Write $p_r(n) = p(16n+r)$. Define k_r to be the smallest k for which $p_r(k)$ is odd. A table of k_r is given below:

r	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k_r	0	0	1	0	0	0	0	0	1	2	5	2	0	0	0	3

Next let l_r be given by the following table:

r	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
l_r	4	5	4	7	8	3	1	2	1	3	4	2	7	8	3	4

Suppose $p_r(n)$ is odd (alternatively even) for $n \geqslant n_0(r)$. We can suppose $n_0 \equiv l_r \pmod 9$ and that $2n_0+1 > k_r$.

Now let $N = N_r = (3n_0^2+n_0)/2+k_r$. Note that

$$16N+r \equiv 16\left((3l_r^2+l_r)/2+k_r\right)+r \equiv 2 \pmod 9, \quad \text{so} \quad c(16N+r) = 0.$$

It follows from (2.2) that, modulo 2,

$$p_r(N)+p_r(N-1)+p_r(N-2)+p_r(N-5)+p_r(N-7)+\ldots \ldots+p_r(n_0+k_r)+p_r(k_r) \equiv 0. \tag{2.3}$$

(The condition $2n_0+1 > k_r$ guarantees that $p_r(k_r)$ is indeed the last non-zero term on the left of (2.3).)

But the left hand side of (2.3) is odd (there is an odd number $(2n_0+1)$ of terms, the last is odd, the others are all odd (alternatively even)). So we have a contradiction, and our theorem is proved.

References

[1] M. D. Hirschhorn, *On the residue* mod 2 *and* mod 4 *of* $p(n)$, Acta Arith. 38 (1980), pp. 105–109.

[2] O. Kolberg, *Note on the parity of the partition function*, Math. Scand. 7 (1959), pp. 377–378.

[3] Morris Newman, *Advanced Problem No. 4944*, Amer. Math. Monthly 69 (1962), p. 175.

[4] M. V. Subbarao, *Some remarks on the partition function*, ibid. 73 (1966), pp. 851–854.

SCHOOL OF MATHEMATICS
UNIVERSITY OF NEW SOUTH WALES
Kensington, Australia, 2033

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ALBERTA
Edmonton, Canada, T6G 2G1

Received on 16.5.1986 (1637)

ACTA ARITHMETICA
L (1988)

Finiteness criteria for decomposable form equations

by

J. H. Evertse (Amsterdam) and K. Győry (Debrecen)

1. Introduction. Let K be a finitely generated extension field of $\mathbf{Q}$, and R a finitely generated extension ring of $\mathbf{Z}$ in K. Let $F(X_1, \ldots, X_m)$ be a form in $m \geqslant 2$ variables with coefficients in K, and suppose that F is *decomposable* (i.e. that it factorizes into linear factors over some finite extension, G say, of K). Let b be an element of K^*[1] and consider the *decomposable form equation*

$$F(x_1, \ldots, x_m) = b \quad \text{in} \quad x_1, \ldots, x_m \in R. \tag{1}$$

The decomposable form equations are of basic importance in the theory of diophantine equations and have many applications in algebraic number theory. Important classes of decomposable form equations are Thue equations (when $m = 2$), norm form equations, discriminant form equations and index form equations. The Thue equations are named after A. Thue [31] who proved in the case $K = \mathbf{Q}$, $R = \mathbf{Z}$, $m = 2$, that if F is a binary form having at least three pairwise linearly independent linear factors in its factorization over the field of algebraic numbers, then (1) has only finitely many solutions. After several generalizations, Lang [13] finally extended Thue's result to the general case considered above (when K is an arbitrary finitely generated extension of $\mathbf{Q}$ and R is an arbitrary finitely generated subring of K over $\mathbf{Z}$).

In the case that $K = \mathbf{Q}$, $R = \mathbf{Z}$, and F is a norm form, Schmidt [24] gave a necessary and sufficient condition for F such that (1) has only finitely many solutions for every $b \in \mathbf{Q}^*$. Later he generalized [25] this result by showing that all solutions of an arbitrary norm form equation over $\mathbf{Z}$ belong to finitely many families (cf. [25]) of solutions. These results of Schmidt were later extended by Schlickewei [20] to the case of arbitrary finitely generated subrings R of $\mathbf{Q}$ and by Laurent [14] to the above general case (when R is

[1] K^* denotes the set of non-zero elements of K. In general, for any integral domain R, R^* will denote the unit group (i.e. the multiplicative group of invertible elements) of R.

an arbitrary finitely generated subring of an arbitrary finitely generated field K over $\mathbf{Q}$).

For discriminant form equations and index form equations, Győry (cf. [3] in the case $K = \mathbf{Q}$, $R = \mathbf{Z}$ and [7], [8] in the general case) gave general (and effective) finiteness criteria by using Baker's method. These led to various applications in algebraic number theory (cf. Győry [4], [11]).

Under various restrictive conditions made for F and R, Schmidt [24], [26], [28], Schlickewei [21], [22], Győry and Papp [12], Győry [4], [5], [6], [7], [8], [9] and Evertse and Győry [2] obtained finiteness theorems also for certain other decomposable form equations.

In Section 2, we shall establish some general finiteness criteria for (1) and for some more general equations. Let $\mathscr{L}$ be a finite set of pairwise linearly independent linear forms from $G[X_1, \ldots, X_m]$ which contains a maximal set $\mathscr{L}_0$ of pairwise linearly independent linear factors of F over G. We give a necessary and sufficient condition (cf. Theorem 2), expressed in terms of K, G, $\mathscr{L}_0$ and $\mathscr{L}$ only, such that the equation

$$(2) \quad F(x_1, \ldots, x_m) = b \quad \text{in} \quad (x_1, \ldots, x_m) \in R^m \quad \text{with } l(x_1, \ldots, x_m) \neq 0 \text{ for all } l \in \mathscr{L}$$

has only finitely many solutions for every $b \in K^*$ and every finitely generated subring R of K. If in particular $\mathscr{L} = \mathscr{L}_0$, our result provides a finiteness criterion (cf. Theorem 1) for equation (1). Our general finiteness theorems concerning decomposable form equations imply (in an ineffective form) the previously mentioned finiteness results about Thue equations (cf. Corollary to Theorem 1), norm form equations (cf. Theorems 5, 6, 6'), discriminant form equations and index form equations.

The main tool in the proof of our finiteness theorems is the so-called *Theorem on unit equations* (cf. Section 4) which was proved independently by Evertse [1] (in the algebraic number field case) and by van der Poorten and Schlickewei [17] (in the general case). Its proof is based on the Schmidt–Schlickewei subspace theorem (cf. [23], [25], [27], [19]).

In case $G = K$, we shall state the finiteness condition of our finiteness criteria (Theorems 1, 2) concerning decomposable form equations in two different ways: one of them follows naturally from the Theorem on unit equations, and the other shows that this condition is effectively decidable, provided that K and the coefficients of the forms in $\mathscr{L}$ can be given explicitly (cf. Section 3). Using the latter formulation of our finiteness condition, we shall show (cf. Section 4) that the Theorem on unit equations is a consequence of our Theorem 2. Thus the finiteness assertion in our Theorem 2 on decomposable form equations is in fact equivalent to the Theorem on unit equations.

Section 5 is devoted to applications of our finiteness theorems on decomposable form equations to norm form equations. We give, as a consequence, another proof for the above-mentioned results of Schmidt [24], [25], Schlickewei [20] and Laurent [14] on norm form equations. The finiteness criteria of Győry [3], [8] concerning discriminant form and index form equations can also be deduced, in an ineffective form, from our Theorem 2. We shall not, however, deal with these applications, because these criteria followed in the same way from some earlier, less general (but effective or quantitative) versions (cf. [4], [8], [2]) of Theorem 2 concerning decomposable form equations.

Our results will be proved in Sections 6 to 8.

We thank the referee for calling our attention to some simplifications and necessary corrections in the manuscript.

2. General finiteness criteria. Before stating our results we have to introduce some notions from linear algebra. Let K be a finitely generated extension field of $\mathbf{Q}$, let G be a finite extension field of K, let m be a positive integer, let V be a non-zero subspace of the K-vector space K^m and let $\mathscr{L}$ be a finite set of linear forms in m variables with coefficients in G. A set of linear forms $\{l_1, \ldots, l_r\}$ with coefficients in G is called *linearly (in)dependent* on V if there are (no) $\alpha_1, \ldots, \alpha_r \in G$, not all 0, such that $\alpha_1 l_1 + \ldots + \alpha_r l_r = 0$ identically on V. The subspace V is said to be *$\mathscr{L}$-non-degenerate* or *$\mathscr{L}$-degenerate* according as $\mathscr{L}$ does or does not contain a subset of at least three linear forms which are linearly dependent on V, but pairwise linearly independent on V. In particular, V is $\mathscr{L}$-degenerate if V has dimension 1. We call V an *$\mathscr{L}$-admissible* subspace if no form in $\mathscr{L}$ is identically zero on V.

In the remaining part of Section 2 it will be supposed that $m \geqslant 2$ and that G is a normal extension of K. Let $F(X) = F(X_1, \ldots, X_m)$ be a decomposable form of degree $n \geqslant 2$ with coefficients in K, which factorizes into linear factors over G. Let $\mathscr{L}_0$ be a maximal set of pairwise linearly independent linear factors of F.

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

(1.1) *Every $\mathscr{L}_0$-admissible subspace of K^m of dimension $\geqslant 2$ is $\mathscr{L}_0$-non-degenerate;*

(1.2) *For every subring R of K which is finitely generated over $\mathbf{Z}$ and for every $b \in K^*$, the equation*

$$F(x) = b \quad \text{in} \quad x = (x_1, \ldots, x_m) \in R^m$$

has only finitely many solutions.

In the case $m = 2$ we immediately obtain the following result on Thue equations (see also Lang [13]).

COROLLARY. *Let $F_0(X_1, X_2)$ be a binary form with coefficients in K which factorizes into linear factors over G. Then the following statements are equivalent:*

(i) *F_0 has at least three pairwise linearly independent linear factors in $G[X_1, X_2]$;*

(ii) *For every subring R of K which is finitely generated over $\mathbf{Z}$ and for every $b \in K^*$, the equation*

$$F_0(x_1, x_2) = b \quad \text{in} \quad x_1, x_2 \in R$$

has only finitely many solutions.

