element of G over K, we can rewrite (6.2) as a system of inhomogeneous linear equations in A^m like in Corollary 3.4 (ii). Thus, it can be decided effectively whether (6.2) is solvable, and if so, a solution can be computed. Equivalently, it can be decided effectively whether (6.1) is solvable and if so, a solution can be computed.

For each choice of $\gamma_{ij} \in \mathscr{F}'$ ($1 \leq i, \leq n$, $i \neq j$), we check if (6.1) is solvable and if so, we compute a solution. Let $\mathcal{T} = \{\alpha_1, \ldots, \alpha_g\}$ be the finite set obtained in this manner. By Corollary 3.10 (ii) we can compute a full system of representatives $\{\theta_1, \ldots, \theta_h\}$ for $(O \cap K)^+ / A^+$. Using Lemma 6.1, we can compute a maximal subset $\mathcal{U}$ of $\{\alpha_i + \theta_j : i = 1, \ldots, g,\ j = 1, \ldots, h\}$ such that any two distinct elements of $\mathcal{U}$ are not A-equivalent. We show that $\mathcal{U}$ is a full system of representatives for the A-equivalence classes of solutions of (1.3).

Let α be a solution of (1.3). Then α satisfies (6.1) for certain $\gamma_{ij} \in \mathscr{F}'$. Let α_0 be an element from $\mathcal{T}$ satisfying (6.1) for these γ_{ij}. Then $\alpha^{(i)} - \alpha^{(j)} = \alpha_0^{(i)} - \alpha_0^{(j)}$

for $i, j \in \{1, \dots, n\}$, hence

$$\alpha^{(1)} - \alpha_0^{(1)} = \cdots = \alpha^{(n)} - \alpha_0^{(n)}.$$

It follows that $\alpha - \alpha_0 =: a \in O \cap K$. Hence $a = \theta_j + c$ for some $j \in \{1, \dots, h\}$ and $c \in A$, and so, $\alpha = \alpha_0 + \theta_j + c$. Now clearly, α is A-equivalent to an element of $\mathcal{U}$. This completes our proof of Theorem 2.2. □

References

[1] M. Aschenbrenner, *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. **17** (2004), 407–442.

[2] I. Borosh, M. Flahive, D.Rubin and B. Treybig, *A sharp bound for solutions of linear Diophantine equations*, Proc. Amer. Math. Soc. **105** (1989), 844–846.

[3] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer Verlag, 1994.

[4] J.-H. Evertse, K. Győry, *Effective results for unit equations over finitely generated domains*, Math. Proc. Cambridge Phil. Soc. **154** (2013), 351–380.

[5] J.-H. Evertse, K. Győry, *Discriminant Equations in Diophantine Number Theory*, Cambridge Univ. Press, to appear.

[6] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. **23** (1973), 419–426.

[7] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné II*, Publ. Math. Debrecen **21** (1974), 125–144.

[8] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné III*, Publ. Math. Debrecen **23** (1976), 141–165.

[9] K. Győry, *On polynomials with integer coefficients and given discriminant IV*, Publ. Math. Debrecen **25** (1978), 155–167.

[10] K. Győry, *On polynomials with integer coefficients and given discriminant V,* $\mathfrak{p}$*-adic generalizations*, Acta Math. Acad. Sci. Hung. **32** (1978), 175–190.

[11] K. Győry, *On discriminants and indices of integers of an algebraic number field*, J. Reine Angew. Math. **324** (1981), 114–126.

[12] K. Győry, *On certain graphs associated with an integral domain and their applications to diophantine problems*, Publ. Math. Debrecen **29** (1982), 79–94.

[13] K. Győry, *Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains*, J. Reine Angew. Math. **346** (1984), 54–100.

[14] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788.

[15] T. de Jong, *An Algorithm for Computing the Integral Closure*, J. Symbolic Computation **26** (1998), 273–277.

[16] R. Matsumoto, *On computing the integral closure*, Comm. in Algebra **28** (2000), 401–405.

[17] H. Matsumura, *Commutative Ring Theory*, Cambridge Univ. Press, 1986.

[18] M. Nagata, *A general theory of algebraic geometry over Dedekind domains I*, Amer. J. Math. **78** (1956), 78–116.

[19] P. Roquette, *Einheiten und Divisorenklassen in endlich erzeugbaren Körpern*, Jahresber. Deutsch. Math. Verein **60** (1957), 1–21.

[20] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.

J.-H. Evertse
Leiden University, Mathematical Institute
P.O.Box 9512, 2300 RA Leiden, The Netherlands

E-mail address: evertse@math.leidenuniv.nl

K. Győry
Institute of Mathematics, University of Debrecen
H-4032 Debrecen, Egyetem Tér 1, Hungary

E-mail address: gyory@science.unideb.hu