

*SOME APPLICATIONS OF DECOMPOSABLE
FORM EQUATIONS TO RESULTANT EQUATIONS*

BY

K. GYŐRY (DEBRECEN)

1. Introduction. The purpose of this paper is to establish some general finiteness results (cf. Theorems 1 and 2) for resultant equations over an arbitrary finitely generated integral domain R over \mathbb{Z} . Our Theorems 1 and 2 improve and generalize some results of Wirsing [25], Fujiwara [6], Schmidt [21] and Schlickewei [17] concerning resultant equations over \mathbb{Z} . Theorems 1 and 2 are consequences of a finiteness result (cf. Theorem 3) on decomposable form equations over R . Some applications of Theorems 1 and 2 are also presented to polynomials in $R[X]$ assuming unit values at many given points in R (cf. Corollary 1) and to arithmetic progressions of given order, consisting of units of R (cf. Corollary 2). Further applications to irreducible polynomials will be given in a separate paper.

Our Theorem 3 seems to be interesting in itself as well. It is deduced from some general results of Evertse and the author [3] on decomposable form equations. Since the proofs in [3] depend among other things on the Thue–Siegel–Roth–Schmidt method and its p -adic generalization, all results of the present paper are ineffective.

2. Finiteness theorems for resultant equations and decomposable form equations. Let $P(X)$ be a polynomial of degree m with integer coefficients and without multiple zeros, and let a be a non-zero integer. Consider those polynomials $Q(X)$ with integer coefficients for which

$$(1) \quad \text{Res}(P, Q) = a,$$

where $\text{Res}(P, Q)$ denotes the resultant of P and Q . Equation (1) is called a *resultant equation*. It can be considered as a polynomial diophantine equation in the coefficients of Q . It follows from a theorem of Wirsing [25]

1991 *Mathematics Subject Classification*: 11D57, 11E76.

Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research.

that if n is a positive integer such that

$$(2) \quad 2n \left(1 + \frac{1}{3} + \dots + \frac{1}{2n-1} \right) < m,$$

then there are only finitely many polynomials $Q \in \mathbb{Z}[X]$ of degree n which satisfy (1). Fujiwara [6] proved (but did not express it in this way) that if P is irreducible over \mathbb{Q} and

$$(3) \quad 2n < m$$

then equation (1) has only finitely many solutions in polynomials $Q \in \mathbb{Z}[X]$ of degree n . By a theorem of Schmidt [21], the irreducibility of P can here be replaced by the weaker condition that P has no non-constant factor of degree $\leq n$ in $\mathbb{Z}[X]$. Further, Schmidt showed that assumption (3) is already best possible in the sense that his result concerning (1) does not remain valid in general for $2n = m$.

Let now R be a subring of \mathbb{Q} which is a finitely generated extension ring of \mathbb{Z} , and let a be a non-zero element of R . As a generalization of Schmidt's result, Schlickewei [17] showed that if m, n are positive integers satisfying (3) and $P \in R[X]$ is a polynomial of degree m without multiple zeros which has no non-constant factor of degree $\leq n$ in $R[X]$ then, up to a proportional factor from $(1) R^*$, there are only finitely many polynomials $Q \in R[X]$ of degree n which satisfy

$$(4) \quad \text{Res}(P, Q) \in a \cdot R^*.$$

It should be remarked that Wirsing, Schmidt and Schlickewei obtained their results in a more general form, for resultant inequalities in place of (1) and (4). Further, we note that recently equations (1) and (4) have also been studied in Györy [7], [9], [10] and Evertse and Györy [5] in the case when both P and Q are unknown, but their splitting fields are fixed. Finally, under certain additional assumptions (e.g. P, Q monic, $\deg(Q) = 3, Q(0)$ fixed) Pethő [14]–[16] has developed a method for determining or describing all solutions of (1) in $Q(X)$.

In what follows, we consider equations (1) and (4) in the following more general situation. Let K be a finitely generated extension field of \mathbb{Q} , and R a finitely generated extension ring of \mathbb{Z} in K . Then the unit group R^* of R is finitely generated (see e.g. [11]).