We shall now state a few extensions of Theorem 1. Let K, G, F, $\mathscr{L}_0$ be as above and let now $\mathscr{L} \supseteq \mathscr{L}_0$ be a finite set of pairwise linearly independent linear forms in $X_1, \ldots, X_m$ with coefficients in G.

THEOREM 2. *The following two statements are equivalent:*

(2.1) *Every $\mathscr{L}$-admissible subspace of K^m of dimension $\geqslant 2$ is $\mathscr{L}_0$-non-degenerate;*

(2.2) *For every subring R of K which is finitely generated over $\mathbf{Z}$ and for every $b \in K^*$, the equation*

(2) $\quad F(x) = b \quad$ *in* $x = (x_1, \ldots, x_m) \in R^m$, $\quad$ *with* $l(x) \neq 0$ *for all* $l \in \mathscr{L}$

has only finitely many solutions.

Theorem 2 immediately implies Theorem 1, because all solutions x of (1) satisfy $l(x) \neq 0$ for all l in $\mathscr{L}_0$. Let R be a subring of K. The following result which deals with the equation

(2′) $\quad F(x) = \varepsilon \quad$ in $x = (x_1, \ldots, x_m) \in R^m$, $\quad \varepsilon \in R^*$ with $l(x) \neq 0$ for all $l \in \mathscr{L}$,

is in fact equivalent to Theorem 2. Two solutions (x_1, ε_1), (x_2, ε_2) of (2′) are called *linearly (in)dependent* if x_1, x_2 are linearly (in)dependent vectors in K^m. Notice that if (2′) is solvable and if R^* is infinite, then the solutions of (2′) can be divided into sets, each containing infinitely many pairwise linearly dependent solutions.

THEOREM 2′. *The following two statements are equivalent:*

(2′.1) *Every $\mathscr{L}$-admissible subspace of K^m of dimension $\geqslant 2$ is $\mathscr{L}_0$-non-degenerate;*

(2′.2) *For every subring R of K which is finitely generated over $\mathbf{Z}$, equation (2′) has at most finitely many pairwise linearly independent solutions.*

The statements (2.2), (2′.2) are in fact equivalent. (2′.2) follows from (2.2) by observing that R^* is finitely generated (cf. [18]), whence that the cosets in $R^*/(R^*)^n$ have a finite full set of representatives, $\mathscr{S}$ say. Since every solution (x, ε) of (2′) is linearly dependent on a solution (x', ε') with $\varepsilon' \in \mathscr{S}$, equation (2′) can be reduced to a finite number of equations of type (2). (2.2) follows from (2′.2) by taking in (2) $R[b, b^{-1}]$ instead of R and noticing that for

every solution x of (2) there are at most finitely many solutions x' linearly dependent on x; namely those solutions x' for which $x' = \varrho x$, where $\varrho^n = 1$ for some $\varrho \in K^*$.

Let V be a subspace of K^m. If V is $\mathscr{L}_0$-non-degenerate, then we denote by $S(V, \mathscr{L}_0)$ the smallest integer r such that $\mathscr{L}_0$ contains r forms which are linearly dependent on V but pairwise linearly independent on V. Thus for $\mathscr{L}_0$-non-degenerate V, $S(V, \mathscr{L}_0) \geqslant 3$. If V is $\mathscr{L}_0$-degenerate, we put $S(V, \mathscr{L}_0) = 2$. In [2] we stated without proof that statement (2′.1) implies statement (2′.2) (with (2′.1) replaced by the obviously equivalent condition that $S(V, \mathscr{L}_0) \geqslant 3$ for all $\mathscr{L}$-admissible subspaces V of K^m of dimension $\geqslant 2$). Moreover, under the restriction that $S(V, \mathscr{L}_0) = 3$ for all $\mathscr{L}$-admissible subspaces V of K^m of dimension $\geqslant 2$, we derived explicit upper bounds for the number of solutions of (2) and for the maximal number of pairwise linearly independent solutions of (2′). These upper bounds depend on the choice of the transcendence basis of K over $\mathbf{Q}$, as well as on R, b, the degree of F and the degree of G over K, but not on the coefficients of F. As a consequence of our results on decomposable form equations, we obtained in [2] explicit upper bounds of the same type for the numbers of solutions of Thue–Mahler equations, norm form equations from a restricted class, discriminant form equations, index form equations and power integral bases of algebraic number fields. We remark that effective versions of these quantitative finiteness assertions were earlier established by Győry [8], [9], [10].

The implications (2.1) $\rightarrow$(2.2), (2.2) $\rightarrow$(2.1) in Theorem 2 are easy consequences of Theorems 3, 4 stated below. Let K, G, F, $\mathscr{L}_0$, $\mathscr{L}$ have the same meaning as in Theorem 2.

THEOREM 3. *For every $b \in K^*$ and every subring R of K which is finitely generated over $\mathbf{Z}$, the solutions of (2) are contained in finitely many $\mathscr{L}$-admissible, $\mathscr{L}_0$-degenerate subspaces of K^m.*

The implication (2.1) $\rightarrow$(2.2) of Theorem 2 follows immediately from Theorem 3 by observing that every subspace of K^m of dimension 1 can contain only finitely many solutions of (2). The implication (2.2) $\rightarrow$(2.1) is immediate from the next theorem.

THEOREM 4. *For every $\mathscr{L}$-admissible, $\mathscr{L}_0$-degenerate subspace V of K^m of dimension $\geqslant 2$, there exist a $b \in K^*$ and a subring R of K which is finitely generated over $\mathbf{Z}$ for which (2) has infinitely many solutions contained in V.*

3. Decidability of conditions (1.1) and (2.1). The importance of Theorem 2 is that it relates a statement (cf. (2.2)) about the finiteness of the number of solutions of decomposable form equations to a condition (cf. (2.1)) which can be formulated in terms of linear algebra. The question arises if there exists an algorithm which decides in a finite number of steps whether condition (2.1) holds. The following proposition gives such an algorithm in case $G = K$,

provided that K and the coefficients of the forms in $\mathscr{L}$ are given in an appropriate form which will be detailed below. Recently we obtained such an algorithm without assuming $G = K$. We shall not describe it here.

For any system $\mathfrak{M}$ of linear forms with coefficients in K, let $\mathscr{V}(\mathfrak{M})$ denote the K-vector space generated by the forms of $\mathfrak{M}$. If $\mathscr{V}_1, \ldots, \mathscr{V}_r$ are K-vector spaces consisting of linear forms with coefficients in K, then $\sum_{i=1}^{r} \mathscr{V}_i$ denotes the smallest K-vector space containing $\mathscr{V}_1, \ldots, \mathscr{V}_r$.

PROPOSITION. *Let m, K, G, $\mathscr{L}_0$, $\mathscr{L}$ be the same as in Theorem 2, and suppose that $G = K$. Then the following two statements are equivalent:*

(i) *Every $\mathscr{L}$-admissible subspace of K^m of dimension $\geqslant 2$ is $\mathscr{L}_0$-non-degenerate;*

(ii) *The forms in $\mathscr{L}_0$ have rank m over K and for each proper non-empty subset $\mathscr{L}_1$ of $\mathscr{L}_0$*

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

In [8] and [10] it has been explained that every element of K can be represented by a finite tuple of integers once K satisfies certain conditions. For convenience of the reader, we shall shortly describe how these representations are established. The field K has a transcendence basis, say $\{z_1, \ldots, z_q\}$, over $\mathbf{Q}$, and can be written in the form $K = \mathbf{Q}(z_1, \ldots, z_q, y)$ where y is algebraic over $\mathbf{Q}(z_1, \ldots, z_q)$. We may assume without loss of generality that

$$y^d + f_1 y^{d-1} + \ldots + f_{d-1} y + f_d = 0,$$

where d denotes the degree of y over $\mathbf{Q}(z_1, \ldots, z_q)$ and $f_1, \ldots, f_d$ are polynomials in $\mathbf{Z}[z_1, \ldots, z_q]$. We call the tuple $(f_1, \ldots, f_d)$ an *effective representation of* K (relative to $\{z_1, \ldots, z_q\}$). Given such an effective representation of K, every element α of K has a unique representation (up to sign) in the form

$$\alpha = \frac{P_0 + P_1 y + \ldots + P_{d-1} y^{d-1}}{P_d} \tag{3}$$

where $P_0, \ldots, P_d$ are relatively prime polynomials from $\mathbf{Z}[z_1, \ldots, z_q]$. The tuple $(P_0, \ldots, P_d)$ is called an *effective representation of* α (relative to the effective representation of K considered above). If effective representations of K and α, $\beta \in K$ are given, then it is possible to compute effective representations of $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ and, if $\beta \neq 0$, α/β. For these and further remarks,

see [8], [10]. It is now clear that starting with effective representations of K and the coefficients of the forms in $\mathscr{L}$, one can decide whether statement (ii) of the Proposition is true. Therefore, in case $G = K$ the Proposition provides indeed an algorithm for deciding whether statement (2.1) of Theorem 2 holds.

4. Decomposable form equations and unit equations. Using the above Proposition, it is easy to deduce the following result as a consequence of Theorem 2'.

THEOREM ON UNIT EQUATIONS. *Let K be a finitely generated field of characteristic 0, Γ a finitely generated multiplicative subgroup of K^*, and $m \geqslant 2$ an integer. Then the equation*

$$x_1 + x_2 + \ldots + x_m = 1 \quad \text{in} \quad x_1, x_2, \ldots, x_m \in \Gamma$$

has at most finitely many solutions with the property that $x_{i_1} + x_{i_2} + \ldots + x_{i_s} \neq 0$ for each non-empty subset $\{i_1, \ldots, i_s\}$ of $\{1, \ldots, m\}$.

This theorem on unit equations can be obtained by applying Theorem 2' with $G = K$, $F(X) = X_1 X_2 \ldots X_m (X_1 + \ldots + X_m)$, $\mathscr{L}$ being the set of all linear forms of the type $X_{i_1} + \ldots + X_{i_s}$ where $\{i_1, \ldots, i_s\}$ is a non-empty subset of $\{1, \ldots, m\}$. It is easy to verify that condition (ii) of the Proposition is satisfied for this $\mathscr{L}$ and for $\mathscr{L}_0 = \{X_1, \ldots, X_m, X_1 + \ldots + X_m\}$. Indeed, rank $\mathscr{L}_0 = m$ over K and for each proper, non-empty subset $\mathscr{L}_1$ of $\mathscr{L}_0$, $\mathscr{V}(\mathscr{L}_1) \cap \mathscr{V}(\mathscr{L}_0 \setminus \mathscr{L}_1) \cap \mathscr{L}$ always contains either the sum of the forms in $\mathscr{L}_1$ or the sum of the forms in $\mathscr{L}_0 \setminus \mathscr{L}_1$. The subring R of K, generated by the elements of Γ, is finitely generated over $\mathbf{Z}$, and Theorem 2' together with the Proposition above imply that the equation

$$x_1 x_2 \ldots x_m (x_1 + \ldots + x_m) = \varepsilon \text{ in } x = (x_1, \ldots, x_m) \in R^m, \ \varepsilon \in R^*$$

$$\text{with } l(\mathbf{x}) \neq 0 \text{ for all } l \in \mathscr{L}$$

has at most finitely many pairwise linearly independent solutions. Since $\Gamma \subseteq R^*$, this proves the Theorem on unit equations.

The theorem on unit equations has been proved by Evertse [1] in case that K is an algebraic number field and by van der Poorten and Schlickewei [17] in general. We shall prove our Theorem 3 as a consequence of the Theorem on unit equations. Hence the above arguments show that the Theorem on unit equations, Theorem 3, the implication (2.1) $\rightarrow$ (2.2) of Theorem 2 and the implication (2'.1) $\rightarrow$ (2'.2) of Theorem 2' are equivalent statements. We mention that, for $m = 2$, the equivalence of the Theorem on unit equations (in two variables) and the implication (i) $\rightarrow$ (ii) of the Corollary to Theorem 1 follow easily from observations made by Siegel in his paper [30].

5. Applications to norm form equations. Let K be a finitely generated extension of $\mathbf{Q}$, M a finite extension of K of degree $n \geqslant 2$ and G a finite, normal extension of K containing M. There are n distinct K-isomorphisms of M into G, $\sigma_1, \ldots, \sigma_n$ say. Let $\alpha_1, \ldots, \alpha_m$ ($m \geqslant 2$) be elements of M which are linearly independent over K and consider the linear form $l(X) = \alpha_1 X_1 + \ldots + \alpha_m X_m$. For $i = 1, \ldots, n$, we put $l^{(i)}(X) = \sigma_i(\alpha_1) X_1 + \ldots + \sigma_i(\alpha_m) X_m$. Then

$$N(\alpha_1 X_1 + \ldots + \alpha_m X_m) = \prod_{i=1}^{n} l^{(i)}(X)$$

is a norm form with coefficients in K. Let $\mathscr{V}$ be the K-vector space generated by $\alpha_1, \ldots, \alpha_m$ in M. We say that $\mathscr{V}$ is *degenerate* if there exist a $\mu \in M^*$ and an intermediate field M' with $K \subsetneqq M' \subseteqq M$ such that $\mu M' \subseteqq \mathscr{V}$. We shall now deal with the norm form equation

$$N(\alpha_1 x_1 + \ldots + \alpha_m x_m) = b \quad \text{in} \quad x_1, \ldots, x_m \in R, \tag{4}$$

where $b \in K^*$ and R is a finitely generated subring of K over $\mathbf{Z}$. For $K = \mathbf{Q}$, $R = \mathbf{Z}$, Schmidt [24] proved that (4) has at most finitely many solutions for all $b \in \mathbf{Q}^*$ if and only if $\mathscr{V}$ has no a subspace of the form $\mu M'$, where $\mu \in M^*$ and M' is a subfield of M different from $\mathbf{Q}$ and the imaginary quadratic number fields. An easy consequence of Corollary 1.1 of Schlickewei [20] is that in case $K = \mathbf{Q}$, (4) has at most finitely many solutions for all $b \in \mathbf{Q}^*$ and all finitely generated subrings R of $\mathbf{Q}$ over $\mathbf{Z}$ if and only if $\mathscr{V}$ is non-degenerate. Laurent [14] extended Schlickewei's results [20] to the case when K is an arbitrary finitely generated extension of $\mathbf{Q}$ and R is an arbitrary subring of K which is finitely generated over $\mathbf{Z}$.

We shall derive Theorem 5 below, due to Laurent [14], from our Theorem 2. We remark that Theorem 5 was earlier claimed without proof in our paper [2], p. 13.

THEOREM 5. *The following two statements are equivalent:*

(5.1) *$\mathscr{V}$ is non-degenerate;*

(5.2) *For all $b \in K^*$ and all subrings R of K which are finitely generated over $\mathbf{Z}$, equation (4) has only finitely many solutions.*

One can assume without loss of generality that $\alpha_1 = 1$ and that $M = K(\alpha_2, \ldots, \alpha_m)$ when $l^{(1)}, \ldots, l^{(n)}$ are pairwise linearly independent. We shall derive Theorem 5 from Theorem 2 by showing that for $\mathscr{L}_0 = \{l^{(1)}, \ldots, l^{(n)}\}$, the $\mathscr{L}_0$-admissible, $\mathscr{L}_0$-degenerate subspaces of K^m are exactly those subspaces V of K^m for which

$$l(V) = \{l(\mathbf{x}) : \mathbf{x} \in V\} = \mu M' \tag{5}$$

for some $\mu \in M^*$ and an intermediate field M' with $K \subseteqq M' \subseteqq M$ such that $\mu M' \subseteqq l(K^m) = \mathscr{V}$. Since here $\dim V = 1$ if and only if $M' = K$, statement (5.1) is equivalent to statement (2.1) with $\mathscr{L}_0 = \mathscr{L} = \{l^{(1)}, \ldots, l^{(n)}\}$.

Using Theorem 3, one can show that the solutions of (4) are contained in finitely many subspaces V of K^m of the type (5). We shall derive a more general result from Theorem 3. Suppose that K and M have the same meaning as above. Let R be a subring of K which is finitely generated over $\mathbf{Z}$ and has K as its quotient field. Let $\mathfrak{M}$ be a finitely generated R-module contained in M. Let $\mathscr{V}$ be the K-vector space in M generated by the elements of $\mathfrak{M}$. For any intermediate field M' with $K \subseteqq M' \subseteqq M$, let $R_{M'}$ denote the integral closure of R in M' and $U_{M'}$ the multiplicative group of elements ε of $R_{M'}^*$ with $N_{M'/K}(\varepsilon) = 1$.

THEOREM 6. *For every $b \in K^*$, the set of solutions of the equation*

$$N_{M/K}(\mu) = b \quad \text{in} \quad \mu \in \mathfrak{M} \tag{6}$$

is the union of finitely many sets of the type $(\mu' U_{M'}) \cap \mathfrak{M}$ where μ' is a solution of (6) and M' is a field with $K \subseteqq M' \subseteqq M$, $\mu' M' \subseteqq \mathscr{V}$.

If the vector space $\mathscr{V}$ generated by the elements of $\mathfrak{M}$ in M is non-degenerate then, by Theorem 6, all solutions of (6) are contained in finitely many sets of the form $(\mu' U_K) \cap \mathfrak{M} = (\mu' \{1\}) \cap \mathfrak{M} = \{\mu'\}$, i.e. (6) has only finitely many solutions. Thus the implication (5.1) $\rightarrow$ (5.2) of Theorem 5 follows at once from Theorem 6.

Laurent [14], Th. 8, proved the following generalization of Theorem 6 which is in fact equivalent to Theorem 6. For any subgroup E of R^*, $U_{M',E}$ denotes the multiplicative group of elements ε of $R_{M'}^*$ with $N_{M'/K}(\varepsilon) \in E$.

THEOREM 6'. *For every $b \in K^*$ and every subgroup E of R^*, the set of solutions μ of the equation*

$$N_{M/K}(\mu) = \nu b \quad \text{in} \quad \mu \in \mathfrak{M},\ \nu \in E, \tag{6'}$$

is the union of finitely many sets of the type $(\mu' U_{M',E}) \cap \mathfrak{M}$, where μ' is a solution of (6') and M' is a field with $K \subseteqq M' \subseteqq M$, $\mu' M' \subseteqq \mathscr{V}$.

Theorem 6 follows from Theorem 6' by taking $E = \{1\}$. Theorem 6' follows from Theorem 6 by observing that E/E^n is finite, whence that (6') can be reduced to a finite number of equations of type (6), and that $U_{M'} \subseteqq U_{M',E}$. As Laurent pointed out (cf. [14], Th. 9), in the case $K = \mathbf{Q}$ Theorem 6' implies the classical results of Schmidt [25], Th. 1 (see also [28], Ch. 7, Th. 4B) and Schlickewei [20], Th. 1.2, on the finiteness of the number of families of solutions of norm form equations. We remark that Laurent [14] obtained Theorem 6' in another way, as a consequence of his general finiteness theorem concerning intersections of a subvariety of a linear torus $\mathscr{G}$ with subgroups of finite rank of $\mathscr{G}$.

6. Proofs of Theorems 3 and 4. In the proof of Theorem 3 we shall need the following consequence of the Theorem on unit equations.

LEMMA 1. *Let K be a finitely generated field of characteristic 0, let Γ be a finitely generated multiplicative subgroup of K^*; and let $t \geqslant 2$ be an integer. Then the solutions of the equation*

$$x_1 + \ldots + x_t = 1 \quad \text{in} \quad (x_1, \ldots, x_t) \in \Gamma^t \tag{7}$$

are contained in finitely many proper subspaces of K^t.

Proof. The solutions of (7) having some non-zero subsum obviously belong to finitely many proper subspaces of K^t. Further, by the Theorem on unit equations (cf. Section 4), the solutions of (7) with no non-zero subsum, being finite in number, are also contained in finitely many proper subspaces of K^t. This proves Lemma 1. ∎

Let K, G, F, m, $\mathscr{L}_0$, $\mathscr{L}$ have the same meaning as in Theorem 2. Let $b \in K^*$ and let R be a subring of K finitely generated over $\mathbf{Z}$. Theorem 3 follows immediately from the next lemma by taking $W = K^m$.