THEOREM 1. *Let m and n be positive integers with $m > 2n$, and let a be a non-zero element of K . Further, let $P(X)$ be a polynomial of degree m with coefficients in K and without multiple zeros. Then there are only*

⁽¹⁾ For any integral domain A , we denote by A^* the unit group of A , i.e. the multiplicative group of invertible elements of A .

finitely many polynomials $Q(X)$ with degree n and coefficients in R which satisfy (1).

For equation (4), we have the following result.

THEOREM 2. *Let m, n, a and P be as in Theorem 1. Then up to a proportional factor from R^* , there are only finitely many polynomials $Q(X)$ with degree n and coefficients in R which satisfy (4).*

If, in Theorem 2, we consider monic polynomials $Q(X)$ only, the condition $m > 2n$ can be replaced by $m \geq 2n$.

For $K = \mathbb{Q}$ and $R = \mathbb{Z}$, Theorem 1 gives the result of Wirsing on equation (1) in an improved form, under assumption (3) instead of (2). Further, for $K = \mathbb{Q}$, Theorems 1 and 2 imply the results of Fujiwara, Schmidt and Schlickewei concerning (1) and (4), without any condition on the factors of the polynomial P .

Theorem 1 follows from Theorem 2. Indeed, every solution Q of (1) satisfies (4). But if Q and cQ are solutions of (1) for some $c \in R^*$ then $c^m = 1$ and hence Theorem 2 implies the finiteness of the number of solutions Q of (1). Conversely, Theorem 2 follows from Theorem 1 by observing that $R^*/(R^*)^m$ is finite, whence that (4) can be reduced to a finite number of equations of type (1). Thus Theorems 1 and 2 are in fact equivalent.

We remark that if in Theorem 1 or 2, P has all its coefficients in R then the number of polynomials Q under consideration can be bounded above by a number which depends on m, n, a, R and the splitting field of P over K , but not on the coefficients of P . Moreover, when K is an algebraic number field, such a bound can be given explicitly in terms of each parameter. Bounds of this type can be derived from quantitative versions of our Lemma 1 (cf. Section 4) on decomposable form equations. We shall not work these out here.

Finally, we note that Theorems 1 and 2 can be adapted to the case when, in (1) and (4), P and Q are binary forms with coefficients in K and R , respectively. For results of this type we refer to the papers [5] and [10].

The polynomial $P(X) \in K[X]$ can be written in the form

$$P(X) = a_0(X - \alpha_1) \dots (X - \alpha_m),$$

where $a_0 \in K \setminus \{0\}$ and $\alpha_1, \dots, \alpha_m$ are distinct elements of a finite extension, say L , of K . If $Q(X) = x_0X^n + x_1X^{n-1} + \dots + x_n$ is a polynomial in $R[X]$ then

$$\text{Res}(P, Q) = a_0^n \prod_{i=1}^m (x_0\alpha_i^n + x_1\alpha_i^{n-1} + \dots + x_n).$$

It is easy to see that this is a decomposable form in x_0, \dots, x_n with coefficients in K . Hence (1) leads to a *decomposable form equation*, i.e. an

equation of the form

$$(5) \quad F(x_0, x_1, \dots, x_n) = a$$

in $x_0, x_1, \dots, x_n \in R$, where F is a homogeneous polynomial with coefficients in K which factorizes into linear forms over L .

For $K = \mathbb{Q}$, Schmidt's result on equation (1) follows from the following theorem [21]. Let $F(\underline{X}) = F(X_0, \dots, X_n)$ ($n \geq 1$) be a decomposable form of degree m with coefficients in \mathbb{Q} such that for some integer k with $n+1 \leq k$ and $m > 2(k-1)$, F is not divisible by a rational form of degree less than k and that any k linear factors in the factorization $F(\underline{X}) = l_1(\underline{X}) \dots l_m(\underline{X})$ into linear forms have rank $n+1$. Then equation (5) has only finitely many solutions in $x_0, \dots, x_n \in \mathbb{Z}$ for every non-zero $a \in \mathbb{Z}$. Later, Schlickewei [17] extended this theorem to the solutions x_0, \dots, x_n of (5) in an arbitrary finitely generated subring R of \mathbb{Q} . We note that Schmidt and Schlickewei established their results in a more general form, for inequalities concerning decomposable forms instead of (5).

We shall deduce Theorem 1 from Theorem 3 below. We recall that K is a finitely generated extension field of \mathbb{Q} , R is a finitely generated extension ring of \mathbb{Z} in K , and a denotes a non-zero element of K .