LEMMA 2. *For every subspace W of K^m, the solutions of equation (2) belonging to $R^m \cap W$ are contained in at most finitely many $\mathscr{L}$-admissible, $\mathscr{L}_0$-degenerate subspaces of W.*

Proof. We shall prove Lemma 2 by induction on $r = \dim W$. The case $r = 1$ is trivial. Suppose that Lemma 2 is true for all $r < p$, where $p \geqslant 2$ (induction hypothesis), and let W be a subspace of K^m of dimension p. If W is $\mathscr{L}_0$-degenerate, then there is nothing to prove. So suppose that W is $\mathscr{L}_0$-non-degenerate, and that equation (2) has a solution in W. Then there exist linear forms $l_0, l_1, \ldots, l_t$ in $\mathscr{L}_0$ which are pairwise linearly independent on W such that

$$\sum_{i=0}^{t} c_i l_i(X) = 0 \quad \text{identically on } W$$

for some $c_0, c_1, \ldots, c_t \in G^*$. Let t be the smallest integer with this property. Since by assumption W is $\mathscr{L}_0$-non-degenerate, we have $t \geqslant 2$. Every solution $x \in R^m \cap W$ of (2) satisfies

$$\sum_{i=1}^{t} \left(-\frac{c_i l_i(x)}{c_0 l_0(x)} \right) = 1. \tag{8}$$

Let Γ be the unit group of the smallest extension ring of R which contains b, the c_i, their inverses as well as all the coefficients of the linear factors of F. Since this extension ring is finitely generated, Γ is also finitely generated. Further, for every solution $x \in R^m \cap W$ of (2), the numbers $c_i l_i(x)/c_0 l_0(x)$ belong to Γ. Hence, by (8) and Lemma 1, the vectors

$$(-c_1 l_1(x)/c_0 l_0(x), \ldots, -c_t l_t(x)/c_0 l_0(x))$$

belong to finitely many proper subspaces of G^t. If $\hat{V}$ is such a subspace of G^t and if $(-c_1 l_1(x)/c_0 l_0(x), \ldots, -c_t l_t(x)/c_0 l_0(x)) \in \hat{V}$ then there are $d_i \in G$, not all zero, such that

$$\sum_{i=1}^{t} d_i \frac{c_i l_i(x)}{c_0 l_0(x)} = 0,$$

whence

$$\sum_{i=1}^{t} (d_i c_i) l_i(x) = 0. \tag{9}$$

But by the minimality of t, $\sum_{i=1}^{t} (d_i c_i) l_i(X)$ is not identically zero on W. Hence the $x \in W$ satisfying (9) belong to a proper subspace of W. This shows that the solutions of (2) in $R^m \cap W$ are already contained in at most finitely many proper subspaces of W. Together with the induction hypothesis this completes the proof of Lemma 2. ∎

Proof of Theorem 4. K, G, F, $\mathscr{L}_0$, $\mathscr{L}$ will have the same meaning as in Theorem 4. Let V be an $\mathscr{L}$-admissible, $\mathscr{L}_0$-degenerate subspace of K^m of dimension $\geqslant 2$. It will be enough to prove Theorem 4 in the special case $V = K^m$ (with $m \geqslant 2$) and $l(\mathbf{e}_1) \neq 0$ for all $l \in \mathscr{L}$ where $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in K^m$ with a 1 on the ith place. Indeed, suppose that $\dim V = r \leqslant m$. Then there exists an $\mathbf{a} \in V$ with $l(\mathbf{a}) \neq 0$ for all l in $\mathscr{L}$ and a bijective linear mapping $A\colon K^r \to V$ such that $A(\mathbf{e}'_1) = \mathbf{a}$, where now $\mathbf{e}'_1 = (1, 0, \ldots, 0) \in K^r$. Let

$$\mathscr{L}'_0 = \{l(A\tilde{X})\colon l \in \mathscr{L}_0\}, \qquad \mathscr{L}' = \{l(A\tilde{X})\colon l \in \mathscr{L}\}$$

(with $\tilde{X}$ being an abbreviation for $(X_1, \ldots, X_r)$) and $F'(\tilde{X}) = F(A\tilde{X})$. Now K^r is $\mathscr{L}'_0$-degenerate and $l'(\mathbf{e}'_1) \neq 0$ for all l' in $\mathscr{L}'$. If the equation

$$F'(\tilde{x}) = b \quad \text{in } \tilde{x} \in R^r \quad \text{with} \quad l'(\tilde{x}) \neq 0 \text{ for all } l' \text{ in } \mathscr{L}'$$

has infinitely many solutions for some $b \in K^*$ and some finitely generated subring R of K over $\mathbf{Z}$, then it follows at once that (2) has infinitely many solutions in $x \in R^m \cap V$, provided that R contains the entries of the matrix of A.

Henceforth we shall assume that K^m (with $m \geqslant 2$) is $\mathscr{L}_0$-degenerate and that $l(\mathbf{e}_1) \neq 0$ for all l in $\mathscr{L}$. Then

$$F(X) = b_0 F_1(X)^{a_1} \ldots F_t(X)^{a_t} \tag{10}$$

where $F_1, \dots, F_t$ are irreducible decomposable forms in $K[X]$ with $F_i(e_1) = 1$ and $a_i \in N$ for $i = 1, \dots, t$, and $b_0 \in K^*$. We may assume without loss of generality that all forms l in $\mathscr{L}$ satisfy $l(e_1) = 1$. Let $l_1^*, \dots, l_t^*$ be linear factors of $F_1, \dots, F_t$, respectively, belonging to $\mathscr{L}_0$ and let K_i be the smallest extension of K containing the coefficients of l_i^*, $i = 1, \dots, t$. Then we have $\deg F_i = [K_i : K]$ for $i = 1, \dots, t$. Put $[K_i : K] = r_i$ and suppose that $r_1 \geqslant r_2 \geqslant \dots \geqslant r_t$. Let $r = r_1 + r_2 + \dots + r_t$. For $1 \leqslant i \leqslant t$ and $1 \leqslant j \leqslant r_i$ we denote by $\langle i, j \rangle$ the integer $r_1 + r_2 + \dots + r_{i-1} + j$ if $i \geqslant 2$, and j if $i = 1$. For $1 \leqslant i \leqslant t$, let $\sigma_{i1}, \dots, \sigma_{i,r_i}$ be the distinct K-isomorphisms of K_i in G. Let $l_1, \dots, l_r$ be the forms in $\mathscr{L}_0$ and suppose that these forms are ordered such that $l_{\langle i,j \rangle} = \sigma_{ij}(l_i^*)$. We call a vector $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_r) \in G^r$ *admissible* if there are $\alpha_1^* \in K_1, \dots, \alpha_t^* \in K_t$ such that $\alpha_{\langle i,j \rangle} = \sigma_{ij}(\alpha_i^*)$ for $1 \leqslant i \leqslant t$, $1 \leqslant j \leqslant r_i$. Then for $k = 1, \dots, m$, the vectors $(l_1(e_k), \dots, l_r(e_k))$ are admissible. For $1 \leqslant i \leqslant t$, let $\{\omega_{i1}, \dots, \omega_{i,r_i}\}$ be a K-basis of K_i and let the $r \times r$ matrix Ω be defined by

$$\Omega = \begin{bmatrix} \Omega_1 & & 0 \\ & \Omega_2 & \\ & & \ddots \\ 0 & & \Omega_t \end{bmatrix}$$

where, for $1 \leqslant i \leqslant t$, Ω_i is the $r_i \times r_i$ matrix given by

$$\Omega_i = \begin{bmatrix} \sigma_{i1}(\omega_{i1}) & \dots & \sigma_{i1}(\omega_{i,r_i}) \\ \dots\dots & \dots & \dots\dots \\ \sigma_{i,r_i}(\omega_{i1}) & \dots & \sigma_{i,r_i}(\omega_{i,r_i}) \end{bmatrix}.$$

It is easy to see that

(11) $\qquad \boldsymbol{\alpha} \in G^r$ admissible $\Leftrightarrow \boldsymbol{\alpha}^{\mathrm{T}} = \Omega \boldsymbol{\beta}^{\mathrm{T}}$ (2) for some $\boldsymbol{\beta} \in K^r$.

Let Λ be the $r \times m$ matrix

$$\begin{bmatrix} l_1(e_1) & \dots & l_1(e_m) \\ \dots\dots & \dots & \dots\dots \\ l_r(e_1) & \dots & l_r(e_m) \end{bmatrix}.$$

Then there exists an $r \times m$ matrix M, with entries in K, such that

(12) $\qquad \Lambda = \Omega M.$

We are now in a position to prove our theorem under the restrictions we made before, namely that $V = K^m$ and that $l(e_1) = 1$ for all l in $\mathscr{L}$. $\mathscr{L}_0$ contains exactly r pairwise linearly independent linear forms. By the assumption that K^m is $\mathscr{L}_0$-degenerate, these forms are linearly independent. Hence $r \leqslant m$. We distinguish two cases:

(2) We denote by B^{T} the transposed matrix of a matrix B.

First suppose that $r < m$. Then there exists a vector $y \in K^m \setminus \{0\}$ with $My^{\mathrm{T}} = \mathbf{0}$. By (12) we have $\Lambda y^{\mathrm{T}} = \mathbf{0}$, whence $l_i(y) = 0$ for $i = 1, \dots, r$. Put $x_\lambda = e_1 + \lambda y$ for all $\lambda \in N$. It follows from (10) that

$$F(x_\lambda) = F(e_1) = b_0 \quad \text{for all } \lambda \in N.$$

Further, there are only finitely many λ in N such that

$$l(x_\lambda) = l(e_1) + \lambda l(y) \neq 0 \quad \text{for some } l \in \mathscr{L}.$$

This proves our theorem with $b = b_0$ and R being the ring generated by the coordinates of y over $\boldsymbol{Z}$.

Suppose now that $r = m$. For any integer i with $1 \leqslant i \leqslant t$ and $r_i \geqslant 2$ there is an $\eta_i \in K_i^*$ such that $N_{K_i/K}(\eta_i) = 1$ and that $\sigma_{ij}(\eta_i)/\sigma_{ij'}(\eta_i)$ is not a root of unity for $j, j' \in \{1, \dots, r_i\}$ with $j \neq j'$. Indeed, choose $\eta_i' \in K_i$ such that $K_i = K(\eta_i')$. Let w be the number of roots of unity in G and let s be an integer with $s \geqslant w r_i^2$. Suppose that for each v in $\{0, 1, \dots, s\}$ there are $j, j' \in \{1, \dots, r_i\}$ with $j \neq j'$ and a root of unity ϱ in G such that

$$\sigma_{ij}(\eta_i' + v)/\sigma_{ij'}(\eta_i' + v) = \varrho.$$

By our choice of s, there are v_1, v_2 in $\{0, 1, \dots, s\}$ with $v_1 \neq v_2$ and j, j' in $\{1, \dots, r_i\}$ with $j \neq j'$ such that

$$\sigma_{ij}(\eta_i' + v_1)/\sigma_{ij'}(\eta_i' + v_1) = \sigma_{ij}(\eta_i' + v_2)/\sigma_{ij'}(\eta_i' + v_2).$$

This implies that $\sigma_{ij}(\eta_i') = \sigma_{ij'}(\eta_i')$ which contradicts our choice of η_i'. Hence there is an element η_{0i} in K_i such that $\sigma_{ij}(\eta_{0i})/\sigma_{ij'}(\eta_{0i})$ is not a root of unity for j, j' in $\{1, \dots, r_i\}$ with $j \neq j'$. It is now obvious that $\eta_i = \eta_{0i}^{r_i}/N_{K_i/K}(\eta_{0i})$ satisfies the required conditions.

Let $t_0 \geqslant 0$ be the greatest integer for which $r_{t_0} \geqslant 2$. If $t_0 < t-1$, then there are pairwise distinct rational integers $h_{t_0+1}, \dots, h_t$ such that

$$\sum_{l=t_0+1}^{t} a_l h_l = 0. \tag{13}$$

(For instance, we may take $h_l = a_t \cdot l$ for $l = t_0+1, \dots, t-1$ and $h_t = -\sum_{l=t_0+1}^{t-1} a_l \cdot l$). Take $\xi \in K^*$ such that ξ is not a root of unity. It is easily seen that there are non-zero rational integers $h_1, \dots, h_{t_0}$ such that if we define $\xi_1, \dots, \xi_m$ by

$$\xi_{\langle i,j \rangle} = \begin{cases} (\sigma_{ij}(\eta_i))^{h_i} & \text{for } i \leqslant t_0 \text{ and } j = 1, \dots, r_i; \\ \xi^{h_i} & \text{for } i > t_0 \text{ and } j = 1 \text{ if } t_0 < t-1; \\ 1 & \text{for } i > t_0 \text{ and } j = 1 \text{ if } t_0 = t-1, \end{cases}$$

then ξ_p/ξ_q is not a root of unity for $p, q \in \{1, \dots, m\}$ with $p \neq q$.

Let now $\alpha_{p\lambda} = \xi_p^\lambda$ for $p = 1, \dots, m$ and $\lambda = 1, 2, \dots$ Then the vectors $\boldsymbol{\alpha}_\lambda = (\alpha_{1\lambda}, \dots, \alpha_{m\lambda})$ are admissible and pairwise distinct. Since $r = m$, the matrix

A is invertible. Hence for every $\lambda \in N$, there exists a unique $x_\lambda \in G^m$ such that

$$A x_\lambda^T = \alpha_\lambda^T. \tag{14}$$

Further, by (11) there exists a $\beta_\lambda \in K^m$ such that $\alpha_\lambda^T = \Omega \beta_\lambda^T$. This together with (12) shows that

$$M x_\lambda^T = \beta_\lambda^T.$$

Hence $x_\lambda \in K^m$. Moreover, $x_\lambda \in R'^m$, where R' denotes the ring generated by the entries of A^{-1} and by the coordinates of the vectors α_λ ($\lambda \in N$). The ring R' is obviously finitely generated over $\mathbf{Z}$. Hence there exists a ring $R \subset K$, containing $R' \cap K$, which is finitely generated over $\mathbf{Z}$. Thus $x_\lambda \in R^m$ for $\lambda \in N$, and, by (14), the x_λ are pairwise distinct. By (13) we have

$$\prod_{i=1}^{t} \prod_{j=1}^{r_i} \alpha_{\langle i,j \rangle, \lambda}^{a_i} = 1 \quad \text{for all } \lambda \in N$$

which together with (10) and (13) implies

$$F(x_\lambda) = b_0 \quad \text{for all } \lambda \in N.$$

We shall now show that for all but finitely many λ, $l(x_\lambda) \neq 0$ for all l in $\mathscr{L}$. Let $l \in \mathscr{L}$. Since $l_1, \ldots, l_m$ are linearly independent, there are $c_1, \ldots, c_m \in G$, at least two of which are different from zero, such that

$$l(X) = \sum_{p=1}^{m} c_p l_p(X) \quad \text{identically in } X = (X_1, \ldots, X_m).$$

Suppose $l(x_\lambda) = 0$. Then

$$\sum_{p=1}^{m} c_p \alpha_{p\lambda} = 0. \tag{15}$$

We recall that $\alpha_{p\lambda} = \xi_p^\lambda$ for $p = 1, \ldots, m$ and that ξ_p/ξ_q is not a root of unity for $p, q \in \{1, \ldots, m\}$ with $p \neq q$. Putting now $u_\lambda = \sum_{p=1}^{m} c_p \xi_p^\lambda$ for $\lambda \in N$, (15) can be written as

$$u_\lambda = 0. \tag{16}$$

The sequence $\{u_\lambda\}_{\lambda \in N}$ is however a non-degenerate, homogeneous, linear recurrence sequence (cf. [29]). As a consequence of the Skolem–Mahler–Lech theorem (cf. [15], [29]), (16) has only finitely many solutions in $\lambda \in N$. This shows indeed that $l(x_\lambda) \neq 0$ for all but finitely many $\lambda \in N$. By repeating the above argument for each l in $\mathscr{L}$, one completes the proof of the theorem. ∎

7. Proofs of Theorems 5 and 6. Let K be a finitely generated extension of $\mathbf{Q}$, M a finite extension of K of degree $n \geq 2$ and G a finite, normal extension of K which contains M. By $l(X)$ we shall denote the form $\alpha_1 X_1 + \ldots + \alpha_m X_m$ where $2 \leq m \leq n$ and $\alpha_1 = 1, \alpha_2, \ldots, \alpha_m$ are K-linearly independent elements of M such that $M = K(\alpha_2, \ldots, \alpha_m)$. Let $\sigma_1, \ldots, \sigma_n$ be the K-isomorphisms of M in G and put $l^{(i)}(X) = \sigma_i(\alpha_1) X_1 + \ldots + \sigma_i(\alpha_m) X_m$ for $i = 1, \ldots, n$. Finally, let $\mathscr{L}_0 = \{l^{(1)}, \ldots, l^{(n)}\}$. As we already observed after the statement of Theorem 5, Theorem 5 follows at once from Theorem 2 and Lemma 3 below.

LEMMA 3. *Let V be a subspace of K^m with $V \neq (0)$. Then the following two statements are equivalent:*

(i) *V is $\mathscr{L}_0$-admissible and $\mathscr{L}_0$-degenerate;*

(ii) *$l(V) = \mu M'$ for some $\mu \in l(V) \setminus \{0\}$ and some field M' with $K \subseteq M' \subseteq M$.*

Proof. First we shall prove the implication (i) → (ii). Let V be an $\mathscr{L}_0$-admissible, $\mathscr{L}_0$-degenerate subspace of K^m and choose $\mu \in l(V)$ with $\mu \neq 0$. Put $W' = l(V)$ and $W = \mu^{-1} l(V)$. Then both W and W' are vector spaces over K. Further, $1 \in W$ and W, W' have the same dimension over K which will be denoted by p. Let $M' \supseteq K$ be the smallest subfield of M containing W, and let $[M' : K] = q$. Then $q \geq p$. The vector space W has a basis of the form $\{\omega_1 = 1, \omega_2, \ldots, \omega_p\}$ over K. Let $L(Y) = \omega_1 Y_1 + \ldots + \omega_p Y_p$ and put $L^{(i)}(Y) = \sum_{j=1}^{p} \sigma_i(\omega_j) Y_j$ for $i = 1, \ldots, n$. Among these linear forms there exist q pairwise linearly independent forms, $L^{(1)}, \ldots, L^{(q)}$ say, such that any other form $L^{(j)}$ with $j > q$ is linearly dependent on one of the forms in $\mathscr{L}_0' = \{L^{(1)}, \ldots, L^{(q)}\}$. It follows from (i) that K^p is $\mathscr{L}_0'$-admissible and $\mathscr{L}_0'$-degenerate. Therefore $L^{(1)}, \ldots, L^{(q)}$ are linearly independent. This implies however that $q \leq p$ and hence that $q = p$. Consequently, $M' = W$ and so $l(V) = \mu M'$ which proves (ii).