THEOREM 3. *Let $F(X_0, X_1, \dots, X_n)$ ($n \geq 1$) be a decomposable form of degree m with coefficients in K . Suppose that there is an integer k with $n \leq k-1$ and $m > 2(k-1)$ such that any k linear factors in the factorization of F have rank $n+1$. Then equation (5) has only finitely many solutions in $x_0, \dots, x_n \in R$.*

For $K = \mathbb{Q}$, our Theorem 3 implies an improved version of the above-quoted results of Schmidt and Schlickewei on equation (5).

In Section 4, we shall deduce Theorem 3 from a general finiteness criterion (cf. Lemma 1 in Section 4) of Evertse and the author [3] on decomposable form equations. The finiteness condition in Theorem 3 is simpler than that of [3], especially when $k = n+1$. This may be useful for some applications. For $n = 1$ and $k = 2$, Theorem 3 gives a well-known finiteness result on Thue equations (see e.g. Lang [11]).

We remark that if F has all its coefficients in R , then the number of solutions of (5) considered in Theorem 3 can be bounded above by a number which depends only on m, n, a, R and the splitting field of F over K , but not on the coefficients of F . Further, if K is an algebraic number field then such a bound can be given explicitly in terms of each parameter. These follow from some quantitative versions of the criterion in [3] mentioned above (see the Remark after the statement of Lemma 1 in Section 4).

3. Applications. Throughout this section, let again K be a finitely generated extension field of \mathbb{Q} , R a finitely generated extension ring of \mathbb{Z}

in K , and a a non-zero element of R . Further, let $\{r_1, \dots, r_m\}$ be a finite set in R with $m \geq 3$ elements, and consider those non-constant polynomials $Q(X)$ in $R[X]$ for which

$$(6) \quad Q(r_i) \in a \cdot R^* \quad \text{for } i = 1, \dots, m.$$

If $Q(X)$ satisfies (6) then so does $c \cdot Q(X)$ for every $c \in R^*$. Putting now $P(X) = (X - r_1) \dots (X - r_m)$, (6) implies

$$\text{Res}(P, Q) \in a^m \cdot R^*$$

and hence Theorem 2 immediately gives the following.

COROLLARY 1. *Up to a proportional factor from R^* , there are only finitely many non-constant polynomials $Q(X)$ in $R[X]$ with degree less than $m/2$ for which (6) holds.*

Here the bound $m/2$ is already best possible in general. Indeed, suppose that $m = 2n$, and let d be a positive integer for which $\sqrt[n]{d}$ is of degree m over \mathbb{Q} . Denote by r_1, \dots, r_m the conjugates of $\sqrt[n]{d}$ over \mathbb{Q} , by K the algebraic number field $\mathbb{Q}(r_1, \dots, r_m)$ and by R the ring of integers of K . Then there are infinitely many pairwise non-proportional pairs of rational integers x_0, x_n such that $x_0 \sqrt[n]{d} + x_n \in R^*$ and $-x_0 \sqrt[n]{d} + x_n \in R^*$. Consequently, there are infinitely many pairwise non-proportional polynomials $Q(X) = x_0 X^n + x_n$ of degree n with rational coefficients for which

$$Q(r_i) \in R^* \quad \text{for } i = 1, \dots, m.$$

The next application is concerned with arithmetic progressions consisting of units. In [12] (see also [13]), Newman proved that an algebraic number field of degree $n \geq 4$ can contain at most n units in arithmetic progression, and that this bound is sharp. In the more general situation of the present paper, a weaker but explicit upper bound can be derived from Theorem 1 of [2] for the maximal length of arithmetic progressions in R^* . From Corollary 1 we shall deduce a general finiteness result for arithmetic progressions of a given order and given length in R^* .

COROLLARY 2. *Let m and n be positive integers with $m > 2n$. Up to a proportional factor from R^* , there are only finitely many arithmetic progressions of length m and order n which consist of elements of R^* .*

In particular, for $n = 1$ there are only finitely many three-term arithmetic progressions in R^* , apart from a proportional factor from R^* . We note that in the number field case an explicit upper bound can be given for the number of arithmetic progressions considered in Corollary 2.