We shall now show that (ii) → (i). Suppose that $l(V) = \mu M'$ for some $\mu \in l(V)$ with $\mu \neq 0$ and some field M' with $K \subseteq M' \subseteq M$. Then V is $\mathscr{L}_0$-admissible. We shall prove that V is $\mathscr{L}_0$-degenerate. Let $q = [M' : K]$. We rearrange the K-isomorphisms of M in G such that the distinct K-isomorphisms of M' in G are exactly the restrictions of $\sigma_1, \ldots, \sigma_q$ to M', respectively, while for $q+1 \leq i \leq n$, the restriction of σ_i to M' is equal to one of the restrictions of $\sigma_1, \ldots, \sigma_q$ to M'. Hence for $q+1 \leq i \leq n$, $l^{(i)}$ is linearly dependent on one of the forms $l^{(1)}, \ldots, l^{(q)}$ on V. The forms $l^{(1)}, \ldots, l^{(q)}$ are linearly independent on V. For suppose that there are elements $\beta_1, \ldots, \beta_q$ in G, not all zero, such that $\beta_1 l^{(1)} + \ldots + \beta_q l^{(q)}$ is identically zero on V. Then, with $\beta_i' = \beta_i \sigma_i(\mu)$ $(i = 1, \ldots, q)$,

$$\beta_1' \sigma_1(\xi) + \ldots + \beta_q' \sigma_q(\xi) = 0 \quad \text{for all } \xi \in M'.$$

This implies however that for any K-basis $\{\omega_1, \ldots, \omega_q\}$ of M', the determinant of the matrix $(\sigma_i(\omega_j))$ is 0 which is impossible. It follows that V is $\mathscr{L}_0$-degenerate. This completes the proof of (i). ∎

We shall now derive Theorem 6 from Theorem 3 and Lemmas 3, 4. Let R be a subring of K which is finitely generated over $\mathbf{Z}$ and has K as its quotient field. Let $\mathfrak{M} \subset M$ be a finitely generated R-module. Let $\mathscr{V}$ be the K-vector space generated by the elements of $\mathfrak{M}$. Then $\mathscr{V}$ has a K-basis $\{\alpha_1, \ldots, \alpha_m\}$ such that $\mathfrak{M} \subseteq \mathfrak{M}' = R\alpha_1 + \ldots + R\alpha_m$. This can be seen by taking a set of generators of $\mathfrak{M}$ over R, $\beta_1, \ldots, \beta_{m'}$ say, and finding a set of K-linearly independent elements $\alpha_1, \ldots, \alpha_m$ of $\mathscr{V}$ such that the β_i can be expressed as linear combinations in the α_i with coefficients in R. We may suppose without loss of generality that $\alpha_1 = 1$. For $m = 1$ Theorem 6 trivially holds with $M' = K$, hence it suffices to consider the case $m \geqslant 2$. Further, we may assume that $M = K(\alpha_2, \ldots, \alpha_m)$. The solutions of the equation

$$N_{M/K}(\mu) = b \tag{6}$$

in $\mu \in \mathfrak{M}'$ are, by Theorem 3 and Lemma 3, contained in at most finitely many sets of the form $\mu_0 M'$, where $0 \neq \mu_0 \in \mathfrak{M}'$ and M' is a field with $K \subseteq M' \subseteq M$ such that $\mu_0 M' \subseteq \mathscr{V}$. But then the same finiteness assertion holds for all solutions $\mu \in \mathfrak{M}$ of (6) with $0 \neq \mu_0 \in \mathfrak{M}$ which are now solutions of (6). Therefore it suffices to show that for every set $\mu_0 M'$ of the type just mentioned, the solutions of (6) in $\mu_0 M' \cap \mathfrak{M}$ are contained in finitely many sets of the type $(\mu' U_{M'}) \cap \mathfrak{M}$, where μ' is a solution of (6) in $\mathfrak{M}$ and $U_{M'}$ is the multiplicative group of units ε in the integral closure $R_{M'}$ of R in M' with $N_{M'/K}(\varepsilon) = 1$. If now $\mu \in \mu_0 M' \cap \mathfrak{M}$ is a solution of (6), then $\mu_0^{-1}\mu \in M' \cap \mu_0^{-1}\mathfrak{M}$ and $N_{M'/K}(\mu_0^{-1}\mu)$ is equal to one of the dth roots of $N_{M/K}(\mu_0)^{-1} b$, where $d = [M : M']$. Hence the assertion follows from the following lemma with the choice $\mathfrak{M}' = M' \cap \mu_0^{-1}\mathfrak{M}$, $\xi = \mu_0^{-1}\mu$.

LEMMA 4. *Let $\mathfrak{M}'$ be a finitely generated R-module in M' and let $b' \in K^*$. Then all solutions of the equation*

$$N_{M'/K}(\xi) = b' \quad \text{in } \xi \in \mathfrak{M}' \tag{17}$$

are contained in finitely many subsets of the form $(\xi' U_{M'}) \cap \mathfrak{M}'$, where ξ' is a solution of (17).

Proof. Our proof of Lemma 4 will contain similar arguments as those used by Laurent [14] in the proof of his Theorem 8. For convenience of the reader, we shall give the complete proof of Lemma 4. As before, $R_{M'}$ and R_K denote the integral closures of R in M' and in K, respectively.

By a theorem of Nagata [16], R_K and $R_{M'}$ are finitely generated over $\mathbf{Z}$. Further, they are integrally closed (in their quotient fields). Hence on both fields K, M' there exist sets of additive valuations $\mathscr{M}_K$, $\mathscr{M}_{M'}$ respectively, having the following properties:

$$R_K = \bigcap_{v_\mathfrak{p} \in \mathscr{M}_K} \{\alpha \in K : v_\mathfrak{p}(\alpha) \geqslant 0\}, \qquad R_{M'} = \bigcap_{V_\mathfrak{P} \in \mathscr{M}_{M'}} \{\alpha \in M' : V_\mathfrak{P}(\alpha) \geqslant 0\} \tag{18}$$

and

$$\begin{cases} \text{for } \alpha \in K^*, \ v_\mathfrak{p}(\alpha) \neq 0 & \text{for all but finitely many } v_\mathfrak{p} \in \mathscr{M}_K; \\ \text{for } \alpha \in M'^*, \ V_\mathfrak{P}(\alpha) \neq 0 & \text{for all but finitely many } V_\mathfrak{P} \in \mathscr{M}_{M'}. \end{cases} \tag{19}$$

Further, every $V_\mathfrak{P} \in \mathscr{M}_{M'}$ is an extension of some $v_\mathfrak{p} \in \mathscr{M}_K$. If $V_\mathfrak{P}$ is an extension of $v_\mathfrak{p}$ to M' we write $\mathfrak{P} \mid \mathfrak{p}$ and we say that $\mathfrak{P}$ divides $\mathfrak{p}$. For every $v_\mathfrak{p} \in \mathscr{M}_K$ and every $\xi \in M'^*$ we have

$$v_\mathfrak{p}(N_{M'/K}(\xi)) = \sum_{\mathfrak{P}\mid\mathfrak{p}} f_\mathfrak{P} V_\mathfrak{P}(\xi), \tag{20}$$

where the sum is taken over all $\mathfrak{P}$ dividing $\mathfrak{p}$, and where the $f_\mathfrak{P}$ are positive integers, the residue class degrees of the $\mathfrak{P}$'s with respect to M'/K.

For all solutions ξ of (17) and for every $v_\mathfrak{p} \in \mathscr{M}_K$, we have by (20)

$$\sum_{\mathfrak{P}\mid\mathfrak{p}} f_\mathfrak{P} V_\mathfrak{P}(\xi) = v_\mathfrak{p}(b'). \tag{21}$$

Since $\mathfrak{M}'$ is finitely generated over $\mathbf{Z}$, there are integers $c_\mathfrak{P}$ ($V_\mathfrak{P} \in \mathscr{M}_{M'}$), only finitely many of which are non-zero, such that $V_\mathfrak{P}(\xi) \geqslant c_\mathfrak{P}$ for all $\xi \in \mathfrak{M}'$. But, by (19), at most finitely many of the integers $v_\mathfrak{p}(b')$ are non-zero, hence (21) implies that there are only finitely many distinct tuples $(V_\mathfrak{P}(\xi) : V_\mathfrak{P} \in \mathscr{M}_{M'})$ with $\xi \in \mathfrak{M}'$ satisfying (17). In view of (18), two elements η_1, η_2 of M'^* satisfy $V_\mathfrak{P}(\eta_1) = V_\mathfrak{P}(\eta_2)$ for all $V_\mathfrak{P} \in \mathscr{M}_{M'}$ if and only if $\eta_2 = \varepsilon\eta_1$ for some $\varepsilon \in R_{M'}^*$. All solutions of (17) are therefore contained in finitely many sets of the type $\xi' R_{M'}^*$ with $\xi' \in M'^*$. We may assume that ξ' is a solution of (17). Then for any $\varepsilon \in R_{M'}^*$ for which $\xi'\varepsilon$ is a solution of (17) we have $N_{M'/K}(\varepsilon) = 1$. This shows that all solutions of (17) are contained in finitely many sets of the type $(\xi' U_{M'}) \cap \mathfrak{M}'$, where ξ' is a solution of (17). ∎

8. Proof of the Proposition. We shall establish two lemmas which are more general than necessary for proving the Proposition. We shall need these lemmas in a later paper.

We shall use the same notation as in Section 2. In particular, K is a field which is finitely generated over $\mathbf{Q}$ and G is a normal extension of K of finite degree g. For any linear form $l(X) = \alpha_1 X_1 + \ldots + \alpha_m X_m$ with $\alpha_1, \ldots, \alpha_m \in G$, the forms $l^{(i)}(X)$ are defined by $\sigma_i(\alpha_1) X_1 + \ldots + \sigma_i(\alpha_m) X_m$ $(i = 1, \ldots, g)$, where $\sigma_1, \ldots, \sigma_g$ are the distinct K-automorphisms of G. If $\mathscr{S}$ is a set of linear forms in $G[X_1, \ldots, X_m]$, we put $\mathscr{S}^{(i)} = \{l^{(i)} : l \in \mathscr{S}\}$. The set $\mathscr{S}$ is called *self-conjugate* if $\mathscr{S} = \mathscr{S}^{(1)} = \mathscr{S}^{(2)} = \ldots = \mathscr{S}^{(g)}$. In case $G = K$, $\mathscr{S}$ is trivially self-conjugate. The rank of a set $\mathscr{S}$ of linear forms with coefficients in G, denoted by $\mathrm{rank}_G(\mathscr{S})$, is defined as the maximal number of linear forms in $\mathscr{S}$ which are linearly independent over G. Let $\mathscr{V}(\mathscr{S})$ be defined as in Section 3.

LEMMA 5. *Let $\mathscr{S}$ be a self-conjugate set of linear forms in $G[X_1, \ldots, X_m]$. Then $\mathscr{V}(\mathscr{S})$ has a basis of linear forms with coefficients in K.*

Proof. Let $\{\omega_1, \ldots, \omega_g\}$ be a K-basis of G and let $l(X) \in \mathscr{S}$. Then there are linear forms $k_1(X), \ldots, k_g(X)$ with coefficients in K, such that $l(X) = \sum_{j=1}^{g} \omega_j k_j(X)$. Since $\mathscr{S}$ is self-conjugate, the forms $l^{(i)}(X) = \sum_{j=1}^{g} \sigma_i(\omega_j) k_j(X)$ $(i = 1, \ldots, g)$ also belong to $\mathscr{S}$. However, the determinant of the matrix with entries $\sigma_i(\omega_j)$ is non-zero. Hence $k_1(X), \ldots, k_g(X)$ can be expressed as linear combinations of $l^{(1)}(X), \ldots, l^{(g)}(X)$. Therefore $\mathscr{V}(\mathscr{S})$ is generated by linear forms with coefficients in K. This implies that $\mathscr{V}(\mathscr{S})$ has a basis of linear forms with coefficients in K. ∎

LEMMA 6. *Let $\mathscr{N}$, $\mathscr{N}'$, $\mathscr{N}_0, \mathscr{N}_1, \ldots, \mathscr{N}_{s-1}$ be finite, non-empty sets of non-zero linear forms in $G[X_1, \ldots, X_r]$ $(s \geqslant 1, r \geqslant 2)$ such that*

(22) *$\mathscr{N}$ is self-conjugate, $\mathscr{N} \subseteq \mathscr{N}'$, $\mathscr{N} = \mathscr{N}_0 \cup \mathscr{N}_1 \cup \ldots \cup \mathscr{N}_{s-1}$,*

(23) *if $s \geqslant 2$ then $\mathscr{V}(\mathscr{N}_i) \cap \big(\sum_{\substack{j=0 \\ j \neq i}}^{s-1} \mathscr{V}(\mathscr{N}_j)\big) = (\mathbf{0})$ for $i = 0, \ldots, s-1$.*

Then there exists an $\mathscr{N}'$-admissible, $\mathscr{N}$-degenerate subspace of K^r of dimension $\geqslant r - \operatorname{rank}_G(\mathscr{N}) + s$.

Proof. We shall prove Lemma 6 under the additional assumption that

(24) for each i in $\{0, \ldots, s-1\}$ and h in $\{1, \ldots, g\}$, there is an i' in $\{0, \ldots, s-1\}$ with $\mathscr{N}_i^{(h)} = \mathscr{N}_{i'}$.

For $s = 1$ or $g = 1$, (24) is trivially true. We shall now show that assumption (24) is no restriction when $s \geqslant 2$ and $g \geqslant 2$. To this end, we define sets $\mathscr{N}_{kj}$ $(k = 1, \ldots, g,\ j = 0, \ldots, s^k - 1)$ by

$$\mathscr{N}_{kj} = \mathscr{N}_{i_1}^{(1)} \cap \mathscr{N}_{i_2}^{(2)} \cap \ldots \cap \mathscr{N}_{i_k}^{(k)},$$

where $j = i_1 s^{k-1} + i_2 s^{k-2} + \ldots + i_k$ with integers $0 \leqslant i_1, \ldots, i_k < s$. Since $\mathscr{N}$ is self-conjugate, we have the relations

$$\mathscr{N}_{k-1,j} = \bigcup_{q=0}^{s-1} \mathscr{N}_{k,sj+q} \quad \text{for} \quad k = 2, \ldots, g;\ j = 0, \ldots, s^{k-1} - 1. \tag{25}$$

We shall show by induction on k that

$$\mathscr{V}(\mathscr{N}_{k,i}) \cap \Big(\sum_{\substack{r=0 \\ r \neq i}}^{s^k - 1} \mathscr{V}(\mathscr{N}_{k,r})\Big) = (\mathbf{0}) \quad \text{for} \quad i = 0, \ldots, s^k - 1. \tag{26}$$

By (23), (26) is obvious for $k = 1$. Suppose that (26) has been proved for $k = p-1$, say, where $p \geqslant 2$. Let $k = p$ and $0 \leqslant i \leqslant s^p - 1$. Write $i = sj + q$,

where $0 \leqslant q \leqslant s-1$ and $0 \leqslant j \leqslant s^{p-1} - 1$. Let

$$l \in \mathscr{V}(\mathscr{N}_{p,i}) \cap \Big(\sum_{\substack{r=0 \\ r \neq i}}^{s^p - 1} \mathscr{V}(\mathscr{N}_{p,r})\Big).$$

By (25) there are forms l_t in $\mathscr{V}(\mathscr{N}_{p,sj+t})$ $(0 \leqslant t \leqslant s-1,\ t \neq q)$ and $\tilde{l}$ in $\sum_{\substack{u=0 \\ u \neq j}}^{s^{p-1}-1} \mathscr{V}(\mathscr{N}_{p-1,u})$ such that

$$l = \sum_{\substack{t=0 \\ t \neq q}}^{s-1} l_t + \tilde{l}.$$

The form $l - \sum_{\substack{t=0 \\ t \neq q}}^{s-1} l_t$ belongs to

$$\mathscr{V}(\mathscr{N}_{p-1,j}) \cap \Big(\sum_{\substack{u=0 \\ u \neq j}}^{s^{p-1}-1} \mathscr{V}(\mathscr{N}_{p-1,u})\Big).$$

Together with the induction hypothesis, we obtain $l = \sum_{\substack{t=0 \\ t \neq q}}^{s-1} l_t$. We have, however, $l \in \mathscr{V}(\mathscr{N}_q^{(p)})$, $l_t \in \mathscr{V}(\mathscr{N}_t^{(p)})$ for $t \neq q$ and, by (23),

$$\mathscr{V}(\mathscr{N}_q^{(p)}) \cap \Big(\sum_{\substack{t=0 \\ t \neq q}}^{s-1} \mathscr{V}(\mathscr{N}_t^{(p)})\Big) = (\mathbf{0}).$$

This proves that $l = 0$. Hence (26) holds for $k = p$.

Another consequence of (25) is that for $k = 1, \ldots, g$, at least s sets among the $\mathscr{N}_{k,j}$ $(0 \leqslant j \leqslant s^k - 1)$ are non-empty. In view of (25), (26) it follows easily that (22), (23), (24) are satisfied if $\mathscr{N}_0, \ldots, \mathscr{N}_{s-1}$ are replaced by the non-empty sets among $\mathscr{N}_{g,0}, \ldots, \mathscr{N}_{g,sg-1}$. Since there are at least s of such non-empty sets, it suffices to prove Lemma 6 for these non-empty sets, instead of $\mathscr{N}_0, \ldots, \mathscr{N}_{s-1}$.

From now on, we shall assume that $\mathscr{N}_0, \ldots, \mathscr{N}_{s-1}$ satisfy (24), too. Let $\mathscr{N}_i^*$ $(i = 0, \ldots, s-1)$ be maximal subsets of $\mathscr{N}_0, \ldots, \mathscr{N}_{s-1}$ respectively, such that the forms in $\mathscr{N}_i^*$ are linearly independent and for all i in $\{0, \ldots, s-1\}$ and h in $\{1, \ldots, g\}$, $\mathscr{N}_i^{*(h)}$ is equal to one of the sets $\mathscr{N}_0^*, \ldots, \mathscr{N}_{s-1}^*$. Then, by (23), the forms in $\mathscr{N}^* = \mathscr{N}_0^* \cup \ldots \cup \mathscr{N}_{s-1}^*$ are linearly independent. For $i = 0, \ldots, s-1$ we construct spaces $\mathscr{W}_i$ of linear forms in $G[X_1, \ldots, X_r]$ as follows. Let

$$\mathscr{N}_i^* = \{l_{i1}, \ldots, l_{i,r_i}\} \quad (i = 0, \ldots, s-1).$$

If $\mathscr{N}_i^{*(h)} = \mathscr{N}_k^*$, say, then we assume that l_{kp} is obtained from l_{ip} by applying

σ_h to the coefficients of l_{ip}, for $p = 1, \ldots, r_i$ $(= r_k)$. Put $\mathscr{W}_i = (\mathbf{0})$ if $r_i = 1$ and if $r_i \geqslant 2$, let $\mathscr{W}_i$ be the vector space over G generated by the forms $l_{i2} - \xi_{i2} l_{i1}, \ldots, l_{i,r_i} - \xi_{i,r_i} l_{i1}$ for certain $\xi_{i2}, \ldots, \xi_{i,r_i} \in K$ which can be chosen so that

$$\mathscr{W}_k = \mathscr{W}_i^{(h)} \quad \text{if} \quad \mathscr{N}_k^* = \mathscr{N}_i^{*(h)}, \tag{27}$$

and

$$(\mathscr{W}_0 + \ldots + \mathscr{W}_{s-1}) \cap \mathscr{N}' = \emptyset. \tag{28}$$

Indeed, if $r_0 = \ldots = r_{s-1} = 1$ then (27), (28) are trivially satisfied. Suppose that $r_i \geqslant 2$ for some i. Condition (27) can be satisfied by choosing the ξ_{ip}'s so that $\xi_{ip} = \xi_{kp}$ whenever $\mathscr{N}_k^* = \mathscr{N}_i^{*(h)}$ for some h. Further, it is easily seen that in view of the linear independence of the forms in $\mathscr{N}^*$ and the finiteness of $\mathscr{N}'$, we can choose the tuple of ξ_{ip}'s to satisfy also (28). Putting $\mathscr{W} = \mathscr{W}_0 + \ldots + \mathscr{W}_{s-1}$, let V be the K-vector space defined by

$$V = \{x \in K^r\colon\ l(x) = 0 \text{ for all } l \in \mathscr{W}\}.$$

By (27), $\mathscr{W}$ is self-conjugate. This implies together with Lemma 5 that $\mathscr{W}$ has a basis of linear forms with coefficients in K. Hence V has dimension

$$r - \operatorname{rank}_G(\mathscr{W}) = r - (\operatorname{rank}_G(\mathscr{N}^*) - s) = r - \operatorname{rank}_G(\mathscr{N}) + s.$$

From Lemma 5 and from the fact that $\mathscr{W}$ has a basis of linear forms with coefficients in K, it follows that the linear forms in $G[X_1, \ldots, X_r]$ which vanish identically on V are exactly those belonging to $\mathscr{W}$. Together with (28) this shows that V is $\mathscr{N}'$-admissible. We shall complete the proof of Lemma 6 by showing that V is $\mathscr{N}$-degenerate. Firstly, all forms in $\mathscr{N}_i$ are linearly dependent on l_{i1} on V, for $i = 0, \ldots, s-1$. Secondly, $l_{01}, \ldots, l_{s-1,1}$ are linearly independent on V. For suppose that $\alpha_0 l_{01} + \ldots + \alpha_{s-1} l_{s-1,1} = 0$ identically on V, that is that $\alpha_0 l_{01} + \ldots + \alpha_{s-1} l_{s-1,1} \in \mathscr{W}$ for some $\alpha_0, \ldots, \alpha_{s-1} \in G$. Since the forms in $\mathscr{N}^*$ are linearly independent, we have $\alpha_i l_{i1} \in \mathscr{W}_i$ for $i = 0, \ldots, s-1$. In view of (28), this implies however that $\alpha_i = 0$ for $i = 0, \ldots, s-1$ which completes the proof of Lemma 6. ∎