4. Proofs. We keep the notation of Sections 2 and 3. Let K denote a finitely generated extension field of \mathbb{Q} , and $F(\underline{X}) = F(X_0, \dots, X_n)$

$\in K[X_0, \dots, X_n]$ a decomposable form which factorizes into linear forms $l_1(\underline{X}), \dots, l_m(\underline{X})$ over a finite extension, say L , of K . Denote by \mathcal{L}_0 a maximal subset of pairwise linearly independent linear forms in $\{l_1, \dots, l_m\}$ over L . A non-zero K -linear subspace V of K^{n+1} is said to be \mathcal{L}_0 -non-degenerate or \mathcal{L}_0 -degenerate according as \mathcal{L}_0 does or does not contain a subset of at least three linear forms whose restrictions to V are linearly dependent, but pairwise linearly independent over L . Further, V is called \mathcal{L}_0 -admissible if no form in \mathcal{L}_0 vanishes identically on V .

LEMMA 1. *The following two statements are equivalent:*

- (i) *Every \mathcal{L}_0 -admissible K -linear subspace V of K^{n+1} of dimension ≥ 2 is \mathcal{L}_0 -non-degenerate;*
- (ii) *For every $a \in K^*$ and every subring R of K which is finitely generated over \mathbb{Z} , equation (5) has only finitely many solutions x_0, \dots, x_n in R .*

Proof. This is Theorem 1 of Evertse and the author [3]. ■

Remark. For some quantitative versions of Lemma 1, see Evertse, Gaál and the author [1] and the author [8]. When R contains a and the coefficients of F , these quantitative results provide upper bounds for the number of solutions of (5) and these bounds depend only on m, n, a, R, K and L , but not on the coefficients of F . Further, in the case when K is an algebraic number field, completely explicit upper bounds of this kind are given in [8]. In the proofs of these results of [1] and [8] some quantitative finiteness theorems of Evertse and the author [4] and Schlickewei [19] are used on unit equations which depend, among other things, on Schlickewei's p -adic generalization [18] of Schmidt's Subspace Theorem [22] and their recent quantitative versions (cf. [23], [20]). We note that, in the number field case, some improvements of the above-mentioned quantitative results have recently been obtained by Evertse (private communication).

For any system \mathfrak{M} of linear forms with coefficients in K , let $\mathcal{V}_K(\mathfrak{M})$ denote the K -vector space generated by the forms of \mathfrak{M} .

LEMMA 2. *Let K, \mathcal{L}_0 and L be the same as in Lemma 1, and suppose that $L = K$. Then the following two statements are equivalent:*

- (i) *Every \mathcal{L}_0 -admissible K -linear subspace V of K^{n+1} of dimension ≥ 2 is \mathcal{L}_0 -non-degenerate;*
- (ii) *The forms in \mathcal{L}_0 have rank $n + 1$ over K and for each proper non-empty subset \mathcal{L}_1 of \mathcal{L}_0 , we have*

$$(\mathcal{V}_K(\mathcal{L}_1) \cap \mathcal{V}_K(\mathcal{L}_0 \setminus \mathcal{L}_1)) \cap \mathcal{L}_0 \neq \emptyset.$$

Proof. This is the Proposition in [3]. ■

Proof of Theorem 3. Let K, R, a and F be as in Theorem 3. Then F can be written in the form

$$F(\underline{X}) = a_0 l_1^{b_1}(\underline{X}) \dots l_r^{b_r}(\underline{X}),$$

where $a_0 \in K^*, b_1, \dots, b_r$ are positive integers and l_1, \dots, l_r are pairwise linearly independent linear forms with coefficients in a finite extension, say L , of K . Put $\mathcal{L}_0 = \{l_1, \dots, l_r\}$, and let \mathcal{L}'_0 be the system of linear forms l_1, \dots, l_r counted with multiplicities b_1, \dots, b_r , respectively. Then \mathcal{L}'_0 has cardinality m . Consider a proper non-empty subset $\mathcal{L}_1 = \{l_{i_1}, \dots, l_{i_t}\}$ of \mathcal{L}_0 , and denote by \mathcal{L}'_1 the subsystem of \mathcal{L}'_0 consisting of l_{i_1}, \dots, l_{i_t} counted with multiplicities b_{i_1}, \dots, b_{i_t} , respectively. By assumption, there is an integer k with $n \leq k - 1$ and $m > 2(k - 1)$ such that any k linear forms in \mathcal{L}'_0 have rank $n + 1$ over L . Hence \mathcal{L}_0 also has rank $n + 1$ over L . Further, in view of $m > 2(k - 1)$, at least one of \mathcal{L}'_1 and $\mathcal{L}'_0 \setminus \mathcal{L}'_1$, say \mathcal{L}'_1 , has cardinality $\geq k$. Thus \mathcal{L}'_1 has rank $n + 1$ and hence \mathcal{L}_1 also has rank $n + 1$ over L . Consequently, $\mathcal{L}_0 \setminus \mathcal{L}_1 \subseteq \mathcal{V}_L(\mathcal{L}_1)$ and so

$$\mathcal{L}_0 \setminus \mathcal{L}_1 \subset (\mathcal{V}_L(\mathcal{L}_1) \cap \mathcal{V}_L(\mathcal{L}_0 \setminus \mathcal{L}_1)) \cap \mathcal{L}_0.$$

If $\mathcal{L}'_0 \setminus \mathcal{L}'_1$ is of cardinality $\geq k$ then in a similar way we get

$$\mathcal{L}_1 \subset (\mathcal{V}_L(\mathcal{L}_1) \cap \mathcal{V}_L(\mathcal{L}_0 \setminus \mathcal{L}_1)) \cap \mathcal{L}_0.$$

It now follows from Lemmas 2 and 1 that equation (5) has only a finite number of solutions in every finitely generated subring of L over \mathbb{Z} . This completes the proof of Theorem 3. ■

Proof of Theorem 1. Let K, R, a, m, n and P be as in Theorem 1. We write $P(X) = a_0(X - \alpha_1) \dots (X - \alpha_m)$, where $\alpha_1, \dots, \alpha_m$ are distinct elements of the splitting field, say L , of P over K . Let $Q(X) = x_0 X^n + x_1 X^{n-1} + \dots + x_n$ be an arbitrary polynomial with degree n and coefficients in R which satisfies (1). Then (1) can be written in the form

$$(7) \quad F(x_0, x_1, \dots, x_n) = a \quad \text{in } x_0, x_1, \dots, x_n \in R$$

where

$$F(X_0, X_1, \dots, X_n) = a_0^n \prod_{i=1}^m (X_0 \alpha_i^n + X_1 \alpha_i^{n-1} + \dots + X_n)$$

is a decomposable form of degree m with coefficients in K . Put

$$l_1(\underline{X}) = a_0^n (X_0 \alpha_1^n + X_1 \alpha_1^{n-1} + \dots + X_n),$$

$$l_i(\underline{X}) = X_0 \alpha_i^n + X_1 \alpha_i^{n-1} + \dots + X_n \quad \text{for } i = 2, \dots, m,$$

and $\mathcal{L}_0 = \{l_1, \dots, l_m\}$. Since, by assumption, the zeros of P are distinct, any $n + 1$ of the linear forms in \mathcal{L}_0 have rank $n + 1$. But $m > 2n$, hence Theorem 3 can be applied to equation (7) with the choice $k = n + 1$, and

it follows that (7) has only finitely many solutions in $x_0, \dots, x_n \in R$. This proves Theorem 1. ■

Proof of Corollary 2. Let m and n be positive integers with $m > 2n$, R a finitely generated extension ring of \mathbb{Z} in K and a_1, \dots, a_m an arithmetic progression of order n consisting of elements of R^* . We may assume without loss of generality that this arithmetic progression contains at least two different terms. We define

$$a_2 - a_1 = \Delta a_1, \quad a_3 - a_2 = \Delta a_2, \quad \dots, \quad a_m - a_{m-1} = \Delta a_{m-1}$$

and, recursively,

$$\Delta^l a_2 - \Delta^l a_1 = \Delta^{l+1} a_1, \quad \Delta^l a_3 - \Delta^l a_2 = \Delta^{l+1} a_2, \quad \dots$$

for $l = 1, \dots, n-1$. Set

$$f(X) = a_1 + \Delta a_1(X-1) + \frac{\Delta^2 a_1}{2!}(X-1)(X-2) + \dots + \frac{\Delta^n a_1}{n!}(X-1)\dots(X-n).$$