Proof of the Proposition. Next suppose that $G = K$. First we prove the implication (i) → (ii). Suppose that (i) holds. If $\operatorname{rank}_K(\mathscr{L}_0) < m$, then, by Lemma 6 with $r = m$, $s = 1$, there exists an $\mathscr{L}$-admissible, $\mathscr{L}_0$-degenerate subspace of K^m of dimension $\geqslant m - \operatorname{rank}_K(\mathscr{L}_0) + 1 \geqslant 2$ which is impossible. Hence $\operatorname{rank}_K(\mathscr{L}_0) = m$. Suppose that there exists a proper, non-empty subset $\mathscr{L}_1$ of $\mathscr{L}_0$ with

$$\mathscr{V} \cap \mathscr{L} = \emptyset, \tag{29}$$

where

$$\mathscr{V} = \mathscr{V}(\mathscr{L}_1) \cap \mathscr{V}(\mathscr{L}_0 \setminus \mathscr{L}_1). \tag{30}$$

Let V be the subspace of K^m defined by

$$V = \{x \in K^m\colon\ l(x) = 0 \text{ for all } l \text{ in } \mathscr{L}\}.$$

There are no linear forms in $K[X_1, \ldots, X_m]$ vanishing identically on V other than those in $\mathscr{V}$. Hence, by (29), V is $\mathscr{L}$-admissible. Denote by r the dimension of V. Since, by (29), (30), $\dim \mathscr{V} < m$, we have $r = m - \dim \mathscr{V} \geqslant 1$. Let $A\colon\ K^r \to V$ be a bijective linear mapping. For any set $\mathscr{S}$ of linear forms in $K[X_1, \ldots, X_m]$, put

$$\mathscr{S}^A = \{lA\colon\ l \in \mathscr{S}\}.$$

Then $\mathscr{V}^A = (\mathbf{0})$ and, by (29), no form in $\mathscr{L}^A$ is identically zero. Further, we have by (30)

$$\mathscr{V}(\mathscr{L}_1^A) \cap \mathscr{V}((\mathscr{L}_0 \setminus \mathscr{L}_1)^A) = (\mathbf{0}).$$

Since $\mathscr{L}_1^A$ and $(\mathscr{L}_0 \setminus \mathscr{L}_1)^A$ are non-empty, this implies that $(\mathscr{L}_0 \setminus \mathscr{L}_1)^A = \mathscr{L}_0^A \setminus \mathscr{L}_1^A$. Thus

$$\mathscr{V}(\mathscr{L}_1^A) \cap \mathscr{V}(\mathscr{L}_0^A \setminus \mathscr{L}_1^A) = (\mathbf{0}),$$

where both sets $\mathscr{L}_1^A$, $\mathscr{L}_0^A \setminus \mathscr{L}_1^A$ are non-empty. But these sets consist of linear forms in r variables, hence $r \geqslant 2$. Moreover, $\mathscr{L}_0^A$ is self-conjugate. Together with Lemma 6 this implies that there is an $\mathscr{L}^A$-admissible, $\mathscr{L}_0^A$-degenerate subspace W of K^r of dimension at least 2. This shows that AW is an $\mathscr{L}$-admissible, $\mathscr{L}_0$-degenerate subspace of V of dimension $\geqslant 2$ which contradicts assertion (i) of the Proposition.

We shall now prove the implication (ii) → (i). Suppose that (ii) holds. Let V be an $\mathscr{L}$-admissible subspace of K^m of dimension $r \geqslant 2$ and let $A\colon\ K^r \to V$ be a bijective linear mapping. Then no form in $\mathscr{L}^A$ is identically zero. Denote by $\mathscr{L}_0'$ a maximal set of pairwise linearly independent linear forms in $\mathscr{L}_0^A$. Since $\operatorname{rank}_K(\mathscr{L}_0) = m$, we have $\operatorname{rank}_K(\mathscr{L}_0^A) = r$ and hence $\mathscr{L}_0'$ has cardinality at least 2. Let $\mathscr{L}_1'$ be a proper, non-empty subset of $\mathscr{L}_0'$. Let $\mathscr{L}_1$ be the largest subset of $\mathscr{L}_0$ with the property that each form in $\mathscr{L}_1^A$ is linearly dependent on one of the forms in $\mathscr{L}_1'$. Then each form in $(\mathscr{L}_0 \setminus \mathscr{L}_1)^A$ is linearly dependent on one of the forms in $\mathscr{L}_0' \setminus \mathscr{L}_1'$. From (ii) we infer that

$$\mathscr{V}(\mathscr{L}_1') \cap \mathscr{V}(\mathscr{L}_0' \setminus \mathscr{L}_1') \cap \mathscr{L}^A = \mathscr{V}(\mathscr{L}_1^A) \cap \mathscr{V}(\mathscr{L}_0 \setminus \mathscr{L}_1)^A \cap \mathscr{L}^A \neq \emptyset.$$

Thus

$$\mathscr{V}(\mathscr{L}_1') \cap \mathscr{V}(\mathscr{L}_0' \setminus \mathscr{L}_1') \neq (\mathbf{0}).$$

Therefore, there are linear forms $l_1, \ldots, l_p \in \mathscr{L}_1'$, $l_{p+1}, \ldots, l_q \in \mathscr{L}_0' \setminus \mathscr{L}_1'$ $(q > p \geqslant 1)$ such that

$$\sum_{i=1}^{p} \alpha_i l_i = -\sum_{i=p+1}^{q} \alpha_i l_i \neq 0,$$

whence

$$\sum_{i=1}^{q} \alpha_i l_i = 0 \quad \text{with non-zero } \alpha_i \in K \text{ for } i = 1, \ldots, q.$$

Since the forms in $\mathscr{L}'_0$ are pairwise linearly independent, we have $q \geqslant 3$. Hence K^r is $\mathscr{L}'_0$-non-degenerate. This implies however that V is $\mathscr{L}_0$-non-degenerate, which completes the proof of our Proposition. ∎

References

[1] J. H. Evertse, *On sums of S-units and linear recurrences*, Comp. Math. 53 (1984), pp. 225–244.

[2] J. H. Evertse and K. Győry, *On unit equations and decomposable form equations*, J. Reine Angew. Math. 358 (1985), pp. 6–19.

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

[4] – *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Applied Math. 56, Kingston, Canada 1980.

[5] – *On the representation of integers by decomposable forms in several variables*, Publ. Math. Debrecen 28 (1981), pp. 89–98.

[6] – *On S-integral solutions of norm form, discriminant form and index form equations*, Studia Sci. Math. Hungar. 16 (1981), pp. 149–161.

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

[8] – *Bounds for the solutions of norm form, discriminant form and index form equations*, Acta Math. Hungar. 42 (1983), pp. 45–80.

[9] – *On norm form, discriminant form and index form equations*, Coll. Math. Soc. J. Bolyai 34. *Topics in Classical Number Theory*, Budapest 1981. North-Holland Publ. Comp. 1984, pp. 617–676.

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

[11] – *Sur les générateurs des ordres monogènes des corps de nombres algébriques*, Séminaire de Théorie des Nombres, 1983–84, Univ. Bordeaux, No. 32, (1984), pp. 12.

[12] K. Győry and Z. Z. Papp, *Effective estimates for the integer solutions of norm form and discriminant form equations*, Publ. Math. Debrecen 25 (1978), pp. 311–325.

[13] S. Lang, *Fundamentals of diophantine geometry*, Springer Verlag, Berlin–Heidelberg–New York 1983.

[14] M. Laurent, *Equations diophantiennes exponentielles*, Invent. Math. 78 (1984), pp. 299–327.

[15] C. Lech, *A note on recurring series*, Archiv Math. 2 (1953), pp. 417–421.

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

[17] A. J. van de Poorten and H. P. Schlickewei, *The growth conditions for recurrence sequences*, Report 82.0041, Macquarie University, N. S. W. Australia, 1982.

[18] P. Roquette, *Einheiten und Divisorenklassen in endlich erzeugbar Körpern*, J. Deutsch. Math. Verein. 60 (1957), pp. 1–21.

[19] H. P. Schlickewei, *The p-adic Thue–Siegel–Roth–Schmidt theorem*, Archiv Math. 29 (1977), pp. 267–270.

[20] – *On norm form equations*, J. Number Theory 9 (1977), pp. 370–380.

[21] – *On linear forms with algebraic coefficients and diophantine equations*, ibid. 9 (1977), pp. 381–392.

[22] – *Inequalities for decomposable forms*, Astérisque 41–42 (1977), pp. 267–271.

[23] W. M. Schmidt, *Linear forms with algebraic coefficients, I*, J. Number Theory 3 (1971), pp. 253–277.

[24] – *Linearformen mit algebraischen Koeffizienten II*, Math. Ann. 191 (1971), pp. 1–20.

[25] – *Norm form equations*, Annals of Math. 96 (1972), pp. 526–551.

[26] – *Inequalities for resultants and for decomposable forms*, Proc. Conf. Diophantine approximation and its applications, Washington 1972. New York and London, 1973, pp. 235–253.

[27] – *Simultaneous approximation to algebraic numbers by elements of a number field*, Monatsh. Math. 79 (1975), pp. 55–66.

[28] – *Diophantine approximation*, Lecture Notes in Math. 785, Springer Verlag, 1980.

[29] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge University Press, 1986.

[30] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. 1929, pp. 1–41.

[31] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135 (1909), pp. 284–305.

CENTRE OF MATHEMATICS AND COMPUTER SCIENCE
PO Box 4079,
1009 AB Amsterdam, The Netherlands

KOSSUTH LAJOS UNIVERSITY
MATHEMATICAL INSTITUTE
4010 Debrecen, Hungary

Received on 3.7.1986
and in revised form on 27.10.1986 (1661)