Then, as is known (see e.g. [24]), we have

$$a_i = f(i) \quad \text{for } i = 1, \dots, m.$$

By the assumptions made on the elements a_1, \dots, a_m , $Q(X) := n!f(X)$ is a non-constant polynomial of degree at most n with coefficients in R and $Q(i) \in n! \cdot R^*$ for $i = 1, \dots, m$. Our arithmetic progression is uniquely determined by $Q(X)$. Further, for proportional arithmetic progressions of order n in R^* , the corresponding polynomials $Q(X)$ differ only by a proportional factor from R^* . Hence Corollary 2 follows from Corollary 1 with the choice $a = n!$ and $r_i = i$ for $i = 1, \dots, m$. ■

REFERENCES

- [1] J. H. Evertse, I. Gaál and K. Györy, *On the numbers of solutions of decomposable polynomial equations*, Arch. Math. (Basel) 52 (1989), 337–353.
- [2] J. H. Evertse and K. Györy, *On unit equations and decomposable form equations*, J.Reine Angew. Math. 358 (1985), 6–19.
- [3] —, —, *Finiteness criteria for decomposable form equations*, Acta Arith. 50 (1988), 357–379.
- [4] —, —, *On the numbers of solutions of weighted unit equations*, Compositio Math. 66 (1988), 329–354.
- [5] —, —, *Lower bounds for resultants I*, to appear.
- [6] M. Fujiwara, *Some applications of a theorem of W. M. Schmidt*, Michigan Math. J. 19 (1972), 315–319.
- [7] K. Györy, *On arithmetic graphs associated with integral domains*, in: A Tribute to Paul Erdős, Cambridge Univ. Press, 1990, 207–222.

- [8] K. Györy, *On the numbers of families of solutions of systems of decomposable form equations*, Publ. Math. Debrecen 42 (1993), 65–101.
- [9] —, *On the number of pairs of polynomials with given resultant or given semi-resultant*, Acta Sci. Math., to appear.
- [10] —, *Some new results connected with resultants of polynomials and binary forms*, Grazer Math. Berichte 318 (1993), 17–27.
- [11] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.
- [12] M. Newman, *Units in arithmetic progression in an algebraic number field*, Proc. Amer. Math. Soc. 43 (1974), 266–268.
- [13] —, *Consecutive units*, ibid. 108 (1990), 303–306.
- [14] A. Pethő, *Application of Gröbner bases to the resolution of systems of norm equations*, in: Proc. ISSAC' 91, ACM Press, 1991, 144–150.
- [15] —, *Über kubische Ausnahmeeinheiten*, Arch. Math. (Basel) 60 (1993), 146–153.
- [16] —, *Systems of norm equations over cubic number fields*, Grazer Math. Berichte 318 (1993), 111–120.
- [17] H. P. Schlickewei, *Inequalities for decomposable forms*, Astérisque 41-42 (1977), 267–271.
- [18] —, *The p -adic Thue–Siegel–Roth–Schmidt theorem*, Arch. Math. (Basel) 29 (1977), 267–270.
- [19] —, *S -unit equations over number fields*, Invent. Math. 102 (1990), 95–107.
- [20] —, *The quantitative Subspace Theorem for number fields*, Compositio Math. 82 (1992), 245–273.
- [21] W. M. Schmidt, *Inequalities for resultants and for decomposable forms*, in: Diophantine Approximation and its Applications, Academic Press, New York 1973, 235–253.
- [22] —, *Simultaneous approximation to algebraic numbers by elements of a number field*, Monatsh. Math. 79 (1975), 55–66.
- [23] —, *The subspace theorem in diophantine approximations*, Compositio Math. 69 (1989), 121–173.
- [24] H. Weber, *Lehrbuch der Algebra*, Erster Band, Verlag Vieweg, Braunschweig 1898.
- [25] E. Wirsing, *On approximations of algebraic numbers by algebraic numbers of bounded degree*, in: Proc. Sympos. Pure Math. 20, Amer. Math. Soc., Providence 1971, 213–247.

INSTITUTE OF MATHEMATICS
LAJOS KOSSUTH UNIVERSITY
H-4010 DEBRECEN, HUNGARY

Reçu par la Rédaction le 1.2.1993